Kofax FraudOne
Installation and Migration Guide

Version: 4.6.0

Date: 2023-08-04

KOFAX

Table of Contents

Preface

Related documentation

The full documentation set for Kofax FraudOne is available at the following location:

https://docshield.kofax.com/Portal/Products/FO/4.6.0-e4jy6kf7pr/FO.htm

In addition to this guide, the documentation set includes the following items:

Release notes
- *Kofax FraudOne Release Notes*

Technical specifications
- *Kofax FraudOne Technical Specifications*

Guides
- *Kofax FraudOne Administrator's Guide*
- *Kofax FraudOne Archive Interface Server*
- *Kofax FraudOne ASV Blackbox*
- *Kofax FraudOne Common API Specifications for GIA Engines*
- *Kofax FraudOne Data Warehouse Installation and Operation Guide*
- *Kofax FraudOne Extended Reporting Features and Statistics*
- *Kofax FraudOne Feature Codes*
- *Kofax FraudOne Global Fraud Signature Web Service Developer's Guide*
- *Kofax FraudOne Java Client Customization Guide*
- *Kofax FraudOne Java Client Customization Layer*
- *Kofax FraudOne Report Component Installation Guide*
- *Kofax FraudOne Service Program Configuration*
- *Kofax FraudOne Service Program Interfaces*
- *Kofax FraudOne SignCheck Result Codes*
- *Kofax FraudOne Standard Reporting Features and Statistics*
- *Kofax FraudOne The Book on CRS*
- *Kofax FraudOne Thin Client Customization Guide*
- *Kofax FraudOne Variant Cleanup Utility*

Help

- *Kofax FraudOne Administration Client Help*
- *Kofax FraudOne Error Messages Help*
- *Kofax FraudOne Java Client Help*
- *Kofax FraudOne Server Monitor Help*
- *Kofax FraudOne Thin Client Help*

Training

Kofax offers both classroom and computer-based training that will help you make the most of your Kofax FraudOne solution. Visit the Kofax website at www.kofax.com for complete details about the available training options and schedules.

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

Preconditions

The following information in this chapter is only necessary, if an installation is done on new hardware.

If the installation is an update to an existing FraudOne Release 4.4 installation, all steps mentioned in this chapter are not necessary anymore - unless a new version of either database structure, Java, Tomcat or other components is requested.

Requirements

For detailed information on system requirements see the *Kofax FraudOne Technical Specifications* document.

Java installation

Use the Java version given to you by Kofax or download a version which is currently approved for FraudOne Release 4.6.0 from the Internet. Currently it is the Java SE Development Kit 8 for Windows (32 bit), such as

```
jdk-8u131-windows-i586.exe
```
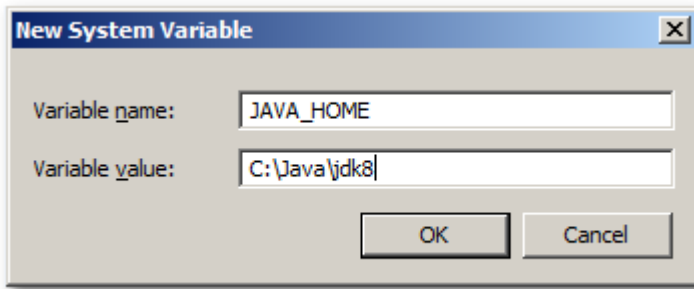
We strongly suggest that you install Java into a directory without blanks, such as

```
C:\Java\jdk8
```

instead of the one suggested by the installer to simplify further administration and configuration.

After installation completed successfully, add a new system environment variable JAVA_HOME, which points to the Java home directory jdk8 on the selected drive.

When using software installed by someone else, an additional Java version might exist as well. In order to verify that the correct Java version is used, you can open a command window and then type in:

```
java -version
```

The output should be:

```
C:\SignPlus>java -version
java version "1.8.0_131"
Java(TM) SE Runtime Environment (build 1.8.0_131-b11)
Java HotSpot(TM) Client VM (build 25.131-b11, mixed mode)
C:\SignPlus>
```

Tomcat installation

The FraudOne Thin Client requires a Web Application Server. See requirements documentation Kofax FraudOne Technical Specifications document for a list of supported Web Application Servers. Apache Tomcat will be used as an example here.

The latest version of Tomcat release 8 can be downloaded free of charge from the internet (Apache Tomcat). In most of the cases this is not required since a Web Application Server is already available. If an installation needs to be done, we recommend to download the zip-file instead of installer exe-file.

Similar to the Java installation, we strongly suggest to extract the downloaded zip-file into a simplified directory structure such as:

```
C:\Tomcat8
```

ParaScript CheckStock installation

The FraudOne GIA CheckStock requires the Third Party Application ParaScript CheckStock. If an installation needs to be done, unzip CheckStock_x_x_x.zip, go to the unzipped directory CheckStock_x_x_x\Installation\Regular Setup and execute the setup.exe file. Then follow the installation instructions.

ParaScript CheckPlus installation

The FraudOne GIA Image Analysis requires the Third Party Application ParaScript CheckPlus. If an installation needs to be done, unzip CheckPlus x.x.x.zip, go to the unzipped directory CheckPlus x.x.x\x86 and execute the setup.exe file. Then follow the installation instructions.

Installation guidelines

In this section FraudOne 4.6.0 release components will be installed. Following list includes the different steps necessary for setting up FraudOne 4.6.0 in the typical sequence.

Installation package

A FraudOne shipment is usually provided as a ZIP file called:

`FraudOne_4.6.0_for_<dbms>.zip`

A current Release 4.6.0 FraudOne base shipment for MSSQL would be named:

`FraudOne_4.6.0_for_MSSQL.zip`

A current Release 4.6.0 FraudOne FixPack 1 for MSSQL would be named:

`FraudOne_4.6.0.1_for_MSSQL.zip`

The nomenclature refers to the sub-release-level the shipment is built on.

Installation of single FraudOne components

In case a single Kofax FraudOne component, for example only Data Warehouse (plus optionally the report server) has to be installed into an existing Kofax FraudOne system the following chapter summarizes all necessary steps to install the component.

Kofax FraudOne Data Warehouse

See *Kofax FraudOne Data Warehouse Installation and Operation Guide* for detailed information on setting up the FraudOne Data Warehouse.

Kofax FraudOne Report Server

See chapter about Kofax FraudOne Reports with Kofax Insight 5.x.

Components installation

After unzipping the installation package, the following command files can be used to copy the files required for the respective component:

Command file	Description
InstDBScripts.cmd	Scripts to create the FraudOne tables.
InstServer.cmd	Files necessary to run a FraudOne Server.
InstLicense.cmd	FraudOne evaluation license files. ⓘ Do not install if a full license already exists and has been installed.
InstSrvMon.cmd	Files necessary to Monitor and Control a FraudOne Server.
InstAdminClient.cmd	Administration Client
InstJClient.cmd	Java Client

For all installation commands, FullDestinationPath parameter has to be specified as a target directory. The installation commands will create a SignPlus directory in the specified destination path. As predefined, the software will be installed in this directory.

Example

To install the specific components open a command window and go to the location where the scripts are and then type in:

```
InstServer.cmd C:
```

It will create the directory:

```
C:\SignPlus
```

and copy all required files into this directory.

