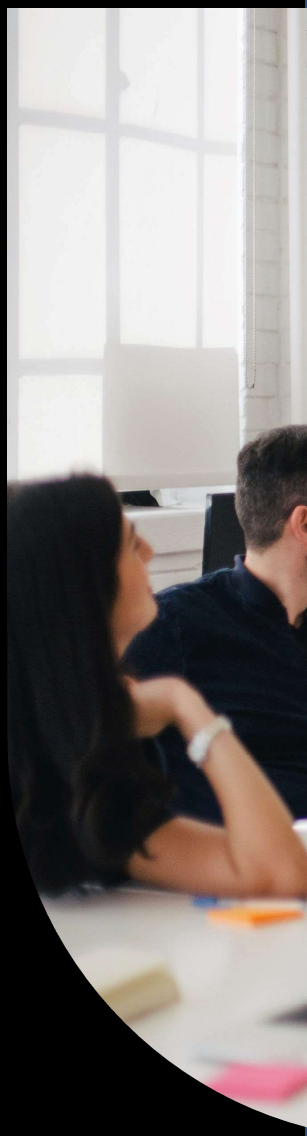
Sage XRT Solution Common Services

Guide utilisateur Common Services

Version 2026



Sommaire

Installation 5

Présentation 5

Ajouts de la version 5.1.100 ..... **Erreur ! Signet non défini.**
Ajouts de la version 5.2 ..... **Erreur ! Signet non défini.**
Ajouts de la version 5.3 ..... **Erreur ! Signet non défini.**
Ajouts de la version 6.0 ..... **Erreur ! Signet non défini.**
Ajouts de la version 6.1 ..... **Erreur ! Signet non défini.**

Recommandations 5

Déploiement 6

Configuration 1 6
Configuration 2 6
Configuration 3 8
Configuration avec SAGE XRT Solution Advanced Treasury et SAGE XRT Solution Advanced Signature / Communication 8

Exemple d'éléments mis en œuvre – Gestion des paiements depuis SXA 9

Workflow et traitements 9
SAGE XRT Solution Advanced Treasury 9
SAGE XRT Solution Common Services 9
SAGE XRT Solution Advanced Communication & Signature 10

JAVA Open Source 10

Tenants Management 14

Tenants 14

Création 14

Bases de données 18

Mise à jour 18
SQL Server et Profils non-SYSADMIN 20
Modifications 21

Première connexion 22

Utilisateurs 22

Ajout à un tenant 23
Modification 25

XRT Solution Common Administration Services 26

Service d'authentification 27

Configuration 27
Paramétrage de la page de connexion 27

Service d'Administration 29

Configuration 29

Connexion ... 30
Licences ... 31
Création ... 32
Modification ... 32
Suppression ... 33
Application ... 33
Paramétrage authentification ... 33
Authentification Windows NT ... 34
Authentification UMAPI ... 34
Authentification LDAP ... 35
Authentification SAML ... 37
Double Authentification ... 39
Règles des mots de passe ... 40
Activation des données et règle des 4 yeux ... 40
Compte utilisateur ... 45
Profils ... 47
Création ... 48
Droits d'accès ... 50
Duplication ... 51
Modification ... 52
Suppression ... 52
Activation ... 52
Désactivation ... 52
Sites ... 52
Création ... 52
Modification ... 54
Suppression ... 54
Activation ... 54
Désactivation ... 54
Mon compte ... 54
Audits et logs ... 55
Paramétrage ... 55
Audit ... 57
Log ... 59
XDLO (obsolète) ... 60
SAGE XRT Solution Common Services ... 61
Configuration ... 61
Connexion ... 61
Librairie Sage.FCS.Client ... 63
Utilisation ... 63
Description des méthodes intégrées ... 64
Application sage.fcs.apifmt.exe ... 67
Installation ... 67

Configuration 67
Service d'authentification 67
Service de transformation des données 68
Permissions 68
Utilisation 69
Paramètres de base 69
Exemples 71
Application sage.fcs.pwdencode.exe 74
Installation 74
Utilisation 74
Encodage en base64 uniquement 74
Chiffrement et encodage en base64 75
Description du fichier de configuration 75
Utilisation de l'exécutable 76
Annexes 77
Configuration SCAS 77
Configuration SCPS 77
Configuration SCDTS 77
Configuration SXABCP 77
Configuration SXAPDS 77

Installation

Présentation

La version 2026 de **SAGE XRT Solution** correspond à la version 9 de **SAGE XRT Common Services**.

Seules persistent dans une interface *Win32* la gestion des tenants (ex. : **workgroups**) et la partie *DBInstaller*.

Recommandations

Sage XRT Common Services	Recommandations
Serveur	• Moteur de base de données : SQL Server 2017, SQL Server 2019 • Serveur Microsoft : IIS 10 ou supérieur • Version JRE 8 (64 bits) pour le bon fonctionnement de **XRT Solution Bank Formats Library** • Activation de l'exécution du *PowerShell* : *PS> Set-ExecutionPolicy -ExecutionPolicy RemoteSigned*
Poste client	Version du provider SQL identique à celle du serveur

Important !

L'installation de SAGE XRT Solution Common Services sur chaque poste client n'est désormais plus nécessaire lors de l'installation des produits SAGE XRT Solution Advanced Communication & Signature et SAGE XRT Solution Advanced Treasury.

SAGE XRT Solution Common Services doit être installé uniquement sur le poste serveur.

Pour SAGE XRT Solution Advanced Communication & Signature, SAGE XRT Solution Common Services doit être installé sur la même machine que le serveur de communication.

Pour SAGE XRT Solution Business Exchange, tant que le wrapper sage.fcs.client n'est pas intégré, SAGE XRT Solution Common Services doit être installé sur la même machine que SAGE XRT Solution Business Exchange.

Lorsqu'un tenant est créé avant l'installation d'autre produit, la base de données de SAGE XRT Solution Common Services doit être mise à jour.

Déploiement

Configuration 1

Dans le cas où tout est installé sur la même machine, il est recommandé de suivre l'ordre d'installation suivant :

- **SAGE XRT Solution Bank Formats Library**
- **SAGE XRT Solution Common Services**
- **SAGE XRT Solution Advanced Communication**
- **SAGE XRT Solution Advanced Signature**
- **SAGE XRT Solution Advanced Treasury**

Vous devez utiliser :

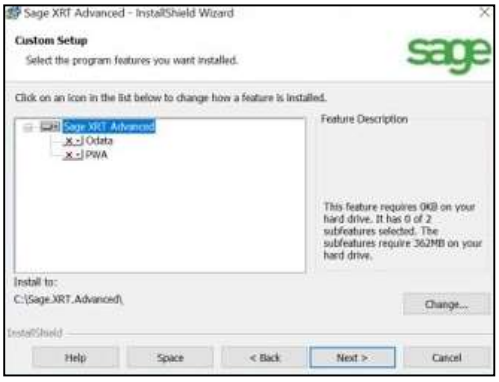
- La procédure d'installation **Complète** de **SAGE XRT Solution Common Services**
- La procédure d'installation **Complète** de **SAGE XRT Solution Advanced Communication**
- La procédure d'installation **Complète** de **SAGE XRT Solution Advanced Signature**

La base de données de **SAGE XRT Solution Common Services** doit être mise à jour avec le *DBInstaller*.

- La procédure d'installation **Custom** ou **Complète** de **SAGE XRT Solution Advanced Treasury**.

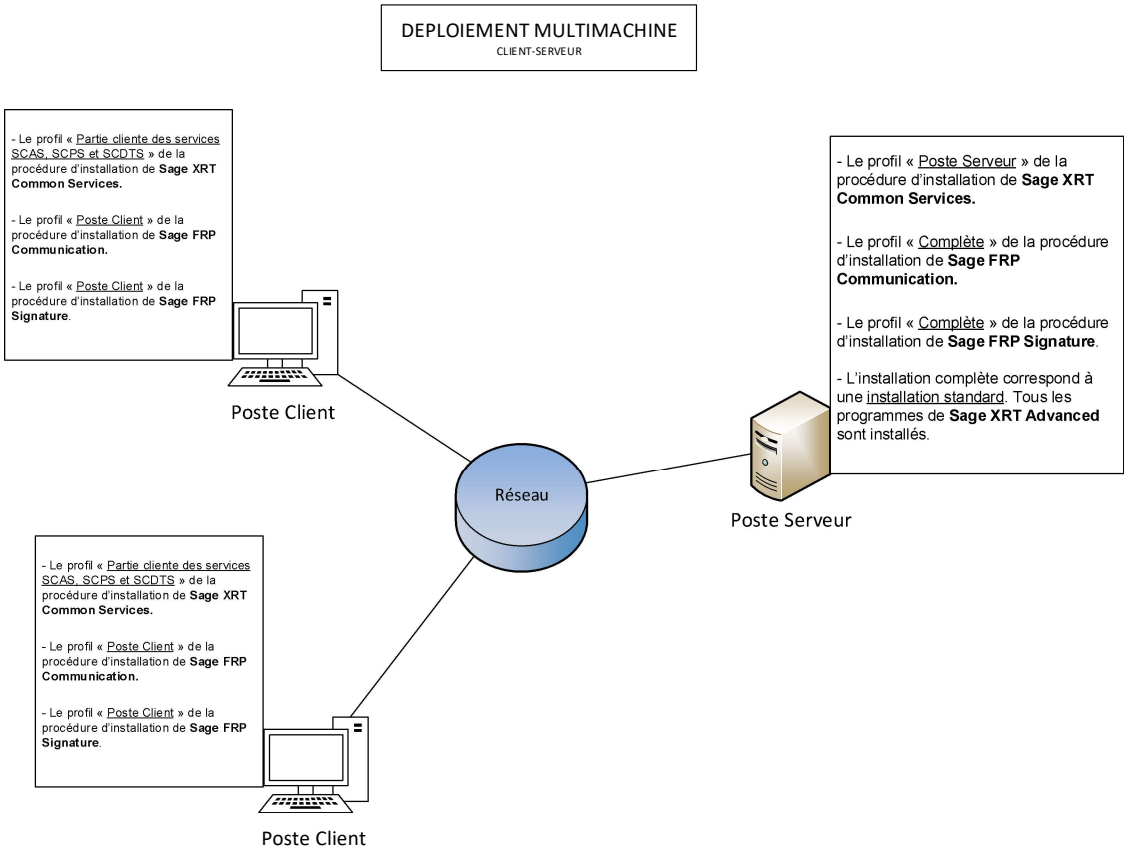
L'installation **Complète** correspond à une installation standard où tous les programmes de **SAGE XRT Solution Advanced Treasury** sont installés.

L'installation **Custom** ouvre la fenêtre suivante.



Configuration 2

Cette configuration concerne l'installation standard dite *on-premise* (sur site).



Dans le cas de **1 à n** machine cliente et une machine serveur, sur la machine cliente, vous devez utiliser :

- La procédure d'installation Partie cliente des services SCAS, SCPS et SCDTS de SAGE XRT Solution Common Services
- La procédure d'installation Poste Client de **SAGE XRT Solution Advanced Communication**
- La procédure d'installation Poste Client de **SAGE XRT Solution Advanced Signature**

Et sur la machine serveur :

- La procédure d'installation Poste Serveur de **SAGE XRT Solution Common Services**
- La procédure d'installation Complète de **SAGE XRT Solution Advanced Communication**
- La procédure d'installation Complète de **SAGE XRT Solution Advanced Signature**
- La procédure d'installation Complète ou Custom de **SAGE XRT Solution Advanced Treasury**.

L'installation complète correspond à une installation standard. Tous les programmes de **SAGE**

XRT Solution Advanced Treasury sont installés.

La base de données de **SAGE XRT Solution Common Services** doit ensuite être mise à jour avec le *DBInstaller*.

Et sur la machine serveur :

- La procédure d'installation Poste Serveur de **SAGE XRT SolutionCommon Services**
-

Configuration 3

Dans le cas de **1 à n machines clientes et une machine serveur** pour **SAGE XRT Solution Advanced Communication/Signature** et une machine serveur pour **SAGE XRT Solution Common Services**, sur la machine cliente, vous devez utiliser :

- La procédure d'installation Partie cliente des services SCAS, SCPS et SCDTS de **SAGE XRT Solution Common Services**
- La procédure d'installation Poste Client de **SAGE XRT Solution Advanced Communication**
- La procédure d'installation Poste Client de **SAGE XRT Solution Advanced Signature**

Sur la machine serveur de **SAGE XRT Solution Advanced Communication & Signature**, vous devez utiliser :

- La procédure d'installation Poste Client de **SAGE XRT Solution Common Services**
- La procédure d'installation Complète de **SAGE XRT Solution Advanced Communication**
- La procédure d'installation Complète de **SAGE XRT Solution Advanced Signature**

Sur la machine serveur de SAGE XRT Solution Common Services, vous devez utiliser :

- La procédure d'installation Poste Serveur de **SAGE XRT Solution Common Services**
- La procédure d'installation Scripts de base de données de **SAGE XRT Solution Common Services**
- La procédure d'installation Scripts de base de données de **SAGE XRT Solution Advanced Signature**

La base de données de **SAGE XRT Solution Common Services** doit ensuite être mise à jour avec le *DBInstaller*.

Configuration avec SAGE XRT Solution Advanced Treasury et SAGE XRT Solution Advanced Signature / Communication

Dans le cas d'une installation avec **SAGE XRT Solution Advanced Treasury** et **SAGE XRT Solution Advanced Communication & Signature**, suivez la procédure qui suit.

1. Activez *powershell* : *Set-ExecutionPolicy - ExecutionPolicy RemoteSigned -Scope LocalMachine*

2. Dans le fichier de config *Sage.SCDTSServer.Service.exe.config*, paramétrez l'URL du service **REST SXCS** pour la demande de statuts et activez le traitement : action=**YES**.

3. Paramétrez l'URL du service **REST SXCS** pour la demande d'ajout.

En cas de migration de **SAGE XRT Solution Common Services** 3.9 vers 6.0, l'utilisateur standard *XRT* pré-paramétré dans les fichiers de configuration des services n'existe pas encore. Vous devez soit le créer, soit modifier les fichiers de configuration en utilisant un nom d'utilisateur qui existe.

Exemple d'éléments mis en œuvre – Gestion des paiements depuis SXA

Workflow et traitements

Les paragraphes de ce chapitre présentent le workflow d'un paiement et ses traitements par produit, ainsi que les actions manuelles à effectuer.

Produit	Acronyme
SAGE XRT Solution Advanced Treasury	SXA
SAGE XRT Solution Common Services	SCS
SAGE XRT Solution Advanced Communication & Signature	SXCS

SAGE XRT Solution Advanced Treasury

L'utilisateur initie un paiement depuis la plateforme **SXA**.

SXA génère une demande au format *JSON* qu'elle transmet ensuite à **SCS** via le protocole **API Rest**.

SXA suit cette demande (toujours via **API Rest**) et tient informé en temps réel l'utilisateur du statut du paiement et donc de son cheminement.

SAGE XRT Solution Common Services

Le service **SCDTS** reçoit la demande de paiement de **SXA** et fournit un ID de transaction à **SXA** pour les futures demandes de statut. Par la suite, deux étapes s'enchainent :

- La conversion du flux *JSON* initial en fichier bancaire.
- L'enrichissement des données initiales si l'option a été activée.

Ce fichier sera ensuite posté sur le module de **Signature**.

Important ! Une phase d'initialisation manuelle du flux des paiements est nécessaire par banque (session/connexion). Elle est réalisée en effectuant le premier envoi d'un paiement depuis SXA. Ensuite il faut modifier la correspondance dans la table de transcodage EXITPOSTGEN.

Dans le fichier *Sage.SCDTSServer.Service.exe.config,* vous devez effectuer les actions suivantes :

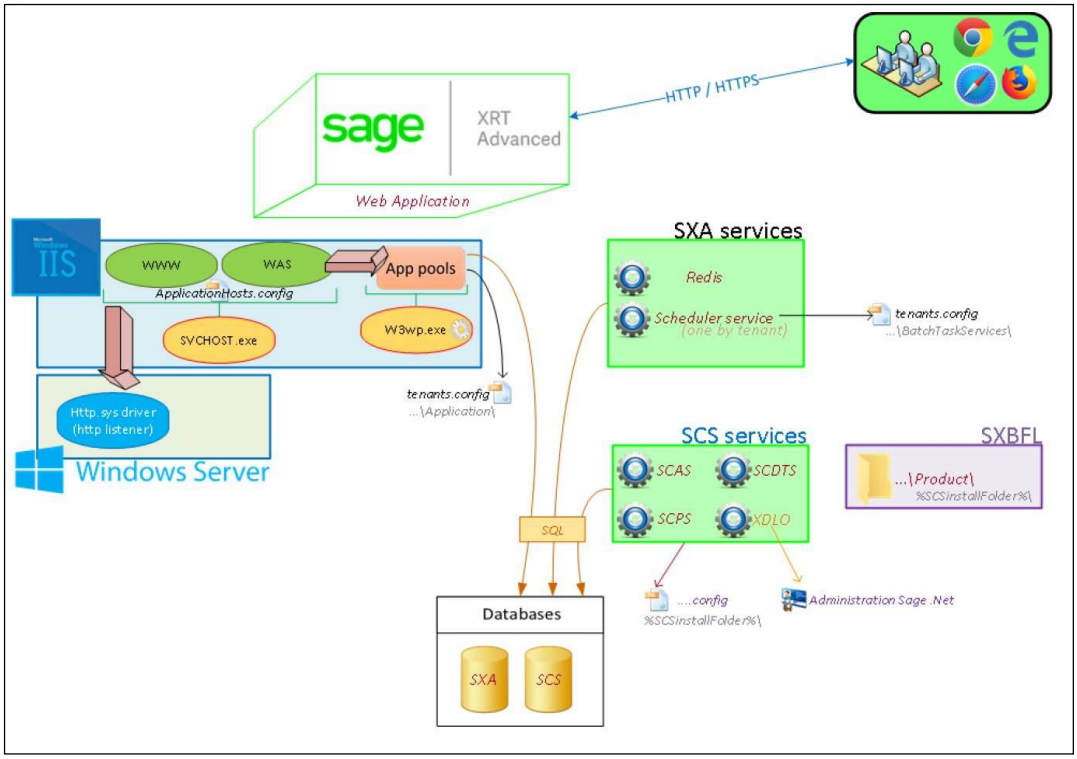
- Paramétrer l'URL du service REST SXCS pour la demande de statut
- Activer le traitement : action=YES
- Paramétrer l'URL du service REST SXCS pour la demande d'ajout

SAGE XRT Solution Advanced Communication & Signature

Le service **ComSignAPI** prend en charge la demande en provenance de **SCDTS** pour son insertion dans le flux de travail correspondant au contrat sélectionné.

Important ! N'oubliez pas que sur le poste client dans une configuration multi-machine, vous devez paramétrer l'adresse du service LAD et les adresses des services SCDTS, SCAS et SCPS dans le fichier <INSTALLPATH_DE_SCS_CLIENT>\sage.fcs.client.dll.config.

Schéma d'échange des flux à partir de la solution d'initiation des Paiements de **SAGE XRT Solution Advanced Treasury**

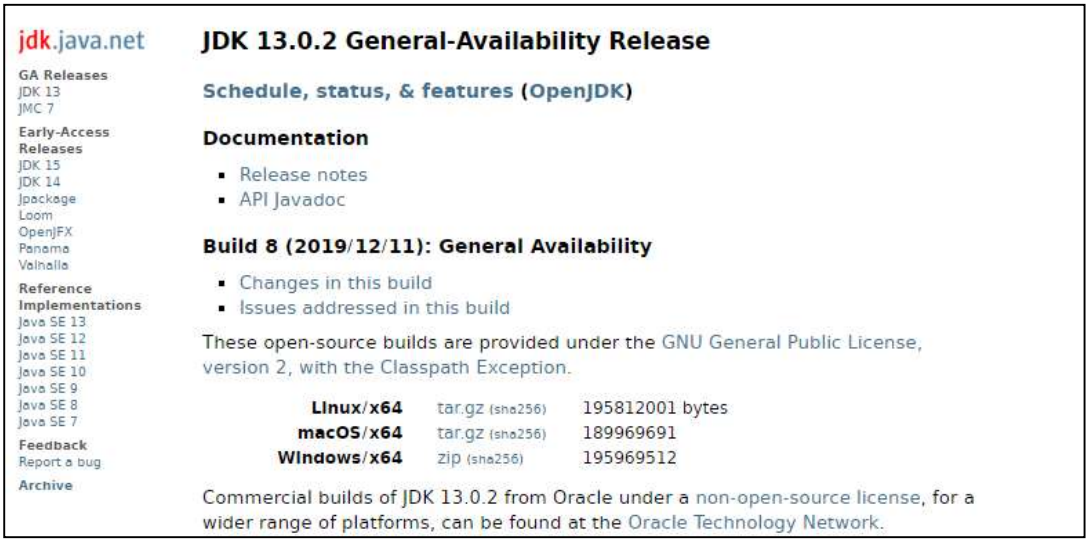


JAVA Open Source

Désinstallez le programme *Java* existant.

Testez grâce à une ligne de commande la génération d'un fichier bancaire à partir d'un fichier intermédiaire. Ce test aboutit au message d'erreur : **jvm.dll required for Sun JDK**.

Téléchargez le fichier *Windows/x64* zip de la dernière version disponible depuis le site **https://jdk.java.net** : *openjdk-13.0.2_windows-x64_bin.zip* (187 Mo).

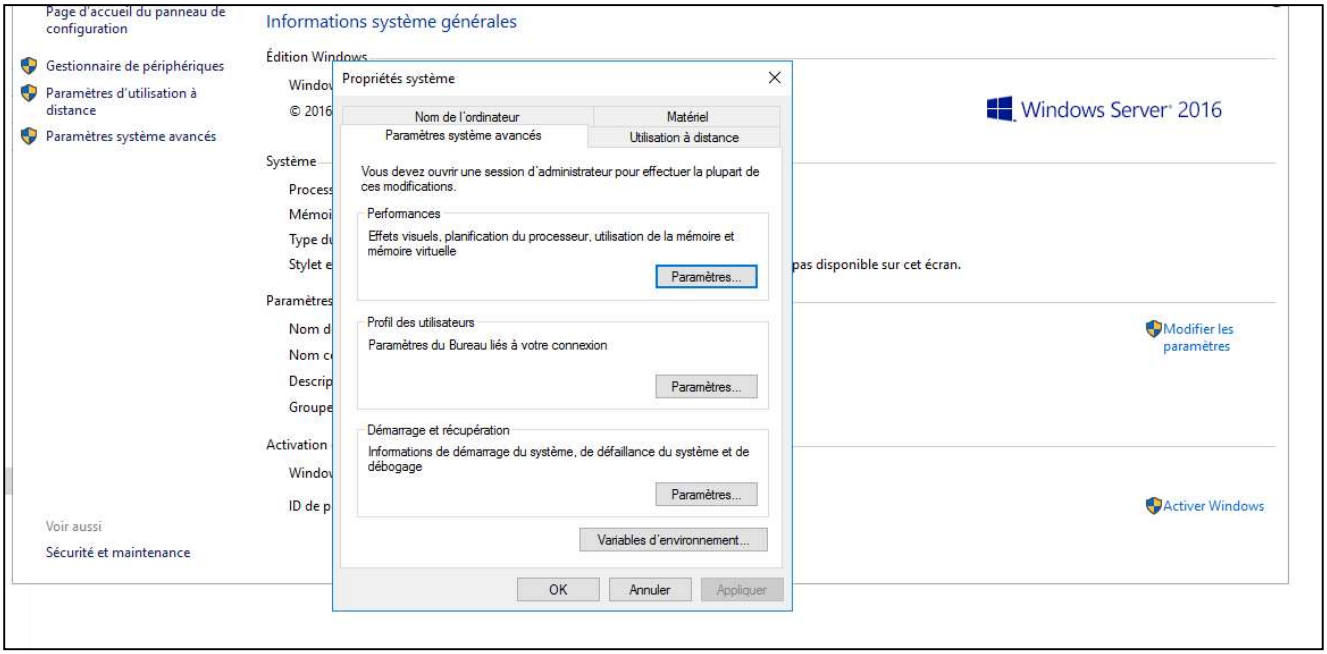


Créez un répertoire **JAVA** sous **C:\Programmes** et dézippez le zip téléchargé dans ce nouveau répertoire : un dossier *jdk* est généré.

