

Setup Guide

Sage FRP Common Services

English version





Contents

1 General Information	6
2 Installation Guidelines	9
2.1.a General Guidelines	9
2.2 Special Recommendations for Oracle	9
3 CD-ROM Contents	11
4 Managing Workgroups	26
4.1 XDLO Presentation	26
4.1.a	26
4.1.b Introduction	26
4.1.c References	26
4.1.d Definitions	26
User	26
DBA	26
DataBase Administrator	26
DBO	27
System Administrator	27
Windows NT Account	27
Database	27
Database Access Account	28
Administrator	28
Workgroup	28
Data Link	29
4.1.e Architecture	29
General Overview	29
Storage	29
Exchange Schema	30
4.1.f Setup	31
Administration Computer	31
Client Station	32
4.2 Creating Workgroup (SQL Server)	33
4.2.a Defining a Workgroup Name	33
4.2.b Selecting a Provider	34
4.2.c Selecting a Database	36
4.2.d Configuration of Logical Units	37
4.2.e Creating/Updating Models	38
4.2.f Execution of Actions	39
4.2.g Selecting a Product	40
4.3 Creating Workgroup (Oracle 11g Server)	42
4.3.a Special Recommendations for Oracle	42
4.3.b Defining a Workgroup Name	42
4.3.c Selecting a Provider	42
4.3.d Selecting a Database	43
4.3.e Creating/Updating Models	45
4.3.f Script Execution	46
4.3.g Selecting a Product	47
4.4 Updating a Database	48
4.4.a Updating Data	48

4.5 Adding Workgroups	48
4.6 Updating the Databases of a Workgroup	49
4.7 Managing Workgroup's Users	52
5 User Management	59
5.1 Introduction	59
5.2 Authentication	59
5.2.a Definition	59
5.2.b Windows NT Authentication	59
5.2.c UMAPI Authentication	60
5.2.d LDAP Authentication	61
5.2.e User Account	64
5.2.f Login.....	67
o The administration of access permissions for users of the selected workgroup.	68
o The administration of the selected workgroup formats	68
o The administration of transcoding tables for the selected workgroup	68
5.3 Access Management	69
5.3.a Permissions	69
5.3.b Welcome Screen	70
5.3.c Profile or Role	71
5.3.d Managing Profile Rights	73
Managing rights with a single Security Administrator.....	73
Managing Rights with Two Security Administrators.....	76
5.4 Audit.....	83
5.4.a Definition	83
5.4.b Audit Management	83
Tables Organization	83
Deleting/exporting System/User Audit Events and Database	88
6 Traces.....	91
7 Formats.....	95
8 Transcoding Tables	106
8.1 Introduction	106
8.2 General Tables	106
8.2.a "CurrencyDecimals" Table	106
8.2.b "RIBs" Table	106
8.2.c "GenerationNumbers" Table	106
8.2.d "RIB_DESC" Table.....	106
8.3 "AFB320_PARAM", the AFB 320 Table	107
8.3.a Setting up Amount Type	107
8.3.b Setting up Account Number Type	107
8.4 "PAYEXT96A_PARAM", the PAYEXT 96A Table.....	108
8.4.a Setting up the Structure of NAD Segments	108
8.4.b Setting up RFF Segment	108
8.5 "ascaebdv.dat", the IAEB 43 Table.....	108
8.6 AFB 120 Tables.....	109
8.6.a "ACSAFBVDV.DAT" Table	109
8.6.b "ACSAFBPA.DAT" Table	109
8.6.c "ACSAFBVE.DAT" Table	109
8.6.d "AFB120RT_PARAM" Table	109
8.7 FINSTA 96A Tables.....	110

8.7.a "acsfinstapa.dat" Table	110
8.7.b "ACSAFBVE.DAT" Table	110
8.8 "ACSMT_OP.DAT", the MT 940 Table	110
8.9 "MT101CAI_PARAM", the MT101 CAI Table	110
8.9.a Setting up Header Generation (Block 4)	110
8.9.b Setting up "Identifiant Telecom" (Tag 20)	111
8.9.c Setting up Tag 21	111
8.10 "MT101SG_PARAM", the MT101 SG Table	111
8.10.a Setting up "Identifiant Telecom" (Tag 20)	111
8.11 CODA Tables	111
8.11.a Isobbl Table	111
8.11.b convcib Table	112
8.11.c RES_CPT Table	112
8.11.d RES_DEV Table	112
8.11.e RES_COD Table	112
8.11.f RES_MES Table	113
8.12 "PAYORD91.2_PARAM", the PAYORD 91.2 Table	113
8.12.a Setting up SIRET Number	113
8.13 "PAY_CRLF" Table	113
8.13.a Setting up CRLF Type	113
8.14 "BAI2_PARAM", the BAI2 Table	114
8.14.a Setting up RTRIM process	114
8.14.b Controlling File Integrity	114
8.14.c Setting up Reference Type	114
8.15 "CALENDAR" Table	114
8.15.a Format of "VALUE" Column	115
8.16 "COUNTRY_CURRENCY" Table	115
8.17 "PAYMUL96A_PARAM" Table	115
8.18 "SWIFT_NET" Table	115
8.19 MT101 Fortis Table	116
8.20 DORMANTS_ACCOUNTS Table	116
9 License Management	117
9.1 License	117
9.2 Adding a New Product License	118
9.3 Modifying a Product License	118
10 Faults	120
10.1 XDLO does not work with a firewall between client station and administration computer	120
10.2 XDLO cannot be retrieved from the server	121
10.3 Display error of the screen resolution following a specific DPI configuration	121
10.4 The saving of the report in PDF format generates an error message after closing	123
10.5 The connection to the product using an NT account in lower case is not possible with ORACLE	124
11 Rules for Regular Identifiers	125
12 Details about the Database Installation Wizard	126
12.1 Product Installation Scenario	126
12.2 Actions on the Database	128
SQL SERVER 2005	129
Accessing SQL Server	129
Wizard Automatic Operations	129
Structure of SAGE ERP Treasury database (ex-XRT Universe)	129



Oracle 10G R2	129
Accessing Oracle.....	130
Wizard Automatic Operations.....	130
Warning:	130
Products, Tablespaces and Default Users.....	131
Tablespaces	132
Sage FRP Treasury (ex-XRT Universe) Tablespaces	132
13 Creating SQL 2008 and Oracle 11G Databases in a 64-bit Environment	134



1 General Information

Product Name	Sage FRP Common Services
Version No.	3.4
Patch	No
Minimum Previous Version	N/A
Available Modules	Administration Sage .NET – Sage License Manager
Tools	Clint3 – Microsoft MDAC 2.8 – Windows Script 5.6
License File	Yes
Configuration	
Databases	Microsoft SQL Server 2008 R2 (Standard edition and Professional edition) Microsoft SQL Server 2012 ORACLE 10G R2 with 32-bit client driver – version 10.2.0.1/4; ORACLE 11G R2 64-bit with 32-bit client driver
Validated Configurations	Client Stations: Windows 7 32-bit and 64-bit, Windows 8 Server Stations: Windows 2008 Server 32-bit and 64-bit R2, Windows 2012 Server Virtual environments: VMWare ESXi4, Windows 2008 Publication Server and Windows 2008 Server Virtualization
Non-validated configurations	Windows 95/2000/2003/XP SP3, Vista SP1, MS SQL Server 7, Internet Explorer 5 & 6, Oracle 9i, SQL 2005
Communication equipment	None
Compatibility with other XRT products	Sage Business Exchange Edition V11.35 Sage FRP/Bank Communication 3.21 Sage FRP/Bank Signature 3.21 Sage FRP Treasury Universe Edition 3.21
Coexistence on one PC	Only one version of Sage FRP Common Services can be installed
Hardware Prerequisites	Client station: 1 Go RAM minimum /3 GHz processor minimum Database server station: see DBMS editor recommendations Java Runtime: JRE Sun virtual machine (v1.6.0.20) 32-bit
Minimum Disk Space	Programs: 500 Mo Database server station: according to type (250 Mo minimum) Database: variable according to volume and type (250 Mo minimum)
Additional Information	
Internal Version No.	3.4.1.1
Project Name in TFS	CTO
User Documentation	Online documentation, Online help
Technical Documentation	Setup Guide
Demo Kit	Not Available

Important To manage the creation of SDD and SCT formats in FRP Treasury Payment or SBE Payment Web, you must install Java runtime, delivered along with XCS common services setup: "jre-6u17-



windows-i586-s.exe". Java runtime version 6 is required.

Important Java runtime must be **32-bit** in order to operate with our 32-bit applications. If installed, you will have to replace Jre 64-bit with "jre-6u17-windows-i586-s.exe", delivered along with Common Services setup.





2 Installation Guidelines

2.1.a General Guidelines

Guidelines included in this document describe how to install Sage Common Services. To install other XRT applications, such as Sage Business Exchange, see the guide related to the relevant product.

Before updating Sage platform, you need **to back up all your data**. You must remove all Sage applications first, then the tools.

Close all running applications before starting the installation of Sage Common Services.

Avoid using the **Previous** command while the application is being installed. In case of error, abort the installation and start again.








2.2 Special Recommendations for Oracle

Sage applications are tested on Windows operating systems. If Oracle server runs under another operating system, please contact the client's database administrator. (see 4.3)





3 CD-ROM Contents

	Products	Folder including the installation programs
	Common	
	Adobe	Acrobat Reader 6.0
	MDAC	Microsoft Data Access Component
	XCS	Sage Common Services installation program
	According to product	
	Guides	Setup Guide

The **Readme** folder includes the following installation guide(s) in Word or PDF format:

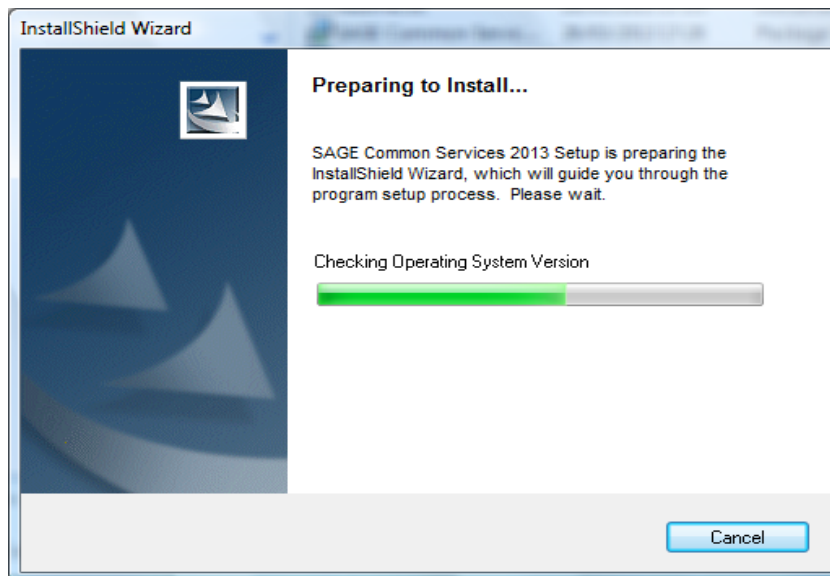
Sage FRP Common Services – Setup Guide 3 4 EN:

Setup guide for Sage FRP Commons Services

This folder contains various guides, depending on the product you purchased.

Important Sage FRP Common Services must be installed prior to installing any other programs. Make sure you remove any older version of Sage FRP Common Services!!

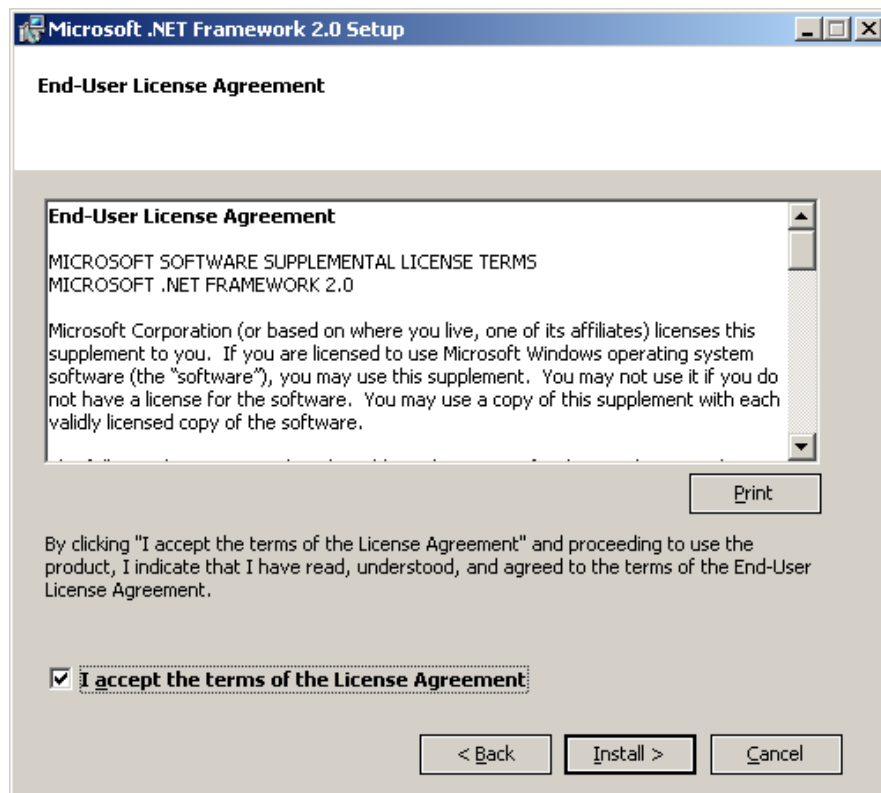
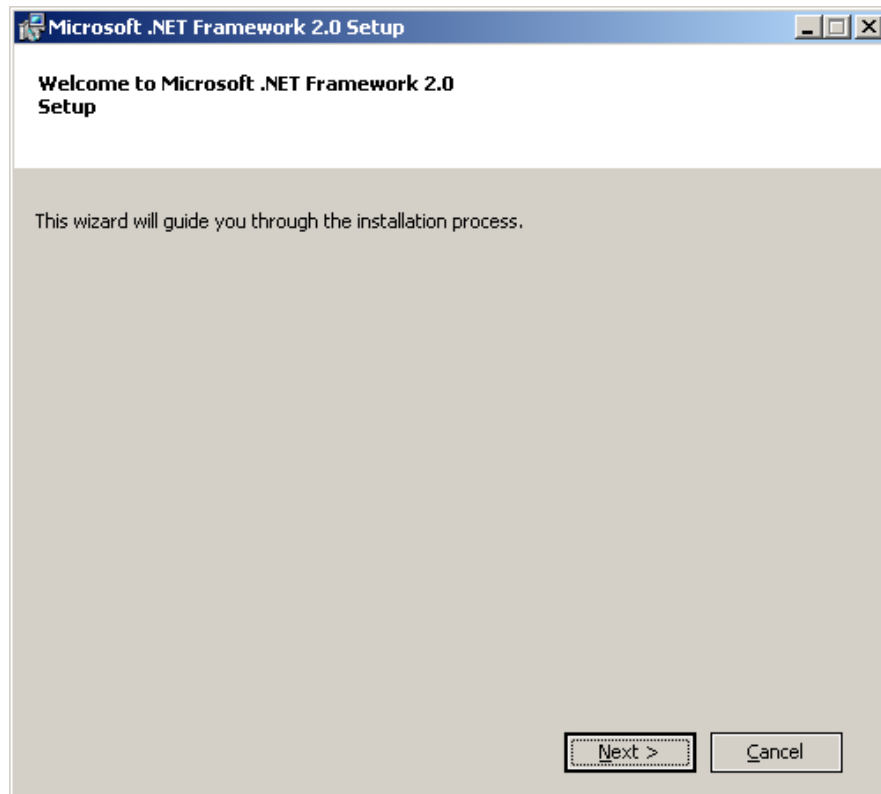
- 1 Insert the CD-ROM, go to **Products/Common/XCS**, and launch **Setup.exe**. The Install Shield Wizard starts.



Note If the Windows Installer or the Windows Script is not up-to-date, the **Install Shield** will automatically launch a new configuration and restart the system.

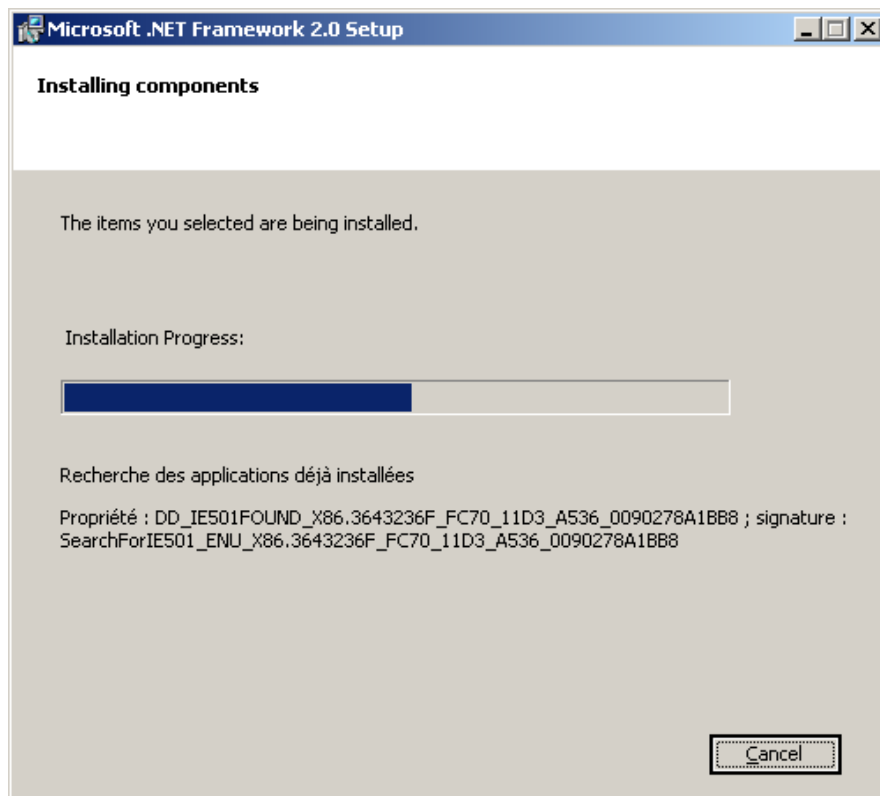
Important If you are installing Microsoft .NET 2.0 Framework for the first time, complete steps 2 to 4. Otherwise, go directly to step 5. Concerning 2003 Server Operating System, Microsoft .NET 2.0 Framework is integrated to the system.

- 2 Install Shield detects that Microsoft (R) .NET 2.0 Framework is not installed and prompts the user to install it. The **Install of Microsoft .NET 2.0 Framework** screen appears.
- 3 Click **Yes**. You must install Microsoft .NET Framework 2.0 for Sage products to function. The **Microsoft .NET Framework 2.0 Setup** screen appears:

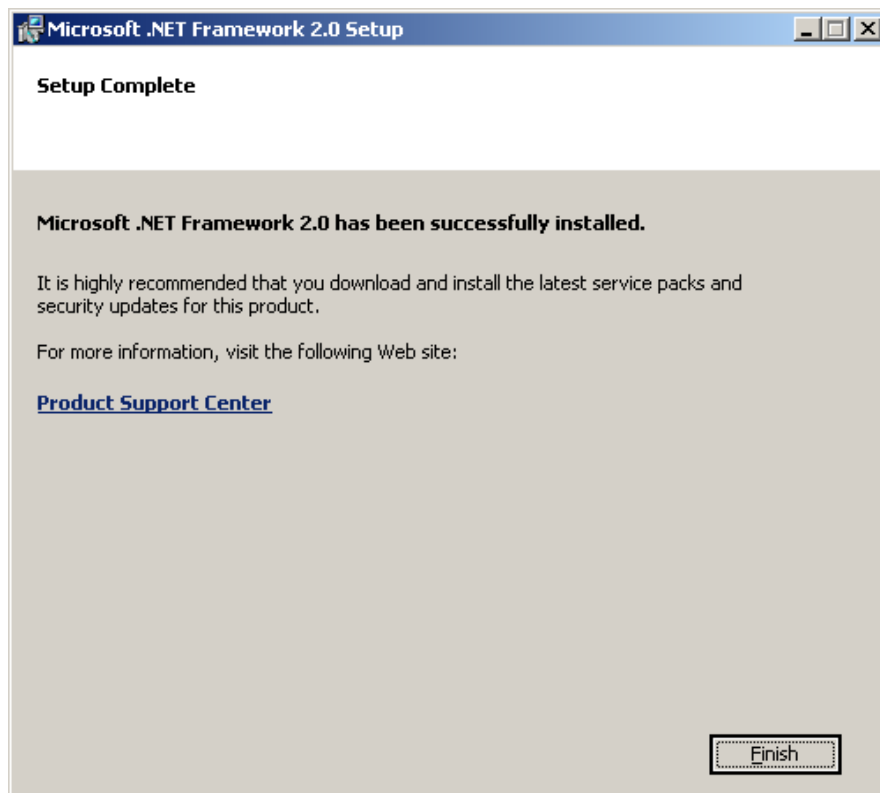


Select **I agree** (License of Framework 2.0).

- 4 Click **Install**.



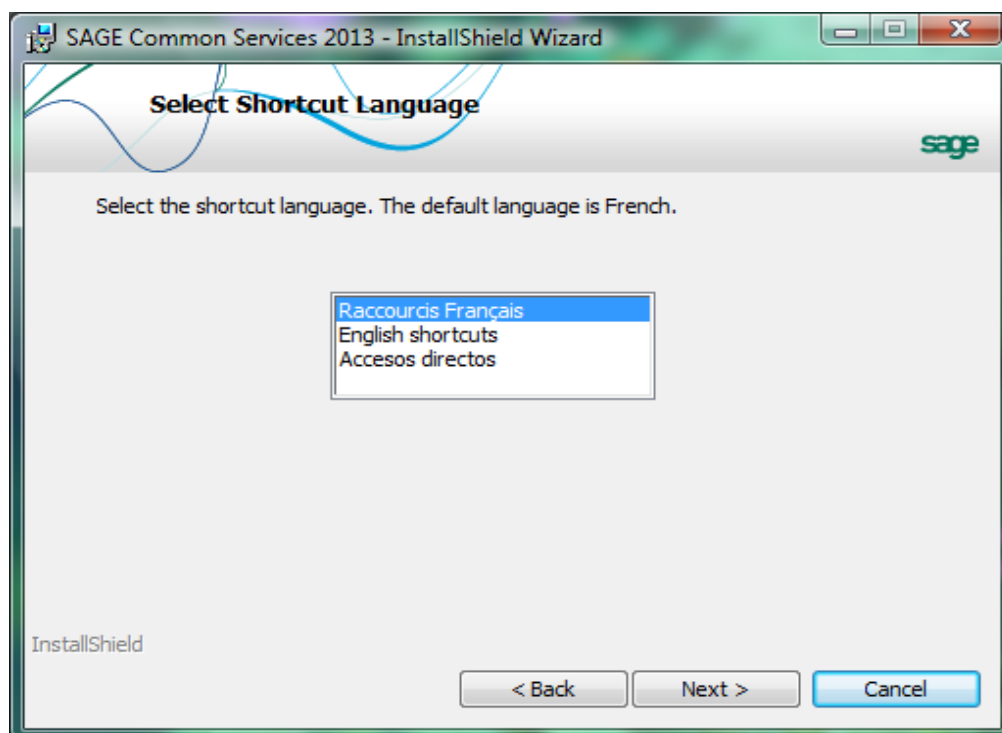
It may take a few minutes to install Framework 2.0 Components.



Click **Finish**.

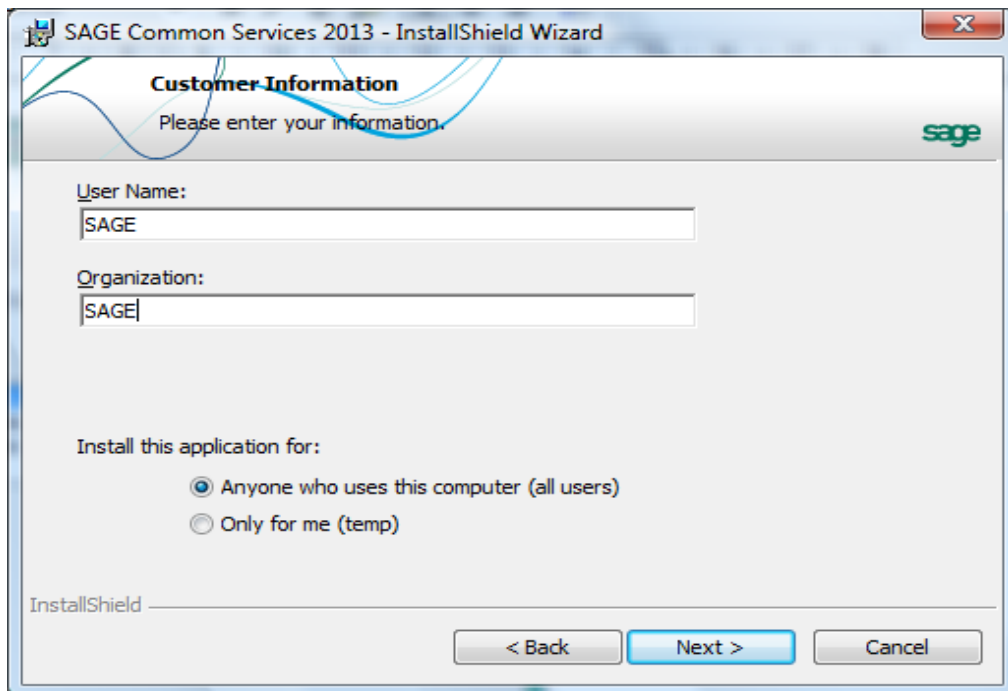


- 5 Click **Next**. The **Select Shortcut Language** screen appears:



Select a language.

- 6 Click **Next**.
The **Customer Information** screen appears:

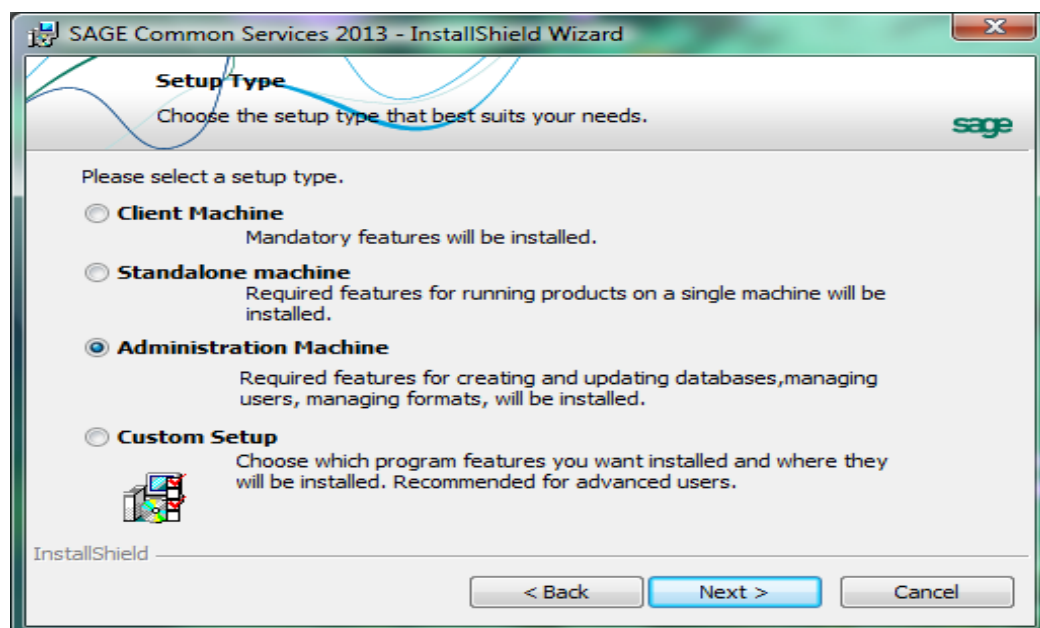


Enter your login name in the **User Name** field and the name of your company in the **Organization** field.

Select an accessibility option:

- The **Anyone who uses this computer (all users)** option allows any user of the station to access Sage FRP Common Services.
- The **Only for me** option allows restricting access to Sage FRP Common Services to the user logged in when the product was installed.

7 Click **Next**. The **Setup Type** screen appears:



Four types of installations are available:

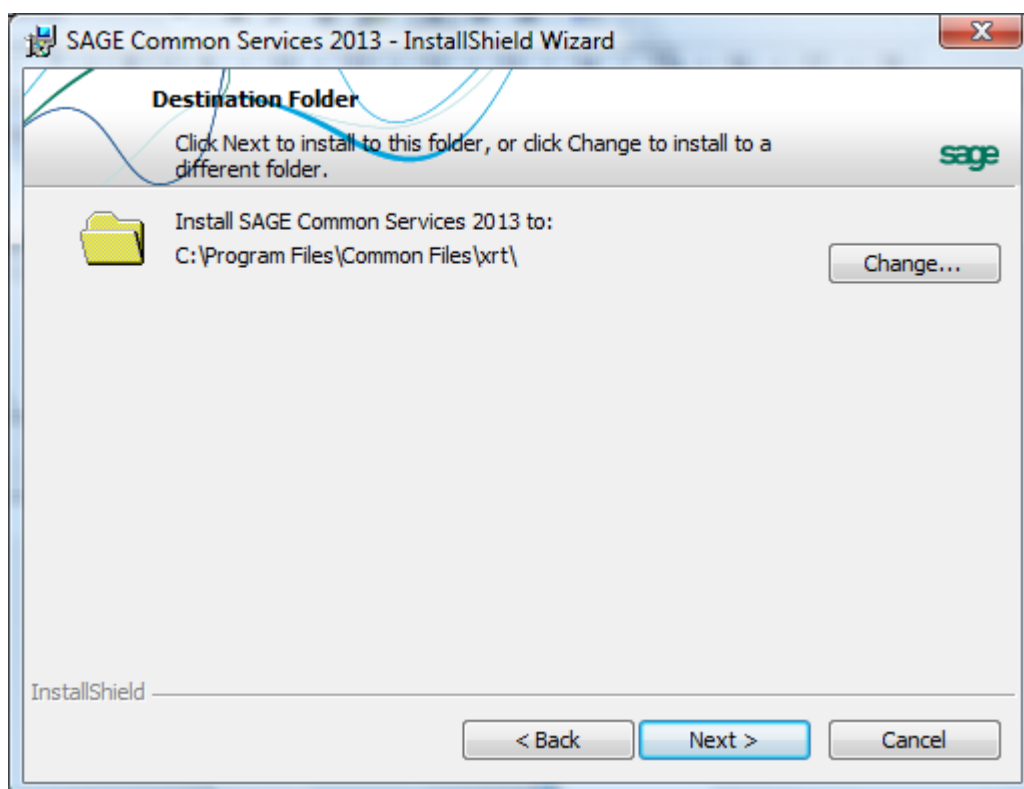
- **Standalone Machine:** To install administrations tools and products on the same computer. This option installs everything except the XCS service, which is required for automatic bank imports (**recommended by default**).
- **Administration Machine:** To set a dedicated Administration computer. All the components are installed.
- **Client Machine:** To install the tools required by Sage applications in network configuration (with a computer dedicated to the administration of Sage applications). This does not include the Administration tools.
- **Custom Setup:** To select the component(s) you want to install.

Features by installation type:

Feature	Standalone Machine	Administration Machine	Client Machine	Custom Setup
Administration Tools	✓	✓		
SQL Scripts	✓	✓		
SAGE Common Services Management Console	✓	✓		
XCS Service (which is required for automatic bank imports)		✓		
OWC (Office Web Components)		✓		
SAGE Common Services	✓	✓	✓	✓
FMTAPI	✓	✓	✓	✓
FMTPAY	✓	✓	✓	✓
Clint	✓	✓	✓	✓
X Mail	✓	✓	✓	✓
ICAPI	✓	✓	✓	✓
XDLO Service	✓	✓	✓	✓
Third Parties Components	✓	✓	✓	✓
DirectSkin30b	✓	✓	✓	✓
XML	✓	✓	✓	✓

Farpoint	✓	✓	✓	✓
Skin	✓	✓	✓	✓
Microsoft Runtimes	✓	✓	✓	✓
License Manager	✓	✓	✓	✓

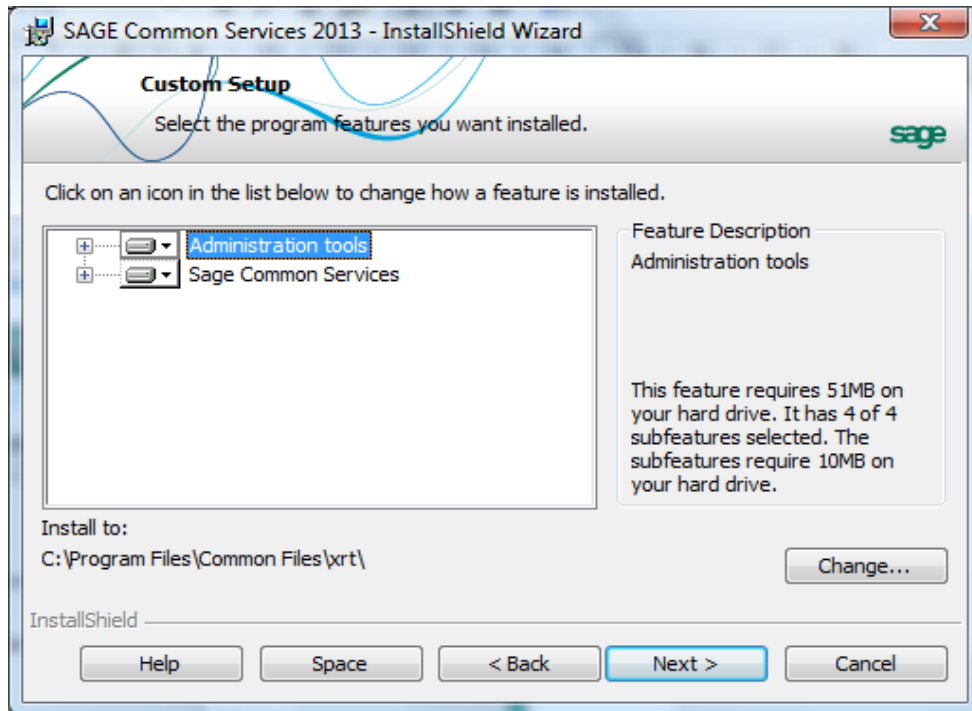
8. The Standalone Machine, Client Machine and Administration Machine installation types of XCS 2011 installation process enable to modify the installation path of the product without using the customized installation.



Note:

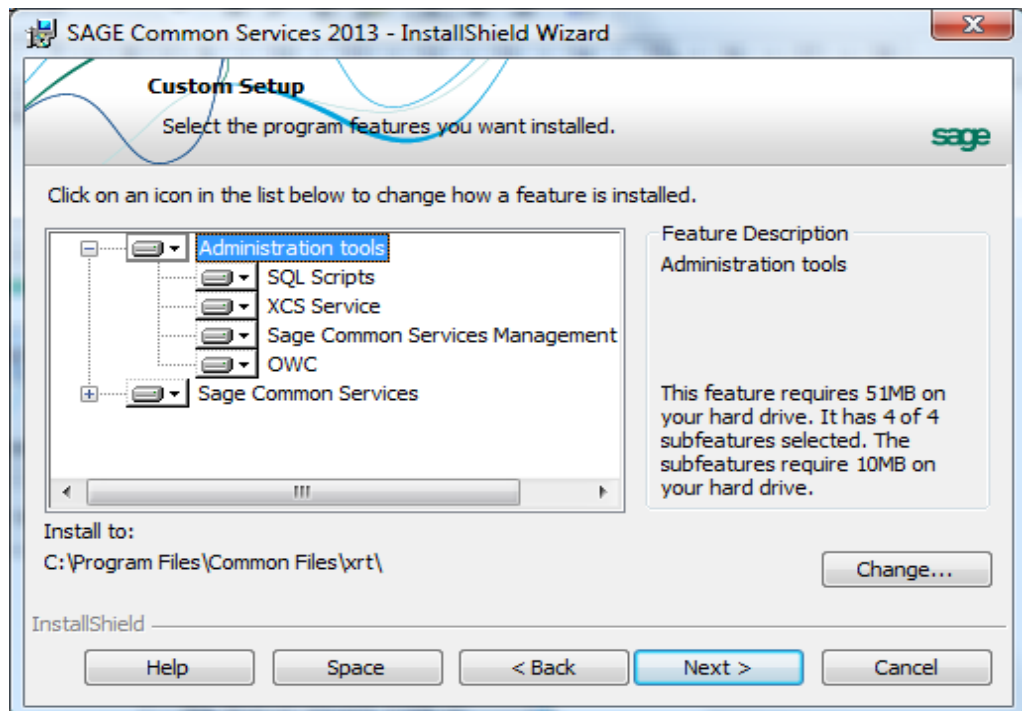
To install XCS service, which is required for automatic bank imports, you need to choose the "Administration Machine" installation type, or to choose the "Custom Setup" installation type and to follow these guidelines (for the standalone installation type, go to step 11):

9. Select the **Custom** option and click **Next**. The **Custom Setup** screen appears:

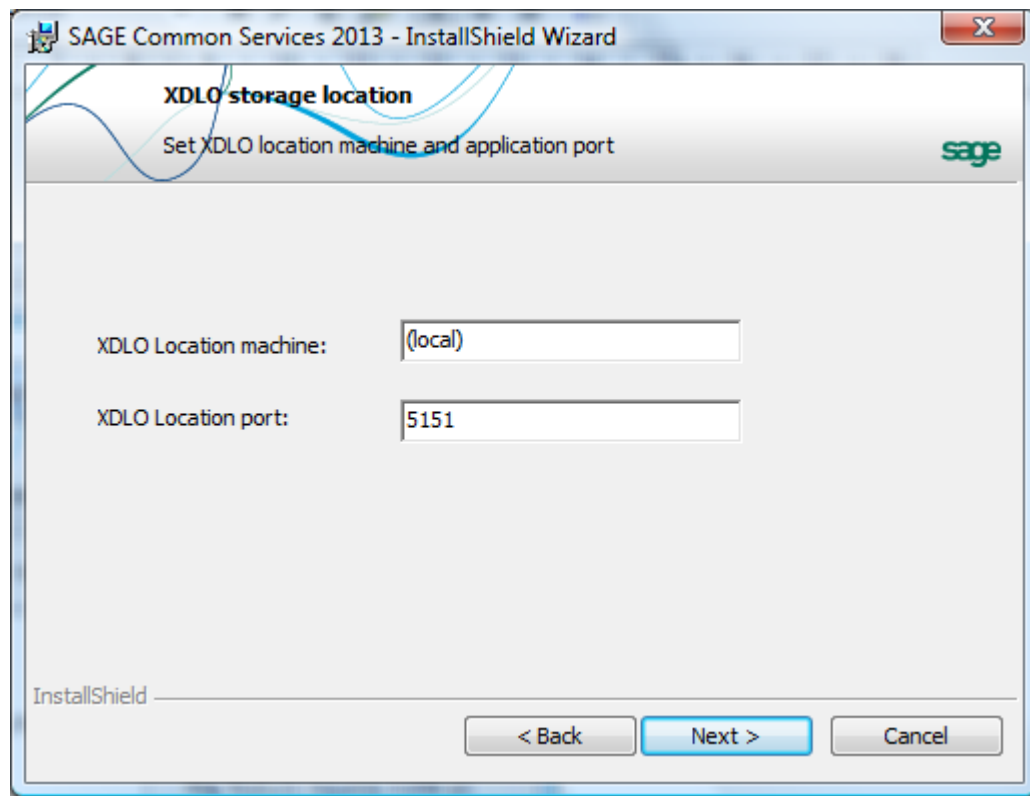


- Click the **Administration Tools** icon to scroll down the contextual menu of each component.
- Select **This feature and all of its sub features will be installed on local hard drive.**

10. The following screen appears:



11. Keep the default installation path and click **Next**. The **XDLO storage location** screen appears:



Important For more information on XDLO, see paragraph 4.1.

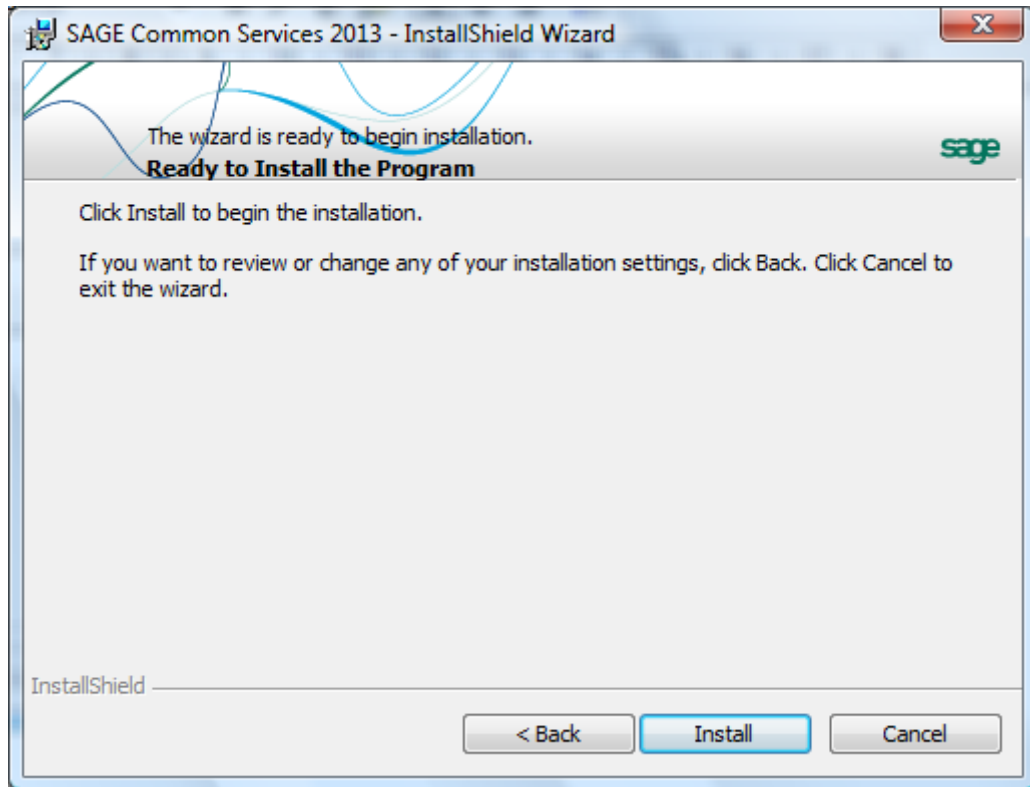
In the **XDLO Location machine** field, enter the computer name on which the XDLO service will be executed and in the **XDLO Location port** field the port number corresponding to the machine:

- For "**Standalone Machine**" installation, keep the "**(local)**" default value.
- For multistation installation, XDLO repository should reside in a dedicated administration station.

Important As with the database server, users must have access to this computer at any time.

Click Next.

12. The **Ready to Install the Program** screen appears:

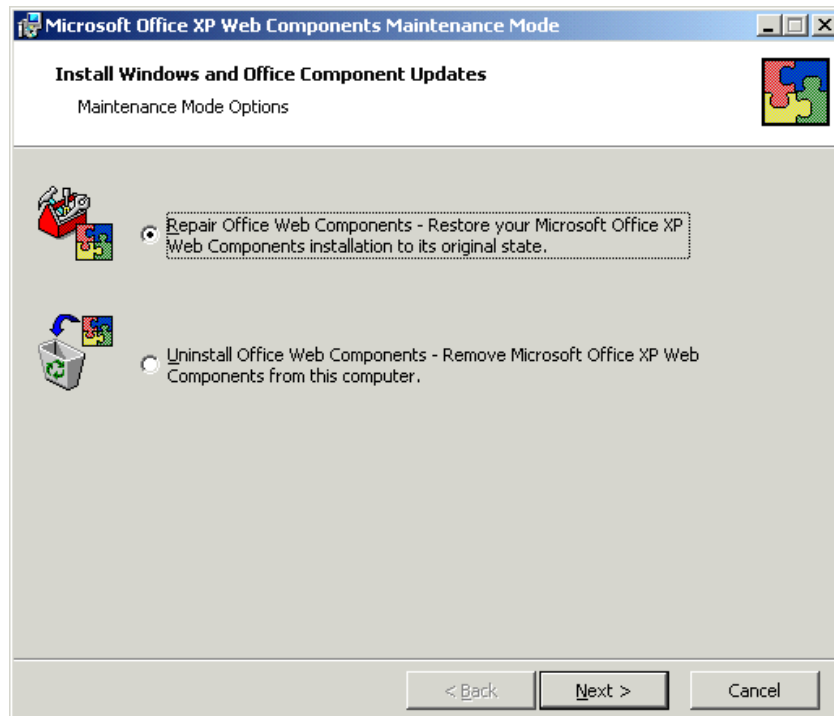


Click **Install**.

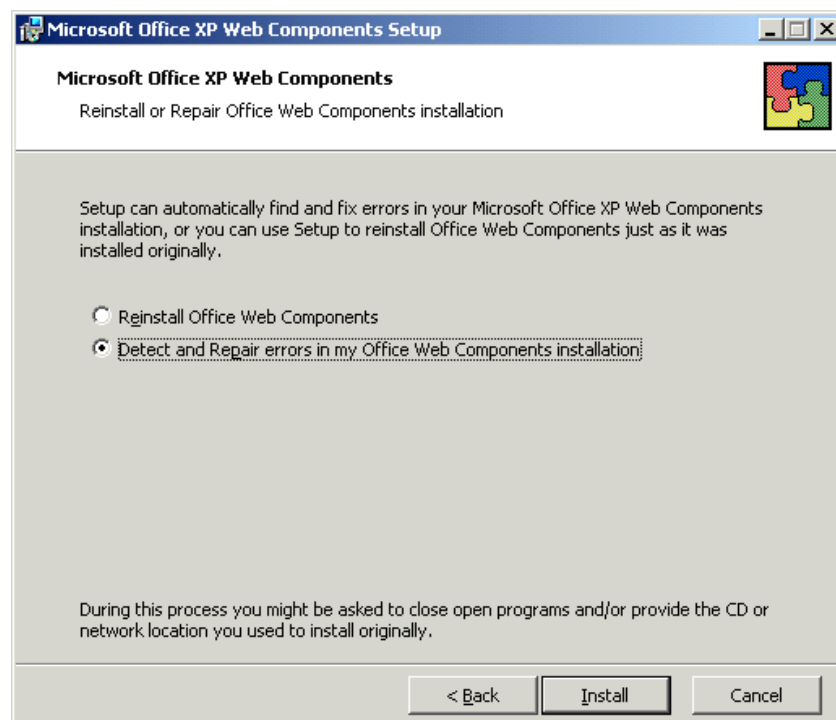
Important If installing Microsoft office XP Web (.net) Components for the first time, go to step 13. These components are necessary only in case of SBE Web server deployment.

