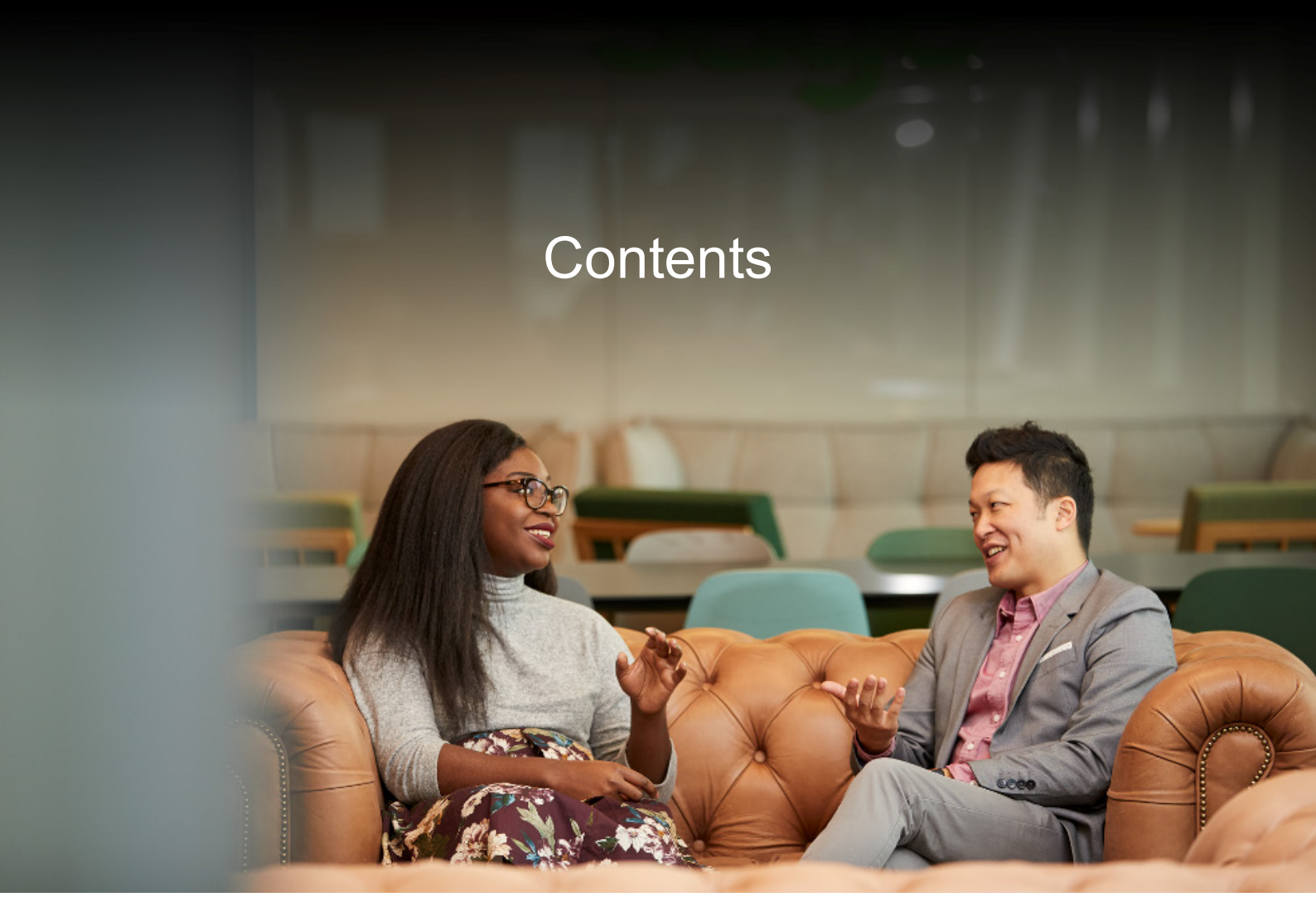
Sage XRT Business Exchange

Version 12.1.0

Personal Data

Contents



Purpose **4**

European Basic Requirements **5**

Data Security **6**

Database Access Security 6

Access Rights Management 6

Selection of Authentication Strategy 6

Definition of Security Policy through SXCS 7

Management of Profiles, Roles and Users 7

Audit Functions for Access and Identities 8

Security Reporting 9

Compliance with Sarbanes Oxley Act 9

Personal Data and Associated Processing **12**

Personal Data List 12

User Management 14

Security Options by Entity 14

Setup 14

Reporting 15

Signatories 15
Purpose of Data Processing 15
Management: creation-modification-deletion 15
Database Report 16
Third Parties: Clients-Providers-Employees 16
Purpose of Data Processing 18
Third Party Management 21
Amendment Management 22
Export to Database 23
Bank Branch Contacts 23
Purpose of Data Processing 23
Management 23
Database Report 24
Rights of Rectification and Erasure - Retention Period 24
Additional Security Measures 25
General Measures 25
Using https 25
Strengthening Passwords 25
Securing Servers through Access Rights 25
Protecting Servers 26
Using Transparent Data Encryption 26
Encrypting Data in Transit 27
Encrypting Database Backups 27
File System Security 27
Application Measures 27
Web Site and Application Signature 27
Authorizations 28
Protection against Attacks 29
Website Access Frequency 30
For Further Information 30
Disclaimer 31

Purpose

The general data protection regulation (GDPR) applies in all EU Member States from 25 May 2018.

This document aims at identifying the existing functions from **Sage XRT Business Exchange** that could help your company to comply with this European regulation.

©Sage 2018

European Basic Requirements

Basic Requirements for Personal Data Protection	Sage XRT Business Exchange
Ensuring appropriate security	
The company must install appropriate technical and organizational safeguards that ensure the security of the personal data such as the securing of work stations and storage spaces, as well as confidentiality policies and clauses.	
Stronger Passwords and Protection of certain stored or exchanged data See the existing functions for security	✔
Managing individuals rights: data portability, right of erasure, right of objection to the processing/consent, right of rectification, etc.	
It must provide functions to correct and import/export personal data, as well as functions to select the individuals subject to processing of their data.	
Modification/Deletion functions available in every product, according to the user rights See the existing functions for personal data	✔
Helping demonstrate compliance	
The company must keep records of all the documents that demonstrate the actions set up to comply with the general data protection regulation - they could be presented in case of inspection, such as: documents describing the technical and organizational safeguards that it has installed to ensure the security of personal data use, the processing registry.	
Sage makes available records of all personal data and associated processing activities for **Sage XRT Business Exchange**. See the list of personal data and associated processing activities	✔

©Sage 2018

Data Security

Database Access Security

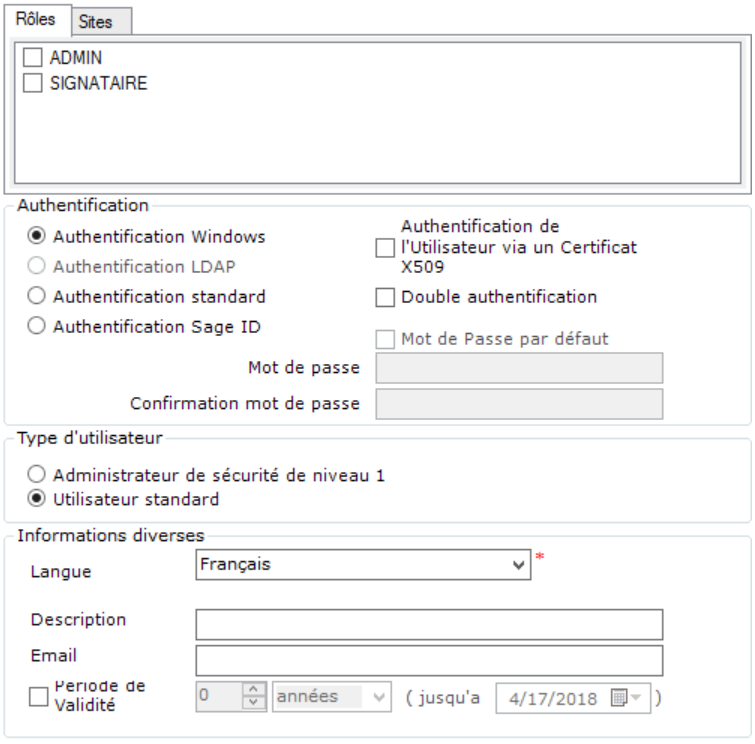
Sage XRT Common Services Administration Console enables you to define the management of user access rights for **Sage XRT** applications.

Access Rights Management

Two modes to grant access rights are available:

- 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 every action taken by Security Administrator to be validated by a second one.

Selection of Authentication Strategy



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

- **Use Windows NT integrated security**: the DBA is authenticated by its NT account, we recommend this authentication level.

©Sage 2018

- **Use a specific username and password**: the DBA is authenticated by a username and a password.
- **Authentication via X509 Certificate**: for the web client, the strong authentication consists of two phases.
    - Check of the certificate by searching the company's **Active Directory**
    - Challenge/Answer between the client and the authentication component to check client identity
- **Double authentication**: a second factor is used for user authentication to generate a single-use password.
- **SageID**

Definition of Security Policy through SXCS

Management of Profiles, Roles and Users

Profiles enable the creation of user and administrator roles to define access permissions.

