

Kofax PSIsafe Desktop Installation Guide

Version: 12.2.0

Date: 2023-06-08

KOFAX

© 2022-2023 Kofax. All rights reserved.

Kofax is a trademark of Kofax, Inc., registered in the U.S. and/or other countries. All other trademarks are the property of their respective owners. No part of this publication may be reproduced, stored, or transmitted in any form without the prior written permission of Kofax.

Table of Contents

Preface.....	6
Product documentation.....	6
Offline mode.....	6
System requirements.....	7
Training.....	7
Getting help with Kofax products.....	7
Chapter 1: Kofax PSIsafe pre-installation reference.....	8
Configure firewall ports for PSIsafe.....	8
Configure antivirus and Windows permissions for PSIsafe.....	8
Permissions and exclusions by registry key names and program folders.....	9
PSIsafe Desktop.....	9
PSIsafe Web.....	10
PSIsafe API.....	10
PSIsafe Open API & 64-bit Server.....	10
PSIsafe Synchronizer.....	11
PSIsafe Books.....	11
Chapter 2: Install SQL Server.....	12
Configure PSIsafe Desktop ports.....	12
Install SQL Server.....	12
Install SQL Server Management Studio (SSMS).....	13
Configure SQL Server for PSIsafe Desktop.....	13
Configure existing SQL installation for PSIsafe Desktop.....	14
Upgrade SQL Express.....	14
Chapter 3: Install PSIsafe Desktop On-Premise Server.....	15
PSIsafe Desktop On-Premise server installation prerequisites.....	15
Windows Operating System installation prerequisites.....	15
Windows Server Operating System installation prerequisites.....	15
PSIsafe Desktop server installation procedure.....	16
Configure PSIsafe Desktop ports.....	16
Install new SQL instance.....	16
Initial SQL configuration.....	16
PSIsafe Desktop Server installation and database setup.....	16
PSIsafe Desktop server upgrade procedure.....	17
PSIsafe Desktop server full installation and existing database connection.....	17

PSIsafe Desktop server upgrade installation and existing database connection.....	17
Chapter 4: Install PSIsafe Desktop client.....	18
PSIsafe Desktop client installation prerequisites.....	18
PSIsafe Desktop client installation procedure.....	18
PSIsafe Desktop port exceptions.....	18
Install PSIsafe Desktop.....	18
PSIsafe Desktop client silent installation procedure.....	19
Discreet Uninstallations (No UI).....	20
PSIsafe Desktop client upgrade procedure.....	20
PSIsafe Desktop port exceptions.....	20
Upgrade PSIsafe Desktop client.....	20
Connect to PSIsafe Desktop server.....	21
Connect to database: on-premise installations.....	21
Connect to database: cloud installations.....	21
Register PSIsafe Desktop.....	21
Post-registration tasks.....	22
Log in to PSIsafe Desktop.....	22
Username and password settings.....	22
Chapter 5: Install PSIsafe Web.....	24
Chapter 6: Install PSIsafe API.....	25
Chapter 7: Install PSIsafe DocuSign.....	26
PSIsafe DocuSign prerequisites.....	26
PSIsafe DocuSign installation procedure.....	26
Initial Configuration (On-Premise Only).....	26
Configure DocuSign Administrator (Optional).....	26
Enable DocuSign Integration.....	27
Activate a PSIsafe DocuSign User.....	27
Use PSIsafe DocuSign and Grant Consent.....	28
Chapter 8: Install PSIsafe Open API and 64-bit server.....	29
PSIsafe Open API and 64-bit server installation and upgrade.....	29
PSIsafe Open API and 64-bit Server installation prerequisites.....	29
PSIsafe Open API 64-bit server installation procedure.....	30
On-premise installation without customer code example.....	30
Cloud installation with customer code example.....	30
Install PSIsafe Open API and verify connection.....	30
Optional configuration for separate API and server locations.....	31
Verify connection.....	31
Chapter 9: Install PSIsafe Mobile Client.....	32

PSIsafe Desktop Mobile Client installation prerequisites.....	32
PSIsafe Mobile Client installation procedure.....	32
Chapter 10: Install PSIsafe Synchronizer.....	34
PSIsafe Synchronizer prerequisites.....	34
Pre-configuration considerations for PSIsafe Synchronizer.....	34
PSIsafe Synchronizer installation procedure.....	35
Chapter 11: Install PSIsafe Books.....	37
PSIsafe Books installation prerequisites.....	37
PSIsafe Books installation procedure.....	37
Connect to your PSIsafe Desktop database.....	38
Chapter 12: Install PSIsafe Retriever.....	39
Pre-configuration considerations.....	39
Configure PSIsafe Retriever.....	39
Chapter 13: Install PSIsafe PDF Forms Monitor.....	42
Installation process.....	42
Prepare database.....	42

Preface

This guide provides instructions for administrators who are responsible for installing Kofax PSIsafe applications and components.


Product documentation

The documentation set for Kofax PSIsafe is available here:

<https://docshield.kofax.com/Portal/Products/PSIsafe/12.2.0-tqza8tn68d/PSIsafe.htm>

The full set of Kofax PSIsafe documentation includes:

- *Kofax PSIsafe Release Notes*
- *Kofax PSIsafe Technical Specifications*
- *Kofax PSIsafe Installation Guide*
- *Kofax PSIsafe User Help*
- *Kofax PSIsafe Administrator Help*

 If the security policy for your organization restricts Internet access or the Internet connection is not stable, you can access the documentation in [offline mode](#) while using Kofax PSIsafe products.

Offline mode

To make the documentation available for use in offline mode, obtain the following file from the Kofax PSIsafe product package that you downloaded from the [Kofax Fulfillment Site](#).

- KofaxPSIsafeDocumentation_12.2.0_EN.zip

Copy the .zip file to your computer and extract the contents:

- `Print` folder: Includes the *Kofax PSIsafe Installation Guide*.
- `Help` folder: Includes the *Kofax PSIsafe Help* and *Kofax PSIsafe Administrator Help*.

System requirements

The primary source of information about system requirements is the *Technical Specifications* document, which is available on the [Kofax PSISafe Product Documentation site](#). The document is updated regularly, and we recommend that you review it carefully to ensure success while working with your Kofax PSISafe product.


Training

Kofax offers both classroom and online training to help you make the most of your product. To learn more about training courses and schedules, visit the [Kofax Education Portal](#) on the Kofax website.

Getting help with Kofax products

The [Kofax Knowledge Portal](#) repository contains articles that are updated on a regular basis to keep you informed about Kofax products. We encourage you to use the Knowledge Portal to obtain answers to your product questions.

To access the Kofax Knowledge Portal, go to <https://knowledge.kofax.com>.

 The Kofax Knowledge Portal is optimized for use with Google Chrome, Mozilla Firefox, or Microsoft Edge.

The Kofax Knowledge Portal provides:

- Powerful search capabilities to help you quickly locate the information you need.
Type your search terms or phrase into the **Search** box, and then click the search icon.
- Product information, configuration details and documentation, including release news.
To locate articles, go to the Knowledge Portal home page and select the applicable Solution Family for your product, or click the View All Products button.

From the Knowledge Portal home page, you can:

- Access the Kofax Community (for all customers).
On the Resources menu, click the **Community** link.
- Access the Kofax Customer Portal (for eligible customers).
Go to the [Support Portal Information](#) page and click **Log in to the Customer Portal**.
- Access the Kofax Partner Portal (for eligible partners).
Go to the [Support Portal Information](#) page and click **Log in to the Partner Portal**.
- Access Kofax support commitments, lifecycle policies, electronic fulfillment details, and self-service tools.
Go to the [Support Details](#) page and select the appropriate article.