Otherwise, go to step 14.

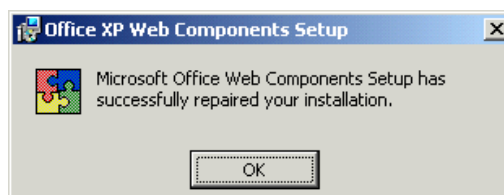
13. Since the **Microsoft XP Web Components** are already installed, the **Maintenance Mode** window opens. Select **Repair Office Web Components**.



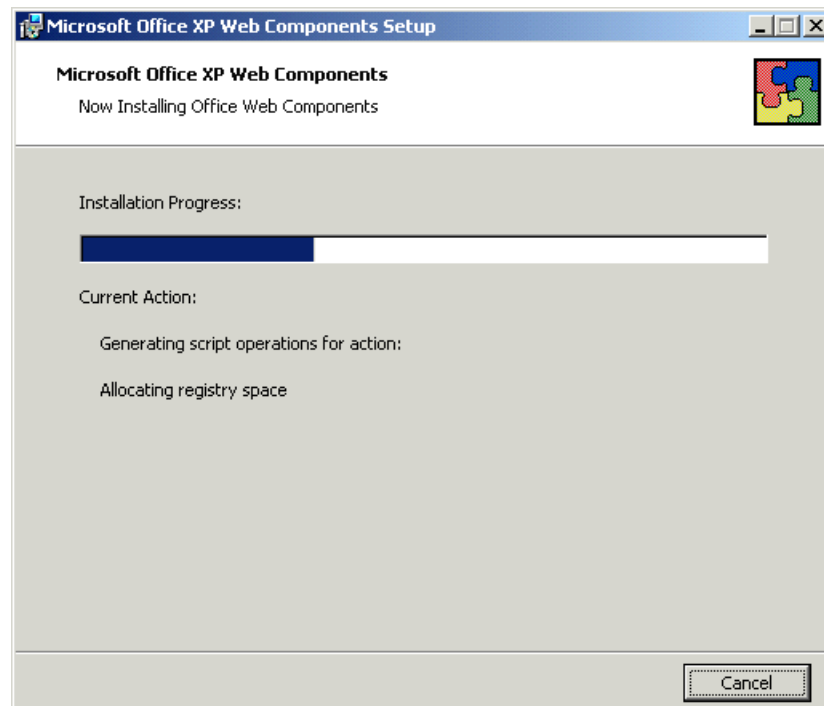
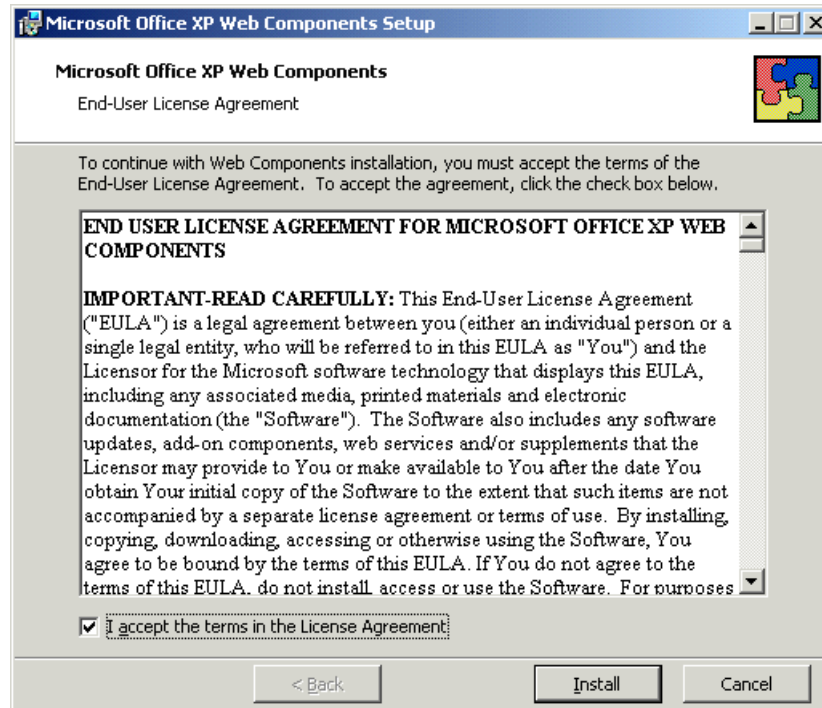
Click **Next**.

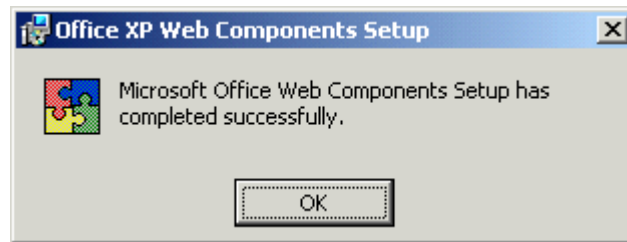


Select **Detect and Repair errors in my Office Web Components installation** and click **Install**.

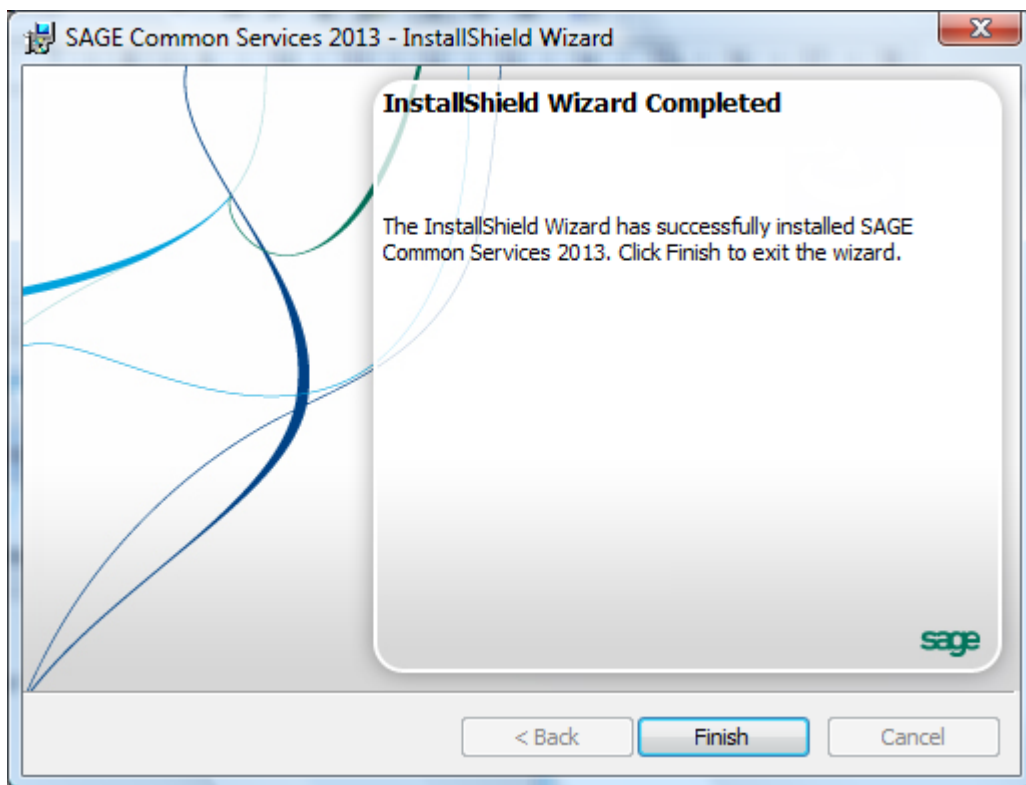


- 14 The Microsoft Office XP Web Components screen appears. Select **I accept the terms in the License Agreement**, then click **Install**





15 Click **Ok**.



16 Click **Finish** in the **InstallShield Wizard Completed** screen.

Important InstallShield may prompt you to restart the computer.

The **Sage\Sage Administration** shortcut now appears in the program list available from the **Start** menu.





4 Managing Workgroups

4.1 XDLO Presentation

4.1.a

4.1.b Introduction

XDLO (XRT Data Link Objects) is a new component which enables the structured management of database connection strings. It replaces the former system based on the xrt_ds.ini file:

- The connection strings are stored in a secured repository shared by user groups,
- The connection strings are defined by the system administrators,
- Each user belongs to a "Workgroup" — group of users that share the same databases —,
- Users can change workgroups, provided that the administrator has configured the relevant connection strings.

4.1.c References

[Wikipedia](#)

[OnLine MSDN](#)

4.1.d Definitions

User

Wikipedia definition:

*"**User** in a computing context refers to one who uses a computer system".*

Users have to identify themselves for security reasons, audit of the operations or use of resources.

A person who participates to an NT domain must have a Windows NT account to connect to the network and use the resources of the domain such as files, directories, printers.

DBA

DBA stands for *"DataBase Administrator"*.

DataBase Administrator

Wikipedia definition:

***A database administrator (DBA)** is a person who is responsible for the environmental aspects of a database" which include creation, test, coordination, integrity and security. "Although logical and physical database design are traditionally the duties of a **database analyst** or **database designer**, a DBA may be tasked to perform those duties".*

The database Administrator is mainly responsible for:

- Integrity - Verifying or helping to verify data consistency so that they do not break the system's business rules. For this purpose, he/she is in charge of the application of integrity constraints.

- Security - Defining and/or implementing access controls to the data by granting access for users or to authorize them to modify data according to their needs.
- Performance – Ensuring a quick access to data. He/she needs to provide optimized tables, indexes, statistics and SQL queries by using SQL optimization tools (tuning SQL).
- Development and testing support – providing support for development teams. For example, he/she can partially replicate data on a test database, optimize the database with developers and modify the schema to implement new functions.
- Data Recoverability – Creating and testing backup solutions so that if a data entry error, program bug or hardware failure occurs, the DBA can bring the database backward in time to its state at an instant of logical consistency before the damage was done.

DBO

DBO stands for "*DataBase Owner*". It is the owner of the database.

System Administrator

Wikipedia definition:

*"A **system administrator**, systems administrator, or sysadmin is a person employed to maintain and operate a computer system or network" of a company, association or organization.*

A Sysadmin is usually in charge of installation, maintenance, update, backup, restoring, planning, supervision, support and technological watch for servers within the technical scope of hardware and software mainly operating systems. He/she may also be in charge of the network administration or database administration for small size organizations.

He/she works within the Information Services department or a Software and Computing Services Company.

He/she works with the Information Services Manager, DBAs (Database Administrators), Network Administrators, Webmasters and related parties, Developers, Office Support Managers and finally Users.

Windows NT Account

A Windows NT account represents the identity of a user connected to the NT domain.

When a user gets connected, Windows NT creates a token. This includes a security identifier for the user, other identifiers for groups to which the user belongs and other information such as the username, and the names of the groups to which the user belongs. All processes executed under this user account get a copy of this token.

XDLO uses the token to:

- Retrieve automatically, in a multi-database context, the database with which the user needs to be connected.
- Retrieve automatically the connection string to use to open a connection to the database.

Database

Wikipedia definition:

*A computer **database** is a structured collection which enables to stock large amount of data in order to ease their use (add, update, search).*

*A **database** consists of a set of files on disk. Some of them can be accessed via the network, they are called on-line database.*



Database Access Account

The Database access account represents the identity of the user connected to the database. The Database access account granted to a user depends on the way the DB security is managed. In the application distribution, one of the most common scenarios actually consists in reading and entering data on a database. The difficulty which arises is to make this happen securely while maintaining the application scalability. Yet to attain it using a connection pool, we need to give up the idea that the database manages security. This is due to the fact that the connection pool requires that all data links are identical.

There are three options for the Database Administrator:

- To create an access account for each user. In this case, the connection pooling is not used.
- To use the integrated security to establish a trusted connection with SQL Server. It enables the creation of a data link which eliminates the need to store a password in the string, but the connection pool is not used because it creates a pool by "main identity".
- To create an access account for shared data, e.g. SAGEUsers, shared by all application users. This choice ensures the good performance of the connection pool but does not enable the audit of the modifications made by the database users.

For XDLO, a database access account is an entity which contains the authentication credentials (username and password) which must be used upon connection to the database. This entity may be associated to several NT windows accounts depending on the option selected by the DBA.

Administrator

For XDLO, an administrator is the person in charge of the database management. An administrator is responsible for:

- The creation of databases
- The update of databases
- The management of the data access controls

Generally speaking, the database administrator belongs to the Windows NT local group "Administrators". The companies which deny access of Windows NT Administrators local group to people in charge of Sage products' installation and configuration, can create a *XRTDBAdministrators* local group on the administration console of Sage applications. When a local or distant client calls XDLO service, the latter determines whether the NT account of the person calling belongs to the NT *Administrators* or *XRTDBAdministrators* local groups. In other words, any person belonging to the *Administrators* local group or the *XRTDBAdministrators* of the administration console can administrate XDLO from any station declared on the domain.

Workgroup

Workgroups are sets of users sharing common databases. Workgroups are created on a single administration computer accessible to every other user of the group.

Each Workgroup features at least one link to the XRT Common Services database used by security administrators to grant or deny access to Sage products.

Additionally, each Workgroup features a link to every "product" database used by the members of a same group.

Organizing databases in workgroups provides the following benefits:

- This structure enables the system administrator to manage access to bases from a single administration computer.
- As the connection strings to databases are stored on a lockable administration computer, the users are not able to change them.

- The workgroup concept enables authorized users to switch from a working context to another without losing his/her connection string parameters. For example, users can operate on a TEST base before operating on a PRODUCTION base.
- The unique 'workgroup'/'user' combination enables the deployment of the Sage FRP Treasury application on a METAFRAME server common to users working on different production bases. This is the case for groups whose bases cannot be accessed by all subsidiaries.

Data Link

A data link contains the ADO properties (provider, datasource, initial catalog) shared by a usergroup connected to the same database.

Each data link is identified by a mnemonic ("CS", "U2", etc...) used by the product to retrieve the ADO connection string.

The authentication credentials are stored in a database access account which depends on the operation type granted to the user.

Several database access accounts can be associated to a data link:

- A **DBA** access account is automatically created by the administration console when a data link is added. The administration console uses it for database operations which require administrator profile.
- A **DBO** access account is automatically created by the administration console when a data link is added. The administration console uses it for database operations which require the database owner profile.

4.1.e Architecture

General Overview

XDLO is a service-oriented application (SOA) which manages connection strings for Sage applications.

XDLO consists of 2 main components:

- The XDLO objects are included in the COM XDLO_COM.dll component and presented to clients by xdlo_service.exe NT service which executes on the administration console and responds to the requests of connection strings made by clients. This NT service listens to calls on TCP/IP 5151 port (this default value can be modified when installing XCS).
- A client (rem_client.dll) used by Sage applications to send requests to XDLO service. This component uses TCP/IP and DCOM sockets for data exchange.

The administration console name is set up when installing client stations.

Storage

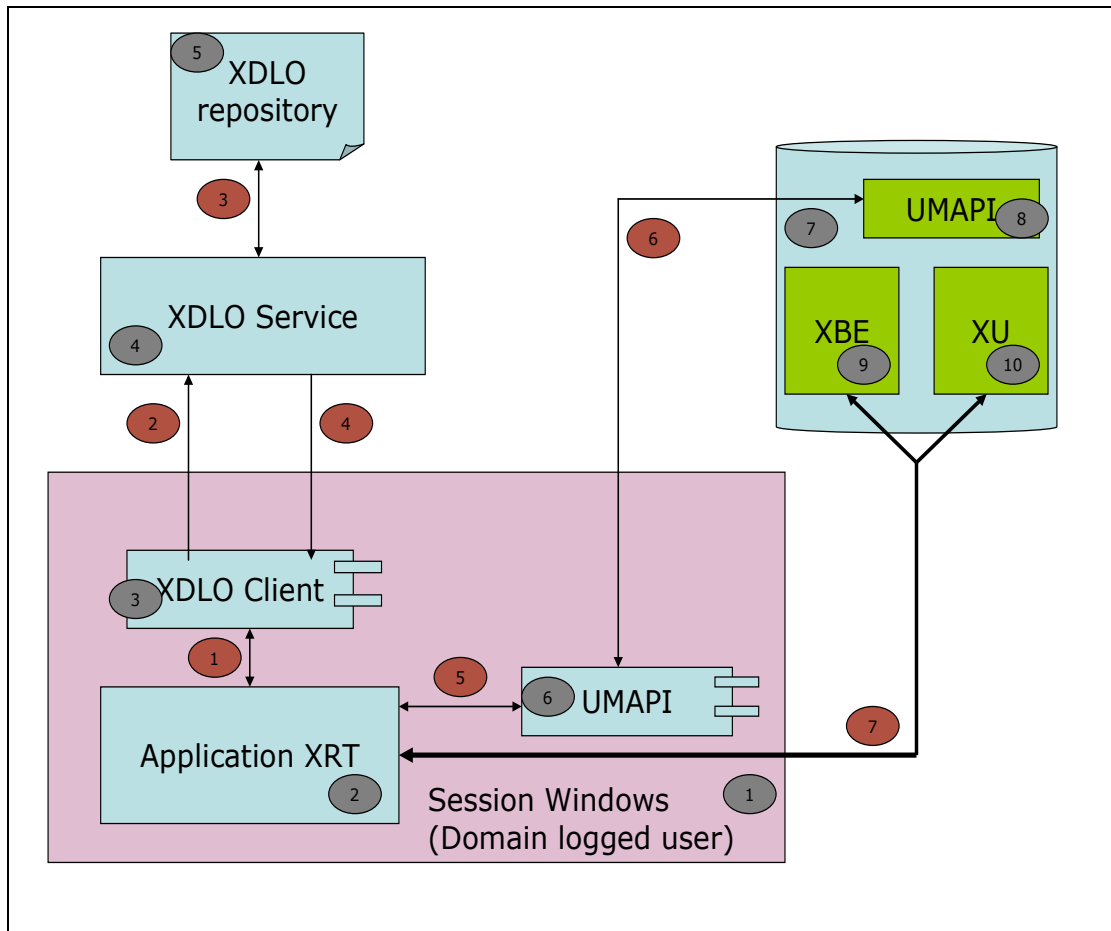
XDLO objects are kept in an xml file stored in the **<All Users> \Application Data \Sage** folder in the administration console. Its location can be changed if required. This file can be installed in a shared directory in case of a cluster deployment.

The XML file is protected by the encryption algorithm 3DES and cannot be directly modified by the users.

On NTFS file system, the "security" panel enables the administrator to set up advanced permissions to restrict access to XDLO storage file.

Exchange Schema

The graph below is a quick representation of exchanges between XDLO components in Sage applications. It represents the different components of the processes (1) and their interactions (1).



Components:

- 1 Windows session of a NT domain user. This session is opened and the connection to Sage application is made through the NT account of the connected user.
- 2 The NT user launches a Sage application (Frp Treasury, SBE, ...).
- 3 The application uses XDLO client component installed by XCS setup to get the connection string to the database.
- 4 The XDLO client component connects to XDLO service which is launched on the administration computer. The communication between the client and the service is ensured by DCOM.
- 5 XDLO file contains the definition of the workgroups and the corresponding connection strings. XDLO service searches XDLO file for information.

6

If the application gets a connection string, it starts UMAPI component in order to check that the user is authorized to use the software and to obtain access permissions to the product.

7

The application connects to the SQL server or Oracle database with a string connection obtained via XDLO.

8

The database contains the UMAPI rights of Sage applications.

9

The database can contain SBE tables and data.

10

The database can contain Sage FRP Treasury tables and data.

Interactions:

1

Sage FRP Common Services application launches XDLO client with the NT credentials of the connected user.

2

XDLO client connects to the service on TCP/IP port and initiates a communication via DCOM.

3

XDLO service searches XDLO repository to find the workgroups set up for the connected NT user.

4

XDLO service returns the information to XDLO client. This information enables the application to create the workgroup list for the connection window.

5

The application instantiates UMAPI component to obtain the user rights on the application.

6

UMAPI component searches UMAPI tables in the database to get user rights. This information is returned to the application which can finish the initialization of its execution environment.

7

The application can connect to its repository and the user can start working.

4.1.f Setup

Administration Computer

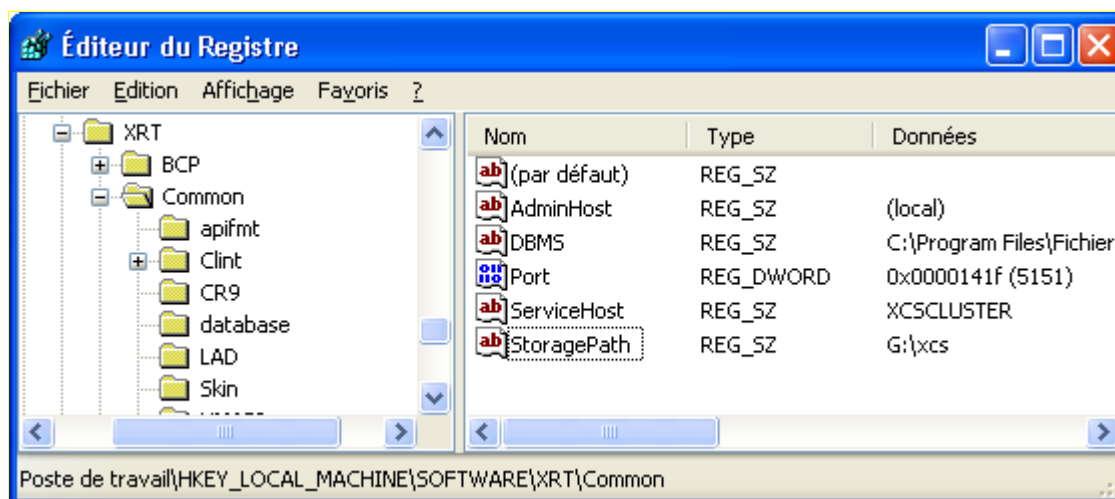
The administration computer is the machine on which XDLO is launched.

The main setup of XDLO on the administration console is defined in the register key: HKEY_LOCAL_MACHINE\SOFTWARE\XRT\Common. It contains the following values:

Value	Description
Port	TCP/IP port on which the service listens to client calls. Upon XCS installation, this setting receives the default value 5151.
StoragePath	Defines the access path to xdlo_storage.xml file. This setting enables the change of the access path for xdlo_storage.xml file when XDLO is installed in cluster mode. Each node of the

ServiceHost

cluster must have a write access on the shared file.
Enables the specification of the name or IP address of the administration station or the virtual name or IP address linked to the administration console. This value is useful when XDLO is installed in cluster mode, since it enables the specification of the virtual name of the cluster. This name can be linked to any of the cluster nodes according to the enabled node.



The optional settings of XDLO are defined in the register key:
HKEY_LOCAL_MACHINE\SOFTWARE\XRT\Common\XDLO. It contains the following values:

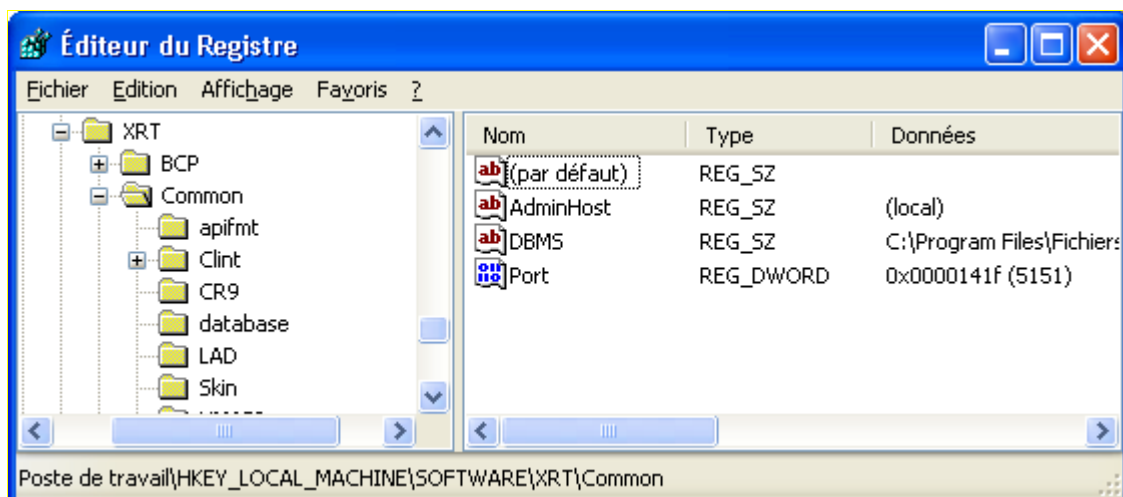
Value	Description
Debug	Enables the debug mode of <code>xdlo_service.exe</code> and <code>XDLO_COM.dll</code> which generate the <code>xdlo_service.log</code> et <code>xdlo.log</code> log files when the value "Y" is given to it. These files are generated in the <i>LocalService\Application Data\XRT\XCS</i> folder.

Client Station

The client station refers to the computer on which Sage applications and XDLO client are executed.

The main settings of the client part of XDLO are defined in the register key:
HKEY_LOCAL_MACHINE\SOFTWARE\XRT\Common. It contains the following settings:

Value	Description
AdminHost	Name or IP address of the station on which XDLO service is executed. The default value of this setting is "(local)".
Port	Number of the IP port on which XDLO service listens to client calls. The default value of this setting is 5151.



The optional settings of the XDLO client part are defined in the register key: HKEY_LOCAL_MACHINE\SOFTWARE\XRT\Common\XDLO. It contains the following values:

Value	Description
DebugRC	Enables the debug mode of the client component which generates the <i>xdlo_remclient.log</i> log file when the "Y" value is given to it. The log file is generated in the <User>\Application Data\XRT\XCS folder.
Cache_lease	Defines the time in seconds during which XDLO uses the cache to retrieve a connection string. When the "cache lease" time is up, XDLO calls the service.

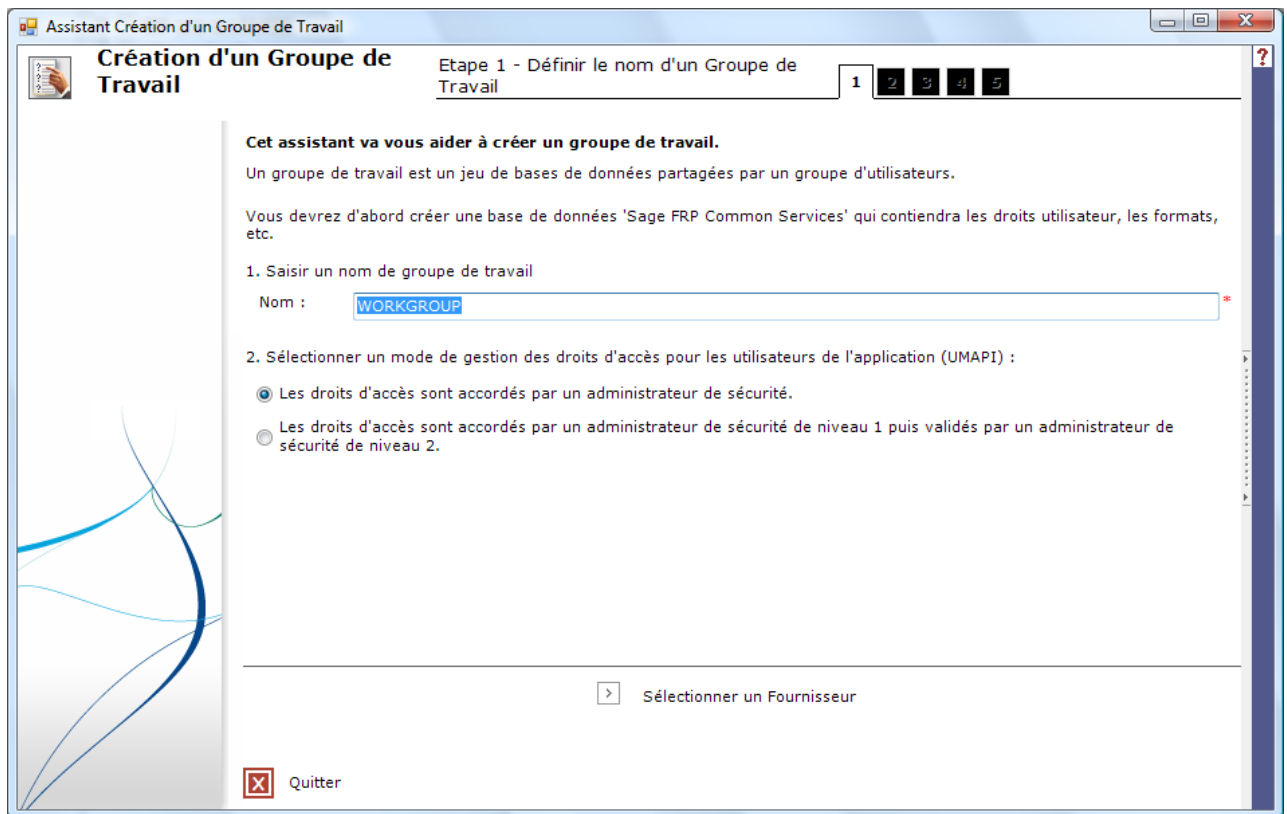
4.2 Creating Workgroup (SQL Server)

Upon first installation of XCS 3.4, there is no workgroup.

Important If there is an existing workgroup, see paragraph 5.

In the Start menu, select Programs – Sage – Sage Administration – Administration Sage .NET to launch the Workgroup Creation Wizard.

4.2.a Defining a Workgroup Name

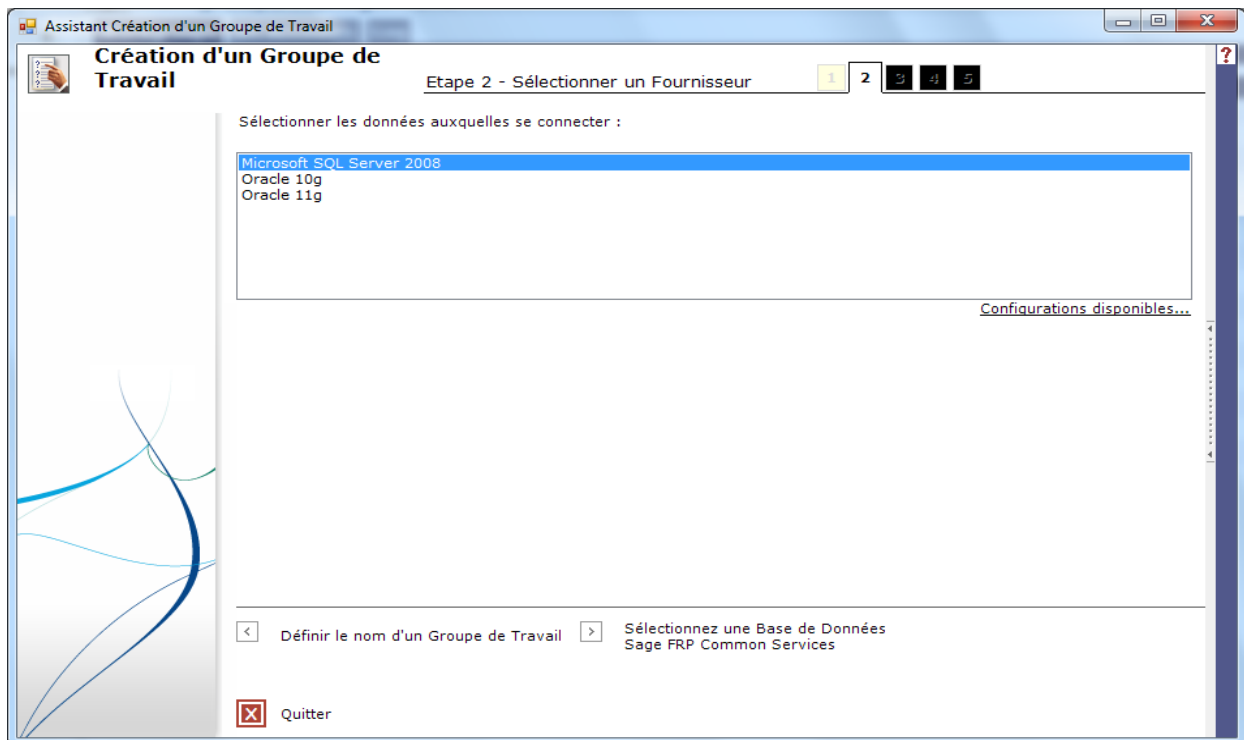


Enter a workgroup name or keep **WORKGROUP** by default.

Define the access permissions management mode for the application users:

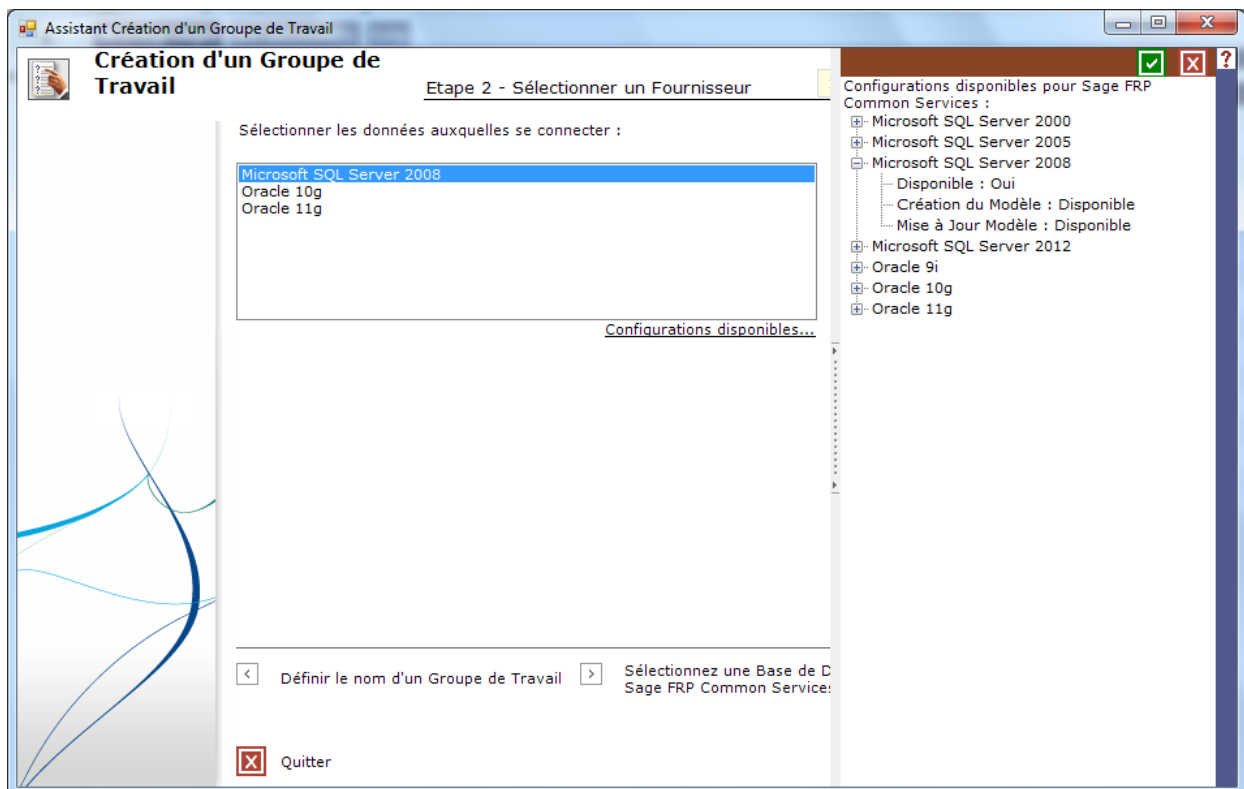
- Define the permission granting mode:
 - Select "**Access permissions are granted by a security administrator**" if you want a simple access permissions management in which only one Security Administrator intervenes.
 - Select "**Access permissions are granted by a level 1 security administrator and validated by a level 2 security administrator**", if you want an access permissions management in which every action taken by Security Administrator must be validated by a second one.

4.2.b Selecting a Provider



Select in the list the installed **database server or client** (here Microsoft SQL Server 2008).

Click on Available configurations... to display the details of the database server and client which are installed on the computer, as well as the authorized operations (creation and update).



Click **Select a Database** and the following screen appears:

4.2.c Selecting a Database

Assistant Création d'un Groupe de Travail

Création d'un Groupe de Travail

Etape 3 - Sélectionnez une Base de Données Sage FRP Common Services

Sélectionner les informations nécessaires à la connexion aux données SQL Server :

1. Sélectionner ou saisir un nom de serveur :

srvr-sql2008 * [Rafraîchir](#)

2. Saisir les crédits de l'administrateur du serveur :

☐ Utiliser la sécurité intégrée de Windows NT

☒ Utiliser un nom d'utilisateur et un mot de passe spécifiques :

Nom Utilisateur : sysadm *

Mot de Passe : ***** * ☐ Pas de Mot de Passe

3. Sélectionner ou créer une base de données sur le serveur :

☐ Sélectionner la base de données :

☒ Créer la base de données :

Nom : kp_3404b *

DBO : XRTDBO * Mot de Passe : ***** *

Utilisateur : XRTUSERS * Mot de Passe : ***** *

Collation string : SQL_Latin1_General_CP1_CI_AS

< Sélectionner un Fournisseur > Produits

[Tester la connexion DBA](#)

[Tester la connexion DBO](#)

[Tester la connexion USERS](#)

☒ Quitter

Enter the **server name** on which the database must be created (here are the available characters to name the server: "(local)", "(LOCAL)", ".", server name). The **Refresh** button enables the display of the Microsoft SQL Servers list connected to the company network.

According to the authentication type used by the **DBA** to connect to the database server, you can select:

- Use Windows NT integrated security: the DBA is authenticated by its NT account.
- **Use a specific username and password:** the DBA is authenticated by a username and a password.

Click **Test DBA connection** to check DBA credentials.

Select the following option:

- **Select the database** if you want to work on an existing database:
 - Select the database (the database list is refreshed upon first display).
 - Enter the password corresponding to the DBO name which appears in the **DBO** field. The default password proposed by the wizard is **password#2005** (when the user selects a database from the list, the wizard searches automatically for the name of its owner; the wizard uses the DBA account to perform this operation).
 - Enter the password of **XRTUSERS** account. Default password is **password#2005**.

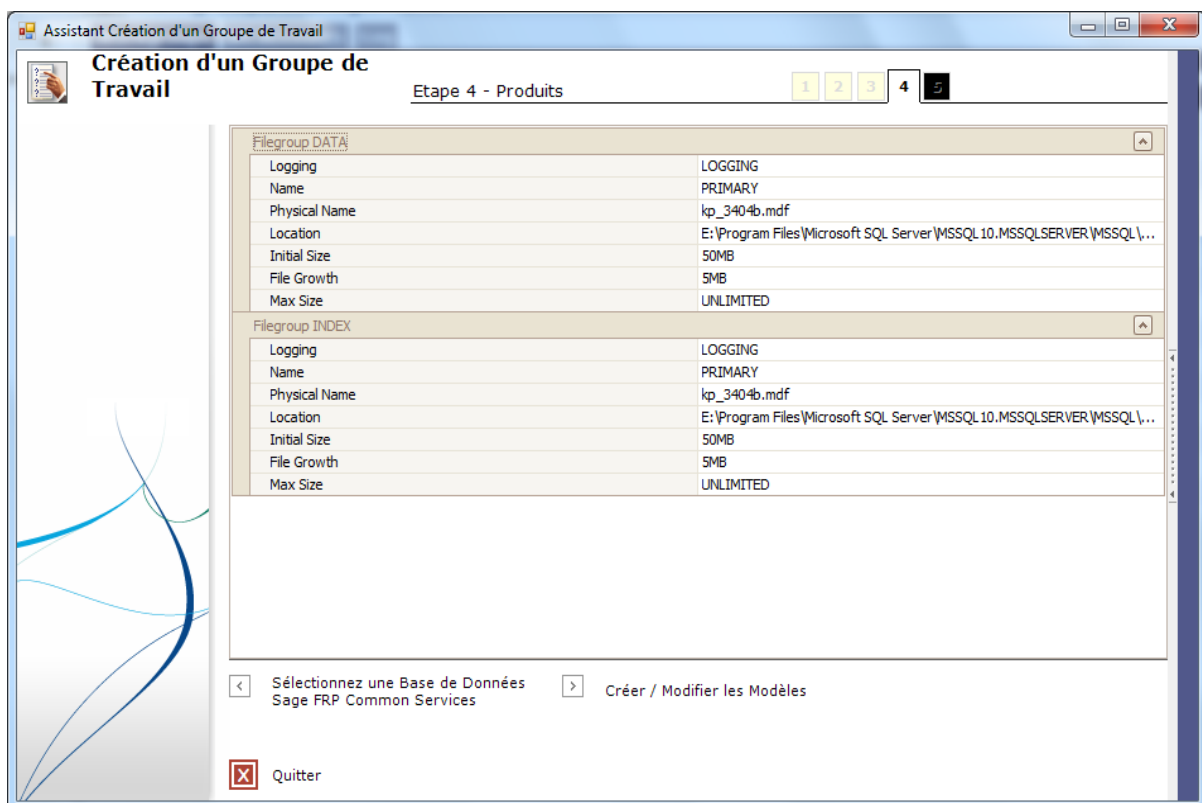
Click **Test DBO connection** to check the DBO credentials.

- **Create the database** if you want to create a database:
 - Enter the **database Name** (the wizard checks that the name has not been already used when the user clicks on "Create/Modify models").
 - In the **DBO** field corresponding to the **XRTDBO** account, leave the default password which is **password#2005**.
 - In the **Users** field corresponding to the **XRTUSERS** account, leave the default password which is **password#2005**.
 - Select the "**Collation string**" or keep the default French_CI_AS (no distinction between uppercase and lowercase).

Important A model represents all the tables used by a product. You can create several models for a database. In this case select "**Select a database**", select the database in the "**Name**" list and use the same "**DBO**", "**Password**" and "**Collation string**" as those created previously.

Click **Products** to display the following screen:

4.2.d Configuration of Logical Units



The wizard proposes a default scenario in which the tables ("**Filegroup DATA**") and indexes ("**Filegroup INDEX**") of XCS model are created in the **PRIMARY** filegroup (default filegroup upon creation of the SQL server database). From this Properties panel, you can:

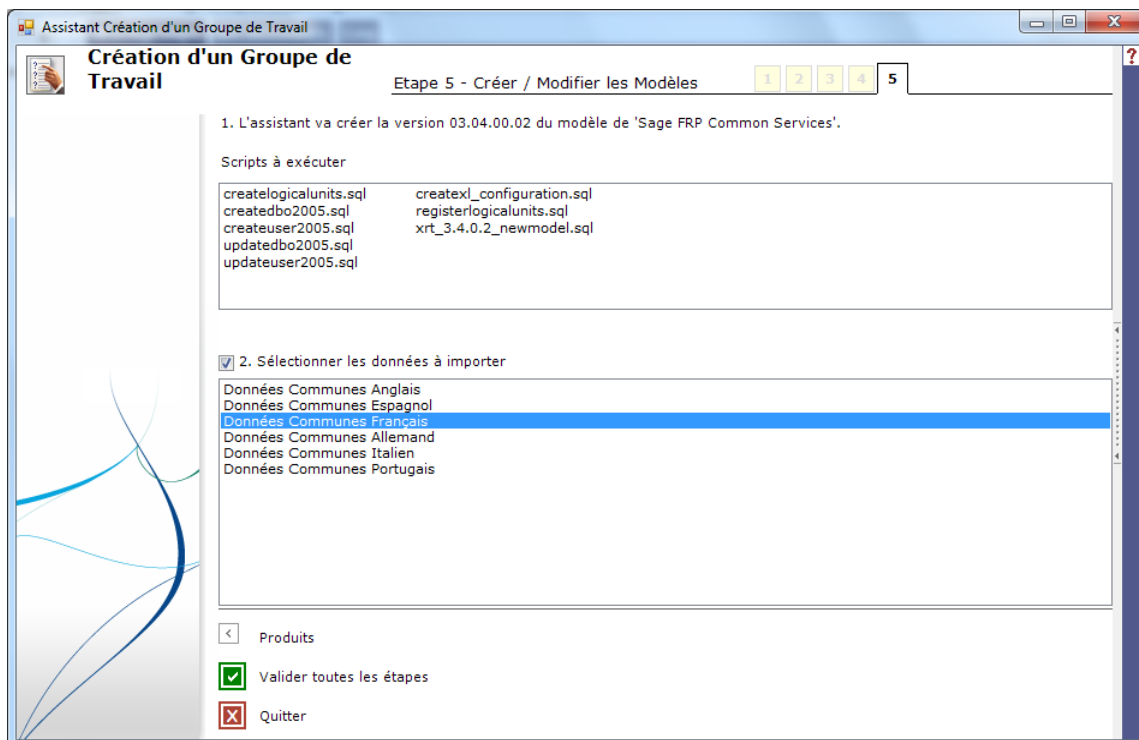
- Either modify the proposed scenario and install indexes in 2 distinct Filegroups (example: XCS_DATA et XCS_INDEX).
- Or modify the filegroup creation settings (storage directory, initial size, maximum size, file growth). Warning: the storage directory must already exist if you want the creation process to work properly.

Important The XCS model scripts are based on a "logical" filegroup **DATA** for the tables and a "logical" filegroup **INDEX** for the indexes. When executing the model creation process, the wizard replaces the logical names by the values entered in the Properties panel (**PRIMARY** for the default scenario).
If the target filegroups do not exist (example XCS_DATA and XCS_INDEX), they are automatically created by the wizard.