©Sage 2018

Audit Functions for Access and Identities

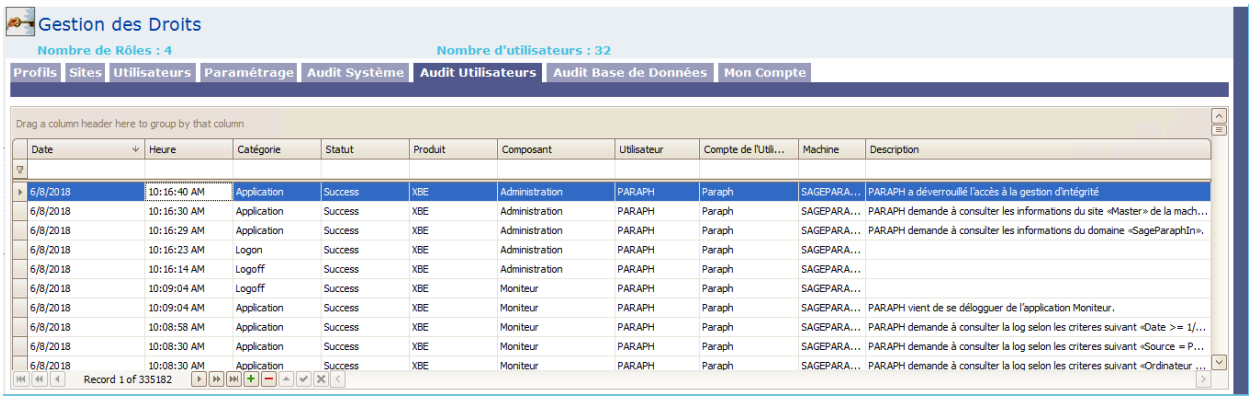
On top of providing the obvious functions, the identity and access management must prove its efficiency.

The evidence must be remitted to auditors upon request and in written to be archived.

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

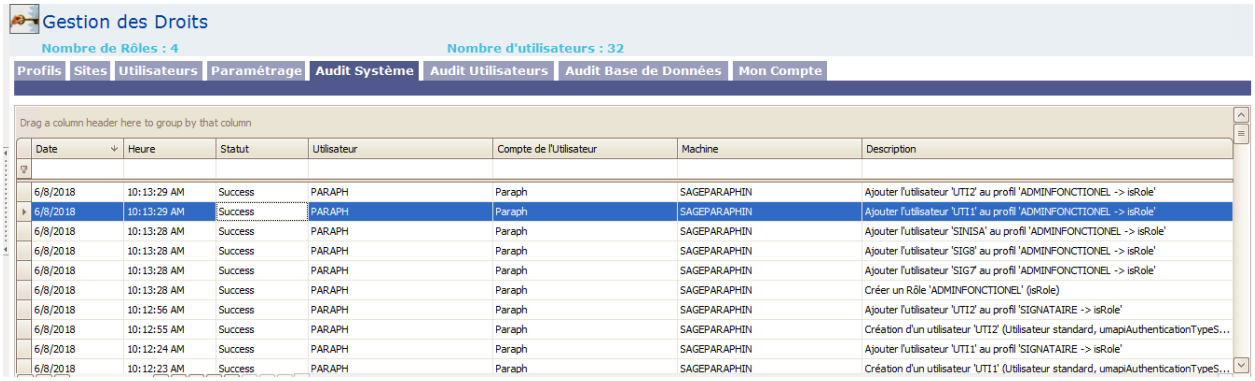
- Administrator Actions
  - Create User
  - Delete User
  - Change User Password
  - Change management strategy of passwords
  - Change access configuration to LDAP directory
  - Access granted
  - Access denied
- Final User Actions
  - Login
  - Logoff
  - Specific messages from the application
- Tests for compliance with security policy
  - User account locked after **n** failed tries log on

The **Users Audit** table describes all actions executed by the users.



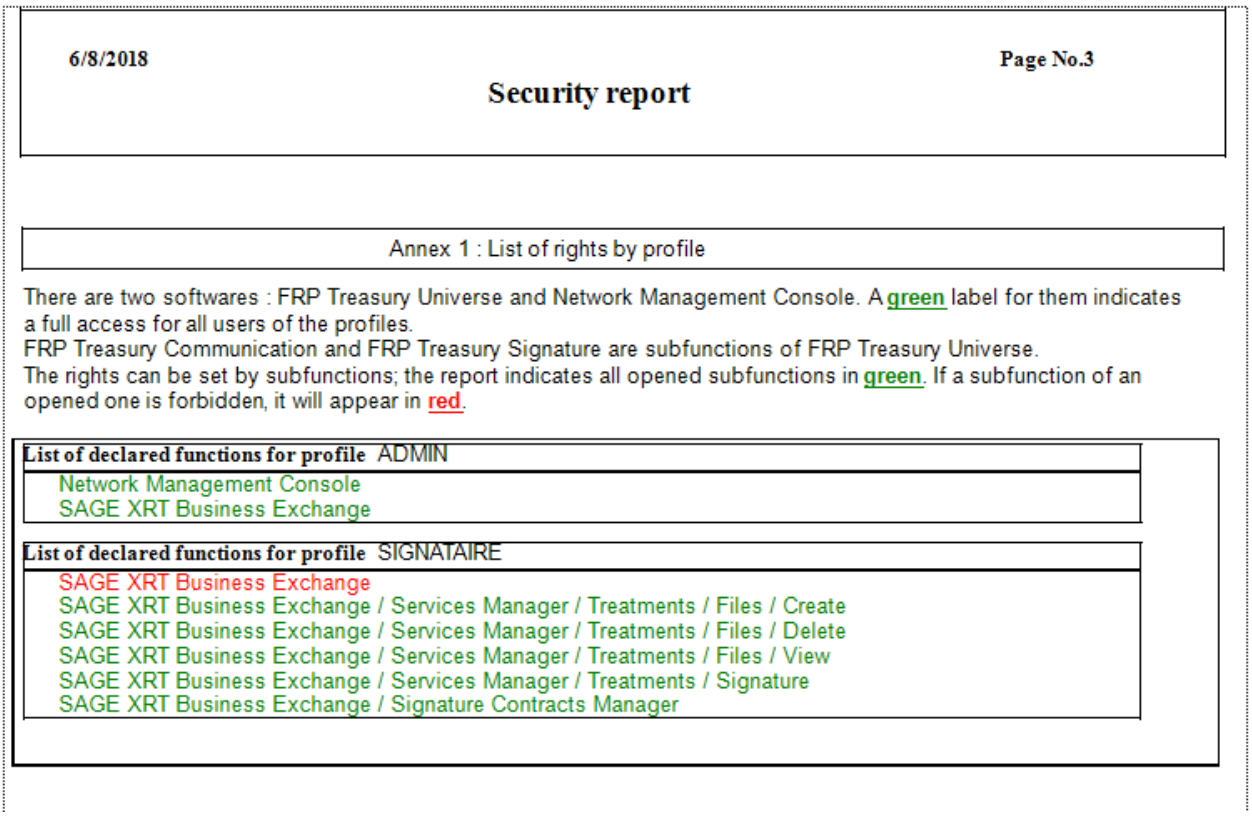
©Sage 2018

The System Audit table describes all actions executed at time *t*.



Security Reporting

Sage XRT Common Services Administration Console enables you to edit reports listing the authorized/denied functions for each profile and each product from the platform.



6/8/2018 Page No.3

Security report

Annex 1 : List of rights by profile

There are two softwares : FRP Treasury Universe and Network Management Console. A green label for them indicates a full access for all users of the profiles.
FRP Treasury Communication and FRP Treasury Signature are subfunctions of FRP Treasury Universe.
The rights can be set by subfunctions; the report indicates all opened subfunctions in green. If a subfunction of an opened one is forbidden, it will appear in red.

List of declared functions for profile ADMIN

Network Management Console
SAGE XRT Business Exchange

List of declared functions for profile SIGNATAIRE

SAGE XRT Business Exchange
SAGE XRT Business Exchange / Services Manager / Treatments / Files / Create
SAGE XRT Business Exchange / Services Manager / Treatments / Files / Delete
SAGE XRT Business Exchange / Services Manager / Treatments / Files / View
SAGE XRT Business Exchange / Services Manager / Treatments / Signature
SAGE XRT Business Exchange / Signature Contracts Manager

Compliance with Sarbanes Oxley Act

The *Sarbanes Oxley Act* imposes security rules to get access to operating systems and applications.

©Sage 2018

Data Security

Here is the list of the Security Issues for access and use of **Sage XRT** applications and for a standard user.

Sage XRT password policy complies with the requirement of the *Sarbanes Oxley Act*.

Security Issues	Sage XRT Business Exchange (rich client)	Sage XRT Business Exchange (web module)
The application manages profiles.	✓	✓
Passwords are mandatory.	✓	✓
A standard password is given to everyone or to a group upon account creation.	✓	✓
The password must be changed upon first connection.	✓ Customizable	✓ Customizable
Passwords must contain at least 6 characters, among which 1 uppercase letter and 1 digit.	✓ Customizable	✓ Customizable
Passwords must be changed every 42 Days.	✓ Customizable	✓ Customizable
The application keeps the passwords history. The four last passwords cannot be used.	✓ Customizable	✓ Customizable
Passwords are not kept to avoid new entry in later connections.	✓ For a complete NT security, the passwords used are the Windows passwords. Customizable ✓ For XRT standard security, the application password is not stored.	✓
The password is locked after 3 unsuccessful entries. It is automatically reactivated after 10 minutes.	✓ Customizable	✓ Customizable
The account is not locked if not used for several days.	✓	✓
The session is locked after 10-minute inactivity.	✗	✓ Customizable

©Sage 2018

Data Security

Security Issues	Sage XRT Business Exchange (rich client)	Sage XRT Business Exchange (web module)
Security rules cannot be modified from user work station.	✔	✔
Every access to application must be logged.	✔	✔
For short-term contract users, the specification of an end date of validity is mandatory corresponding to the end date of contract.	✔ Customizable	✔ Customizable

©Sage 2018

Personal Data and Associated Processing

Personal Data List

Personal Data are used in order:

- To identify users, control access and authorizations in the application
- To check, validate and sign electronically during bank exchanges
- To retrieve bank data files

Financial data of third parties enable the execution of payment orders arising from the contract between the parties.