Throughout this document, it is assumed that all Software components will be installed on:

```
C:\SignPlus
```

Database

The FraudOne system requires one or multiple databases, which must be generated by using the current product environment. For multiple databases in FraudOne, SignBase, SignCheck and Data Warehouse databases must be generated separately.

In case you have to create ODBC data access in 64-bit operating systems, it is mandatory to use the 32-bit ODBC drivers. In order to accomplish this, one must set up the ODBC connection using the 32-bit version of the ODBC Driver. This is done by running an entirely identical ODBC tool which is

kept within the C:\Windows directory. This 32-bit ODBC Data Source Administrator can be found by going to the **Start** menu, selecting **Run** and executing

```
C:\Windows\SysWOW64\odbcad32.exe
```

The necessary databases must be generated before using FraudOne. In order to create database objects (tables, views, etc.), scripts are provided after running InstDBScripts.cmd.

All required scripts are then located in the directory

```
C:\SignPlus\scripts
```

For detailed information on creating and maintaining FraudOne databases see *Kofax FraudOne Administrator's Guide*.

Licenses

Each Server Manager installation comes with a license file contained in the following directory:

```
C:\SignPlus\lmdata
```

The presence of the license file in the correct directory is sufficient. Unlike earlier FraudOne releases, a registry entry is no longer required.

You can use SPLM2View.exe to retrieve the server installation code, which is required to request test and production licenses.

Contact your Kofax sales representative to obtain production license files.

Initial configuration

Every system on which any FraudOne component is installed (with the exception of the Report Server) must be initialized before the installed software can be used. Before this can be done, the SignBase database must be set up correctly.

The first system that should be set up is (one of) the configuration server system(s). Since at this point no configuration server is running, the process described here should be followed.

1. The database should be created and accessible using ODBC as described in chapter Database.

2. Beginning in the server installation directory of the machine to be initialized, use the SetupCfg.cmd "-initlocal" command to initialize the machine and add an empty topography record to the database for it.

3. Still in the same directory, start the SRVMNGR4.exe program. This results in a usable SignBase configuration server.

4. You will have been provided with an initial configuration workspace which will be present in the server directory. You should import this configuration workspace into the database using the SetupCfg.cmd "-importworkspace" command. Notice you will have to tell SetupCfg the machine name(s) of the systems in your installation, the instructions for this are provided together with

the initial configuration workspace. For the product's default initial workspace the command is then:

```
SetupCfg.cmd -importworkspace FraudOneBaseConfiguration.zip clear *:*
samples:samples
```

The user account used during the import operation needs the SP_CoreProperties right granted.

5. If the instructions for your initial configuration workspace include the requirement to restart the configuration server you can do so at this point, otherwise you should follow the instructions to start the Administration Client (below) and complete the configuration for the server system(s) before restarting the configuration server.

If you wish to run the Administration Client on the same system as the configuration server (above) you can start the client now.

To start the Administration Client on another system, you should initialize that system as a client (SetupCfg.cmd "-initclient") and add the configuration server address to its configuration (SetupCfg.cmd "-addserver") before you can start the client.

Remote initialization

Using SetupCfg with the "for" option allows an administrator to configure systems without needing to log on to those systems and run the SetupCfg command locally. The "for" option also allows SetupCfg to be scripted to configure large numbers of systems in batch mode.

When SetupCfg is run using the "for" option, it creates a separate configuration file for each unique system named using the "for" option. These files are created in the same directory as the "real" SPCfgInst.dat file that is created when SetupCfg is used without the "for" option (so, for the local machine). These files are named using the machine name given in the "for" option.

Once these files have been created, they need to be moved, and renamed to SPCfgInst.dat, into the corresponding directory on the respective target systems. This can be done using any method, including software distribution tools.

Configure SignCheck business parameters

⛔ Before you can activate the SignCheck part of a FraudOne application, the SignCheck parameters have to be specified and a workflow has to be defined. Both have to be done by using the Administration Client. But before the Administration Client can be used it's necessary to have the Server Manager and respective SignBase configuration server up and running (see chapter Initial configuration).

System configuration

The Administration Client is available after running InstAdminClient.cmd.

To startup the Administration Client double-click adminClient.cmd in your C:\SignPlus directory.

The System Configuration allows you to see and modify all settings stored in the configuration server. If the active user does not have the SP_CoreProperties right, core configuration elements cannot be managed, but still can be overridden with private configuration elements. For more details see *Kofax FraudOne Administration Client Help*.

CRS Editor

This CRS Editor is also available in the Administration Client. A detailed description on how to create a new workflow or maintain an existing workflow is available in *Kofax FraudOne The Book on CRS*.

Service programs

The FraudOne Service programs are automatically installed when executing the command file InstServer.cmd. Running this command file will provide the following Service Programs:

- Getter
- Putter
- Days Final Processing (DFP)
- Account Loader (AL)
- Image Loader (IL)
- Fraud Feedback File Loader (F3 Loader)
- SignatureReferenceFilter (SRF)

Further details about the unique service programs and their configuration are described in the *Kofax FraudOne Administrator's Guide*.

Thin Client

The FraudOne Thin Client web application is delivered as a war-file with its corresponding rel-file and ver-file, which contain the change log respectively the version information of the Thin Client. Follow the particular deployment instructions of your Web Application Server.

Example

We use Tomcat as an example that is installed as described in chapter Tomcat installation, so a directory

```
C:\Tomcat8\webapps
```

is existing.

Login to a command prompt console with administrator rights, scroll to the directory where the unzipped installation package is kept. E.g.:

```
C:\FraudOne_4.6.0_for_<DBMS>\kofax-fraud-one-YYYYMMDD\
```

Issue the following commands from the command prompt console:

```
copy .\SignPlus.war C:\Tomcat8\webapps\SignPlus.war
copy .\Rel\TClient2.rel C:\Tomcat8\webapps\TClient2.rel
copy .\Rel\TClient2.ver C:\Tomcat8\webapps\TClient2.ver
```

As a next step, the environment variable PATH need to be expanded with the following:

```
C:\Tomcat8\webapps\SignPlus\web-inf\lib\bin
```

Starting the Windows Tomcat services will unpack the file SignPlus.war. If the Web Server and the FraudOne Server reside on different machines, it's necessary to adjust the host settings in the custom.properties configuration file for the Thin Client using the Administration Client. If the host settings were changed restart the Windows Tomcat services.

To start the Thin Client open Internet Explorer and change to the URL (in SignPlus - S and P uppercase):

```
http://localhost:8080/SignPlus
```

Chapter 3

Kofax FraudOne Reports with Kofax Insight 5.x

This section describes the necessary installation steps so that Kofax FraudOne Reports can be called.

General

In case Kofax Insight isn't already installed, an installation has to be made before continuing.

> ⓘ For installation instructions see Kofax Insight documentation.

Before newly generated reports can be used, they must be imported into the Kofax Insight meta-database. Depending on the supported database, a corresponding file has to be imported that is identified by its extension:

```
Project_SB_Reports_<extension>.zip
```

That includes the solution to use the Kofax FraudOne Reports.