Click **Create/Update models** and the following screen appears:

4.2.e Creating/Updating Models

Upon first installation, the wizard displays the following screen:



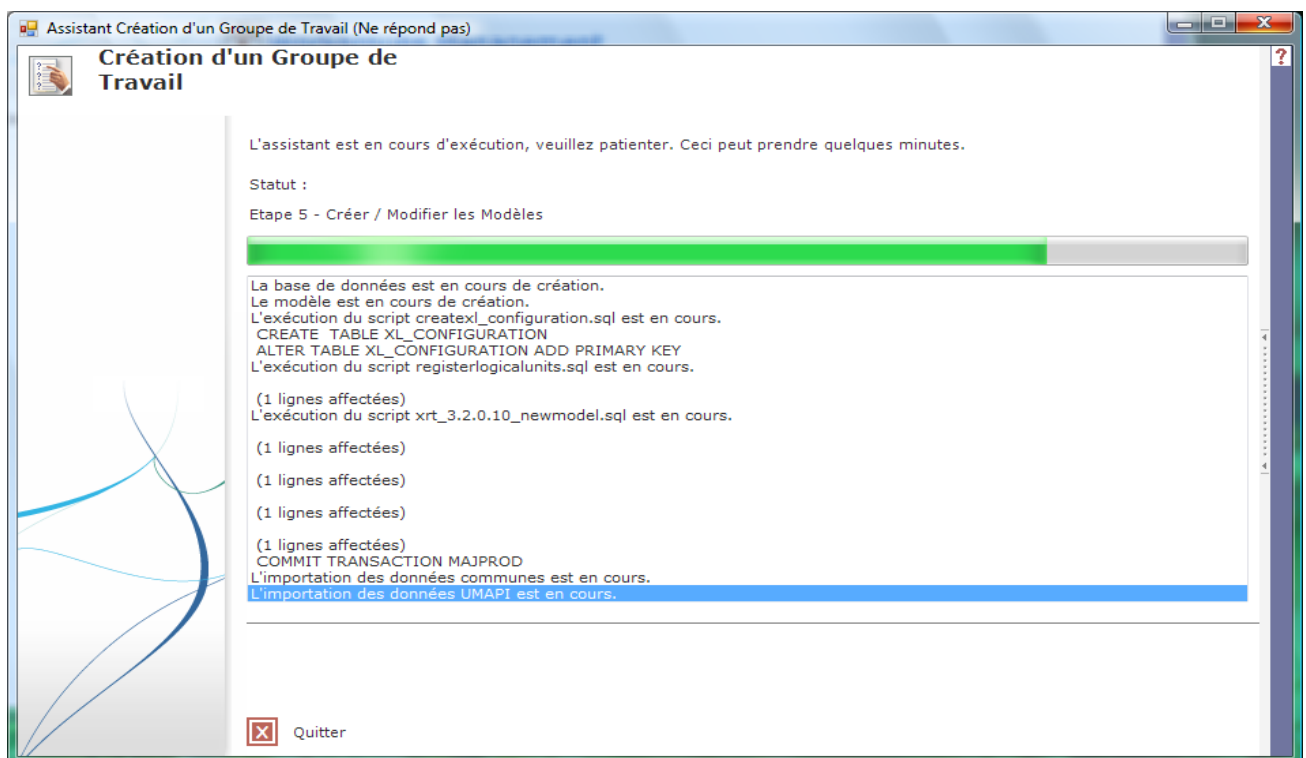
The **Scripts to be executed** list includes all the scripts to be executed to create "Sage FRP Common Services" model. It consists of the creation script of **createlogicalunits.sql** logical units (a logical unit represents a filegroup for the creation of a Microsoft SQL server database), the creation script of **xl_configuration createxl_configuration.sql** table in which the model version will be saved, and the register script of **registerlogicalunits.sql** logical units.

The "product" scripts will follow. Each script is executed on behalf of the DBA or DBO according to its type.

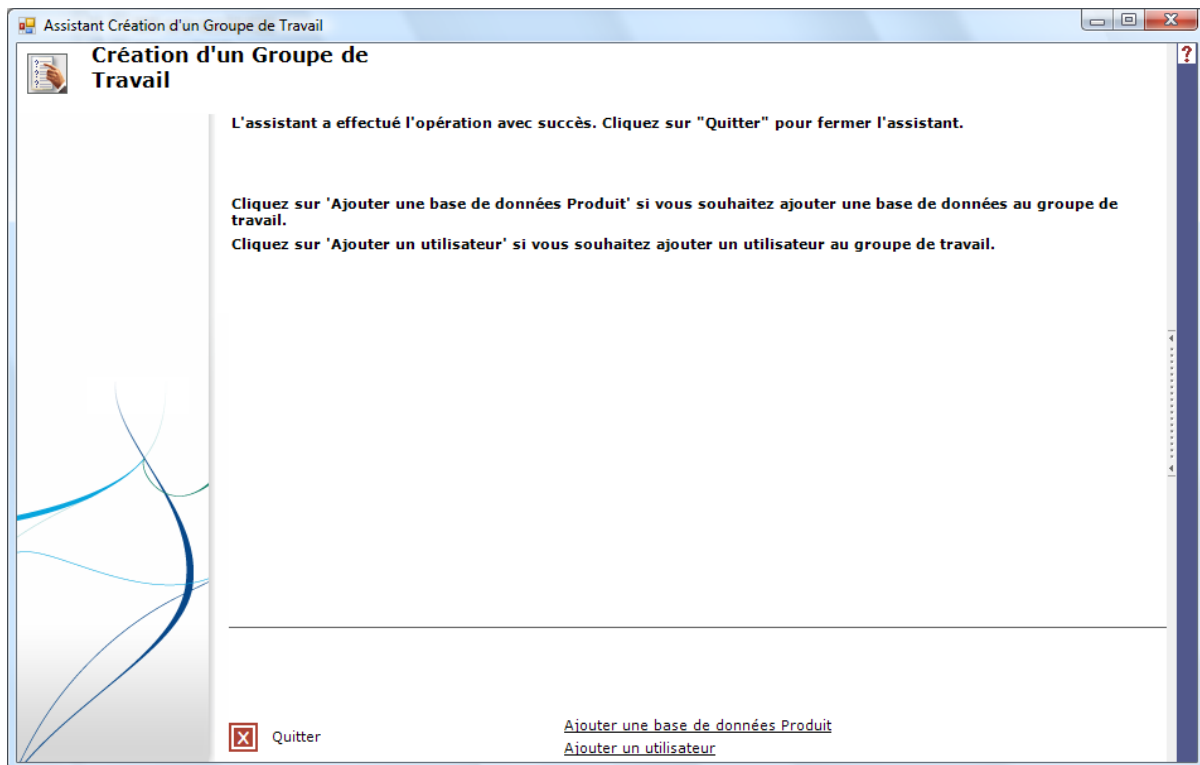
For XCS, selecting **Select data to be imported** in the relevant language is mandatory. They represent data (xml) for APIFMT, TRANSCO and UMAPI.

Click **Validate all steps** and proceed to the execution of the actions set up in steps 1, 2, 3, 4 and 5.

4.2.f Execution of Actions

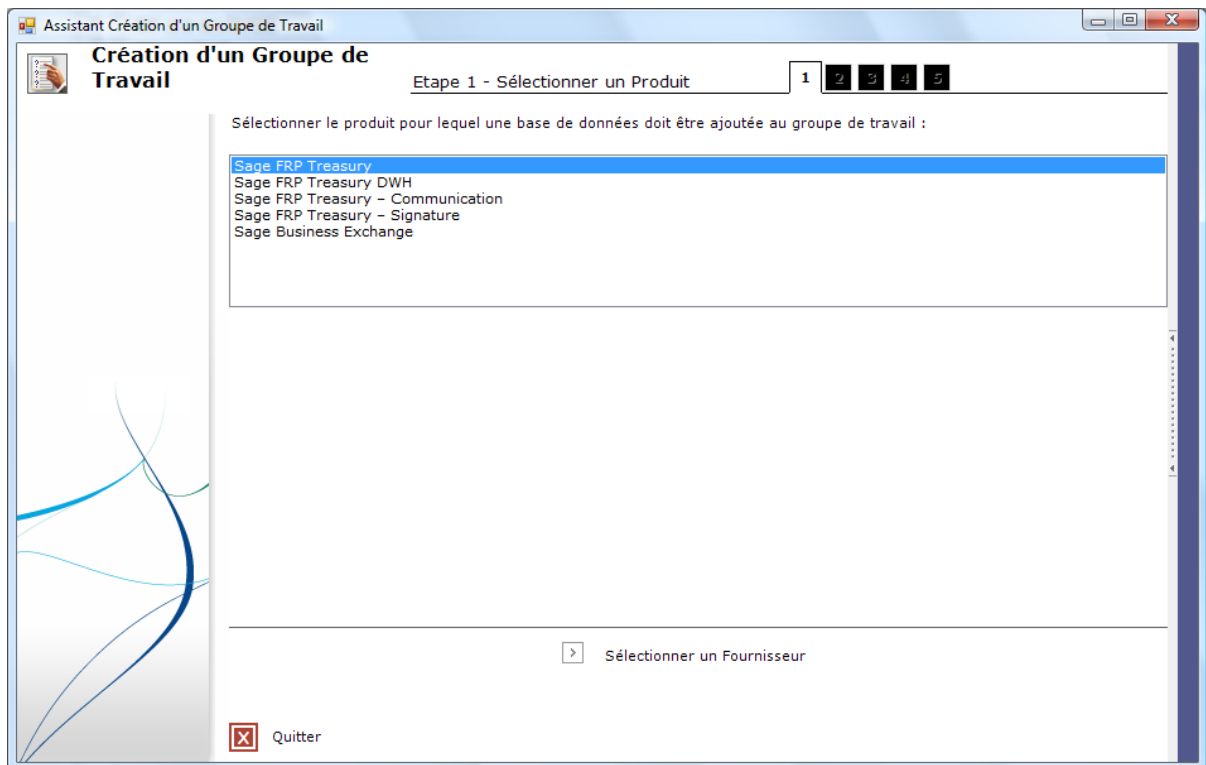


This may take several minutes. When all actions are executed, the following screen appears:



At this stage, XCS model is created; you can **Quit** the Workgroup Creation Wizard and go to the Administration Console or continue to add another Product model. Click **Add a Product Database** and the following screen appears:

4.2.g Selecting a Product



Select a product in the list and click Select a Provider.

Refer to **Select a Provider** section of paragraph 4.2.



4.3 Creating Workgroup (Oracle 11g Server)

Important Creating a Sage database on Oracle server is restricted to users who are familiar with this DBMS. Prior to using Sage Administration, the DBA needs to:

- Create and configure a new database on the server,
- Set up the listener module on the server,
- Set up a local network service to enable access to the database (tnsnames.ora).

4.3.a Special Recommendations for Oracle

SQL scripts are tested on Windows operating systems. They include the creation of Oracle tablespaces and the associated physical files. If the server hosting Oracle runs under another operating system, the client database administrator should create these tablespaces and physical files.

Here are the **tablespaces** to be created:

For XCS

- XRT_DATA (20 MB by default, "static" data)
- XRT_INDEX (20 MB by default)

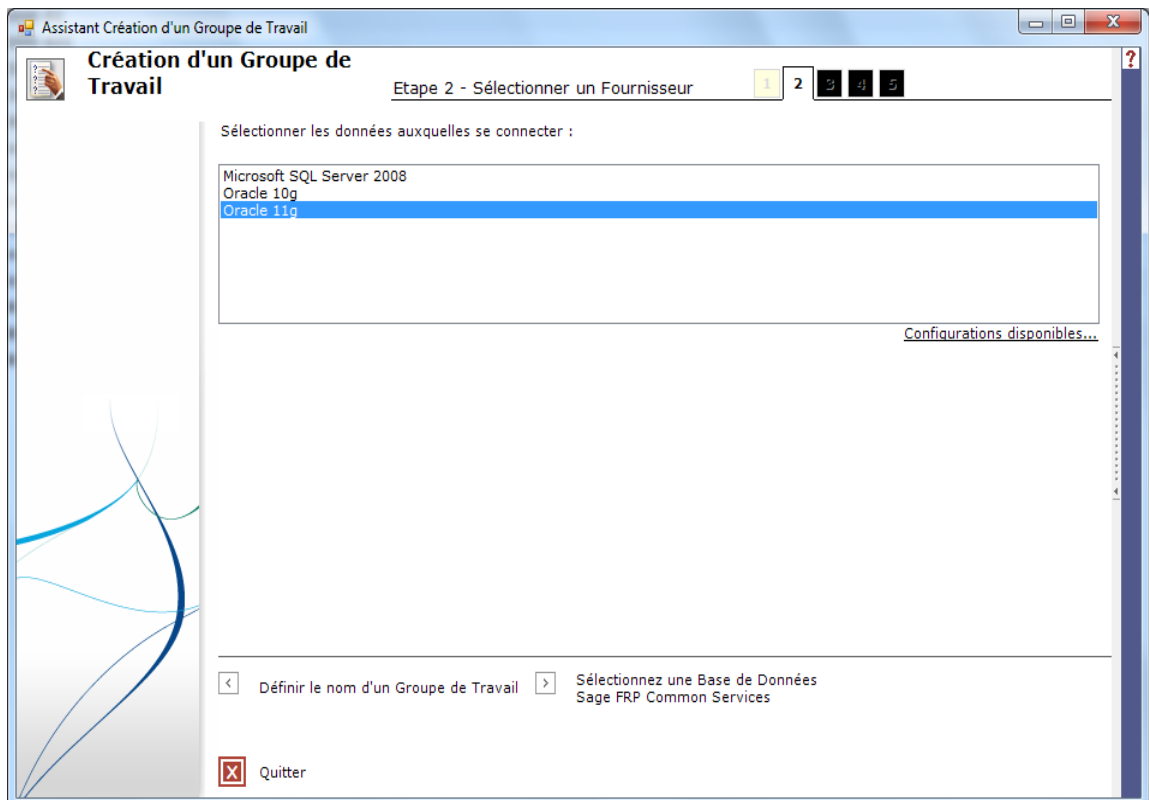
Tablespaces names must be respected, the name of the physical files can be freely chosen as long as Oracle and the operating system accept it.

4.3.b Defining a Workgroup Name

Refer to **Defining a Workgroup Name** section of paragraph 4.2.

Click **Select a provider** and the following screen appears:

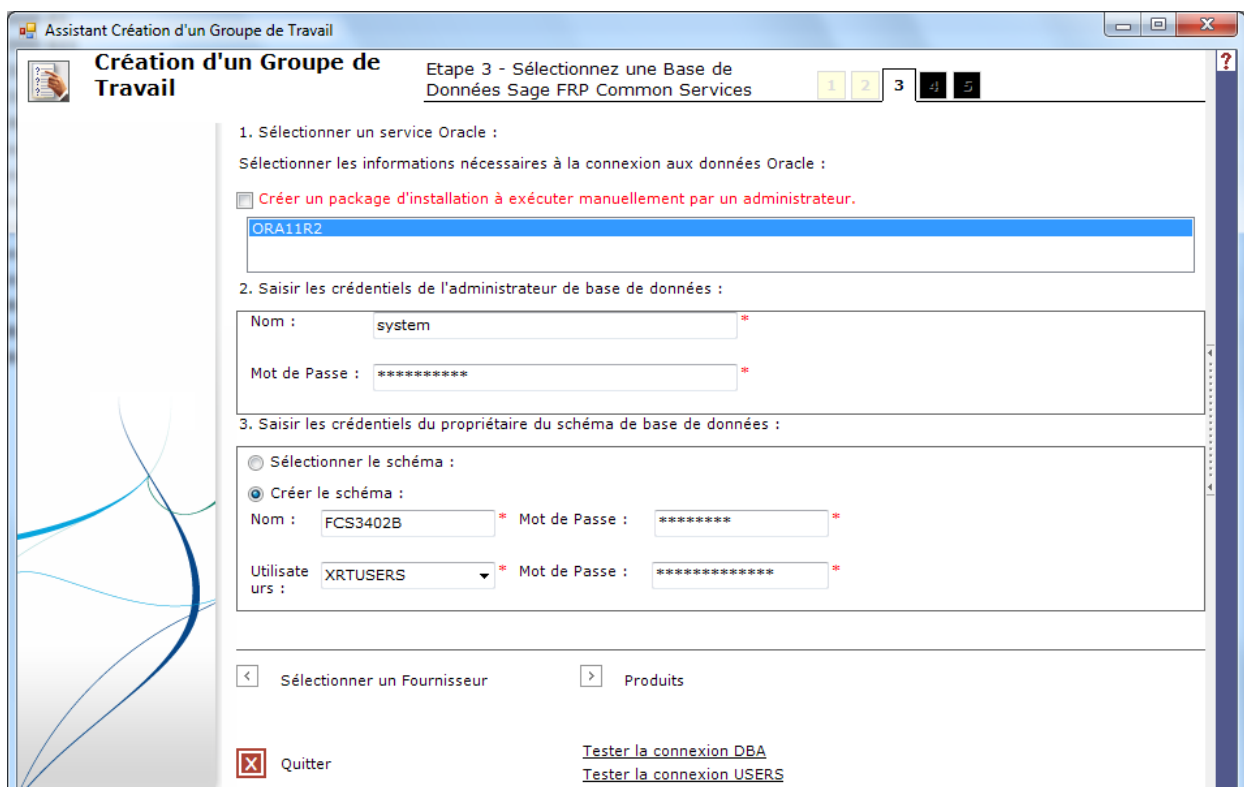
4.3.c Selecting a Provider



Select in the list the **database server or client** (here Oracle 11g).

Click **Select a Database** and the following screen appears:

4.3.d Selecting a Database



Actions on Oracle database can be:

- Automatically executed by the database installer,
- Manually executed by the database administrator. To do so, you need to select **"Create an installation package that will be manually executed by an administrator"**. The database installer collects sql scripts, import files, jscrip and command files to make an installation package in the directory **<APPDATA>\XRT\DBMS**, which is executed in command line.

For more details on the creation of this installation package, see chapter 12.

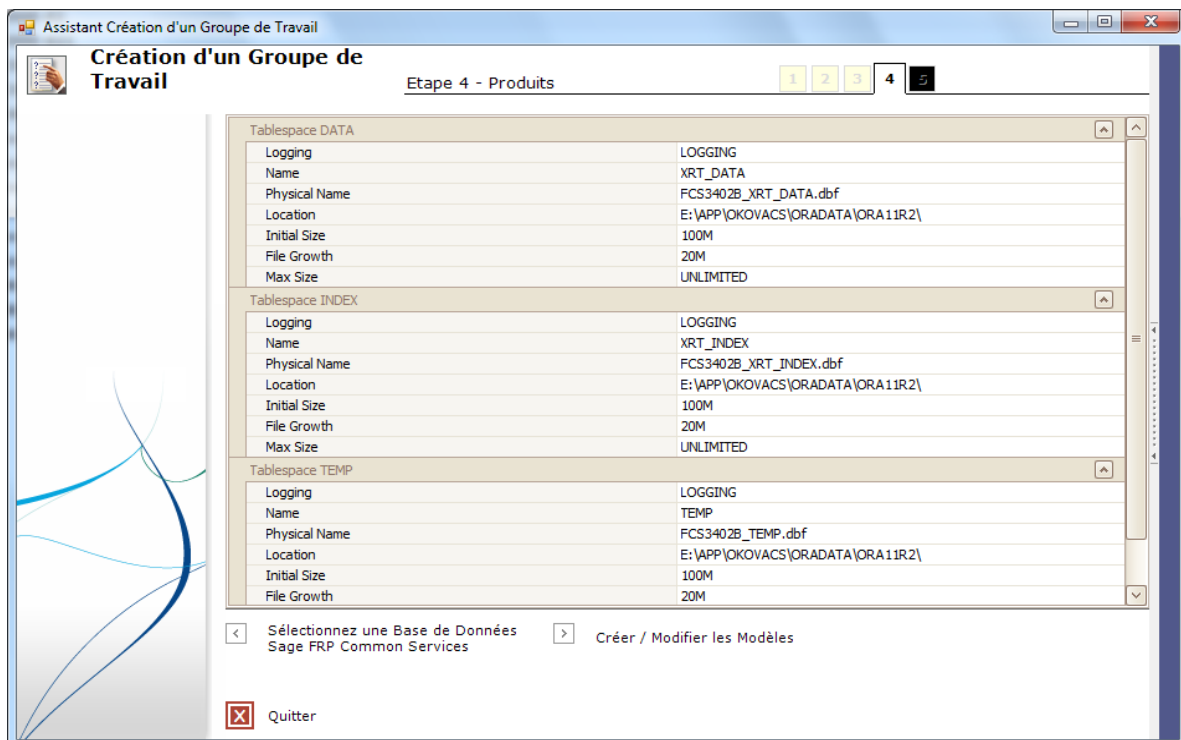
Whatever the operating mode, you need to:

- Select an **Oracle service** (here XU).
- Enter the credentials (name and password) of the database administrator (**DBA**).

Click **Test DBA connection** to check DBA credentials.

- Select the following option:
 - **Select the schema** if you want to work on an existing schema. Select the target schema and enter its password.
- Click **Test DBO connection** to check the DBO credentials.
- **Create the schema** if you want to create a schema. Enter the name and password of the schema to be created.

To create a schema, click on **"Product..."** to display details on the creation of "Sage Common Services" model.



The wizard proposes a default scenario in which the tables of XCS model are created in the XRT_DATA tablespace (**"Tablespace DATA"**), indexes in the XRT_INDEX tablespace (**"Tablespace INDEX"**) and the temporary tables in the TEMP tablespace (**"Tablespace TEMP"**). You can modify the scenario from this properties panel:

- Tablespaces name
- Initial size
- Maximum size
- File growth

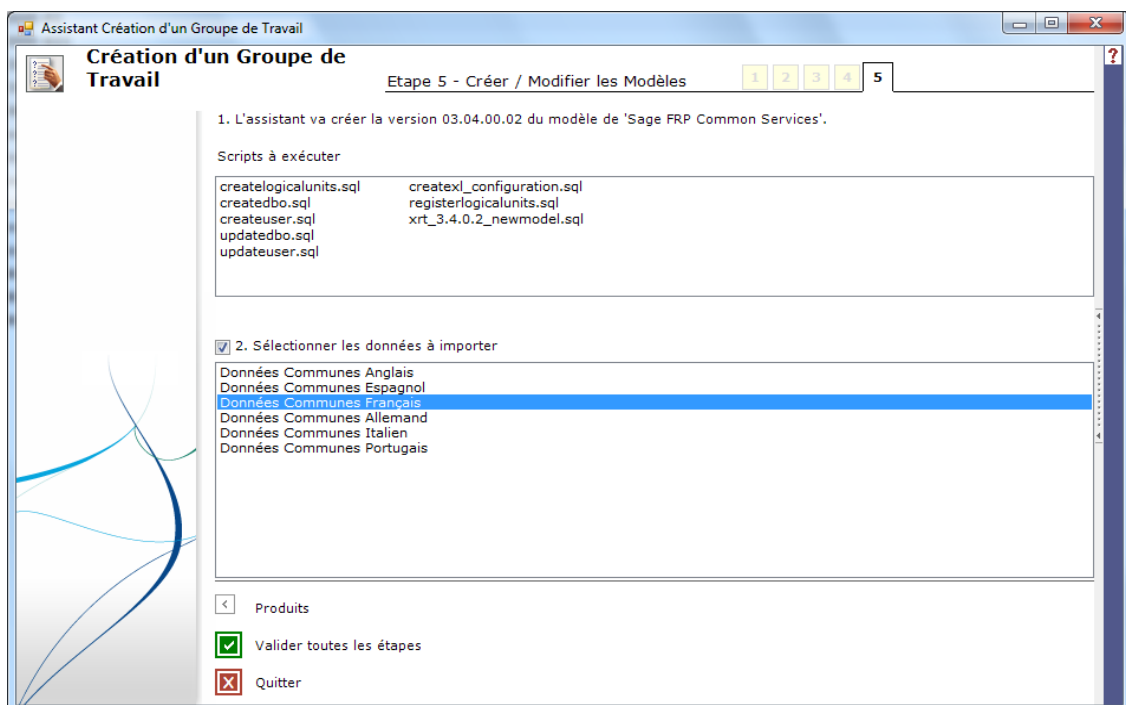
Important The XCS model scripts are based on a "logical" tablespace **DATA** for the tables, a "logical" tablespace **INDEX** for the indexes and a "logical" tablespace **TEMP** for the temporary tables. When executing the model creation process, the wizard replaces the logical names by the values entered in the Properties panel.
If the target tablespaces do not exist (example XCS_DATA), they are automatically created by the wizard.

Note: The TEMP tablespace is not created. Oracle database must have a temporary tablespace, this is the one to use.

Note Creating one schema by product in Oracle is highly recommended, as the tablespaces setup is rather delicate.

Click **Create/Update models** and the following screen appears:

4.3.e Creating/Updating Models



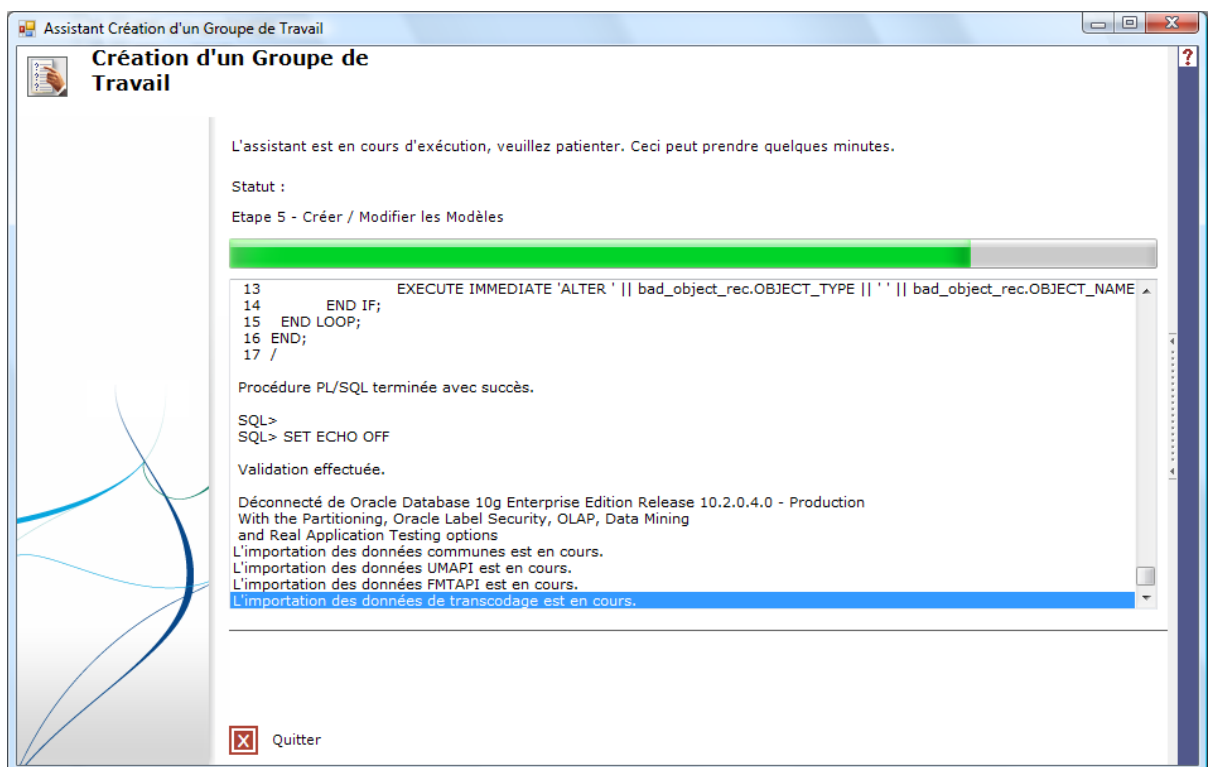
The **Scripts to be executed** list includes all the scripts to be executed to create "Sage Common Services" model. It consists of the creation script of **createlogicalunits.sql** logical units (a logical unit represents a **tablespace** for the creation of an Oracle schema), the creation script of **xl_configuration createxl_configuration.sql** table in which the model version will be saved, and

the register script of **registerlogicalunits.sql** logical units. The "product" scripts will follow. Each script is executed on behalf of the DBA or DBO according to its type.

For XCS, selecting **Select data to be imported** in the relevant language is mandatory. They represent data (xml) for APIFMT, TRANSCO and IAM (UMAPI).

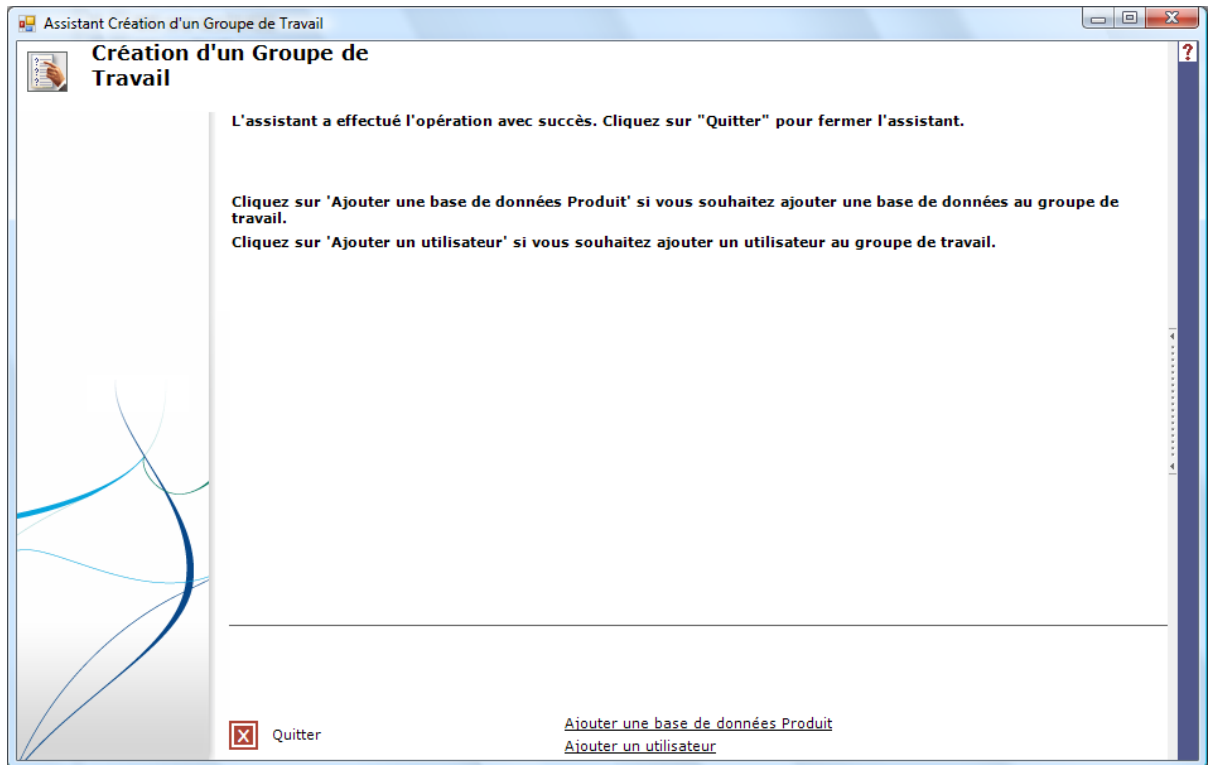
Click **Validate all steps** and the script execution starts.

4.3.f Script Execution



This may take several minutes.

The screen showing the end of the scripts execution appears:

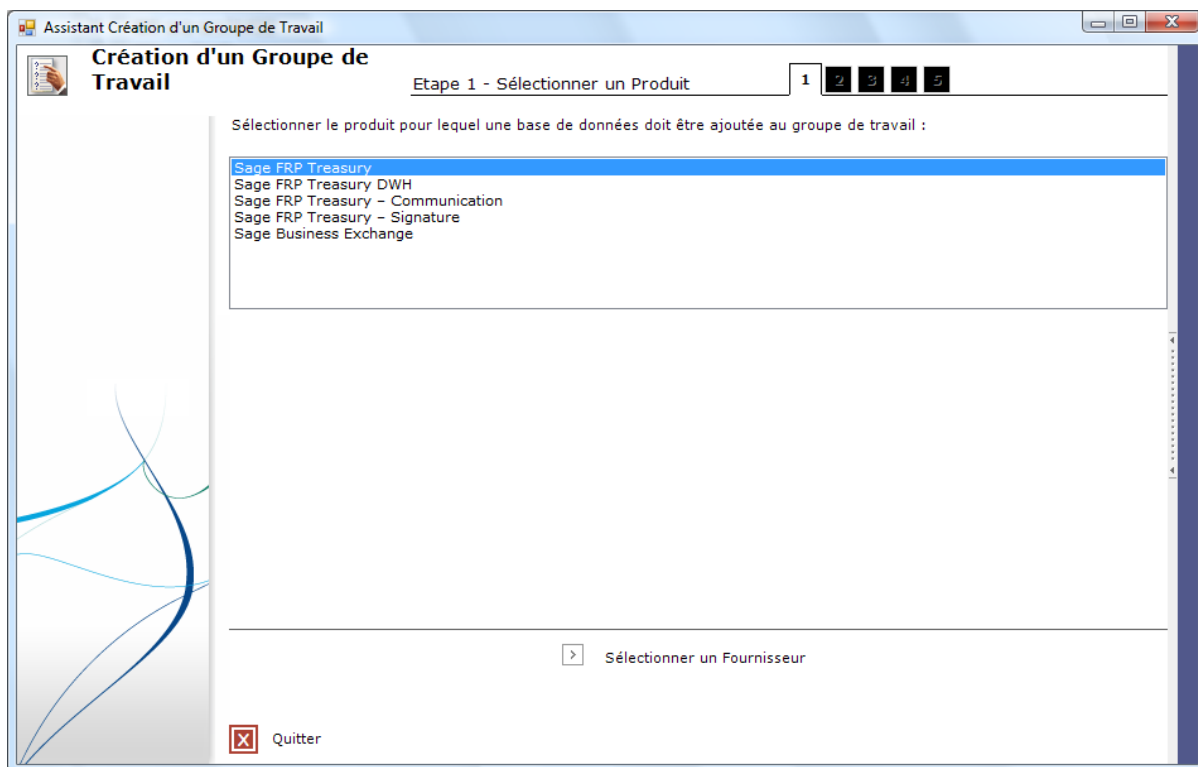


At this stage, XCS model is created; you can:

- **Quit** the Workgroup Creation Wizard and go to the Administration Console,
- Add a Product Database,
- **Add user** to the workgroup.

Click Add a Product Database. The following screen is displayed:

4.3.g Selecting a Product



Select a product in the list and click Select a Provider.

Refer to **Select a Provider** section of paragraph 4.3.

4.4 Updating a Database

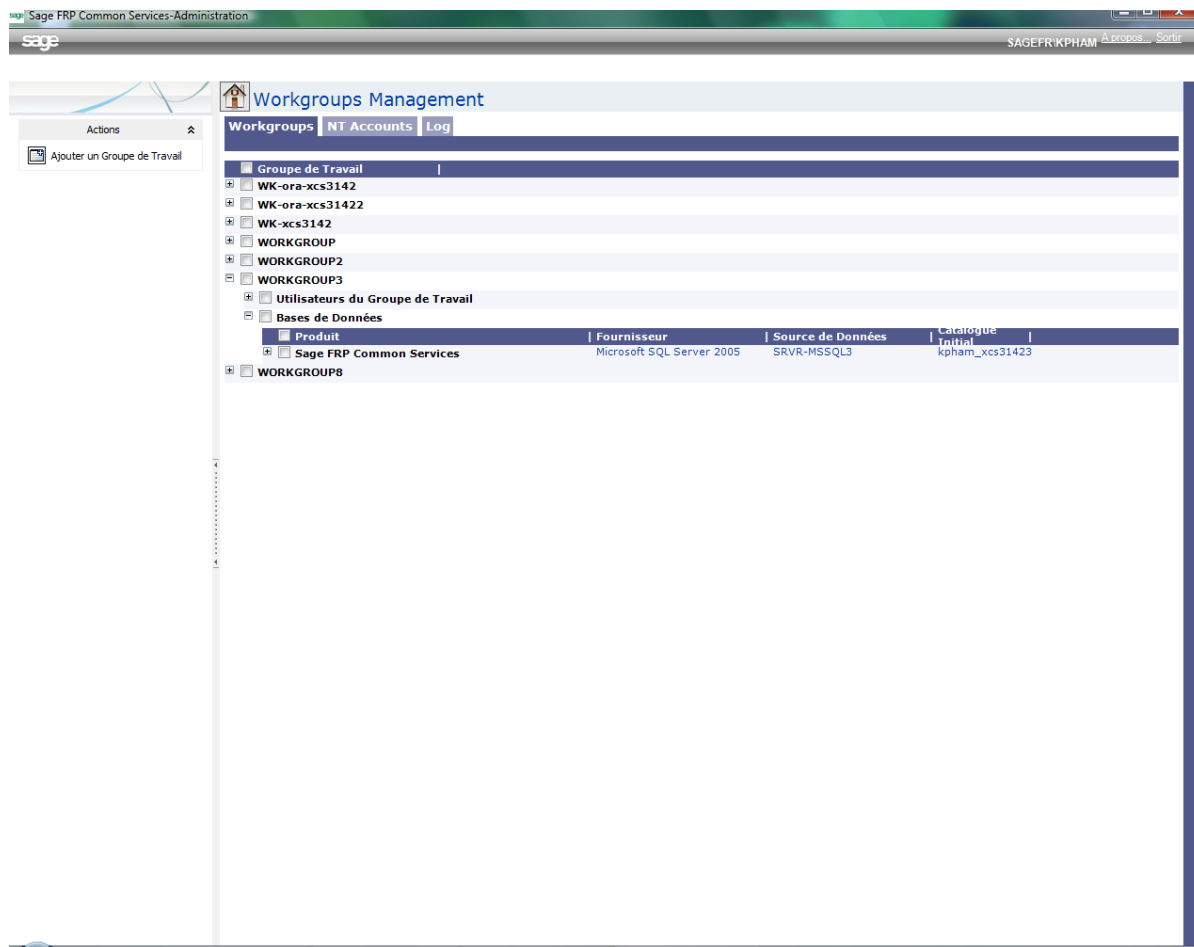
4.4.a Updating Data

The updating system of data stored in a database was developed in addition to the updating system of models based on SQL scripts:

- It is supported by C# classes compiled during execution, which enables the user to intervene on it like he/she does on SQL scripts.
- Source files are organized in the same way as SQL scripts: same storage directory and same naming convention.
- All C# classes implement the same methods, which enables the database installer to discover the classes upon execution and not upon generation.

4.5 Adding Workgroups

Here is the workspace of the Administration Console when opened in **Manage Workgroups**:

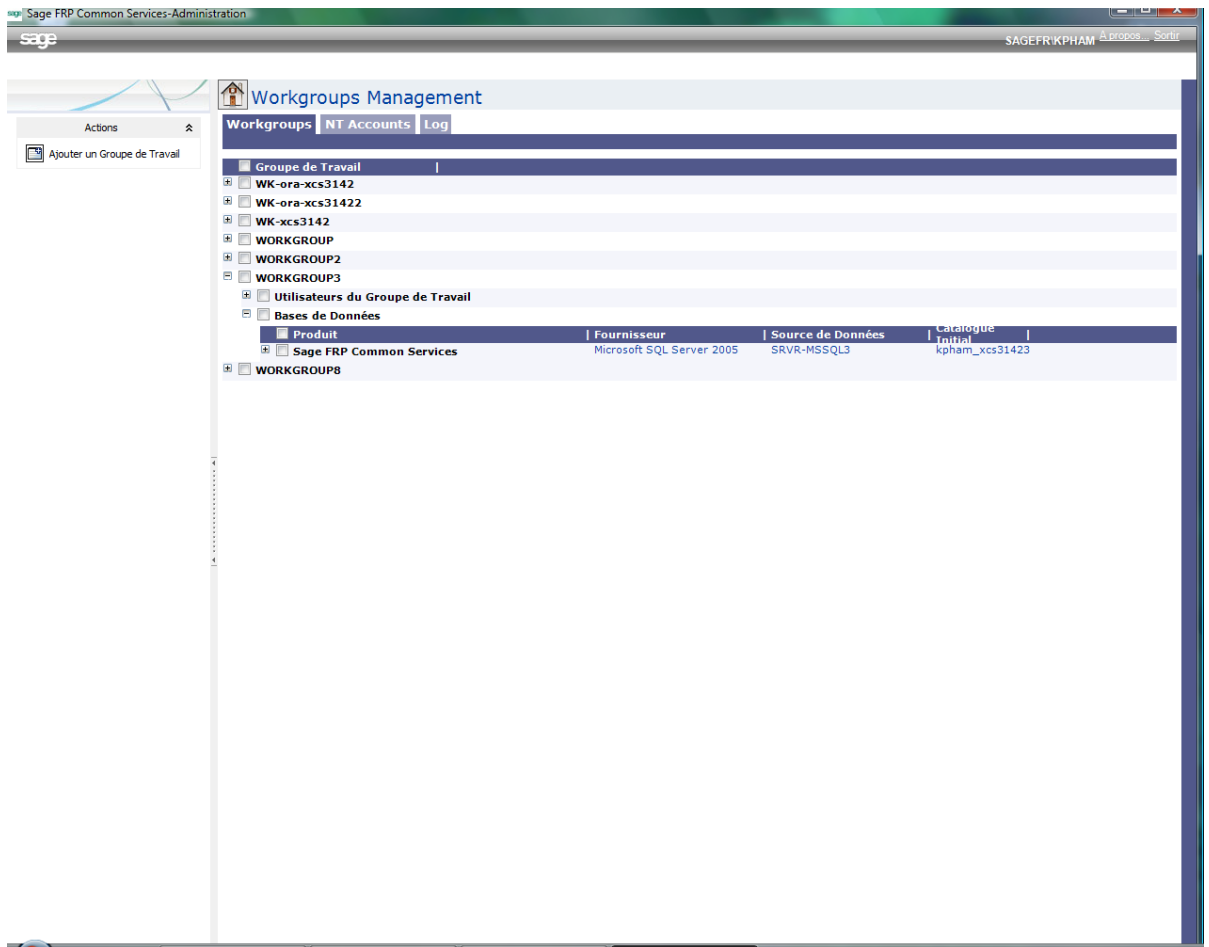


Click Add a Workgroup.

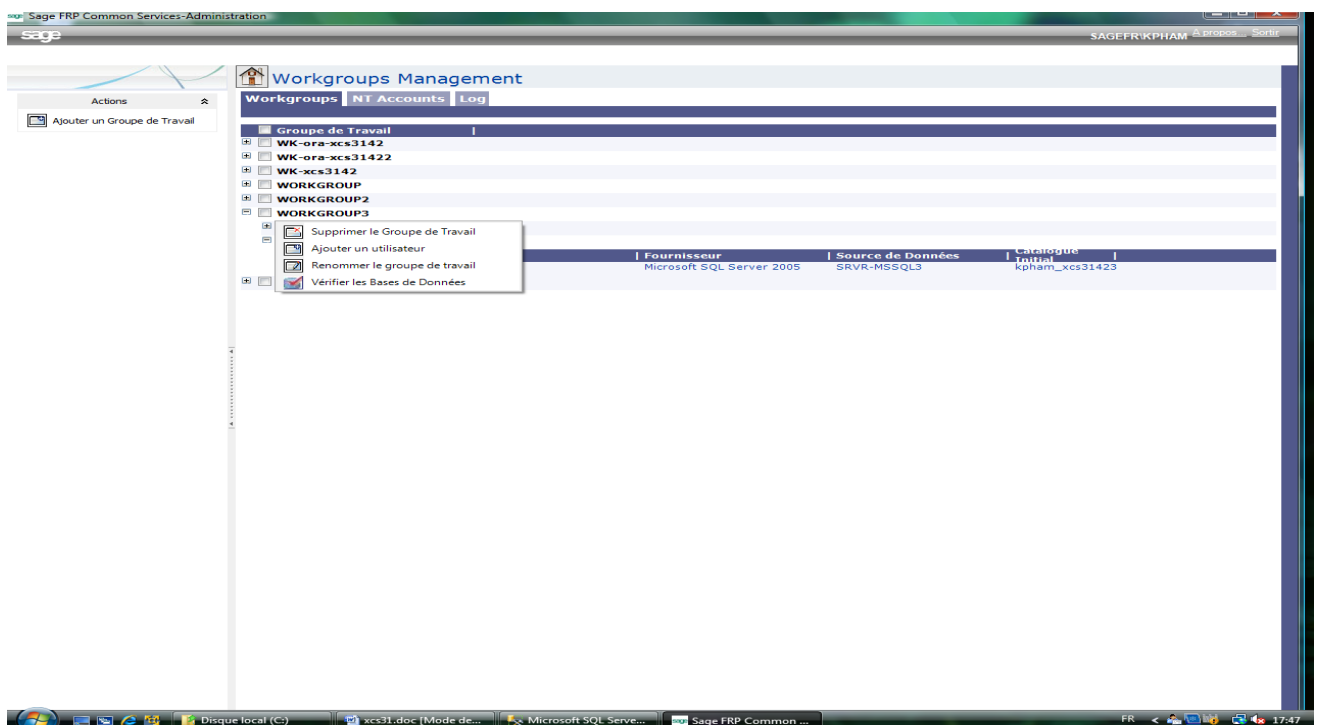
As creating a workgroup follows the same principle as creating a database, see paragraph 4.1.

4.6 Updating the Databases of a Workgroup

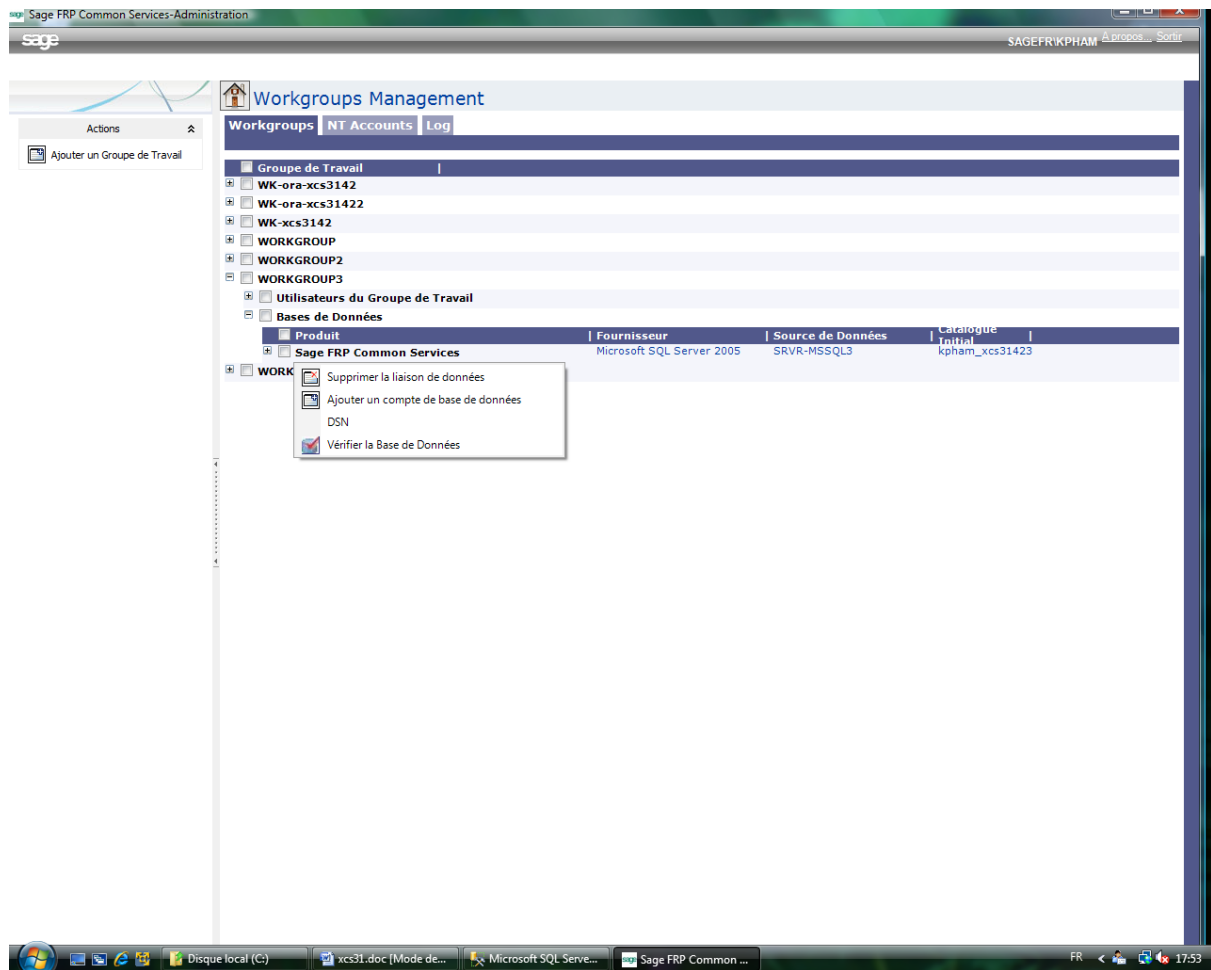
Important The database update may damage the user's data. This is a complex operation that cannot be 100% guaranteed. Do not perform this operation without the prior precaution of backing up your data.