Personal Data	Category	Purpose
Financial Operator Alias	Client Data	User ID
Financial Operator Name	Client Data	User/Signatory ID
Financial Operator First name	Client Data	User/Signatory ID
Financial Operator Capacity	Client Data	User/Signatory ID
Financial Operator Phone	Client Data	User/Signatory ID
Financial Operator Fax	Client Data	User/Signatory ID
Financial Operator E-mail	Client Data	User/Signatory ID
Financial Operator Certificates	Client Data	Signatory ID
Branch Contact Name	Client Data	Bank Contact
Branch Contact Phone	Client Data	Bank Contact
Branch Contact FAX	Client Data	Bank Contact
Branch Contact E-mail	Client Data	Bank Contact
Branch Contact Capacity	Client Data	Bank Contact
Branch Contact Service	Client Data	Bank Contact
Beneficiary Third Party Name	Marital Status	Providers, Salaries Payments, Anti-Fraud Checks
Beneficiary Third Party First Name	Marital Status	Providers, Salaries Payments, Anti-Fraud Checks

©Sage 2018

Personal Data and Associated Processing

Personal Data	Category	Purpose
Beneficiary Third Party Address	Marital Status	Providers, Salaries Payments, Anti-Fraud Checks
Beneficiary Third Party Country Code	Client Data	Providers, Salaries Payments, Anti-Fraud Checks
Beneficiary Third Party Phone	Client Data	Providers, Salaries Payments, Anti-Fraud Checks
Beneficiary Third Party E-mail	Client Data	Providers, Salaries Payments, Anti-Fraud Checks
Beneficiary Third Party FAX	Client Data	Providers, Salaries Payments, Anti-Fraud Checks
Beneficiary Third Party Bank Name	Bank Data	Providers, Salaries Payments, Anti-Fraud Checks
Beneficiary Third Party BIC	Bank Data	Providers, Salaries Payments, Anti-Fraud Checks
Beneficiary Third Party IBAN - Account ID	Bank Data	Providers, Salaries Payments, Anti-Fraud Checks
IBAN - Disbursement Account of Beneficiary Third Party	Bank Data	Providers, Salaries Payments, Anti-Fraud Checks
Debtor Name	Marital Status	Client Drawings, Anti-Fraud Check
Debtor First Name	Marital Status	Client Drawings, Anti-Fraud Check
Debtor IBAN	Bank Data	Client Drawings, Anti-Fraud Check
Debtor Account Currency	Bank Data	Client Drawings, Anti-Fraud Check
Debtor Bank BIC	Bank Data	Client Drawings
Unique Mandate Reference	Contract Data	Client Drawings, Anti-Fraud Check
Mandate Signature Date	Contract Data	Client Drawings, Anti-Fraud Check
Mandate Signature Place	Contract Data	Client Drawings, Anti-Fraud Check
Mandate Recurrence Type	Contract Data	Client Drawings, Anti-Fraud Check

©Sage 2018

User Management

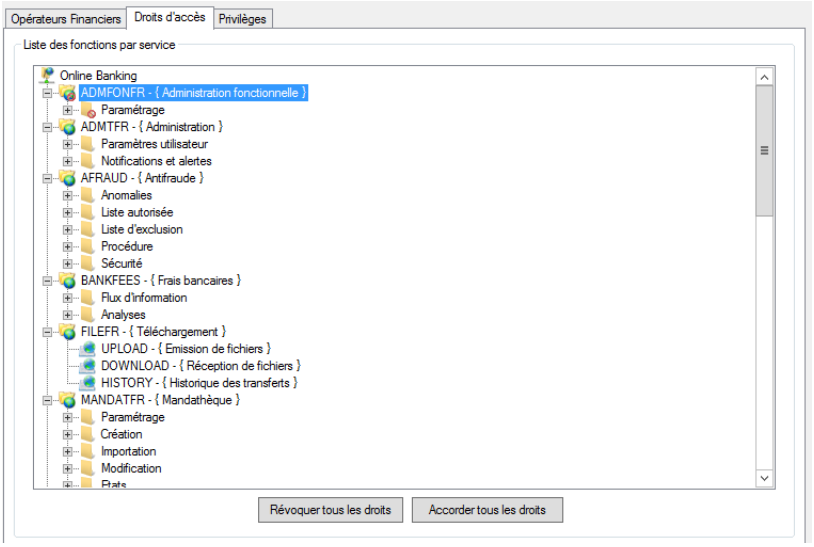
Sage XRT Business Exchange users are created by an administrator with authorizations on each entity, based on the users created in the Administration Console (see § *Definition of Security Policy through SXCS*).

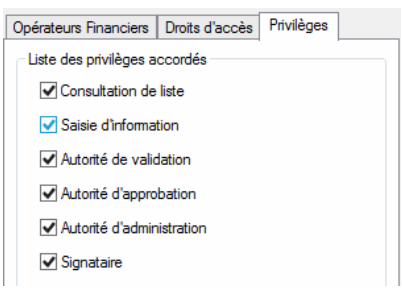
Security Options by Entity

Setup

For each entity, user profiles enable you to specify:

- Access rights for each function of **Sage XRT Business Exchange**
- User rights

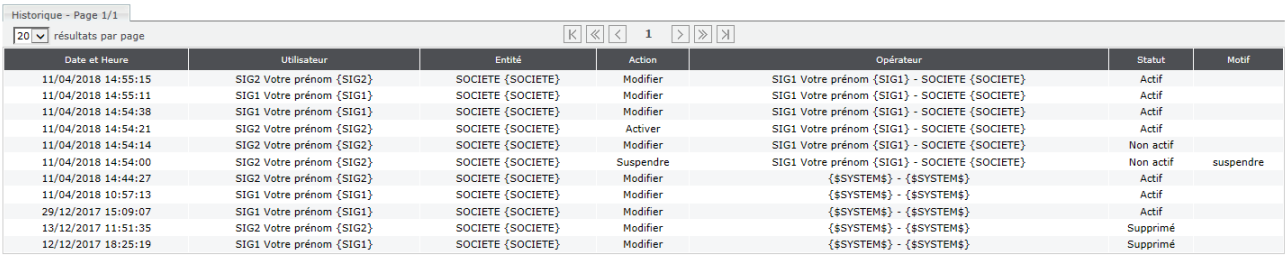




©Sage 2018

Reporting

Every action is registered by user in the audit ledgers for **Online Banking** site (creation-modification-suspension) or in the administration audit (see § *Audit Functions for Access and Identities*).



Historique - Page 1/1

20 résultats par page 1

Date et Heure	Utilisateur	Entité	Action	Opérateur	Statut	Motif
11/04/2018 14:55:15	SIG2 Votre prénom {SIG2}	SOCIETE {SOCIETE}	Modifier	SIG1 Votre prénom {SIG1} - SOCIETE {SOCIETE}	Actif	
11/04/2018 14:55:11	SIG1 Votre prénom {SIG1}	SOCIETE {SOCIETE}	Modifier	SIG1 Votre prénom {SIG1} - SOCIETE {SOCIETE}	Actif	
11/04/2018 14:54:38	SIG1 Votre prénom {SIG1}	SOCIETE {SOCIETE}	Modifier	SIG1 Votre prénom {SIG1} - SOCIETE {SOCIETE}	Actif	
11/04/2018 14:54:21	SIG2 Votre prénom {SIG2}	SOCIETE {SOCIETE}	Activer	SIG1 Votre prénom {SIG1} - SOCIETE {SOCIETE}	Actif	
11/04/2018 14:54:14	SIG2 Votre prénom {SIG2}	SOCIETE {SOCIETE}	Modifier	SIG1 Votre prénom {SIG1} - SOCIETE {SOCIETE}	Non actif	
11/04/2018 14:54:00	SIG2 Votre prénom {SIG2}	SOCIETE {SOCIETE}	Suspendre	SIG1 Votre prénom {SIG1} - SOCIETE {SOCIETE}	Non actif	suspendre
11/04/2018 14:44:27	SIG2 Votre prénom {SIG2}	SOCIETE {SOCIETE}	Modifier	{$SYSTEM$} - {$SYSTEM$}	Actif	
11/04/2018 10:57:13	SIG1 Votre prénom {SIG1}	SOCIETE {SOCIETE}	Modifier	{$SYSTEM$} - {$SYSTEM$}	Actif	
29/12/2017 15:09:07	SIG1 Votre prénom {SIG1}	SOCIETE {SOCIETE}	Modifier	{$SYSTEM$} - {$SYSTEM$}	Actif	
13/12/2017 11:51:35	SIG2 Votre prénom {SIG2}	SOCIETE {SOCIETE}	Modifier	{$SYSTEM$} - {$SYSTEM$}	Supprimé	
12/12/2017 18:25:19	SIG1 Votre prénom {SIG1}	SOCIETE {SOCIETE}	Modifier	{$SYSTEM$} - {$SYSTEM$}	Supprimé	

Signatories

Purpose of Data Processing

Signatories check, validate and sign electronically the financial data exchanges between a company and its banking partner.

These digital data flows consist of payment orders arising from the contract between two parties (salaries, providers invoices, bank direct debits).

