

# Kofax FraudOne

## Release Notes

Version: 4.5.0

Date: 2020-10-28

The logo for KOFAX, consisting of the word "KOFAX" in a bold, blue, sans-serif font.

# Table of Contents

<b>Chapter 1: About this release</b> .....	<b>5</b>
Version information.....	5
System requirements.....	5
Product documentation.....	5
Online documentation.....	5
Offline documentation.....	5
New features.....	5
Integration of the Parascript-Engine.....	6
<b>Chapter 2: Resolved issues</b> .....	<b>7</b>
Server did not communicate long group names in Message2A responses to Message1D.....	7
SCServerInterface tried to instantiate non-existent messages.....	7
Incorrect client behavior.....	7
Oracle Active Directory generated multiple user records.....	8
Server does not communicate group membership from Active Directory to the client.....	8
Admin Client: Unable to get OIDs for Insert GroupAccess.....	8
PacakgeInputStream NPE: buffer was null.....	8
SignBase server chose Active Directory authentication when a migrated SPX_USER table was present.....	9
Admin Client: User-ID could not be copied from the search list into the entry field.....	9
Admin Client: New GroupId and UserId not editable.....	9
Admin Client User-ID field was too short.....	9
Special characters not displayed correctly.....	9
Exception in UserCredClearExtension.....	9
Java Client did not display CheckStock image.....	10
Current queue not selected.....	10
DDL generator error in OID sequences with Oracle DBMS.....	10
Incorrect table name used resetting OID in the Oracle Rules table.....	10
Irregular behavior after account updates were saved.....	10
Java Client for FraudOne 4.3 could not process messages from 4.4.1 servers.....	10
FraudOne Thin Client took message resources from files.....	11
Signature watermark truncated.....	11
Java Client could cause database inconsistency when removing signatory variant.....	11
Missing risk indicators for External Document feature results.....	11
Java Client could not be configured to display "observed" serial number ranges.....	11

Java Client displayed serial number range incorrectly.....	11
Program DWH2SB (Service Programs) fails when a BankCode is non-numeric.....	12
Java Client closed application before AIS operation finished.....	12
Incorrect return code handling from search for signatory name.....	12
SQL Error saving a new Active Directory user group record in Oracle.....	12
Insert User response message did not contain final Logon ID.....	12
OID formatting failed when OID value exceeded 18 digits.....	12
Admin Client failed assigning access rights to new user.....	13
Inconsistent data retrieved for some accounts.....	13
No risk indicator was visible for EXTERNAL_DOCUMENT.....	13
JavaAPI: Extra byte in image data when sending Message1A_BC.....	13
Application server cannot process version of MessageA911.....	13
ServicePrograms: Substitution did not occur when no default value was specified.....	13
WFRouter exception when payment document not found.....	13
LogonSession sent a logon message with no authentication parameters.....	14
Incorrect limit generating Signature or Image licence warning message MGS0408.....	14
Admin Client could not select Active Directory group name longer than 20 characters.....	14
Active Directory integration did not authenticate users.....	14
Automat ASV deposit: Set wrong ResultCode.....	14
SignBase application server failed to create a reference signature.....	14
FraudOne servlet interface rejected a null value password.....	15
CRS reported SQL errors.....	15
Java Client: SignCheck client sent message without authorization data.....	15
AMS0396 error sometimes reported for Attach Manager.....	15
Attach Manager crashed processing Insert Configuration Element message from PS tooling.....	15
Display language change failed in Thin Client.....	16
SQL Error reading STOCKIMAGE records with SQL Server only.....	16
Deletion of authorized Active Directory user caused issues.....	16
SignBase: Application Server failed for deleted Active Directory user.....	16
Dynamic signature length exceeded column limit.....	16
SBNewTabs44_db2.db2 contained incorrect syntax.....	16
SBNewTabs44_db2.db2 failed on DB2 11.....	17
<b>Chapter 3: Known issues.....</b>	<b>18</b>
Oracle: Incorrect timestamps used after DST change.....	18
Validation does not support Content Type 8 or 9.....	18
SetupCfg failed when used with a new Active Directory user as authorization source.....	18
Database migration script generates inconsistent SPX_UR records.....	19
ServerInterface connection pool cannot address the ArchiveInterfaceServer.....	19

SAE Server fails to write a result when throughput license exceeded..... 19  
Server Manager failure after Database connection outage..... 19

## Chapter 1

# About this release

The release notes give you information about Kofax FraudOne 4.5.0. Please read this document carefully, as it may contain information not included in other product documentation.

## Version information

The build number for Kofax FraudOne 4.5.0 is 4.5.0.0.0.210.