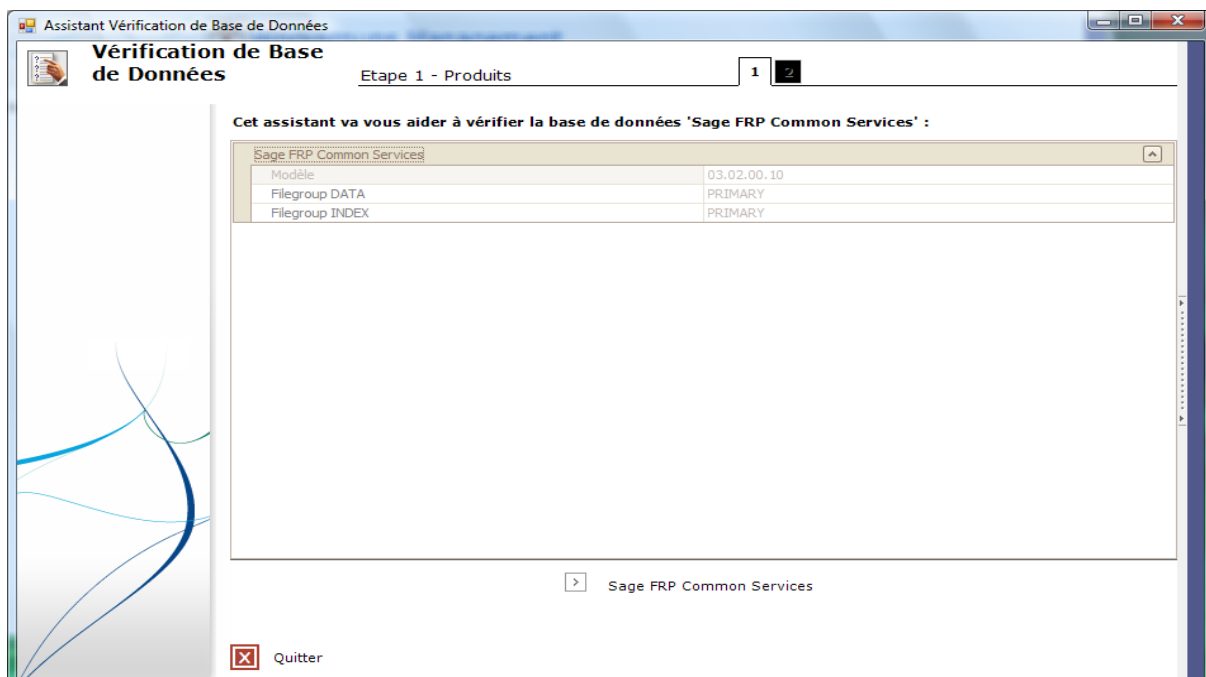
Click on a Workgroup (here **WORKGROUP3**)...



or on a product of Databases (here Sage FRP Common Services).



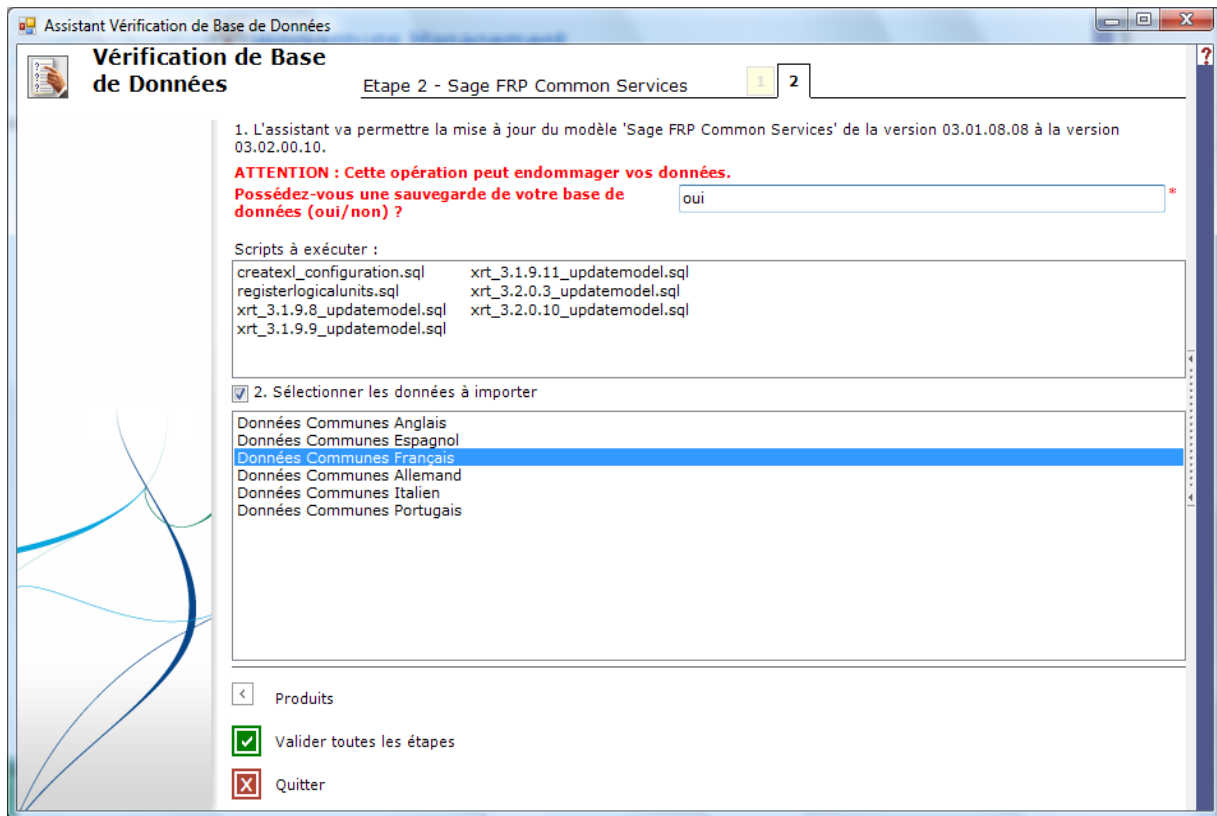
Select **Check Database** to display the **Database Check Wizard**:



Click on the product (here Sage FRP Common Services).

If the wizard detects inconsistency in the versions, it will prompt the user to go back to the updating process of the database.

Otherwise the following screen is displayed:



Answer the question: **Do you have a back up of your database (yes/no)?**

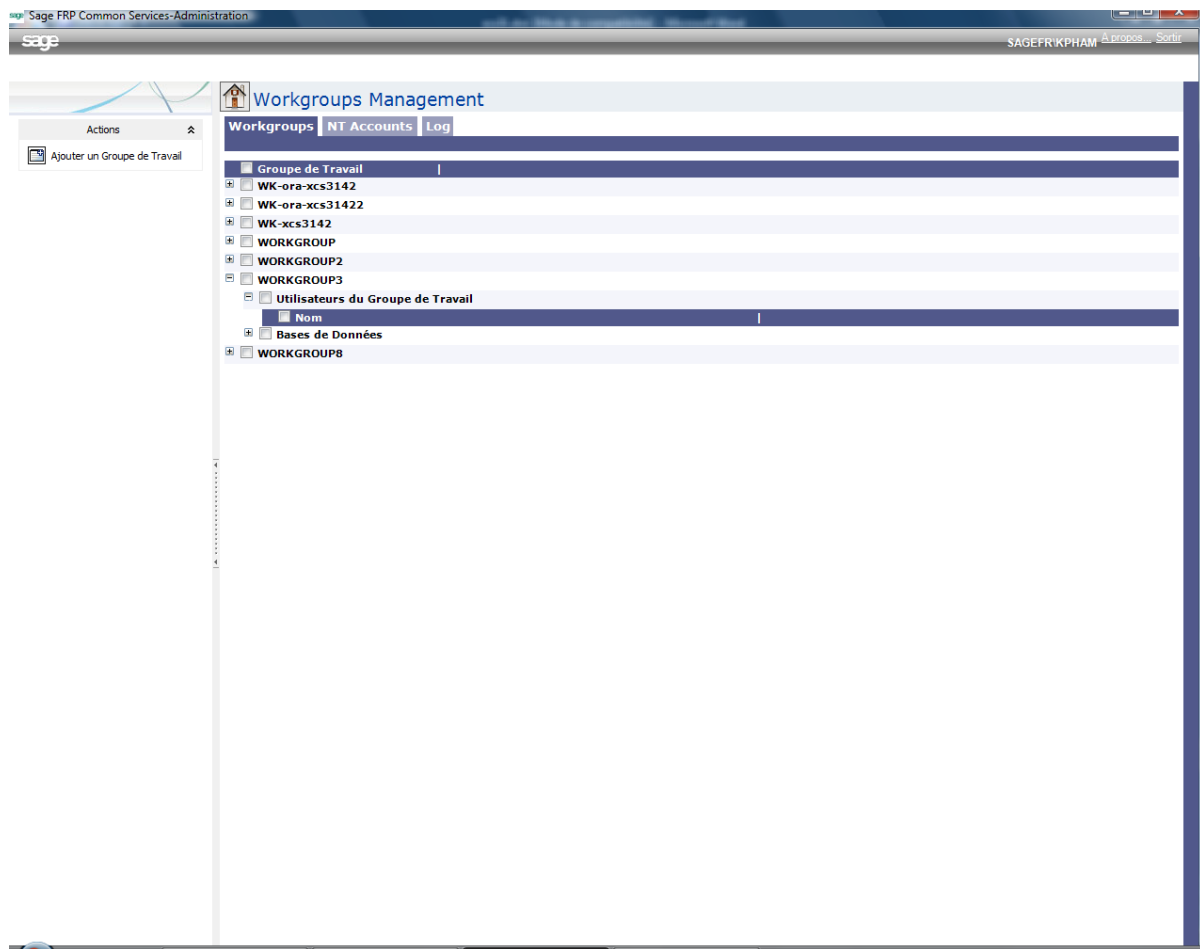
Check **Select data to be imported** if the data in Sage Common Services database are not up-to-date and select **Validate all steps**.

4.7 Managing Workgroup's Users

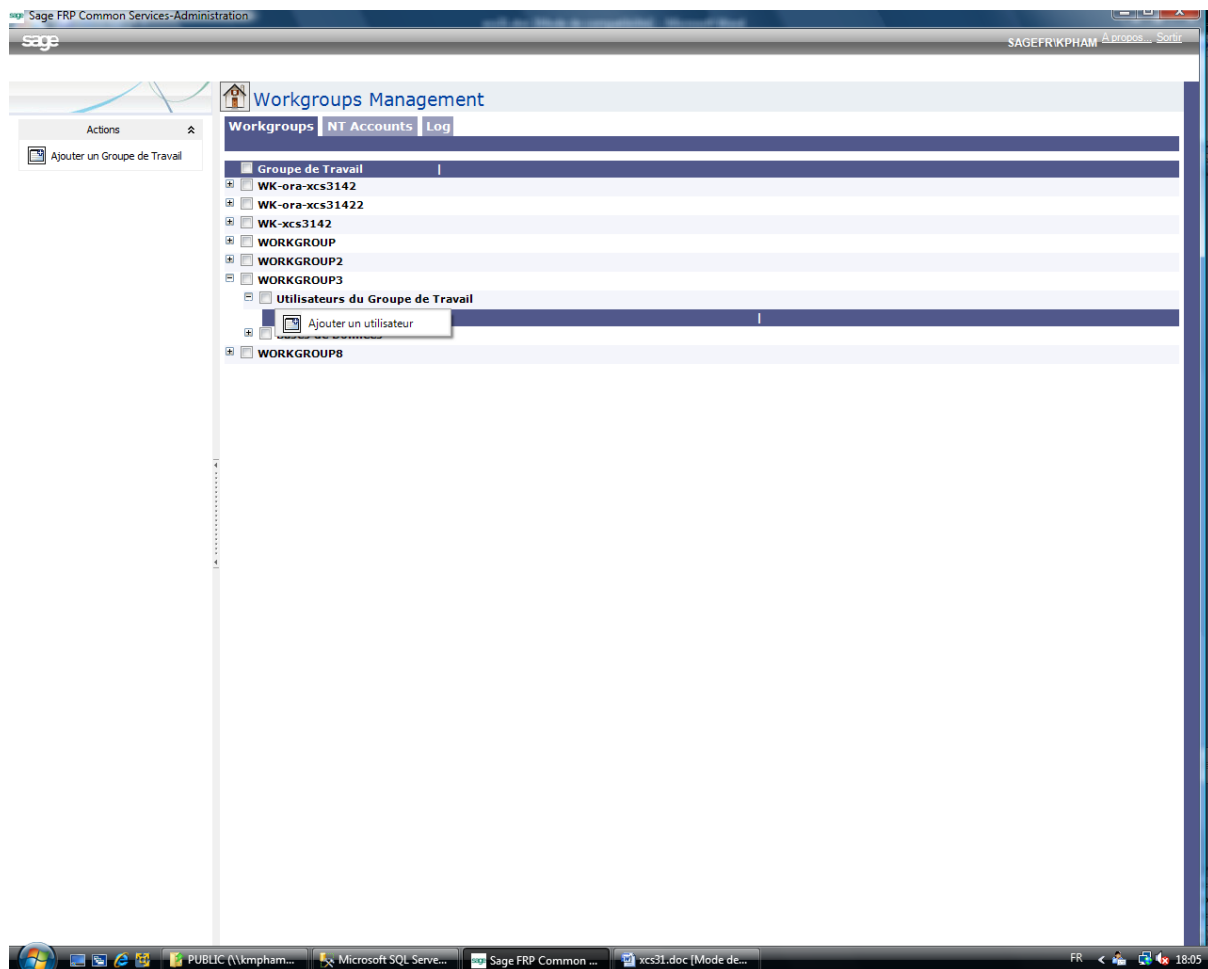
Workgroups are sets of users sharing common databases.

Important When creating a WORKGROUP, Windows NT Administrators and XRTDBAdministrators local groups are automatically declared as administrators of this group.

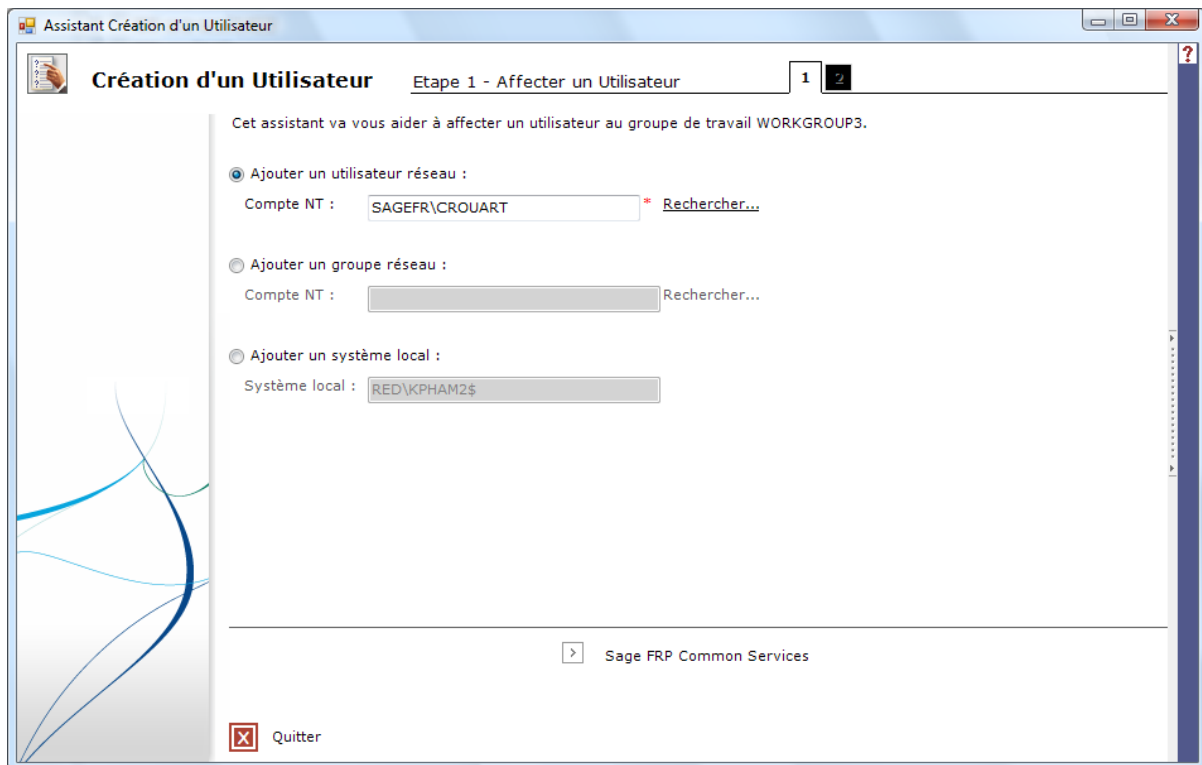
To assign a user to a workgroup, expand **Workgroup's Users**:



Click **Add User**.



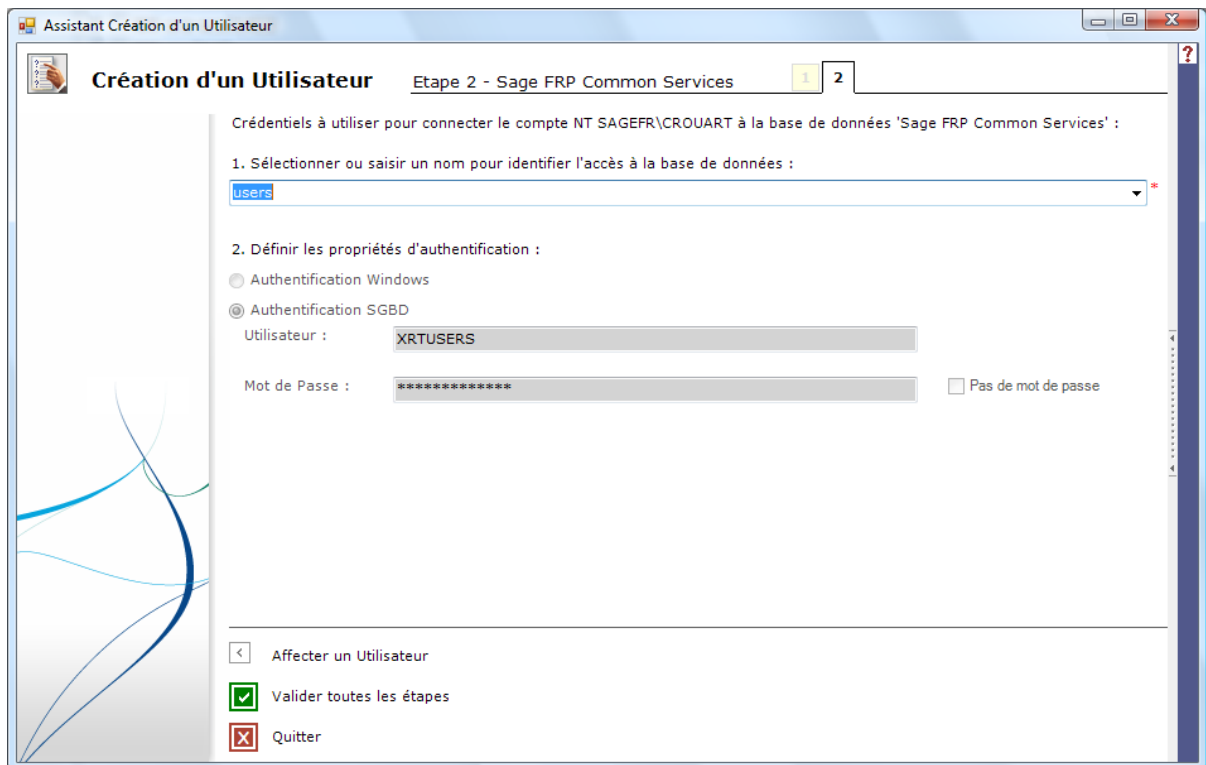
The **User Creation Wizard** appears:



Through the wizard, you can:

- Enter a NT account network user or click Search... to access the Microsoft tool that searches for NT users.
- Add a **network group** to the workgroup. This option enables to link users belonging to the same windows NT group to a WORKGROUP: Click **Search...** to access Microsoft NT search tool.
- Add a local system account to the workgroup: This type of account is aimed to being used by a system service executed for the account of the local system and needs to access a database.

Click Sage FRP Common Services and the following screen appears:

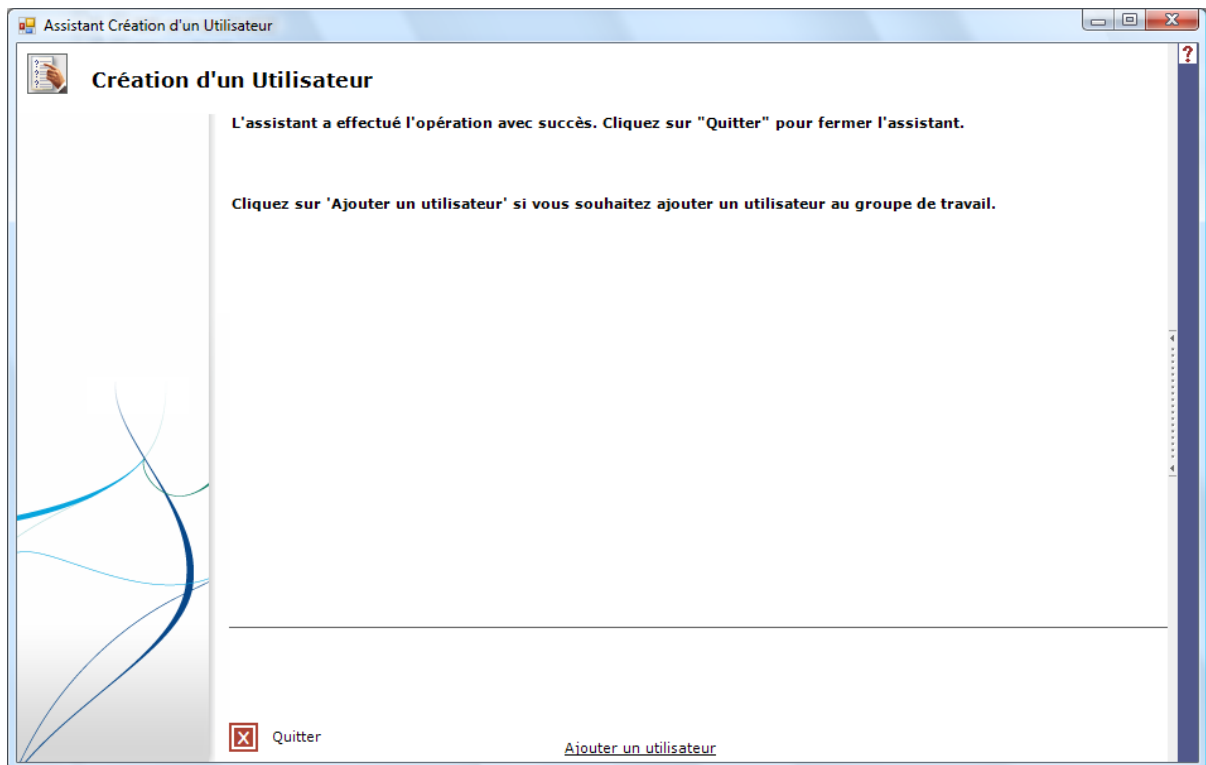


1. Select the name of an existing access to data or enter a new name. The wizard proposes 2 default types of predefined access:
 - a. Dbo: This access type should be reserved to the database owner.
 - b. Users: This access type should be used by users "with no authorization".
2. Select the user authentication mode on the database server:
 - a. Windows Authentication: the user is authenticated by his/her NT account.
 - b. DBMS Authentication: the user is authenticated by an account that was assigned to him/her by his/her database administrator (**DBA**).

Click Sage FRP Treasury (following product)

Go through the same process as for the access to Sage FRP Common Services database.

Click Validate all steps.



The wizard performs the following actions:

1. Adding a user to the workgroup.
2. Creating a "data link" for each workgroup's database to which he/she has access.
3. Creating a DBMS account on the server if the entered account does not exist (Microsoft SQL Server).



5 User Management

5.1 Introduction

UMAPI is the solution of Identity and Access Management for Sage applications (IAM).

5.2 Authentication

5.2.a Definition

Wikipedia definition:

Authentication is the act of establishing or confirming someone as authentic. It consists of verifying his/her identity based on:

- Something the user knows (e.g. password, NIP code...)
- Something the user has (e.g. chip card, digital certificate, cell phone, PDA etc...)
- Something the user is (e.g. biometric identifiers)
- Something the user does (e.g. gesture, signature)

UMAPI login model supports 3 authentication modes:

1. Windows authentication
2. UMAPI authentication
3. LDAP authentication

5.2.b Windows NT Authentication

Windows authentication uses NT Windows security and its user account management. This security mode enables Sage applications to use the credentials of Windows NT users.

Sage applications provide two operating modes:

1. The "trusted connection" for which the user does not need to enter his/her password.
2. The "standard" mode for which the user needs to enter his/her password. It is controlled by the system via Windows API.

The use of Windows authentication offers the following advantages:

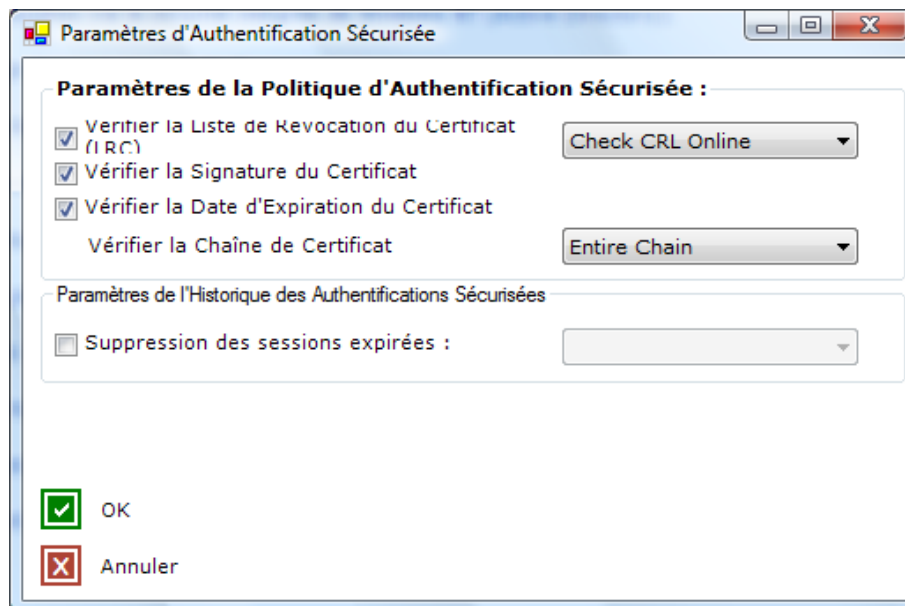
- The user does not need to learn additional credentials,
- When the user changes his/her password, he/she does not have to change it in UMAPI,
- The management of users complies with Sarbanes Oxley Act,
- With this authentication the user makes profit of the other functions of this system such as the periodic password change and the audit of access.

Setting up Windows NT authentication requires a close collaboration with the Windows administrator when creating users and workgroups.

The implementation of Windows authentication in UMAPI is based on the library of the base classes of the System.DirectoryServices namespace of framework Microsoft .NET.

Since version 3.1.8, Windows authentication has been completed with the use of X509 Certificates to connect to SBE Web application.

The Setup tab in the Rights Management feature enables to check the parameters of X509 Certificates and to delete expired sessions.




5.2.c UMAPI Authentication

When using UMAPI authentication, the user who wants to connect to a Sage application needs to enter a username and a password which are controlled on the basis of information contained in the database.

The management of passwords in UMAPI complies with Sarbanes Oxley Act:

- UMAPI saves the last 4 passwords. These cannot be used again when the system prompts the user to change his/her password. This function is settable.
- A default password is assigned to the user upon creation. This password must be changed upon first connection. This function is settable.
- The user account is locked after three consecutive authentication failures. This function is settable.
- A user account is locked and unlocked after a settable period of time.
- Passwords are not saved in the database. Only the SHA1 hash codes of these passwords are saved in the database.
- A password must contain 6 characters and include at least one capital and one digit. This function is settable.
- Passwords must be regularly changed. This function is settable.
- A user account can be locked by the administrator for a settable period of time or permanently.

Note:



When updating XCS database towards version 3.2, UMAPI passwords are automatically converted into SHA1 hash code via the execution of the xrt_2.5.3.5_updatemodel.cs script.

5.2.d LDAP Authentication

LDAP (Lightweight Directory Access Protocol) is a protocol which enables the management of directories which are bases of information on the users of a network, by TCP/IP protocol.

When using LDAP authentication, the user who wants to connect to a Sage application needs to enter a username and a password which are controlled on the basis of information contained in the LDAP directory.

The setup of the access to directory can be done from the screen of user management setup. The administrator must enter the following settings:

1. The IP address of the station that hosts LDAP server
2. the number of the port on which LDAP server must be called
3. The DN base of the directory
4. The user ID attribute name on which is based the user authentication E.g.: cn. It depends on the directory schema.
5. The "User" class name to use when searching the directory for a person.
6. The "Group" class name to use when searching the directory for a group of persons.
7. the credentials allowing to search the directory (the "test Connection" button enables cheking these credentials)

LDAP Settings

☒ Use Windows Active Directory only

☐ Use also custom LDAP server

Host: Port: 389 ☐ SSL ☐

☐ LDAP server supports anonymous bind

☐ Connect using currently logged on NT user credentials

☐ Connect using this credentials:

Bind DN:
example: cn=manager,dc=domain,dc=com

Password:

Test Connection

Base DN:
example: dc=domain,dc=com

User ID attribute name:
example: cn

User objectClass name:
example: person

Group objectClass name:
example: groupOfUniqueNames

Group members attribute:
example: uniqueMember

☒ OK

☐ Annuler

☐ Use secondary LDAP server when the main server is unavailable

Host: Port: 389 ☐ SSL ☐

☐ LDAP server supports anonymous bind

☐ Connect using currently logged on NT user credentials

☐ Connect using this credentials:

Bind DN:
example: cn=manager,dc=domain,dc=com

Password:

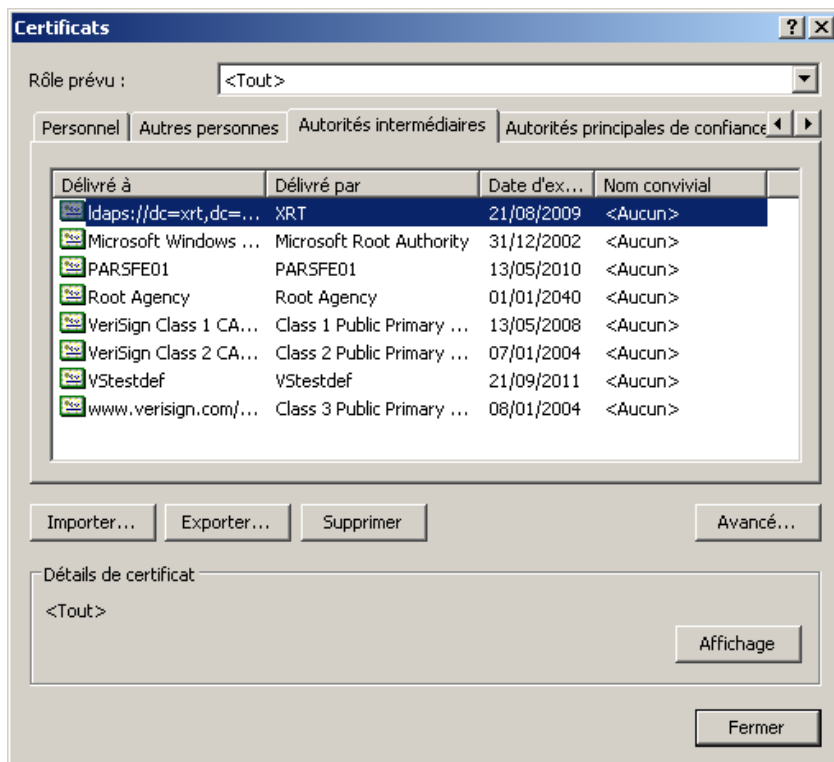
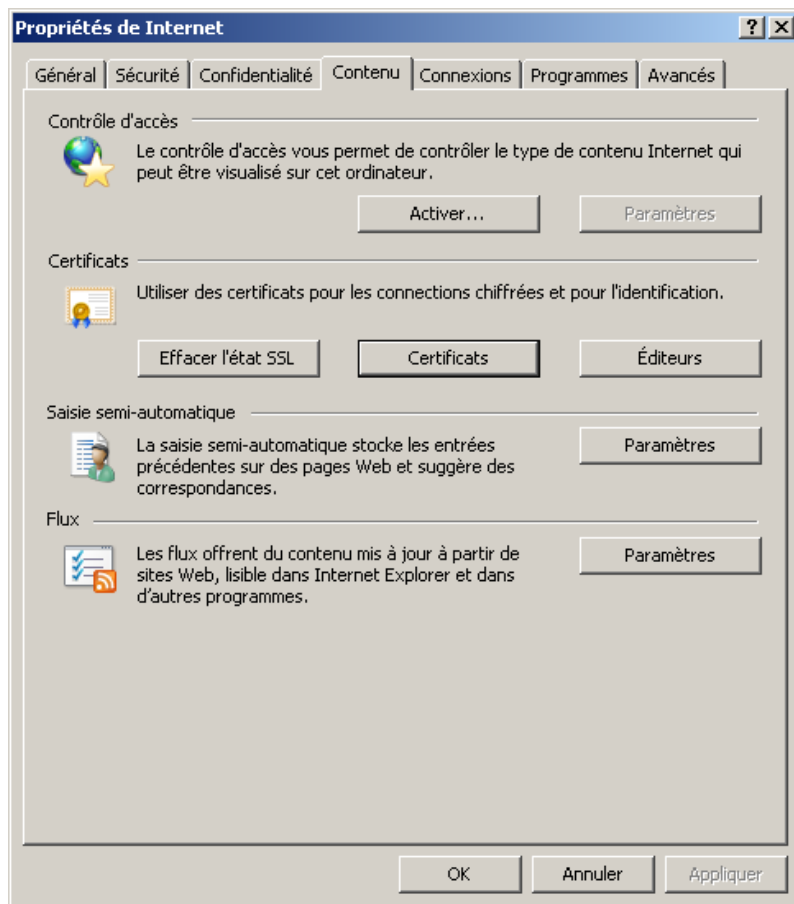
Test Connection

Figure 1: LDAP Settings

The implementation of the LDAP authentication within UMAPI is based on the base class library of the System.DirectoryServices namespace of Framework Microsoft .NET.

LDAP exchanges between client and server are usually made encrypted by standard TCP/IP port (port 389) or via the SSL tunnel (port 636). SSL technology (Secure Sockets Layer) is enabled by installing a certificate published by a certification authority approved by the domain controller and LDAP clients. The approval is obtained by setting up clients and server in order to approve the root certification authority to which the issuing certification authority is bound.

The installed certificate is usually located in the personal certificate store of the local computer in **Internet Properties/Content/Certificates/Intermediate Certification Authorities**.



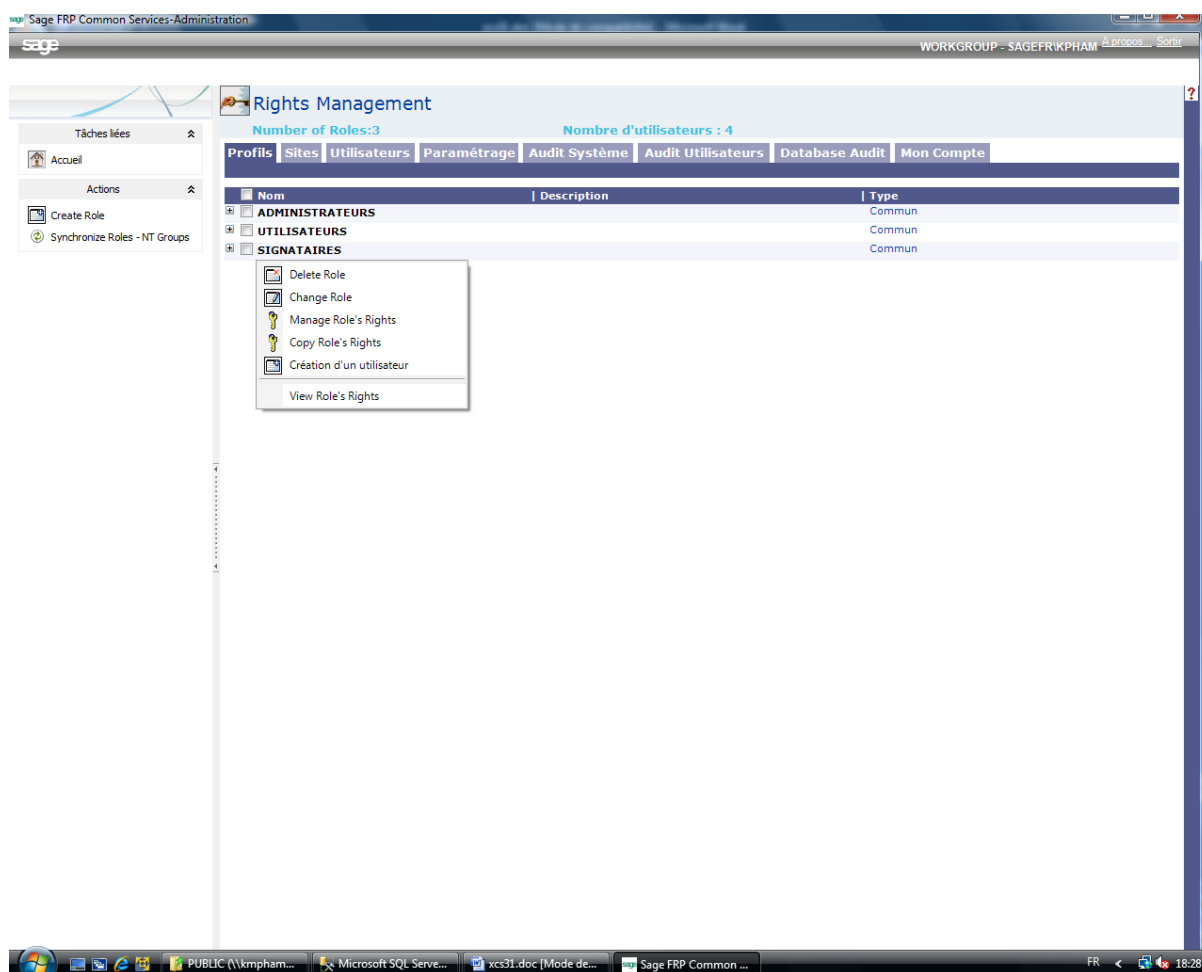
5.2.e User Account

A user account enables a user to be authenticated by Sage applications. It also enables the management of his/her access authorizations for the application functions. However, authentication does not automatically involve authorization management.

A *user account* includes the following elements:

- The user language (French, English, Spanish, Portuguese, Italian, German)
- His/her email address to which notifications will be sent
- A description
- The user type (administrator or standard user)

Click either on the **Users** tab or on the profile - in this case **Signatories** - to add users. A contextual menu is displayed:



Select the **Create a user** menu. The following window is displayed:

Création d'un utilisateur

Utilisateur : SAGEFR\KPHAM *

[Rechercher](#)

Rôles Sites

☒ ADMIN

Authentification

☒ Authentification Windows

☐ Authentification LDAP

☐ Authentification standard

Authentification de l'utilisateur via un Certificat x509 ☐

Mot de passe

Confirmation mot de passe

Type d'utilisateur

☒ Administrateur de sécurité de niveau 1

☐ Utilisateur standard

Informations diverses

Langue Français *

Description

email

☐ Période de Validité 0 years (jusqu'à 20/01/2011)

☒ OK

☐ Annuler

Single administration

Double administration

Select the authentication mode and enter the username:

- **Windows Authentication** offers two adding modes for NT users:
 1. Adding a user by selecting a person from the list in the dialog box relies on the workgroup management. This mode implies the previous definition of the database access for each user.
 2. It is also possible to add a person by searching a user through the company directory. In that case, the user gains access to the **XRTUsers**-type database.

If strong authentication is required – to connect to SBE Web application – select **Authentication via X509 Certificate**.

- **LDAP authentication:** search and select via the **Search** button the users who belong to the directory set up in the LDAP authentication configuration.

- **Standard authentication:** enter a unique identifier for the user.

Important Setting up access management based on NT accounts is highly recommended.

Choose the user type to be created:

- Level 1 security administrator: he/she administrates access permissions of the workgroup's users.
- Level 2 Security Administrator: he/she validates the access permissions granted by the level 1 security administrator. (This type of user can only be created if the system administrator created a workgroup which permissions are defined by 2 security administrators. they validate each other's decisions).
- Standard user: User with no authorization.

Fill in the **Miscellaneous** group box, then click **OK** and **Cancel** to quit the dialog box and go back to the treeview of the profiles list.

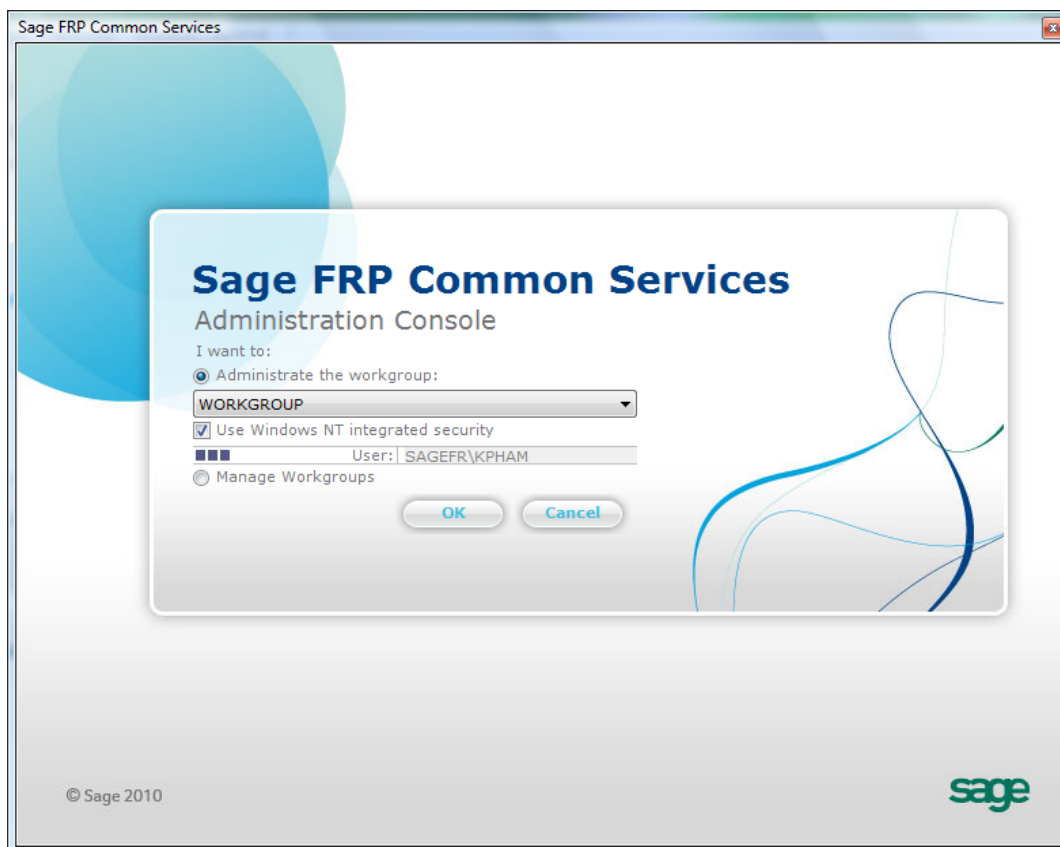
Note

In order to correct some errors and avoid problems with databases (Oracle), all users and profiles are saved in capitals and without any space characters at the beginning and end of the identifier. The values stored in the databases are converted during the update of Sage model via the execution of the script C# xrt_2.5.4.5_updatemodel.cs. The procedure takes into account potential duplicates then adds a _1, _2 suffix if necessary.

5.2.f Login

The Administration Console's welcome screen appears:

1. At the end of datasources migration or upon first definition of a workgroup.
2. In the **Start** menu, select **Programs – Sage – Sage Administration – Administration Sage .NET**. The following screen is displayed:



Important You must install a server or a DBMS client and the Sage applications on the computer to be able to run Sage Administration.

For the Administration Console, two operating modes are available:

- If **Administrate the workgroup** is selected:
this operating mode offers the following services:
 - The administration of access permissions for users of the selected workgroup.
 - The administration of the selected workgroup formats
 - The administration of transcoding tables for the selected workgroup

A user can belong to several workgroups. This is particularly the case for users working on a test and production environment. The login box provides a function that enables the user to change his/her workgroup:

- The login box displays the list of the workgroups to which the user belongs.
- By default, the login box displays the current workgroup.

To access the user management feature, select **Administrate the workgroup** and select the workgroup in the list (here "workgroup").

Access to this operating mode is secure. You need to authenticate yourself with a user account of the workgroup.