Chapter 1

Kofax PSISafe pre-installation reference

Most businesses will operate the Kofax PSISafe product family with their own unique workstation and network security policies. To avoid any issues, all environments hosting PSISafe products must have their firewall, antivirus, and filesystem permissions configured.

Configure firewall ports for PSISafe

The following firewall ports must be configured to allow all the applications within the PSISafe product family to send and receive traffic across the network. Consult your IT Administrator to adjust firewall rules for your unique environment.

1. Open the **Windows Defender and Firewall with Advanced Security** application.
2. Right-click **Inbound Rules** and select **New Rule**.
The new inbound rule wizard appears.
3. In the **Steps** section, select **Rule Type**.
4. Select the **Port** rule type, then select **Protocol and Ports**.
5. Select **TCP/IP**.
6. In the **Specific local ports** field enter the following values.
 - **8993-8994** (Service Ports)
 - **11000** (.NET remoting)
 - **1433** (SQL Service)
7. Select **UDP**.
8. In the **Specific local ports** field enter the following value.
 - **1434** (SQL Browser Service)
9. Repeat the same procedure to set up the **Outbound Rules**.

Configure antivirus and Windows permissions for PSISafe

Antivirus software can interfere with the functionality of PSISafe Desktop, as well as other PSISafe products. It's important to exclude active scanning or heuristic intrusion prevention scanning (HIPS) only on the folders that PSISafe products use to store temporary files.

Additionally, the Windows operating system, depending on the version used, requires permissions to be configured for all applications within the PSISafe product family. Users only need access to the PSISafe Desktop client locations and executables, but backend services and registry values need read/write access to the installation folders and temporary file locations. This may require altering the listed services to log on as a designated Administrator account to achieve the required access. Most Active Directory group policy and security policies are adjusted only for more restricted environments. Most functionality will operate without issue as long as the programs are installed through an Administrator-level account.

i All directories and service names in the following sections are stated as their default values. Your unique installation may have altered paths or customized locations. Consult your IT Administrator to add exclusions for any program folders, registry entries, or executables.

Permissions and exclusions by registry key names and program folders

The PSISafe product family uses the following registry key name folders, each of which includes subfolders for different products. Each corresponding application service, or the user designated to log on for that service, must have read/write permissions to their respective registry entries. Granting access to the root folders listed below is the safest and simplest option. Some legacy product key names are included, but may not apply to your installation.

Local machine registry key names:

```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Cabinet NG  
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Kofax Inc.  
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Kofax, Inc.  
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\PSIGEN Software, Inc.
```

Current user registry key names:

```
HKEY_CURRENT_USER\SOFTWARE\Black Ice Software LLC  
HKEY_CURRENT_USER\SOFTWARE\Cabinet NG  
HKEY_CURRENT_USER\SOFTWARE\CNG-SAFE
```

PSISafe Desktop

Server

Installation folder:

```
C:\Program Files (x86)\CNG\CNGServer
```

Service:

CNG-FullTextSearchService

CNG-ServerService

CNG-WorkflowService

Client

Installation folder:

C:\Program Files (x86)\CNG\CNG-SAFE

Settings folder:

C:\Users\[USERNAME]\AppData\Roaming\CNG

Upgrade installer temporary storage:

C:\Users\[USERNAME]\AppData\Local\PSIGEN_Software_Inc

PSISafe Web

The PSISafe Web site files are stored in a folder determined during installation. By default, some use installation folder:

C:\Program Files (x86)\PSIGEN Software, Inc\PSISafe Web

Legacy PSISafe Web Lite default installation folder:

C:\Program Files (x86)\PSIGEN Software, Inc\PSISafe Web Lite

PSISafe API

The PSISafe API files are stored in a folder determined during installation. By default, some use installation folder:

C:\Program Files\PSISafe

Settings folder:

C:\Program Files\PSISafe\AffinityAPI

PSISafe Open API & 64-bit Server

Installation folder:

C:\Program Files\Cabinet\OpenApi

C:\Program Files\Cabinet\Server

Settings folder:

C:\Program Files\Cabinet\Server

PSIsafe Synchronizer

Installation folder:

C:\Program Files (x86)\CNG\Synchronizer

Settings folder:

C:\Users\[USERNAME]\AppData\Roaming\CNG

PSIsafe Books

Installation folder:

C:\Program Files (x86)\CNG\CNG-Books

Settings folder:

C:\Users\[USERNAME]\AppData\Roaming\CNG

Chapter 2

Install SQL Server

This chapter describes how to prepare your computer to host a Kofax PSIsafe Desktop on-premise server. A SQL Server is required to operate a PSIsafe Desktop Server.

Microsoft SQL Server is the backbone of the Kofax PSIsafe Desktop metadata management architecture. SQL Servers are recognized across the data management industry as a leading solution for storing and managing large volumes of indexed data. Tables within SQL databases house the indexing information stored and displayed within PSIsafe Desktop, and they pair each set of metadata with the corresponding files housed on the data storage volume of your choice. None of your stored content is housed within your SQL database, which contains only the associated metadata.

SQL Servers can be hosted on the computer running your PSIsafe Desktop Server, or on any computer to which the PSIsafe Desktop Server can establish a valid connection. This could be intra-network, over a VPN, or in a cloud-hosted environment. The computer hosting PSIsafe Desktop must have communication access over a network for the corresponding SQL protocols to complete a PSIsafe Desktop Server installation. Ensure that your network IT administrator allows for all corresponding port exceptions within your network firewall, both at a hardware and software level.

Configure PSIsafe Desktop ports

Before proceeding, be sure you have configured your environment for PSIsafe Desktop by following all the steps in [Kofax PSIsafe pre-installation reference](#).

Install SQL Server

Use this procedure to install SQL Server.

1. Download the latest SQL Server version compatible with PSIsafe Desktop from the **Microsoft SQL Server Download** website.
Select SQL Express or SQL Standard, depending on your installation type and purchased licensing.
2. Unblock the installer you downloaded, and select **Run as Administrator**. Then click **Download Media** in the SQL Server installer.
This action downloads the SQL Server Installation Center to the specified location.
3. Click **Download** and, after the download is complete, open the download location by clicking **Open Folder**.
Alternatively, you can manually browse to the download location in File Explorer.

4. Unblock the executable and select **Run as Administrator**.
5. Select **Yes** to allow the installed application to make changes.
6. Set a directory for extracting the SQL Express installation files.
7. Click **OK** to start extracting the files.
The installer window opens automatically.
8. Follow the instructions in the **SQL Server Installation Center**.
9. In the **Installation** section, select **New SQL Server stand-alone installation or add features to an existing installation**.
10. Select **I accept the license terms**.
Click **Next**.
11. In the **Microsoft Update** section, select the **Use Microsoft Update to check for updates** check box and click **Next**.
12. If Windows Firewall displays a warning message, you can ignore it and click **Next** to proceed.
13. In the **Feature Selection** section, confirm the default settings by clicking **Next**.
14. In the **Instance Configuration** section, type **PSIsafe** in the **Named Instance** field and **PSISAFE** in the **Instance ID** field.
Click **Next**.
15. In the **Server Configuration** section, change the SQL Server Browser Startup Type to **Automatic** and click **Next**.
Click **Next**.
16. In the **Database Engine Configuration** section, select the **Mixed Mode** check box and set the password to **Admin-01**. Click **Next** and wait for the installation to complete.