Management: creation-modification-deletion

An authorized administrator can create signatories only if:

- The signatory is a user created in **Sage XRT Common Services** Administration Console (see § *Audit Functions for Access and Identities*).
- The signatory is a user created in **Sage XRT Business Exchange**.
- The user has been granted the **signatory** right.

Authorized users can modify and delete signatories.

©Sage 2018

Database Report

Every signatories' action is registered in the event log for the transaction service.

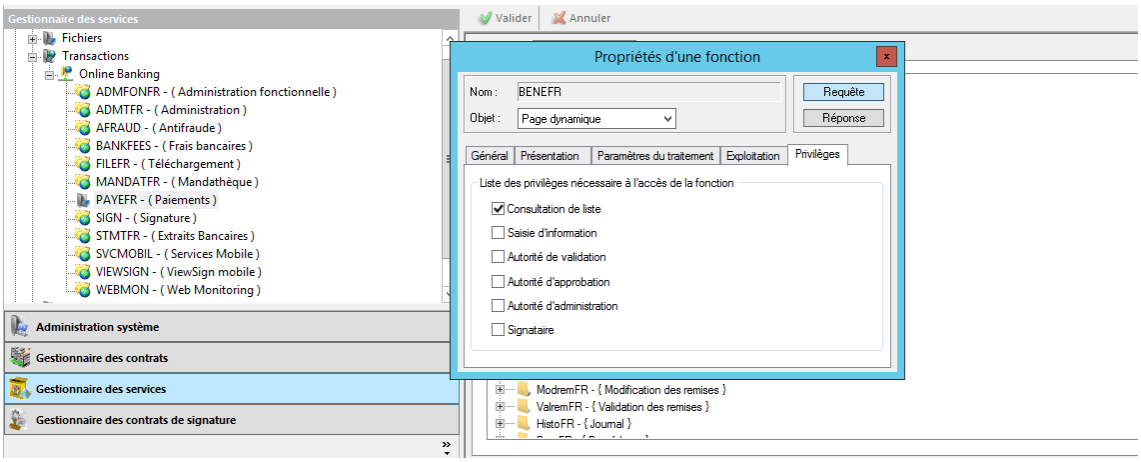
Date & Heure	Entité	Utilisateur	Transaction	Fonction	Description	Ordinateur	Protocole	Référence du moniteur
4/11/2018 11:34:57 AM	SOCIETE	SIG1	SIGN	SIGN	Paraphage du fichier (Validation) : 1521	SAGEPARA...	Online Banki...	T{17EF59CF-7CA9-4FE
4/11/2018 11:34:29 AM	SOCIETE	SIG1	SIGN	SIGN	Demande de signature de fichier(s) : 1524,1523...	SAGEPARA...	Online Banki...	T{04EEF072-5857-46E
4/11/2018 11:34:07 AM	SOCIETE	SIG1	SIGN	ADD	Demande d'ajout (avec préparation automatiq...	SAGEPARA...	Online Banki...	T{3C719490-AEF4-449
4/6/2018 5:42:10 PM	SOCIETE	SIG1	WEBMON	WMFLOW	Demande de relance de transfert par le Modul...	SAGEPARA...	Online Banki...	T{232571D5-224C-42B
4/6/2018 5:42:07 PM	SOCIETE	SIG1	WEBMON	WMFLOW	Demande de relance de transfert par le Modul...	SAGEPARA...	Online Banki...	T{57FEE671-5957-424
4/6/2018 5:42:04 PM	SOCIETE	SIG1	WEBMON	WMFLOW	Demande de relance de transfert par le Modul...	SAGEPARA...	Online Banki...	T{9F785A70-0804-4BF
4/6/2018 5:41:29 PM	SOCIETE	SIG1	SIGN	SEND	Demande d'envoi de fichier(s) vers le logiciel d...	SAGEPARA...	Online Banki...	T{0B7B9570-218C-415
4/6/2018 5:41:20 PM	SOCIETE	SIG1	SIGN	LOCKS	Demande de déverrouillage de fichier(s) : 1520	SAGEPARA...	Online Banki...	T{B5FCA2F7-1DA8-41
4/6/2018 5:39:56 PM	SOCIETE	SIG1	SIGN	SEND	Demande d'envoi de fichier(s) vers le logiciel d...	SAGEPARA...	Online Banki...	T{E8170413-17C8-4EE
4/6/2018 5:39:38 PM	SOCIETE	SIG1	SIGN	SIGN	Demande de signature de fichier(s) : 1520	SAGEPARA...	Online Banki...	T{15D05DB5-B965-43F
4/6/2018 5:39:19 PM	SOCIETE	SIG1	SIGN	ADD	Demande d'ajout (avec préparation automatiq...	SAGEPARA...	Online Banki...	T{69E0D189-B66F-453
4/6/2018 5:35:07 PM	SOCIETE	SIG1	SIGN	ADD	Demande d'ajout (avec préparation automatiq...	SAGEPARA...	Online Banki...	T{CED2F536-9D9B-424
4/6/2018 12:20:31 PM	SOCIETE	SIG1	WEBMON	WMFLOW	Demande de relance de transfert par le Modul...	SAGEPARA...	Online Banki...	T{3FF99B4A-B202-4A1
4/6/2018 11:50:56 AM	SOCIETE	SIG1	WEBMON	WMFLOW	Demande de relance de transfert par le Modul...	SAGEPARA...	Online Banki...	T{8DBDE346-78C0-4F5
4/6/2018 11:50:54 AM	SOCIETE	SIG1	WEBMON	WMFLOW	Demande de relance de transfert par le Modul...	SAGEPARA...	Online Banki...	T{0A86B3FD-7C9B-4FF
4/6/2018 11:50:51 AM	SOCIETE	SIG1	WEBMON	WMFLOW	Demande de relance de transfert par le Modul...	SAGEPARA...	Online Banki...	T{C26113C5-75BB-4D1
4/6/2018 11:50:22 AM	SOCIETE	SIG1	SIGN	SEND	Demande d'envoi de fichier(s) vers le logiciel d...	SAGEPARA...	Online Banki...	T{A44FC8CC-A049-400
4/6/2018 11:49:11 AM	SOCIETE	SIG1	SIGN	SEND	Demande d'envoi de fichier(s) vers le logiciel d...	SAGEPARA...	Online Banki...	T{4BFED8D8-2FC2-415
4/6/2018 11:45:58 AM	SOCIETE	SIG1	WEBMON	WMFLOW	Demande de relance de transfert par le Modul...	SAGEPARA...	Online Banki...	T{5E85A9AE-608A-4C0
4/6/2018 11:45:56 AM	SOCIETE	SIG1	WEBMON	WMFLOW	Demande de relance de transfert par le Modul...	SAGEPARA...	Online Banki...	T{E574D633-7455-49B
4/6/2018 11:45:54 AM	SOCIETE	SIG1	WEBMON	WMFLOW	Demande de relance de transfert par le Modul...	SAGEPARA...	Online Banki...	T{401EA4CD-DBDA-44
4/6/2018 11:45:50 AM	SOCIETE	SIG1	WEBMON	WMFLOW	Demande de relance de transfert par le Modul...	SAGEPARA...	Online Banki...	T{24DEFBE7-9614-402
4/6/2018 11:42:46 AM	SOCIETE	SIG1	WEBMON	WMFLOW	Demande de relance de transfert par le Modul...	SAGEPARA...	Online Banki...	T{663671D6-233B-45C
4/6/2018 11:40:37 AM	SOCIETE	SIG1	SIGN	SEND	Demande d'envoi de fichier(s) vers le logiciel d...	SAGEPARA...	Online Banki...	T{C1BC52D7-69A7-40E
4/6/2018 11:35:18 AM	SOCIETE	SIG1	SIGN	SEND	Demande d'envoi de fichier(s) vers le logiciel d...	SAGEPARA...	Online Banki...	T{9ED17AA6-D3C5-4E
4/6/2018 11:30:55 AM	SOCIETE	SIG1	SIGN	SEND	Demande d'envoi de fichier(s) vers le logiciel d...	SAGEPARA...	Online Banki...	T{6ECD3AC5-DAE5-4E
4/6/2018 11:17:59 AM	SOCIETE	SIG1	SIGN	SEND	Demande d'envoi de fichier(s) vers le logiciel d...	SAGEPARA...	Online Banki...	T{67F60B78-B5BA-484

Third Parties: Clients-Providers-Employees

The third party list is either manually completed or automatically populated through the import of a third party or transaction file.

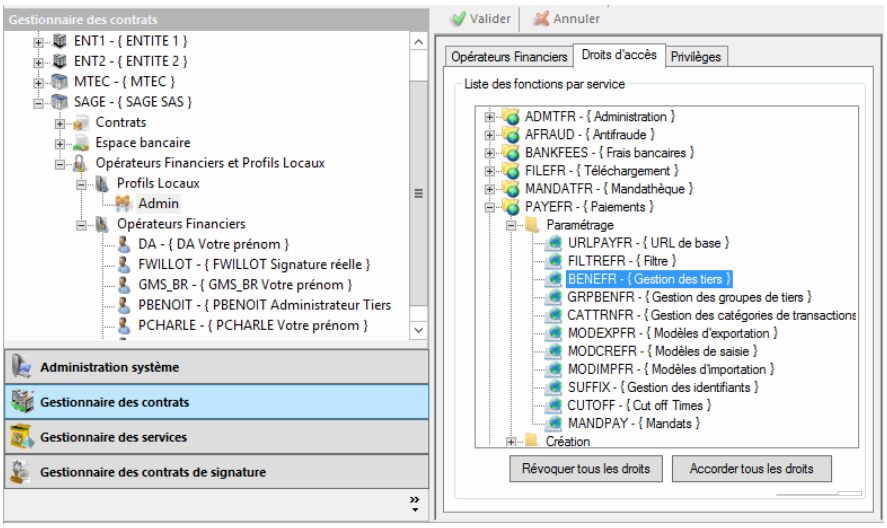
It is available for information purposes and can be modified and deleted.