The NT authentication provides two operating modes:

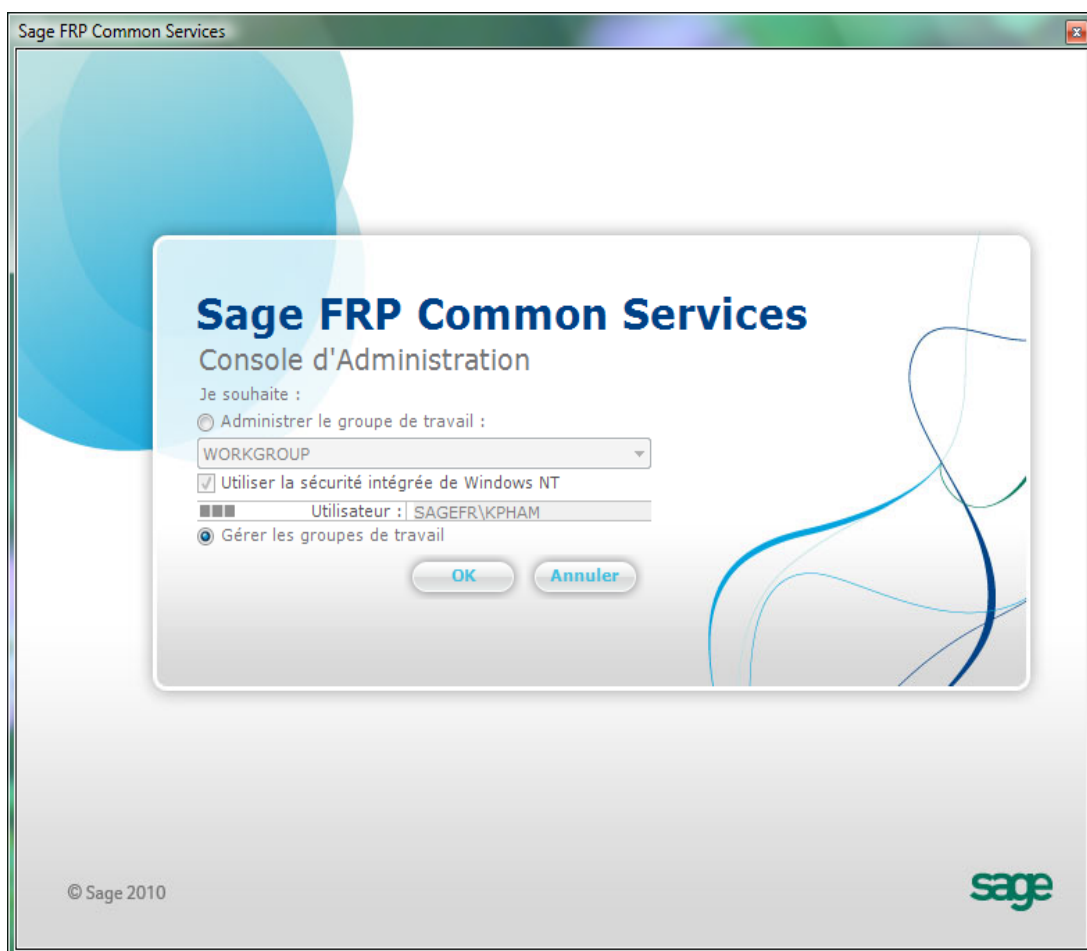
- Trusted connection: The password is not necessary.

- Strong authentication: the user needs to enter his/her password to enter the administration console. This operating mode secures the access to an application available on a station which was not locked.

- **Manage Workgroups:**

This operating mode is designed for the **system administrators** who manage **workgroups**. This mode enables:

- The creation/deletion of a workgroup
- Adding a user to a workgroup
- A user deletion
- The update of workgroup's databases




5.3 Access Management

5.3.a Permissions

The application calls the authorization manager when a user tries to access a given function to check if he/she has the required permissions. These are defined by the UMAPI administrator.

By default, the user has no access to any of the product's functions. The administrator must define the access rights of users.



With UMAPI, companies can choose the authorization management mode:

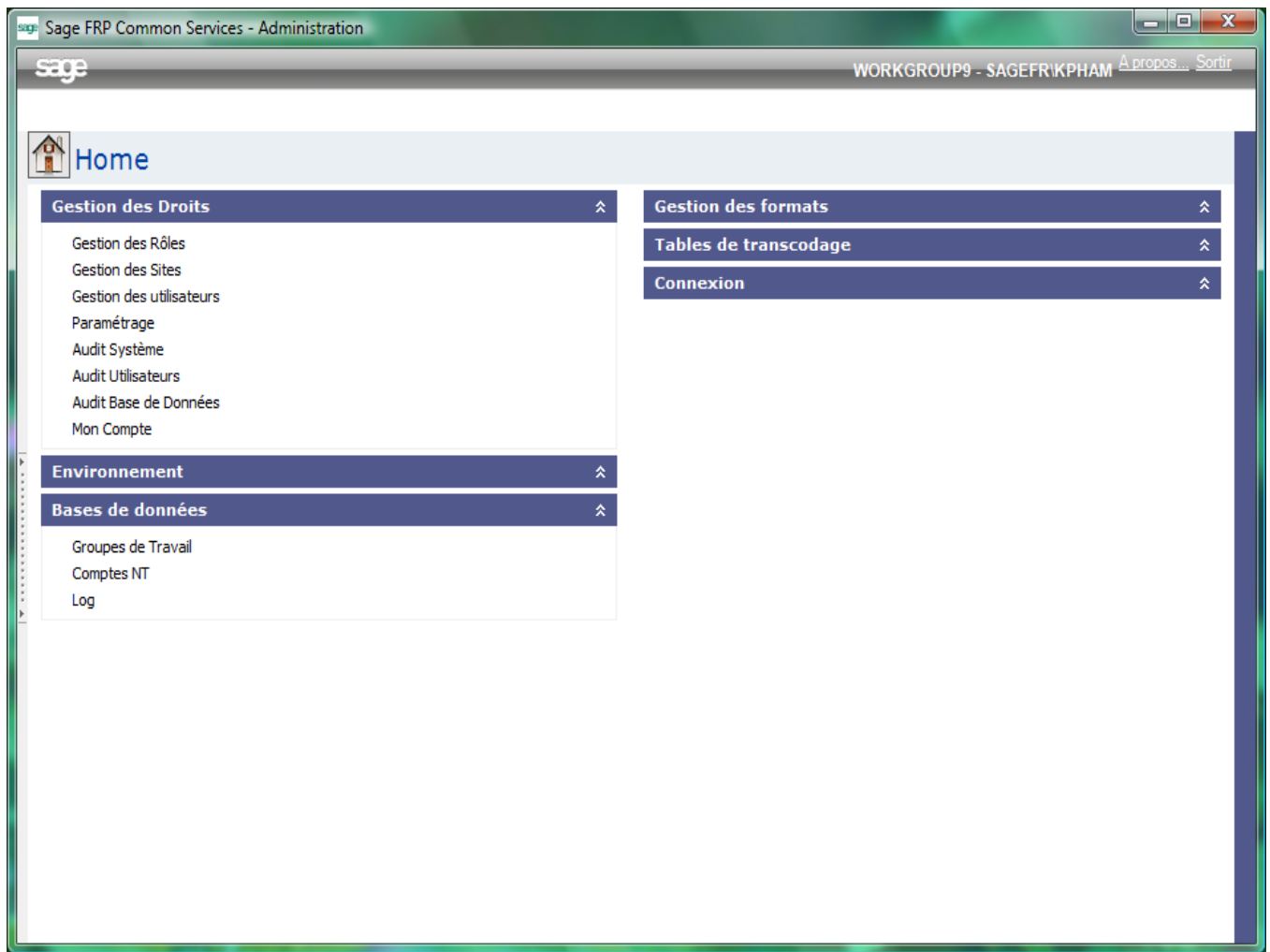
1. Authorizations are managed by one administrator
2. Authorizations are managed by two administrators

According to the operating mode chosen by the administrator, a user can have the following roles:

1. Authorizations are managed by one administrator:
 - a. The Security Administrator is responsible for:
 - i. Creating profiles
 - ii. Defining permissions
 - iii. Creating users
 - iv. Assigning users to profiles
 - b. A standard user has no administration privilege.
2. Authorizations are managed by two administrators:
 - a. The Level 1 Security Administrator is responsible for:
 - i. Creating profiles
 - ii. Defining permissions
 - iii. Creating users
 - iv. Creating Level 2 Administrators
 - v. Assigning users to profiles
 - b. The Level 2 Security Administrator is responsible for:
 - i. Validating permissions defined by the Level 1 Security Administrator
 - ii. Validating user assignments defined by the Level 1 Security Administrator
 - c. A standard user has no administration privilege.

5.3.b Welcome Screen

The Administration Console is now running. If using Sage Business Exchange, you can quit the console as no further action is required. For other Sage product please follow the procedure described below.



5.3.c Profile or Role

A profile (role) consists of users sharing the same rights. A right authorizes or denies to the user the access to a product function.

Important A user can belong to several profiles:

- a user is authorized to access a product function if the corresponding permission is opened in at least one of the profiles to which he/she belongs.
- UMAPI executes an OR operation on permissions.

This operating mode enables the association of a profile with a group of persons with the same activities.

The "standard" profile is defined by the following characteristics:

- A code that identifies the profile (no space)
- A description.

Click on the **Creating a profile or role** action link.

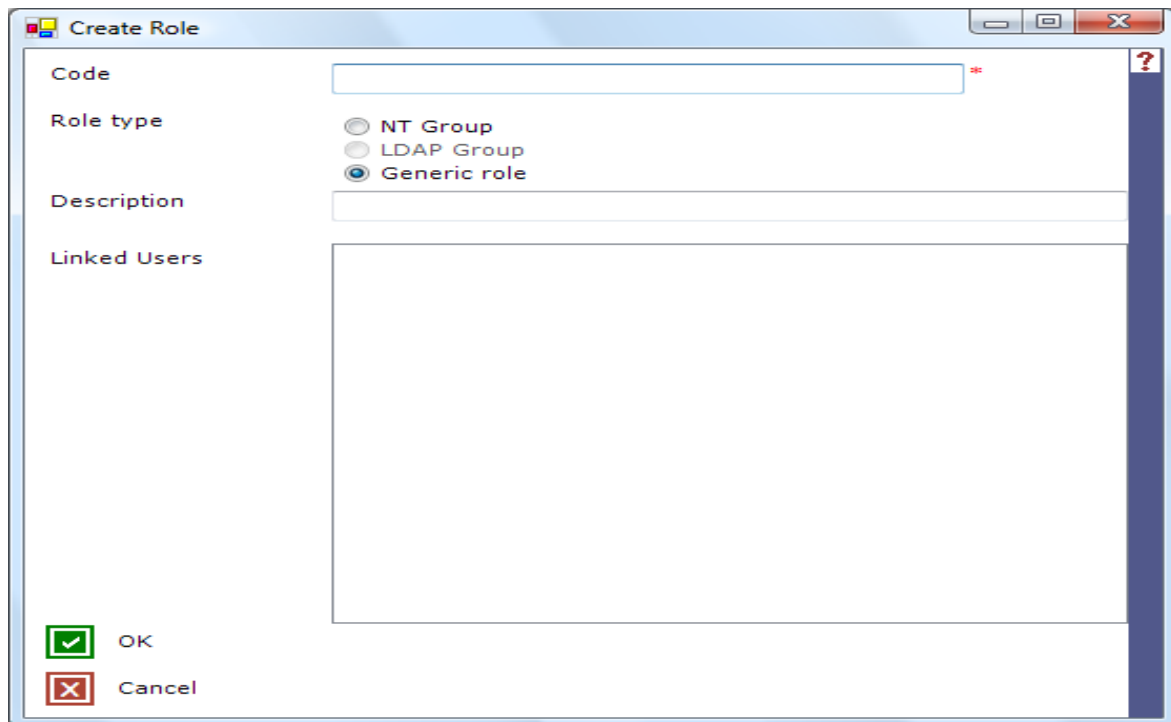


Figure 2: Creating a "standard" profile or role

In order to provide the best integration of Sage applications in companies infrastructures, it is now possible (since version 3.0) to rely on **NT** or **LDAP**-type groups. The creation of an LDAP group is linked to the configuration of the access of the company directory.

Important: when creating a "NT" or "LDAP" profile, all users belonging to the group are automatically registered in the database as SAGE application users.

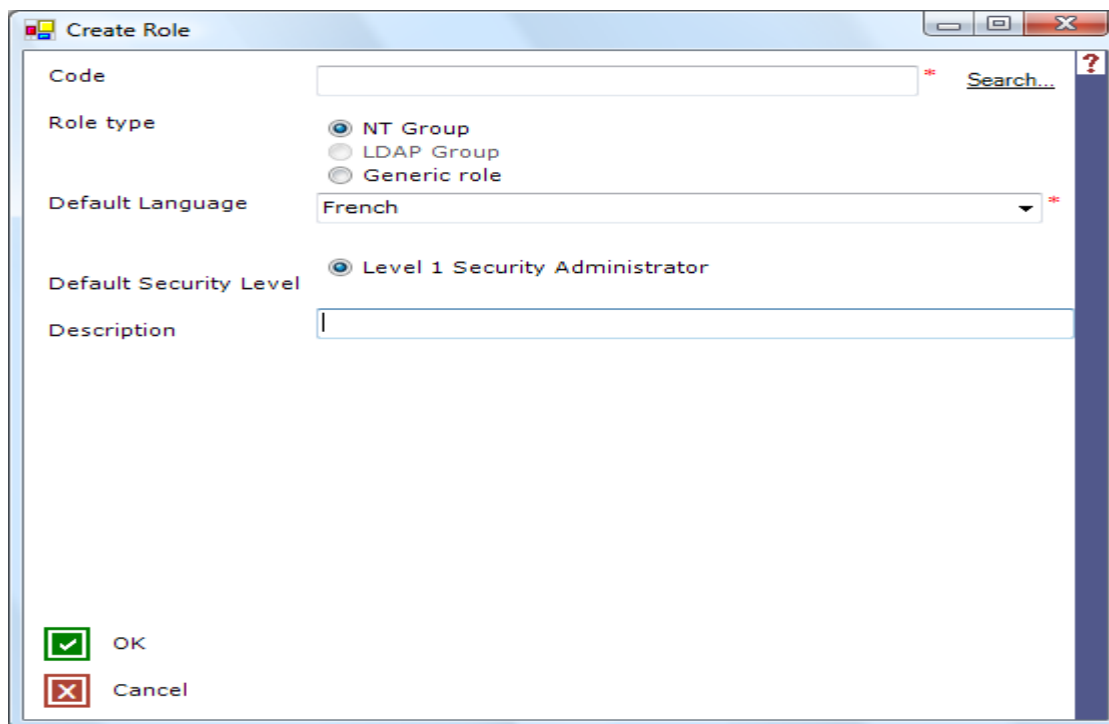
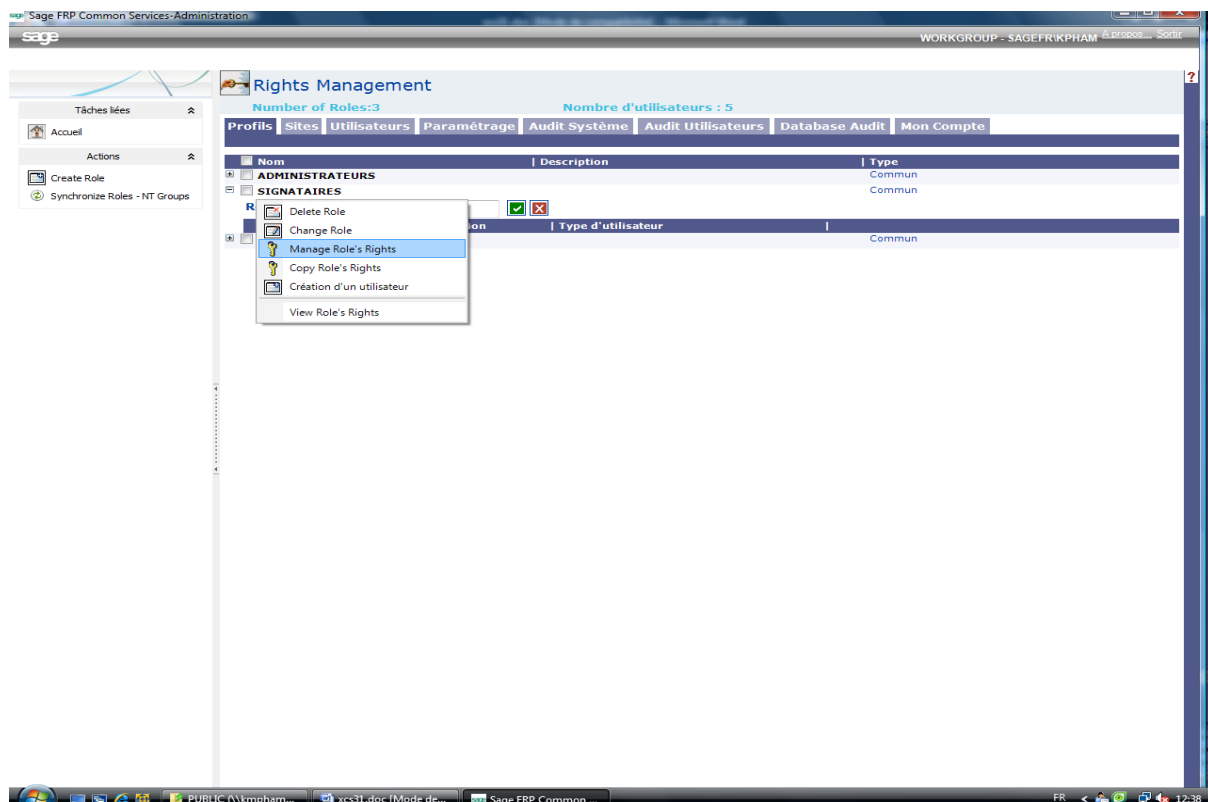


Figure 3: Creating NT Role or Profile

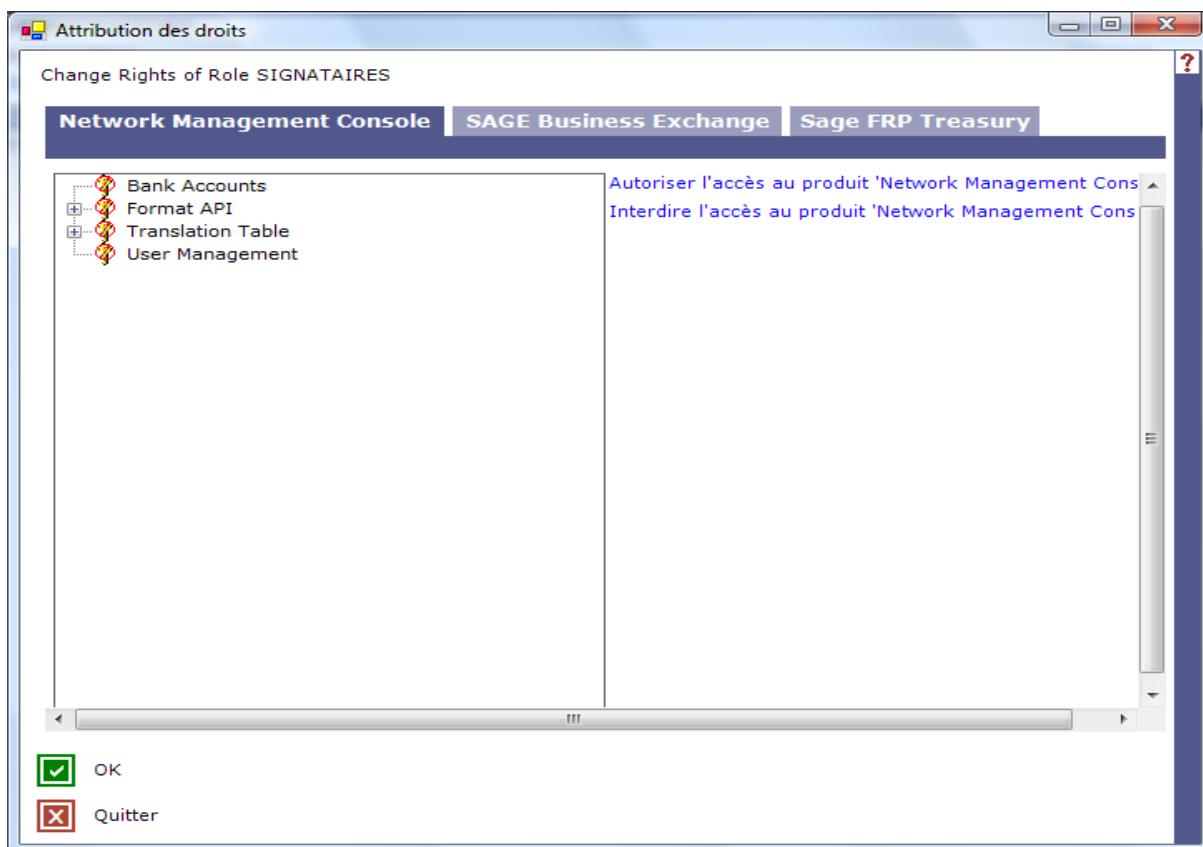
5.3.d Managing Profile Rights

Managing rights with a single Security Administrator

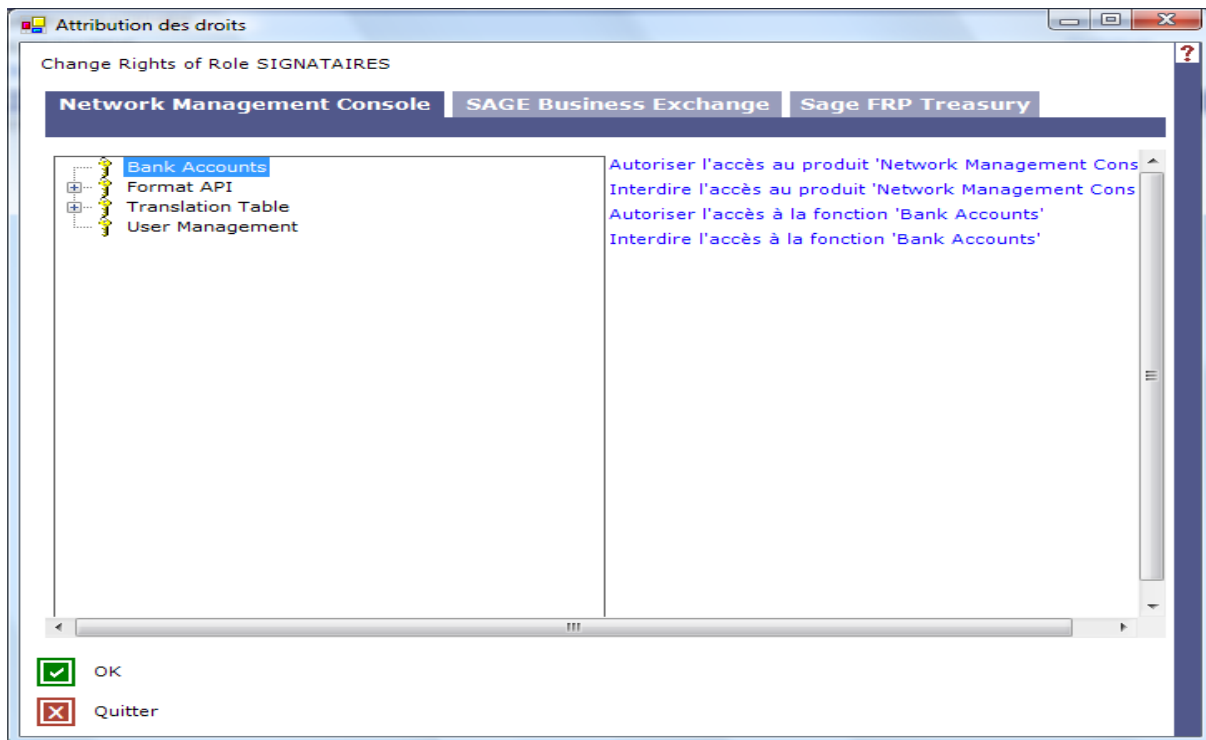


Click the **Manage Profile's Rights** menu of the profile rights that you want to define.

The **Grant Rights** window enables the management of access rights to the various Sage products installed on your server. Click the **Network Management Console** tab.

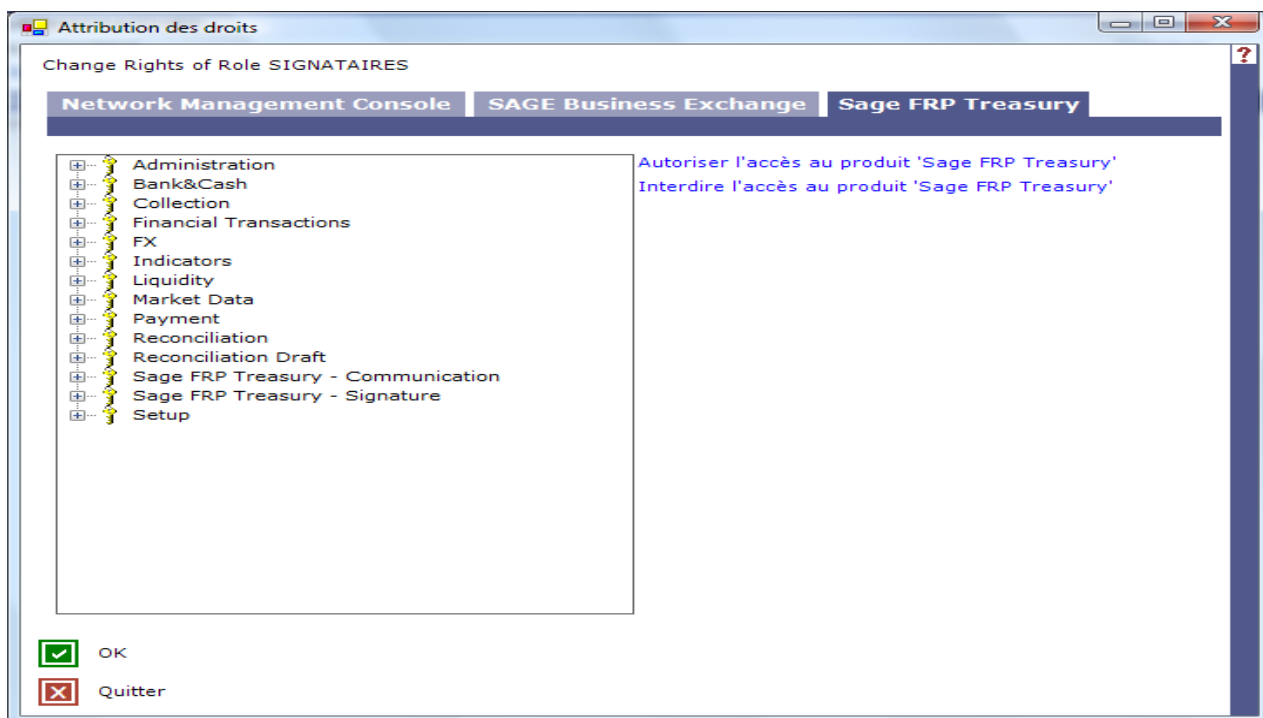


Select **Authorize Access to 'Network Management Console' Product** to give all rights to the Administration Console.

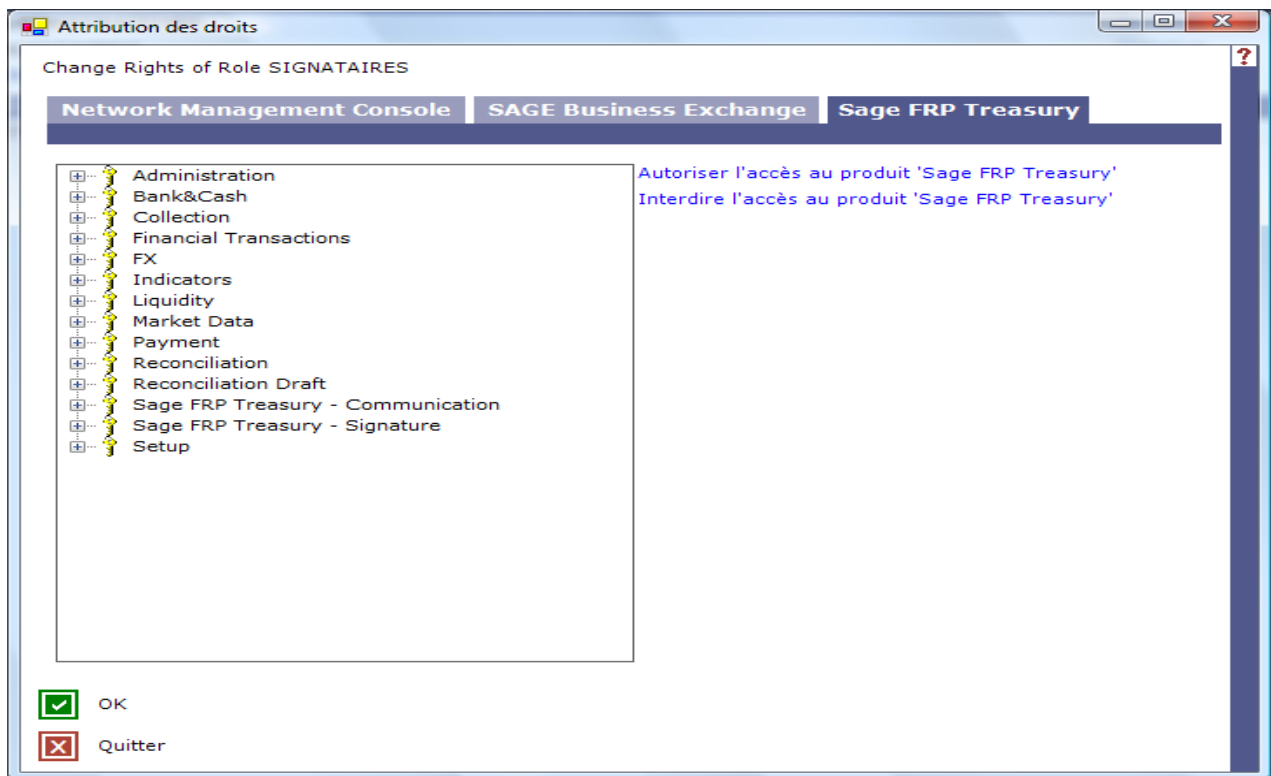


Then according to your needs, go to the tabs of Sage FRP Treasury, Sage Business Exchange to define rights. In our case, all products have all rights.

Select **Authorize the access to 'SAGE FRP Treasury' product** to grant all access rights to Sage FRP Treasury.



Select **Authorize the access to 'SAGE Business Exchange' product** to grant all access rights to the "bank server" application.

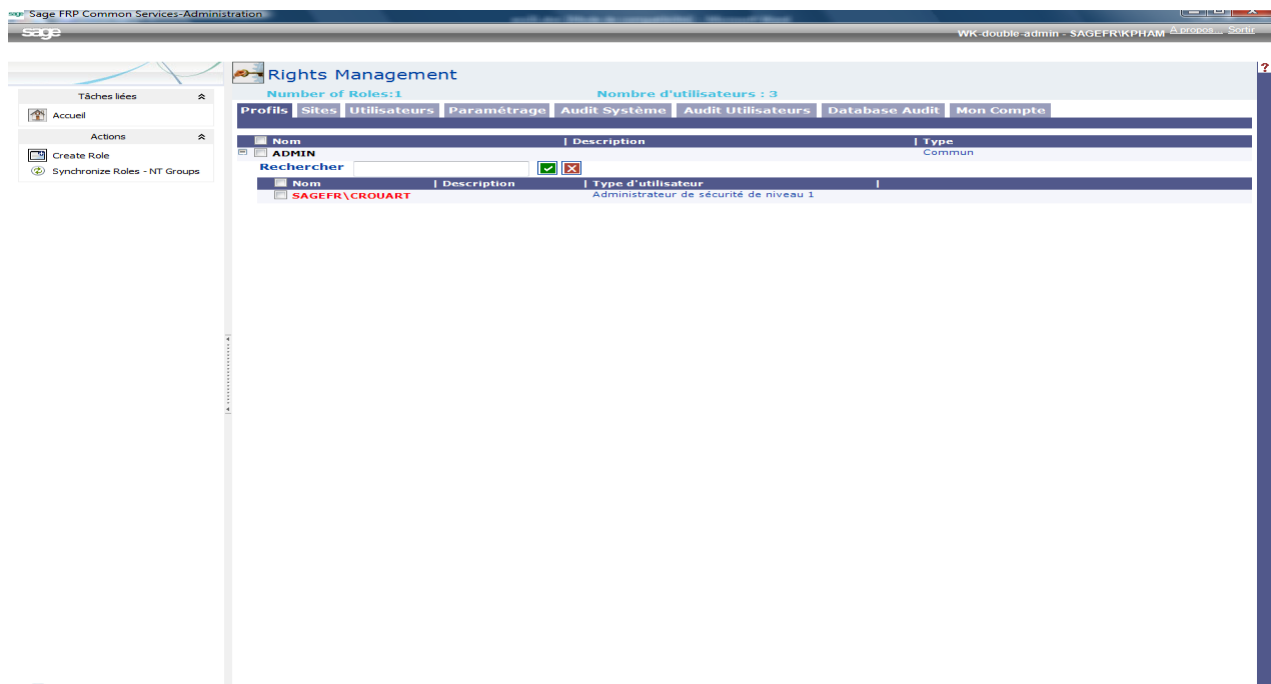


A profile and then a user are created.

You can now quit the Administration Console to enter the different products with the user that has just been created.

Managing Rights with Two Security Administrators

This management starts with the creation of a profile followed by the creation of two users: a Level 1 Security Administrator and a Level 2 Security Administrator. By default this profile cannot be accessed, which is showed by the red color of the created usernames. The Level 2 Security Administrator must validate in his/her own login the association of users to this profile, so it can be exploitable.

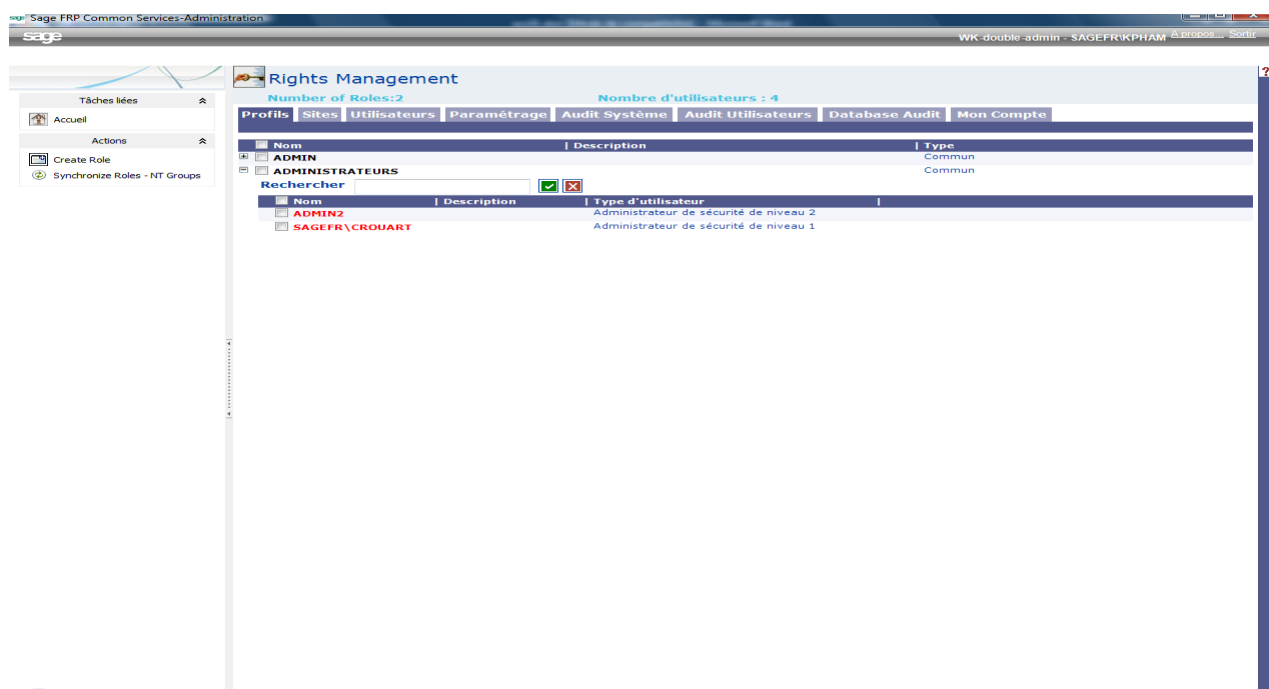


Sagefr\CROUART is the level 1 administrator

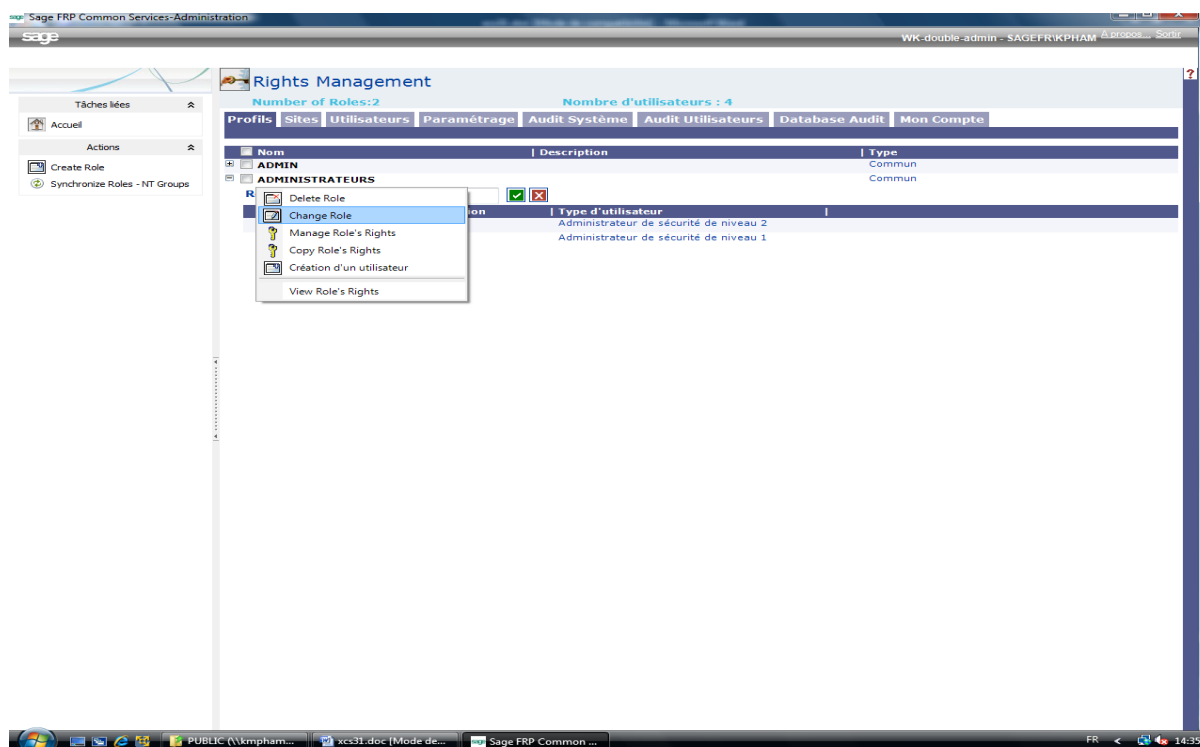
The 'Création d'un utilisateur' dialog box is shown. The 'Utilisateur' field is set to 'admin2'. The 'Rôles' section has 'ADMIN' selected. The 'Authentification' section has 'Authentification standard' selected. The 'Type d'utilisateur' section has 'Administrateur de sécurité de niveau 2' selected. The 'Informations diverses' section has 'Langue' set to 'Français', 'Description' empty, 'email' empty, and 'Période de Validité' set to '0 years'.

Create the Level 2 Security Administrator, here "ADMIN2".

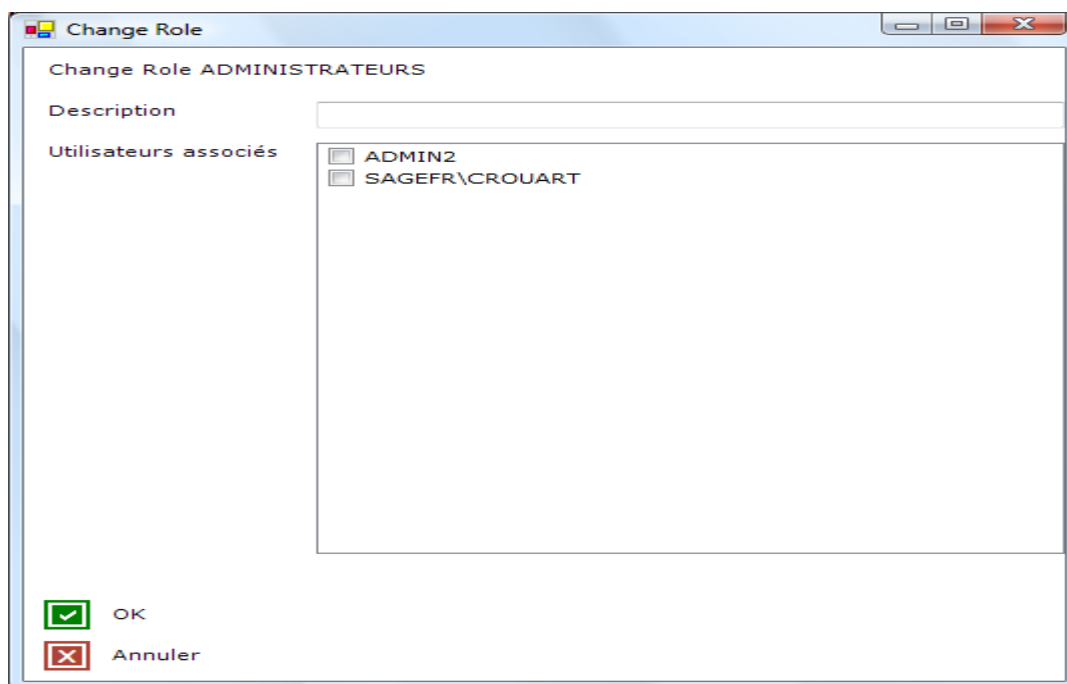
Enter the ADMIN2 login and expand the ADMINISTRATORS profile.



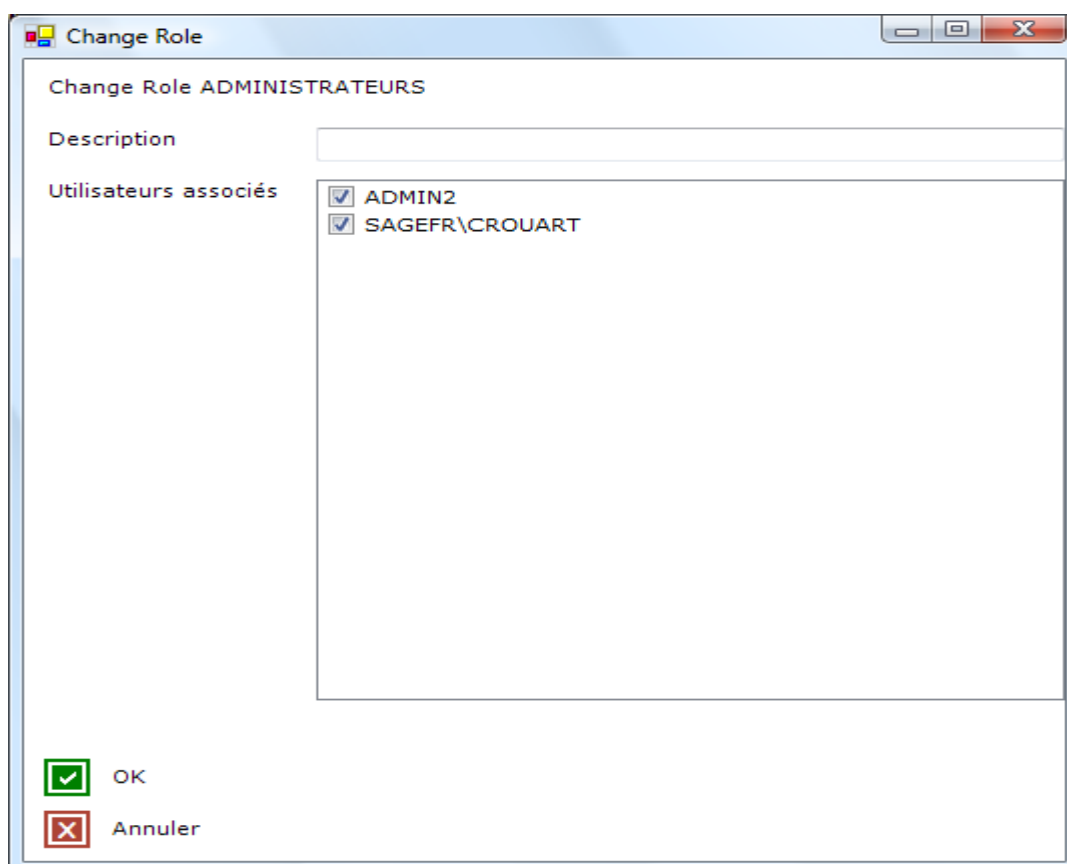
SAGEFR\CROUART and ADMIN2 users are red. They are not yet exploitable.



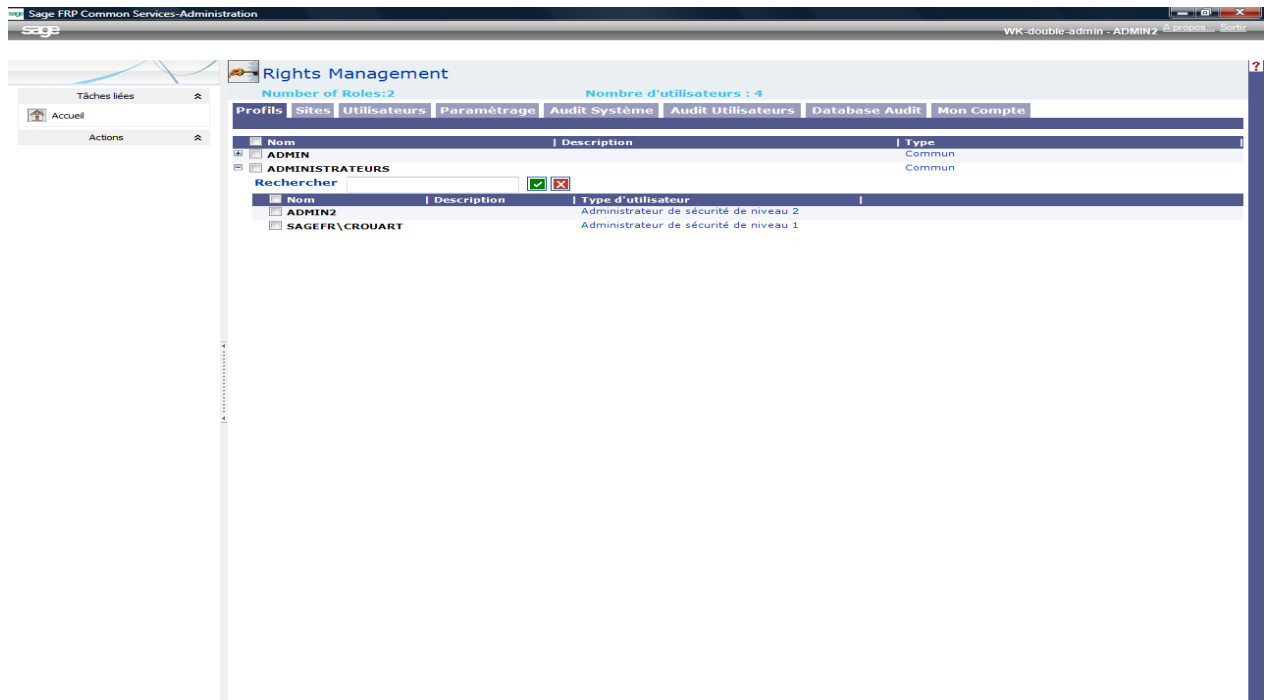
Click the "Change profile or role" menu.