Vous devez créer des variables d'environnement.

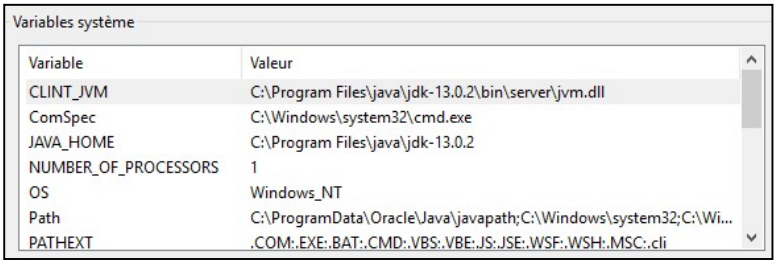
Dans l'explorateur *Windows*, ouvrez par un clic droit sur **Ce PC** le menu contextuel, puis cliquez sur **Propriétés**.

Dans le panneau de gauche, sélectionnez **Paramètres système avancés**. Cliquez sur **Variables d'environnement ...**



Dans la rubrique **Variables utilisateur pour Administrateur**, double-cliquez sur la variable **PATH**, puis sélectionnez **Nouveau** et ajoutez la variable **C:\Program Files\java\jdk-13.0.2\bin**.

Dans la rubrique **Variables système**, cliquez sur **Nouvelle**.
Créez la variable **JAVA_HOME** avec la valeur *C:\Program Files\java\jdk-13.0.2*.
Créez la variable **CLINT_JVM** avec la valeur **C:\Program Files\java\jdk-13.0.2\bin\server\jvm.dll**.



A partir d'une nouvelle ligne de commande, testez la génération d'un fichier bancaire à partir du fichier intermédiaire : le message d'erreur a disparu.

Sécurité

Par défaut au niveau du fichier de config du SCAS, la clé "redirectwhitelisthost"contient la valeur *.

Pour des raisons de sécurité, il est nécessaire de modifier cette valeur pour indiquer une liste blanche d'url exhaustives. Cela permet de sécuriser le CORS.

<add key="redirectwhitelisthost"
value="*,localhost.olbcl01,localhost.sxacl01,localhost.olbcl02,localhost.sxacl02"/>

Il est fortement conseillé d'utiliser l'authentification double facteur quelque soit le type d'authentification.

Il est fortement conseillé de laisser les balises "showfriendlymessage" à NO

Pour tous les services (SCAS, SCDTS, SCPS ...)

Il est fortement conseillé de laisser "helpEnabled" à NO

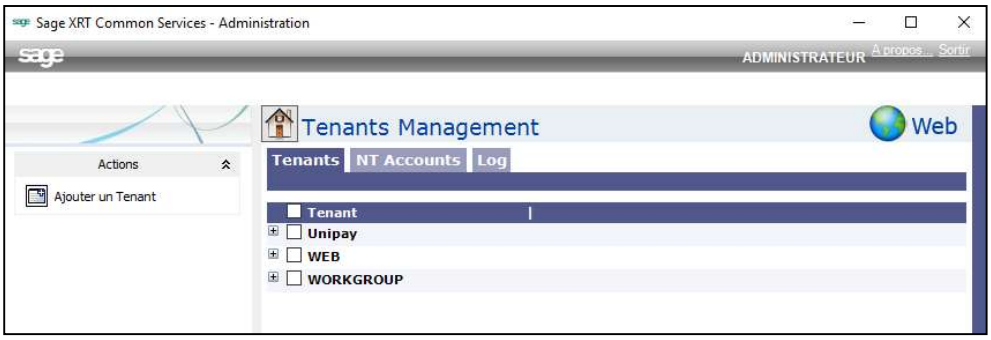
Tenants Management

Tenants

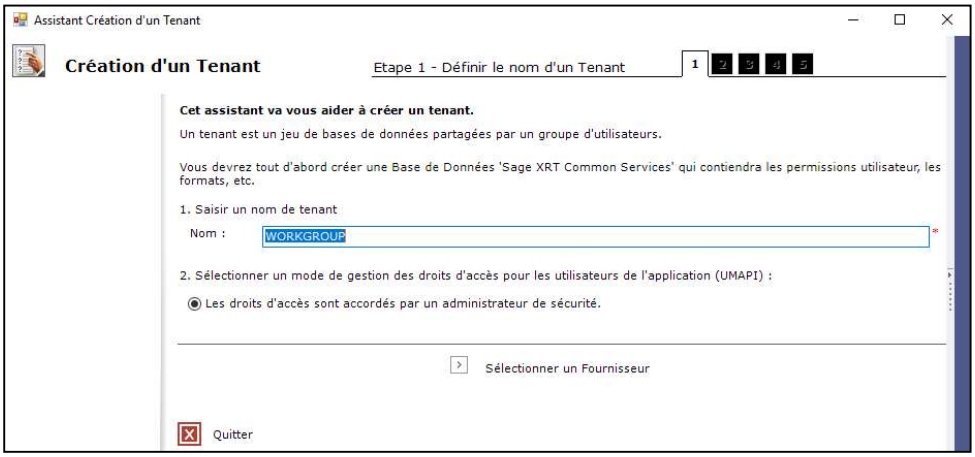
Dans le cas d'une première installation de SAGE XRT Solution Common Services, aucun tenant n'existe : la première étape consiste à créer un ou plusieurs tenants en fonction du type de base de données utilisée (SQL Server ou Oracle).

Création

Dans le menu Démarrer, rendez-vous dans Programmes – Sage – Administration XRT .NET.
L'interface **Tenants Management** s'affiche.



Cliquez sur le lien **Ajouter un tenant** pour lancer l'Assistant **Création d'un Tenant**.



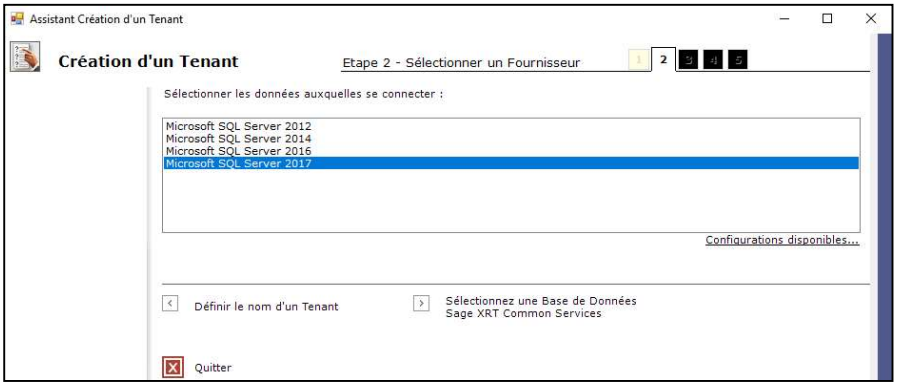
Note : Lorsqu'aucun tenant n'est défini, l'Assistant Création d'un Tenant s'affiche immédiatement à l'écran.

Saisissez un nom de tenant dans le champ **Nom**. Le nom par défaut est **WORKGROUP**.

Définissez le mode de fonctionnement de la gestion des droits d'accès des utilisateurs aux applications **Sage XRT Solution**.

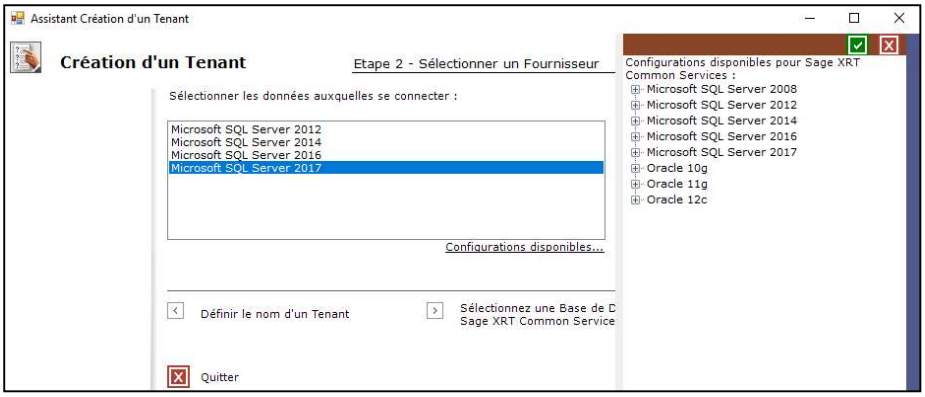
Note : A partir de la version 5.0, la validation des opérations par un administrateur de sécurité de niveau 2 a été remplacée par la fonctionnalité d'activation des données. Cette activation peut être requise ou non selon le paramétrage effectué.

Cliquez sur le lien **Sélectionner un Fournisseur**.



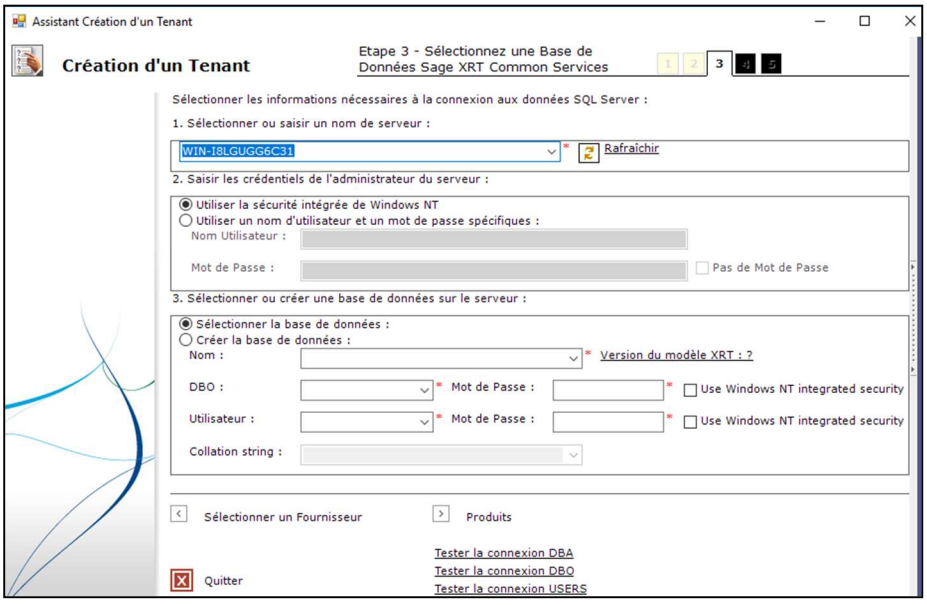
Sélectionnez dans la liste, le serveur ou client de base de données installé.

Cliquez sur **Configurations disponibles** pour visualiser le détail des serveurs ou clients de base de données installés sur la machine et les opérations autorisées (création et mise à jour).



Cliquez sur pour fermer la page et revenir à la page de sélection des fournisseurs d'accès aux bases de données.

Cliquez sur **Sélectionnez une Base de Données SAGE XRT Solution Common Services**.



Saisissez le nom du serveur sur lequel la base de données doit être créée. Les caractères possibles pour indiquer ce serveur sont :

- (local)

- (LOCAL)
- .
- *nom serveur*

Le bouton **Rafraîchir** permet d'obtenir la liste des serveurs *Microsoft SQL Server* connectés au réseau de l'entreprise.

Suivant le type d'authentification utilisé par le DBA (Administrateur de base de données) pour se connecter au serveur de bases de données, sélectionnez une des options qui suivent.

- **Utiliser la sécurité intégrée de Windows NT :** le DBA est authentifié grâce à son compte NT.
- **Utiliser un nom d'utilisateur et un mot de passe** : le DBA est authentifié grâce à un nom d'utilisateur et un mot de passe.

Note : Cliquez sur le lien Tester la connexion DBA au bas de la page pour vérifier les identifiants du DBA.

Vous avez ensuite deux possibilités :

- **Sélectionner la base de données** si vous souhaitez travailler sur une base de données existante.
    - Sélectionnez la base de données dans la liste déroulante. Les bases de données existantes sont actualisées au premier affichage de la liste.
    - Saisissez le mot de passe correspondant au nom du DBO (propriétaire de la base de données) affiché dans le champ **DBO** ou cochez la case **Use Windowd NT integrated security**. Le mot de passe proposé par défaut par l'assistant est : **password#2005**. Lorsque vous sélectionnez une base de données dans la liste, l'assistant recherche automatiquement le nom du propriétaire de celle-ci en utilisant le compte DBA.
    - Saisissez le mot de passe du compte **XRTUSERS** ou cochez la case **Use Windowd NT integrated security**. Le mot de passe par défaut est : **password#2005**

Note : Cliquez sur le lien Tester la connexion DBO en bas de la page pour vérifier les identifiants du DBO.

- **Créer la base de données** si vous souhaitez créer une base de données.
    - Saisissez un nom de base de données. L'assistant vérifie qu'aucune base ne porte ce nom lorsque vous cliquez sur **Créer/Modifier les modèles**.

Important ! Le nom de la base de données ne doit comprendre aucun espace, ni caractère spécial (, ?, \, /, etc.).*

    - Saisissez les identifiants du propriétaire de la base de données. L'assistant propose par défaut un compte avec l'identifiant **XRT** et le mot de passe **XRT**. Il

crée, si nécessaire, le compte et lui affecte le rôle de **db_owner** sur la base.

- Sélectionnez la **Collation string** (chaîne d'interclassement) ou laissez par défaut **French_CI_AS** (pas de distinction entre majuscule et minuscule).

Cliquez sur **Produits**.

Configuration des unités logiques

L'assistant propose par défaut un scénario dans lequel les tables *filegroup* **DATA** et les index *filegroup* **INDEX** du modèle sont créés dans le *filegroup* **PRIMARY** (*filegroup* par défaut lors de la création d'une base de données *Microsoft SQL Server*).

Le panneau de propriétés vous permet de :

- Modifier le scénario proposé et installer les tables et les index dans deux *filegroups* différents (exemple : **XCS_DATA** et **XCS_INDEX**).
- Modifier les paramètres de création des *filegroups* (répertoire de stockage, taille initiale, taille limite, taux de croissance). Le répertoire de stockage doit exister pour que l'opération de création fonctionne correctement.

Important ! Les scripts modèle de Sage XRT Solution Common Services font référence à un filegroup logique DATA pour les tables et un filegroup logique INDEX pour les index.

Lors de l'exécution des opérations de création du modèle, l'assistant remplace ces noms logiques par les valeurs saisies dans le panneau de propriétés (PRIMARY dans le cas du scénario par défaut).

Si les groupes de fichiers cibles n'existent pas (par exemple : XCS_DATA et XCS_INDEX), ceux-ci sont automatiquement créés par l'assistant.

Cliquez sur **Créer/Modifier les modèles**.

Création et modification des modèles

La liste intitulée **Scripts à exécuter** contient l'ensemble des scripts utilisés pour la création du modèle **SAGE XRT Solution Common Services** :

- **createlogicalunits.sql** : Script de création des unités logiques. Une unité logique représente un *filegroup* dans le cas de la création d'une base de données *Microsoft SQL Server*
- **xl_configuration createxl_configuration.sql** : Script de création de la table dans laquelle est enregistrée la version du modèle
- **registerlogicalunits.sql** : Script d'enregistrement des unités logiques

Les scripts produit sont traités par la suite.

Suivant leur type, les scripts sont exécutés avec le compte du DBA ou du DBO.

Activez la case **Sélectionner les données à importer** et choisissez une langue dans la liste. Cette importation concerne les données (format *XML*) pour **APIFMT**, **TRANSCO** et **UMAPI**.

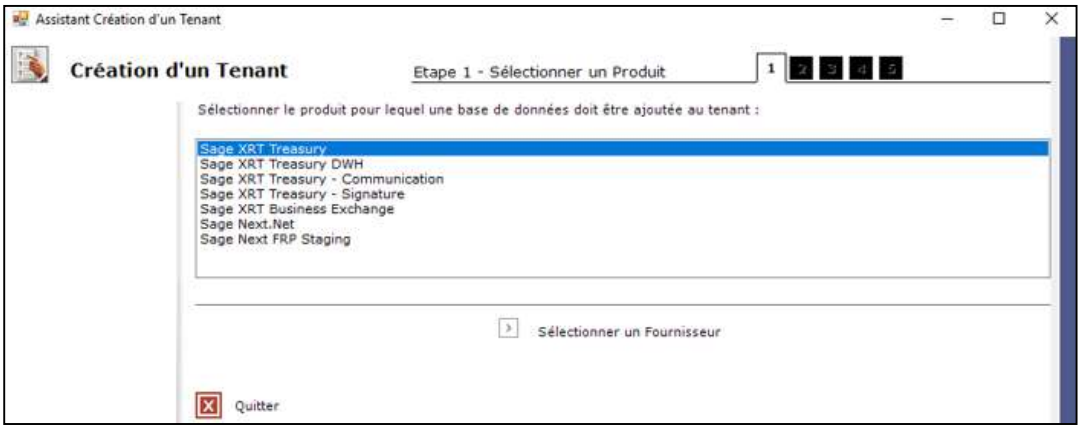
Cliquez sur **Valider toutes les étapes** pour procéder à l'exécution des opérations configurées dans les étapes 1, 2, 3, 4 et 5 de l'assistant.

Exécution des opérations

L'exécution peut durer quelques minutes. A ce stade, le modèle XCS est créé.

Vous pouvez quitter l'assistant Création d'un tenant en cliquant sur l'icône Quitter et lancer le service d'Administration ou ajouter un modèle de produit.

Cliquez sur **Ajouter une base de données Produit**, l'assistant de création de tenant s'affiche.



Sélection du produit

Sélectionnez un produit dans la liste.

Cliquez sur le lien **Sélectionner un Fournisseur**.

Note : Pour plus d'informations sur la marche à suivre pour sélectionner un fournisseur, reportez-vous à la section intitulée Sélectionner un fournisseur.

Bases de données

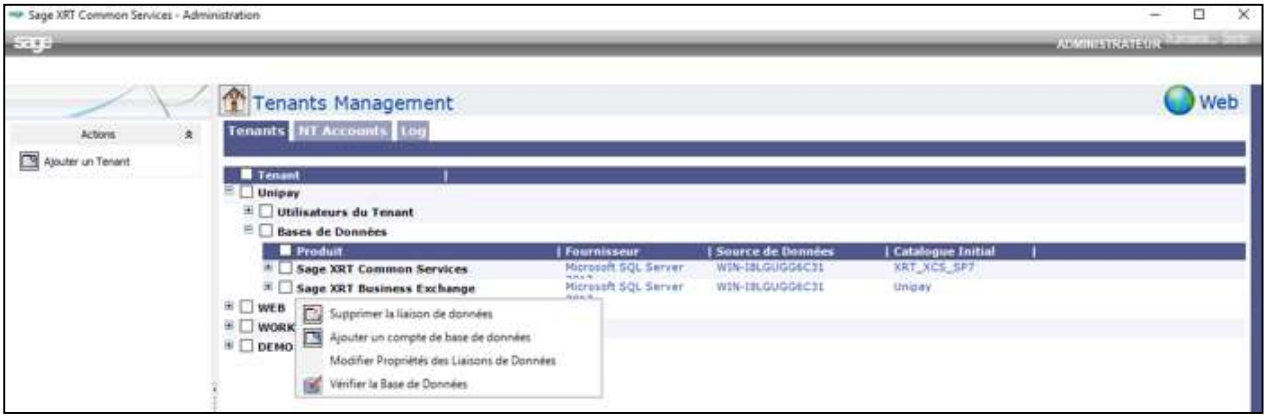
L'interface **Tenants Management** rassemble tenants, utilisateurs et bases de données.

Important ! La mise à jour d'une base de données n'est pas sans risque pour les données de l'utilisateur. Il est donc impératif de sauvegarder ces données au préalable.

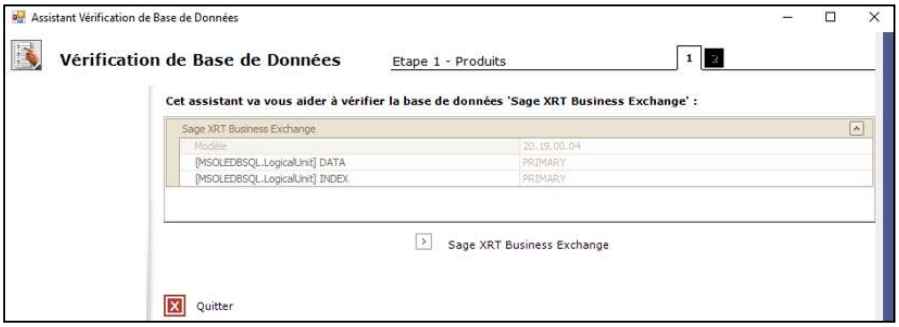
Mise à jour

Développez l'arborescence **Tenant**, puis le tenant concerné, et enfin **Bases de données**.

Après un clic droit sur la ligne correspondant à la base de données à mettre à jour, sélectionnez **Vérifier la base de données** dans le menu contextuel.



L'Assistant Vérification de Base de Données s'affiche.

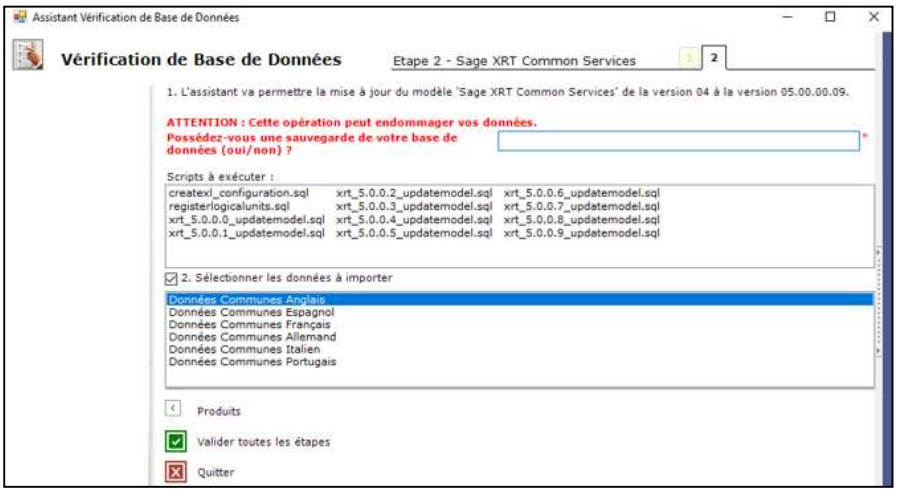


Note : Si l'utilisateur Windows n'est pas enregistré en tant que DBO dans le tenant approprié, il n'est pas autorisé à mettre à jour la base de données. L'assistant ne propose aucune mise à jour de base de données et le lien Produit n'est pas affiché.