Users with access to the third party list can be granted management rights on third parties.

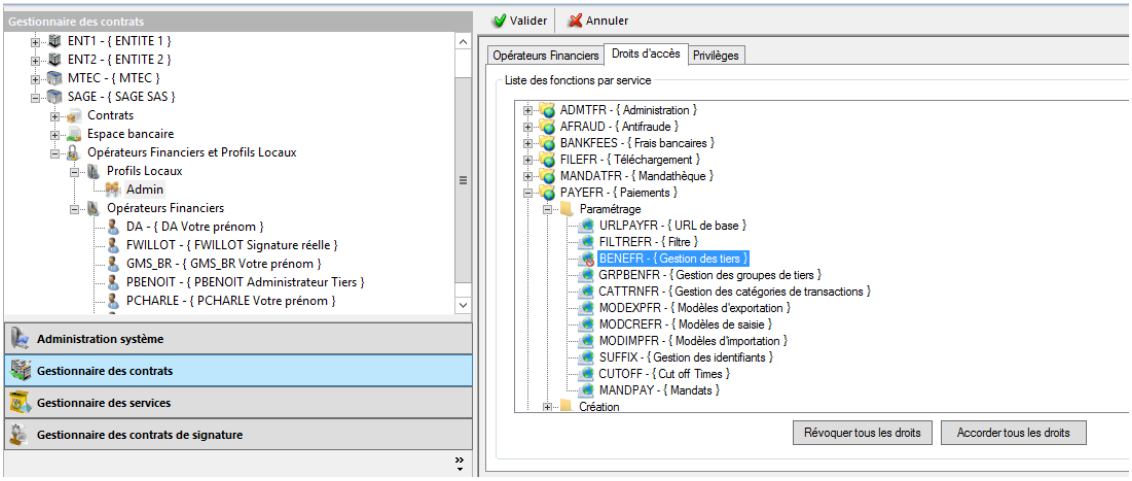


Specification of the minimum right level to access Third Party Management

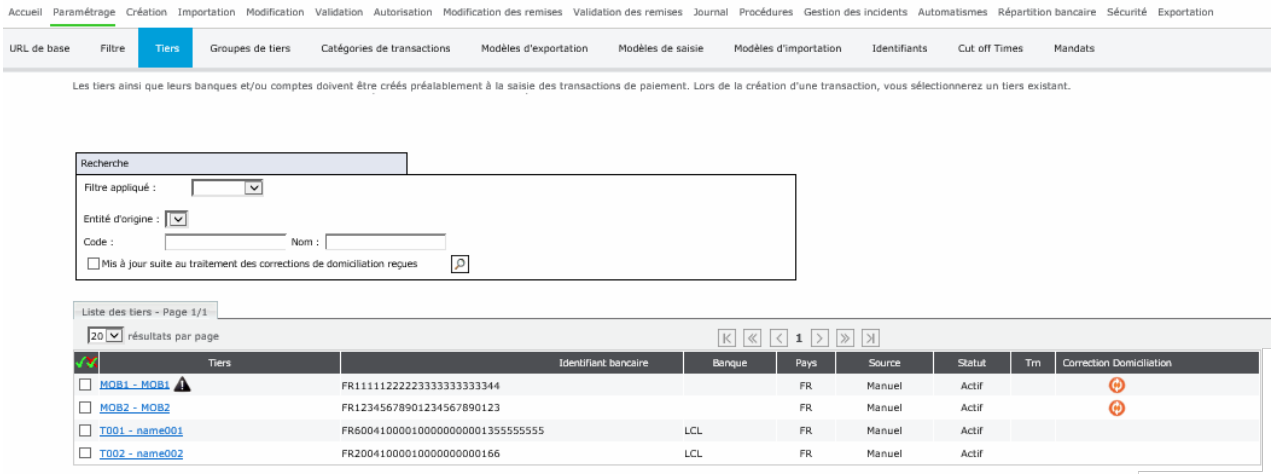
©Sage 2018



Specification of the access right to Third Party Management



Specification of the access restriction to Third Party Management

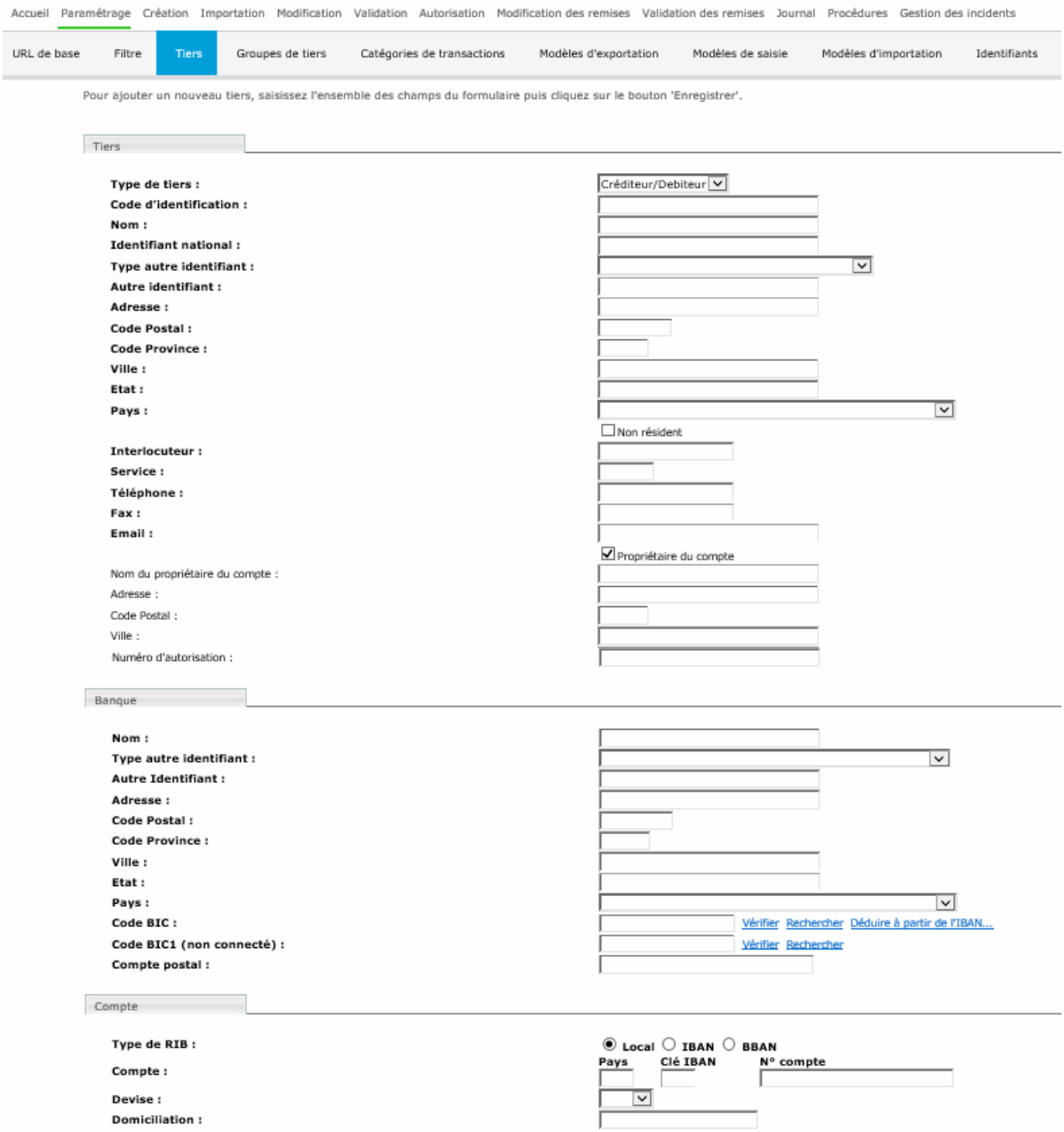


Third party list provided to users with more than access right

©Sage 2018

Personal Data and Associated Processing

Personal Data are:



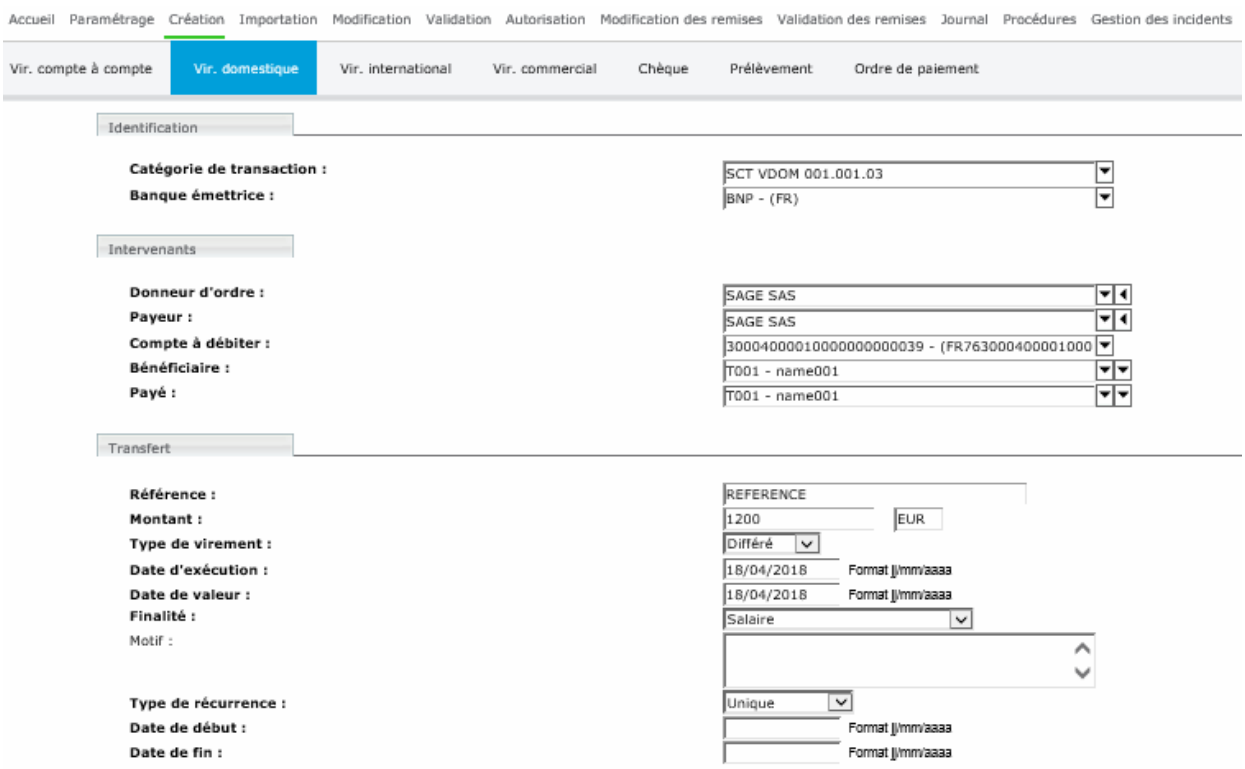
Purpose of Data Processing

The processing activities using Third Parties enable payments and receipts depending on the transfer type used and the third party category.

Payment Management

The various payment types managed in **Sage XRT Business Exchange** are based on the third party fields used for remittance generation.

For example, in Domestic Transfers, third party details are included into the transactions if the corresponding third party is involved in them.



Manual Entry of Domestic Transfer

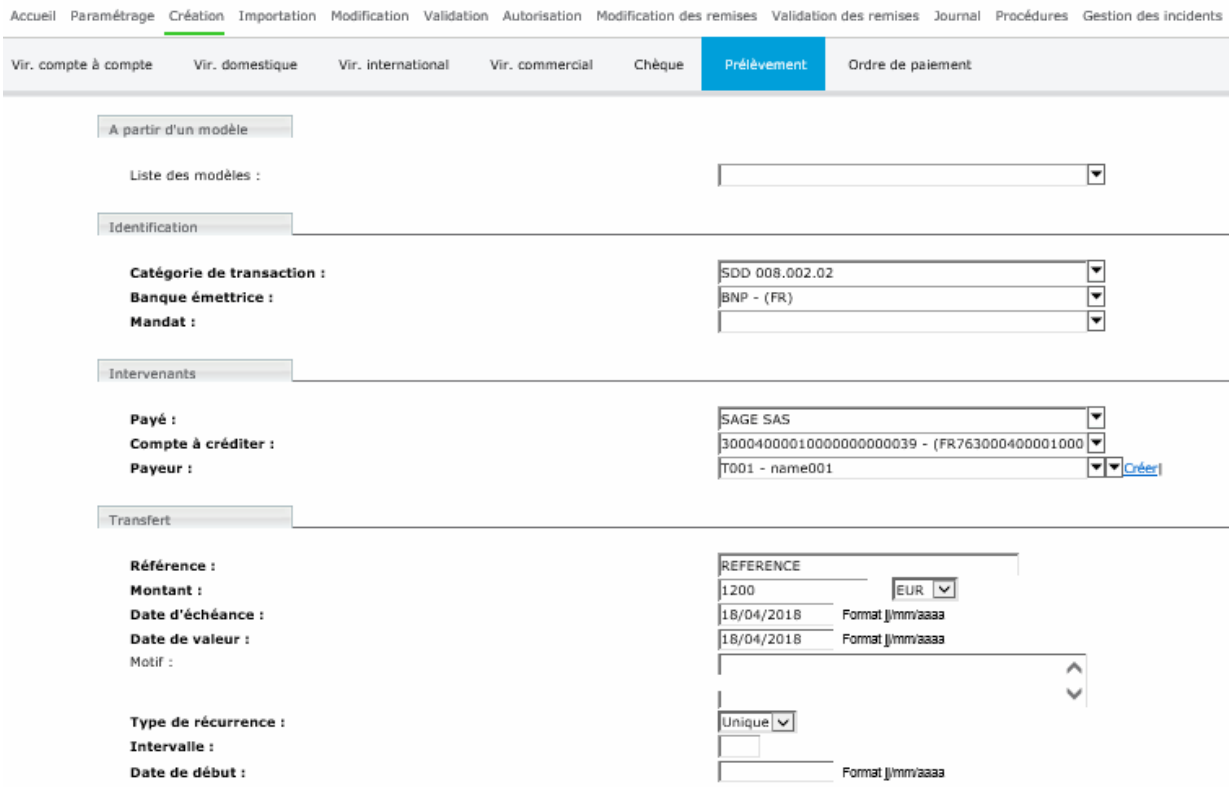
Confirmation of Domestic Transfer Record

©Sage 2018

Receipt Management

The various receipt types managed in **Sage XRT Business Exchange** are based on the third party fields used for remittance generation.

For example, in Domestic Direct Debits, third party details are included into the transactions if the corresponding third party is involved in them.

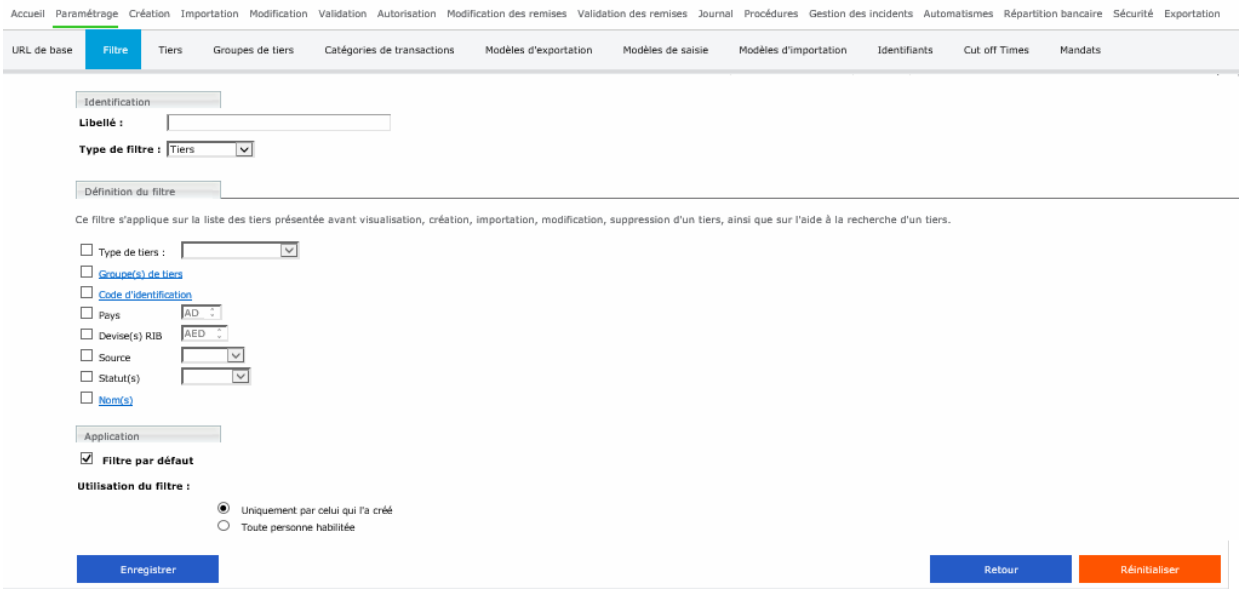


Manual Entry of Direct Debit

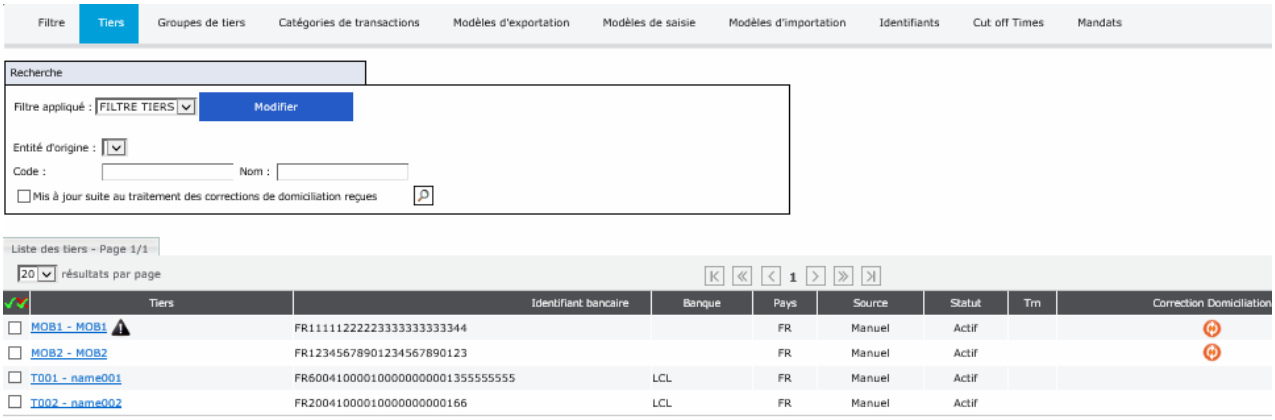
©Sage 2018

Third Party Management

The standard third party filter is used to manage Third Parties. Filters can be private, one-off/repetitive, or default.