## System requirements

For information on supported operating systems and other system requirements, see the *Kofax FraudOne Technical Specifications* document on the [Kofax FraudOne Product Documentation site](#). The document is updated regularly, and we recommend that you review it carefully to ensure success with your FraudOne product.

## Product documentation

The FraudOne product documentation set consists of guides and help systems to assist you with installing, configuring, and using the software.

### Online documentation

The product documentation for Kofax FraudOne 4.5.0 is available online:

<https://docshield.kofax.com/Portal/Products/FO/4.5.0-th2k87ey6r/FO.htm>

### Offline documentation

Customers who require offline documentation can download `KofaxFraudOneDocumentation_4.5.0_EN.zip` from the Kofax Fulfillment Site. The .zip file includes both help and print directories.

## New features

This section lists enhancements introduced to the product in Kofax FraudOne 4.5.0.

## Integration of the Parascript-Engine

The Parascript-Engine enables the analysis of "not on us" checks at the bank of first deposit.

The integration of the Parascript-Engine restores the following A2iA functionality that was available prior to Kofax FraudOne 4.3.0.

- CheckStock verification
- LAR/CAR processing
- Payee Name verification

## Chapter 2

# Resolved issues

This chapter lists issues that have been resolved since Kofax FraudOne 4.4.2R2.

## Server did not communicate long group names in Message2A responses to Message1D

**1539008:** For Active Directory, when a group is inserted, the supplied group name is verified against Active Directory and the name is converted to upper case for storage in the database. In addition, the server generates a short form name in those cases where the real name is longer than 20 characters. In earlier releases, the server did not report both changes to the client in order to generate the short form name.

## SCServerInterface tried to instantiate non-existent messages

**1536854:** When the SCServerInterface client was started, it attempted to instantiate non-existent message.

## Incorrect client behavior

**1536488:** The following incorrect behavior can be observed (Active Directory enabled).

1. Disabled "remove" button in Group Management (probably when there are group membership records present). Notice, although we are not allowed to manage the Active Directory group membership directly, the server does send "invented" group membership records to the client and the client can send "delete" requests to the server for those group memberships. (The server just ignores the delete requests since there are no records in the database backing them.)
2. Adding new group, after searching in active directory and selecting a very long name, (search for %irvine%), the long name (truncated for display) is shown in the list. After pressing "Apply" this changes to the surrogate short name ("@AAA..."). This is incorrect, the short names are never intended for display, they are used for the database linkage in foreign key columns where the length is restricted to 20 characters).
3. After adding a new user by takeover from the Active Directory search results, no rights are shown in the list display even if the user is a member of a group that already has rights in the database. This is because there are no group membership records that would allow the active rights to be shows. In this case, the client would need to ask the server to provide the group membership records

that correspond to the new user. After an "apply", this can be done by simply refreshing the User Management workspace from the server (as is done when the "cancel" button is pressed when changes have been made and not yet applied). Before "apply" however, there is currently no way of asking the server to provide group membership information for a user that is not yet saved to the database. This needs to be discussed.

4. When a new group is added and rights assigned to it, the client is not aware of any group membership information for the new group. If there are users present in the User Management display that are members of the new group, these will not be updated to show any rights assigned to the new group. This information is first available when all changes are applied and the user management workspace is refreshed from the server.
  - a. a) There is no way to trigger this refresh currently other than switching away from User Management and back or logging off and on. The client should refresh the workspace from the server after every apply transaction that creates a group,
  - b. b) Before they apply, there is currently no way of asking the server to provide group membership information for any users and groups not yet saved to the database. This needs to be discussed.

## Oracle Active Directory generated multiple user records

**1536405:** FraudOne created user records in the database dynamically for Active Directory when users with FraudOne access rights from one or more of their group memberships were logged on. A new user record was created incorrectly for every logon attempt for such a user.

## Server does not communicate group membership from Active Directory to the client

**1535960:** The server correctly establishes group membership for each user being logged on and uses this to manage the "effective rights" communicated to the clients. However, the Admin Client function User Management requires the "effective" group membership of each user in the database in order to show the effective rights dynamically in the User Management dialogs.

## Admin Client: Unable to get OIDs for Insert GroupAccess

**1533002:** When changing the access rights for newly created Group, the Admin Client incorrectly retrieved the OID.

## PackageInputStream NPE: buffer was null

**1532756:** The buffer content was referenced even though result messages were not present.

## SignBase server chose Active Directory authentication when a migrated SPX\_USER table was present

**1530604:** The automatic Active Directory authentication mode selection operated incorrectly when the database was migrated from a previous release.