Cliquez sur le produit.

Si l'assistant détecte une incohérence dans les versions, vous êtes renvoyé au processus de mise à jour de base de données.

Dans le cas contraire, l'**Etape 2** de l'assistant s'affiche.



Répondez à la question par oui ou non : Possédez-vous une sauvegarde de votre base de données ?

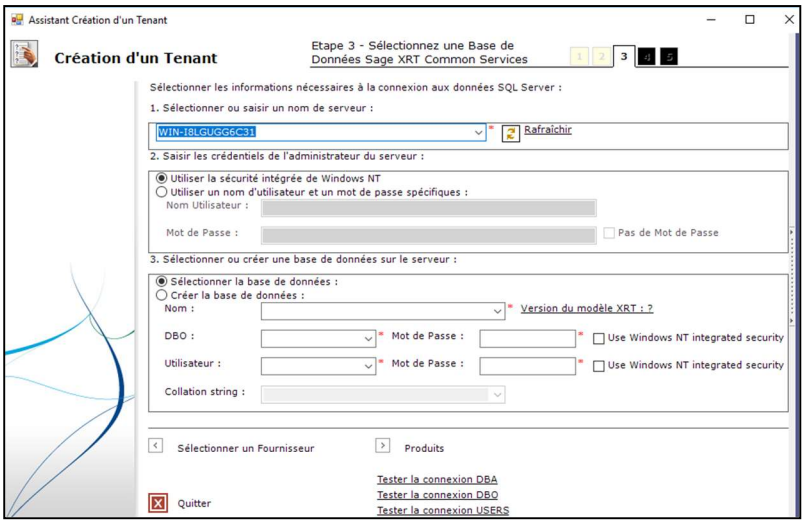
Activez l'option **Sélectionner les données à importer** si les données de la base ne sont pas à jour.

Cliquez sur le lien **Valider toutes les étapes**.

SQL Server et Profils non-SYSADMIN

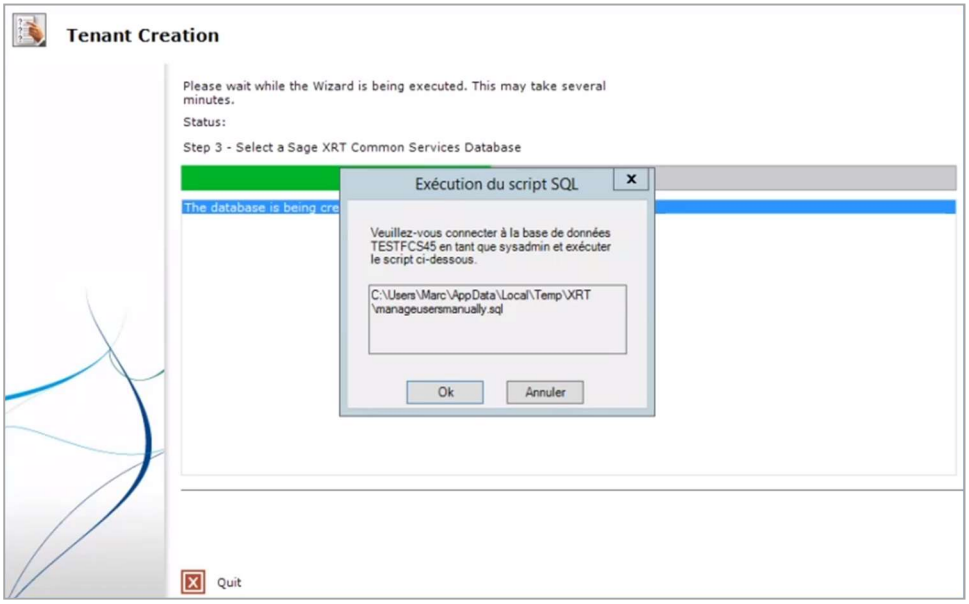
Suivez la procédure décrite dans ce paragraphe

- Vous devez d'abord créer et mettre à jour une base de données avec un profil de type *dbcreator*.
- Lors de la création d'une base de données, renseignez le nom et mot de passe de l'utilisateur de type *dbcreator*.



Note : Lors du test de connexion DBA, le message informant de la nécessité d'une connexion en tant que SYSADMIN a disparu.

Reprenez le processus habituel de gestion de base de données : lors de l'étape de passage des scripts, un message requiert l'intervention d'une personne au profil de *SYSADMIN*.

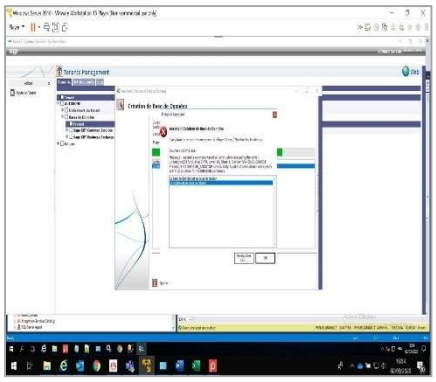


Connectez-vous à **SQL Server** avec un profil SYSADMIN et ouvrez le fichier indiqué.

Lancez le script.

Revenez sur l'**Assistant Création de Base de Données** et cliquez sur **OK** dans la boite de dialogue pour terminer le processus.

Si vous rencontrez l'erreur de la capture ci-dessous, c'est que vous utilisez la version **Microsoft SQL Server 2017 (RTM-GDR) (KB4293803) - 14.0.2002.14 (X64) Jul 21 2018**.



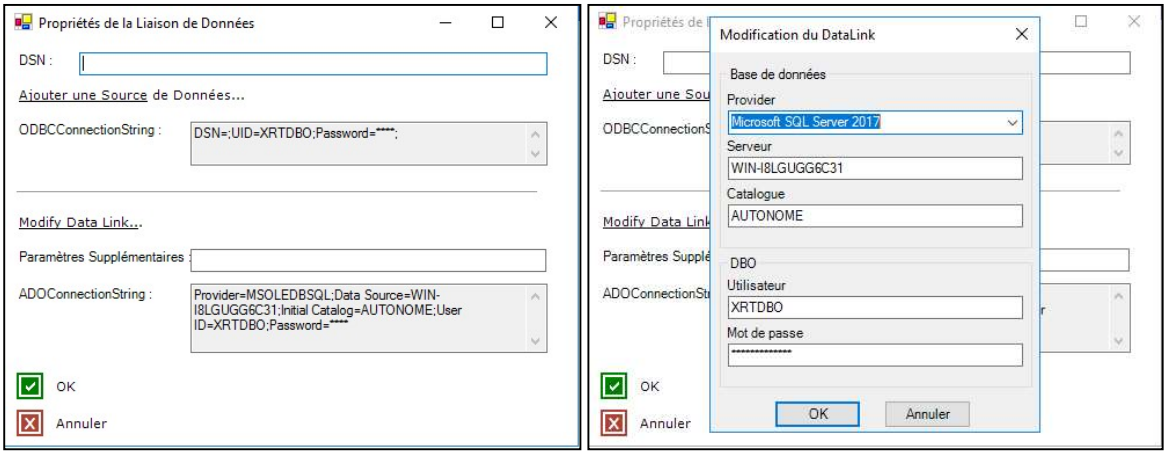
Pour remédier à cette situation, vous devez mettre à jour SQL Server pour utiliser la version **Microsoft SQL Server 2017 (RTM-GDR) (KB4505224) – 14.0.2027.2 (X64) Jun 15 2019**.

Modifications

Vous pouvez modifier les **Provider**, **Source de données** (serveur) et **Catalogue** sans passer par le DB Installer (**Oracle** et **SQL Server**), si vous souhaitez, par exemple, passer d'une base de test à une base de pré-production ou de production.

Pour une base **SQL Server**, sélectionnez la base de données, après un clic droit pour ouvrir le menu contextuel, cliquez sur **Modifier Propriétés des Liaisons de Données**.

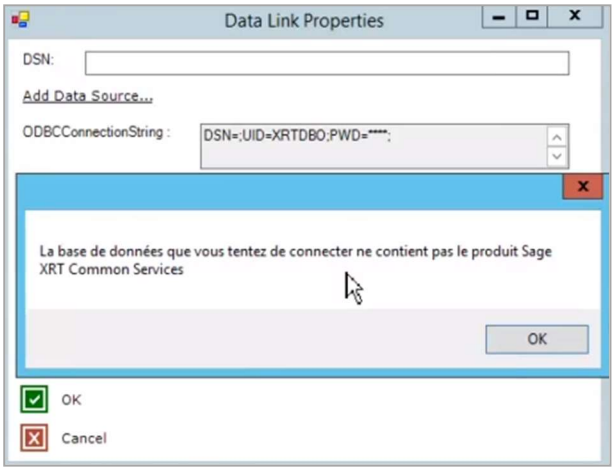




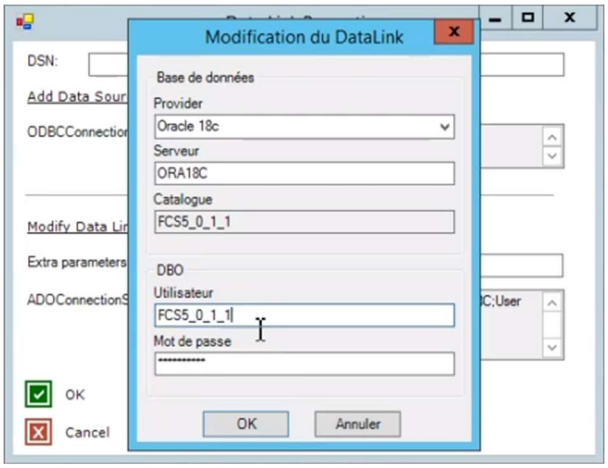
Utilisez le lien **Modify Data Link**.

La modification du **Provider** peut se faire uniquement dans la même famille (**SQL Server 2017** à **SQL Server 2019**, **Oracle** 12 à 18).

Celle du catalogue ne peut se faire que pour une base de même nature ou contenant les données de la base modifiée (modification d'une base **FCS** par une autre base **FCS** ou base **FCS**+**SXBE**), sinon un message bloquant la modification apparaît.



Pour une base **Oracle** : pas d'accès à la modification du catalogue car le catalogue reprend l'utilisateur renseigné.



Première connexion

Lors de la première connexion après création de la base de données, vous pouvez utiliser :

- Le compte NT utilisé pour installer le produit
- Le login **XRT** et mot de passe **S3cret#2018**

Important ! Les identifiants XRT et S3cret#2018 ne sont valables qu'une seule journée !

Utilisateurs

Lors de la création d'un tenant, les groupes locaux **Windows NT Administrators** et **XRTDBAdministrators** sont automatiquement déclarés comme administrateurs du nouveau groupe.

SAGE XRT Solution Common Services propose un assistant pour la gestion des utilisateurs au sein des groupes de travail.

Cet assistant permet les actions suivantes :

- **Ajout d'un utilisateur réseau** : pour ajouter un utilisateur, saisissez le Compte NT d'un utilisateur réseau ou cliquez sur **Rechercher...** pour accéder à l'outil *Microsoft* de recherche d'un utilisateur *Windows NT*.

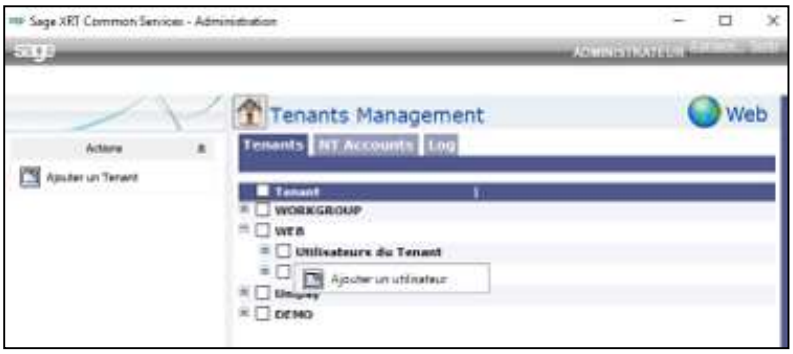
- **Ajout d'un groupe réseau** : cette option vous permet d'associer un groupe d'utilisateurs *Windows NT* à un tenant. Pour cela, cliquez sur **Rechercher...** et accédez ainsi à l'outil *Microsoft* de recherche d'un utilisateur *Windows NT*.

- **Ajout d'un compte système local** : ce type de compte est utilisé par un **service système** exécuté pour le compte du système local et doit accéder à une base de données.

Ajout à un tenant

Pour assigner un utilisateur au tenant, développez l'élément **Tenants** dans l'arborescence.

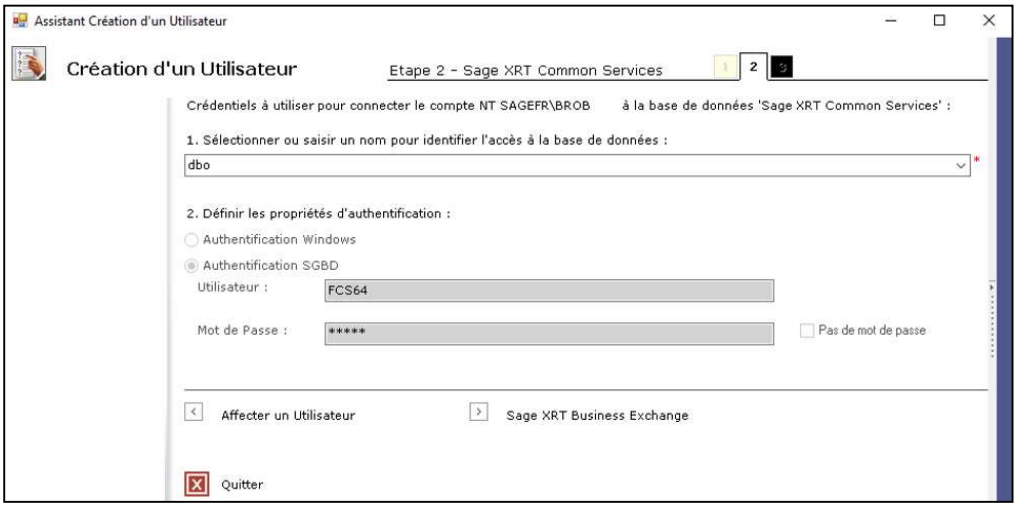
Sélectionnez un tenant dans la liste, et effectuez un clic droit sur le niveau **Utilisateurs du tenant**.



Cliquez sur **Ajouter un utilisateur** pour ouvrir l'**Assistant Création d'un utilisateur**.



Cliquez sur le lien **Sage XRT Solution Common Services** pour atteindre la seconde étape de l'assistant.



Sélectionnez un type d'accès aux données dans la liste déroulante, ou saisissez un nouveau nom. Par défaut, l'assistant propose deux types d'accès prédéfinis :

- **DBO** : Ce type d'accès doit être réservé au propriétaire de la base de données.
- **Users** : Ce type d'accès doit être utilisé par les profils sans pouvoir.

Sélectionnez le mode d'authentification de l'utilisateur sur le serveur de bases de données :

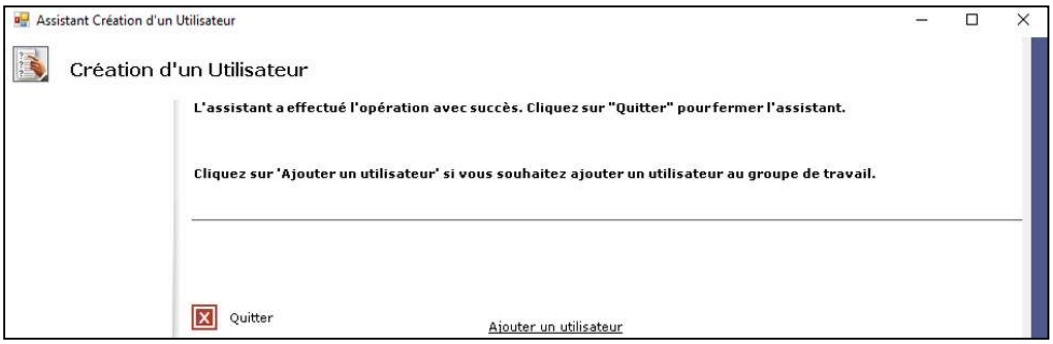
- Authentification Windows : par son compte NT.
- Authentification SGBD : l'utilisateur est authentifié par un compte qui lui a été affecté par l'administrateur du serveur de bases de données.

Important ! Il est recommandé de définir l'accès avec un compte SQL Server, car l'utilisation de l'authentification NT ne permet pas le pooling de connexion.

Il est possible de créer un autre nom d'accès pour un groupe d'utilisateurs donné. Ce nouvel accès est de type **User**.

Ex. : définition d'un accès *TRESORIER* pour la base **SAGE XRT Solution Advanced Treasury**, avec un compte *SQL Server* spécifique intitulé *TRESO*.

Cliquez sur **Valider toutes les étapes**.



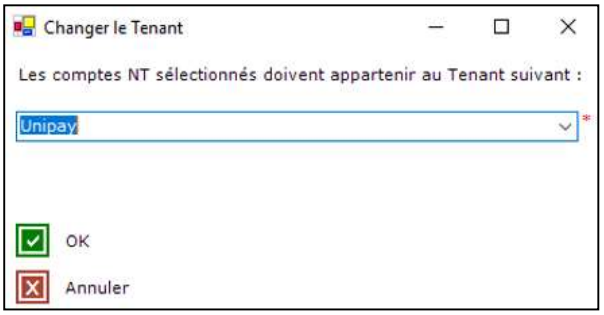
Note : Vous pouvez également gérer les utilisateurs de SAGE XRT Solution Advanced Treasury en

répétant l'opération d'accès à la base SAGE XRT Solution Common Services.

Modification

Vous pouvez modifier l'affectation d'un utilisateur à un tenant.

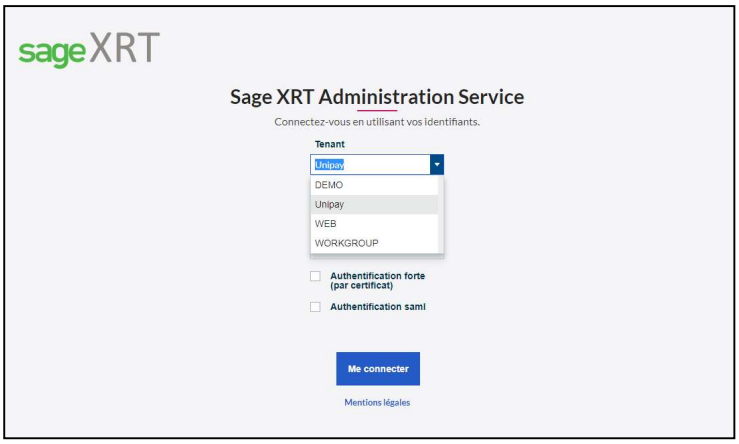
Après un clic droit sur l'utilisateur dont le tenant doit être modifié, sélectionnez l'action **Changer le tenant**.



Sélectionnez le nouveau tenant et cliquez sur le bouton **OK**.

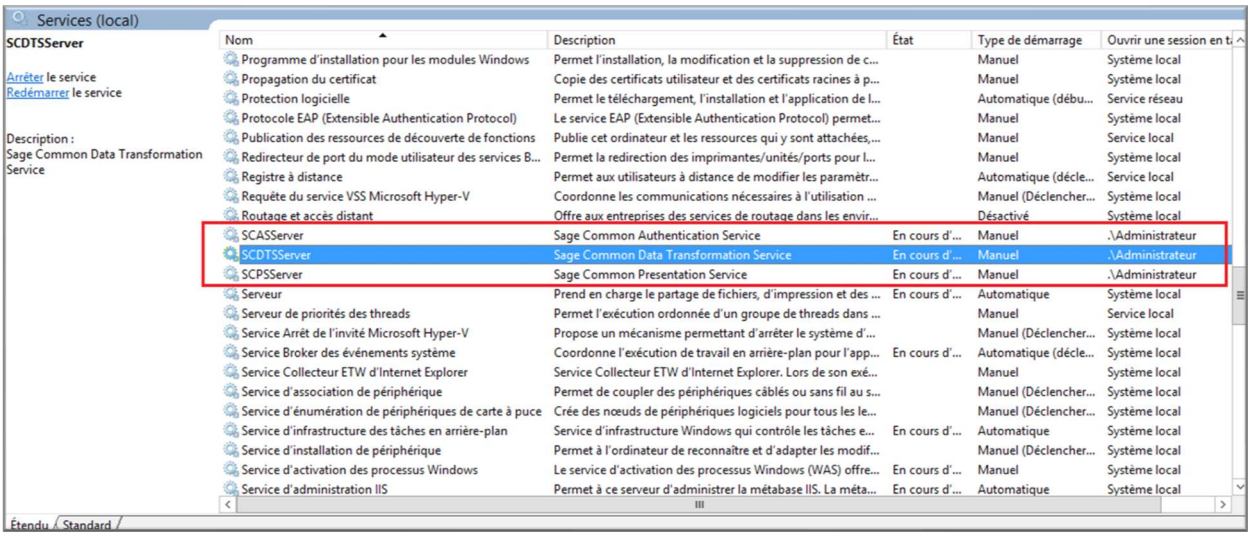
XRT Solution Common Administration Services

L'icône  située en haut à droite de l'interface **Tenants Management** permet un accès direct à **SAGE XRT Solution Common Administration Services**, le service d'administration des utilisateurs, profils, droits, etc.



SAGE XRT Solution Common Services 6.0 est composé de trois services :

- Le service d'authentification (SCAS) qui permet de valider l'authentification des utilisateurs.
- Le service d'administration (SCPS) qui permet de gérer les parties Droits (Utilisateurs, Profils, Sites, etc.), Audits (Audits, Logs) et Transcodages (Conception et correspondances).
- Le service des fonctionnalités (SCDTS) qui couvre les thématiques suivantes :
    - Gestion des formats
    - Gestion des paiements
    - Gestion des relevés bancaires
    - Gestion des contrats de communication standards (SAGE XRT Solution Advanced Communication)
    - Gestion de l'historique de communication (SAGE XRT Solution Advanced Communication)
    - Gestion de l'antifraude



La documentation de ces API est générée par *Swagger*. Le fichier *swagger.json* correspond à une exportation de la documentation au format JSON.

*Note : Accédez à la documentation et au fichier JSON (lien inscrit dans le fichier *.config de chaque service) sous C:\Program Files\Common Files\xrt.*

Chaque service dispose d'un fichier de configuration.

Service d'authentification

Configuration

Le fichier de configuration *Sage.SCASServer.Service.exe.config* se situe par défaut sous :
C:\Program Files\Common Files\xrt

Cf. Annexes pour le détail de chaque paramètre.