Install SQL Server Management Studio (SSMS)

To install the SQL Server Management Studio:

1. Download the SQL Server Management Studio from the Microsoft SQL Download Portal.
2. Browse to the download folder and launch the SQL Server Management Studio installer.
3. Select **Yes** to allow the installation application to make changes.
4. Select **Install** to start the installation process.
5. After all of the components are installed, click **Close**.

Configure SQL Server for PSIsafe Desktop

Some configuration changes are necessary in the SQL Server Configuration Manager to ensure PSIsafe Desktop can communicate properly over the network. To make configuration adjustments, perform the following actions.

1. To open the SQL Server Configuration Manager, type **Configuration Manager** in the **Start** menu, or browse to the following path: `C:\Windows\SysWOW64\SQLServerManagerXX.msc`.
2. Select **SQL Server Network Configuration > Protocols for PSISAFE**.
3. Right-click **TCP/IP** and select **Enabled**.

4. In some environments and installations, you may need to enable **Named Pipes**.
5. When the warning message appears, click **OK**.
6. Restart the SQL Server (PSISAFE) service. To do so, in the SQL Server Configuration Manager, select **SQL Server Services > SQL Server (PSISAFE)**. Right-click and select **Restart**.
7. You may need to set the logon type for **SQL Server Browser** on the **SQL Server Services** tab to **Automatic**.

Configure existing SQL installation for PSISafe Desktop

To change configurations for your existing SQL installation:

1. Make all of the required SQL Server Configuration Manager changes as described in [Install SQL Server](#).
2. Open the SQL Server Management Studio and log in as either an authorized user or the system administrator.
3. Right-click the instance name and select **Properties**.
4. Under the **Security** section and **Server authentication**, select **SQL Server and Windows Authentication mode**.
5. Under the **Connections** section, select the **Allow remote connections to this server** check box.

Upgrade SQL Express

Follow the steps below to upgrade from SQL Express to SQL Standard or Enterprise.

1. To upgrade your SQL Express installation, use the same installer as for deploying a new installation. In the **SQL Server Installation** screen, select **Maintenance > Edition Upgrade**.
2. When prompted, enter your purchased Microsoft SQL Standard or Enterprise key. The installation upgrade process will proceed automatically.

Chapter 3

Install PSISafe Desktop On-Premise Server

This chapter describes the PSISafe Desktop On-Premise Server installation prerequisites and procedure.

PSISafe Desktop On-Premise server installation prerequisites

This topic lists components and required configuration settings to install PSISafe Desktop on your computer and ensure full program functionality.

Windows Operating System installation prerequisites

To ensure that the installation can be completed, first make sure to activate all of the required Windows features.

Open the **Windows Features** configuration area via Control Panel or Search from the Start window. When the dialog window is displayed, select the following features:

- **.NET Framework 3.5**
- **.NET Framework 4.8 Advanced Services**
- In **Internet Information Services > World Wide Web Services > Application Development Features**, select **.NET Extensibility 3.5**, **.NET Extensibility 4.8**, **ASP.NET 3.5**, and **ASP.NET 4.8**.
- In **Internet Information Services > World Wide Web Services > Common HTTP Features**, select **Static Content**.

Windows Server Operating System installation prerequisites

i PSISafe Desktop servers cannot run on Windows Server operating systems dedicated as domain controllers, because of the conflict where the PSISafe Desktop server service cannot properly license a required module without a local user present.

To set the required features, log in as an administrator on the server. Open Server Manager, select **Add roles and features**, and then select the following roles and features:

- **.NET Framework 3.5**
- **.NET Framework 4.8 Advanced Services**
- In **Internet Information Services > World Wide Web Services > Application Development Features**, select **.NET Extensibility 3.5**, **.NET Extensibility 4.8**, **ASP.NET 3.5**, and **ASP.NET 4.8**.

- In **Internet Information Services > World Wide Web Services > Common HTTP Features**, select **Static Content**.

PSIsafe Desktop server installation procedure

Check the following before proceeding with the PSIsafe Desktop Server installation process.

Configure PSIsafe Desktop ports

Before proceeding, ensure you have configured the firewall ports for PSIsafe Desktop as described in the [Install SQL Server](#) topic.

Install new SQL instance

Before proceeding, ensure you have installed Microsoft SQL. See [Install SQL Server](#).

Initial SQL configuration

Before proceeding, you must configure PSIsafe Desktop for SQL server. See [Configure SQL Server for PSIsafe Desktop](#).

PSIsafe Desktop Server installation and database setup

To install the PSIsafe Desktop server, right-click the PSIsafe Desktop server installer and select **Properties**. In the **Properties** window, click **Unblock** and then click **OK**.

1. Right-click the executable and select **Run as Administrator**.
2. Follow the installer prompts and complete the initial installation with the default settings. After the initial installation is complete, a **Kofax PSIsafe Desktop Server Setup** window appears.
3. Click **Next** in the **Kofax PSIsafe Desktop Server Setup** window when it appears towards the end of the installation.
4. In the second **Kofax PSIsafe Desktop Server Setup** screen, enter your SQL Server location, such as the IPv4 address or IPv6 machine name, relative to the computer on which you are installing the PSIsafe Desktop server.
For new installations, ensure that the **Skip SQL Database Creation** check box is cleared (not checked). This ensures that a database with the specified database name is created and associated with your PSIsafe Desktop server.
In the event that you already have a database created, you can select the box to **Skip SQL Database Creation** and associate the existing database in this step instead.
5. Click the **Test Connection** button to check if your PSIsafe Desktop server installation can make a valid connection to your SQL server instance.
Click **Next** to complete the database setup.

PSIsafe Desktop server upgrade procedure

This topic assumes that an existing PSIsafe Desktop server is installed and the environment is configured appropriately. Upgrade installers are included with the default installation package available from Kofax.

PSIsafe Desktop server full installation and existing database connection

If you need to perform a full installation of PSIsafe Desktop, see [PSIsafe Desktop server installation procedure](#).

PSIsafe Desktop server upgrade installation and existing database connection

To upgrade an existing installation of the PSIsafe Desktop server:

1. Right-click the PSIsafe Desktop server upgrade installer and select **Properties**. In the **Properties** window, click **Unblock** and then click **OK**.
2. Right-click the upgrade installer executable and select **Run as Administrator**.
3. Follow the installer prompts and complete the upgrade with the default settings. This completes the server upgrade process.

Chapter 4

Install PSIsafe Desktop client

This chapter describes the PSIsafe Desktop installation prerequisites and procedures that give you access to an on-premise or cloud-based PSIsafe Desktop installation with a previously installed PSIsafe Desktop Server. For more information on the PSIsafe Desktop Server installation, see [Install the PSIsafe Desktop On-Premise Server](#).

PSIsafe Desktop client installation prerequisites

The following is a list of prerequisites for the PSIsafe Desktop installation.

- PSIsafe Desktop On-Premise server or Cloud-hosted server v12.2.0 installed and connected to a SQL database.
- .NET Framework 4.8 and higher
- .NET Framework 3.5

PSIsafe Desktop client installation procedure

Right-click the PSIsafe Desktop standalone installer and select **Properties**. In the **Properties** window, select **Unblock**.

After you unblock the installer, right-click it and select **Run as Administrator**.