## Admin Client: User-ID could not be copied from the search list into the entry field

**1524580:** User-ID could not be copied from the search list into the entry field.

## Admin Client: New GroupId and UserId not editable

**1524565:** The entry fields for both GroupId and UserId could be copied from the search results list but they were not editable.

## Admin Client User-ID field was too short

**1524562:** The AD UserID could not be seen in the status bar. The User-ID field was too short.

## Special characters not displayed correctly

**1524365:** Special characters were not displayed correctly in the client.

## Exception in UserCredClearExtension

**1524189:** If the server did not provide a long user/group logon ID, the following exception occurred in UserCredClearExtension.

```
E 2020-08-27 14:50:02.039 -: PackageInputStream.readNextmessage() - an error
occured: , null E 2020-08-27 14:50:02.041 -: java.lang.NullPointerException E 2020-08-27
14:50:02.041 -: at java.lang.String.<init>(Unknown Source) E 2020-08-27 14:50:02.042 -: at
de.softpro.signplus.serverinterface.UserCredClearExtension.getLogonId(UserCredClearExtension.java:103)
E 2020-08-27 14:50:02.042 -: at
de.softpro.signplus.client.serverinterface.Message2A.setHeaderExtension(Unknown Source) E
2020-08-27 14:50:02.042 -: at
de.softpro.signplus.client.serverinterface.PackageInputStream.readNextMessage(Unknown Source)
```

## Java Client did not display CheckStock image

**1523716:** The client being used was incorrectly generating the content of Message 11, version 9. The client sent an incorrect flag ('4') to the server to get the CheckStock image.

## Current queue not selected

**1517128:** The current queue and the menu bar GUI were not synchronized with each other. When the SignCheck menu was created, the current queue was not selected in the menu bar.

## DDL generator error in OID sequences with Oracle DBMS

**1516707:** The generation of a DDL with the parameter "DisplayOnly=yes" was not successful, and the output did not generate usable SQL.

## Incorrect table name used resetting OID in the Oracle Rules table

**1516478:** After migrating a FraudOne 4.2 Oracle database to version 4.4.2, it was not possible to load the Base Configuration, which caused issues with OID sequences.

## Irregular behavior after account updates were saved

**1511057:** After using Java Client to edit an account, a prompt appeared to save a workspace that was already saved.

## Java Client for FraudOne 4.3 could not process messages from 4.4.1 servers

**1502292:** The following message appeared when the Java Client for FraudOne 4.3 attempted to process messages from FraudOne 4.4.1 servers.

```
D 2020-07-21 15:57:25.884
-: Message.CreateMessage - Create Message of type 20 E 2020-07-21
15:57:25.885 -: PackageInputStream.readNextmessage() - an error
occurred: , Object type mismatch in message20 E 2020-07-21
15:57:25.885 -: java.io.IOException: Object type mismatch in
message20
```

## FraudOne Thin Client took message resources from files

**1497277:** The FraudOne Thin Client took message resources from files instead of the configuration server.

## Signature watermark truncated

**1494852:** For some signatures, the watermark was truncated on both ends when rotated 90 degrees. This issue occurred with some signatures that were short in height.

## Java Client could cause database inconsistency when removing signatory variant

**1491158:** The deletion of signatories with dependent variants did not correctly handle the unusual case of a variant dependent on two different signatories when only one of the signatories was deleted.

## Missing risk indicators for External Document feature results

**1488636:** The risk indicators for the External Document features (1802-1888) are missing.

## Java Client could not be configured to display "observed" serial number ranges

**1488436:** In earlier releases, the Java Client could not be configured to display observed serial number ranges.

## Java Client displayed serial number range incorrectly

**1488423:** As part of the account statistical information, the client displayed information from the STOCKIMAGE table "issued" serial numbers or "observed" serial number records (type 21 and 22 records). For at least some content values, the display was incorrect.

## Program DWH2SB (Service Programs) fails when a BankCode is non-numeric

**1487789:** A NumberFormatException occurs when any of BankCode, BNo or CountryId for a document is non-numeric or has more than nine digits. The application incorrectly assumes these fields are integer values. Any of these fields can contain non-numeric data and / or be longer than the maximum length of an Integer. For example, the BankCode can be 11 digits, which exceeds the limit of 9.5 digits for an integer.

## Java Client closed application before AIS operation finished

**1475619:** Java Client allowed closing the application before the AIS operation (commit document) was completed.

## Incorrect return code handling from search for signatory name

**1473335:** While performing a search for a signatory name, a timeout occurred.

## SQL Error saving a new Active Directory user group record in Oracle

**1472675:** Although an Admin Client search for an Active Directory group was successful, and the group was assigned rights from the user interface, a database error appeared when Apply was selected to save the group.