Paramétrage de la page de connexion

Initialisation du processus de connexion

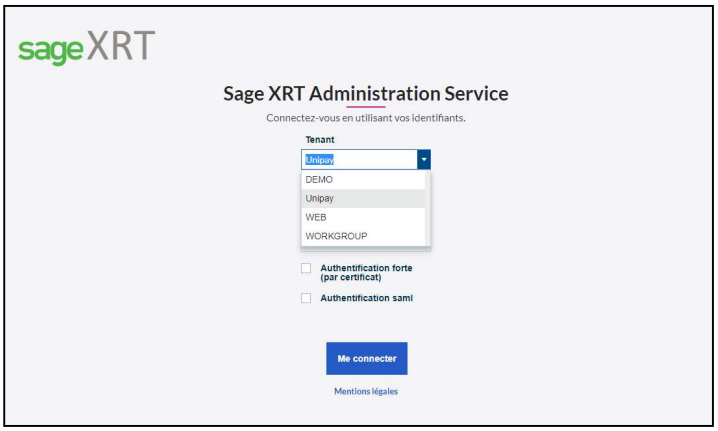
Pour initier le processus de login, postez le formulaire ci-dessous (méthode POST) au service d'authentification de **Sage XRT Solution Common Services** :

http://*nomdemachine*:80/Auth/loginpage ou

https://*nomdemachine*:443/Auth/loginpage

```
<form name="loginpage" method="post" action="http://nomdemachine:80/Auth/loginpage">
    <input type="hidden" name="workgroup" value="">
    <input type="hidden" name="strongauth" value="YES">
    <input type="hidden" name="samlv2" value="YES">
    <input type="hidden" name="product" value="SXSC">
```

<input type="hidden" name="url" value="http://nomdemachine:80/home/homepage">
<input type="hidden" name="xrtloginweborigin" value="">
<input type="hidden" name="goto" value="">
</form>
La page de connexion s'affiche.



Variable du formulaire workgroup

Cette variable permet de pré-paramétrer un tenant. Elle pilote la présence du menu déroulant permettant de sélectionner un tenant.

Cependant, si elle est initialisée avec le nom d'un tenant, elle n'apparaît pas et le couple utilisateur/mot de passe de l'utilisateur est vérifié pour ce tenant.

Variable strongauth

Cette variable permet de donner accès à l'option d'authentification forte.

Si la variable a pour valeur YES alors la case à cocher permettant d'utiliser l'authentification forte apparait.

Si la variable est vide alors l'option est absente.

Variable samlv2

Cette variable permet de donner accès à l'option d'authentification SAML.

Si la variable a pour valeur YES alors la case à cocher permettant d'utiliser l'authentification SAML apparait.

Si la variable est vide alors l'option est absente.

Variable du formulaire product

Cette variable permet de gérer le nom du produit affiché sur la page de connexion. Elle admet soit un code prédéfini, soit un texte libre. Les codes prédéfinis sont les suivants :

- product=SXSC pour SAGE XRT Solution Common Administration Service
- product=SCSDTS pour SAGE XRT Solution Common Services

- product=SXBEONLINEBANKING pour Connexion à OnlineBanking (SAGE XRT Solution Business Exchange)
- product=SXBEADMINISTRATION pour Connexion à SAGE XRT Solution Business Exchange Administration
- product=VIEWANDSIGN pour Sage View & Sign

Lorsqu'on utilise les noms de code, la localisation en FR, ES et US est gérée par le processus de connexion XRTLoginWeb de Sage XRT Common Services.

Un texte libre peut être utilisé comme valeur de la variable.

Variable url

Cette variable permet de définir l'URL de *callback* en cas de succès du processus d'authentification (cf. liste blanche des URL possibles).

Variable xrtloginweborigin

Cette variable permet de définir l'URL du site web du processus d'authentification lorsque celui-ci n'est pas hébergé sur la même machine que la page qui initie le formulaire d'initialisation du processus d'authentification **XRTLoginWeb**. Il y a également possibilité de ne pas utiliser cette variable et de réaliser le paramétrage au niveau du fichier de configuration du service d'authentification (SCAS).

Le processus d'authentification **XRTLoginWeb** permet également de définir si les mots de passe sont cryptés puis encodés en Base64 ou seulement encodés en Base64. Pour cela il suffit de définir un certificat au niveau du fichier de configuration du service d'authentification (SCAS).

Pour le certificat qui crypte le mot de passe :

<add key="serialnumberforpwdcrypt" value="" /> tag

Variable du formulaire goto

Cette variable admet deux valeurs : **SAML** ou **SAGEID**.

Pour être prise en compte, la variable **WORKGROUP** doit être renseignée.

Si ces valeurs sont utilisées, l'utilisateur est directement amené sur le processus d'authentification **SAML** ou **SAGEID** sans passer par la mire de connexion.

Service d'Administration

Configuration

Le fichier de configuration *Sage.SCPSServer.Service.exe.config* se situe par défaut sous : **C:\Program Files\Common Files\xrt**.

Activation des logs

Cf. nœud <system.diagnostics> et <diagnostics>

Définition de l'emplacement du site Web, des ports d'écoute et des hosts des services

Cf. nœud <ApplicationSettings>

<add key="websitehost" value="*" />

<add key="websitehostdefault" value="http://localhost" />

<add key="httpservicehost" value="http://*:80"/>

<add key="httpsservicehost" value="https://*:443"/>

Définition du compte et de la fréquence en seconde de synchronisation des groups NT/LDAP

Cf. nœud <ApplicationSettings>

<add key="syncprofilesiteuser" value="XRT"/>

<add key="syncprofilesitefrequency" value="3600"/>

Définition d'éléments de sécurité

Cf. nœud <ApplicationSettings>

<add key="showfriendlymessage" value="NO"/>

(numéro de version non présenté et messages d'erreur générique)

Documentation SWAGGER

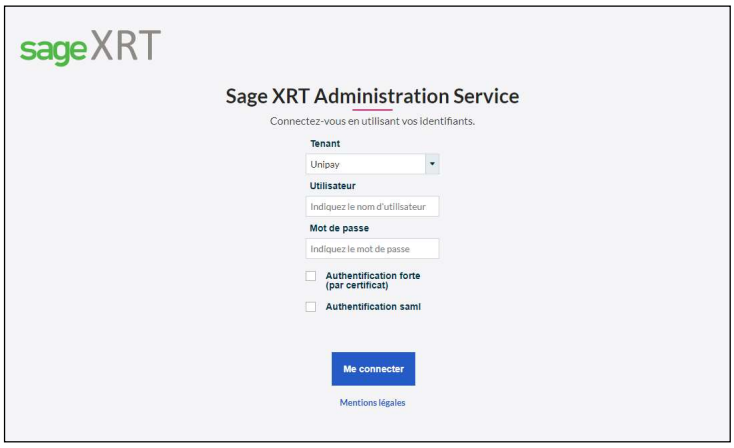
URL de documentation et URL d'exportation

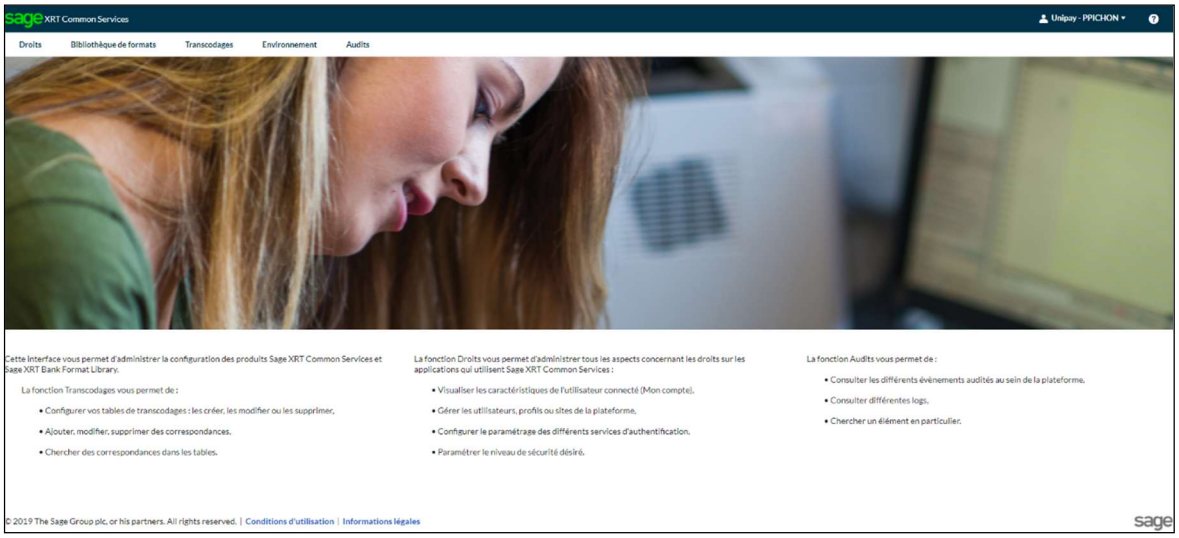
Connexion

L'utilisation de l'interface du service d'administration se fait via l'URL :

http://localhost/SCPS/index.html

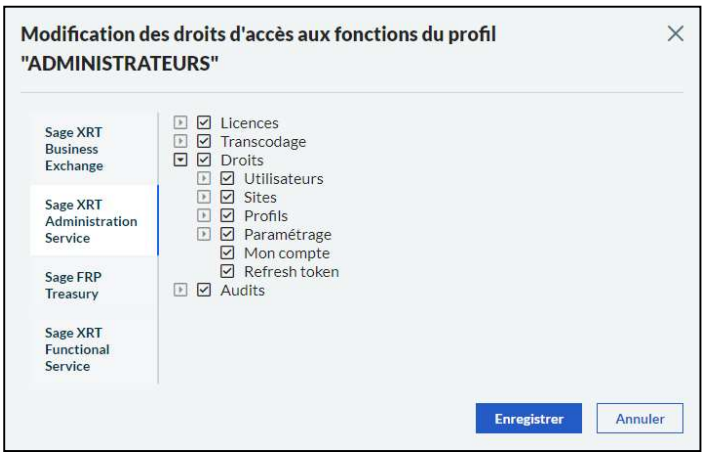
Elle nécessite le démarrage des services d'authentification et d'administration.





Refresh Token

Le Refresh token est utilisé par les services Windows qui consomment les API Rest de SAGE XRT Solution Common Services. Sa mise en place demande l'installation d'un certificat sur le poste client et sur le poste serveur.



Licences

Les licences par défaut sont appliquées à tous les tenants pour lesquels aucune licence n'a été spécifiée.

La fonction **Licences par défaut** est la même que la fonction **Licences**. La licence reste stockée dans la base de registre.

Les interfaces sont identiques pour les deux types de licences.

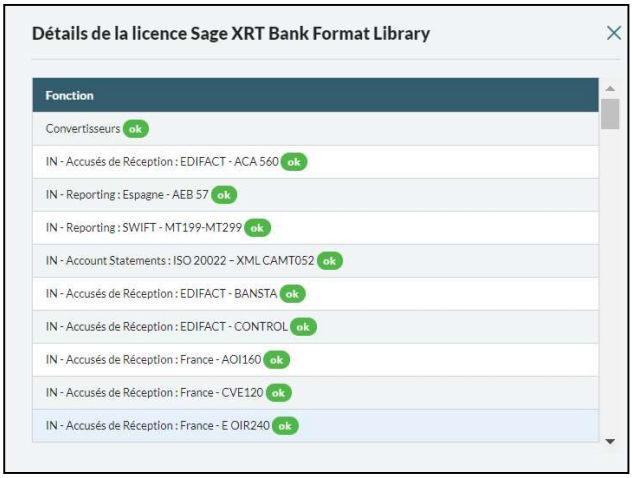
Les licences existant pour le tenant courant sont listées à l'appel de la fonction **Licences pour le tenant courant**.

Les licences existant par défaut sont listées à l'appel de la fonction **Licences par défaut**.



Pour visualiser le détail correspondant à un clé de licence, cliquez sur l'icône *loupe*.

Exemple pour **SAGE XRT Solution Bank Formats Library** :



Création

Dans le menu **Environnement – Licence par défaut**, le bouton **Nouvelle licence** vous permet d'accéder à l'assistant de création.

Vous devez compléter tous champs marqués d'un astérisque.

Cliquez sur le bouton **Enregistrer** pour finaliser la création. Un message vous confirme la création de la licence.



Modification

Cliquez sur le lien disponible sur l'information **Nom** de la licence à modifier. Seules les

informations **Client** et **Clé de licence** sont modifiables.

Cliquez sur le bouton **Enregistrer** pour finaliser la modification de la licence. Un message vous confirme la modification de la licence.

Suppression

A partir de la liste des licences, sélectionnez la licence à supprimer.

Cliquez sur l'icône *corbeille* pour finaliser la suppression de la licence. Un message vous confirme la suppression de la licence.

Application

Lorsqu'une licence pour un tenant est spécifiée, la licence par défaut ne s'applique pas.

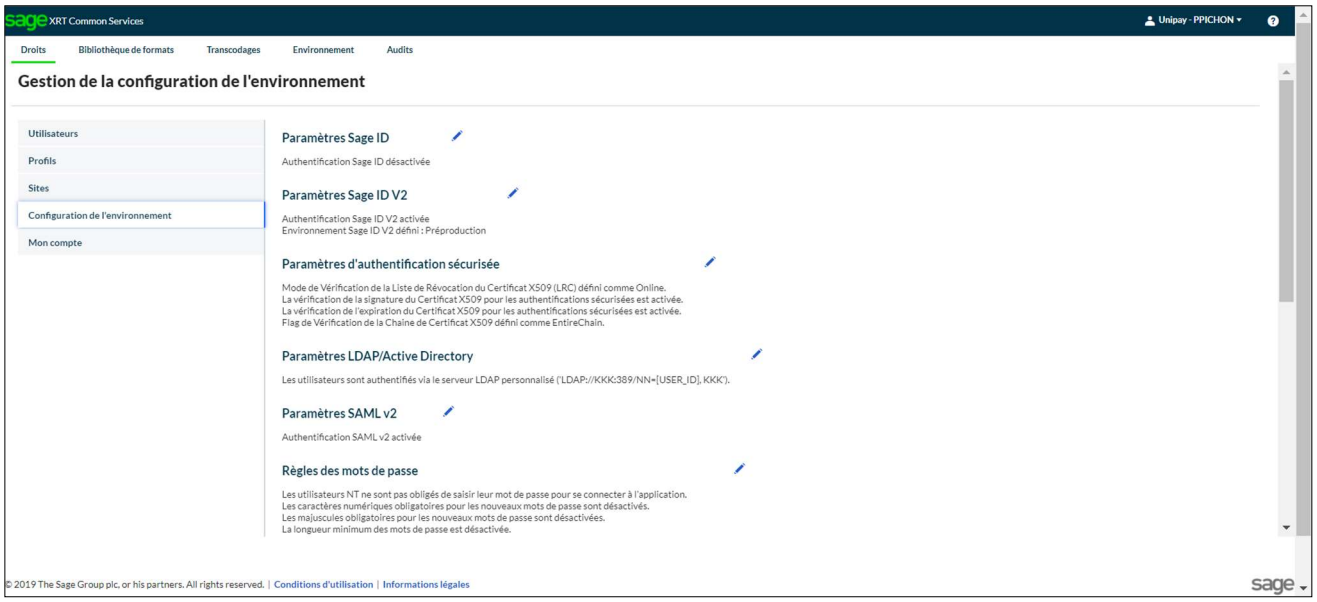
Paramétrage authentification

Le modèle de login UMAPI supporte plusieurs modes d'authentification :

- Windows NT
- UMAPI
- LDAP
- SAML
- CloudID : Sage ID V2

Ces modes d'authentification sont à activer préalablement à leur rattachement à un utilisateur.

Dans le menu **Droits**, cliquez sur l'onglet **Configuration de l'environnement**.



Utilisez l'icône *crayon* pour modifier les paramètres de chaque mode d'authentification.

Authentification Windows NT
L'authentification *Windows NT* tire avantage de la sécurité *Windows NT* et de sa gestion des comptes utilisateur. Ce mode de sécurité permet aux applications Sage XRT Solution d'utiliser les crédentials des utilisateurs *Windows NT*.

Les applications Sage XRT Solution proposent deux modes de fonctionnement avec ce type d'authentification :

- Le mode *trusted connection* (connexion sécurisée) n'est plus supporté à partir de la version 5.0 car **SAGE XRT Solution Common Services** est désormais une application web.
- Le mode standard : l'utilisateur doit saisir son mot de passe car il est contrôlé par le système via les *API Windows*.

Avantages du mode d'authentification *Windows NT* :

- Pas de crédentials supplémentaires à mémoriser
- Pas de répercussion dans *UMAPI* lors d'un changement de mot de passe
- Gestion des mots de passe conforme aux exigences du *Sarbanes-Oxley Act*
- Accès à d'autres fonctionnalités du système comme le changement périodique de mot de passe et l'audit des accès

Note : La mise en place de l'authentification Windows NT nécessite de travailler en étroite collaboration avec l'administrateur Windows lors de la création des utilisateurs et des groupes. L'implémentation dans UMAPI de l'authentification Windows est basée sur la librairie de classes de bases du namespace System.DirectoryServices du framework .NET.

Authentification UMAPI
Lorsqu'il utilise l'authentification *UMAPI*, un utilisateur se connectant à une application Sage XRT Solution fournit un nom d'utilisateur et un mot de passe contrôlés à partir d'informations contenues dans la base de données.

Avantages du mode d'authentification *UMAPI* :

- Gestion des mots de passe conforme aux exigences de la loi *Sarbanes-Oxley*
- Enregistrement des quatre derniers mots de passe qui ne peuvent être réutilisés lorsque le système demande un changement de mot de passe (fonctionnalité paramétrable)
- Compte utilisateur verrouillé après trois échecs successifs d'authentification (fonctionnalité paramétrable)
- Compte utilisateur verrouillé débloqué après une période paramétrable
- Seuls les codes de hachage *SHA1* des mots de passe sont enregistrés dans la base de données, et non les mots de passe
- Mot de passe d'au moins six caractères comprenant au moins une majuscule et un chiffre. Fonctionnalité paramétrable

- Mot de passe à changer périodiquement (fonctionnalité paramétrable)
- Possibilité pour l'administrateur de verrouiller un compte utilisateur pour une durée déterminée ou de façon permanente

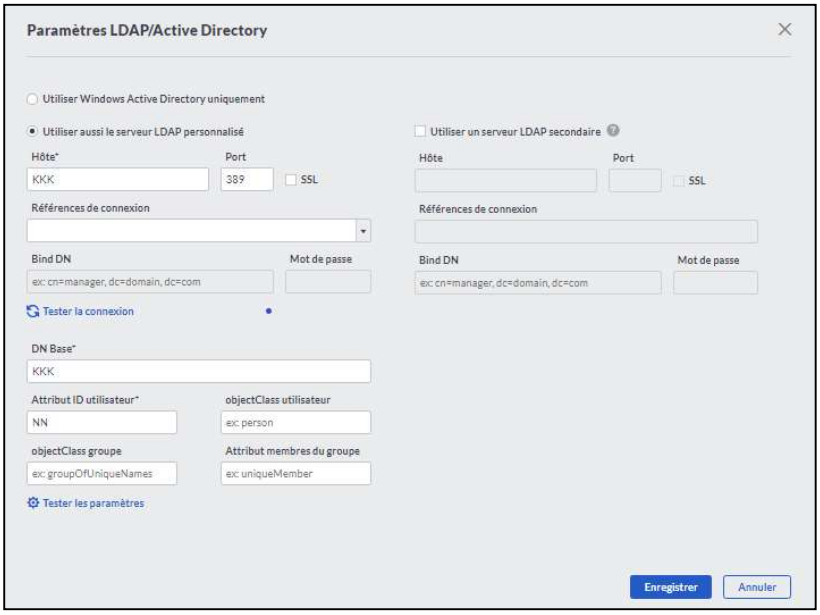
Authentification LDAP
Lorsqu'il utilise l'authentification *LDAP*, un utilisateur se connectant à une application Sage XRT Solution doit fournir un nom d'utilisateur et un mot de passe contrôlés à partir d'informations contenues dans l'annuaire *LDAP*.

Avantages du mode d'authentification *LDAP* :

- Alternative intéressante lorsqu'une société ne souhaite pas utiliser exclusivement le système d'authentification *Windows NT*
- Authentification applicative dans le cadre des produits Sage XRT Solution

La configuration de l'accès à l'annuaire s'effectue à partir de l'écran de paramétrage de la gestion des utilisateurs. L'administrateur doit renseigner les paramètres suivants :

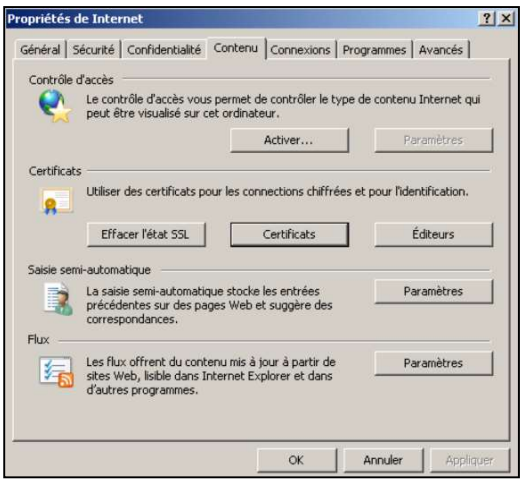
- L'adresse IP de la machine qui héberge le serveur *LDAP*
- Le numéro de port sur lequel le serveur *LDAP* doit être appelé
- Le paramètre **Base DN** de l'annuaire
- L'attribut **User ID attribute name** sur lequel doit se baser l'authentification de l'utilisateur
- Le nom de la classe **Utilisateur** à utiliser lors de la recherche d'un individu dans l'annuaire
- Le nom de la classe **Group** à utiliser lors de la recherche d'un groupe d'individus dans l'annuaire
- Les crédentials permettant d'effectuer une recherche sur l'annuaire (le bouton **Test Connection** permet de vérifier ces crédentials)



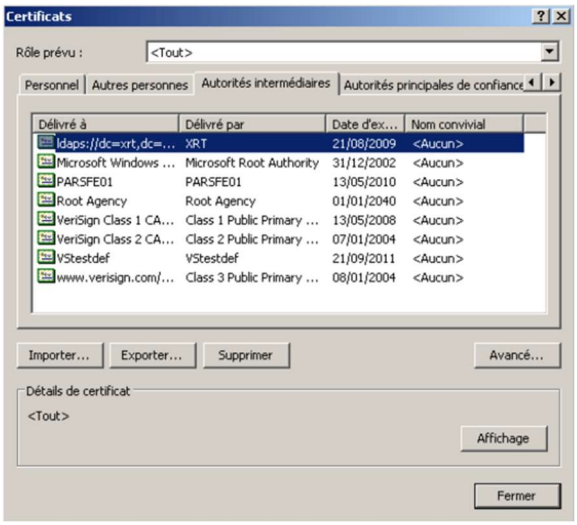
Note : L'implémentation dans UMAPI de l'authentification LDAP est basée sur la librairie de classes de bases du namespace System.DirectoryServices du framework .NET.

En règle générale, les échanges LDAP entre les clients et le serveur transitent par le port *TCP/IP* standard (port 389) sous forme cryptée ou via un tunnel SSL (port 636). La technologie SSL peut être activée en installant un certificat publié par une autorité de certification approuvée par le contrôleur de domaine et les clients LDAPS. L'approbation est établie en configurant les clients et le serveur de façon à approuver l'autorité de certification racine à laquelle est enchaînée l'autorité de certification émettrice.

Le certificat installé se trouve dans le magasin de certificats personnel de l'ordinateur local au niveau propriétés Internet du navigateur : onglet **Contenu**, bouton **Certificats et autorités intermédiaires**.