Possible file extensions for the Kofax FraudOne supported databases are:

| Database	File extension
MS SQL	.ms
Oracle	.ora
IBM DB2	.db2

Create a project for Kofax FraudOne Reports

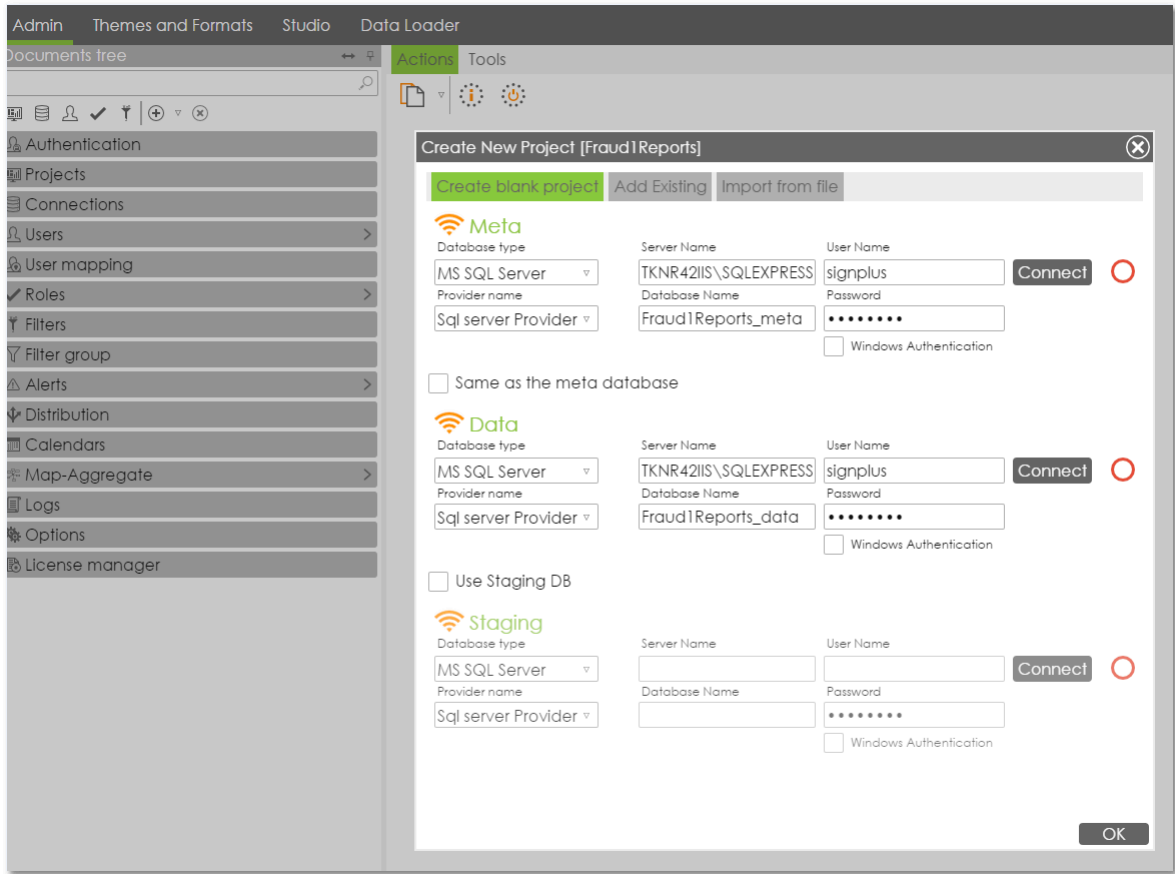To create a project for Kofax FraudOne Reports follow these steps:

1. Start **Insight Admin** selecting from the **Windows Start** menu:
   All Programs > Insight 5.x > Administration > Admin

2. Login into Insight.
   Standard user / password : Administrator / password (see Kofax Insight documentation)
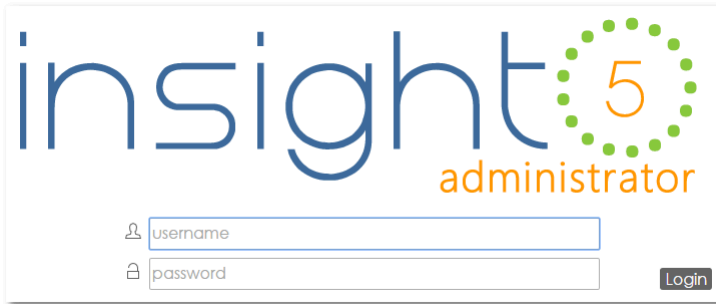
3. Add a project to an existing Insight database.
   With
   Project > New
   you can add a new project (e.g. Fraud1Reports).
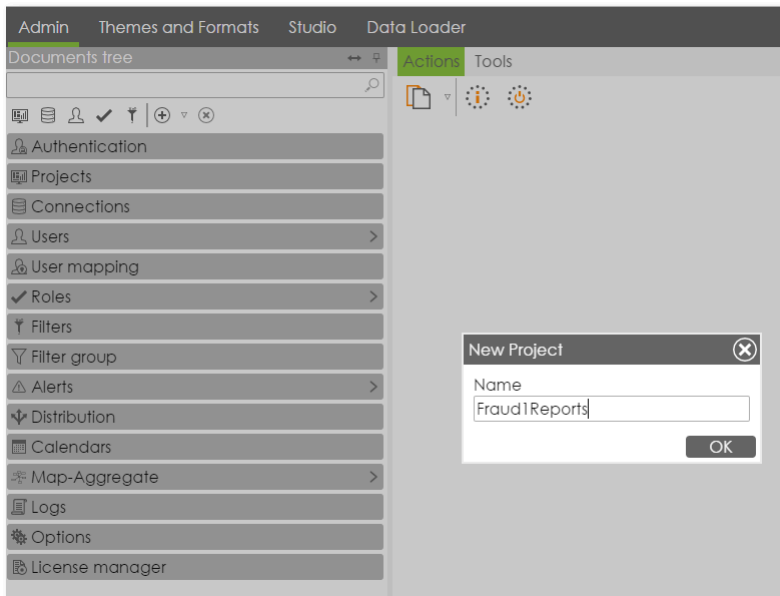
4. If no Kofax Insight meta-database exists, then one can be created, otherwise the existing default Kofax Insight meta-database must be used to store the Kofax FraudOne Report project.

If a new project is created, Kofax Insight automatically suggests to create a database called <Project name _meta> to store the generated reports.
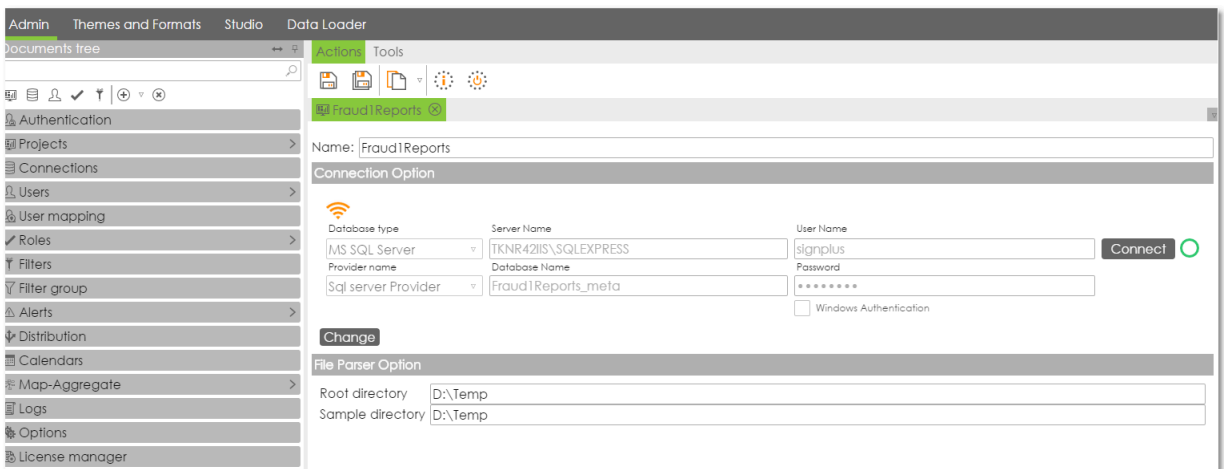
Import the FraudOne Reports Customized Project Settings

The customized project settings Themes and Formats are used only for the FraudOne Reports charts color scheme. It is possible to use the existing color scheme or to define your own colors for the charts.