PSIsafe Desktop port exceptions

Before proceeding, you must configure your firewall ports and antivirus for use with PSIsafe Desktop. See [Kofax PSIsafe pre-installation reference](#).

Install PSIsafe Desktop

Be sure to review the following points before proceeding to install the PSIsafe Desktop client.

- If you installed the Black Ice Printer Driver previously, go to **Printers & Scanners** to uninstall it before installing with the standalone installer.
- If you are upgrading a previous version of PSIsafe Desktop with the standalone installer, go to **Programs and Features** to uninstall the previous version.
- If you are performing an upgrade using the upgrade installer, make sure that your installation directory for your current installation is set in place of the default path, or, change the directory

to your custom installation location when prompted, and follow the steps in [PSIsafe Desktop client upgrade procedure](#).

Installation steps:

1. Run the PSIsafe Desktop executable as an Administrator.
2. Click **Install** to start the installation.
3. Follow the installation steps with the default settings.
Complete the installation process with the default options.

PSIsafe Desktop client silent installation procedure

Our installer uses a bootstrapper to handle the prerequisites and then kick off the main MSI installer. This topic explains the command line parameters available for our bootstrapper, as well as additional parameters that can be passed to the MSI. Discreet Installations (No UI) for PSIsafe Desktop via MSI installation packages are included with the default installation package.

Since .MSI command line parameters must be used, syntax for a simple discreet installation might look something like this:

```
PSIsafe.Client.Install.12.1.2.1004.exe /extract "C:\PSIsetup" cd "C:\PSIsetup"  
msiexec /a "PSIsafeWindowsClient.msi" /qn /l*v c:\silent.log
```

This will use the default directory in which the .MSI resides.

Alternatively, you can specify a specific installation directory instead:

```
msiexec /a "PSIsafeWindowsClient.msi" APPLICATIONFOLDER="C:\Program Files (x86)\PSIsafe\  
\\" /qn /l*v c:\silent.log.
```

i The silent .MSI install doesn't set an internal **APPDIR** value and defaults to **C:**, so it's important to use the above method to specify the installation directory.

For example, by calling **msiexec** as follows, we can perform a silent installation of PSIsafe Desktop 12.2.0.1007:

```
msiexec.exe /i "PSIsafe.Client.Install.12.2.0.1007.msi APPDIR="C:\Program Files  
(x86)\CNG\CNG-SAFE\" /qn /l*v c:\silent.log.
```

Variables include PSIsafe Desktop Client version and **APPDIR** parameters. Additional commands/parameters may be necessary to account for permissions and other elements of your unique environment. This process should be completed by your internal IT department.

i There are two methods of installing an .MSI discreetly, the command parameter **/i** after **msiexec** installs the application normally as the current user, whereas the parameter **/a** installs an Administrator and can be done over a network. This may be an important consideration for your unique environment.

Discreet Uninstallations (No UI)

There are two commonly used methods for uninstalling the PSIsafe Desktop client discreetly. The first mirrors the above example and employs MSI Command line parameters, substituting the **/i** or **/a** installation parameter with the **/x** uninstallation parameter:

```
msiexec /x "PSIsafeWindowsClient.msi" /qn /l*v c:\silent.log
```

The extraction and location of the original EXE used for the installation, as mentioned in the previous section, are necessary. Specify this with the same parameter, unless you have already used the **cd** command line entry to specify a working directory:

```
msiexec /x "PSIsafeWindowsClient.msi" APPLICATIONFOLDER="C:\Program Files (x86)\PSIsafe\" /qn /l*v c:\silent.log
```

The second commonly used method for uninstalling programs discreetly is through **Windows Management Instrumentation**, which allows for the uninstallation of applications via a reference name. An example of a discreet uninstallation command line using **Windows Management Instrumentation** would be:

```
wmic product where name="SAFE" call uninstall /nointeractive
```

PSIsafe Desktop client upgrade procedure

Right-click the PSIsafe Desktop upgrade installer and select **Properties**. In the **Properties** window, select **Unblock**.

After you unblock the installer, right-click it and select **Run as Administrator**.

PSIsafe Desktop port exceptions

In most cases when performing an upgrade your firewall ports and antivirus are already configured for use with PSIsafe Desktop. See [Kofax PSIsafe pre-installation reference](#).

Upgrade PSIsafe Desktop client

Be sure to review the following points before proceeding to upgrading the PSIsafe Desktop client.

- If you installed the Black Ice Printer Driver previously, go to **Printers & Scanners** to uninstall it before installing with the standalone installer.
- If you are upgrading a previous version of PSIsafe Desktop with the standalone installer, go to **Programs and Features** to uninstall the previous version and follow the steps in [PSIsafe Desktop client installation procedure](#).

Upgrade steps:

1. Run the PSIsafe Desktop upgrade executable as an Administrator and click OK to extract the upgrade installer.

The **Kofax PSIsafe Client 12.2 Update** window appears.

Be sure to note the default client installation directory displayed, and if your existing version of PSIsafe Desktop client is installed in a different location, change this path accordingly.

2. Click **Update** to start the upgrade process.
The upgrade process completes automatically.

Connect to PSIsafe Desktop server

The connection configuration process will vary depending on whether your installation is on-premise or cloud-hosted.

The **Connection Configuration** window appears when you first open the PSIsafe Desktop client. If the **Connection Configuration** window does not appear, click the gear icon in the bottom-right of the window and select **Connection Configuration**.

Connect to database: on-premise installations

1. Select **On-premise**.
2. Type the IPv4 address of your local server or the IPv6 computer name.
3. Confirm that the **Customer code** remains "default" as this function is not used for on-premise installations.
4. Click **Save** to apply the changes.


Connect to database: cloud installations

1. Select **Cloud**.
2. Confirm that the PSIsafe Desktop server IP address is not be entered.
3. Enter the **Customer code** provided by your Kofax representative.
4. Click **Save** to apply the changes.

For advanced settings, contact Kofax Support for assistance with configuring connections to reserved, beta, or specialized PSIsafe Desktop Cloud installations, as well as recommendations for adjusting ports and TCP/HTTP connection protocols from their default values.

Register PSIsafe Desktop

The process of licensing PSIsafe Desktop is called **Registration** within the product. **Registration** requires assistance from Kofax Support.

 Skip this section if your installation is already registered and in use.

1. Open PSIsafe Desktop client or Kofax PSIsafe Management after completing the installation process.
2. Click the gear icon and select **System settings**.
The **System settings** window appears with the **Database Connections\Registration** tab selected.
3. Type the default or customized system password and the server IPv4 address or IPv6 computer name.

4. Click **List** and select **Add**.
5. Enter the relevant information into each field, including the **SQL Server, Database**, SQL sysadmin account credentials, and company name.
6. Click **Generate Code**, copy the code to your clipboard, and then contact Kofax Support for your key.
7. Enter the key and click **Register** to finish the registration.

Post-registration tasks

The following tasks are recommended after registering your PSIsafe Desktop installation for the first time.

1. Set up an administrator account designated to an individual responsible for handling configuration and setup changes to PSIsafe Desktop. See the [PSIsafe Administrator Help](#) for more information.
2. Change the system Administrator password from the default to a company-managed password that meets your compliance policies. See the [PSIsafe Administrator Help](#) for more information.
3. Review your organization's compliance policy requirements for user passwords and begin tailoring new user accounts accordingly.
4. Install and configure any database synchronization applications for PSIsafe, such as Kofax PSIsafe Synchronizer, or import metadata through Kofax PSICapture to establish a baseline collection of relevant file structures that are suited to your business needs.