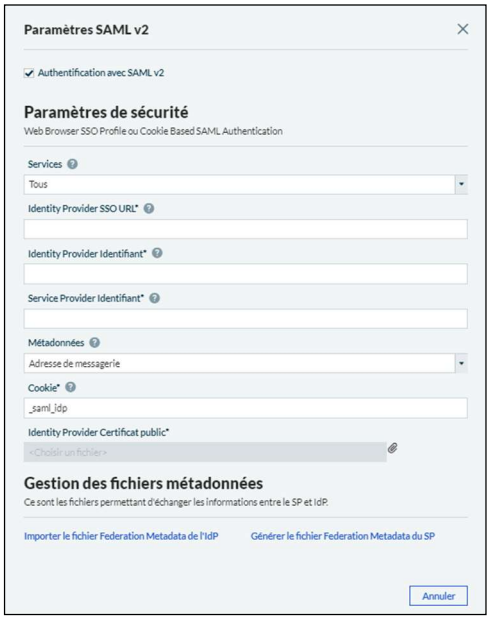
Cliquez sur le bouton **Certificats**. La boîte de dialogue suivante s'affiche.



Authentification SAML

Security Assertion Markup Language (SAML) est un standard informatique définissant un protocole pour échanger des informations liées à la sécurité, basé sur le langage *XML*.

SAML propose l'authentification unique (en anglais *Single Sign-On* ou *SSO*) sur le web. De cette manière, un utilisateur peut naviguer sur plusieurs sites différents en ne s'authentifiant qu'une seule fois.



L'authentification *SAML* fait intervenir :

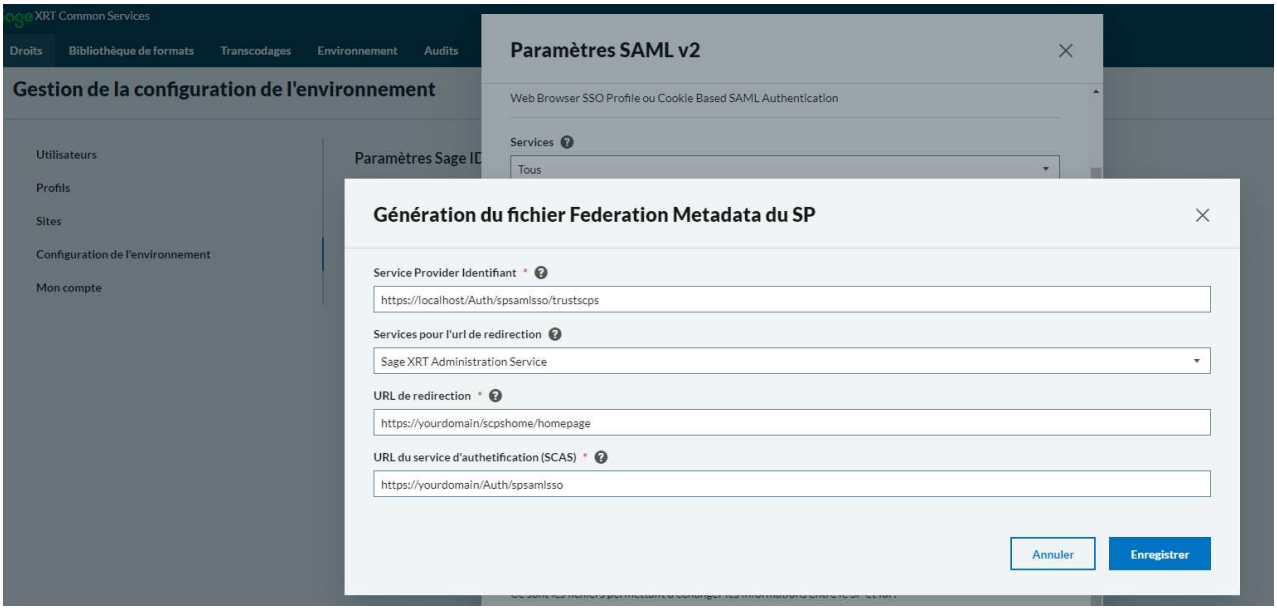
- L'*Identity provider* (l'entité qui détient les identifications) : champs **Identity Provider SSO URL** et **Identity Provider Identifiant.**
- **ADFS** (*Active Directory Federation Services*) et **Azure AD** (*Active Directory*) sont supportés.
- Les *Services providers* (les services qui nécessitent une authentification) : champ **Service Provider Identifiant**. Plusieurs *Services providers* peuvent être renseignés (ils forment le cercle de confiance des services par rapport à un *IdP*).
- L'utilisateur qui est identifié via une donnée déclarée dans les métadonnées (ex. : ID ou e-

mail).

- Des fichiers métadonnées permettant d'échanger des informations entre *SP* et *IdP*.
- Le fichier métadonnées de l'*IdP* contient le certificat pour vérifier le *token SAML* et l'identifiant de l'*IdP*.
- Le fichier métadonnées du *SP* contient l'*ID* du *SP* et l'URL *callback* par service.

Comment mettre en place une authentifation SAML ?

1. Demander le fichier métadonnées à l'IdP et l'url d'accès utilisateur permettant d'initier le token.
2. Envoyer à l'IdP les fichiers métadonnées du SP pour chaque service.



3. Dans le cadre du SSC importer le fichier métadonnées de l'IdP au niveau du SCPS du tenant SXA.

Double Authentification
La technologie choisie est celle du protocole *TOTP* (RFC 6238).

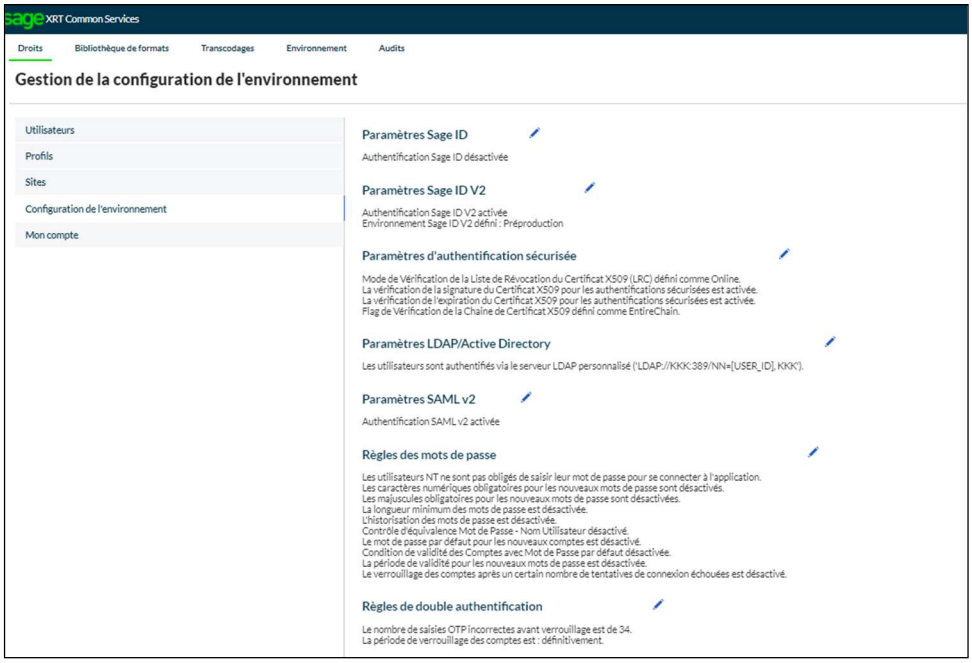
Ce protocole associe une clé secrète à l'heure, en utilisant une fonction de hachage cryptographique pour générer un mot de passe à usage unique. Prenant en compte la latence du réseau et les éventuels retards d'horloges, l'horodatage augmente par intervalles de 30 secondes, ce qui réduit l'espace de recherche potentiel.

L'adoption de ce protocole permet d'utiliser des applications mobiles déjà disponibles, comme par exemple *FreeOTP*, *Microsoft Authenticator* ou *Google Authenticator*.

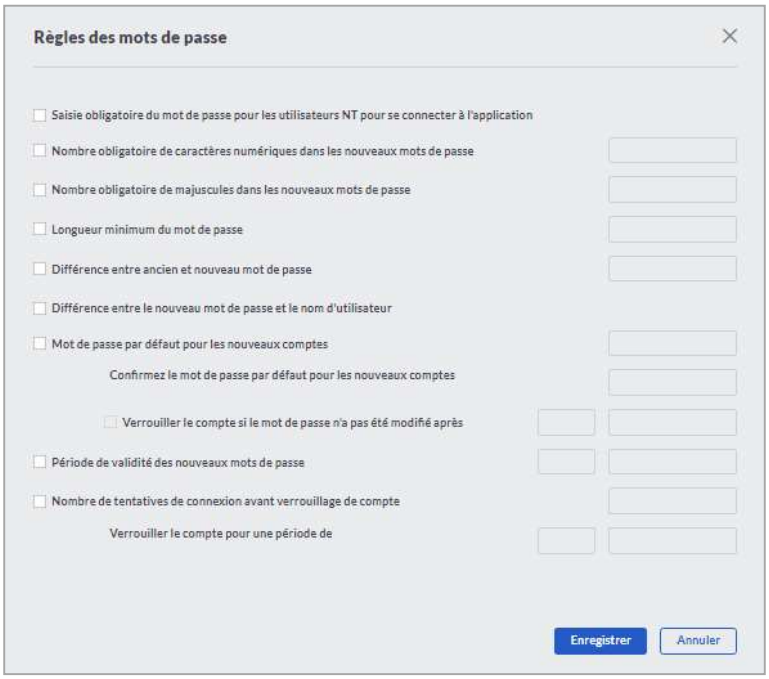
Note : Voir le document SCS.5.0.DoubleAuthentication.UserGuide_FR.

Règles des mots de passe

Ces règles sont définies à partir du menu **Droits**. Cliquez sur l'onglet **Configuration de l'environnement**.



Utilisez l'icône **Modification** pour modifier les règles des mots de passe.



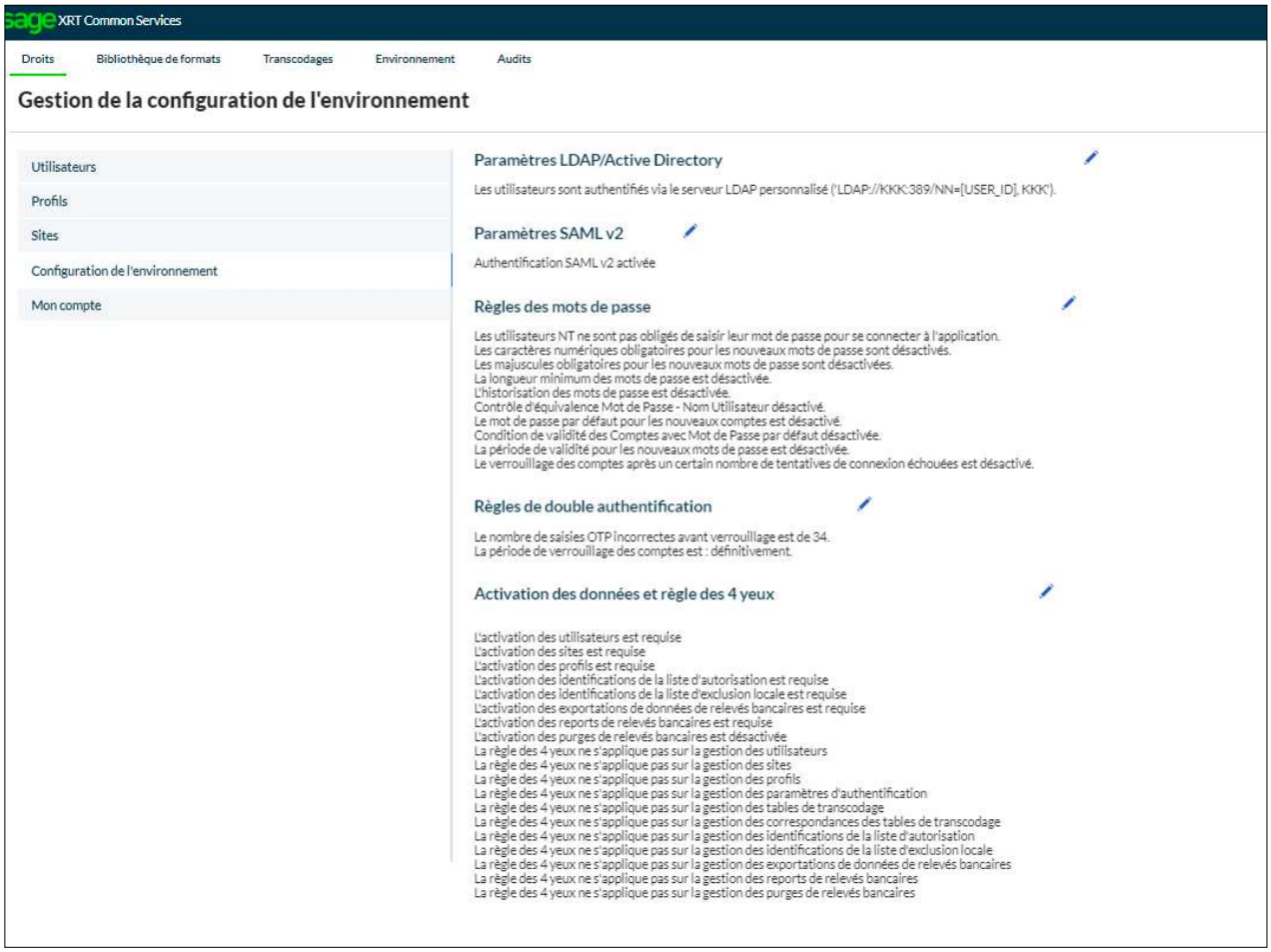
Activation des données et règle des 4 yeux

L’activation et l’application de la règle des *4 yeux* doivent être explicitement demandées. Par défaut, les données ne doivent pas être activées préalablement à leur utilisation et la règle des *4 yeux* ne s’applique pas.

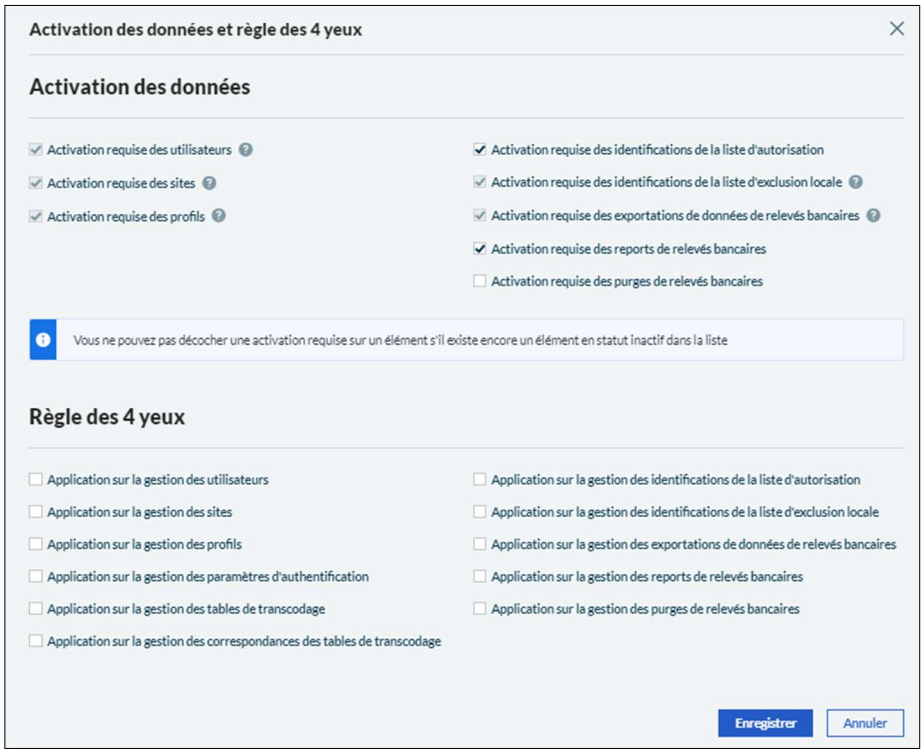
Important ! Rappel du principe de l’activation : une donnée inactive ne peut être utilisée (statut inactif). Cette donnée devra être activée pour pouvoir être utilisée (statut actif).

Rappel du principe de la règle des 4 yeux : un même utilisateur ne peut enchaîner 2 actions sur un même élément (création + modification, création + suppression, création + activation…).

Cliquez sur l'onglet **Configuration de l’environnement**.



Utilisez l’icône **Modification** pour modifier les règles d’activation des données et des *4 yeux*.



L'activation d'un élément ne pourra être demandée que s'il n'existe aucun élément en statut inactif.

L'activation peut être demandée sur :

- Les utilisateurs
- Les profils
- Les sites
- Les identifications de la liste d'autorisation
- Les identifications de la liste locale d'exclusion
- Les exportations de données de relevés bancaires
- Les reports de relevés bancaires
- Les purges de relevés bancaires

La règles des 4 yeux peut s'appliquer sur :

- La gestion des utilisateurs
- La gestion des profils
- La gestion des sites
- La gestion des paramètres d'authentification

- La gestion des tables de transcodage
- La gestion des correspondances des tables de transcodage
- La gestion des identifications de la liste d'autorisation
- La gestion des identifications de la liste locale d'exclusion
- La gestion des exportations de données de relevés bancaires
- La gestion des reports de relevés bancaires
- Les purges de relevés bancaires

Cliquez sur **Enregistrer** pour sauvegarder l'application de ces règles.

En cas d'activation des profils requise :

- Les profils NT/LDAP sont toujours créés actifs et non désactivables. Les autres profils sont toujours créés en inactif.
- Si un utilisateur est rattaché à un profil inactif, il n'aura pas les droits associés à ce profil.

Tous les utilisateurs rattachés à un profil NT/LDAP sont créés actifs et peuvent être désactivés.

En cas d'activation des profils non requise : tous les profils sont créés actifs.

En cas d'activation des sites requise :

- Les sites NT/LDAP sont toujours créés actifs et non désactivables. Les autres sites sont toujours créés en inactif.
- Tous les utilisateurs rattachés à un site NT/LDAP sont créés actifs et peuvent être désactivés.

En cas d'activation des sites non requise : tous les sites sont créés actifs.

En cas d'activation des utilisateurs requise :

- Tous les utilisateurs rattachés à un profil NT/LDAP sont créés actifs et peuvent être désactivés.
- Tous les utilisateurs rattachés à un site NT/LDAP sont créés actifs et peuvent être désactivés.
- Un utilisateur générique est créé inactif.
- Un utilisateur ne peut pas s'auto-activer.

- Un utilisateur inactif ne peut se connecter nulle part.

En cas d'activation des utilisateurs non requise : tous les utilisateurs sont créés actifs.

Le paramétrage de l'activation des données et de l'application de la règle des *4 yeux* est toujours soumis à la règle des *4 yeux*.

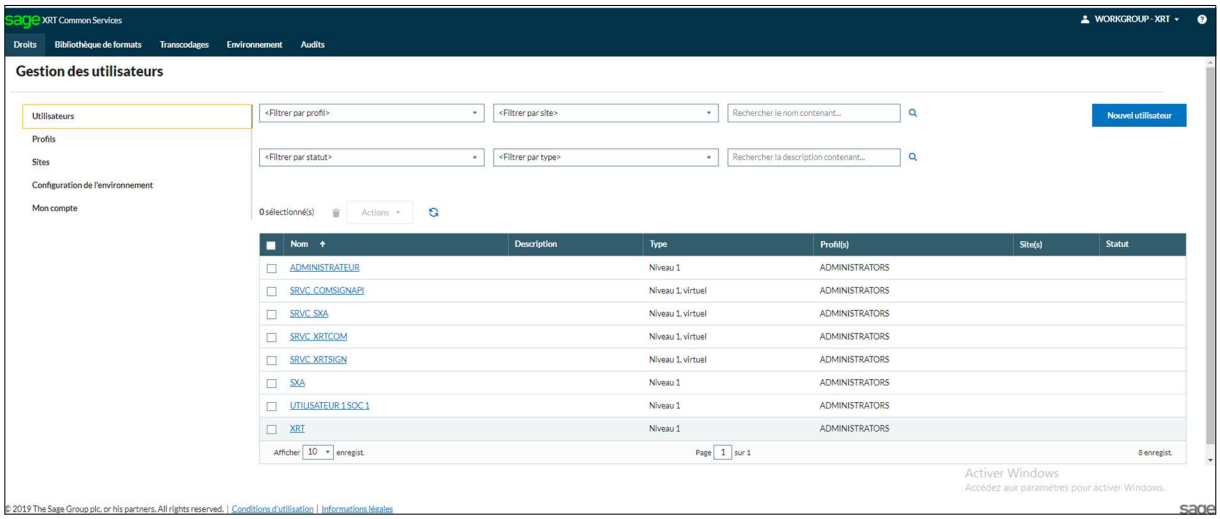
Compte utilisateur

Un compte utilisateur permet à un utilisateur de s'authentifier auprès d'une application *Sage XRT*. Il permet également de gérer les autorisations d'accès de cet utilisateur aux fonctionnalités de l'application.

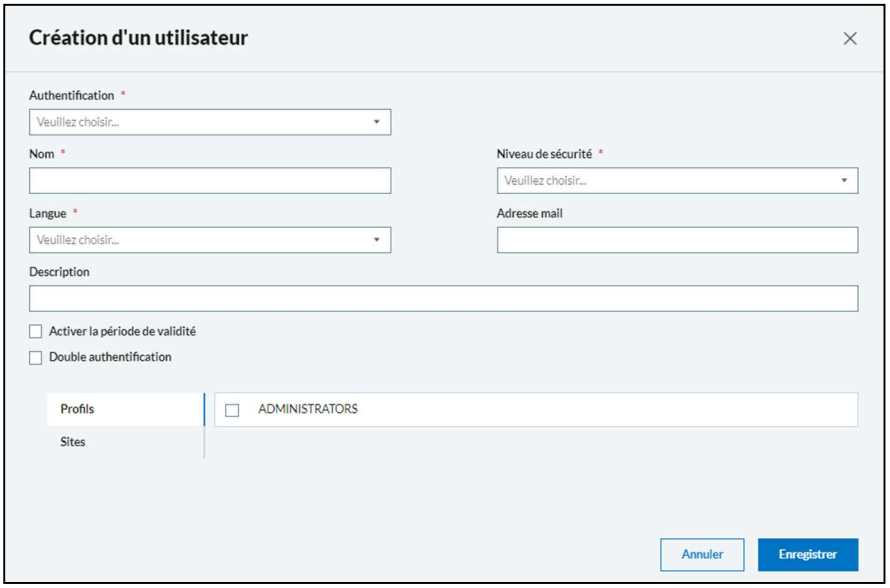
Un compte utilisateur comporte les éléments suivants :

- Langue de l'utilisateur (Français, Anglais, Espagnol, Portugais, Italien, Allemand)
- Adresse électronique de l'utilisateur pour envoi des notifications
- Description
- Type d'utilisateur (administrateur ou simple utilisateur)

Dans le menu **Droits**, cliquez sur l'onglet **Utilisateurs**.



Dans l'onglet **Gestion des utilisateurs**, le bouton **Nouvel utilisateur** vous permet d'accéder à l'assistant de création.



Sélectionnez un mode d'authentification et renseignez le nom de l'utilisateur :

- **Authentification Windows** : deux modes d'ajout d'un utilisateur NT :
    - Ajout via la sélection dans la liste présentée dans la boîte de dialogue. Les accès à la base de données doivent être définis préalablement pour chaque utilisateur.
    - Ajout via la recherche dans l'annuaire de l'entreprise. L'utilisateur hérite de l'accès à la base de données de type *XRTUsers*.
- **Authentification LDAP** : recherche et sélection des utilisateurs appartenant à l'annuaire paramétré dans la configuration de l'authentification *LDAP* donné grâce au bouton **Recherche**.
- **Authentification standard** : saisie d'un identifiant unique pour l'utilisateur.