> ❗ If a Kofax Insight database is already present, make a backup first.

1. Start **Themes and Formats**.

2. Import the Kofax FraudOne Reports project settings with
   Tools > Import

3. Select and open the file
   ExportAdminDatabase.xml
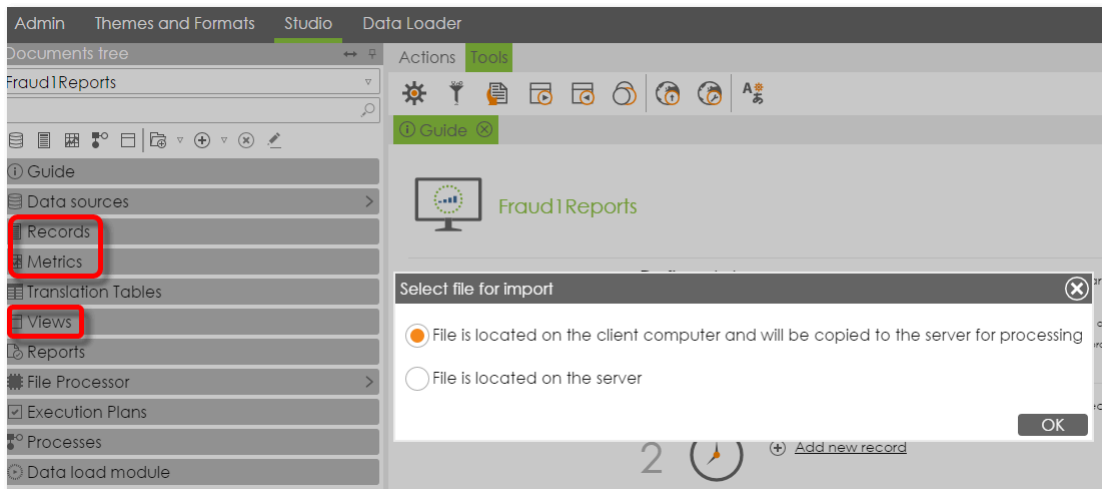
4. Select the following items:
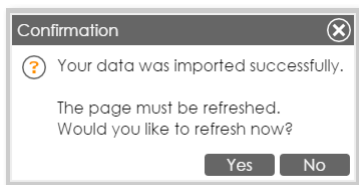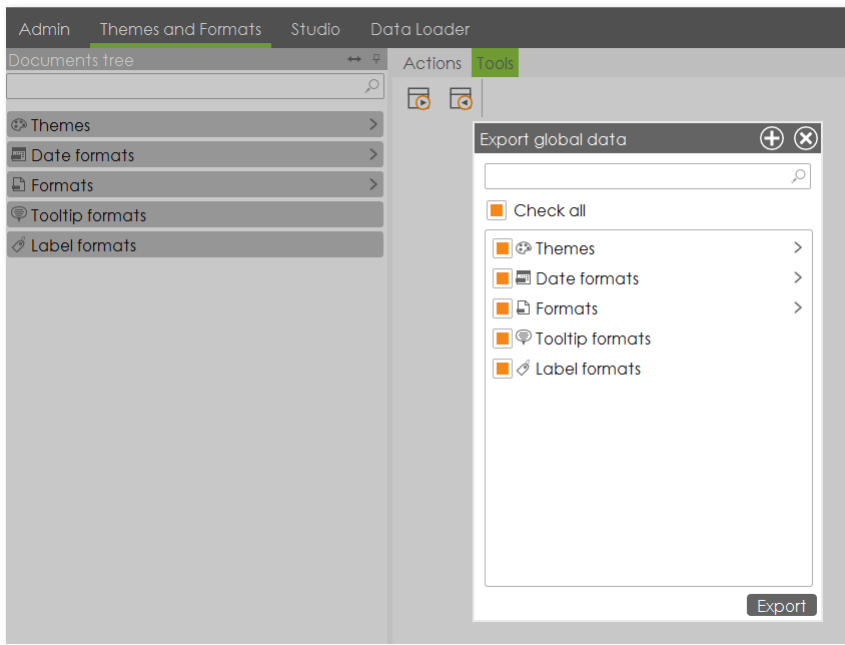
Import the Kofax FraudOne Reports

The Kofax FraudOne Reports are a complete Kofax Insight project. This project includes:
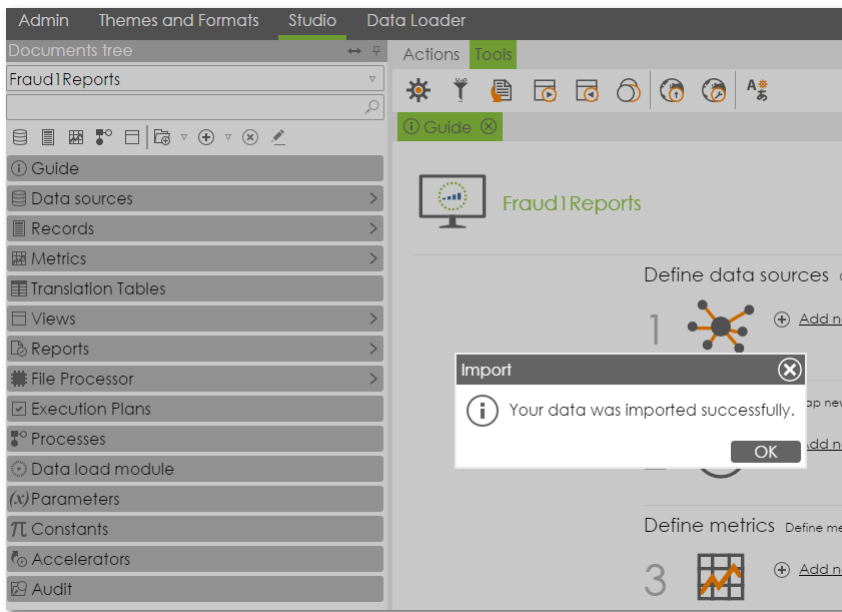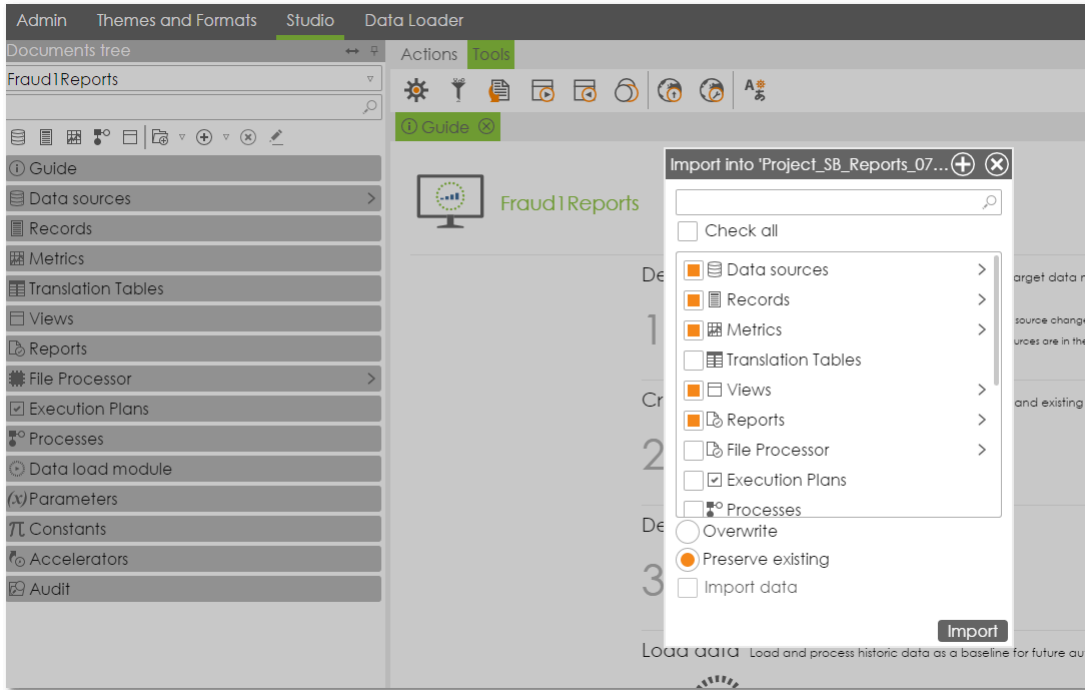
- Data sources
- Records
- Metrics
- Views