Log in to PSIsafe Desktop

After launching PSIsafe Desktop, the login window appears.

i After entering the connection configuration information, you may need to close PSIsafe Desktop and open it again to refresh your connection attempt. You can also use the **Refresh** button on the right side of the **Connect to** field.

Enter the user name and password provided by your PSIsafe Desktop Administrator. Administration of users occurs through PSIsafe Management. In some cases when first logging in, you are prompted to change your password.

i If you need to create a new user name and password, log in to PSIsafe Management and see the **Users** topic of the [PSIsafe Administrator Help](#) for more information. .

Username and password settings

Users can change and reset their own passwords when the corresponding setting is enabled in PSIsafe Management. When password reset is enabled, the Login screen will display **Forgot your password?**

Many parameters are configurable in PSIsafe Management including:


- **Enable Password Reset:** When checked, “Forgot your password?” is displayed and end users are able to reset their passwords without assistance.
- **Enable Password Security Challenge:** Provides an additional layer of security by randomly presenting any one of three user defined challenges that must be answered. An administrator must define the challenges/answers prior to being able to use the Password Reset Security Challenge.
- **Password Policy:** Enforces minimum password requirements.

Change a password

1. To change a password, click the ellipsis next to the **Password** field.
2. Enter the **Old Password**, **New Password**, and **Confirm Password** fields accordingly.
If a password policy is enabled, the user can view the minimum requirements by clicking the **Policy Info** button.
3. Click **Save** to complete the password change process.

Save a username for automatic login

1. To save a username, click the ellipsis next to the **Username** field.
2. Check the box for **Automatic Login** as needed.

 To disable Automatic Login, press and hold the control key while launching PSIsafe Desktop.

Chapter 5

Install PSIsafe Web

For a full set of documentation, see the [PSIsafe Web Installation Guide](#) on the [Kofax PSIsafe Product Documentation](#) page.

Chapter 6

Install PSIsafe API

For a full set of documentation, see the [PSIsafe API Installation Guide](#) on the [Kofax PSIsafe Product Documentation](#) page.

Chapter 7

Install PSISafe DocuSign

This chapter describes the PSISafe DocuSign installation prerequisites and procedures.

PSISafe DocuSign prerequisites

The following is a list of prerequisites for PSISafe DocuSign.

- Ensure you have an active DocuSign account. You need administrative access to the system settings to retrieve certain settings.
- PSISafe Desktop and Server 12.1.2.1002 and higher.
- PSISafe 64-bit server and the PSISafe Open API version 12.1.1.1002 and higher.
 - For PSISafe Desktop Cloud customers, this prerequisite is already installed and configured.
 - For PSISafe Desktop on-premise customers, this prerequisite is required. For information on installing and configuring the PSISafe 64-bit server and PSISafe Open API prerequisites, see [Install PSISafe Open API and 64-bit server](#).

PSISafe DocuSign installation procedure

PSISafe Desktop administrators can use this section to install the product and perform the initial configuration.

The first step before proceeding with the PSISafe DocuSign installation is to determine whether your installation is on-premise or cloud-based. If your installation is on-premise, proceed to the steps below. If your installation is cloud-based, skip to next section entitled **Configure DocuSign Administrator (Optional)**.

Initial Configuration (On-Premise Only)

1. The **PSISafe URI** setting must be configured to match your PSISafe Open API installation. Specify the correct **PSISafe URI** in PSISafe Management under **System > Settings > Options > Paths**.
2. Under the **PSISafe URI** field, ensure that this value matches the network location of the PSISafe Open API or PSISafe API depending on your version and configuration.

Configure DocuSign Administrator (Optional)

1. In PSISafe Management, log in as the global PSISafe Desktop Administrator.
2. Navigate to **User Settings > Users**.

3. Select and edit the user to be granted administrative access to PSIsafe DocuSign.
4. Navigate to **Account Permissions and Settings: Step 2 of 4** for this user account.
5. To enable the **Administrator Only** tab, a user must first be a PSIsafe Desktop Administrator. Enable this check box to continue.
6. From the Administrators Only tab, select the DocuSign Configuration to enable the DocuSign section within PSIsafe Management for this user.

Enable DocuSign Integration

1. From PSIsafe Management, select DocuSign / Configuration to display the DocuSign Configuration screen.
2. Fill out all fields, as every field is required. See your DocuSign administrator for this information.
3. Once each field is properly filled, click the **Grant Consent** button.

Here is a breakdown of each field on this screen with a description:

DocuSign URL	The DocuSign API URL for the environment you are working with (test or production). In DocuSign, select Settings / APP and Keys and copy the value in the Base URI field (see below).
DocuSign OAuth URL	The DocuSign OAuth URL for the environment you are working with (test or production) (see below for location in DocuSign).
Test button	Populates each of the above URL fields with the default value used during testing.
Production button	Populates the DocuSign OAuth URL field with the default value for production.
DocuSign account user ID	The API Account ID value for the account owner. In DocuSign, select Settings / APP and Keys and copy the value in the API Username field (see step 1 of the next section).
Use the Envelope Name as the default email subject	As detailed in later sections, the user must enter a "friendly name" when creating an envelope. Select this option to set the envelope's email subject in DocuSign to this friendly name. Envelopes in the DocuSign application are listed by email subject, so this option allows users to quickly locate their envelope.
Grant Consent button	Grants consent for PSIsafe Desktop to access your DocuSign account.
Save Settings	Saves the settings.

To find this content in the DocuSign web interface, browse to **Settings > Integrations > Apps and Keys**.

Activate a PSIsafe DocuSign User

To submit envelopes, a PSIsafe Desktop Administrator must first configure the PSIsafe Desktop user and associate the required DocuSign User GUID value.

i This procedure requires a DocuSign user account preconfigured at minimum with the **DocuSign Sender (DS Sender)** permission profile rights.

1. Ask your DocuSign administrator to provide the API Username value that corresponds to your PSIsafe user account.
 - a. To find this value, navigate to **Settings > Users and Groups > Users**.
 - b. With all user accounts visible, select the appropriate DocuSign user account (or create one if necessary).
 - c. Within the User Profile screen, copy the API Username value.
2. From PSIsafe Management, select the DocuSign access checkbox within the user's settings. (**User Settings > Users > Edit User > All Users Tab**).
3. Finally, enter the user's API username value from DocuSign in the DocuSign user GUID field. Edit the PSIsafe user in question to display details, then paste the API Username value.

Use PSIsafe DocuSign and Grant Consent

After PSIsafe DocuSign is enabled for a user, the following features are available.

- **DocuSign** menu option from within PSIsafe Desktop client
 - **DocuSign** Speedbar option
 - Context (right-click) menu options for **DocuSign**
1. Each PSIsafe Desktop user must perform a one-time “grant consent” process to use DocuSign by doing one of the following:
 - Select the **Grant Consent** option under the **DocuSign** menu
 - Drag a document to the **DocuSign** Speedbar

This dialog is also displayed if the user selects any other **DocuSign** operations within PSIsafe Desktop when consent has not yet been granted.

2. Click the **Grant Consent** button.

The user is redirected to the DocuSign web application login screen. Once the user logs into DocuSign, the user is directed to a web page for granting consent.
3. Click the **Accept** button on the **DocuSign Permission** window.