Important ! Il est fortement conseillé de mettre en œuvre une gestion des accès reposant sur les comptes NT.

- **Authentification SAML** : saisie d'un identifiant *SSO* obligatoire fourni par l'*Identity Provider*.
- **Authentification Sage Id**

Option **Double authentification** : ce champ pourra être coché ou décoché à la création de l'utilisateur mais aussi quand il aura déjà été créé auparavant (modification utilisateur) quel que soit le type d'authentification (standard, *Windows*, *SageID*, etc.).

Si cette option est cochée, lors de sa première connexion, l'utilisateur doit initialiser cette authentification via la saisie d'un code secret obtenu après scan du code QR (ou saisie du code équivalent) grâce à une application compatible avec le protocole TOTP 6 digits (FreeOTP par exemple).

Tant que cette initialisation n'a pas lieu, l'option apparaît en orange. Par la suite, elle apparait en

vert.



Si un utilisateur perd (ou remplace) son smartphone ou désinstalle l'application d'authentification, il faudra réinitialiser son état pour qu'il puisse recréer le lien.

Pour cela, une option **Réinitialiser Double Authentification** est disponible dans la liste des utilisateurs.

Choisissez le type d'utilisateur à créer :

- **Administrateur de sécurité de niveau 1** : gère les droits d'accès des utilisateurs du groupe de travail.
- **Utilisateur standard** : utilisateur n'ayant aucun droit d'écriture ou de modification.

Complétez les informations qui suivent.

- **Langue** : sélectionnez dans la liste déroulante la langue d'usage de l'utilisateur.
- **Description** : saisissez une description pour l'utilisateur.
- **Adresse mail** : saisissez l'adresse email de l'utilisateur.
- **Période de validité** : cochez la case pour activer les trois champs permettant de définir la période de validité de l'utilisateur.

Rattachez éventuellement l'utilisateur à un profil et site.

Cliquez sur **Enregistrer** ou **Annuler** pour sortir de la boite de dialogue et revenir à la liste des utilisateurs.

Un utilisateur ne peut pas s'auto-activer.

Un utilisateur obtient le statut expiré lorsque sa période de validité a expiré.

Un utilisateur obtient le statut bloqué lorsque suite à l'application des règles de mot de passe, l'utilisateur n'est pas parvenu à se connecter.

Profils

La **Console d'Administration** est désormais activée. Vous avez la possibilité de créer un ou plusieurs profils pour les utilisateurs.

Par défaut, un utilisateur ne peut accéder à aucune fonctionnalité du produit. L'administrateur doit intervenir pour définir les droits d'accès des utilisateurs.

Un profil est constitué d'utilisateurs partageant les mêmes droits. Un droit autorise ou refuse l'accès à une fonction d'un produit par un utilisateur.

Important ! Un utilisateur peut appartenir à plusieurs profils.

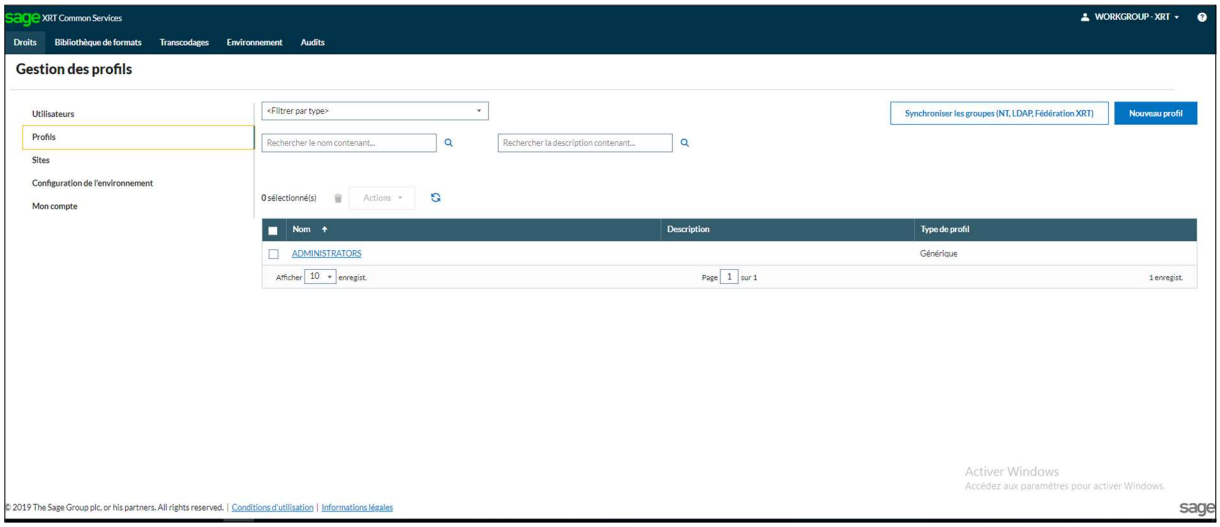
Un utilisateur est autorisé à accéder à une fonction d'un produit si la permission connexe est ouverte dans au moins un des profils auquel il appartient.

UMAPI exécute une opération de type OU sur les permissions. Ce mode de fonctionnement permet d'associer un profil à un groupe de personnes ayant les mêmes activités.

Un profil standard possède les propriétés suivantes :

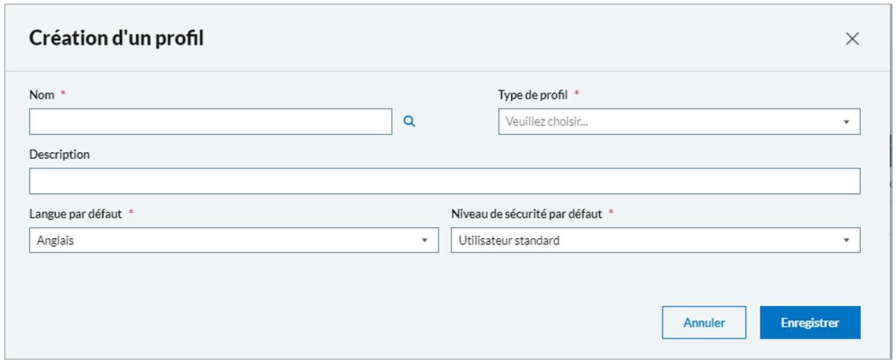
- Un **Code** qui identifie le profil (sans espace)
- Une **Description**

Dans le menu **Droits**, cliquez sur l'onglet **Profils**.



Création

Dans l'onglet **Profils**, le bouton **Nouveau profil** vous permet d'accéder à l'assistant de création.



Renseignez les informations suivantes :

- **Nom** : saisissez un nom pour le profil. Ce champ doit être renseigné obligatoirement.

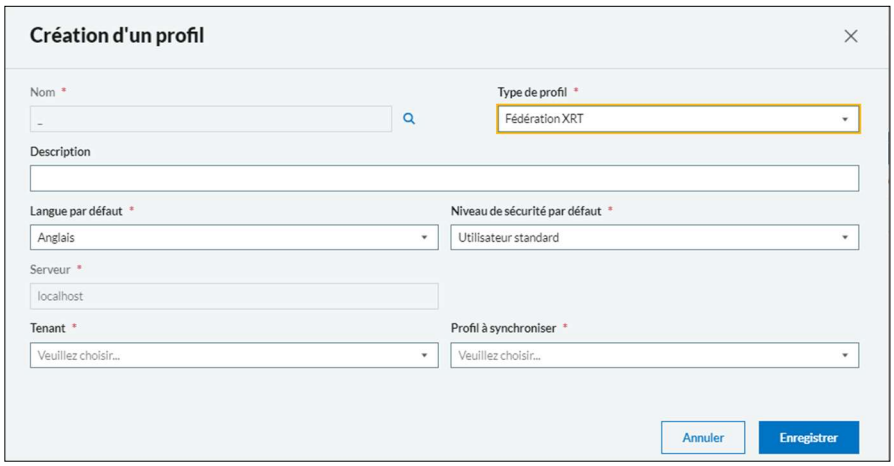
- **Description** : saisissez une description pour le profil.

Sélectionnez le type de profil :

- Générique : sélectionnez les utilisateurs existants à associer au profil.
- Groupe NT : tout utilisateur membre du groupe est automatiquement enregistré dans la base de données comme utilisateur des applications Sage XRT. Le profil de type Groupe AD s'appuie sur les données relatives aux comptes utilisateurs Windows NT. Sélectionnez la langue et le niveau de sécurité par défaut.
- Groupe LDAP : le profil de type Groupe LDAP s'appuie sur les données relatives à un annuaire d'entreprise. La création d'un groupe LDAP est effective uniquement si l'accès à l'annuaire d'entreprise a été paramétré. Sélectionnez la langue et le niveau de sécurité par défaut.
- Fédération XRT : le profil de type Fédération XRT permet de donner des droits aux utilisateurs d'un tenant sur un autre tenant sans avoir à les dupliquer. Sélectionnez la langue et le niveau de sécurité par défaut.

Lors de la création d'un profil NT ou d'un profil LDAP, tout utilisateur membre du groupe est automatiquement enregistré dans la base de données comme utilisateur des applications *Sage XRT*.

Lors de la création d'un profil Fédération XRT, vous devrez renseigner le tenant et le profil qui seront fédérés par le tenant de l'utilisateur connecté.



Exemple d'application pour la Fédération XRT

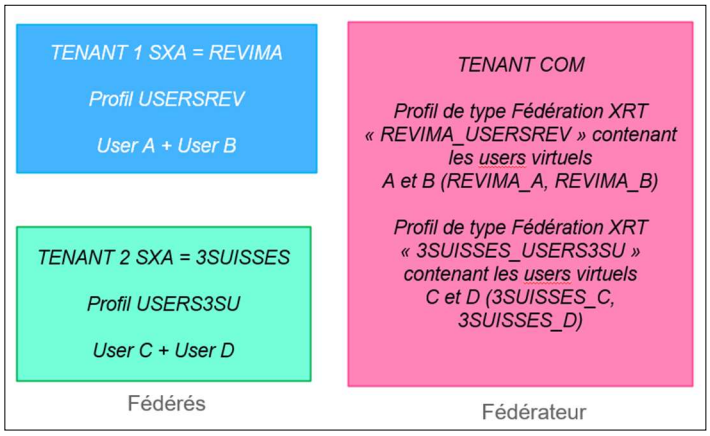
- Des utilisateurs du profil Signataire rattachés à un tenant SXA1 doivent avoir accès à la Signature et la Com rattaché au tenant FRPCOMSIGN.
- Des utilisateurs du profil Signataire rattachés à un tenant SXA2 doivent avoir accès à la Signature et la Com rattaché au tenant FRPCOMSIGN.

Dans cette situation, le tenant FRPCOMSIGN est fédérateur, les tenants SXA1 et SXA2 sont est fédérés. Les droits d'accès sont déclarés dans les tenants SXA.

Côté FRPCOMSIGN,

- un profil de type Fédération XRT va être créé et rattaché au tenant SXA1 et au profil Signataire.
- un profil de type Fédération XRT va être créé et rattaché au tenant SXA2 et au profil Signataire.

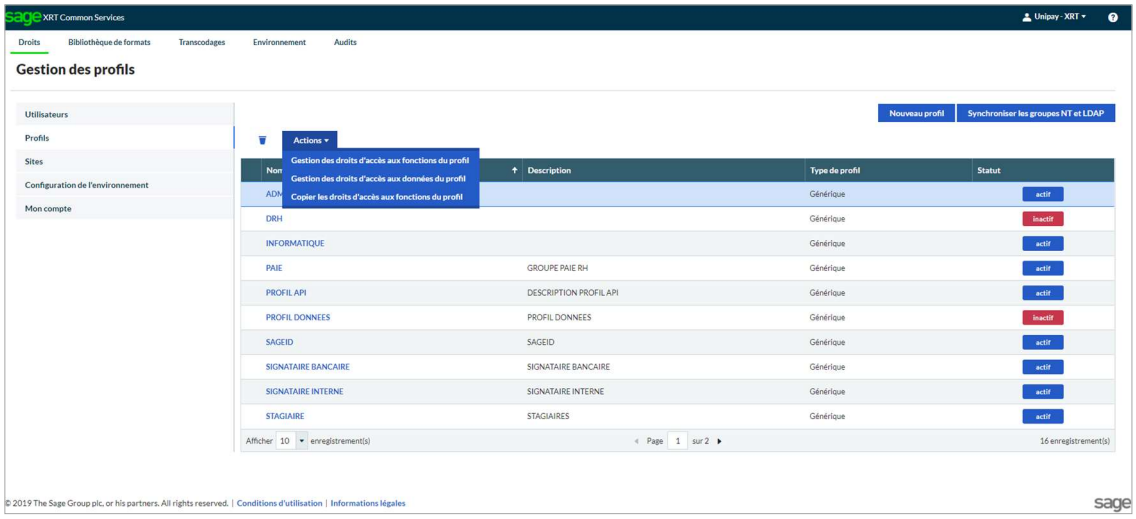
Les modifications des droits du profil doivent toujours se faire dans les tenants fédérés. La synchronisation de ces droits doit toujours se faire dans le tenant fédérateur.



Cliquez sur le bouton **Créer** pour valider la création du profil.

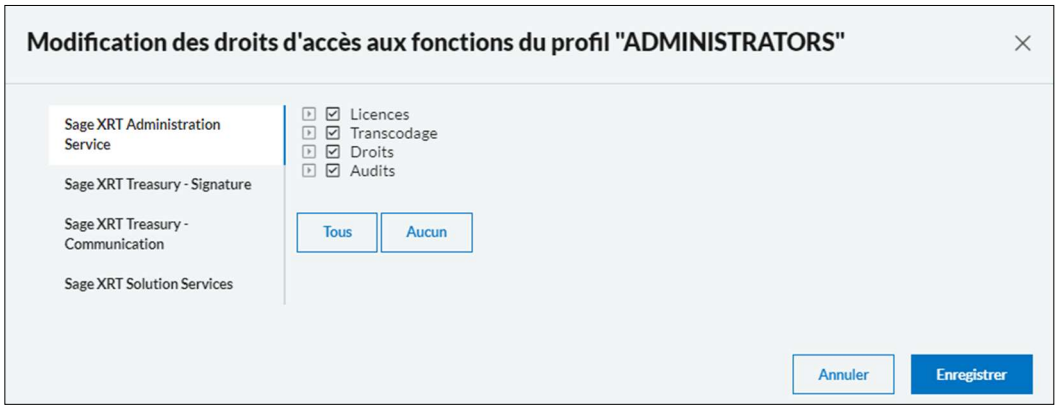
Dans l'onglet Profils, le bouton **Synchroniser les groupes** (NT, LDAP et Fédération XRT) vous permet de déclencher manuellement une synchronisation avec les annuaires.

Droits d'accès
A partir de la liste des profils, sélectionnez un **Profil** et sélectionnez l'action **Gérer les droits d'accès aux fonctions du profil**.



La page **Modification des droits d'accès aux fonctions** du profil permet de gérer les droits d'accès aux fonctions d'un profil pour les différents produits SAGE XRT Solution installés sur le serveur.

Cliquez sur l'onglet Sage XRT Administration Service.



Activez les droits à accorder unitairement ou utilisez les boutons **Tous** et **Aucun**.

Répétez l'opération pour les produits **SAGE XRT Solution AdvancedTreasury, SAGE XRT Solution Business Exchange** et **SAGE XRT Solution Common Services** si vous souhaitez attribuer des droits d'accès à ces deux produits pour le profil.

Cliquez sur **Enregistrer** pour enregistrer les modifications effectuées ou sur **Annuler** pour annuler les modifications.

Gestion des droits d'accès aux données du profil

Cette fonctionnalité est exploitée par **SAGE XRT Solution Functional Service** en mode autonome, i.e. non intégré à un autre produit tel que **SAGE XRT Solution Business Exchange** ou **SAGE XRT Solution Advanced Treasury**.

A partir de la liste des **Profils**, sélectionnez un profil et sélectionnez l'action **Gestion des droits d'accès aux données du profil**.

Par type de données (onglets **Origine**, **Entité**, **Banque**, **Compte**, **Devise**), sélectionnez les éléments ne devant pas être accessibles aux utilisateurs rattachés à ce profil. Par défaut, tous les éléments sont accessibles.

Cliquez sur le bouton **Enregistrer** pour sauvegarder le paramétrage.

La case à cocher **Afficher uniquement les données inaccessibles**, décochée par défaut, permet de filtrer les éléments affichés pour ne faire apparaître que les éléments inaccessibles.



Duplication

A partir de la liste des **Profils**, sélectionnez un profil, puis l'action Copier les droits d'accès aux fonctions du profil. L'assistant de création d'un Profil s'affiche.

Complétez les informations du profil et cliquez sur **Créer.** Ce nouveau profil rassemble automatiquement les droits d'accès aux fonctions du profil copié.

Modification

Dans le menu **Droits**, cliquez sur l'onglet **Profils**. La liste des profils existants s'affiche.

Pour modifier un profil, utilisez le lien disponible sur le nom du profil.

Procédez aux modifications souhaitées et cliquez sur le bouton **Enregistrer**.

Suppression

Dans le menu **Droits**, cliquez sur l'onglet **Profils**. La liste des profils existants s'affiche.

Pour supprimer un profil, sélectionnez la case à cocher correspondante et cliquez sur l'icône *corbeille*.

Activation

Tout profil créé obtient le statut **Inactif** et devra faire l'objet d'une activation par un autre utilisateur de niveau Administrateur.

A partir de la liste des **Profils**, sélectionnez le profil à activer.

Cliquez sur le statut **Inactif** et confirmez l'activation du profil.

Un message vous confirme l'activation du profil.

Désactivation

A partir de la liste des **Profils**, sélectionnez le profil à désactiver.

Cliquez sur le statut **Actif** et confirmez la désactivation du profil.

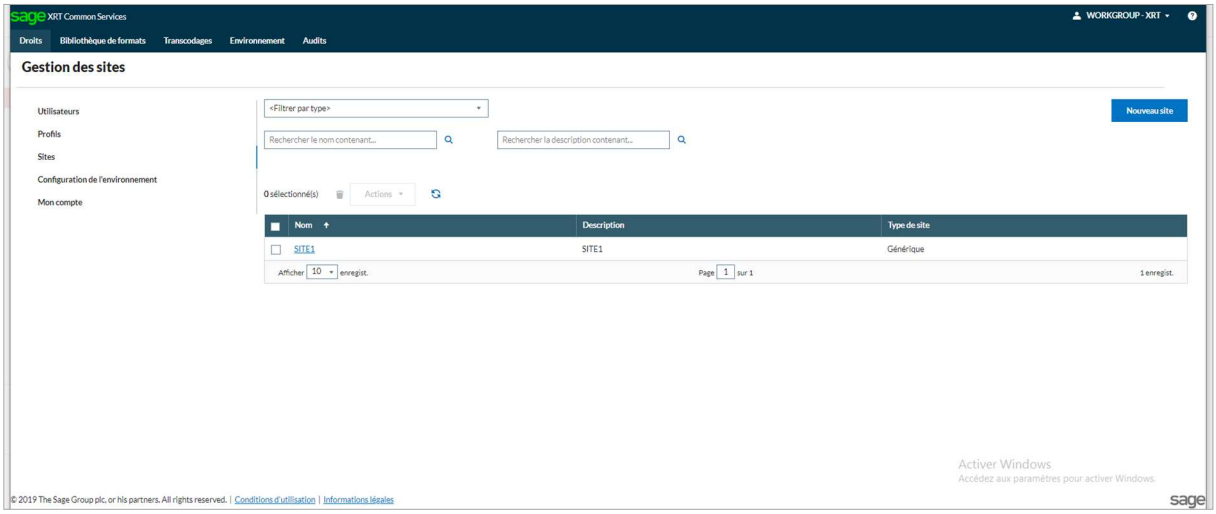
Un message vous confirme la désactivation du profil.

Sites

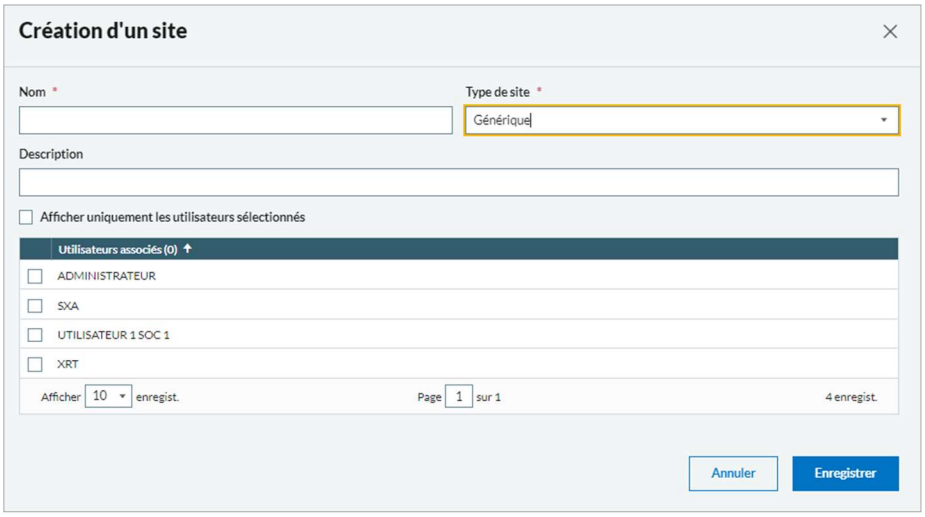
Création

La création des sites suit les mêmes règles que celle des profils.

Dans le menu **Droits**, cliquez sur l'onglet **Site**.



Le bouton **Nouveau site** vous permet d'accéder à l'assistant de création.



Renseignez les informations suivantes :

- **Nom** : saisissez un nom pour le site. Ce champ doit être renseigné obligatoirement.
- **Description** : saisissez une description pour le site.

Sélectionnez le type de site :

- **Générique** : sélectionnez les utilisateurs existants à associer au site.
- **Groupe AD** : tout utilisateur membre du groupe est automatiquement enregistré dans la base de données comme utilisateur des applications *Sage XRT*. Le site de type Groupe AD s'appuie sur les données relatives aux comptes utilisateurs Windows NT.
- **Groupe LDAP** : le site de type **Groupe LDAP** s'appuie sur les données relatives à un annuaire d'entreprise. La création d'un groupe LDAP est effective uniquement si l'accès à l'annuaire d'entreprise a été paramétré.

Cliquez sur le bouton **Créer** pour valider la création du site.

Modification

Dans le menu **Droits**, cliquez sur l'onglet **Site**. La liste des sites existants s'affiche.

Pour modifier un site, utilisez le lien disponible sur le nom du site.

Procédez aux modifications souhaitées et cliquez sur le bouton **Enregistrer**.

Suppression

Dans le menu **Droits**, cliquez sur l'onglet **Site**. La liste des sites existants s'affiche.

Pour supprimer un site, sélectionnez la case à cocher correspondante et utilisez l'icône *corbeille*.

Activation

Tout site créé obtient le statut **Inactif** et devra faire l'objet d'une activation par un autre utilisateur de niveau Administrateur.

A partir de la liste des sites, sélectionnez le site à activer.

Cliquez sur le statut **Inactif** et confirmez l'activation du site. Un message vous confirme l'activation du site.