Creation of third parties filter



Filtered list

Third parties can modify their personal data via an authorized user. Modification in account number may be notified to the corresponding third party through the setup of alerts on third party data.

Right of Erasure

Third parties can delete their personal data via an authorized user.

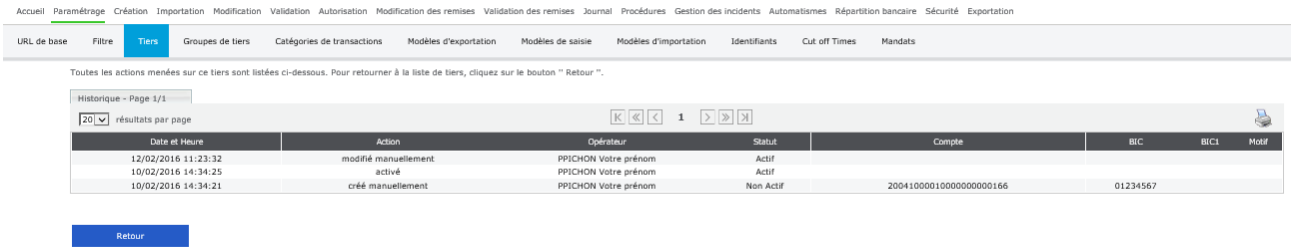
©Sage 2018

Third Party Deletion

Deleting third parties is possible only if:

- They are not associated with transactions.
- Their type is **One-Time** and the transactions associated with them have been purged.

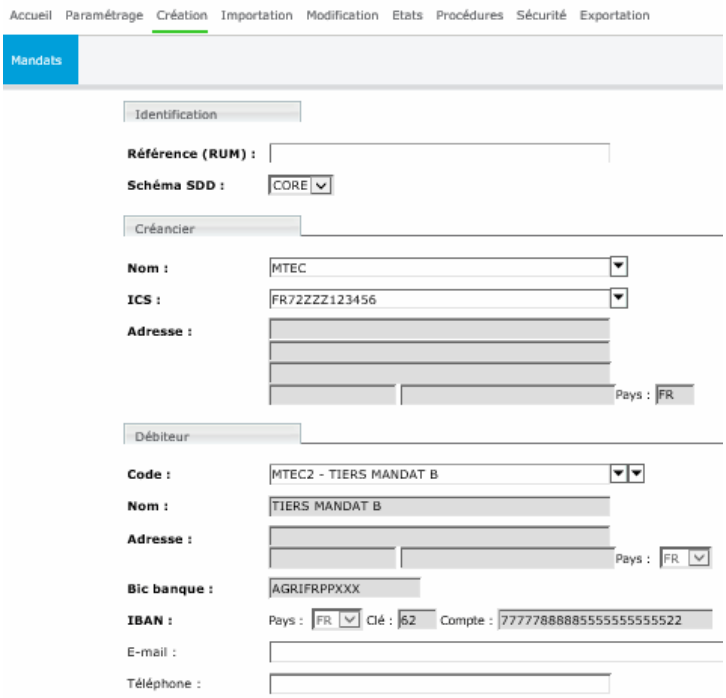
Authorized users have access to third party history.



Amendment Management

Third Party creation comes before Mandate creation. Mandates are associated with existing Third Parties.

They automatically retrieve the relevant data from the mandate **Debtor** tab.



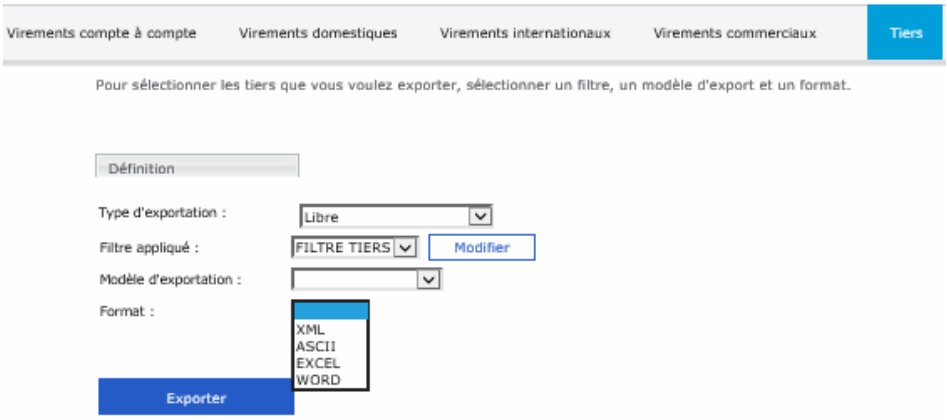
Creation of direct debit mandate

The modifications on third parties associated with mandates have an impact on the fields common to the third party (Debtor) and the associated mandate.

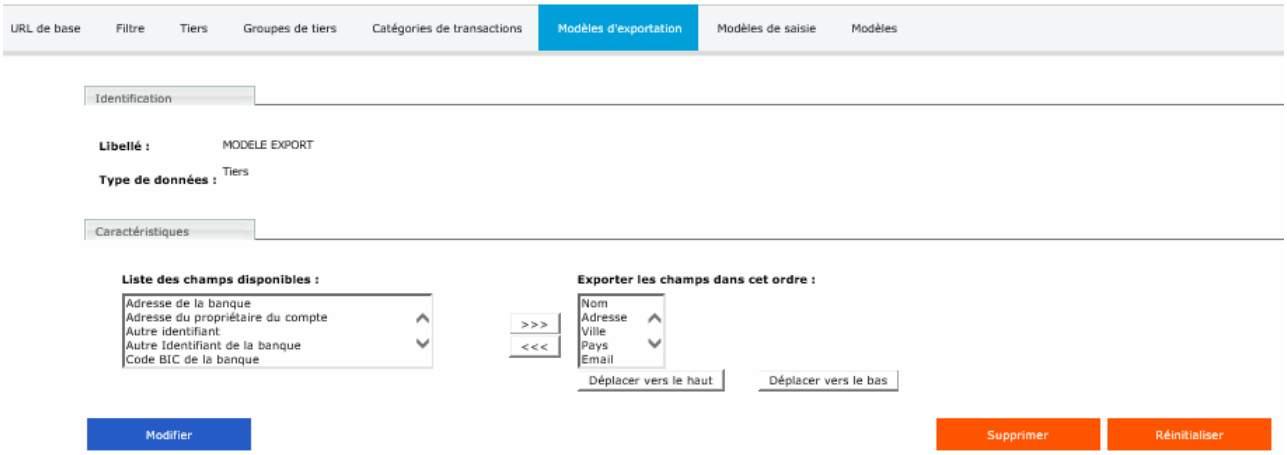
©Sage 2018

Export to Database

Third Party export uses a filter, a template (to specify the data to export) and a format.



Starting export



Setup of export template

Bank Branch Contacts

Purpose of Data Processing

The data from the **Contact** section of the branch are used during:

- Communications related to the electronic data exchange contracts
- Events impeding bank exchanges

Management

Application Administrators can create, modify and delete data of bank contacts.

©Sage 2018

Database Report

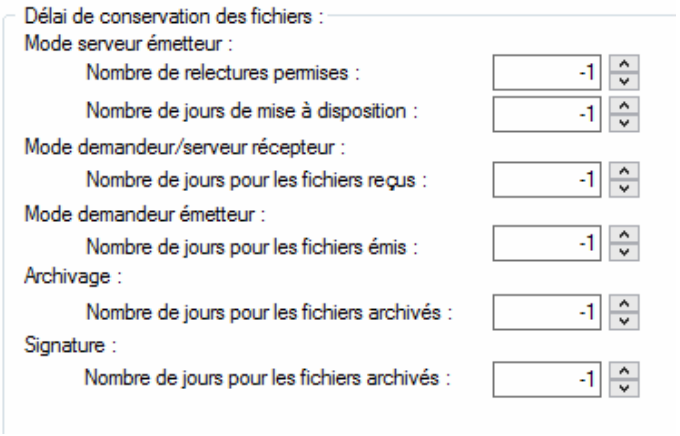
Every access to the bank contact data is registered in the administration audit (see § *Audit Functions for Access and Identities*).

Rights of Rectification and Erasure - Retention Period

You can modify and delete any personal data from your application to deal with an individual's request.

However, the applications process must be respected to complete modifications and erasures.

Important! All the local rules specify data retention periods.



Setup of retention periods for Communication personal data

In **Sage XRT Business Exchange** administration, you may set up automatic purges for:

- Received Files
- Archives

©Sage 2018

Additional Security Measures

To minimize regulation infringement and potential sanctions, some basic principles should be applied.

Even though the system and network security remains your responsibility, the solution platform offers you some tools:

- Standard web browsers and *http* or *https* protocol are used. Web technology guarantees a first layer of isolation between the web server and the workstation.
- Passwords are not transferred onto the network. Authentication system is based on standards. It may be a *Windows* connection checked through the *LDAP* (Lightweight Directory Access Protocol) or an authentication through certificate.
  For simplicity reasons, you can use a method based on users and encrypted passwords stored on the application web server. You may also double the authentication.
- Rights are managed at Entities' level, using function profiles associated with users. Access to contracts can also be granted or restricted from the services of each entity.

General Measures

Using https

The application is a web application accessible through an *http* or *https* connection. Although *http* is available, we recommend you use *https* for production instances, especially if your application is available from the internet.