In the ADMINISTRATORS profile, users SAGEFR\CROUART and ADMIN2 do not belong to this profile yet.



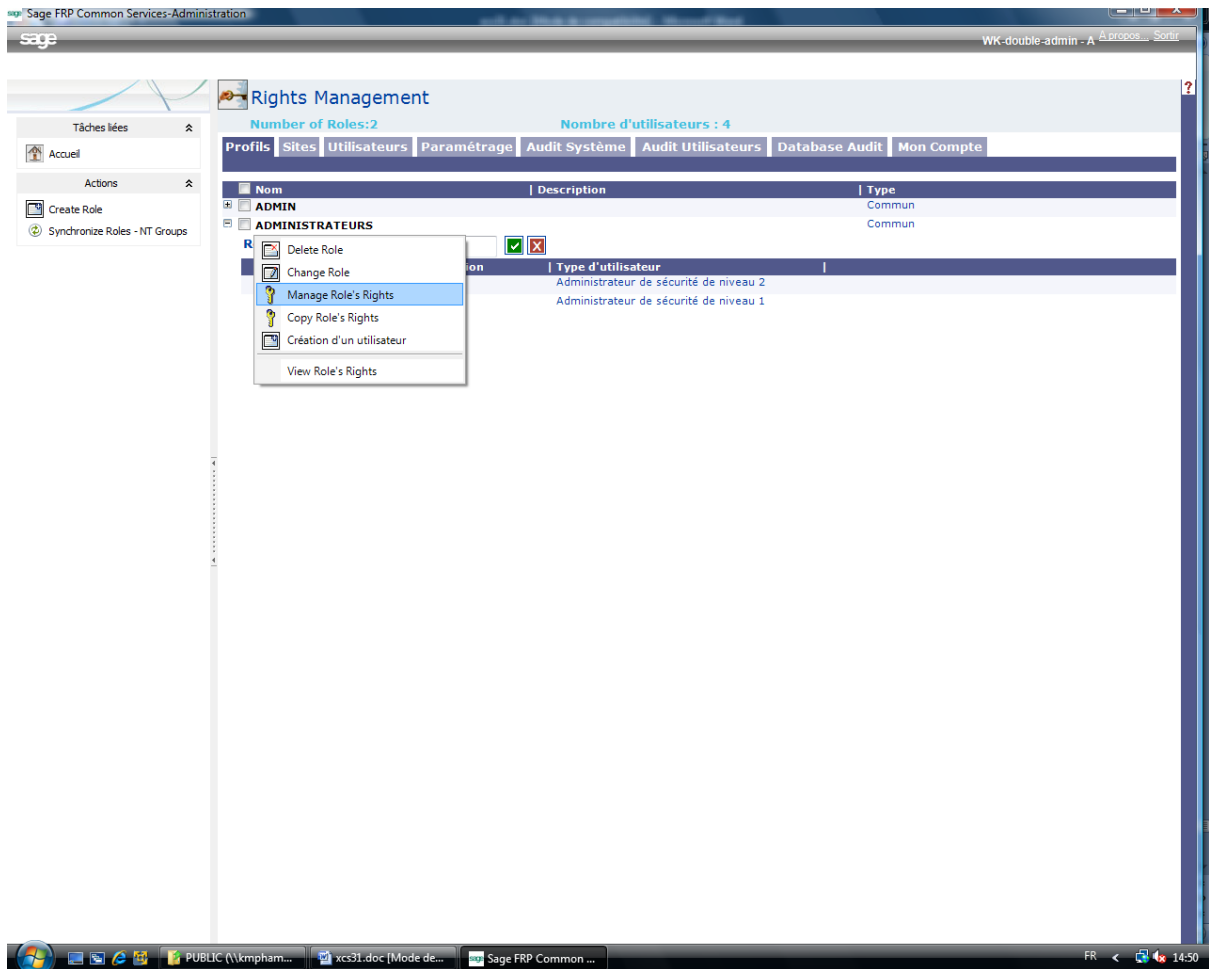
Select the users SAGEFR\CROUART and ADMIN2 associated with the ADMINISTRATORS profile and click OK.



SAGEFR\CROUART and ADMIN2 users are now valid. (color change: red-black).

You can go to the next step: assigning access rights.

Go back to the login of the Level 1 Security Administrator "SAGEFR\CROUART".

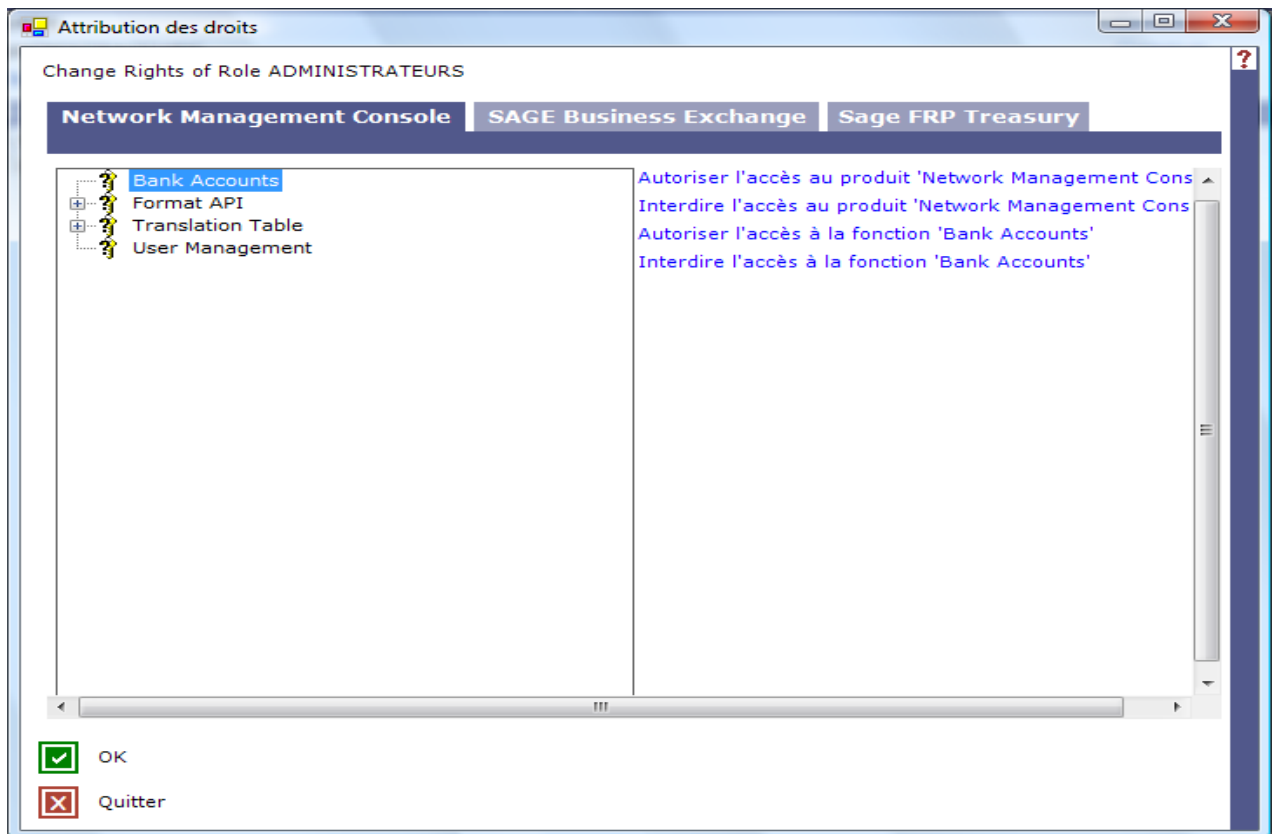


Select "Manage Profile or role's" Rights.

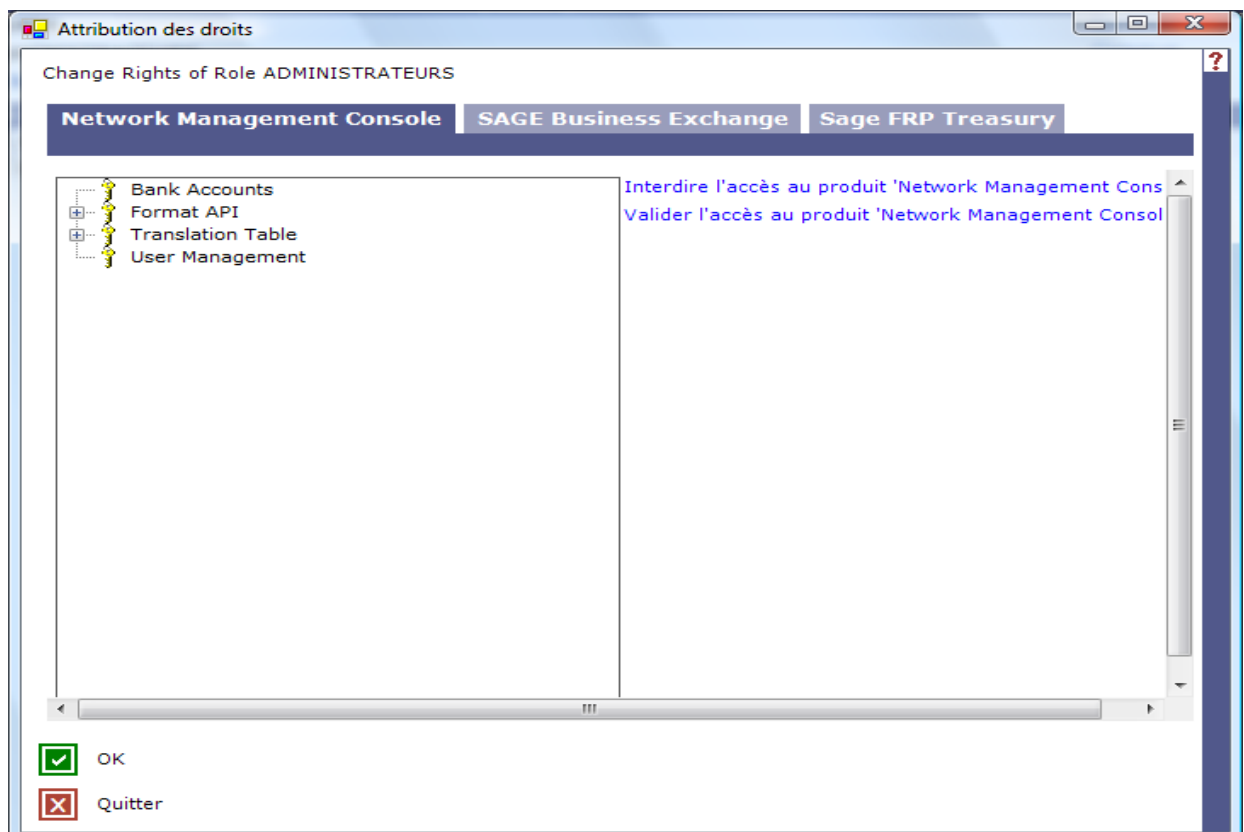
Granting rights with two security administrators instead of a single one changes the following elements:

- The Level 1 Security Administrator authorizes the access rights to modules and products marked with "?". At this stage rights can still be changed.
- The Level 2 Security Administrator validates access rights authorized by the Level 1 Security Administrator marked with a key. Rights are now definitive.

First, give all rights to 'Network Management Console' product.



Select **Authorize Access to 'Network Management Console' Product** and click **OK**.
 Restart the application with the login of the Level 2 Security Administrator.





Select **Validate Access to 'Network Management Console' Product** and click **OK**.

Go through the same process in Sage Business Exchange and Sage FRP Treasury tabs to define rights. In our case, all products have all rights.

You can now quit the Administration Console to enter the different products with the users that have just been created.

5.4 Audit

5.4.a Definition

On top of providing the obvious functions, the identity and access management must prove its efficiency. The proof must be remitted to auditors upon request and in written to be archived.

The proof must cover the frequently audited areas, i.e.:

1. Administrator actions:
 - User Creation
 - User Deletion
 - Change of user's password
 - Change in the management strategy of passwords
 - Change of the access configuration to LDAP directory
 - Access granted
 - Access denied to a function or a product
2. Final User actions:
 - login
 - logoff
 - specific messages from the application
3. *Tests for the compliance with security policy:*
 - User account locked after n failed tries to log on

5.4.b Audit Management

Tables Organization

The **System Audit table** describes all actions executed by UMAPI at time t. It includes the following elements:

The screenshot shows the 'Rights Management' window in Sage FRP Common Services-Administration. The window has a sidebar with 'Tâches liées' (Accueil, Actions) and a main area with tabs: Profils, Sites, Utilisateurs, Paramétrage, Audit Système, Audit Utilisateurs, Database Audit, and Mon Compte. The 'Audit Système' tab is active, displaying a table of system audit events. The table has columns: Date, Heure, Statut, Utilisateur, Compte de l'utilisateur, Machine, and Description. The data shows various successful login and role creation events for users like PHAM, TEST, and SIGNATAIRES on KPHAM2 machines.

Date	Heure	Statut	Utilisateur	Compte de l'utilisateur	Machine	Description
12/11/2009	10:13:48	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Création d'un utilisateur 'PHAM' (Utilisateur standard, umapiA...
12/11/2009	10:13:50	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Ajouter l'utilisateur 'PHAM' au profil 'UTILISATEURS -> isRole'
12/11/2009	10:14:07	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Autoriser l'accès au produit 'SAGE Business Exchange'
12/11/2009	14:48:03	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Création d'un utilisateur 'TEST' (Utilisateur standard, umapiA...
12/11/2009	14:48:03	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Ajouter l'utilisateur 'TEST' au profil 'UTILISATEURS -> isRole'
07/12/2009	18:26:54	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Create Role 'SIGNATAIRES' (isRole)
07/12/2009	18:27:22	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Modification d'un utilisateur 'SAGEFR\KPHAM' (Administrateur ...
09/12/2009	11:51:30	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Création d'un utilisateur 'SAGEFR\KPHAM' (Administrateur ...
09/12/2009	11:51:33	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Ajouter l'utilisateur 'SAGEFR\KPHAM' au profil 'ADMINISTR...
09/12/2009	12:42:59	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Autoriser l'accès au produit 'Network Management Console'
09/12/2009	12:46:55	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Autoriser l'accès au produit 'Sage FRP Treasury'
09/12/2009	14:14:10	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Autoriser l'accès au produit 'SAGE Business Exchange'

- **Date** and **Time** indicate the day and time of actions.
- **Status** indicates the level of the audit (here INFO).
- **User** indicates the login account in xcsmcnet.
- **User's Account** indicates the account of the session in which xcsmcnet is launched.
- **Computer** indicates the name of the computer on which actions are performed.
- **Description** indicates the actions performed by UMAPI.

The **Users Audit table** describes the logins/logoffs for XCS applications and particularly XBE.

Sage FRP Common Services-Administration

WORKGROUP - SAGEFR\KPHAM

Rights Management

Number of Roles:3 Nombre d'utilisateurs : 5

Profils Sites Utilisateurs Paramétrage Audit Système Audit Utilisateurs Database Audit Mon Compte

Drag a column header here to group by that column

Date	Heure	Catégorie	Statut	Produit	Composant	Utilisateur	Compte de l'u...	Machine	Description
10/11/2009	17:38:28	Logon	Success	UMAPI			SAGEFR\KPHAM	KPHAM2	
10/11/2009	17:40:53	Logon	Success	UMAPI			SAGEFR\KPHAM	KPHAM2	
10/11/2009	17:42:20	Logoff	Success	UMAPI			SAGEFR\KPHAM	KPHAM2	
10/11/2009	17:42:29	Logon	Success	UMAPI			SAGEFR\KPHAM	KPHAM2	
10/11/2009	17:42:32	Logoff	Success	UMAPI			SAGEFR\KPHAM	KPHAM2	
10/11/2009	17:44:47	Logoff	Success	UMAPI			SAGEFR\KPHAM	KPHAM2	
10/11/2009	17:44:58	Logon	Success	UMAPI			SAGEFR\KPHAM	KPHAM2	
10/11/2009	17:45:27	Logon	Success	UMAPI			SAGEFR\KPHAM	KPHAM2	
10/11/2009	17:47:43	Logoff	Success	UMAPI			SAGEFR\KPHAM	KPHAM2	
10/11/2009	18:37:33	Logoff	Success	XCS	Console d'Admini...		SAGEFR\KPHAM	KPHAM2	
10/11/2009	18:37:40	Logon	Success	XCS	Console d'Admini...	A	SAGEFR\KPHAM	KPHAM2	
10/11/2009	18:37:43	Logoff	Success	XCS	Console d'Admini...	A	SAGEFR\KPHAM	KPHAM2	
10/11/2009	18:38:32	Logon	Success	U2Com	XRTLogin	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	
10/11/2009	18:38:57	Logon	Success	U2	Sage FRP Treas...	A	SAGEFR\KPHAM	KPHAM2	
12/11/2009	10:04:29	Logoff	Success	XCS	Console d'Admini...		SAGEFR\KPHAM	KPHAM2	
12/11/2009	10:05:12	Logon	Success	U2	Sage FRP Treas...	A	SAGEFR\KPHAM	KPHAM2	
12/11/2009	10:12:29	Logoff	Success	XCS	Console d'Admini...		SAGEFR\KPHAM	KPHAM2	
12/11/2009	10:12:39	Logon	Success	XCS	Console d'Admini...	A	SAGEFR\KPHAM	KPHAM2	
12/11/2009	10:12:43	Logoff	Success	XCS	Console d'Admini...	A	SAGEFR\KPHAM	KPHAM2	
12/11/2009	10:13:17	Logon	Success	XCS	Console d'Admini...	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	
12/11/2009	10:14:21	Logoff	Success	XCS	Console d'Admini...	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	
12/11/2009	11:13:27	Logon	Success	U2	Sage FRP Treas...	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	
12/11/2009	11:14:40	Logon	Success	U2	Sage FRP Treas...	PHAM	pham	KPHAM2	
12/11/2009	12:11:40	Logon	Success	XCS	Console d'Admini...	PHAM	pham	KPHAM2	
12/11/2009	14:39:41	Logoff	Success	XCS	Console d'Admini...	PHAM	pham	KPHAM2	
12/11/2009	14:43:07	Logoff	Success	XCS	Console d'Admini...		SAGEFR\KPHAM	KPHAM2	
12/11/2009	14:46:05	Logon	Success	XCS	Console d'Admini...	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	
12/11/2009	14:48:19	Logoff	Success	XCS	Console d'Admini...	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	
12/11/2009	14:50:21	Logon	Success	XCS	Console d'Admini...	TEST	test	KPHAM2	
12/11/2009	14:50:48	Logoff	Success	XCS	Console d'Admini...	TEST	test	KPHAM2	
12/11/2009	14:57:31	Logon	Success	U2	Sage FRP Treas...	PHAM	pham	KPHAM2	
12/11/2009	15:20:18	Logon	Success	XCS	Console d'Admini...	PHAM	pham	KPHAM2	
12/11/2009	16:03:46	Logoff	Success	XCS	Console d'Admini...	PHAM	pham	KPHAM2	

Record 8 of 134

- **Date** and **Time** indicate the day and time of the logins/logoffs.
- **Category** indicates if the kind of connection (login or logoff).
- **Status** indicates the level of the login/logoff (here INFO).
- **Product** indicates the application.
- **Component** indicates the application's modules.
- **User** indicates the login account in xcsmcnet.
- **User's Account** indicates the account of the session in which xcsmcnet is launched or the service account on which XBE is launched.
- **Computer** indicates the name of the computer on which the user logs in or logs off.
- **Description** contains the specific messages issued by applications such as XBE. This may be useful to diagnose connection failures (e.g. OnlineBanking).

The user can filter the table lines on each column. For example, click on the top right of the User column to obtain the list of the logged users.

Sage FRP Common Services-Administration

WORKGROUP - SAGEFR\KPHAM

Rights Management

Number of Roles:3 Nombre d'utilisateurs : 5

Profils Sites Utilisateurs Paramétrage Audit Système Audit Utilisateurs Database Audit Mon Compte

Tâches liées

Accueil

Actions

Rafraîchir

Supprimer les événements and...

Drag a column header here to group by that column

Date	Heure	Statut	Utilisateur	Compte de l'utilisateur	Machine	Description
12/11/2009	10:13:48	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Création d'un utilisateur 'PHAM' (Utilisateur standard, umapiA...
12/11/2009	10:13:50	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Ajouter l'utilisateur 'PHAM' au profil 'UTILISATEURS -> isRole'
12/11/2009	10:14:07	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Autoriser l'accès au produit 'SAGE Business Exchange'
12/11/2009	14:48:03	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Création d'un utilisateur 'TEST' (Utilisateur standard, umapiA...
12/11/2009	14:48:03	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Ajouter l'utilisateur 'TEST' au profil 'UTILISATEURS -> isRole'
07/12/2009	18:26:54	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Create Role 'SIGNATAIRES' (isRole)
07/12/2009	18:27:22	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Modification d'un utilisateur 'SAGEFR\KPHAM' (Administrateur ...
09/12/2009	11:51:30	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Création d'un utilisateur 'SAGEFR\CROUART' (Administrateur ...
09/12/2009	11:51:33	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Ajouter l'utilisateur 'SAGEFR\CROUART' au profil 'ADMINISTR...
09/12/2009	12:42:59	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Autoriser l'accès au produit 'Network Management Console'
09/12/2009	12:46:55	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Autoriser l'accès au produit 'Sage FRP Treasury'
09/12/2009	14:14:10	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Autoriser l'accès au produit 'SAGE Business Exchange'

Record 1 of 12

E.g. on the **User** column, filter the lines with **SAGEFR\KPHAM** (LDAP user) as user and the following lines are displayed:

Sage FRP Common Services-Administration

WORKGROUP - SAGEFR\KPHAM

Rights Management

Number of Roles:3 Nombre d'utilisateurs : 5

Profils Sites Utilisateurs Paramétrage Audit Système Audit Utilisateurs Database Audit Mon Compte

Tâches liées

Accueil

Actions

Rafraîchir

Supprimer les événements and...

Drag a column header here to group by that column

Date	Heure	Statut	Utilisateur	Compte de l'utilisateur	Machine	Description
12/11/2009	10:13:48	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Création d'un utilisateur 'PHAM' (Utilisateur standard, umapiA...
12/11/2009	10:13:50	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Ajouter l'utilisateur 'PHAM' au profil 'UTILISATEURS -> isRole'
12/11/2009	10:14:07	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Autoriser l'accès au produit 'SAGE Business Exchange'
12/11/2009	14:48:03	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Création d'un utilisateur 'TEST' (Utilisateur standard, umapiA...
12/11/2009	14:48:03	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Ajouter l'utilisateur 'TEST' au profil 'UTILISATEURS -> isRole'
07/12/2009	18:26:54	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Create Role 'SIGNATAIRES' (isRole)
07/12/2009	18:27:22	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Modification d'un utilisateur 'SAGEFR\KPHAM' (Administrateur ...
09/12/2009	11:51:30	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Création d'un utilisateur 'SAGEFR\CROUART' (Administrateur ...
09/12/2009	11:51:33	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Ajouter l'utilisateur 'SAGEFR\CROUART' au profil 'ADMINISTR...
09/12/2009	12:42:59	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Autoriser l'accès au produit 'Network Management Console'
09/12/2009	12:46:55	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Autoriser l'accès au produit 'Sage FRP Treasur'
09/12/2009	14:14:10	Success	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	Autoriser l'accès au produit 'SAGE Business Exchange'

Record 1 of 12

The bottom row indicates the filter, here [User] = 'SAGEFR\KPHAM' or click on Edit Filter to obtain the filter combination.

The **Database Audit table** displays the SQL scripts executed during the creation or update of databases.

Rights Management
 Nombre de Rôles : 1 Nombre d'utilisateurs : 3

Profils | Sites | Utilisateurs | Paramétrage | Audit Système | Audit Utilisateurs | Database Audit | Mon Compte

Drag a column header here to group by that column

Date	Time	Workgroup	Product	User Account	Computer	Status	Description
22/12/2010	14:41:55	WORKGROUP9	Sage FRP Tre...	SAGEFR\pgham	KPHAM2	Success	L'exécution du script updateuser2005.sql est ...
22/12/2010	14:41:53	WORKGROUP9	Sage FRP Tre...	SAGEFR\pgham	KPHAM2	Success	L'exécution du script updatedbo2005.sql est e...
22/12/2010	14:41:52	WORKGROUP9	Sage FRP Tre...	SAGEFR\pgham	KPHAM2	Success	L'exécution du script registerlogicalunits.sql es...
22/12/2010	14:41:41	WORKGROUP9	Sage FRP Tre...	SAGEFR\pgham	KPHAM2	Success	L'exécution du script updateuser2005.sql est ...
22/12/2010	14:41:40	WORKGROUP9	Sage FRP Tre...	SAGEFR\pgham	KPHAM2	Success	L'exécution du script updatedbo2005.sql est e...
22/12/2010	14:41:38	WORKGROUP9	Sage FRP Tre...	SAGEFR\pgham	KPHAM2	Success	L'exécution du script registerlogicalunits.sql es...
16/12/2010	10:40:43	WORKGROUP9	Sage FRP Tre...	SAGEFR\KPHAM	KPHAM2	Success	The script updateuser2005.sql is being execut...
16/12/2010	10:40:41	WORKGROUP9	Sage FRP Tre...	SAGEFR\KPHAM	KPHAM2	Success	The script updatedbo2005.sql is being execut...
16/12/2010	10:40:39	WORKGROUP9	Sage FRP Tre...	SAGEFR\KPHAM	KPHAM2	Success	The script registerlogicalunits.sql is being exec...
16/12/2010	10:40:27	WORKGROUP9	Sage FRP Tre...	SAGEFR\KPHAM	KPHAM2	Success	The script bcp_03_14_updatemodel.sql is bein...
16/12/2010	10:40:27	WORKGROUP9	Sage FRP Tre...	SAGEFR\KPHAM	KPHAM2	Success	The script registerlogicalunits.sql is being exec...
16/12/2010	10:40:26	WORKGROUP9	Sage FRP Tre...	SAGEFR\KPHAM	KPHAM2	Success	The script creatextl_configuration.sql is being ...
16/12/2010	10:40:26	WORKGROUP9	Sage FRP Tre...	SAGEFR\KPHAM	KPHAM2	Success	The script updateuser2005.sql is being execut...
16/12/2010	10:40:24	WORKGROUP9	Sage FRP Tre...	SAGEFR\KPHAM	KPHAM2	Success	The script updatedbo2005.sql is being executed.
16/12/2010	10:39:37	WORKGROUP9	Sage FRP Com...	SAGEFR\KPHAM	KPHAM2	Success	The script updateuser2005.sql is being execut...
16/12/2010	10:39:36	WORKGROUP9	Sage FRP Com...	SAGEFR\KPHAM	KPHAM2	Success	The script updatedbo2005.sql is being execut...

Script : updateuser2005.sql Taille : 2080 Interpréteur : SqlCmd.exe Fournisseur DB : SQLNCLI Version Serveur : 09.00.4053 Source de Données : SRVFR-MSSQL3

Script execution log Script source

Message
 ErrorNumber ErrorMessage

15023 User, group, or role 'XRT_USERS' already exists in the current database.
 (1 lignes affectées)
 Changed database context to 'master'.
 The process sqlcmd.exe exited with code 0

- **Date and Time:** when a specific SQL script was executed.
- **Workgroup:** the Workgroup on which the Database was created or updated.
- **Status:** the login/logoff level (here INFO).
- **Product:** the application name.
- **User Account:** the account of the session in which xcsmcnet is launched or the service account on which XBE is launched.
- **Computer:** the station on which the database was created or updated.
- **Status:** whether the SQL script has been successful or not.
- **Description:** list of all SQL scripts executed.

Deleting/exporting System/User Audit Events and Database

Like all event types (Windows or applicative), the user can manually delete old events or export towards an xml file in order not to saturate the event monitor of XCS application.

Sage FRP Common Services-Administration

WORKGROUP - SAGEFR\KPHAM

Rights Management

Number of Roles:3 Nombre d'utilisateurs : 5

Profils | Sites | Utilisateurs | Paramétrage | Audit Système | Audit Utilisateurs | Database Audit | Mon Compte

Tâches liées

Accueil

Actions

Rafraîchir

Supprimer les événements and...

Drag a column header here to group by that column

Date	Heure	Catégorie	Statut	Produit	Composant	Utilisateur	Compte de l'u...	Machine	Description
10/11/2009	17:38:28	Logon	Success	UMAPI			SAGEFR\KPHAM	KPHAM2	
10/11/2009	17:40:53	Logon	Success	UMAPI			SAGEFR\KPHAM	KPHAM2	
10/11/2009	17:42:20	Logoff	Success	UMAPI			SAGEFR\KPHAM	KPHAM2	
10/11/2009	17:42:29	Logon	Success	UMAPI			SAGEFR\KPHAM	KPHAM2	
10/11/2009	17:42:32	Logoff	Success	UMAPI			SAGEFR\KPHAM	KPHAM2	
10/11/2009	17:44:47	Logoff	Success	UMAPI			SAGEFR\KPHAM	KPHAM2	
10/11/2009	17:44:58	Logon	Success	UMAPI			SAGEFR\KPHAM	KPHAM2	
10/11/2009	17:45:27	Logon	Success	UMAPI			SAGEFR\KPHAM	KPHAM2	
10/11/2009	17:47:43	Logoff	Success	UMAPI			SAGEFR\KPHAM	KPHAM2	
10/11/2009	18:37:33	Logoff	Success	XCS	Console d'Admini...		SAGEFR\KPHAM	KPHAM2	
10/11/2009	18:37:40	Logon	Success	XCS	Console d'Admini...	A	SAGEFR\KPHAM	KPHAM2	
10/11/2009	18:37:43	Logoff	Success	XCS	Console d'Admini...	A	SAGEFR\KPHAM	KPHAM2	
10/11/2009	18:38:32	Logon	Success	U2Com	XRTLogin	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	
10/11/2009	18:38:57	Logon	Success	U2	Sage FRP Treas...	A	SAGEFR\KPHAM	KPHAM2	
12/11/2009	10:04:29	Logoff	Success	XCS	Console d'Admini...		SAGEFR\KPHAM	KPHAM2	
12/11/2009	10:05:12	Logon	Success	U2	Sage FRP Treas...	A	SAGEFR\KPHAM	KPHAM2	
12/11/2009	10:12:29	Logoff	Success	XCS	Console d'Admini...		SAGEFR\KPHAM	KPHAM2	
12/11/2009	10:12:39	Logon	Success	XCS	Console d'Admini...	A	SAGEFR\KPHAM	KPHAM2	
12/11/2009	10:12:43	Logoff	Success	XCS	Console d'Admini...	A	SAGEFR\KPHAM	KPHAM2	
12/11/2009	10:13:17	Logon	Success	XCS	Console d'Admini...	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	
12/11/2009	10:14:21	Logoff	Success	XCS	Console d'Admini...	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	
12/11/2009	11:13:27	Logon	Success	U2	Sage FRP Treas...	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	
12/11/2009	11:14:40	Logon	Success	U2	Sage FRP Treas...	PHAM	pham	KPHAM2	
12/11/2009	12:11:40	Logon	Success	XCS	Console d'Admini...	PHAM	pham	KPHAM2	
12/11/2009	14:39:41	Logoff	Success	XCS	Console d'Admini...	PHAM	pham	KPHAM2	
12/11/2009	14:43:07	Logoff	Success	XCS	Console d'Admini...		SAGEFR\KPHAM	KPHAM2	
12/11/2009	14:46:05	Logon	Success	XCS	Console d'Admini...	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	
12/11/2009	14:48:19	Logoff	Success	XCS	Console d'Admini...	SAGEFR\KPHAM	SAGEFR\KPHAM	KPHAM2	
12/11/2009	14:50:21	Logon	Success	XCS	Console d'Admini...	TEST	test	KPHAM2	
12/11/2009	14:50:48	Logoff	Success	XCS	Console d'Admini...	TEST	test	KPHAM2	
12/11/2009	14:57:31	Logon	Success	U2	Sage FRP Treas...	PHAM	pham	KPHAM2	
12/11/2009	15:20:18	Logon	Success	XCS	Console d'Admini...	PHAM	pham	KPHAM2	
12/11/2009	16:03:46	Logoff	Success	XCS	Console d'Admini...	PHAM	pham	KPHAM2	

Record 8 of 134

To do so, select the action: **Delete old events** and the following window opens:

Supprimer/exporter les événements anciens de l'audit Users

Supprimer les événements anciens de l'audit Users

antérieurs à : jeudi 12 novembre 21 (14 enregistrements seront supprimés)

☐ Souhaitez-vous une sauvegarde des enregistrements d'audit à supprimer ?

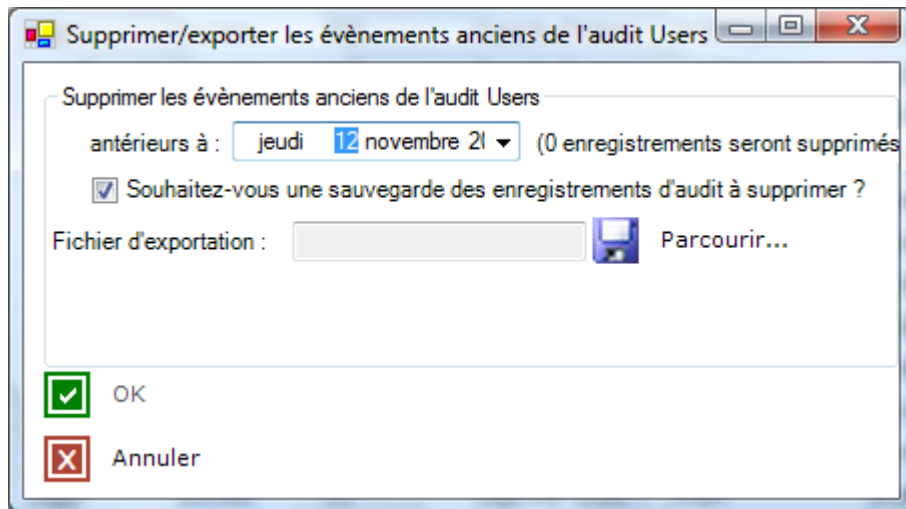
Fichier d'exportation : Parcourir...

☒ OK

☐ Annuler

Select a date in the calendar (here November 12, 2009). Depending on the date, the number of events to delete is indicated on the right.

Or save them in an xml file:



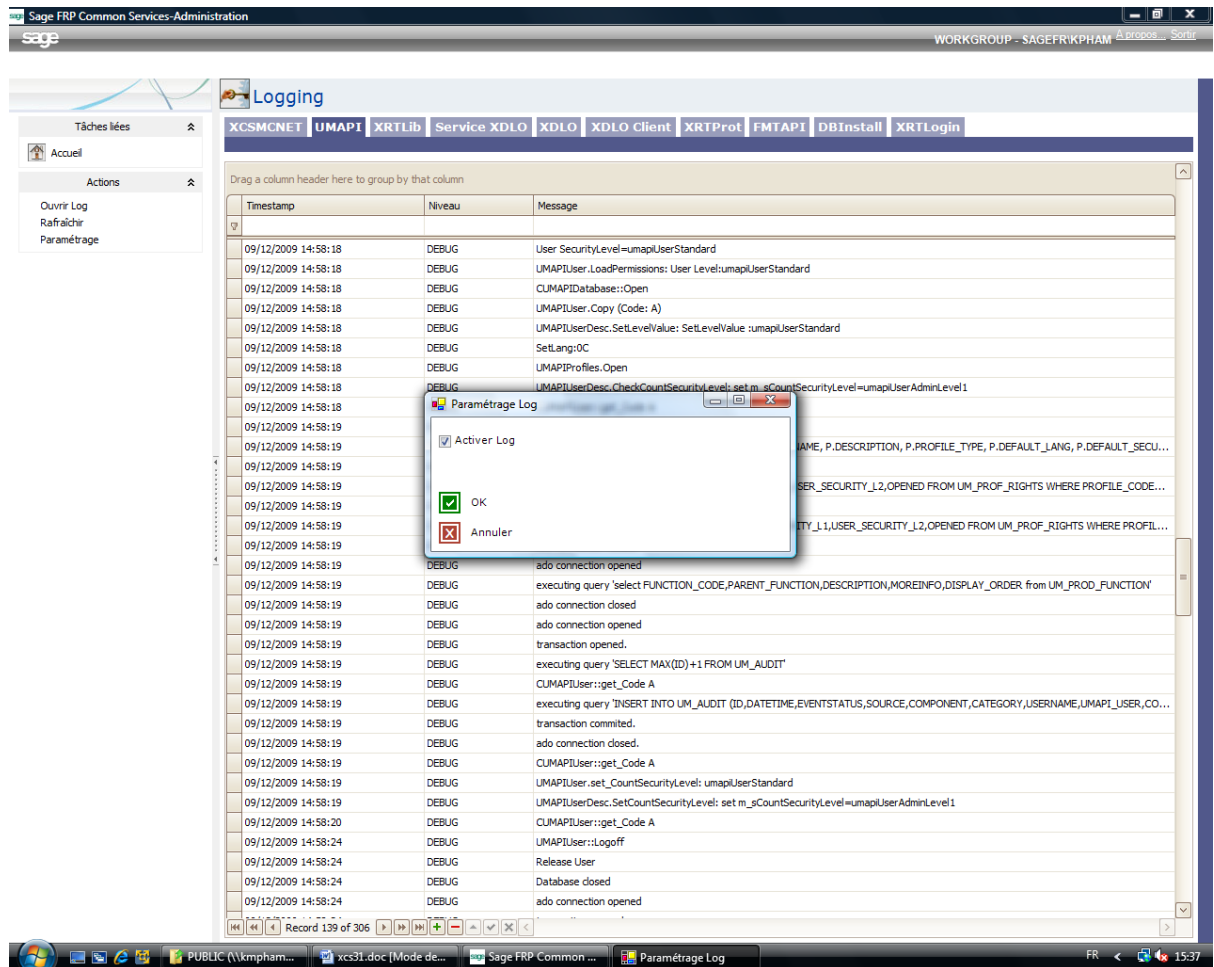
- Select "**Do you want to backup Audit records you are deleting?**" with the entered date.
- Click on the disk button or **Browse...**
- Select the path as well as the file to be exported (without extension).
- Click **OK**.

6 Traces

When Sage FRP Common Services is started, trace files for the DbInstaller and the Administration Console or XRTLogin are systematically generated and enabled.

For other components such as XDLO service, XDLO, Client XDLO, XRTLlib or FMTAPI and XRTProt, trace files can be enabled:

- Either from the Administration Console interface, **Connection** menu and **Setup** action for each component. (for eg.: here the UMAPI log setup)



Select **Enable logging** and click Ok.

- Or create manually in the registry a key and a Debug string for each component in **HKEY_LOCAL_MACHINE\SOFTWARE\XRT\Common**. Here is the key list:

UMAPI -----> **Debug string = Y**

XDLO -----> **Debug string = Y** (for XDLO service and XDLO)

DebugRC string = Y (for XDLO CLIENT)

XRTLlib -----> **Debug string = Y**

APIFMT -----> **Debug string = Y**

XRTProt -----> **Debug string = Y**

These trace files are stored by default under **C:\Documents and settings\nom machine\Application Data\XRT\XCS**. Here is the list of the trace file names corresponding to each component:

DbInst.log	-----> Db Insaller component
Xcsmcnet.log	-----> Administration Console component
UmapiLib.log	-----> UMAPI component
Xdlo_remclient.log	-----> CLIENT XDLO component
XrtLib.log	-----> XRTLIB component (useful to diagnose DSN connections between Sage applications, for eg. between SBE and XCS)
ApiFmt.log	-----> FORMATS module
XrtProt	-----> License component

Concerning XDLO Service and XDLO, the **Xdlo_service.log** and **Xdlo.log** trace files are stored under **C:\ Documents and settings\Local Service\Application Data\XRT\XCS**. The user can view the Local Service folder only if the "Hide protected operating system files" option is selected in Windows display options.

Trace tables enable the step-by-step display of the actions executed by each component. They consist of the following elements:

The screenshot displays the 'Logging' window in Sage FRP Common Services-Administration. The window has a sidebar with 'Tâches liées' (Accueil, Actions) and 'Actions' (Ouvrir Log, Rafraîchir, Paramétrage). The main area shows a table of log entries. The table has columns: Timestamp, Niveau, and Message. The log entries are filtered by the 'Service XDLO' component. The 'Timestamp' column shows dates from 09/12/2009 14:58:18 to 14:58:24. The 'Niveau' column shows 'DEBUG'. The 'Message' column contains various system events such as 'User SecurityLevel=umapiUserStandard', 'UMAPIUser.LoadPermissions: User Level:umapiUserStandard', 'CLMAPIDatabase::Open', 'UMAPIUser.Copy (Code: A)', 'UMAPIUserDesc.SetLevelValue: SetLevelValue :umapiUserStandard', 'SetLang:0C', 'UMAPIProfiles.Open', 'UMAPIUserDesc.CheckCountSecurityLevel: set m_sCountSecurityLevel=umapiUserAdminLevel1', 'CLMAPUser::get_Code A', 'ado connection opened', 'executing query 'SELECT P.PROFILE_CODE, P.PROFILE_NAME, P.DESCRPTION, P.PROFILE_TYPE, P.DEFAULT_LANG, P.DEFAULT_SECU...', 'ado connection closed', 'Query='SELECT FUNCTION_CODE,USER_SECURITY_L1,USER_SECURITY_L2,OPENED FROM UM_PROF_RIGHTS WHERE PROFILE_CODE...', 'ado connection opened', 'executing query 'SELECT FUNCTION_CODE,USER_SECURITY_L1,USER_SECURITY_L2,OPENED FROM UM_PROF_RIGHTS WHERE PROFIL...', 'ado connection closed', 'ado connection opened', 'executing query 'select FUNCTION_CODE,PARENT_FUNCTION,DESCRIPTION,MOREINFO,DISPLAY_ORDER from UM_PROD_FUNCTION'', 'ado connection closed', 'ado connection opened', 'transaction opened.', 'executing query 'SELECT MAX(ID)+1 FROM UM_AUDIT'', 'CLMAPUser::get_Code A', 'executing query 'INSERT INTO UM_AUDIT (ID, DATETIME, EVENTSTATUS, SOURCE, COMPONENT, CATEGORY, USERNAME, UMAP1_USER, CO...', 'transaction committed.', 'ado connection closed.', 'CLMAPUser::get_Code A', 'UMAPIUser.set_CountSecurityLevel: umapiUserStandard', 'UMAPIUserDesc.SetCountSecurityLevel: set m_sCountSecurityLevel=umapiUserAdminLevel1', 'CLMAPUser::get_Code A', 'UMAPIUser::Logout', 'Release User', 'Database closed', 'ado connection opened'.

- **Timestamp** indicates date and time.

- **Level** indicates the message type. These types are mainly: "ALL", "INFO", "DEBUG" and "ERROR".
- **Message** means the actions developed and executed by the components, here UMAPI.

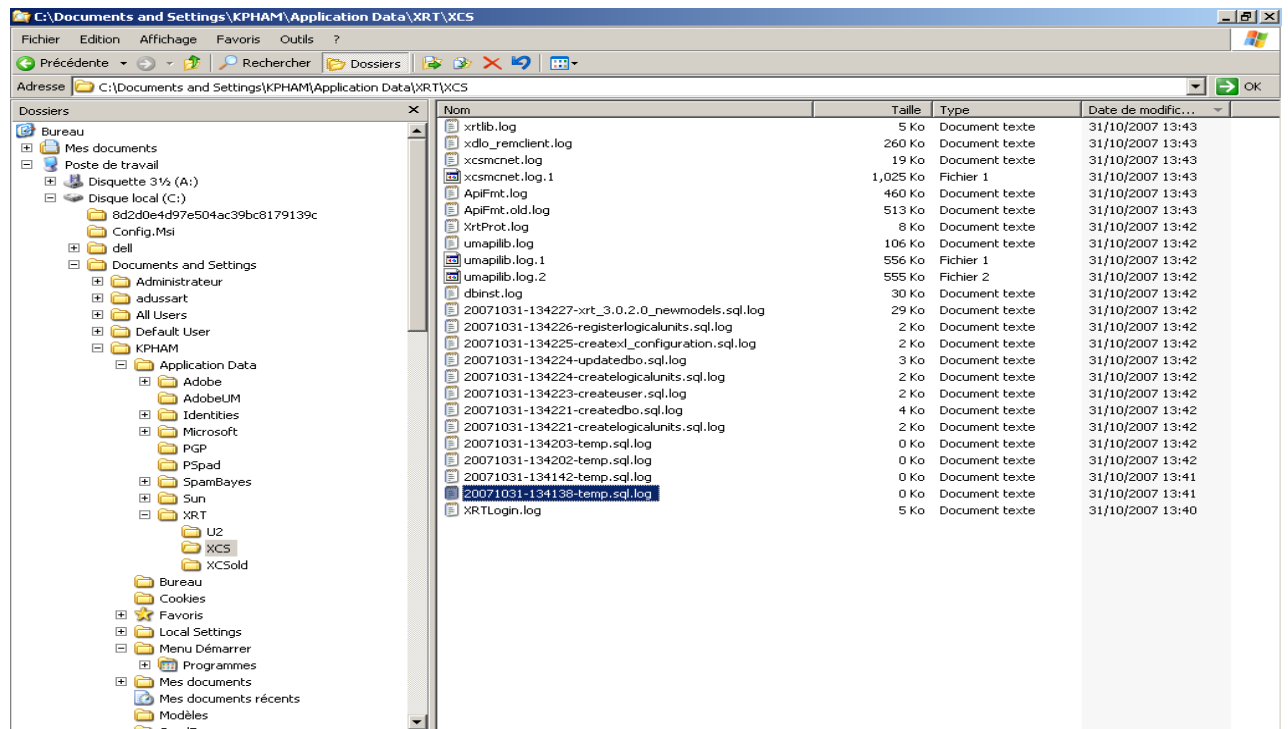
These tables work in the same way as the audit management. You can sort and filter lines by column element. For example, to display the UMAPI trace with the DEBUG level, click on the top right of the LEVEL column to obtain the list of all levels.

Select the "DEBUG" level and you will get all the lines for it.

For more information, see paragraph 5.4.1.1.

Trace files are generated by computer and date.

Let us have a look at the trace files generated when creating a database. They are located in the same place as the other trace files, under **C:\Documents and settings\nom machine\Application Data\XRT\XCS**. You can recognize their ".sql" extension. Since the execution order of scripts is important, they are sorted by execution order in the file. For example, concerning the creation of a XCS database in Oracle, here are the generated script files:



- 20071031-134203-temp.sql.log
- 20071031-134221-createlogicalunits.sql.log
- 20071031-134221-createdbo.sql.log
- 20071031-134223-createuser.sql.log
- 20071031-134224-createlogicalunits.sql.log
- 20071031-134224-updatedbo.sql.log
- 20071031-134225-createxl_configuration.sql.log
- 20071031-134226-registerlogicalunits.sql.log
- 20071031-134227-xrt_3.0.2.0_newmodels.sql.log

You need to open each script to know the execution details.