Désactivation

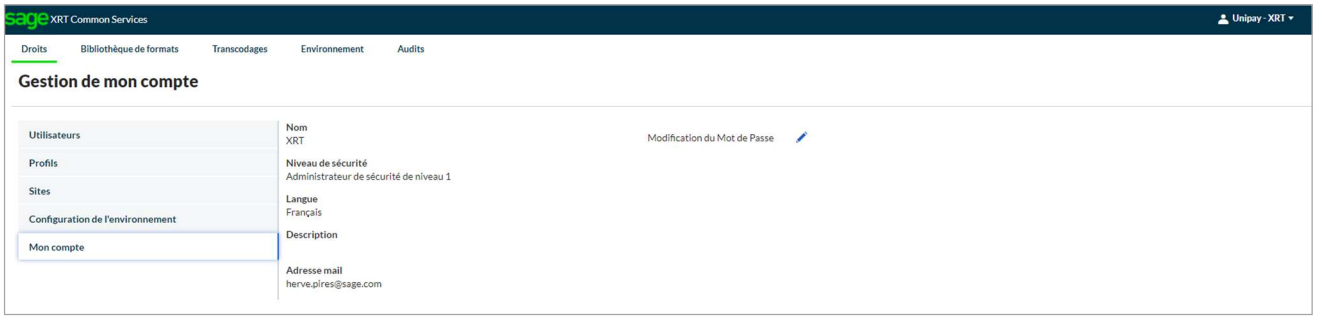
A partir de la liste des sites, sélectionnez le site à désactiver.

Cliquez sur le statut **Actif** et confirmez votre action. Un message vous confirme la désactivation du site.

Mon compte

Cet onglet est accessible aux utilisateurs de type **Standard**. Elle permet de modifier le mot de passe de l'utilisateur connecté.

Dans le menu **Droits**, cliquez sur l'onglet **Mon compte**.



Les informations de l'utilisateur sont rappelées : **Nom**, **Niveau de sécurité**, **Langue**, **Description**, **Adresse mail**.

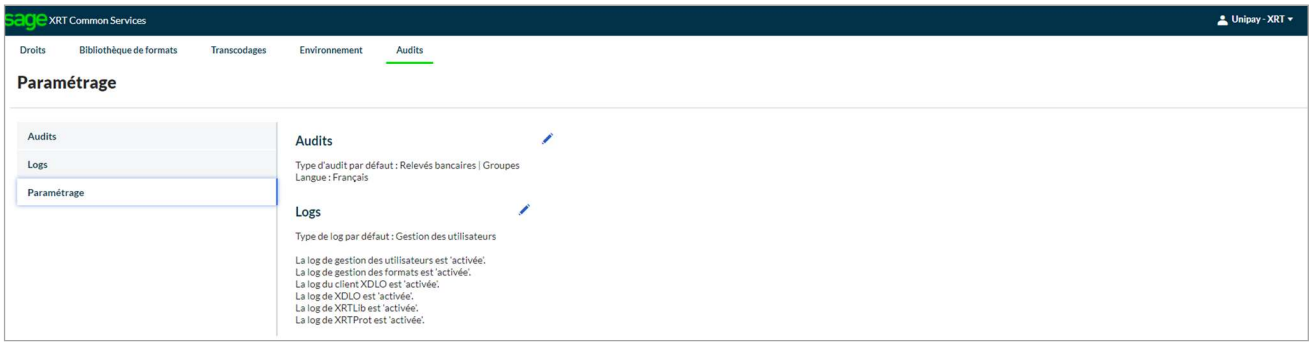
Seul le mot de passe peut être modifié en utilisant l'icône *crayon*.

Audits et logs

Paramétrage

Vous devez définir le type d'audit présenté ainsi que l'activation des logs avant de pouvoir consulter des informations.

Dans le menu **Audits**, cliquez sur l'onglet **Paramétrage**.



Le paramétrage est ici résumé. Il peut être modifié en cliquant sur l'icône *crayon*.

Sélectionnez le type d'audit à proposer par défaut :

- Système
- Base de données
- Utilisateurs
- Relevés bancaires | Relevés de compte
- Relevés bancaires | Relevés intraday
- Relevés bancaires | Relevés d'opération
- Relevés bancaires | Relevés de statut
- Relevés bancaires | Importation de relevés
- Relevés bancaires | Exportation de données
- Relevés bancaires | Reporting
- Relevés bancaires | Purge

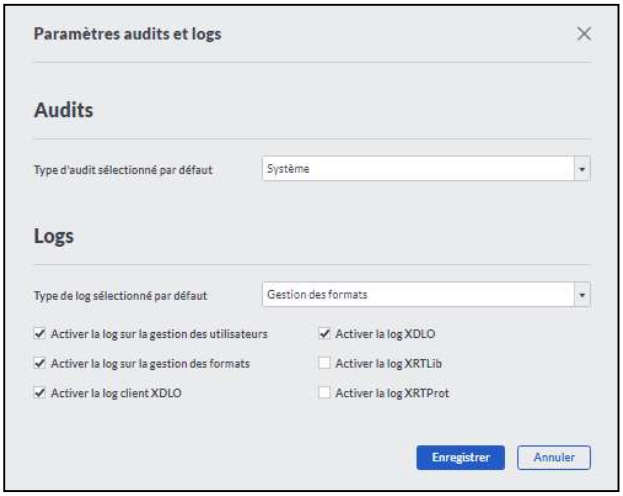
- Relevés bancaires | Groupes
- Signature | Certificats
- Signature | Mots de passe
- Signature | Fichiers
- Signature | Tableaux de bord
- Antifraude | Liste blanche
- Antifraude | Liste noire
- Antifraude | Listes officielles
- Antifraude | Liste des mandats autorisés
- Antifraude | Transactions à risque

Sélectionnez le type de log à proposer par défaut :

- Gestion des formats
- Gestion des utilisateurs
- Gestion base de données
- Gestion de la console
- Client XDLO
- XDLO
- Service XDLO
- XRTProt
- XRTLogin
- XRTLib

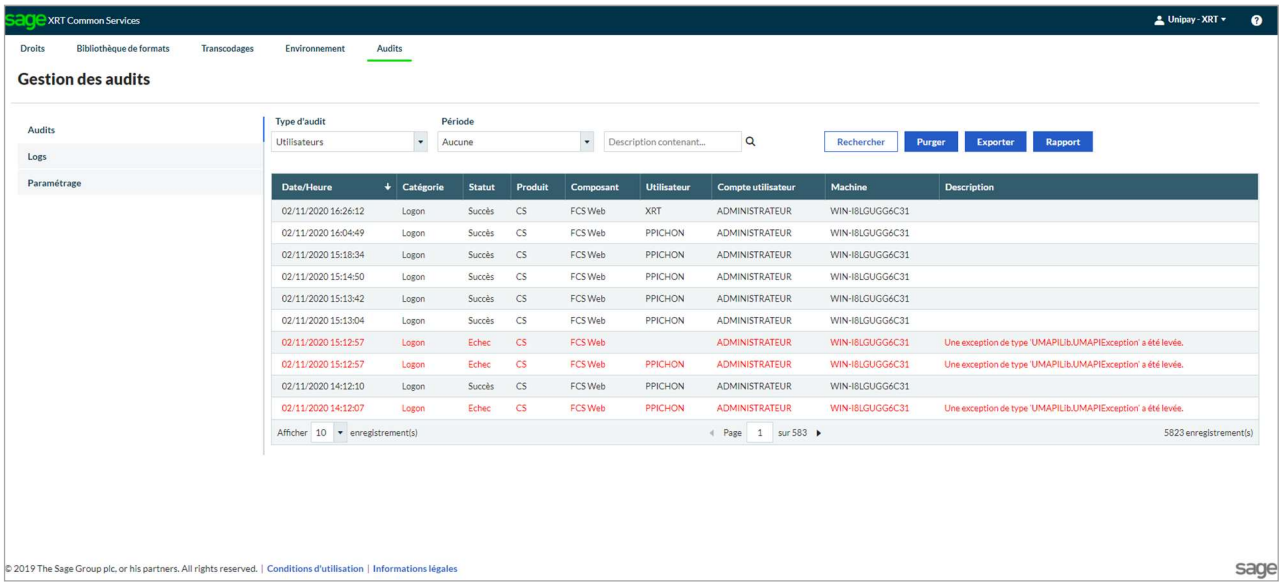
Sélectionnez les logs à activer.

Cliquez sur le bouton **Enregistrer** pour terminer votre paramétrage.



Audit

Dans le menu **Audits**, cliquez sur l'onglet **Audit**. Le type d'audit défini par défaut s'affiche.



Pour modifier le type d'audit par défaut, sélectionnez une option dans la liste déroulante **Type d'audit**.

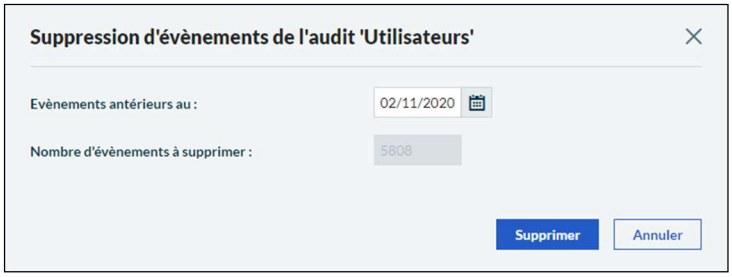
Pour filtrer les informations du tableau, sélectionnez une **Période** dans liste déroulante :

- Aujourd'hui
- 7 derniers jours
- 30 derniers jours
- 12 derniers mois
- Cette semaine
- Ce mois

- Cette année

Vous pouvez accéder à d'autres critères de sélection en utilisant le bouton **Rechercher**. Les critères de filtre appliqués sont rappelés au-dessus de la liste.

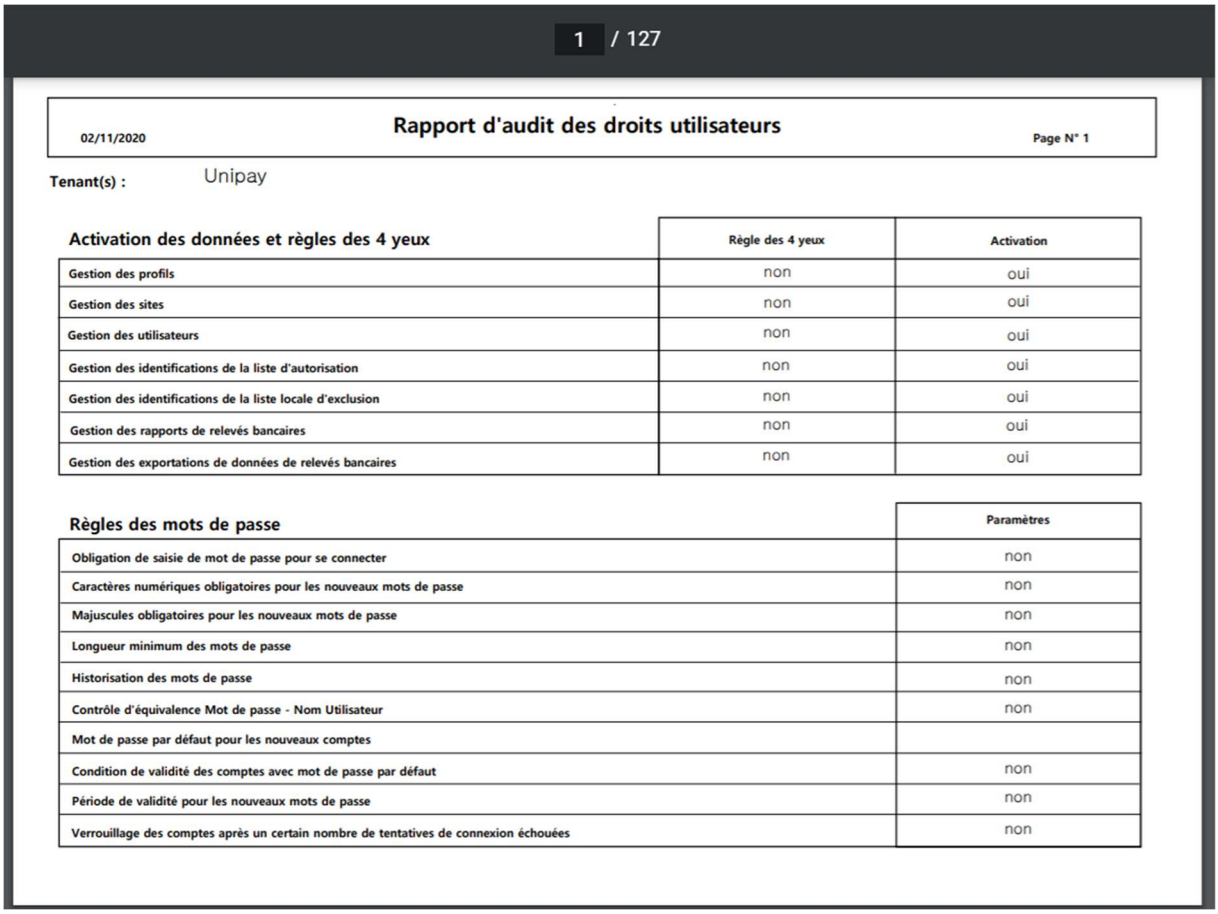
Cliquez sur le bouton **Purger** pour supprimer des évènements de la liste.



Cliquez sur le bouton **Exporter** pour exporter des évènements de la liste.



Lorsque le type d'audit est **Utilisateurs**, le bouton **Rapport** vous permet de lancer l'édition du rapport d'audit des utilisateurs (état des droits de chaque utilisateur et des règles de sécurité appliquées).



1 / 127

02/11/2020 **Rapport d'audit des droits utilisateurs** Page N° 1

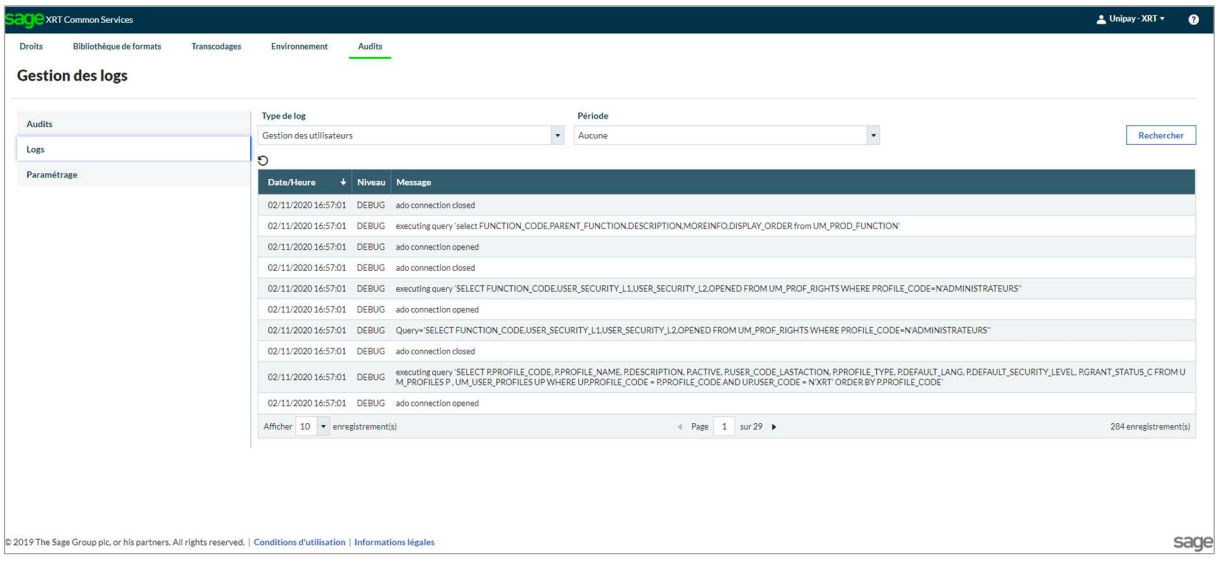
Tenant(s) : Unipay

Activation des données et règles des 4 yeux	Règle des 4 yeux	Activation
Gestion des profils	non	oui
Gestion des sites	non	oui
Gestion des utilisateurs	non	oui
Gestion des identifications de la liste d'autorisation	non	oui
Gestion des identifications de la liste locale d'exclusion	non	oui
Gestion des rapports de relevés bancaires	non	oui
Gestion des exportations de données de relevés bancaires	non	oui

Règles des mots de passe	Paramètres
Obligation de saisie de mot de passe pour se connecter	non
Caractères numériques obligatoires pour les nouveaux mots de passe	non
Majuscules obligatoires pour les nouveaux mots de passe	non
Longueur minimum des mots de passe	non
Historisation des mots de passe	non
Contrôle d'équivalence Mot de passe - Nom Utilisateur	non
Mot de passe par défaut pour les nouveaux comptes	
Condition de validité des comptes avec mot de passe par défaut	non
Période de validité pour les nouveaux mots de passe	non
Verrouillage des comptes après un certain nombre de tentatives de connexion échouées	non

Log

Dans le menu **Audits**, cliquez sur l'onglet **Log**. Le type de log par défaut s'affiche.



Pour le modifier, sélectionnez un **Type de log** dans la liste déroulante.

Pour filtrer les informations du tableau, sélectionnez une **Période** dans liste déroulante :

- Aujourd'hui

- 7 derniers jours
- 30 derniers jours
- 12 derniers mois
- Cette semaine
- Ce mois
- Cette année

Vous pouvez accéder à d'autres critères de sélection en utilisant le bouton **Rechercher**. Les critères de filtre appliqués sont rappelés au-dessus de la liste.

XDLO (obsolète)

Le service XDLO n'existe plus.

SAGE XRT Solution Common Services

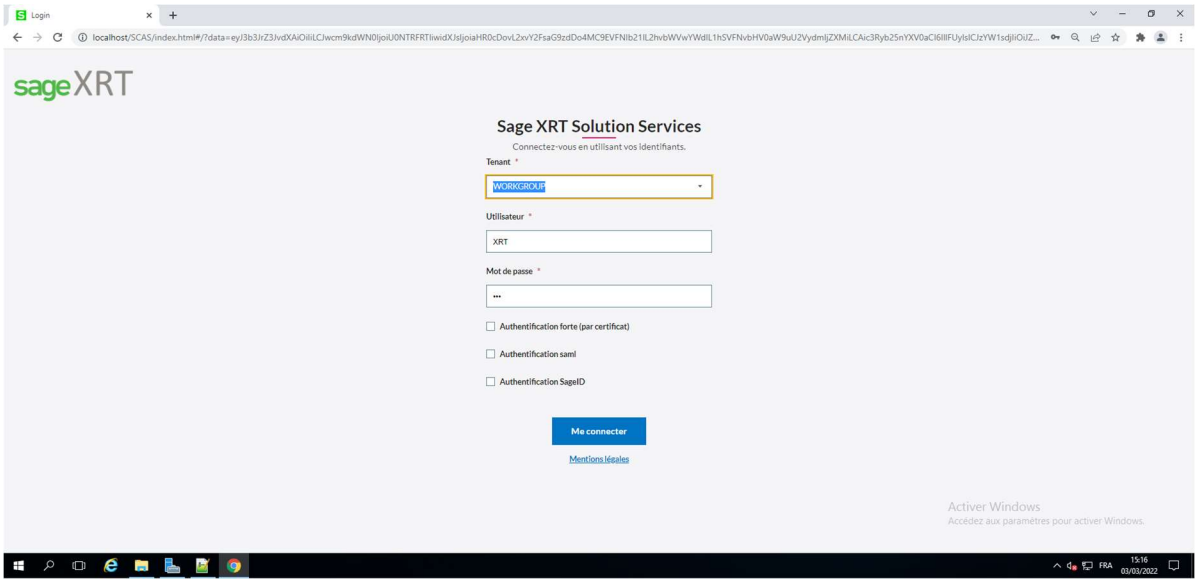
Configuration

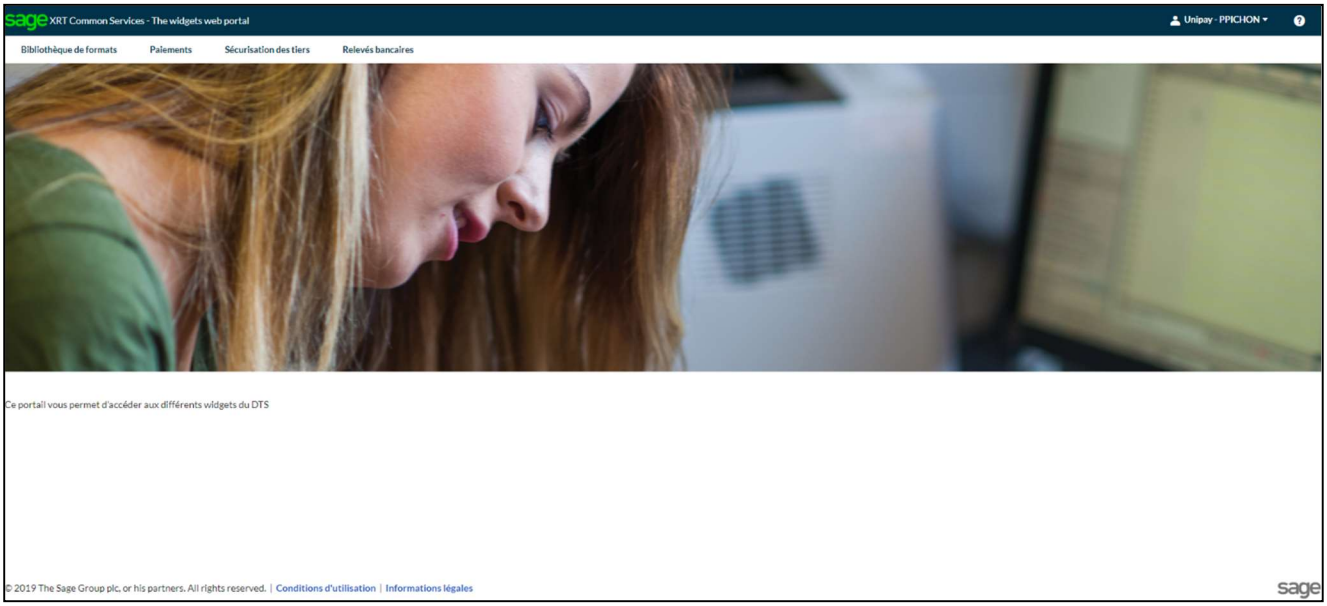
Le fichier de configuration *Sage.SCDTSServer.Service.exe.config* pour le service des fonctionnalités se situe par défaut sous : **C:\Program Files\Common Files\xrt**.

Cf. Annexes pour le détail de chaque paramètre.

Connexion

L'utilisation de l'interface de **SAGE XRT Solution Common Services** se fait via l'URL **http://localhost/XRTSolutionervices/index.html** et nécessite le démarrage des services d'authentification et des fonctionnalités.