Strengthening Passwords

If you use this authentication mode, do not forget to adopt a Password Management Policy that imposes strong passwords.

Strong passwords must:

- have at least six characters (the more characters, the stronger the password).
- use a combination of lowercase letters, uppercase letters, numbers, and symbols such as @ # $%!? &, etc.
- cannot contain the keyboard's own letter combinations such as *qwerty*.
- cannot contain the user's DBO.
- must not be used for other applications.

Securing Servers through Access Rights

The servers that host the application components contain sensitive setup files and data which remain vulnerable to internal threats.

The administrators must be the only users authorized to connect to the servers.

©Sage 2018

Make sure you granted them with the rights specific to the application administration on the relevant directories.

Important! The server administrators must be different from the application administrators.

Protecting Servers

The application servers must be based on the industry best practices.

Using Local Firewalls

Use local firewalls on your servers to lock all IP ports that are not required for the application operation nor for the user access.

Usually, when all the application components are installed on the same server, the application requires only *http* or *https* ports for its operation.

For multi-server installations, you must open the ports (or range of ports) required for the communication between components.

Securing Internet Architecture

Your architecture is the key to your security, especially if your application is available from the internet.

To connect your systems and make them available on the internet, you must answer the following questions:

- Which servers and ports must be seen from the outside?
- How the external requests are blocked, translated and redirected to these servers and ports?

This involves equipments such as:

- A firewall between your private network and the internet to block and redirect external requests to the relevant servers of your network.
- *DMZ* or demilitarized zone which is a physical or logical subnetwork that isolates your private network form the internet.

The firewall is the guardian of your *DMZ checkpoints*.

Note: These recommendations are relevant only if your application is visible on the internet. You do not need to set up any DMZ, nor firewall if you use your own private network.

Using Transparent Data Encryption

To further improve the security of your database, you can use *TDE (Transparent Data Encryption)*.

It enables you to encrypt the database.

©Sage 2018

Sage XRT Business Exchange 12.1 has been validated in the following environments:

- SQL Server 2016 TDE
- Oracle 12c TDE

Encrypting Data in Transit

You can use the *TLSTransparent Layer Security* standard for the communication between your application layer and your database.

The **ForceEncryption** option in **SQL Server** forces the protocol encryption which guarantees the data privacy.

Encrypting Database Backups

To further protect data, we recommend the encryption of database backups.

TDE automatically protects the backups since no file restoration nor attachment can be performed without the certificate.

Important! Keeping the certificate in a safe place is crucial, as is storing the backups in a different place than the certificate. For *Oracle*, you can use the native network encryption.

File System Security

The security of the file system for the servers must be implemented with the corresponding tools (antivirus, network access security, etc.).

Make sure these tools do not cause performance issues.

For example, avoid running a continuous antivirus scan on a database server.

Application Measures

Web Site and Application Signature

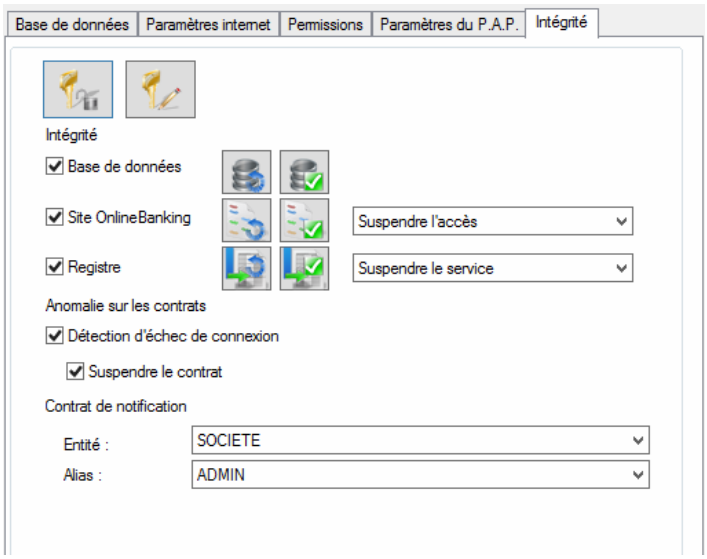
The code of your application has been signed. This signature certify that the program is legit and corresponds to the initial development, and that the integrity of the application binary files is intact.

To ensure **Online Banking**'s integrity, you can calculate a signature.

©Sage 2018

Additional Security Measures

The authorized administrator manages the calculation and controls the signature on the *master* site of **Sage XRT Business Exchange**.



Important! To activate the site integrity, you need to specify a passphrase. This passphrase must be kept in a safe place.

The application provides several authentication modes:

- **Use Windows NT integrated security**: the user is authenticated by its NT account. We recommend this authentication level.
- **Use a specific username and password**: the user is authenticated by a username and a password.
- **Authentication via X509 Certificate**: for the web client, the strong authentication consists of two phases:
    - Check of the certificate by searching the company's *Active Directory*
    - Challenge/Answer between the client and the authentication component to check client identity
- **Double authentication**: a second factor is used for user authentication to generate a single-use password.
- **SageID**

Authorizations

A single user has access to one or more entities. They are associated with a profile which defines their access rights and privileges: viewing lists, entering data, validation, administration and signature.

Import packages determine user rights.

Specific authorizations can be set up for users and signatories on each bank contract (contract access, report access, archiving and exporting rights).

©Sage 2018

This enables you to differentiate access rights to sensitive data for each entity and user.

Important! Make sure you continue applying these rules in the future. Keep them as simple as possible while enforcing your security policy.

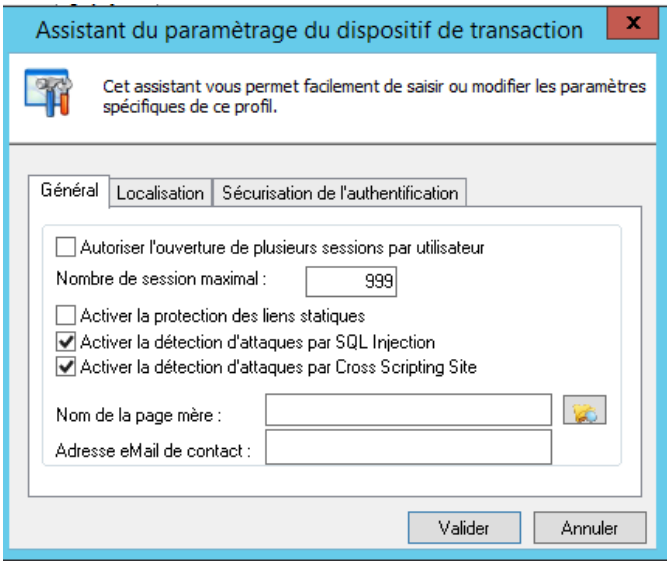
Protection against Attacks

Certain cyber attacks may jeopardize your data and domain security.

SQL injection attacks try to insert nefarious SQL statements into an entry field for execution which can compromise the application security.

Cross-site scripting is a type of computer security vulnerability which enables attackers to inject client-side scripts into web pages.

You can activate the options of attack detection in the transaction service.

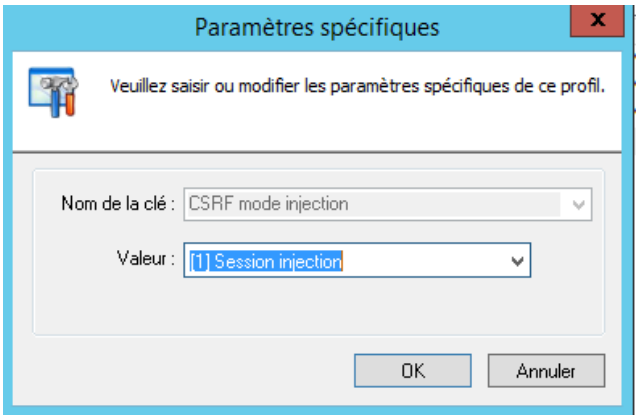


In *Cross-Site Request Forgery*, attackers who can find a reproducible link that executes a specific action on the target page while the victim is logged in there, can embed such link on a page they control and trick the victim into opening it.

©Sage 2018

Additional Security Measures

Enable the option in the service's specific parameters.



DTD attacks are vulnerabilities on *XML* parsers.

These vulnerabilities have already been used for attacks through denial of service. They can also provide the file content through the integration of an external entity.

The application code uses the *XSL.NET* compiler of the latest generation.

Website Access Frequency

You can define a calendar to control the legitimacy of the connections.

E.g.: Access to **Online Banking** website restricted on week-ends.

For Further Information

Setting up all these additional Security Measures requires technical skills and feedbacks which our consulting teams can provide you with.

Do not hesitate to contact them if you want to apply these recommendations.

©Sage 2018

Disclaimer

The information on GDPR provided hereby is intended as advice of a general nature for information purposes and is not to be construed as professional nor legal advice. *Sage* cannot guarantee the provided information exactly reproduces an officially adopted text. In case of dispute, the Official Journal of the European Union prevails.

While we have made every effort to ensure that the information provided is correct and up to date, the information is delivered on an *as is* basis without any warranties, express or implied. *Sage* will not accept any liability for errors or omissions and will not be liable for any damage (including, without limitation, damage for loss of business or loss of profits) arising in contract, tort or otherwise from the use of or reliance on this information or from any action or decisions taken as a result of using Information.

Our products include functions that could help and accompany users to comply with the GDPR. However, we would like to draw your attention to the fact that the sole use of our products does not guarantee your compliance with the GDPR.

The information provided hereby is not to be construed as professional nor legal advice, if you need more advice on GDPR compliance, you should consult a suitably qualified professional.

©Sage 2018