## Insert User response message did not contain final Logon ID

**1471994:** When the server was preparing the response message for an InsertUser action, the final version of the LogonId string inserted into the database should have been returned to the client in the message header but was not present. The similar field, UserId (short name) was correctly returned.

## OID formatting failed when OID value exceeded 18 digits

**1471237:** The OID passed to the function to read a signature, the originating signatory OID, was not correctly formatted when the number of active digits exceeded 18 digits.

## Admin Client failed assigning access rights to new user

**1471167:** Using the Admin Client to create a user and assign access rights to that new user failed in some cases.

## Inconsistent data retrieved for some accounts

**1470522:** When inquired for some accounts, the client produced this message: "Inconsistent data received from server." The error message appeared: "Expected monochrome signature not found for signatory." However, the signature for the signatories existed in the database.

## No risk indicator was visible for EXTERNAL\_DOCUMENT

**1468430:** The Risk Indicator for the SC\_INTERFACE field EXTERNAL\_DOCUMENT was not visible in the CRS editor of the configuration client.

## JavaAPI: Extra byte in image data when sending Message1A\_BC

**1467445:** Saving the CheckStock image in Blacklist Administration wrote an extra byte to the NCSTOCKIMAGE table. As a result, it caused errors when loading saved message from the server.

## Application server cannot process version of MessageA911

**1466153:** If a client sends an older format of MessageA911 to read a Blacklist Image, the server reports that it cannot find the image record (with a database "Record not found" generic error).

## ServicePrograms: Substitution did not occur when no default value was specified

**1461404:** There was a problem with the substitution logic in service programs. If you had a where<n> clause without a default<n> clause, the value did not get substituted.

## WFRouter exception when payment document not found

**1460730:** When the Getter attempted to insert the CRS result for a document and that document was not present in the SC\_INTERFACE table, the WFRouter process could fail.

## LogonSession sent a logon message with no authentication parameters

**1456698:** The LogonSession for the LogonPlugin sent a logon message without authentication parameters if a password was not provided.

## Incorrect limit generating Signature or Image licence warning message MGS0408

**1455936:** The Server Manager code calculating the licence warning limit was incorrect.

## Admin Client could not select Active Directory group name longer than 20 characters

**1454419:** Using the Admin Client User Administration to create a new group, after searching for new group names, the resulting list contained entries with names longer than 20 characters. When one of the names longer than 20 characters was selected, the OK button was disabled.

## Active Directory integration did not authenticate users

**1453919:** Using Active Directory integration did not work for some domains.

## Automat ASV deposit: Set wrong ResultCode

**1453549:** When processing deposit checks with the ASV, the resultcode was set incorrectly in the table SC\_RESULT.

## SignBase application server failed to create a reference signature

**1450501:** The SignBase application server generated a corrupt signature object and returned an error in this situation:

1. Feature to create a dynamic reference from three dynamic signatures was activated.
2. Feature to perform a multiple signatory update was also activated.
3. Database contained multiple target signatories, and at least two of them shared the same SIGNO.

## FraudOne servlet interface rejected a null value password

**1445998:** The FraudOne servlet interface did not accept an empty password.

## CRS reported SQL errors

**1414166:** When the CRS server was started with a customer hook enabled, the following errors occurred:

```
E 2020-03-16
02:59:19.2 Q CRS-1: VBS2268 [ZU90H]
ODBC: Error in
synchroniseAccumulators:synchroniseAccumulators fetch DK -1
SQL_ERROR E 2020-03-16 02:59:19.2 Q CRS-1: VBS2269 [ZU90H]
ODBC:
State:22003, Native Error:0, Message: [Microsoft][SQL Server Native
Client 11.0]Numeric value out of range And, variables in
CRSDBHelper.ini cannot be loaded.
```

## Java Client: SignCheck client sent message without authorization data

**1412286:** The SignCheck client sent a message that did not include the required authorization data.

## AMS0396 error sometimes reported for Attach Manager

**1409309:** When a single client process (with a persistent connection to the Attach Manager) generated a high volume of transactions the Attach Manager sometimes issued the following AMS0396 error before terminating the client session: Unexpected data received from client

## Attach Manager crashed processing Insert Configuration Element message from PS tooling

**1407547:** The message sequence Logon, Read AddressMap, Fetch Configuration Item, Insert Configuration Item (00,AA0C,AA00,AA02) caused the Attach Manager process to end without an error message.

## Display language change failed in Thin Client

**1402236:** If you attempted to change the display language from English to German for the Thin Client, it did not work, even though a success message appeared.