The same procedure is used to create/update FRP Treasury and SBE applications.



7 Formats

Formats represent the financial flows existing between financial institutions and companies. Generally speaking, they are divided into several categories:

Company -----> Bank (payments)

- Domestic Transfers
- Commercial Transfers
- International Transfers
- Treasury Transfers
- Direct Debits
- Cheques
- Drafts

Bank -----> Company

- Account Statements
- Acknowledgements and Reports
- Documentary Credits

An unlimited number of bank file standards exist, but the following are the most used by Sage applications:

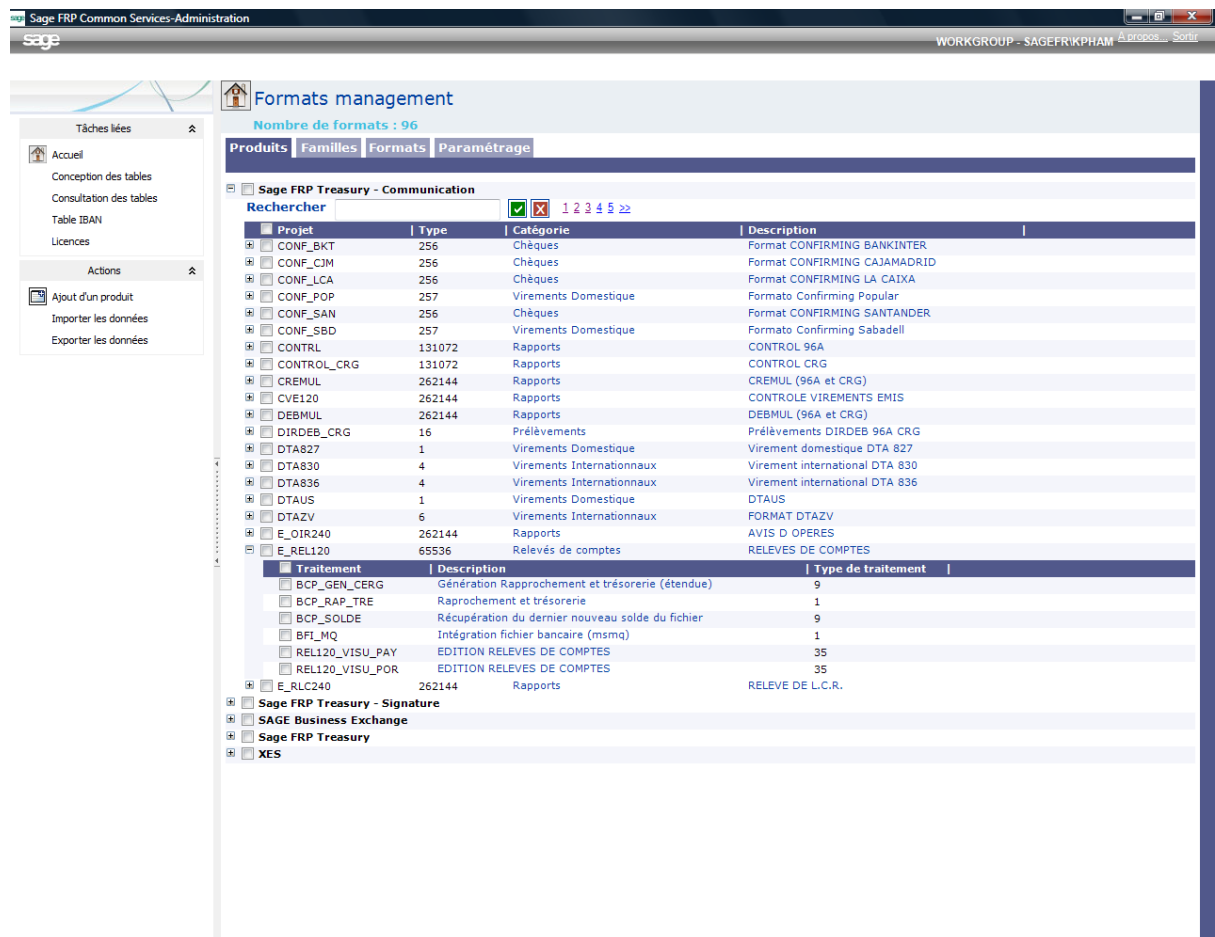
- **AFB** (CFONB): AFB_160, AFB_160_DIRDEB, AFB_160_DRAFT, AFB_320, AFB_320_DOM, RRE_240, E_REL120, E_OIR240, E_RLC240
- **SWIFT** (Belgian): MT101, MT100, MT102, MT103, CIRI128, MT940, MT941, MT942, CODA, MT700_707, MT700_707_AR, MT300, MT199, MT299, MT500...
- **EDIFACT**: PAYMUL, PAYORD, PAYEXT, DIRDEB_CRG, BDF_912d, BDF_93AI, BANSTA, CONTROL, FINSTA, CREMUL, DEBMUL, FINSTA_INTRADAY
- **Spanish**: AEB_19, AEB_19_DEV, AEB_32, AEB_32_DEV, AEB_34, AEB_34_1, AEB_43, AEB_58, AEB_58_DEV, AEB_RCF, AEB_68, AEB_100, AEB_57, JUZGADOS, TINBBVA, AEB_67...
- **German**: DTAUS, DTAZV, DTAUS_DIRDEB, CLIEOP_DIRDEB, CLIEOP_DOM
- **Italian**: CBI_PC, CBI_RH, CBI_IB, CBI_IR
- **Portuguese**: PS2, PSC
- **Swiss**: DTA827, DTA830_836, OPAE
- **American**: BAI2
- **Proprietary**: VIRCOM_400, ACA560, ACH, AOI160, ALPHA, ALPHABOR/LCR, GAMMA, CVE120, APERAK, I_RELNAT, RCP120, RFT320, SETIF, SG_QUAND, SG_QUOI, SIT, TEXT80
- **IDOC**
- **SEPA**: SCT and SDD

Important To manage the creation of SDD and SCT formats in FRP Treasury Payment or SBE Payment Web, you must install Java runtime, delivered along with XCS common services setup: "jre-6u17-windows-i586-s.exe".

For better exploitation, these formats are organized in treeviews:

- At the root level, there are the products: **FRP Communication** and **Sage Business Exchange** which gather all view and integration processing of bank files, **FRP Signature** which gathers all view and control processing of bank files, **FRP Treasury** and **Sage Business Exchange** which gather all generation processing of bank files (payments).
- Under the root, there are projects corresponding to the key words for format names which you can physically find under: **C:\Program Files\Fichiers communs\xrt\Product** of XCS installation where all Clint scripts are stored.
- Under the projects, there is the clint **processing** which enables the execution of a certain number of processes.

Example of process: BCP_GEN_CERG, generating the extended form of E_REL120 account statement.



Sage FRP Common Services-Administration

WORKGROUP - SAGEFRKPHAM

Formats management
Nombre de formats : 96

Produits | Familles | Formats | Paramétrage

Sage FRP Treasury - Communication

Rechercher

Projet	Type	Catégorie	Description
CONF_BKT	256	Chèques	Format CONFIRMING BANKINTER
CONF_CJM	256	Chèques	Format CONFIRMING CAJAMADRID
CONF_LCA	256	Chèques	Format CONFIRMING LA CAIXA
CONF_POP	257	Virements Domestique	Formato Confirming Popular
CONF_SAN	256	Chèques	Format CONFIRMING SANTANDER
CONF_SBD	257	Virements Domestique	Formato Confirming Sabadell
CONTRL	131072	Rapports	CONTROL 96A
CONTROL_CRG	131072	Rapports	CONTROL CRG
CREMUL	262144	Rapports	CREMUL (96A et CRG)
CVE120	262144	Rapports	CONTROLE VIREMENTS EMIS
DEBMUL	262144	Rapports	DEBMUL (96A et CRG)
DIRDEB_CRG	16	Prélèvements	Prélèvements DIRDEB 96A CRG
DTA827	1	Virements Domestique	Virement domestique DTA 827
DTA830	4	Virements Internationaux	Virement international DTA 830
DTA836	4	Virements Internationaux	Virement international DTA 836
DTAUS	1	Virements Domestique	DTAUS
DTAZV	6	Virements Internationaux	FORMAT DTAZV
E_OIR240	262144	Rapports	AVIS D OPERES
E_REL120	65536	Relevés de comptes	RELEVES DE COMPTES

Traitement	Description	Type de traitement
BCP_GEN_CERG	Génération Rapprochement et trésorerie (étendue)	9
BCP_RAP_TRE	Rapprochement et trésorerie	1
BCP_SOLDE	Récupération du dernier nouveau solde du fichier	9
BFI_MQ	Intégration fichier bancaire (msmq)	1
REL120_VISU_PAY	EDITION RELEVES DE COMPTES	35
REL120_VISU_POR	EDITION RELEVES DE COMPTES	35
E_RLC240	Rapports	RELEVÉ DE L.C.R.

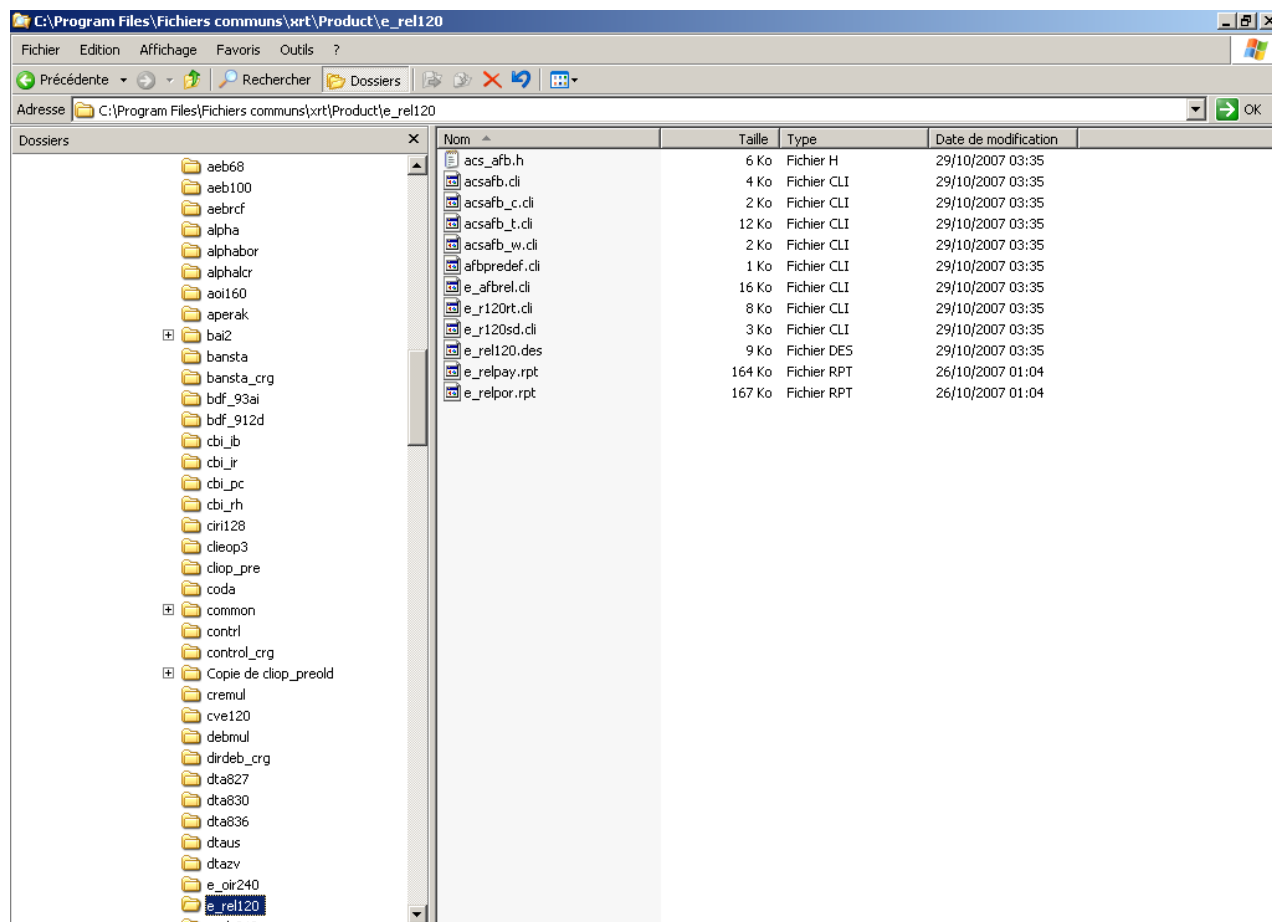
Sage FRP Treasury - Signature

SAGE Business Exchange

Sage FRP Treasury

XES

BCP_GEN_CERG process belongs to project E_REL120 which belongs to Sage FRP Communication.



This project must be located under **C:\Program Files\Fichiers communs\xrt\Product\e_rel120** where the clint scripts of the statement are stored, and particularly the acsafb.cli script which enables the execution of the BCP_GEN_CERG processing.

Sage FRP Common Services-Administration

WORKGROUP - SAGEFRWPHAM

Formats management

Nombre de formats : 96

Produits | Familles | Formats | Paramétrage

Sage FRP Treasury - Communication

Rechercher

Projet	Type	Catégorie	Description
CONF_BKT	256	Chèques	Format CONFIRMING BANKINTER
CONF_CJM	256	Chèques	Format CONFIRMING CAJAMADRID
CONF_LCA	256	Chèques	Format CONFIRMING LA CAIXA
CONF_POP	257	Virements Domestique	Formato Confirming Popular
CONF_SAN	256	Chèques	Format CONFIRMING SANTANDER
CONF_SBD	257	Virements Domestique	Formato Confirming Sabadell
CONTRL	131072	Rapports	CONTROL 96A
CONTROL_CRG	131072	Rapports	CONTROL CRG
CREMUL	262144	Rapports	CREMUL (96A et CRG)
CVE120	262144	Rapports	CONTROLE VIREMENTS EMIS
DEBMUL	262144	Rapports	DEBMUL (96A et CRG)
DIRDEB_CRG	16	Prélèvements	Prélèvements DIRDEB 96A CRG
DTA827	1	Virements Domestique	Virement domestique DTA 827
DTA830	4	Virements Internationaux	Virement international DTA 830
DTA836	4	Virements Internationaux	Virement international DTA 836
DTAUS	1	Virements Domestique	DTAUS
DTAZV	6	Virements Internationaux	FORMAT DTAZV
E_OIR240	262144	Rapports	AVIS D OPERES
E_REL120	65536	Relevés de comptes	RELEVES DE COMPTES

Traitement	Description	Type de traitement
BCP_GEN_CERG	Génération Rapprochement et trésorerie (étendue)	9
Suppression d'un traitement	Suppression d'un traitement	1
Modification d'un traitement	Modification d'un traitement	9
Intégration Bancaire	Intégration Bancaire	1
Détails du processus	Détails du processus	35
E_f	Relevés de comptes	35
Sage FRP Treasury - Signature	Signature	RELEVÉ DE L.C.R.
SAGE Business Exchange	SAGE Business Exchange	
Sage FRP Treasury	Sage FRP Treasury	
XES	XES	

Through the interface, you can recognize the clint script which is called to execute this processing by selecting "**Process details**".

Sage FRP Common Services-Administration

WORKGROUP - SAGEFRKPHAM 6 pages - Sage

Formats management

Nombre de formats : 96

Produits | Familles | **Formats** | Paramétrage

Sage FRP Treasury - Communication

Rechercher

Projet	Type	Catégorie	Description
CONF_BKT	256	Chèques	Format CONFIRMING BANKINTER
CONF_CJM	256	Chèques	Format CONFIRMING CAJAMADRID
CONF_LCA	256	Chèques	Format CONFIRMING LA CAIXA
CONF_POP	257	Virements Domestique	Formato Confirming Popular
CONF_SAN	256	Chèques	Format CONFIRMING SANTANDER
CONF_SBD	257	Virements Domestique	Formato Confirming Sabadell
CONTRL	131072	Rapports	CONTROL 96A
CONTROL_CRG	131072	Rapports	CONTROL CRG
CREMUL	262144	Rapports	CREMUL (96A et CRG)
CVE120	262144	Rapports	CONTROLE VIREMENTS EMIS
DEBMUL	262144	Rapports	DEBMUL (96A et CRG)
DIRDEB_CRG	16	Prélèvements	Prélèvements DIRDEB 96A CRG
DTA827	1	Virements Domestique	Virement domestique DTA 827
DTA830	4	Virements Internationaux	Virement international DTA 830
DTA836	4	Virements Internationaux	Virement international DTA 836
DTAUS	1	Virements Domestique	DTAUS
DTAZV	6	Virements Internationaux	FORMAT DTAZV
E_OIR240	262144	Rapports	AVIS D OPERES
E_REL120	65536	Relevés de comptes	RELEVES DE COMPTES
E_RLC240	262144	Rapports	RELEVÉ DE L.C.R.

Traitement

Traitement	Description	Type de traitement
BCP_GEN_CERG	Génération Rapprochement et trésorerie (étendue)	9
BCP_RAP_TRE	Rapprochement et trésorerie	1
BCP_SOLDE	Récupération du dernier nouveau solde du fichier	9
BFI_MQ	Intégration fichier bancaire (msmq)	1
REL120_VISU_PAY	EDITION RELEVES DE COMPTES	35
REL120_VISU_POR	EDITION RELEVES DE COMPTES	35

Sage FRP Treasury - Signature

SAGE Business Exchange

Sage FRP Treasury

XES

Détails du traitement BCP_GEN_CERG

Description : Génération Rapprochement trésorerie (étendue)

Exécutable : CLINT.EXE

Type de traitement :

- ☐ Exécution asynchrone du traitement
- ☒ Redirection de la sortie de l'exécutable
- ☐ Exécution asynchrone des tâches du
- ☐ Paramètres identiques à toutes les t
- ☐ Traitement permettant de visualiser
- ☐ Vue permettant la gestion des pouvo

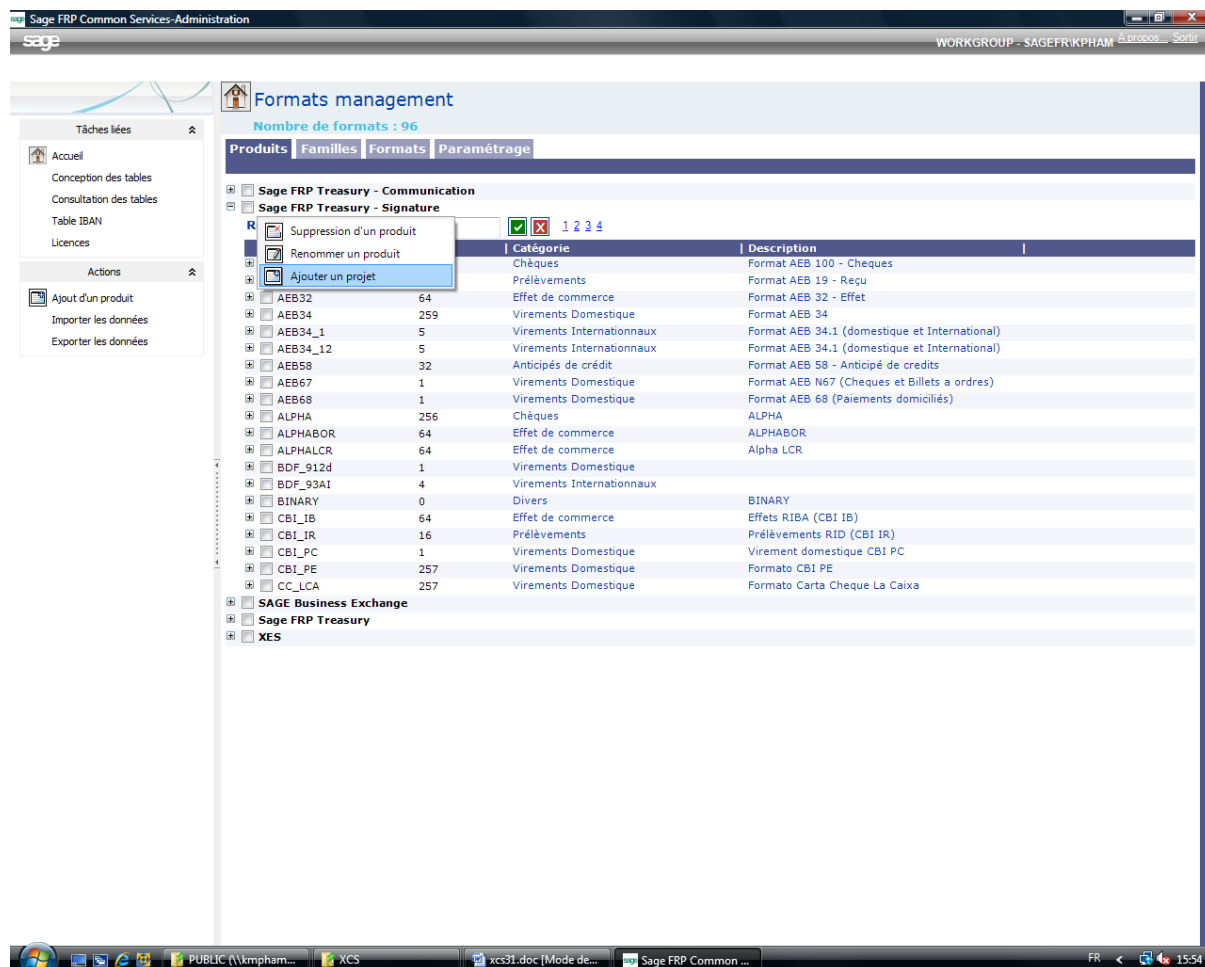
Liste des tâches :

acsafb cli

Acсаfb.cli appears in the task list.

You will be able to manually add a specific product or project and a specific processing according to the client's needs by following the process:

(In our example, we create a project and a processing under Sage FRP Signature by taking the same clint scripts of the VIR_160 project)



Select Add Project in Sage FRP Signature. The following screen is displayed:

Ajout d'un projet au produit XRT Signature

Nom: VIR

Description: Démonstration d'intégration d'un projet dans la gestion des formats

Catégorie: Virements Domestique

Format: SPECIFIC

Type: 1

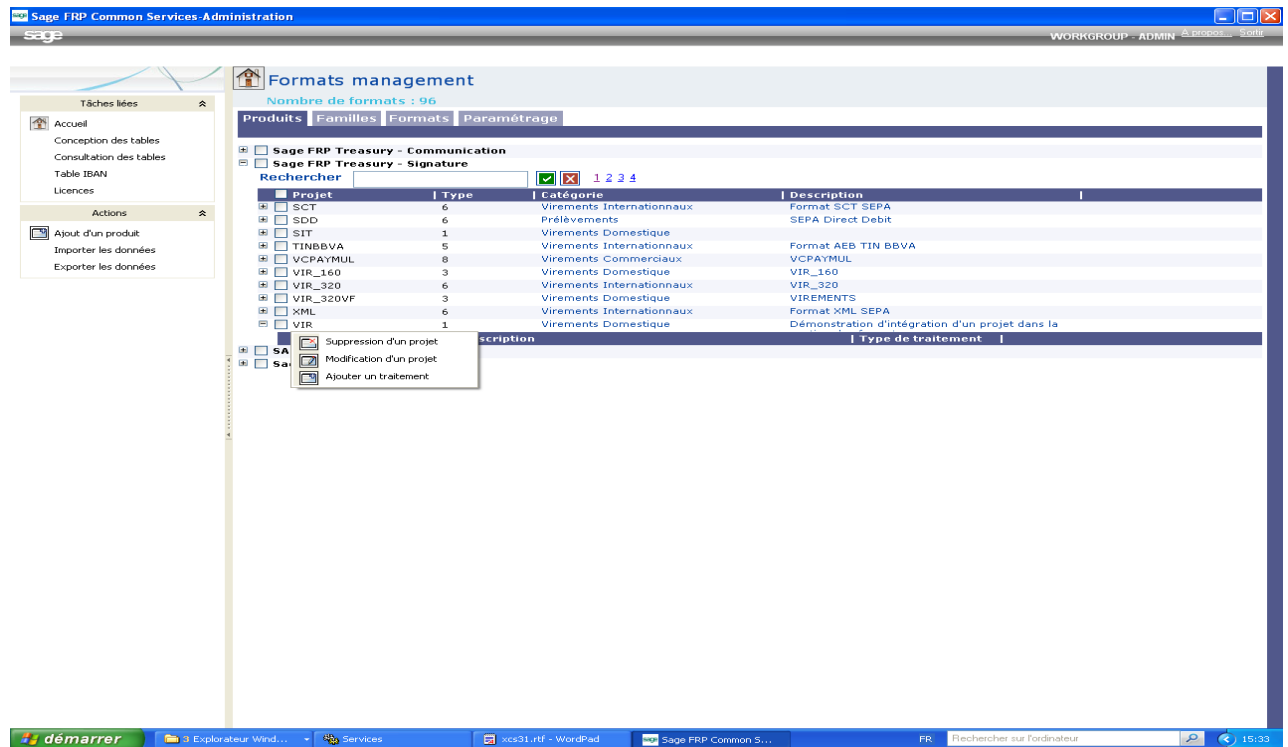
☒ OK ☐ Annuler

Type de projet

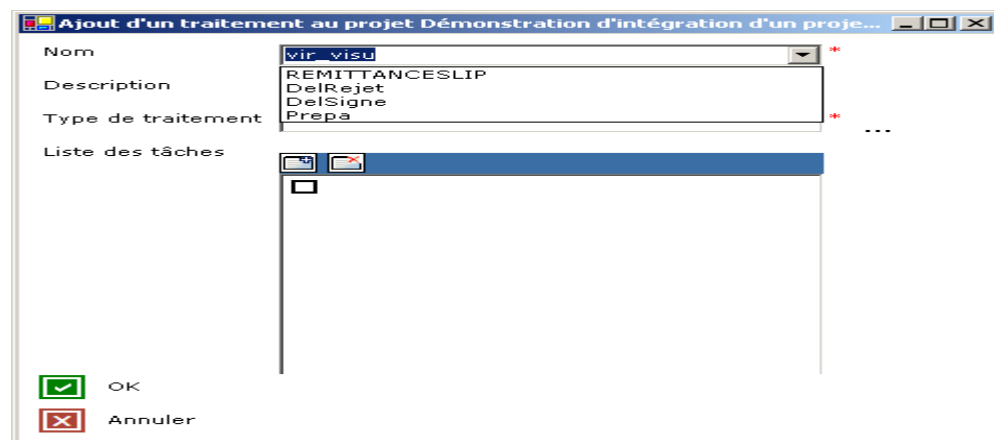
- ☒ Virement domestique
- ☐ Virement de trésorerie
- ☐ Virement international
- ☐ Virement commercial
- ☐ Prélèvement domestique
- ☐ Anticipé de crédit
- ☐ Effet
- ☐ Lettre de crédit
- ☐ Chèques
- ☐ Relevé de compte

- Enter project name (here VIR).
- Enter the description.
- In the list, select the category or family (here Domestic Transfer).
- In the list, select the format (here SPECIFIC).
- Select the project type (here Domestic Transfer converted into "1").
- OK.

The user can see the "VIR" project under Sage FRP Signature and needs to add a processing under this project.



Select Add Process. The following screen is displayed:



Ajout d'un traitement au projet Démonstration d'intégration d'un projet dans la gestion des formats

Nom: *

Description:

Type de traitement: *

Liste des tâches:

- ☐

Type de traitement

- ☒ Exécution asynchrone du traitement
- ☒ Redirection de la sortie de l'exécutable
- ☒ Exécution asynchrone des tâches du traitement
- ☐ Paramètres identiques à toutes les tâches
- ☒ Traitement permettant de visualiser un fichier
- ☒ Vue permettant la gestion des pouvoirs bancaire

☒ OK ☐ Annuler

Modification d'un traitement

Modification du traitement vir_visu

Description:

Type de traitement: *

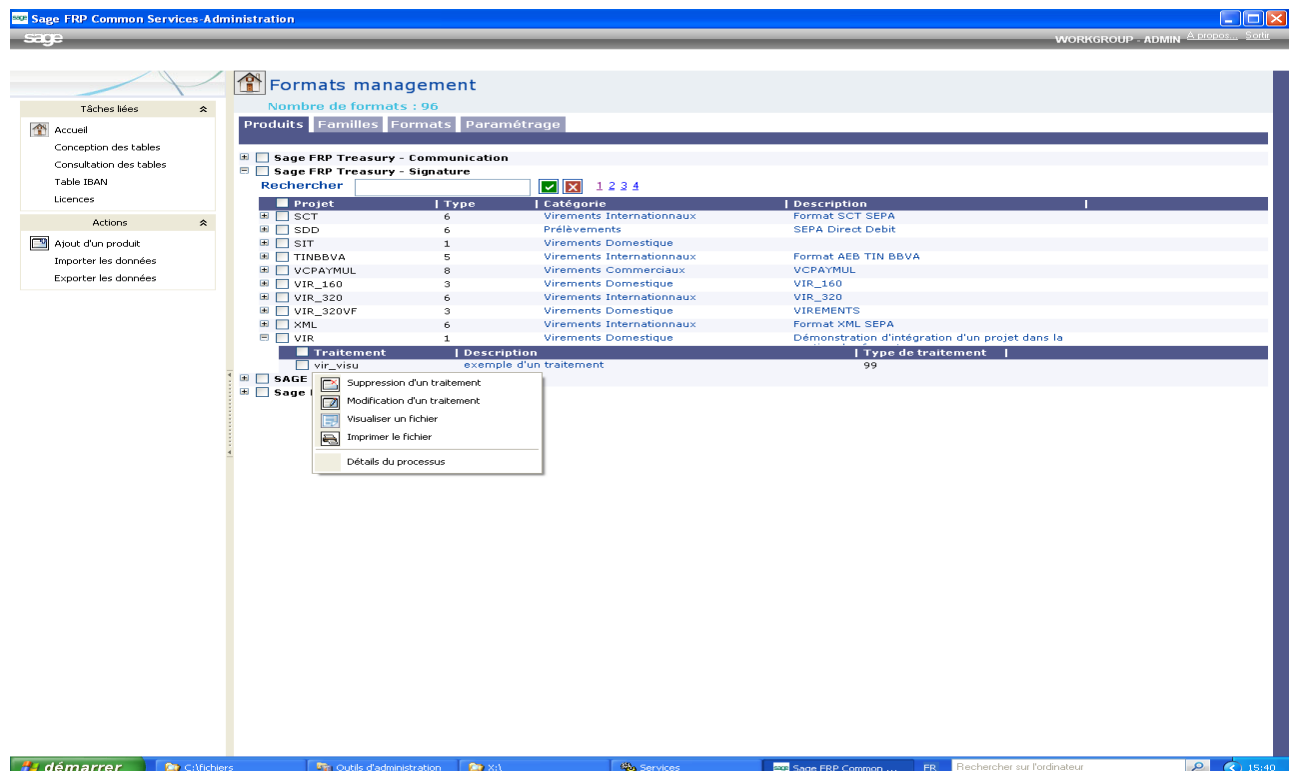
Liste des tâches:

- ☐ afb_vir.cli vir_por.rpt

☒ OK ☐ Annuler

- Enter a processing name if no default Signature processing in the list corresponds to the required processing (here vir_visu).
- Enter the description.
- Select processing types or enter a number (for Signature viewing processing, it is highly recommended to take the same value as the other default viewing processing, i.e. it is an asynchronous execution of process and process tasks, the executable output is redirected, and the processing enables the view and management of bank powers, here 99).
- In the task list, enter the clint scripts that are supposed to be launched (here afb_vir.cli and vir_por.rpt).
- OK.

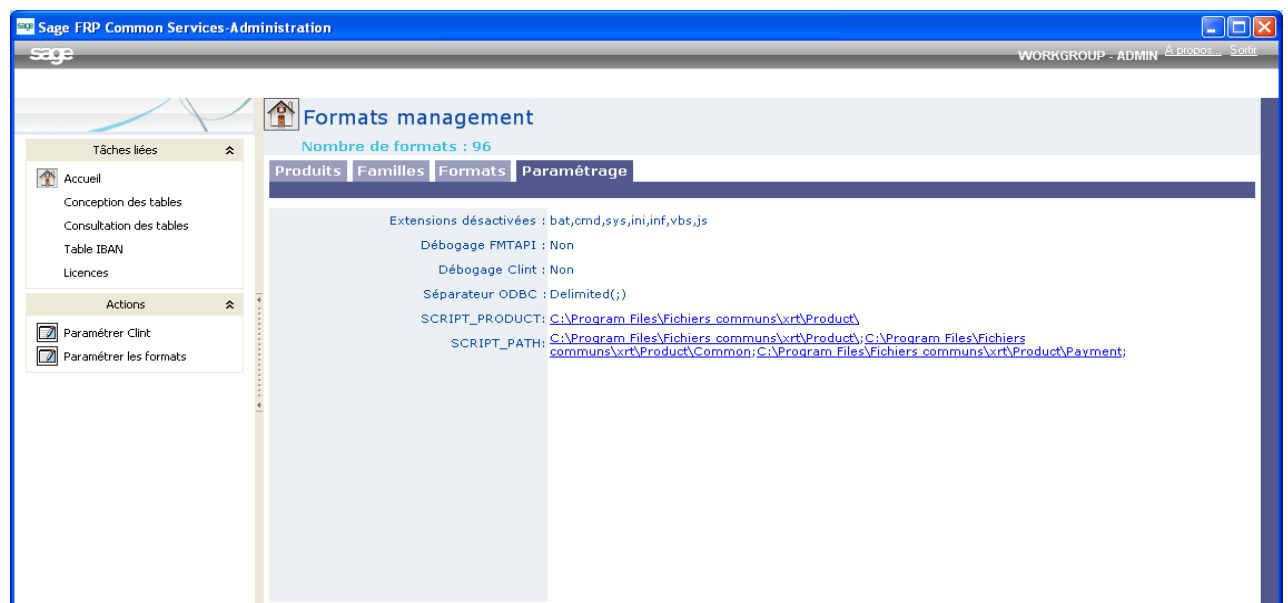
The "vir_visu" processing is then associated to the "VIR" project with the potential task: "View File".



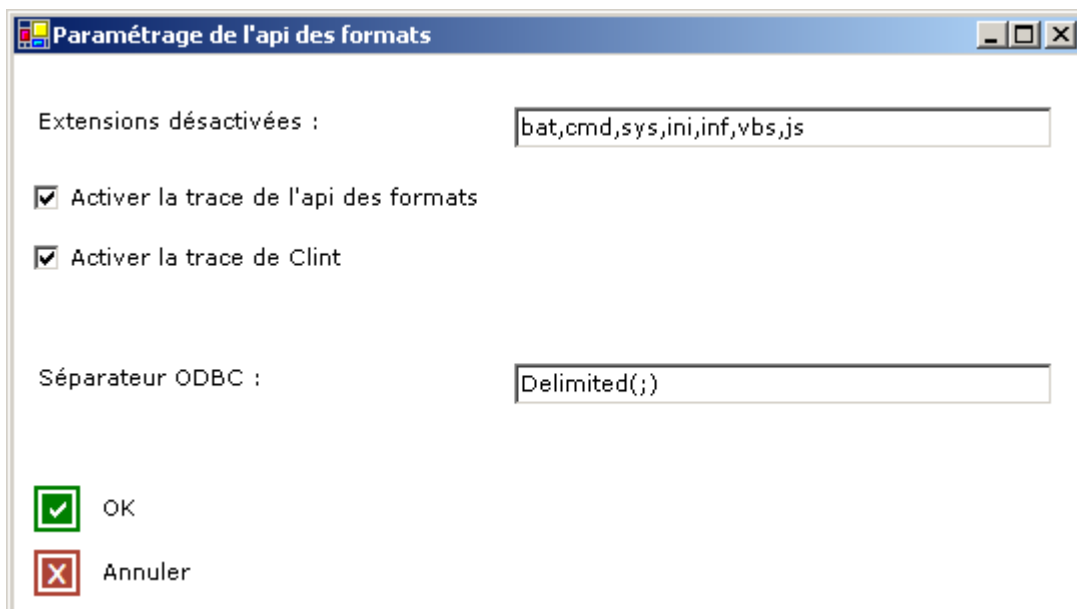
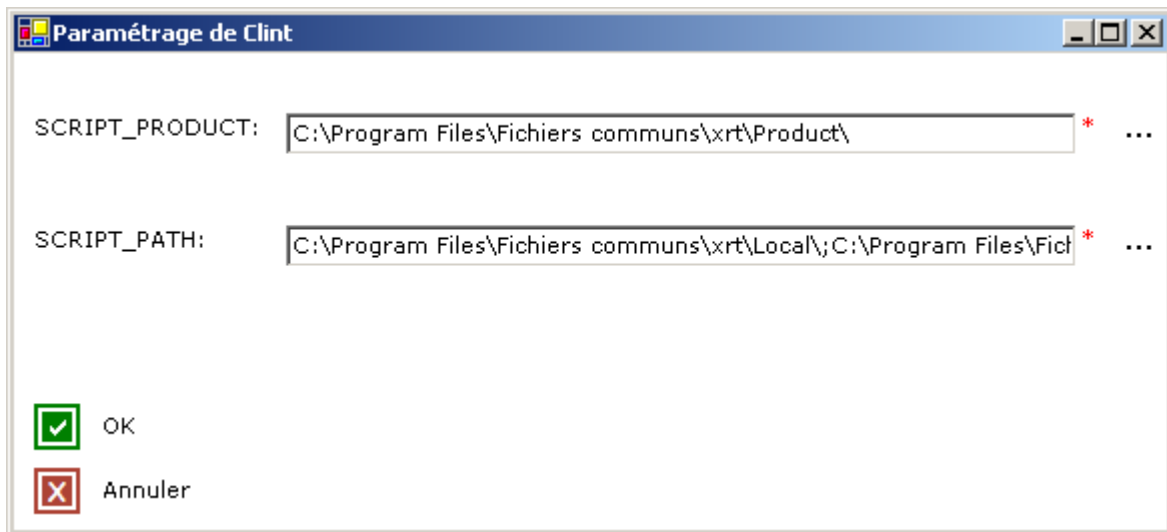
The user can view a file under this processing only if the clint scripts have been created under the directory: **C:\Program Files\Fichiers communs\xrt\Product\vir**.

Importing a format under an xml file is a second way to add processing, project or product in the formats management. The structure of the xml file needs to comply with the default one. You can also find the "apifmt.xml" which was initially imported when installing XCS under **C:\Program Files\Fichiers communs\xrt\DBMS\import\fr**.

Settings of formats configuration



Select the **"Set Up Clint"** or **"Set Up Formats"** action and the following screens appear:



- Upon installation, clint scripts are installed and stored in the registry under **SCRIPT_PATH, SCRIPT_PRODUCT** variables of **HKEY_LOCAL_MACHINE\SOFTWARE\XRT\CLINT\SETTING**, which indicate the installation path.
- Enable **Clint** and **formats Api** tracing by selecting them.
- As the **Disabled Extensions** and **ODBC Separator** settings are both settings of ODBC pilots, here is a reminder on how Clint exchanges data with Crystal Report or another programming tool. Clint uses the temporary text files belonging to the type Microsoft driver text for the exchange. Crystal Report or another programming tool reads these data through the ODBC CERG_TXT data source. These files extensions are defined by default " *.* " in the registry variables:
HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBCINST.INI\Microsoft Text Driver or
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Jet\4.0\Engines\Text for Clint 1.8.
However Clint does not function for any type of extension. You need to specify the non-authorized extensions, and that is the reason for the "DisabledExtensions" variable.

Let us have a look at data contained in these temporary files. By default, these data are separated by ";" in the file. However in specific configurations, the separator does not function. This raises, in the interface, the possibility to change separators, and that is the reason for "ODBC Separator".



8 Transcoding Tables

8.1 Introduction

Transcoding tables are used to establish correspondences between format codes and standard codes. They can also be specifically used by certain format. For example, to set up script behavior.

8.2 General Tables

8.2.a "CurrencyDecimals" Table

It provides the decimal number according to the currency. The input column of the table shows the iso code of the currency and the output column shows the number of decimals.

Data Example:

CURRENCY	DECIMALS
EUR	2

8.2.b "RIBs" Table

This table enables the setup of descriptions for account numbers. It is used for viewings. It is automatically fed. Every time a new account number appears, it is added to the RIBs table. The input column of the table shows the account number and the output column shows the description of the account.

A particular behavior has been implemented for P5. By providing the formats api with a DSN, this behavior prompts it to retrieve descriptions in the CPTE table of P5. If no description is found in the CPTE table, then the one from the RIBs table is chosen.

Data Example:

ACCOUNT	DESCRIPTION
300040072500020023 961	Account of Mr SMITH

8.2.c "GenerationNumbers" Table

This table enables the numbering of the files generated in one day. The number of generations made during the day is kept in this table. This table is used by 96A and CH PAYMUL. It is also used by MT101 CAI format to number the remittances generated in the day.

This table consists of two input columns (format and family) and two output columns (day of the year and generation number for one day).

Data Example:

FORMAT	FAMILY	DAYOFYEAR	COUNTER
PAYMUL96ACRG	INTT	125	12

8.2.d "RIB_DESC" Table

This table enables the description of the account number composition according to the country. It is used when generating bank files, to split Account ID into bank code, branch code, account number and key. This table consists of one input column (country code of the account number) and eight output columns (bank code position, bank code length, branch code position, branch code length, account number position, account number length, key position, key length).

Data Example:

COUNTRY	BANK_POS	BANK_LEN	DOM_POS	DOM_LEN	ACC_POS	ACC_LEN	KEY_POS	KEY_LEN
FR	0	5	5	5	10	11	21	2

8.3 "AFB320_PARAM", the AFB 320 Table

It is used when Universe payment, P5 or U2 generate AFB 320 bank files. It enables the setup of amount types and account number types according to the bank code. This table consists in two input columns "CODE_BANK", "PARAMETER" and one output column "VALUE".

Note that for Sage FRP Treasury, this table is a retrieve table set up through Sage FRP Treasury interface and located in the "pafb320.dat" file.

The value of the bank code can be "DEFAULT".

8.3.a Setting up Amount Type

Here are the available values:

"T", the amount in the transfer currency.

"D", the amount in the currency of the debit account.

"L" is equivalent to "D" if the transfer currency equals the currency of the debit account; is equivalent to "T" if the transfer currency differs from the currency of the debit account.

Data Example:

CODE_BANK	PARAMETER	VALUE
DEFAULT	MONTANT	T

8.3.b Setting up Account Number Type

Here are the accounts that can be set up:

- Debit Account "DEBIT"
- Credit Account "CREDIT"
- Disbursement Account "FRAIS"

Here are the available values:

- "LOCAL", the format of the account number is local
- "BBAN", the format of the account number is BBAN
- "IBAN", the format of the account number is IBAN

Data Example:

CODE_BANK	PARAMETER	VALUE
30003	DEBIT	IBAN

The default value of the account number type depends on the subformat code and therefore on the executed script. For AFB 320 generation, three scripts are available:

- cfpa320.cli, the account number type is local
- cfpa320a.cli, the account number type is IBAN
- cfpa320b.cli, the account number type is BBAN

8.4 "PAYEXT96A_PARAM", the PAYEXT 96A Table

It is used when Universe payment, P5 or U3 generate PAYEXT 96A bank files. It enables the setup of the EDIFACT "NAD" and "RFF" segments' generation according to the bank code. This table consists of two input columns "BANK", "SEGMENT" and one output column "VALUE".

Note that for Sage FRP Treasury, this table is a btrieve table set up through Sage FRP Treasury interface and located in the "VCOM96_A.dat" file.

The value of the bank code can be "DEFAULT".

8.4.a Setting up the Structure of NAD Segments

Here are the NAD segments that you can set up: "NADBE", "NADPE", "NADPL" and "NADOY".

The available values are: "STRUCTURE" and "NON STRUCTURE". The default value is "STRUCTURE".

Data Example:

BANK	SEGMENT	VALUE
30004	NADOY	NON STRUCTURE

8.4.b Setting up RFF Segment

RFZ2 is the only segment that can be set up. The value is the client reference. If this segment is not set up in the correspondence table, it is not generated in the bank file.

Data Example:

BANK	SEGMENT	VALUE
30003	RFFZ2	123456789

8.5 "ascaebbdv.dat", the LAEB 43 Table

It is used during the integration of AEB 43 bank files. It establishes the correspondence between AEB currency codes and ISO currency codes. This table consists of one input column (AEB currency codes) and one output column (ISO currency codes).

Data Example:

CODE	ISO
978	EUR

8.6 AFB 120 Tables

8.6.a "ACSAFBVDV.DAT" Table

It is used during the integration of AFB 120 bank files. It establishes the correspondence between AFB currency codes and ISO currency codes according to the bank codes. This table consists of two input columns (bank code and AFB currency code) and one output column (ISO currency code).

The value for the bank code as well as for the currency code can be "DEFAULT".

Data Example:

BANK	CURRENCY_CODE	CURRENCY
DEFAULT	BLANK	EUR

8.6.b "ACSAFBPA.DAT" Table

This table is used for the integration of AFB 120 bank files. It enables or disables controls on the records sequence and on final balances, according to bank codes. This table consists of one input column (the bank to process, it is the argument provided in command line for integration processing) and one output column (the value "O" or "N" depending on whether controls are enabled or not). Controls are enabled by default.

The value of the bank to process can be "DEFAULT".

Data Example:

KEY	VALUE
30003	O

8.6.c "ACSAFBVE.DAT" Table

It is used when integrating AFB 120 and FINSTA 96A bank files. This table indicates the exchange rate of each currency against Euro. This table consists of one input column (ISO currency codes) and one output column (exchange rate against Euro).

Data Example:

CURRENCY	RATE
FRF	6,55957

8.6.d "AFB120RT_PARAM" Table

It is used during the integration of AFB120 bank files. This table has a "PARAMETER" input column and a "VALUE" output column. The "PARAMETER" field can have one of the two values: "05TRE" or "05RAP". Both values respectively represent records of additional information for Treasury or Reconciliation. The "VALUE" field has the "Y" or "N" value depending on whether the user wants to delete the records of additional information or not.

Data Example:

PARAMETER	VALUE
05TRE	Y

8.7 FINSTA 96A Tables

8.7.a "acsfinstapa.dat" Table

It is used when integrating FINSTA 96A bank files. It allows enabling or disabling controls according to bank codes. This table consists of two input columns (bank code and control to perform) and one output column ("Y" or "N" values depending on whether controls are enabled or not). Controls are disabled by default. The only available is the final balance control. To enable it, you need to enter the "CHK_BALANCE" value in the second input column.

The value of the bank code can be "DEFAULT".

Data Example:

BANK	PARAMETER	VALUE
DEFAULT	CHK_BALANCE	Y

8.7.b "ACSAFBVE.DAT" Table

It is used when integrating FINSTA 96A bank files. This table is shared with the AFB 120.