> ⛔ If a Kofax Insight database is already present, make a backup first.

1. Start **Insight Studio**.

2. Select your project name (e.g. Fraud1Reports) as project.

3. Import the reports with
   Studio > Tools > Import

4. Select and open the ZIP file
   Project_SB_Reports_<extensions>.zip

5. Select the following items:
   - Data sources
   - Records
   - Metrics
   - Views
   - Reports
   - Others

Connect to Kofax FraudOne Data Warehouse

After the reports are imported, a connection to the Data Warehouse database must be made.

1. Set up the Data Warehouse connection.

   Therefore the menu item **Data sources** must be extended and the data source SB_Reports_DB selected. Then the database settings for the Data Warehouse database (e.g. DB Type, Server Name, user and password) need to be provided.
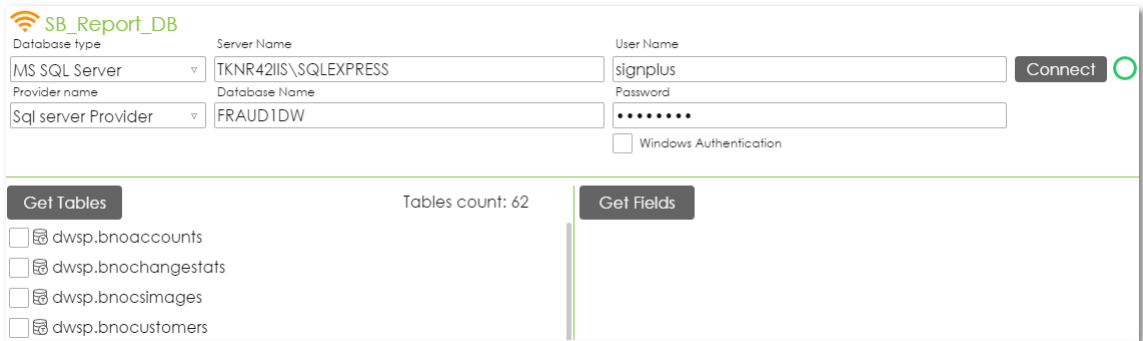
   The database name for the Data Warehouse is e.g. Fraud1DW.

2. Test the connection to Fraud1DW.

   The connection to the Data Warehouse database can be tested in clicking the **Connect** button.
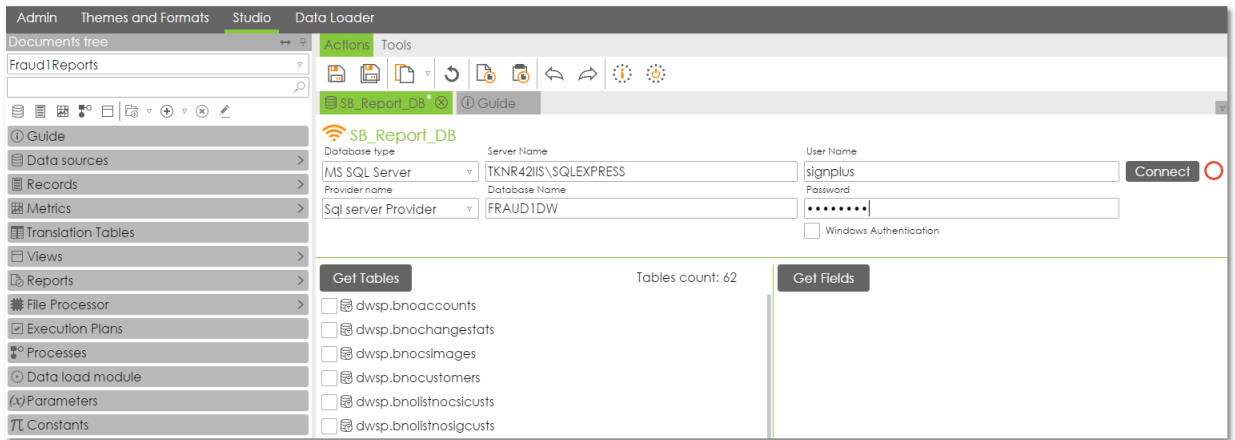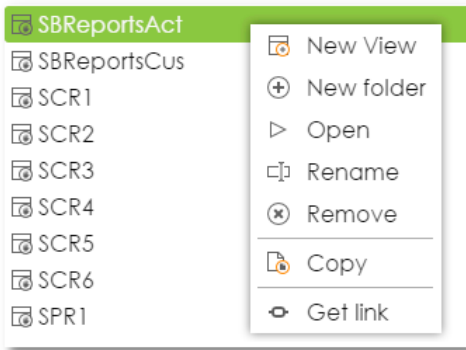

When the color of the circle after the **Connect** button changes from red to green, the connection attempt was successful.
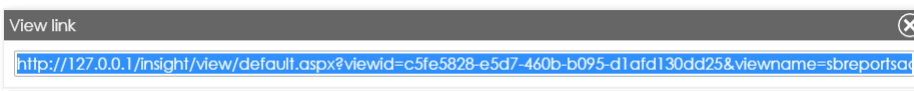

Display the Kofax FraudOne Reports

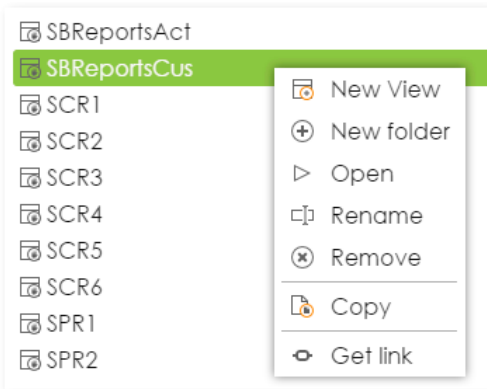There are two collections of reports the Account Model and the Customer Model.