## SQL Error reading STOCKIMAGE records with SQL Server only

**1401435:** When a ReadCompleteCustomer request included one or more STOCKIMAGE records, the server reported the following error.

```
VBS2268 [Zu90R]
ODBC: Error in ReadStockImageData:StockImage ResultSet Fetch 1 SQL_SUCCESS_WITH_INFO
VBS2269 [Zu90R]
ODBC: State:01004, Native Error:0, Message: [Microsoft][SQL Server Native Client
11.0]String data, right truncation
```

## Deletion of authorized Active Directory user caused issues

**1400832:** The Admin Client could not display the current list of authorized users if the following situation occurred:

1. FraudOne Active Directory Integration was active.
2. An Active Directory user was removed for someone who was also an authorized Admin Client user.

## SignBase: Application Server failed for deleted Active Directory user

**1399973:** The application server failed on a deleted user in Active Directory when accessing user management in Admin Client.

## Dynamic signature length exceeded column limit

**1364151:** When the length of dynamic reference signatures exceeded the database column limit of 32K bytes, a failure occurred.

## SBNewTabs44\_db2.db2 contained incorrect syntax

**1342511:** Line 26 of SBNewTabs44\_db2.db2 contained the incorrect syntax:

```
set current schema = DEB; -- !
```

## SBNewTabs44\_db2.db2 failed on DB2 11

**1342503:** When running the script SBNewTabs44\_db2.db2 to upgrade the database, the following statement resulted in the following error:

```
alter table SP_ADDRESSMAP
add column LCMACHINENAME varchar(40) not null generated always as
(lower(MACHINENAME ))
add column LCFILENAME varchar(40) not null generated always as (lower(FILENAME ))
add column LCINSTANCENAME varchar(40) not null generated always as
(lower(INSTANCENAME))
add column LCINSTANCETYPE varchar(40) not null generated always as
(lower(INSTANCETYPE));
Error: DB21034E. The command was processed as an SQL statement because it was not a
valid Command Line Processor command.
During SQL-processing it returned: SQL20054N. The operation was not performed because
the table is in an invalid state for the operation.
Table name: "DEB.SP_ADDRESSMAP". Reason code: "22".
SQLSTATE=55019
```

## Chapter 3

# Known issues

This section contains information about potential issues that you may encounter while using Kofax FraudOne 4.5.0. Workarounds are provided, as applicable.

## Oracle: Incorrect timestamps used after DST change

**713838:** Customer records displayed as "Verify Pending" cannot be verified due to an incorrectly stored timestamp (TIME\_STAMP\_VERIFY).

**Workaround:** This Oracle ODBC driver issue can be partially resolved using a wording ODBC driver/DBMS combination.

## Validation does not support Content Type 8 or 9

**1542583:** When trying to use the validation script, the following error message appears:

```
EXTENSION6:1,1: Extension incorrect type (8)
```

Entries with Content Type = 8 or 9 have been detected in the extension tables.

## SetupCfg failed when used with a new Active Directory user as authorization source

**1536287:** If the user id supplied for example to SetupCfg -importworkspace is an Active Directory user that is not already present in the user table but has the required access rights through a group membership then SetupCfg fails during the import.

**Workaround:** The "superuser" configuration to use an Active Directory group as the superuser should not be used before the SetupCfg activities are completed. Once SetupCfg work is completed, the superuser can be changed to a group using SBDebTab -resetusermanagement.

## Database migration script generates inconsistent SPX\_UR records

**1523983:** The FraudOne 4.4.1 SignBase database migration script can generate invalid records in the SPX\_UR table when it adds the new access rights for SB\_EditSerial, SB\_EditHighlight and SP\_CoreProperties rights. Records can be generated that contain a duplicate key for a key that must be unique. For these records to be created, the database must be missing the index UXSXUR1 or this index must be incorrectly defined.

## ServerInterface connection pool cannot address the ArchiveInterfaceServer

**1472408:** The Java Client expects to use the server type "SIGNINFO" to address an AIS server (typical port 2015) and NOT the real "SIGNINFO" server, which is just a sub function of the SignBase server.

## SAE Server fails to write a result when throughput license exceeded

**1468746:** When the GIA-SAE Automat/Server are processing documents and the throughput license limit has been reached, the GIA Server attempts to write a result for each document and fails with an error message such as: 2020-05-19 08:10:23.7 L GIA-Server-2: AUS0237 GIA Throughput license exceeded!

## Server Manager failure after Database connection outage

**1461443:** A Server Manager process termination was reported with error code C0000374. This code is, generally, caused by a corrupted memory management block in the C runtime. The termination appears to be a consequence of a broken communication link to the Oracle database server.