8.8 "ACSMT_OP.DAT", the MT 940 Table

It is used when integrating MT 940 bank files. It establishes the correspondence between MT 940 transaction type and transaction code (AFB standard). This table consists of one input column (transaction type) and one output column (AFB transaction code).

Data Example:

KEY	XRT_CODE
MSC	91

8.9 "MT101CAI_PARAM", the MT101 CAI Table

It is used when Universe payment, P5 or U2 generate MT101 CAI bank files. It enables the setup of the generation of header block 4, a reference at the level of tag 20 and a counter at the level of tag 21, according to the branch and the company. This table consists of three input columns "PARAMETER", "AGENCY", "COMPANY" and one output column "VALUE".

For P5, the company is not the company code contained in the remittance reference but the applicant description.

Note that for Universe, this table is a btrieve table set up through Sage FRP Treasury interface and located in the "ParMT101.dat" file.

The "AGENCY" and "COMPANY" input columns can have "DEFAULT" as key value.

8.9.a Setting up Header Generation (Block 4)

The value of the "PARAMETER" column must be "HEADER". For each branch and company, you can set up the "Y" or "N" values depending on whether you want to manage block 4 or not.

Data example for the "CAI" branch and the "UCI" company:

PARAMETER	AGENCY	COMPANY	VALUE
HEADER	CAI	UCI	N

8.9.b Setting up "Identifiant Telecom" (Tag 20)

The value for the "PARAMETER" column must be "ID". For each branch and company, you can set up the CAI "Identifiant Telecom".

Data example for the "CAI" branch and the "UCI" company:

PARAMETER	AGENCY	COMPANY	VALUE
ID	CAI	UCI	IC0065TQ

8.9.c Setting up Tag 21

The MT101CAI_PARAM table is also used to count the number of generated tags 21. The use of the table is transparent to the user. Records, in which the "PARAMETER" column, will equal "CPT", will be automatically created in this table. The counter is in base 36.

Data Example:

PARAMETER	AGENCY	COMPANY	VALUE
CPT	CAI	UCI	0001A

8.10 "MT101SG_PARAM", the MT101 SG Table

It is used when Universe payment, P5 or U2 generate MT101 SG bank files. It enables the setup of a reference at the level of tag 20. This table has a "PARAMETER" input column and a "VALUE" output column.

Note that for Universe, this table is a btrieve table set up through Sage FRP Treasury interface and located in the "ETB1SOG.dat" file.

8.10.a Setting up "Identifiant Telecom" (Tag 20)

The value for the "PARAMETER" column must be "ID". You can then set up the "identifiant télécom".

Data Example:

PARAMETER	VALUE
ID	IC0065TQ

8.11 CODA Tables

8.11.a Isobbl Table

It is used when integrating CODA bank files. It establishes the correspondence between BBL currency codes and ISO currency codes. This table consists of one input column (BBL currency code) and one output column (ISO currency code).

Data Example:

KEY	VALUE
955	FRF

8.11.b convcib Table

It is used when integrating CODA bank files. It establishes correspondence between CODA transaction code and AFB transaction code. This table consists of one input column (CODA transaction code) and one output column (AFB transaction code).

Data Example:

OPE_CODA	OPE_AFB
123	456

8.11.c RES_CPT Table

It is used when integrating CODA bank files. It enables the setup of restrictions at the header level according to the account number (the remittance is rejected). This table consists of one input column (account number) and one output column (a non empty string to specify the restriction).

Data Example:

KEY	VALUE
30004123451234567890 1	Y

8.11.d RES_DEV Table

It is used when integrating CODA bank files. It enables the setup of restrictions at the header level according to the account currency (the remittance is rejected). This table consists of one input column (BBL currency code) and one output column (a non empty string to specify the restriction).

Data Example:

KEY	VALUE
30003	Y

8.11.e RES_COD Table

It is used when integrating CODA bank files. It enables the setup of restrictions at the header level according to the transaction code (the remittance is rejected). This table consists of one input column (transaction code) and one output column (a non empty string to specify the restriction).

Example of data:

KEY	VALUE
-----	-------

123	Y
-----	---

8.11.f RES_MES Table

It is used when integrating CODA bank files. It enables the setup of restrictions at the details level according to the message or the record description (the record is rejected if the message corresponds to the entry form entered in the table). The "like" SQL command is used to establish the correspondence. This table consists of one input column (message or form) and one output column (a non empty string to specify the restriction).

Example of data:

KEY	VALUE
Message	Y

8.12 "PAYORD91.2_PARAM", the PAYORD 91.2 Table

It is used when Universe payment, P5 or U2 generate PAYORD 91.2 bank files. It enables the setup of the SIRET number of the UNB segment according to the bank code. This table consists in two input columns "CODE_BANK", "PARAMETER" and one output column "VALUE".

8.12.a Setting up SIRET Number

The PARAMETER column must be equal to "UNB_SIRET". This parameter is the only one to be taken into account by the scripts of PAYORD 91.2 bank files generation. A SIRET number can be set up for several bank codes.

The value of the bank code can be "DEFAULT".

Example of data:

CODE_BANK	PARAMETER	VALUE
DEFAULT	UNB_SIRET	75480071200012
30004	UNB_SIRET	31417225500015

8.13 "PAY_CRLF" Table

It is used when Universe payment, P5 or U2 generate bank files. It enables the setup of the CRLF type to use for generation according to the format. This table consists of one input column "FORMAT" and one output column "OUTPUT".

8.13.a Setting up CRLF Type

The values for the OUTPUT column can be: NOCRLF, LF, CRLF or CRCRLF. In these cases the characters used to separate records are respectively: none, "0A", "0D0A" and "0D0D0A". (hexadecimal ascii code of characters)

Example of data:

FORMAT	OUTPUT
AFB320	NOCRLF
CBI_PC	LF
AEB_19	CRLF

8.14 "BAI2_PARAM", the BAI2 Table

It is used when integrating BAI2 bank files. It enables the setup of the execution for certain processing according to the bank code. This table consists of one input column "CODE_BANK" and three output columns "RTRIM", "CHECK" and "TYPE".

8.14.a Setting up RTRIM process

Some banks complete their records with blanks, so that the length of all records is 80 bytes. In this case we first need to process the file in order to delete these blank characters. This process is enabled by default. For good performance reasons, it will be interesting to disable it when it is not necessary. The available values are: "1" to enable it, and "0" to disable it.

The value of the bank code can be "DEFAULT".

8.14.b Controlling File Integrity

Some banks can provide files which do not comply with BAI2 standard. However these files are valid and must be executed. Therefore you need to disable the file integrity control. This process is enabled by default. The available values are: "1" to enable it, and "0" to disable it.

8.14.c Setting up Reference Type

Clients can look up specific information such as account numbers, control numbers, in the reference column. This reference must be the bank reference or the client reference according to the involved bank. This table allows consultants to choose the reference type to use. The available values are "1" for the use of the bank reference column and "0" for the use of the client reference column.

Example of data:

CODE_BANK	RTRIM	CHECK	TYPE
DEFAULT	1	1	0
30004	0	1	1

8.15 "CALENDAR" Table

It is used when integrating BAI2 bank files. It enables the storage of calendars used to set up worked days of a year. This table consists of one input column ("NAME") and one output column ("VALUE").

8.15.a Format of "VALUE" Column

The first 6 figures represent the start date of the calendar. (number of days as of January 1, 1970). The following 244 bytes stand for the base-64-encoded 366 days of the year. Each day (encoded on 4 bytes) can combine the following values: day worked (value 0), non-working day (value 1), fixed bank holiday (value 2), variable bank holiday (value 4) and holidays (value 8). To create calendars, see the readme file of the BAI2 "calendar.cli" script.

Example of data:

NAME	VALUE
Bank2005	012784TAAAEAAAEBIAARAAAQEAAA...

8.16 "COUNTRY_CURRENCY" Table

It allows retrieving a country currency; which helps determining whether the transfer is domestic or international, through a comparison between the transfer currency and the country currency. This table consists of one input column "COUNTRY" and one output column "CURRENCY".

Example of data:

COUNTRY	CURRENCY
FR	EUR

8.17 "PAYMUL96A_PARAM" Table

This table is used in the script of payment generation for PAYMUL 96A Belron. It enables the setup of a script behavior. Remittance breaking down or not according to transfer type. This table consists of one input column ("PARTNER" which is the SIRET of the applicant branch) and one output column ("SPLIT" which can have Yes or No value to authorize breaking down or not).

Example of data:

PARTNER	SPLIT
66204244900014	Yes

8.18 "SWIFT_NET" Table

This table is used in the script of SWIFT payment generation. (MT 100, 101, 102, 103) It enables the setup of a script behavior. Generation - or not - of blocks 1, 2 and 3. (PARAM_KEY = "BUILDHEADER") Setup of the type of certification wanted (PARAM_KEY = "URGENT" or "NORMAL") This table consists of three input columns "FORMAT", "CODE_BANK" et "PARAM_KEY". "FORMAT" is the type of flow. (MT100, MT101, etc...), CODE_BANK is the issuer bank code et "PARAM_KEY" is the parameter type. Three values are available for PARAM_KEY: "BUILDHEADER", "URGENT" and "NORMAL". The value for the first two entry columns can be "DEFAULT". In this case, the setup is applied to all flows or banks. The "OUTPUT" field can have one of the two values: "Yes" or "No" for "BUILDHEADER" parameter (generation - or not - of blocks 1, 2 and 3. It can be "1" or "3" for the parameter "URGENT" (warning for non-delivery "1" or warning for non-delivery and delivery

certifications "3"). It can be "BLANK" or "2" for the parameter "NORMAL". (delivery certifications "2" or nothing "BLANK"). In case of incorrect setup, the default values are "3" for "URGENT" and "BLANK" for "NORMAL".

Example of data:

FORMAT	CODE_BANK	PARAM_KEY	OUTPUT
MT103	DEFAULT	BUILDHEADER	No
MT101	30998	BUILDHEADER	Yes
DEFAULT	DEFAULT	URGENT	3
DEFAULT	DEFAULT	NORMAL	BLANK
MT101	DEFAULT	NORMAL	2

8.19 MT101 Fortis Table

This table is used in the script of payment generation for Fortis MT101 formats. It enables the setup of a script behavior. Setup of the contractual data used to fill up the headers of the file and of blocks 1 and 2. This table has two input columns "PARAM_ID" and "CODE_BANK". PARAM_ID, is the parameter name. The managed parameters are the following: CLIENT_NAME, INPUT_TYPE, FEEDBACK_TYPE and MIR_SEQ_NR. CODE_BANK is the issuer bank code. The value for this input column can be DEFAULT. In this case, the setup is applied to all banks. The OUTPUT column value can be the parameter value.

Example of data:

PARAM_ID	CODE_BANK	OUTPUT
CLIENT_NAME	DEFAULT	01XRTTST
FEEDBACK_TYPE	DEFAULT	AH
INPUT_TYPE	30998	XRTMT101
MIR_SEQ_NT	30004	000000

8.20 DORMANTS_ACCOUNTS Table

This table is used in the scripts to view the account statements. It enables to set up the behavior of the viewing, i. e. the possibility to display (or not) the accounts with no transactions. This table has an input column, "FORMAT". "FORMAT" is the type of flow. Now, five values are managed in this column: "AEB43", "CBI_RH", "E_REL120", "I_RELNAT" and "MT940". They correspond to the five account statement formats managing the accounts with no transactions in the formats api. The value for this input column can be DEFAULT. In this case, the setup is applied to all flows. The "OUTPUT" column can take the value "Yes" or "No". (display, or not, of the accounts with no transactions).

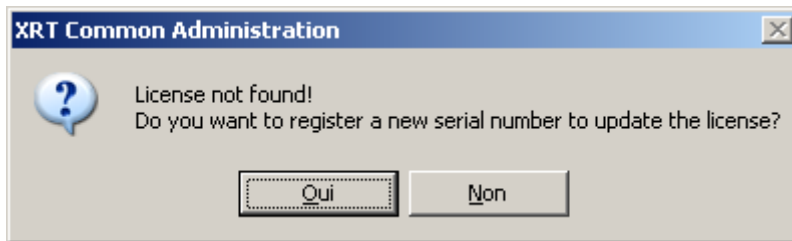
Example of data:

FORMAT	OUTPUT
AEB43	No
MT940	Yes
E_REL120	No
DEFAULT	Yes

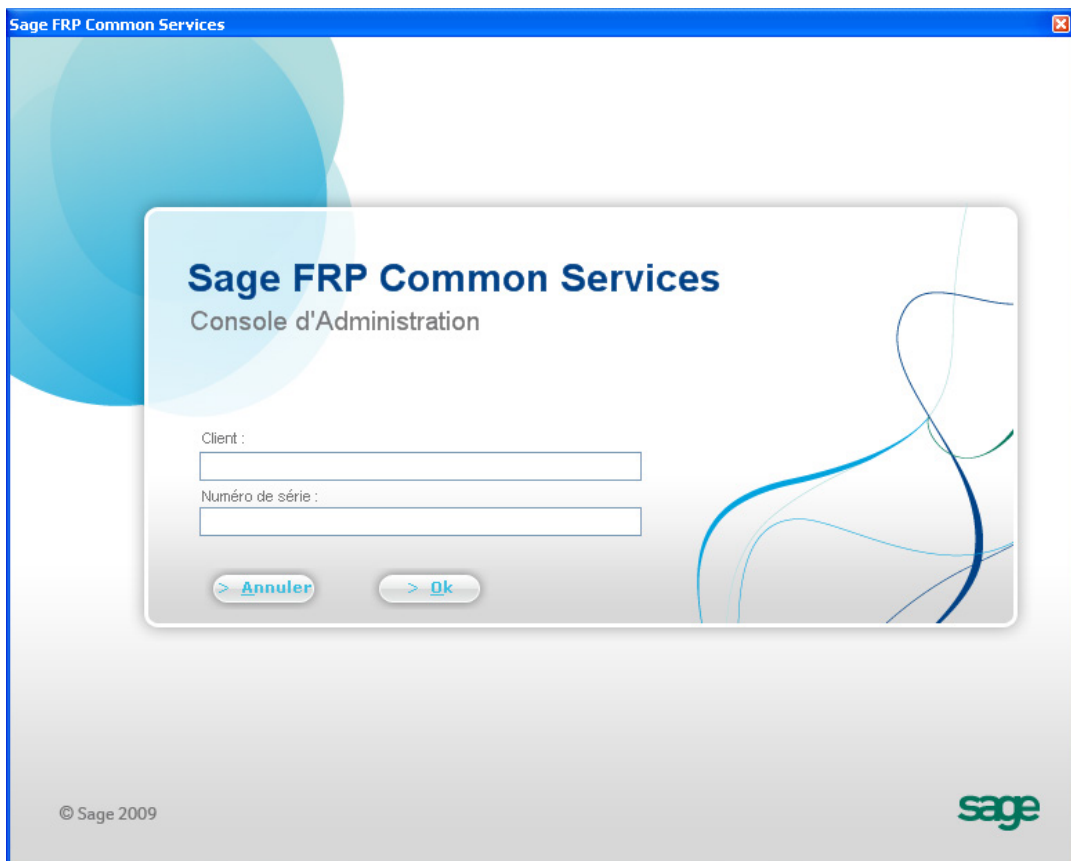
9 License Management

9.1 License

If the following window is displayed:



Click **Yes**. The following screen is displayed:



Enter the required information and click **OK**.

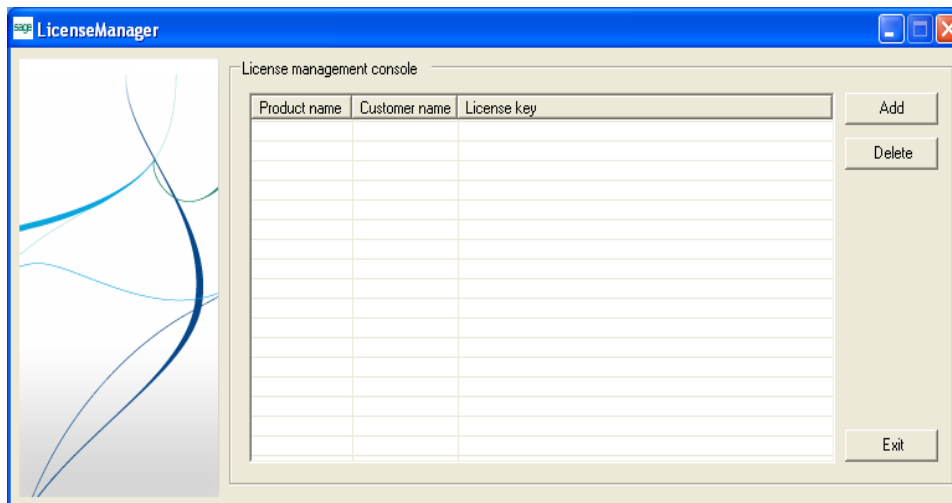
Note	Entering a Format License number is mandatory upon first connection to the Administration Console. For future installations or updates, the same license will be used again. Refer to Chapter 9.3 to know how to modify a license number.
-------------	---

A license number can be added:

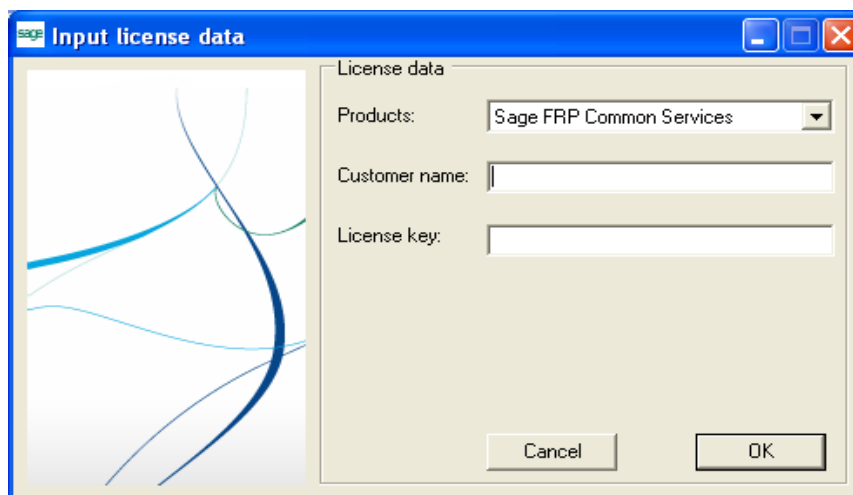
- Upon first connection to the product (XCS, Universe, etc.).
- By launching the License Manager application.

9.2 Adding a New Product License

In the **Start** menu, select **Programs – Sage – Sage Administration – Sage License Manager**. The following screen is displayed:



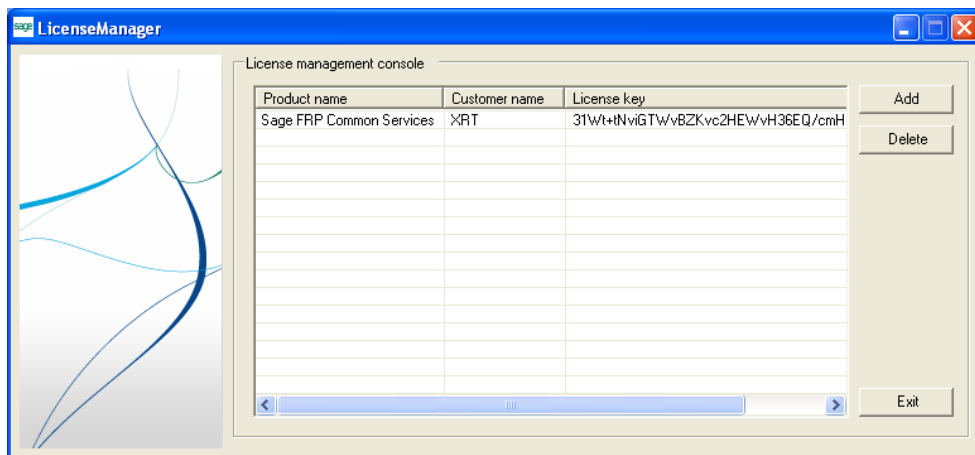
Click **Add** to display the **Input License Data** dialog box:



1. Select the product requiring a new license; complete the **Customer name** and **License Key** fields.
2. Click **Ok**.

9.3 Modifying a Product License

1. In the **Start** menu, select **Programs – Sage – Sage Administration – Sage License Manager**. The following screen is displayed:



2. Select a line and click on **Delete** or **Add** to change the license. If you selected **Add**, the application prompts you to confirm: **"Are you sure you want to overwrite existing license?"**.
Refer to 9.2 to add a row.



10 Faults

10.1 XDLO does not work with a firewall between client station and administration computer

As described in paragraph 0 , XDLO uses DCOM for data exchange between client and administration stations.

Wikipedia definition for DCOM:

Distributed Component Object Model is a Microsoft proprietary technology for communication among software components across networked computers. For security reasons, setting up DCOM with a firewall or between two untrusted computers might be difficult.

Extracts of the French article <http://support.microsoft.com/kb/467787/fr>: « Utilisation de DCOM avec des firewalls »:

"Unlike most Internet applications which have fixed TCP and/or UDP ports, DCOM dynamically assigns—at run time—one TCP port and one UDP port to each executable process serving DCOM objects on a computer. *That is, even if a process is hosting 2,000 clients and 50,000 objects, any client wishing to communicate with objects owned by it will always connect to the same TCP or UDP port. Clients discover the port associated with a particular object by connecting to and using the services provided by DCOM's Service Control Manager (SCM). The SCM always operates at a fixed network port on every computer; in the Internet case this is always port 135 for both TCP and UDP. The SCM offers several RPC-based (not DCOM/ORPC-based) services which handle operations like: "create a new COM class object for me and tell me what TCP and UDP port it is on" or "I have an interface pointer, tell me where I need to go to actually use it", and so forth.*

DCOM's dynamic port allocation feature offers great flexibility in that programmers and administrators alike are free from the burden of having to configure (or hard code) applications to specific ports, free from resolving conflicts between multiple applications attempting to use the same port(s), and so on. Unfortunately, because DCOM (by default) is free to use any port between 1024 and 65535 when it dynamically selects a port for an application, it is rather firewall unfriendly out of the box. Configuring your firewall to leave such a wide range of ports open would present a serious security hole. Microsoft's developers realized this and have implemented a feature that allows you to restrict the range of ports that DCOM will use to assign to applications.

The mechanism mentionned above is described in the article, in English, published by Microsoft <http://support.microsoft.com/kb/30008300083/en-us>:


SUMMARY

Distributed Component Object Model (DCOM) uses Remote Procedure Call (RPC) dynamic port allocation. By default, RPC dynamic port allocation randomly selects port numbers above 1024. You can control which ports RPC dynamically allocates for incoming communication and then configure your firewall to confine incoming external communication to only those ports and port 135 (the RPC Endpoint Mapper port).

MORE INFORMATION

To control RPC dynamic port allocation, follow these steps:

- 1. From the Start menu, point to Programs, point to Administrative Tools, and then click Component Services to start Component Services.*
- 2. Click to expand the Component Services and Computers nodes. Right-click My Computer, and then click Properties.*

- 
3. *On the Default Protocols tab, click Connection-oriented TCP/IP in the DCOM Protocols list box, and then click Properties.*
 4. *In the Properties for COM Internet Services dialog box, click Add.*
 5. *In the Port range text box, add a port range (for example, type 5000-5020), and then click OK.*
 6. *Leave the Port range assignment and the Default dynamic port allocation options set to Internet range.*
 7. *Click OK three times, and then restart your computer.*

10.2 XDLO cannot be retrieved from the server

Description:

As described in section **Architecture** of paragraph 4.1, XDLO uses DCOM for data exchange between client and administration stations. This implies, as a prerequisite, that DCOM is enabled on the station on which XDLO is executed. Otherwise, the application displays this error message: **"XDLO cannot be retrieved from the server"**. Enabling XDLO tracing triggers the detailed message "Marshaler error: -2147418111" corresponding to the RPC_E_CALL_REJECTED code.

Problem resolution:

Here is the procedure to enable DCOM: Using the *components services*, follow this process:

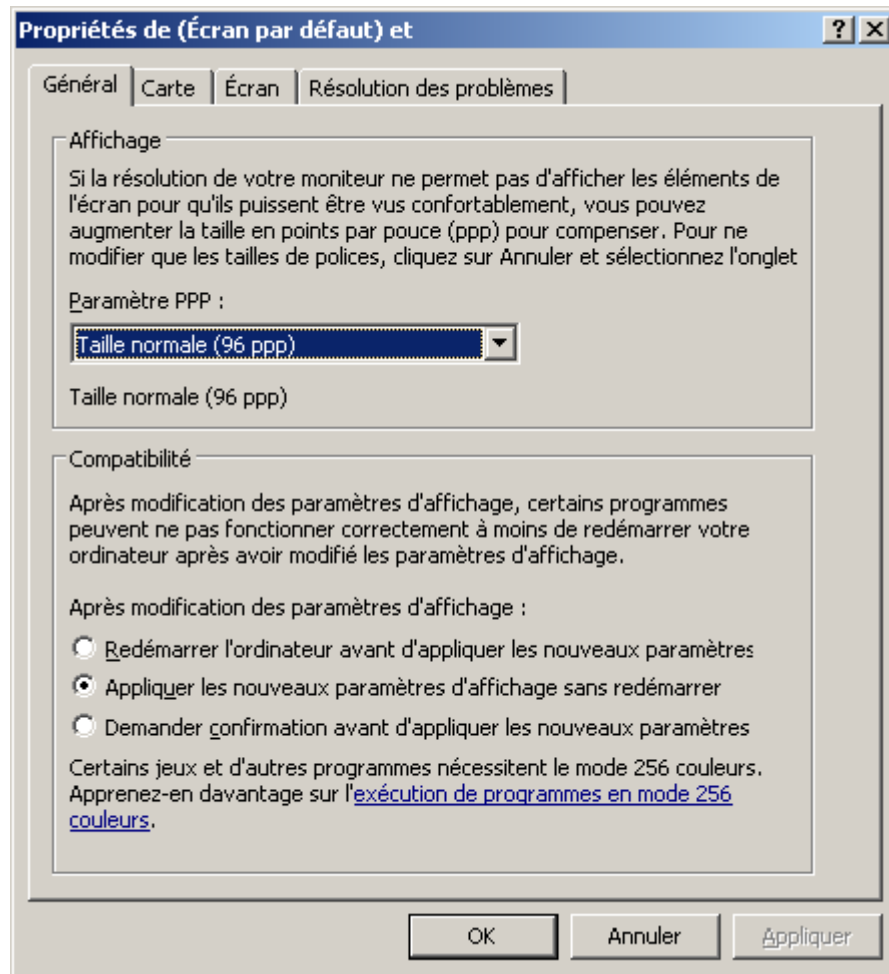
1. In the Start menu, point on Control Panel and Administrative Tools, click Component Services.
2. Expand Component Services and Computers.
3. Right-click on My Computer and Properties.
4. In the Default Properties tab, select the checkbox Enable Distributed COM on this computer.

10.3 Display error of the screen resolution following a specific DPI configuration

If the Login screen of the administration console changes and looks like this:



You need to select 96 DPI for the **DPI setting** by clicking **Advanced** in the settings tab of **Display**.



10.4 The saving of the report in PDF format generates an error message after closing

In specific conditions, saving the report in PDF format can generate the following error message after it is closed:



As presented in the article

<http://technicalsupport.businessobjects.com/cs/forums/post/8818.aspx> the error is corrected by deleting u2post.dll dynamic library from Crystal Report installation directory.



***10.5 The connection to the product
using an NT account in lower case is
not possible with ORACLE***

The problem is solved in version 3.0.



11 Rules for Regular Identifiers

(Quote from SQL Server 2005 documentation)

The rules for the format of regular identifiers depend on the database compatibility level. This level can be set by using `sp_dbcmplevel`. When the compatibility level is **90**, the following rules apply:

1. The first character must be one of the following:

- A letter as defined by the Unicode Standard 3.2. The Unicode definition of letters includes Latin characters from a through z, from A through Z, and also letter characters from other languages.
- The underscore (`_`), at sign (`@`), or number sign (`#`).

Certain symbols at the beginning of an identifier have special meaning in SQL Server. A regular identifier that starts with the at sign always denotes a local variable or parameter and cannot be used as the name of any other type of object. An identifier that starts with a number sign denotes a temporary table or procedure. An identifier that starts with double number signs (`##`) denotes a global temporary object. Although the number sign or double number sign characters can be used to begin the names of other types of objects, we do not recommend this practice.

Some Transact-SQL functions have names that start with double at signs (`@@`). To avoid confusion with these functions, you should not use names that start with `@@`.

2. Subsequent characters can include the following:

- Letters as defined in the Unicode Standard 3.2.
- Decimal numbers from either Basic Latin or other national scripts.
- The at sign, dollar sign (`$`), number sign, or underscore.

3. The identifier must not be a Transact-SQL reserved word. SQL Server reserves both the uppercase and lowercase versions of reserved words.

4. Embedded spaces or special characters are not allowed.

5. Supplementary characters are not allowed.

When identifiers are used in Transact-SQL statements, the identifiers that do not comply with these rules must be delimited by double quotation marks or brackets.

12 Details about the Database Installation Wizard

You must use the wizard to install product databases.

Option **Create an installation package that will be manually executed by an administrator** must only be used by Sage or Oracle product experts. If different products are included to the package, review and adaptation of the scripts will be required. In most cases, this solution should not be applied. The only conceivable case is a DBA refusing the installation by Sage of the client's database.

12.1 Product Installation Scenario

- Prerequisites:
 - a database client installed with the same version as the target database instance
 - the possibility to connect to the database instance with this client
 - an administration account for this instance
- Installation:
 - selection of the product to be installed
 - selection of the target database engine
 - selection of the target database instance
 - entry of information about the instance administration account (1)
 - entry or selection of the target database (2)
 - entry of information about the DBO account (owner of the product objects) (3)
 - entry of information about user accounts (product users)
 - [entry of the classification name for SQL server]
 - [modification of the information about logical units and physical files] (4)
 - creation of the list of scripts to be executed
 - execution and generation of the script execution logs. (5)
 - [import of initialization data]

Note:

1 – The administration account is:

- for sql server: a login with the **sysadmin** server role on the target sql server instance.
- for Oracle, it depends on products: generally an account with the Oracle DBA role is enough. By default, the wizard proposes the **system** account, except for Sage FRP Treasury which requires the login **sys**. Sage FRP Treasury grants rights on objects of the **sys** schema. The rights granted by Sage FRP Treasury on the **sys** schema are the following:
 - GRANT EXECUTE ON DBMS_DDL TO XRTDBO;
 - GRANT SELECT ON V_\$SESSION TO XRT_U2_USER;
 - GRANT SELECT ON V_\$INSTANCE TO XRT_U2_USER;
 - GRANT SELECT ON GV_\$SESSION TO XRT_U2_USER;
 - GRANT SELECT ON GV_\$INSTANCE TO XRT_U2_USER;
 - GRANT EXECUTE ON DBMS_LOCK TO <XUOwner>;

- GRANT SELECT ON V_\$SESSION TO <XUOwner>;
- GRANT SELECT ON V_\$INSTANCE TO <XUOwner>;
- GRANT SELECT ON GV_\$SESSION TO <XUOwner>;
- GRANT SELECT ON GV_\$INSTANCE TO <XUOwner>;

The XRTDBO role is the role of the owners of SAGE product schemas.

The XRT_US_USER role is the role of SAGE FRP Treasury user logins.

<XUOwner> is the owner of Sage FRP Treasury schema.

If these rights are not granted, you cannot launch the application.

2 – Target Database:

- for sql server: user database on the sql server instance.
- for Oracle, the schema is on an Oracle instance.

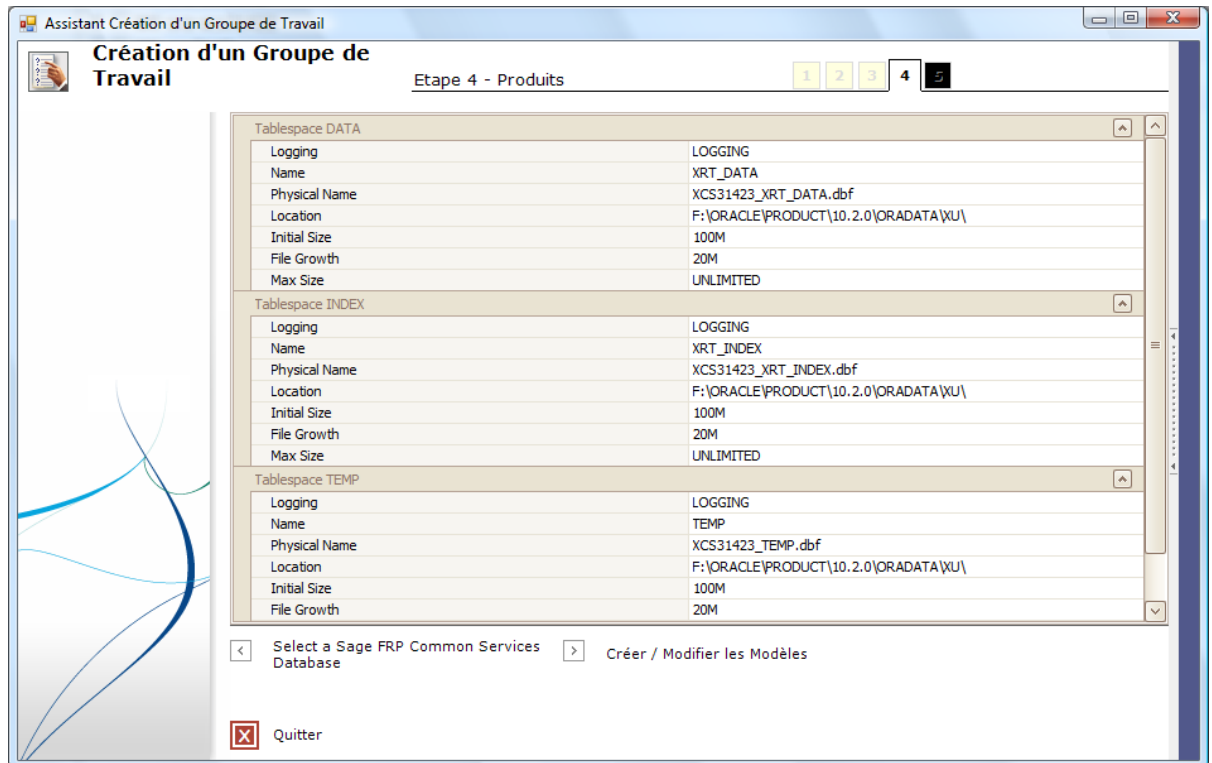
3 – The DBO account is:

- for sql server: sql server login mapped to the **DBO** user of the target database.
- for Oracle, the Login linked to the schema created or to be created.

4 – Storage organization for the product:

- A logical unit is a Filegroup for sql server and a tablespace for Oracle.
- The logical units are used in the storage clauses during the creation of the database objects.
- Each logical unit corresponds to a physical file.
- The name of the logical units can be modified in order to meet the customer's requirements.

Example 1: an oracle DBA does not want to have a tablespace for data and a tablespace for indexes when XCS contains few data.



Consequently, the DBA just needs to replace the "PhysicalName" and the "Name" of the INDEX tablespace by the information of the DATA tablespace. Thus, all objects will be created in the same tablespace.

Example 2: the oracle DBA wants to modify XRT_DATA and XRT_INDEX names to point to existing tablespaces. The DBA just needs to modify the "Name" property to enter the expected value(s).

NOTE: for SQL server as well as for Oracle, if the Filegroup or the tablespace defined in the wizard is already in the target database, there is no modification of the database structure. The elements used are the existing ones.

- The name of the physical files and their locations can be modified in order to meet the customer's requirements.

5 – Script Execution Logs:

Each executed SQL script generates a log file.

- For sql server: according to the products, the logs are more or less precise. This is not very important as, in case of error, the script is interrupted and the actions linked are roll-backed.
- For Oracle, logs are more precise. In case of errors, scripts are not roll-backed. All errors are not systematically logged, as some of them are not critical (e.g. drops on inexistent objects). However, it is recommended to browse these logs and search the "ORA-" string to check that the operation has been normally completed.

12.2 Actions on the Database

This section describes the interactions between the wizard and the target database. SQL Server and Oracle will operate the same way. However, specific information on each engine is useful.

SQL SERVER 2005

Accessing SQL Server

The wizard uses two tools to access SQL Server instance: SMO (SQL Server Management Objects) and the sqlcmd command line utility program.

SMO is used to check the environment and create the user database.

sqlcmd is used with **sysadmin** administration account to:

- Create the DBO login
- Create the XRT_USERS user role (DML on the base objects)
- Select the database options
- Create the SQL Server filegroups and related files if required

sqlcmd is used with the dbo account to:

- Create an XL_CONFIGURATION table to store product information
- Save the information about logical units
- Create the objects of the product template
- Import initialization data

Wizard Automatic Operations

The wizard performs processes on the scripts to execute:

- Replacing the variables in the scripts in order to take into account the data entered by the user
- Adding the **transact-SQL** code to encapsulate the script in a database transaction
- Adding the **transact-SQL** code to spot errors and stop the script execution
- Registering the product model and its version in the XL_CONFIGURATION table

Structure of SAGE FRP Treasury database (ex-XRT Universe):

In the previous versions of the product, the database was structured in three SQL Server filegroups: PRIMARY, DATA, INDEX.

In version 3, three new filegroups are necessary: AUD, AUDIDX, U2_TEMP.


U2_AUD and U2_AUDIX tablespaces are used to store the audit data of the application. These objects can grow larger over time, but the information is rarely modified. As its life cycle is specific, this information is now stored apart from production data.

U2_TEMP filegroup is used to create "temporary" objects on user sessions in Sage FRP Treasury. These data do not take part in the production data, they last as long as the user session does and are deleted at the end of it. This filegroup contains important input/output volumes with lots of created and deleted objects.

Oracle 10G R2

The wizard does not create any instance and/or Oracle database. The instance/Oracle database must exist with a local service (tnsnames.ora) on the computer hosting the wizard (defined and tested service).

If these conditions are met, the installation is similar to an SQL server scenario.



Important: the wizard does not have any reliable method to find the client or oracle server version installed without any connection. It relies on the inventory.xml file in the Oracle folder in Program files. In this file, the **HOME NAME** entry should include the "**10g**" string. This is normally the case when the name is not modified at installation. Consequently, if a client is installed and the wizard does not detect the Oracle engine, check **HOME NAME**.

Accessing Oracle

The wizard uses **sqlplus** tool to access Oracle instance.

sqlplus is used to check the environment (administration account):

- List of the existing users: **all_users** view
- Compatibility level of the instance: **v\$parameter** view
- SYSTEM tablespace default path: **v\$tablespace,v\$datafile** view

sqlplus is used with the administration account to:

- Create the Oracle tablespaces and related files if necessary
- Create the Oracle login owning the product schema
- Give it the necessary rights to implement the product
- Create the XRT_USERS user role (DML on Sage products)
- Give quotas on the tablespaces to the login owning the schema

sqlplus is used with the dbo account to:

- Create an XL_CONFIGURATION table to store product information
- Save the information about the tablespaces in XL_CONFIGURATION
- Create the objects of the product template
- Import initialization data

Wizard Automatic Operations


The wizard performs processes on the scripts to execute:

- Replacing the variables in the scripts in order to take into account the data entered by the user
- Registering the product model and its version in the XL_CONFIGURATION table

Warning:

The wizard does not create (or badly) any tablespaces when Oracle operates with other operating system than Microsoft. In this case, you need to ask the dba to create them. We cannot ensure that the security context of the different unix under which Oracle operates, is totally reliable. Consequently, we do not want to create the database physical files with these environments. If the dba creates them, the wizard will use them properly.

If the database uses **ASM** (Automatic Storage Management) **the dba must create the tablespaces**. Our tablespace creation process retrieves the path of the SYSTEM tablespace and uses it as default path to create physical files. In **ASM**, this process **can damage the existing database**.



Before version 3, the wizard used to create an **XRTDBO** role. This role is reserved to the owners of Sage application schemas (dbo). It includes too many rights. The following rights can be deleted:

- GRANT ALTER USER
- GRANT CREATE USER
- GRANT DROP USER
- GRANT GRANT ANY ROLE²

The wizard creates an **XRT_USERS** role. This role is reserved to Sage product users. It includes too many rights. The following rights can be deleted:

- GRANT ALTER TABLESPACE
- GRANT SELECT ANY SEQUENCE
- GRANT EXECUTE ANY PROCEDURE

In version 3, the wizard does not create any XRTBDO role, but directly grants the rights to the dbo login. His/her rights are the minimum rights, the only questionable privilege for the DBO is "GRANT CREATE PUBLIC SYNONYM TO".

Products, Tablespaces and Default Users

Reminder: for Oracle instances operating in Unix, the tablespaces must be created by the DBA of the client.

Each Sage product will create its own tablespaces. The names of these tablespaces and the access path to the linked files can be modified, as described earlier. However, if the information in the wizard is not modified, Sage products will be installed as described below.

SCS (Sage Common Services):

- User XRT and Password XRT are created
- 2 tablespaces . XRT_DATA and XRT_INDEX are created.

Sage FRP Treasury:

- User UN2 and Password UN2 are created
- 5 tablespaces . U2_DATA, U2_INDEX, U2_AUD, U2_AUDIX and U2_TEMP are created.

Sage FRP Signature:

- User PDS and Password PDS are created
- 2 tablespaces . PDS_DATA and PDS_INDEX are created.

SBE (Sage Business Exchange):

- User SMP and Password SMP are created
- 2 tablespaces . SMP_DATA and SMP_INDEX are created.

Sage Frp Communication:

- User BCP and Password BCP are created
- 2 tablespaces . BCP_DATA and BCP_INDEX are created.

Tablespaces

All Sage tablespaces are created from the same command:

```
CREATE TABLESPACE <%=logicalUnit.Name%>
    <%=logicalUnit.Logging%>
    DATAFILE ''' || data_path || '<%=logicalUnit.Physical_Name%>'''
    SIZE <%=logicalUnit.Initial_Size%>
    AUTOEXTEND ON
    NEXT <%=logicalUnit.File_Growth%>
    MAXSIZE <%=logicalUnit.Max_Size%>
    EXTENT MANAGEMENT LOCAL
    SEGMENT SPACE MANAGEMENT AUTO;
```

The variables in this command correspond to the information available in the wizard.

Management of the data file will be the responsibility of Oracle. This has proven to be efficient.

Nevertheless, should a DBA wish to specify more parameters for tablespace management, he will have to carry out the creation of the tablespaces before installing the applications. Then the Wizard will use them.

The product scripts do not contain any storage clause upon object creation.

The storage is directly linked to the tablespace parameters.

Sage FRP Treasury (ex-XRT Universe) Tablespaces

SAGE FRP Treasury is a product performing complex processes. That is the reason why a PERMANENT U2_TEMP tablespace, in NOLOGGING, is planned to be created.

This tablespace will be used to store intermediary results, user filters, etc.

This tablespace does not need to be saved, nor restored: it is NOLOGGING.

The object names of this tablespace start with TMP_, but these objects are Oracle-standard objects, they are not temporary.

These objects have a life cycle corresponding to the user session, but some of them will not be systematically removed.

The number of objects can reach several thousands and make the tablespace size grow rapidly.

If a dba notes that the tablespace size is growing too fast, he/she may consider how disk space has been allocated for this tablespace. For each table created, if 1MB is occupied on the disk, the required space will grow exponentially with 1000 objects, even if these objects contain few or no data at all.

If the number of objects matters, the launch of the next block should be automated, using the schema owner's login.

```
begin
    MSTEMPTABLEEMUL.ClearDeadTemps;
end;
/
```

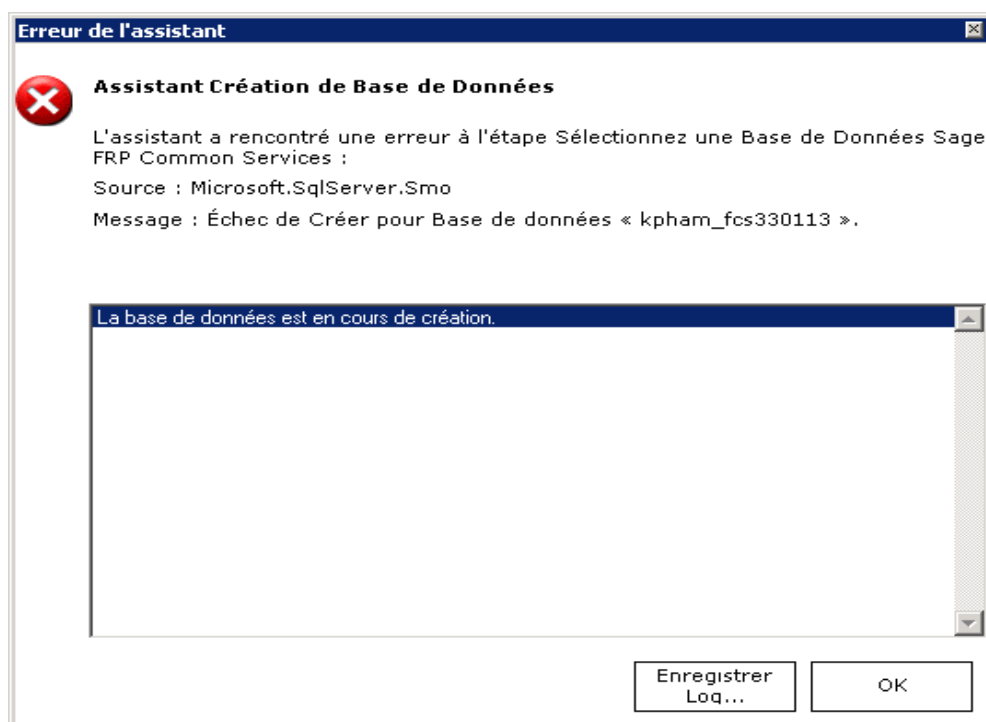
This block will delete any object from U2_TEMP tablespace if its user session is no longer active. By default, SAGE FRP Treasury calls this block every fifteen user disconnections. However, this may be insufficient.



U2_AUD and U2_AUDIX tablespaces are used to store the audit data of the application. These objects can grow larger over time, but the information is rarely modified. As its life cycle is specific, this information is now stored apart from production data.

13 Creating SQL 2008 and Oracle 11G Databases in a 64-bit Environment

In a 64-bit environment, given that Sage applications are 32-bit, the coexistence of SQL2008 client 64-bit (or Oracle11g 64-bit) and SQL2008 client 32-bit (or Oracl11g 32-bit) on one PC may affect the functioning of the application, particularly the creation of the database. The following message will be displayed:



Two solutions are proposed :

either install the 32-bit client on another 64-bit client station, and access to SQL2008 64-bit server (or Oracle11g) will be made through the 32-bit client,
or remove SQL2008 64-bit client (or Oracle11g 64-bit) from the 64-bit server and access to SQL2008 64-bit server (or Oracle11g) will be made through the 32-bit client.