To start the reports for Account Model move the mouse to

Studio > Views > SBReportsAct
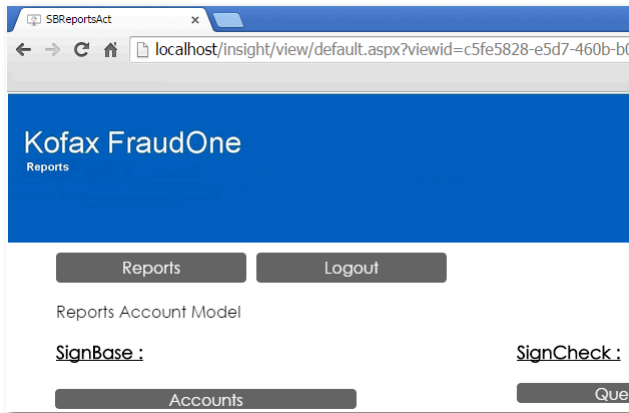
then right-click and select **Get link**.

or

to start the reports for the Customer Model move the mouse to

Studio > Views > SBReportsCus

then right-click and select **Get link**.

Open the copied link in a browser to run the reports.

Kofax FraudOne Extended Reports

The Kofax FraudOne Extended Reports are not included in the standard delivery package and can be added separately.

Import the Kofax FraudOne Extended Reports

Import the extended Kofax FraudOne reports.

> ⛔ If a Kofax Insight database is already present, make a backup first.

1. Start **Insight Studio**.

2. Select **Fraud1Reports** as project.

3. Import the reports with
   Studio > Tools > Import

4. Select and open the ZIP file
   Project_SB_ExReports_<extension>.zip
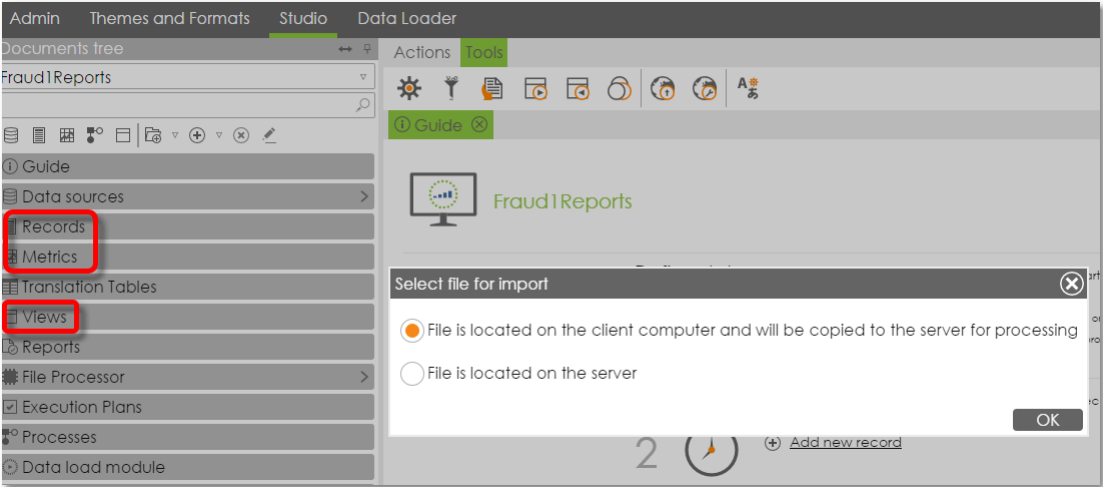
Migration guidelines

These guidelines are intended to use if you want to upgrade from a FraudOne version prior to Release 4.4.2.

> ℹ️ For FraudOne 4.6.0 no special database migration is necessary, since there only has been reintroduced functionality that already existed earlier using the ParaScript engine.

Database migration from Release 4.4.1 to Release 4.4.2

Migration of an existing Data Warehouse database is done using customer specific scripts supplied as part of the migration package by Kofax. Follow the instructions for the Data Warehouse migration supplied with these scripts after the normal completion of the DFP for the last Release 4.4.1 production day.

The normal migration path for a SignCheck database from Release 4.4.1 to Release 4.4.2 requires that the database is empty of production data (after the DFP has copied any data to be saved for the last production day to the Data Warehouse). The SignCheck database tables are then deleted and the empty tables in the Release 4.4.2 format are created. This is done using the normal SCDebTab installation program.

The following SignBase database migration procedure need be followed only if the customer is not migrating to the FraudOne product's Active Directory Integration feature. If the customer will migrate (during the installation of 4.4.2) to use this feature, no SignBase database migration is required and the procedure described in Migration to the Active Directory Integration feature should be followed.

Migration of the SignBase database from Release 4.4.1 to Release 4.4.2 is carried out using a database script. The script is

`SBNewTabs442.cmd`

For SQL Server only: After running the migration scripts, the FraudOne stored procedures must be refreshed using the SBDebTab command program with the "--storedprocedureonly" parameter.

In the descriptions below, the script options (the same for all database types) are

```
"-schema    <db-schema>"         default "DEB"
"-server    <db-server>"
"-port      <db-port>|DYNAMIC"   default DYNAMIC
"-database <db-name>"            default "SIGNPLUS"
"-user-id  <db-user>"           default is current user
"-password <db-password>"       prompted if not supplied
"-?"
```

Choose the correct command for your installed database type and follow the appropriate instructions below:

Oracle

```
SBNewTabs442.cmd {options} ORACLE
```

MS-SQL

```
SBNewTabs442.cmd {options} MSSQL
```

DB2 UDB

```
SBNewTabs442.cmd {options} DB2UDB
```

DB2 for z/OS

```
SBNewTabs442.cmd {options} DB2ZOS
```

Migration to the Active Directory Integration feature

A customer who intends using the Active Directory Integration feature at the same time as migrating their installation to Release 4.4.2 does not need to perform any migration steps for their SignBase database. Instead they should follow the instructions in the *Kofax FraudOne Administrator's Guide* dealing with the installation of the Active Directory Integration feature.

In summary, this consists of setting up the SBDebTab.properties file to describe their Active Directory installation and running the command

```
SBDebTab --resetusermanagement
```

Notice that there is no way to preserve any existing user, group and access rights information during the conversion to Active Directory Integration (even if some customer specific Active Directory solution was in use previously.)

Database migration from releases before 4.4.1

If an update of the database from a release before Release 4.4.1 is required it is necessary to follow the migration steps for each release step separately (so from 4.2 to 4.3 then 4.3 to 4.4.1) in the correct order. The migration scripts and programs for the earlier releases are included in the Release 4.4.2 shipment. The description of the migration steps from 4.3 to 4.4.1 are included in Migration guidelines for earlier releases below. Migration steps from earlier releases should be taken from the migration guides of the appropriate release(s).