After clicking the **Accept** button, the web browser is redirected to the consent completion web page assigned to the integration.

i Note that if consent is already granted in DocuSign, the user does not see the **Accept / Cancel** page. The user is redirected to the consent completion web page assigned to the integration.

Close the web browser and click **Grant Complete** on the **DocuSign User Consent Process** dialog box.

The user configuration process is complete.

Chapter 8

Install PSISafe Open API and 64-bit server

The PSISafe Open API and the 64-bit server connects the 32-bit PSISafe Desktop server to a 64-bit PSISafe Desktop server that can communicate with any downstream applications, including PSISafe Mobile3.0, PSISafe DocuSign 12.1, and more. The PSISafe Open API and the 64-bit Server are considered legacy backend architecture, and were replaced by the Kofax PSISafe API and service in version 12.2.

This chapter describes how to install and configure the PSISafe Open API and the 64-bit server for use with legacy downstream applications until upgrading each to their latest versions.

PSISafe Open API and 64-bit server installation and upgrade

The PSISafe Open API and server work together to allow various PSISafe products, as well as custom applications, to communicate with your PSISafe Desktop installation. This not only enables 64-bit applications to work with your PSISafe Desktop installation, but also enables programmers to create custom programs that can send and receive data as it suits your unique business application needs.

You may install PSISafe Open API in a new environment or upgrade an existing PSISafe Open API installation.

PSISafe Open API and 64-bit Server installation prerequisites

The following is a list of prerequisites for the PSISafe Open API and the 64-bit Server. Technical Specifications match the overall PSISafe Desktop specifications.

- PSISafe Desktop 32-bit server that matches the version of PSISafe Open API and 64-bit Server you are attempting to install. The PSISafe Desktop Server 32-bit must be installed and registered.
- SSL Certificate (recommended)
- Microsoft Visual C++ Redistributable Package for Visual Studio 2008 SP1 (included in PSISafe Desktop Server x64 version 12.1.2.1003 and higher).
- See [Kofax PSISafe pre-installation reference](#) for more information on configuring an environment for the PSISafe Open API.

PSIsafe Open API 64-bit server installation procedure

To get the latest PSIsafe Open API and 64-bit server installation packages, contact Kofax Support. Then, perform the following actions.

1. Right-click the installer and select **Properties**.
2. In the **Properties** window, click **Unblock** and then click **OK**.
3. After you unblock the installer, right-click it and select **Run as Administrator**.
4. Complete the installation process with the default options. If you are installing the server on a different drive, note this for your configuration.
5. Copy the **CNGDBList.XML** file from the following default PSIsafe Desktop 32-bit Server directory (or otherwise): `C:\Program Files (x86)\CNG\CNGServer` to the PSIsafe Desktop 64-bit server default directory (or otherwise): `C:\Program Files\Cabinet\Server`.
6. Restart the 64-bit server service **Cabinet Server** using **Services.msc**.

On-premise installation without customer code example

1. `http://[BaseURL]/cabinet/api/database?customercode=default`
2. **Example:** `http://localhost/cabinet/api/database?customercode=default`

Cloud installation with customer code example

1. `http://[BaseURL]/cabinet/api/database?CustomerCode=testing`
Where "testing" is a sample customer code.
2. **Example:** `http://10.0.0.24/cabinet/api/database?CustomerCode=00001`

Install PSIsafe Open API and verify connection

Before you start installing the PSIsafe Open API, ensure that you have installed IIS.

1. Run the downloaded executable provided by PSIsafe Open API support and complete the installation process with the default options.
2. The PSIsafe Open API is a REST-compliant web service. It is a required installation if you are using PSIsafe Mobile, PSIsafe Mobile, or any custom integration unique to your company's business needs.

i The external permissions for the PSIsafe Open API to interact with your application may need to be configured to allow communication between PSIsafe Open API and the PSIsafe Desktop Server. Because the PSIsafe Desktop Server uses a 32-bit architecture, the PSIsafe 64-bit server runs side-by-side with the 32-bit version to relay commands to any 64-bit applications.

Optional configuration for separate API and server locations

When you install the PSIsafe 64-bit server and the PSIsafe Open API on separate servers, you must modify this connection.

1. Modify this file only if the PSIsafe Open API is on a different server than the PSIsafe 64-bit server.
2. File to be edited: **SystemServiceModelClient.config**
3. File location: C:\Program Files\Cabinet\OpenApi\cabinet\config
4. Change "localhost" to match the address or hostname of the PSIsafe 64-bit server.

Verify connection

Open the website in IIS or browse to the following address: <http://localhost/cabinet/>

1. This verifies that you can successfully connect to the PSIsafe Open API at [localhost]. The highlighted section in the image below specifies the database that the PSIsafe Open API uses.

```
▼<ArrayOfDatabaseModel xmlns:i="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.datacont
  ▼<DatabaseModel>
    <ConnectTo>CNG_Main</ConnectTo>
  </DatabaseModel>
  ▼<DatabaseModel>
    <ConnectTo>PSIsafe_10d4</ConnectTo>
  </DatabaseModel>
</ArrayOfDatabaseModel>
```

2. Enter the PSIsafe Open API URL provided below in your web browser to test connectivity to the CNGDBList.XML file previously copied. This will return all the databases that are connected to the web service.

Chapter 9

Install PSIsafe Mobile Client

With PSIsafe Mobile application for iOS and Android, your organization can access your PSIsafe Desktop installation from any location. With PSIsafe Mobile, you can view and edit the content stored in your PSIsafe Desktop installation using your Apple or Android device.

PSIsafe Mobile uses the PSIsafe API to communicate with your PSIsafe Desktop Server.

PSIsafe Desktop Mobile Client installation prerequisites

The following is a list of prerequisites for PSIsafe Desktop Mobile Client.


- PSIsafe Desktop Server 12.2
- PSIsafe Open API and 64-bit server 12.2
- Apple iOS 9.3 and higher, or Google Android 5.0 and higher

PSIsafe Mobile Client installation procedure

Download the PSIsafe Mobile application. For iOS, open the App Store and search for "PSIsafe." For Android, open Google Play and search for "Kofax PSIsafe Mobile."

By default, most on-premise installations use the IPv4 address of the computer hosting the 64-bit Server and OpenAPI installations in the configuration of the SystemServiceModelClient.config file, which tells applications where and from which port to access your PSIsafe Desktop installation. In this case, users can connect to your local network through a VPN and access your PSIsafe Desktop installation through the mobile app with this same IPv4 address.

This setup can be modified to point to custom domains or other network locations based on your unique business preferences. Note that changes to the PSIsafe Desktop URI must be updated both in this file and in the PSIsafe Management System Settings under **Options > Paths > PSIsafe URI**.

 Modify the SystemServiceModelClient.config file only if the PSIsafe Open API is on a different server than the PSIsafe 64-bit server.

File location: C:\Program Files\Cabinet\OpenApi\cabinet\config

1. Change "localhost" to match the address or hostname of the PSIsafe 64-bit server.

i The custom domains must have a valid certificate installed to be used as an external address. Also, port forwarding to the computer in question is necessary within the router settings in many cases for external connections.

2. Connect to your PSIsafe Installation via the **Connect** button on the mobile app.

Chapter 10

Install PSIsafe Synchronizer

To request a link to download PSIsafe Synchronizer, contact Kofax Support.

Install the PSIsafe Synchronizer installation program on the same computer as the external database which will be linked to PSIsafe Desktop. Install the program with the default settings provided.