Migration guidelines for earlier releases

These guidelines are intended to use if you want to upgrade from a FraudOne version prior to Release 4.4.1.

Database migration from Release 4.3 to Release 4.4.1

Migration of an existing Data Warehouse database is done using customer specific scripts supplied as part of the migration package by Kofax. Follow the instructions for the Data Warehouse migration supplied with these scripts after the normal completion of the DFP for the last Release 4.3 production day.

The normal migration path for a SignCheck database from Release 4.3 to Release 4.4.1 requires that the database is empty of production data (after the DFP has copied any data to be saved for the last production day to the Data Warehouse). The SignCheck database tables are then deleted and the empty tables in the Release 4.4.1 format are created. This is done using the normal SCDebTab installation program.

Migration of the SignBase database from Release 4.3 to Release 4.4.1 is carried out using 2 database scripts. The installation package includes 2 scripts for each of the supported database type. The scripts are called SBNewTabs44_db2.db2, SBNewTabs441_db2.db2, SBNewTabs44_MS.sql, SBNewTabs441_MS.sql, SBNewTabs44_Oracle.sql and SBNewTabs441_Oracle.sql.

For SQL Server only: After running the migration scripts, the FraudOne stored procedures must be refreshed using the SBDebTab command program with the "--storedprocedureonly" parameter.

You may need to modify the scripts before execution. The scripts assume a database schema name which may be different to that used in your installation and you must change the schema name to match your installation before you execute your script.

Choose the correct scripts for your installed database type and follow the appropriate instructions below:

Oracle Syntax

```
sqlplus "<user>[@connect_identifier] AS SYSDBA"@SBNewTabs44_Oracle.sql
sqlplus "<user>[@connect_identifier] AS SYSDBA"@SBNewTabs441_Oracle.sql
```

(Notice "as SYSDBA" may not be required/allowed depending on the permissions given to the user-id you are using.)

MS-SQL Syntax

```
sqlcmd –S <server> -U <user> –d <database> –i SBNewTabs44_MS.sql
```

```
sqlcmd –S <server> -U <user> –d <database> –i SBNewTabs441_MS.sql
SBDebTab.cmd --storedprocedureonly –s <sv> –u <us> –x <pw> –d <db>
```

DB2 Syntax

```
db2 connect to <database> user <user>
db2 –tvf SBNewTabs44_db2.db2
db2 –tvf SBNewTabs441_db2.db2
db2 connect reset
```

Access rights after migration

Release 4.4.1 includes new access rights controlling the ability to edit highlight patterns, check serial numbers and core properties files. After migration, these access rights are automatically assigned to all users that currently have the SB_Administrator access right. The customer should modify the assignments to ensure that these rights are correctly assigned to only those users that require them.

Database migration from releases before 4.3

If an update of the database from a release before Release 4.4.1 is required it is necessary to follow the migration steps for each release step separately (so from 4.2 to 4.3 then 4.3 to 4.4.1) in the correct order. Since the migration to 4.4.0 is obsolete with the availability of Release 4.4.1, the step from 4.3 to 4.4.0 is included here. The migration scripts and programs for the earlier releases are included in the Release 4.4.1 shipment. The descriptions of the migration steps should be taken from the migration guides of the appropriate release(s).

ParaScript installation

Introduction

CheckStock® verification and CheckPlus® recognition are a simple protection against fraud checks.

CheckStock® - compares the checks against reference checks stored in the system.

CheckPlus® - recognizes defined fields on the checks, such as CAR (Courtesy Amount Reading), LAR (Legal Amount Reading) and Payee names.
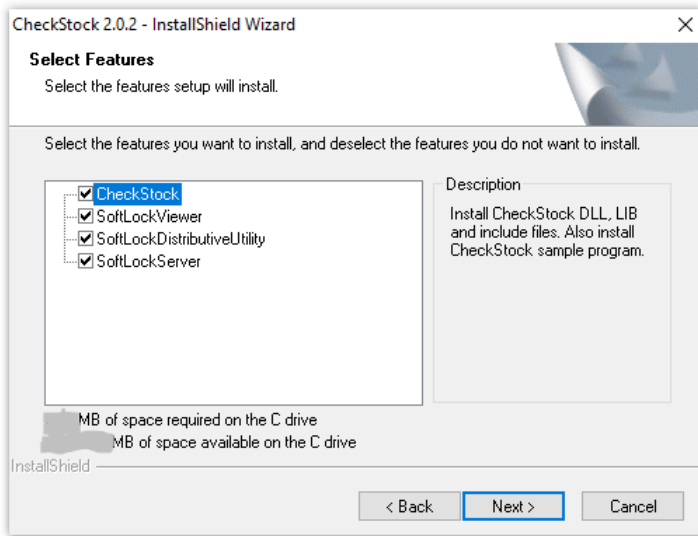
Install CheckStock

Preconditions

For detailed information on the requirements for installing CheckStock, see section ParaScript CheckStock installation.

Installation

To install CheckStock, follow these steps:

1. Go to the Kofax FraudOne installation directory.
2. Search for the CheckStock_x_x_x.zip file and unzip this file in a tmp directory.
3. Go to the unzipped CheckStock directory.
4. Change into the setup directory and execute the file Setup.exe.
5. Follow the instructions on the screen.

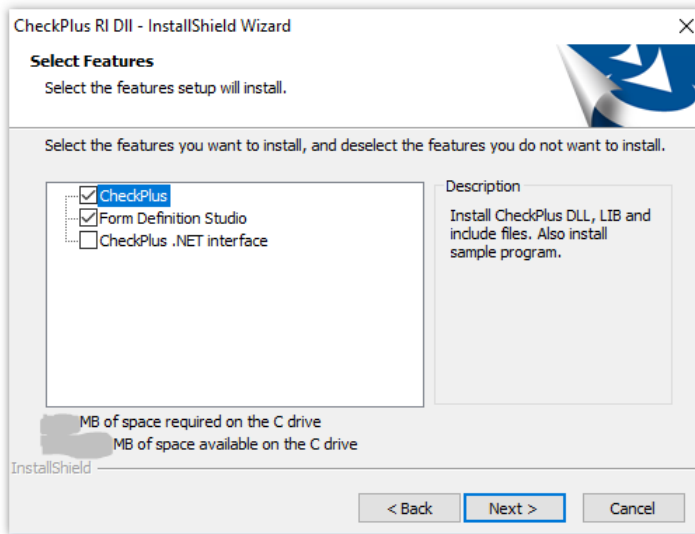ℹ️ We recommend to keep the default settings.

Install CheckPlus

Preconditions

For detailed information on the requirements for installing CheckPlus, see section ParaScript CheckPlus installation.

Installation

To install CheckPlus, follow these steps:

1. Go to the Kofax FraudOne installation directory.
2. Search the CheckPlus_x_x_x.zip file and unzip this file in a tmp directory.
3. Go to the unzipped CheckPlus directory.
4. Change into the setup directory and execute the file Setup.exe.
5. Follow the instructions on screen.

Kofax FraudOne Installation and Migration Guide

ⓘ We recommend to keep the default settings.

6. After the CheckPlus setup is finished, copy the checkplus.DLL of the CheckPlusx.x.x\bin directory into the CheckPlus installation ..\bin directory.