Before you start the installation, select **Properties > Unblock** to unblock the downloaded installers. Right-click the installation program and select **Run as Administrator**. Ensure that you have proper rights and that the Windows-based security permissions allow access to the PSIsafe Desktop repository from this computer.

By default, PSIsafe Synchronizer is installed in `C:\Program Files (x86)\CNG\Synchronizer`. Double-click the **Synchronizer.exe** file. Follow the installer instructions.

You can create a service account specifically for PSIsafe Synchronizer to use. To do so, you can establish specific permissions to your repository and add permissions to the task scheduler instance.

Ensure you have prepared the environment for PSIsafe Synchronizer by following the configuration requirements in [Kofax PSIsafe pre-installation reference](#).

PSIsafe Synchronizer prerequisites

The PSIsafe Synchronizer prerequisites are the following.


- PSIsafe Desktop Server and Desktop 11.x
- External ODBC DSN or SQL Connection String
- Windows Server 2016 and higher
- External database credentials
- All configuration requirements in the Kofax PSIsafe pre-installation reference.

Pre-configuration considerations for PSIsafe Synchronizer

Before configuring PSIsafe Synchronizer, be sure to review the following considerations.

1. Gather database information.
 - a. Where is the database located?
 - b. What type of database is it?
 - SQL Server

- Oracle
 - Microsoft Access
 - Other
2. Connect to the database.
 - a. Do you have an OLE DB or ODBC driver, or DSN for the database?
 - b. Can a Data Source Name (DSN) be built to point to the database?
 3. Access the data in the database.
 - a. What table or query will be connected to PSIsafe Desktop?
 - b. Do you need to build a query spanning several tables?
 - c. What is the primary key field for the database or query?
 - d. Do you have all credentials required to perform read actions to the database?
 4. Determine the PSIsafe Desktop repository and cabinet to use.
 - a. Do the field definitions in the table match the folder index definitions?
 - For example, the data table has separate fields for last name, first name, then the PSIsafe Desktop folder indexes should as well.
 5. Match each index field independently.
 - a. For each required field in the database table/query, you need a corresponding field in the PSIsafe Desktop folder indexes.
 6. Determine how often PSIsafe Synchronizer runs.
 - a. Hourly, daily, weekly, or otherwise?
 - b. Stress will occur on the server briefly during this time period, so be aware of peak usage times of PSIsafe DesktopPSIsafe Desktop.

 PSIsafe Synchronizer can be used to connect to different databases and cabinets. Separate Synchronizer instances are required for each database connection. Each scheduled synchronization runs all configured profiles at once.

PSIsafe Synchronizer installation procedure

To install PSIsafe Synchronizer:

1. Download the PSIsafe Synchronizer installer.

To request a link to download PSIsafe Synchronizer, contact Kofax Support.

Install the PSIsafe Synchronizer installation program on the same computer as the external database that will be linked to PSIsafe Desktop.
2. Right-click the PSIsafe Synchronizer installer and select **Properties**. In the **Properties** window, select **Unblock**.

After you unblock the installer, right-click it and select **Run as Administrator**.

Ensure that you have proper rights and that the Windows-based security permissions allow access to the PSIsafe Desktop repository from your computer.

3. Install PSIsafe Synchronizer with the default settings provided.

You can create a service account specifically for Synchronizer to use, so that you can establish specific permissions to your repository and add permissions to the task scheduler instance.

4. Assign "Full control" permissions to the user who starts PSIsafe Synchronizer.

To do so, browse to `C:\Program Files (x86)\CNG\Synchronizer`. Right-click the **Synchronizer** folder and select **Properties**.

The **Synchronizer Properties** window appears.

5. Select the user from the list and select **Full control**. Click **OK** to apply the changes.

Example: Connect PSIsafe Synchronizer to a PSIsafe Desktop database

In some cases, when you start PSIsafe Desktop Synchronizer, the **Connection Configuration** window may not appear. To access this window manually, click the gear, and select **Connection Configuration**.

Also, after you change your connection settings, the **Connection Configuration** window may not open automatically when you start PSIsafe Synchronizer. To fix this issue, go to `C:\Program Files (x86)\CNG\Synchronizer`. In the **Synchronizer** folder, delete the **CNG-Server-Info.xml** file. Restart PSIsafe Desktop Synchronizer and ignore the message boxes until the **Connection Configuration** window appears.

Chapter 11

Install PSISafe Books

PSISafe Books is a downstream application of PSISafe Desktop, and a companion product to Intuit QuickBooks®. The PSISafe Books application serves as a connection between QuickBooks and PSISafe Desktop. Documents such as invoices are imported into PSISafe Books. The user keys data from the invoice into PSISafe Books using the convenient side panel.

This chapter describes the PSISafe Books installation prerequisites and procedure.

PSISafe Books installation prerequisites

The following is a list of prerequisites for PSISafe Books.

- PSISafe Desktop 32-bit Server 12.2
- PSISafe Desktop 32-bit Desktop 12.2
- Intuit QuickBooks Enterprise 19 and higher
- PSISafe BooksLicense (To request the license, contact Kofax Support)
- PSISafe Desktop installation: Windows settings, supporting Microsoft applications, and the PSISafe Desktop 32-bit Client and Management applications must be installed before proceeding with the Books installation.
- PSISafe Desktop configuration: Prior to PSISafe Books installation, configure users, repository, cabinet, and workflow definitions.

Set up two cabinets for your PSISafe Desktop instance: one cabinet for customers and one cabinet for vendors.

Two default cabinets, QB Customers and QB Vendors, are built into PSISafe Desktop. You can use these cabinets to speed up the process and avoid common configuration issues. Do not alter the structure of these cabinets, which are specifically designed to work with PSISafe Books.

- Proper security settings: Set the security in QuickBooks so that you have access to A/R and A/P. No access to payroll or employees is needed.

PSISafe Books installation procedure

Follow the procedure below to install PSISafe Books.

1. Download the PSISafe Books installers. Contact Kofax Support for a PSISafe Books installation package link.
2. Right-click the installer and select **Properties**.
3. In the **Properties** window, click **Unblock** and then click **OK**.

4. After you unblock the installer, right-click it and select **Run as Administrator**.
5. Follow the instructions in the screen to complete the installation process with the default options.

To upgrade a previous version of the PSIsafe Books Client with the standalone installer, uninstall the previous version in **Programs and Features** first.

To upgrade a Client using the upgrade installer, ensure that the installation folder for your current installation is default, and if not, change it when prompted.

Before proceeding, ensure you've prepared your environment for PSIsafe Books by referencing the configuration requirements in [Kofax PSIsafe pre-installation reference](#).

Connect to your PSIsafe Desktop database

First, your PSIsafe Books installation must configure the appropriate connection to your existing PSIsafe Desktop Server installation. Proceed with one of the two following connection types based on your PSIsafe Desktop installation configuration. When you first open PSIsafe Books, the **Connection Configuration** window appears.

i If the **Connection Configuration** window does not appear, but displays your pre-configured PSIsafe Desktop installation connection information, proceed to the next section. Otherwise, select the gear icon in the lower-right of the login screen to display the **Connection Configuration** window.

Connect to database: on-premise installations

1. Select **On-premise**.
2. Type the IPv4 address of your local server or the IPv6 computer name.
3. Confirm that the **Customer code** remains "default" as this function is not used for on-premise installations.
4. Click **Save** to apply the changes.

Connect to database: cloud installations

1. Select **Cloud**.
2. Confirm that the PSIsafe Desktop server IP address is not be entered.
3. Enter the **Customer code** provided by your Kofax representative.
4. Click **Save** to apply the changes.

For advanced settings, contact Kofax Support for assistance with configuring connections to reserved, beta, or specialized PSIsafe Desktop Cloud installations, as well as recommendations for adjusting ports and TCP/HTTP connection protocols from their default values.

Chapter 12

Install PSIsafe Retriever

PSIsafe Retriever is a companion application to PSIsafe Desktop that allows quick and easy referencing, searching, and browsing based on a defined area of your screen where PSIsafe Retriever monitors and watches an external program for correlating index data. The application is installed automatically with PSIsafe Desktop. For more information, see [Install PSIsafe Desktop](#).

PSIsafe Desktop Retriever is client-specific and must be installed on each computer that will use it.

- Make sure access is also available to the PSIsafe Desktop repository.
- Install the program with the default settings provided.
- Alternate settings should only be used as directed by Kofax Support.

Pre-configuration considerations

Before proceeding, it's good to consult your internal team to answer the following questions.

1. Application information

- a. Which application/data are you connecting with?
- b. Is a PSIsafe Desktop setup that matches this data available?
 1. If not, you may use PSIsafe Synchronizer to transfer the application's database data to the corresponding folder indexes.

2. Location of PSIsafe Desktop data

- a. Which repository/cabinet will be mapped?
- b. Which folder index value in the cabinet contains the same data used by the business application? Name, account number, and so on.
- c. Does the user have access rights to the cabinet in PSIsafe Desktop?

Configure PSIsafe Retriever

To use PSIsafe Retriever, you must first set up an area of your screen where a third-party program will display correlating index data. For example, if your company uses an inventory management application, there may be a unique ID used within each folder of your PSIsafe Desktop installation that matches what is displayed in the external application. You can then configure PSIsafe Retriever

to monitor this application or portion of your screen and watch for the corresponding number, name, or other kind of value.

1. Launch PSISafe Retriever.

By default Retriever is installed on a 64-bit system in C:\Program Files (x86)\CNG\CNG-SAFE. The executable name is CNG.Retriever.exe. Double-click this executable to run PSISafe Retriever. A shortcut is also installed on the Windows Start menu.

2. Enter the PSISafe Desktop username and password to use PSISafe Retriever.

A new setup must be configured before using Retriever for the first time. In the system tray, right click the Retriever icon and select Setup.

Enter the Administrator password.

3. Enter a new setup/Edit an Existing setup. Retriever can be used to connect to many different databases and cabinets. A setup name is required for each connection.

Enter a new setup name or select an existing one from the menu.

4. Select the correct PSISafe settings.

PSISafe Retriever connects a field in another software application to a designated PSISafe repository, cabinet, and folder index. Data is pulled from the other software application and matched against the data in the folder index. If there is a match than the folder information is retrieved and the document list is made available to the user.

Select the appropriate repository/cabinet/index combination to connect and proceed to the next steps.


5. Select the application to connect PSISafe Retriever.

PSISafe Retriever connects to another application based on the application executable name. In general these files are stored in the C:\Program Files\<appname> (C:\Program Files VACT). Consult your IT professional or Kofax Support to determine which executable file is the correct one.

This button displays a file browsing screen. Navigate to the correct executable and press the **Open** button.

6. Select the positioning of the PSISafe Retriever button.

PSISafe Retriever attaches a small button to the application selected in Step 5. This button can be placed in one of three locations. This is dependent on where the best place to display the PSISafe Retriever icon may be for your external application. Select the top right (most common), bottom left or bottom right.

 Most applications use the top left for their context and file menus, so this is not an option.


7. Set up the remaining PSISafe Retriever options that control how each setup functions. This section goes through each one of the options and explains how it affects the PSISafe Retriever application.

- **Global:** Makes the setup available to other users using the same repository/cabinet AND the same application. When unchecked, the setup is only available to this user/computer.
- **Auto Open:** When PSISafe Retriever finds the folder that matches the data in the connected application, it can automatically open the document list if this option is checked. If it is not checked, the user can click the Show Document List button to see the list of documents.
- **Use Capture:** Connects the folder index data to data from the screen of the connected application. Simply follow the directions on the Select Capture Field screen.

- **Use Matching:** Configures specific variables for PSIsafe Retriever to match to your third party database. It is used to take data from the screen and run it through a regular expression parser to extract a piece of data that can be used to match the folder index.

Example: A medical office uses a software package that displays a patient ID number in plain text. In this scenario, the external application displays information like "Patient - John Ferry - 93847" where 93847 is the patient number. If 93847 matches a corresponding folder index configured in PSIsafe Desktop, then this data could be extracted from the string by using a regular expression after configuring PSIsafe Retriever to monitor the section of the application that displays this information.

8. Save the current setup by clicking **Save Settings**. Click **Exit** to exit setup mode. If the global option is set, the setup becomes available to all other users of PSIsafe Retriever.

 PSIsafe Retriever can be connected to more than one application. For instance, it could be set up to connect to ACT! for contact management and MAS-90 for the accounting function. PSIsafe Retriever always follows the application that has the mouse focus.

Chapter 13

Install PSIsafe PDF Forms Monitor

PSIsafe PDF Forms Monitor has the same system requirements as the rest of the PSIsafe product family.

Installation process

1. Contact Kofax Support to receive a link for the latest version of PSIsafe PDF Forms Monitor.
2. Run the installation package on the same workstation that has the PSIsafe Desktop server and client installed.
3. Specify an installation path if different from the default. Make sure to note the changed installation path if applicable.
4. Open Services.msc and ensure that the **Cabinet PDF Forms Monitor** service is started. It should be started and set to **Automatic** startup by default.
5. Set up a PSIsafe Desktop user account that is dedicated to running PSIsafe PDF Forms Monitor. Several configuration elements must be properly configured for the program to function:
 - a. The user account needs to be designated as a **Cabinet Administrator** through PSIsafe Management for any cabinets which they will be affecting
 - b. The user account should be using a **Regular Full** license if possible, since interruptions to the service can be caused if any **Concurrent Full** licenses are not available in the given pool at the time that the service requests a login.
 - c. The user account should be given full permissions up to **Create** for the affected cabinets to ensure the account can create and modify PDF Forms as needed. Ensure that each security class is accounted for in these permissions.

Prepare database

To process rows from an SQL table, some method of entering data into the table must already exist. This could be a stand-alone program or some type of Web form. The table must have the following columns:

1. A Unique Identifier of some type, such that no two rows will have the same value in this column.
2. A migration column that indicates which rows have been processed. This must be an integer value. The PSIsafe PDF Forms Monitor will search for one value (the "Get Value") in this column that indicates unprocessed rows. Upon processing the row, this value will be changed to the

"Update Value." These two values must be different. For example, a 1 may specify a "Get Value" to update, and a 2 may specify a "Updated Value" signaling that the update has completed.

3. A column that uniquely identifies a folder in the destination cabinet. It must match the folder index precisely or a new folder will be created.
4. There should also be columns that can be used to create folder index values and to fill in form fields.
5. Optionally, the table can also have a condition column, which is used to limit processing to a subset of the records matching the "Get Value" of the migration column.

Other optional columns that indicate the following.

1. A PSISafe Desktop user or group to route a form to using workflow after creation.
2. Folder and document security classes to apply to the document or folder.