Install licenses

CheckStock uses a softlock mechanism. To use CheckStock you must request and install a softkey from Kofax.
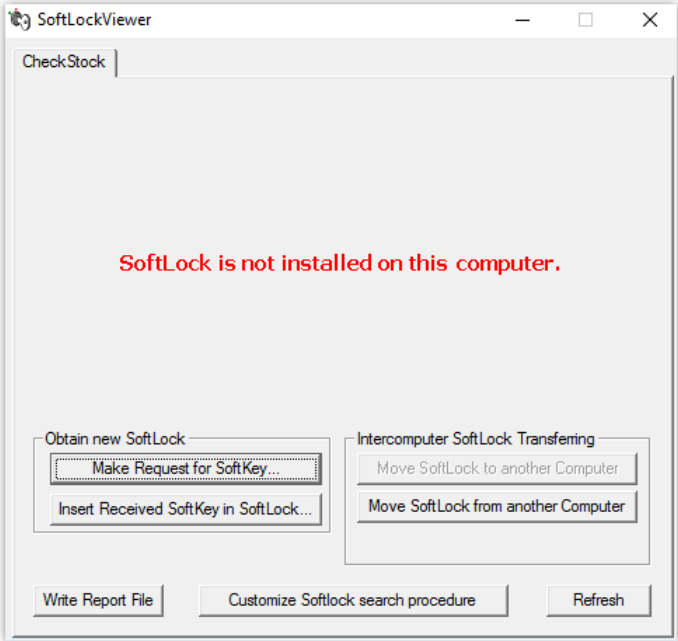
Follow these steps:

1. Open a command window from Windows with cmd.exe.

2. Go to the directory C:\Program Files (x86)\Parascript\Common Files\SoftLock, if you had selected the default settings.
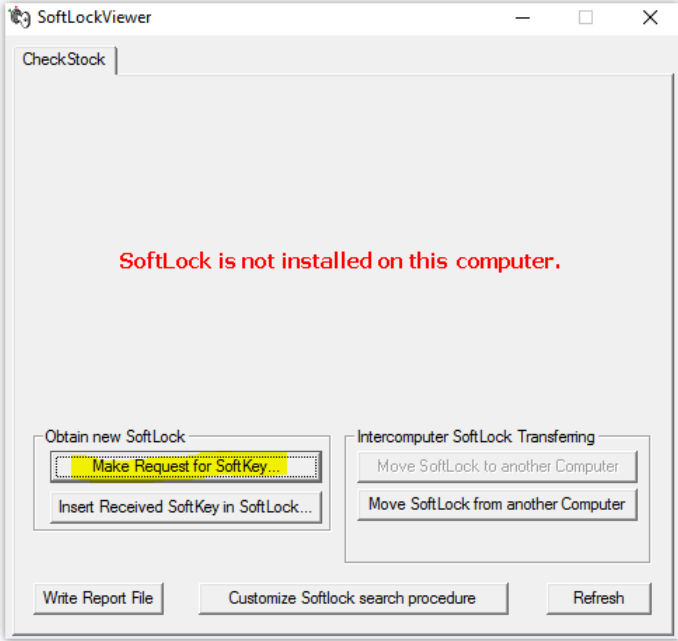
On the real production machine:

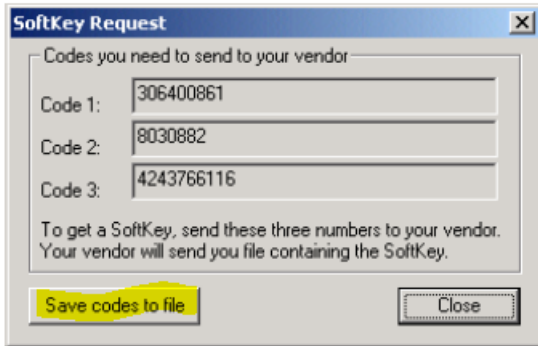1. Run the SoftLockViewer2.exe file.

On the virtual production machine:

1. Run SoftLockViewer2.exe /psenablevm.

32

2. Create the softkey request file by clicking **Make Request SoftKey**.


3. The following request appears:

4. Click **Save codes to file** and save the numbers in a file with an .slc extension.

5. Send this softkey request file (e.g. CheckStock.slc) to licensing@kofax.com and Kofax will send the softkey to you. The softkey file has the extension .psk (e.g. CheckStock.psk).

6. Close the SoftLock Viewer.

After you received the softkey:

1. Run SoftLock Viewer again with SoftLockViewer2.exe.

2. Click **Insert Received SoftKey in SoftLock**.

.
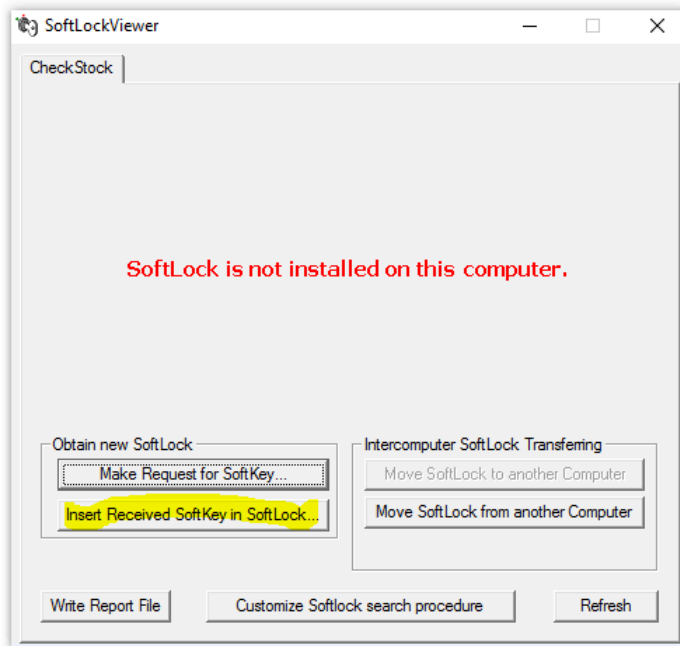
3. Locate and select the SoftKey file and click **Open**.
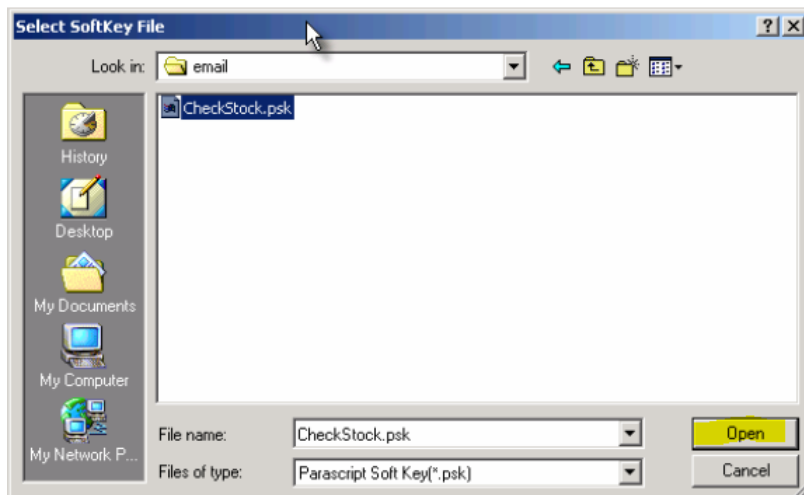
4. Now the installation is finished and you can close the SoftLock Viewer.