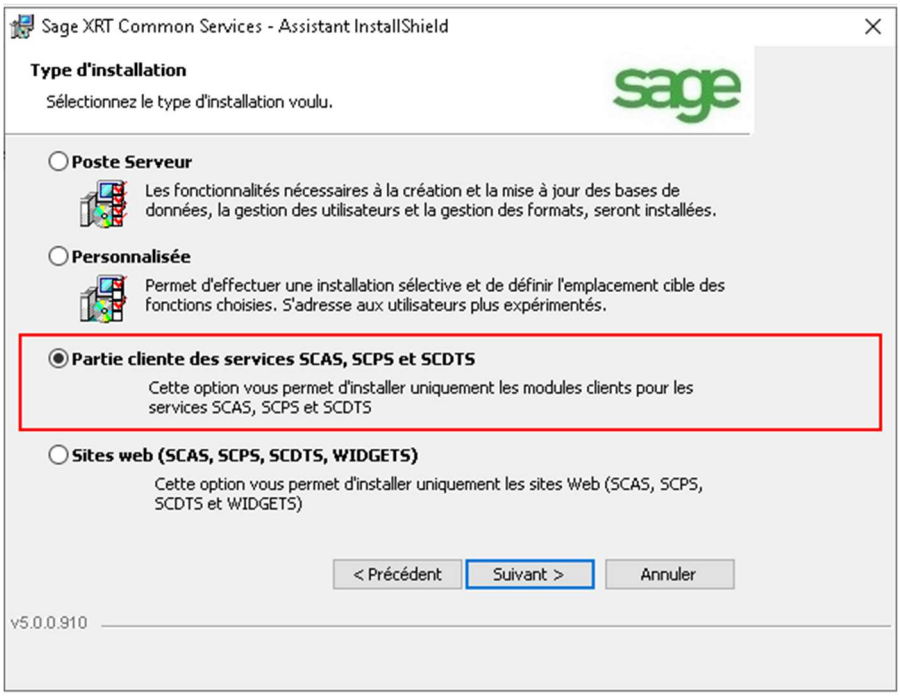
Ce service offre des fonctionnalités autour des thèmes :

- Bibliothèque des formats et transcodage
- Gestion des paiements
- Relevés bancaires (disponible à partir de la version 5.1)
- Contrats de communication standard
- Historique de communication
- Contrôles Antifraude

Chaque famille de fonctionnalités fait l'objet d'un document dédié.

Librairie Sage.FCS.Client

Cette librairie est une *DLL* compatible en 32 bits et 64 bits. Elle peut être utilisée soit comme une librairie *.NET* soit comme un composant *COM*. Cette librairie s'installe sur le poste client à travers le profil **Partie cliente des services SCAS, SCPS et SCDTS** de la procédure d'installation de **SAGE XRT Solution Common Services**.



Pour une intégration en tant que composant *COM* dans une application 32 bits il faut enregistrer la *DLL* avec le *RegAsm.exe* du *framework .NET* 32 bits.

Utilisation

Sage.Fcs.Client permet de consommer de façon transparente un ensemble d'API Rest hébergé par les services d'Authentification (**SCASServer**), d'Administration (**SCPSServer**) et de Fonctionnalités (**SCDTSServer**) de **SAGE XRT Solution Common Services**. Ainsi les applications intégrant cette librairie feront juste des appels à des méthodes. La localisation du serveur **SAGE XRT Solution Common Services** se fait grâce au paramétrage du fichier de configuration *Sage.Fcs.Client.dll.config*.

Exemple de fichier de configuration :

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <!-- The auto generate certificate CN is Sage.fcs.client -->
```

```
 <appSettings>
  <add key="securitylevel" value="http"/>
  <add key="http_servicehost_SCASServer" value="http://localhost:80/Auth" />
  <add key="https_servicehost_SCASServer" value="https://localhost:443/Auth" />
  <add key="http_servicehost_SCDTSServer" value="http://localhost:80" />
  <add key="https_servicehost_SCDTSServer" value="https://localhost:443" />
  <add key="http_servicehost_SCPSServer" value="http://localhost:80"/>
  <add key="https_servicehost_SCPSServer" value="https://localhost:443"/>
  <add key="AutoGenerateCertificate" value="true"/>
  <add key="SerialNumber" value=""/>
  <add key="ApifmtResponseTimeout" value="180"/>
  <add key="ApifmtBaseTimeTry" value="2"/>
  <add key="ApifmtPdfViewer" value="none"/>
  <add key="ApifmtPrinter" value="none"/>
 </appSettings>
</configuration>
```

Description des méthodes intégrées

ID	
2	object WorkgroupList()
3	void DoLogin(object p_oReq)
4	void CheckSession()
5	void CheckUser(object p_oReq)
6	void Disconnect()
7	void DoLoginForm(LoginProductID product, string version, string component, LanguageID language)
8	void DoLoginService(object p_oReq)
9	void PasswordUpdatingByActionForm()
10	void PasswordUpdatingByAction(object p_oReq)
11	object ProjectList(object p_oReq)
12	object WorkList(object p_oReq)

ID	
13	object UserList(object p_oReq)
14	object UserInfos(object p_oReq)
15	void RefreshToken()
16	object TranscoTableList()
17	object ProfileList()
18	object FormatList()
19	object FamilyList()
20	object ProductList()
21	object FunctionRights(object p_oReq)
22	object PwdInfos()
23	object LicenseDetails(object p_oReq)
24	object LicenseList()
25	void LicenseCreateForm()
26	void LicenseMigrate(object p_oReq)
27	object ConnectionString(object p_oReq)
28	object UmDataVersion()
29	void ImpStmt(object p_oReq)
30	object WorkExec(object p_oReq)
31	object GenericWorkExec(object p_oReq)
32	object OdbcTextSeparator()
33	void SetConfigFile(object p_oReq)
34	object UmFeaturesProductKey(object p_oReq)
35	object ProductRights(object p_oReq)
36	object ParamsInfosForClint()
37	void GrpImportBatchStmt(object p_oReq)
38	object PayPostTrn(object p_oReq)

ID	
39	object PayFollowBatch(object p_oReq)
40	object WorkgroupListNt(object p_oReq)
41	void OpeGetDataToCtrl(object p_oReq)
42	object GetFrpSessionConnInfo(object p_oReq)
43	object GetSxaCodetrnIssuingagentbic(object p_oReq)

Application sage.fcs.apifmt.exe

Cette application console permet d'obtenir le résultat de l'exécution distante d'un traitement de l'API des formats.

Installation

L'installation de cette application est effectuée par l'installation du produit **SAGE XRT Solution Common Services**, par la sélection du composant **FCS DLLs** ou du composant **Partie cliente des services SCAS, SCPS et SCDTS**. Hors désélection de ces deux composants lors d'une installation personnalisée, cette application est donc installée par défaut dans toutes les configurations sauf **Sites Web (SCAS, SCPS, SCDTS et WIDGETS)**.

Deux fichiers sont installés : *sage.fcs.apifmt.exe* et *sage.fcs.apifmt.exe.config*.

Le fichier de configuration *sage.fcs.apifmt.exe.config* associé à l'exécutable *sage.fcs. apifmt.exe* est utilisé pour la déclaration de l'emplacement du service d'authentification ainsi que celui du service de transformation des données.

Configuration

Le contenu du fichier *sage.fcs.apifmt.exe.config* est par défaut le suivant :

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <appSettings>
    <add key="securitylevel" value="http"/>
    <add key="http_servicehost_SCASServer" value="http://localhost:80/Auth" />
    <add key="https_servicehost_SCASServer" value="https://localhost:443/Auth" />
    <add key="http_servicehost_SCDTSServer" value="http://localhost:80" />
    <add key="https_servicehost_SCDTSServer" value="https://localhost:443" />
  </appSettings>
</configuration>
```

Service d'authentification

Ce fichier permet d'effectuer la déclaration du service d'authentification qui est contacté pour la vérification du mot de passe de l'utilisateur.

Dans le cas où celui-ci fonctionne en mode sécurisé *HTTPS*, il faut apporter la modification à la ligne suivante :

<add key="securitylevel" value="https"/>

Pour un mode non sécurisé, la ligne suivante est exploitée :

<add key="http_servicehost_SCASServer" value="http://localhost:80/Auth" />

Pour un mode sécurisé, la ligne suivante est exploitée :

<add key="https_servicehost_SCASServer" value="https://localhost:443/Auth" />

Vous devez effectuer la modification de *value* pour tenir compte des spécificités de chaque installation.

Pour rappel, l'utilisation d'un certificat au niveau du service d'authentification (pour effectuer le déchiffrement du mot de passe) se fait en modifiant le fichier de configuration de ce dernier (*Sage.SCASServer.Service.exe.config*) et en renseignant le numéro de série du certificat sur la ligne suivante :

<add key="serialnumberforpwdcrypt" value="3526df91b8be9ab046a226d0390a764f" />

Si la *value* de cette zone est laissée vide, alors le paramètre **/PWT=RSA** (cf. Utilisation) ne pourra pas être exploité avec ce service d'authentification.

Service de transformation des données

Ce fichier permet également d'effectuer la déclaration du service de transformation des données qui est contacté pour effectuer l'exécution du traitement demandé.

Dans le cas où celui-ci fonctionne en mode sécurisé *https*, il faut apporter la modification à la ligne suivante :

<add key="securitylevel" value="https"/>

Pour un mode non sécurisé, la ligne suivante est exploitée :

<add key="http_servicehost_SCDTSServer" value="http://localhost:80/Auth" />

Pour un mode sécurisé, la ligne suivante est exploitée :

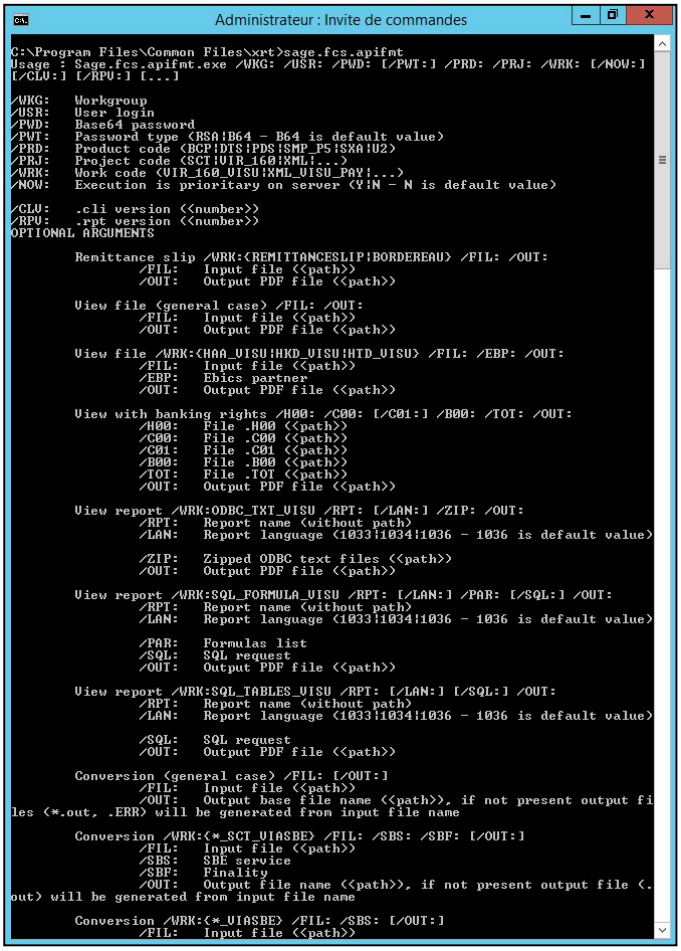
<add key="https_servicehost_SCDTSServer" value="https://localhost:443/Auth" />

Vous devez effectuer la modification de *value* pour tenir compte des spécificités de chaque installation.

Permissions

Afin de pouvoir exécuter un traitement sans erreur, l'utilisateur passé en paramètre (**/USR**) doit appartenir à un profil ayant au minimum les permissions suivantes dans **SAGE XRT Solution Common services**, partie **Bibliothèque de formats – Formats – Produits** :

- Visualiser les détails d'un traitement (dans tous les cas)
- Exécuter un traitement synchrone (si **/NOW :YES** est utilisé)
- Exécuter un traitement asynchrone et Récupérer le résultat d'un traitement asynchrone (si **/NOW :FALSE** est utilisé)



Utilisation

Paramètres de base

Tenant /WKG

Ce paramètre est obligatoire puisqu'il permet d'indiquer quelle base de données est utilisée avec les services d'authentification et de transformation de données.

Utilisateur /USR

Ce paramètre est obligatoire puisqu'il permet d'indiquer quel utilisateur est utilisé pour l'authentification et les permissions associées au profil auquel celui-ci est rattaché.

Mot de passe /PWD

Ce paramètre est obligatoire puisqu'il permet d'indiquer quel est le mot de passe associé à l'utilisateur. Celui-ci ne doit pas apparaitre en clair : il doit être obtenu à l'aide de l'application console **sage.fcs.pwdencode.exe** (cf. ci-après).

Type de mot de passe /PWT

Ce paramètre est optionnel.

La valeur à positionner dépend du paramétrage de chiffrement souhaité pour le mot de passe du service d'authentification. Par défaut il a pour valeur **B64**, ce qui correspond à un encodage Base64 uniquement. Dans le cas où l'encodage par défaut ne convient pas, vous devez positionner

la valeur **RSA** pour ce paramètre.

Produit /PRD

Ce paramètre est obligatoire puisqu'il correspond au code produit contenant le traitement à exécuter (ex. : **BCP** pour **Sage XRT Solution Advanced Communication**).

Projet /PRJ

Ce paramètre est obligatoire puisqu'il correspond au code projet contenant le traitement à exécuter (ex. : **SCT** pour Format SCT SEPA).

Traitement /WRK

Ce paramètre est obligatoire puisqu'il correspond au code du traitement à exécuter (ex. : **SCT_VISU_PAY** pour Edition du SCT SEPA).

Type d'exécution (/NOW)

Ce paramètre est optionnel.

Par défaut sa valeur est positionnée à **N**, ce qui correspond à une demande d'exécution asynchrone du traitement. L'application demande si l'exécution a été traitée par le serveur de transformation des données, l'attente étant déterminée par la taille du fichier en entrée. Par défaut, l'attente est de 30 secondes.

Un traitement déterminé comme relativement léger peut être exécuté en positionnant le paramètre à **Y**. L'exécution est alors synchrone et le résultat est obtenu aussitôt son traitement sur le serveur terminé.

Version du fichier Clint /CLV

Ce paramètre n'est pas encore exploitable. Il permet d'indiquer la version du fichier *.cli* à exécuter dans le cas où un traitement Clint spécifique a été dérivé du traitement *Clint* original.

Version du fichier Crystal Report /RPV

Ce paramètre n'est pas encore exploitable. Il permet d'indiquer la version du fichier *.rpt* à exécuter dans le cas où un rapport *Crystal Report* spécifique a été dérivé du rapport original.

Paramètres spécifiques

Plusieurs familles de traitements ont été définies par défaut et une aide sur l'utilisation de paramètres spécifiques est disponible sur la ligne de commande sous la rubrique **OPTIONAL ARGUMENTS**.

Remittance slip /WRK:{REMITTANCESLIP|BORDEREAU} /FIL: /OUT:

View file (general case) /FIL: /OUT:

View file (Ebics) /WRK:{HAA_VISU|HKD_VISU|HTD_VISU} /FIL: /EBP: /OUT:

View with banking rights /H00: /C00: [/C01:] /B00: /TOT: /OUT:

View report /WRK:ODBC_TXT_VISU /RPT: [/LAN:] /ZIP: /OUT:

View report /WRK:SQL_FORMULA_VISU /RPT: [/LAN:] /PAR: [/SQL:] /OUT:

View report /WRK:SQL_TABLES_VISU /RPT: [/LAN:] [/SQL:] /OUT:

Conversion (general case) /FIL: [/OUT:]

Conversion /WRK:{*_SCT_VIASBE} /FIL: /SBS: /SBF: [/OUT:]

Conversion /WRK:{*_VIASBE}/FIL: /SBS: [/OUT:]

Conversion /WRK:P160_2_SDD_VIA_FRPPAIEMENT /FIL: /FPT: /FPR: [/OUT:]

Conversion /WRK:{*_RB7|*_RB9}/FIL: /RBB: [/OUT:]

Prepare file /WRK:Prepa /FIL: /OUT:

Invalid records /WRK:DelRejet /FIL: /REJ: /OUT:

Valid records /WRK:DelSigne /FIL: /REJ: /OUT:

Bank Import /WRK:{BCP_GEN_CERG|CONV_FMT_CERG}/FIL: /OUT:

Filter bank statements /WRK:UPDATEFILE /FIL: /UFP: /UFT: /UFS: /UFC: /OUT:

Bank Import /WRK:BFI_MQ /FIL: /QUE: /BNK: /OUT:

File generation for U2 /FIL: /OUT:

Execute /ARG: [/FIL: /OUT:]

Exemples

Vous devez positionner les paramètres de base (cf. plus haut) avant les paramètres spécifiques des exemples qui suivent.

Exemple : Dans le cas où un utilisateur **XRT**, ayant pour mot de passe **XRT**, veut exécuter un traitement synchrone sur un workgroup **SXBE32TO64**, il faut ajouter cette partie de code au préalable :

Sage.fcs.apifmt.exe /NOW:Y /WKG:SXBE32TO64 /USR:XRT /PWD:WFJU

Remittance slip /WRK:{REMITTANCESLIP|BORDEREAU}/FIL: /OUT:

/PRD:BCP /PRJ:VIR_160 /WRK:BORDEREAU /FIL:"C:\file.160" /OUT:"C:\file.pdf"

View file (general case) /FIL: /OUT:

PRD:SMP_P5 /PRJ:SCT /WRK:SCT_VISU_PAY /FIL:"C:\file.xml" /OUT:"C:\file.pdf"

View file (Ebics) /WRK:{HAA_VISU|HKD_VISU|HTD_VISU}/FIL: /EBP: /OUT:

/PRJ:EBICS_Requests /WRK:HKD_VISU /FIL:"C:\file.hkd" /EBP:Partner /OUT:"C:\file.pdf"

View with banking rights /H00: /C00: [/C01:] /B00: /TOT: /OUT:

/PRD:PDS /PRJ:SCT /WRK:SCT_VISU_PAY /H00:"C:\file.H00" /C00:"C:\file.C00" /B00:"C:\file.B00" /TOT:"C:\file.TOT" /OUT:"C:\file.pdf"

View report /WRK:ODBC_TXT_VISU /RPT: [/LAN:] /ZIP: /OUT:

/PRD:SMP_P5 /PRJ:EDITIONS /WRK:ODBC_TXT_VISU /RPT:ticketr.rpt /ZIP:"C:\file.zip" /OUT:"C:\file.pdf"

View report /WRK:SQL_FORMULA_VISU /RPT: [/LAN:] /PAR: [/SQL:] /OUT:

/PRD:SMP_P5 /PRJ:EDITIONS /WRK:SQL_FORMULA_VISU /RPT:status.rpt /PAR:"title='Statuts des fichiers de signature';partner='*';protocol='*';service='*';client='*';int=' - ';ext='';cre=' - ';sta='Fichier ajouté, Fichier archivé, Fichier bloqué, Fichier préparé, Fichier signé';l0='Signature interne';l1='Entité';l2='Protocole';l3='Service';l4='Client';c1='Référence';c2='Référence externe';c3='Date d''ajout';c4='Montant';c5='Nb signatures réalisées';c6='Première

signature';c7='Premier signataire';c8='Deuxième signature';c9='Statut';edit='Edité le';yes='Oui';no='Non';ajoute='Ajouté';prepare='Préparé';bloque='Bloqué';archive='Archivé';signe='Signé';refustotal='Refus total';rejetstotal='Rejets total';avecrejets='avec Rejets';avecrefus='avec Refus';verrouille='Verrouillé';afreject='modifié par le module anti-fraude'" /SQL:"{S_TFI.CNTR_TFI} in[1,2,64,32,16]" /OUT:"C:\file.pdf"

View report /WRK:SQL_TABLES_VISU /RPT: [/LAN:] [/SQL:] /OUT:

/PRD:SMP_P5 /PRJ:EDITIONS /WRK:SQL_TABLES_VISU /LAN:1033 /RPT:client.rpt /SQL:"{S_SES."VPS_SES"}='BNP' AND {S_SES."PRO_SES"}=134217728 AND {S_SES."VFS_SES"}='AFB160' AND {S_SES."CLIENT_SES"}='SAGE' AND {S_SES."SIGNINT_SES"}=0" /OUT:"C:\file.pdf"

Conversion (general case) /FIL: [/OUT:]

/PRD:SMP_P5 /PRJ:CONVERTISSEURS /WRK:VIR160_TO_SCT03 /FIL:"C:\file.160"

Conversion /WRK:{*_SCT_VIASBE} /FIL: /SBS: /SBF: [/OUT:]

/PRD:SMP_P5 /PRJ:VIR_160 /WRK:VIR160_TO_SCT_VIASBE /FIL:"C:\file.160" /SBS:SCT /SBF:SALARY

Conversion /WRK:{*_VIASBE} /FIL: /SBS: [/OUT:]

/PRD:SMP_P5 /PRJ:PRE_160 /WRK:PREL160_TO_SDD_VIASBE /FIL:"C:\file.160" /SBS:SDD

Conversion /WRK:P160_2_SDD_VIA_FRPPAIEMENT /FIL: /FPT: /FPR: [/OUT:]

/PRD:U2 /PRJ:PRE_160 /WRK:P160_2_SDD_VIA_FRPPAIEMENT /FIL:"C:\file.160" /FPT:160 /FPR:1

Conversion /WRK:{*_RB7|*_RB9} /FIL: /RBB: [/OUT:]

/PRD:SMP_P5 /PRJ:CONVERTISSEURS /WRK:VIR160_TO_SCT_RB7 /FIL:"C:\file.160" /RBB:1

Prepare file /WRK:Prepa /FIL: /OUT:

/PRD:PDS /PRJ:SCT /WRK:Prepa /FIL:"C:\file.xml" /OUT:"C:\file.zip"

Invalid records /WRK:DelRejet /FIL: /REJ: /OUT:

/PRD:PDS /PRJ:SCT /WRK:DelRejet /REJ:"C:\fil.rej" /FIL:"C:\file.xml" /OUT:"C:\filereject.xml"

Valid records /WRK:DelSigne /FIL: /REJ: /OUT:

/PRD:PDS /PRJ:SCT /WRK:DelSigne /REJ:"C:\fil.rej" /FIL:"C:\file.xml" /OUT:"C:\fileaccept.xml"

Bank Import /WRK:{BCP_GEN_CERG|CONV_FMT_CERG} /FIL: /OUT:

/PRD:BCP /PRJ:AEB43 /WRK:BCP_GEN_CERG /FIL:"C:\file.aeb43" /OUT:"C:\file.conv"

Filter bank statements /WRK:UPDATEFILE /FIL: /UFP: /UFT: /UFS: /UFC: /OUT:

/PRD:BCP /PRJ:AEB43 /WRK:UPDATEFILE /FIL:"C:\file.aeb43" /UFP:INTER /UFT:FILE /UFS:AEB43 /UFC:SAGE /OUT:"C:\file.out"

Bank Import /WRK:BFI_MQ /FIL: /QUE: /BNK: /OUT:

/PRD:BCP /PRJ:AEB43 /WRK:BFI_MQ /FIL:"C:\file.aeb43" /QUE:QU1 /BNK:BNP /OUT:"C:\file.out"

File generation for U2 /FIL: /OUT:

/PRD:U2 /PRJ:AFB320 /WRK:Standard /FIL:"C:\file.320" /OUT:"C:\file.conv"

Execute /ARG: [/FIL: /OUT:]

/PRD:PDS /PRJ:SCT /WRK:SCT_TEST /ARG:"$INPUTFILE$ Y P $OUTPUTFILE$" /FIL:"C:\file.xml"

/OUT:"C:\file.pdf"

Dans ce cas, le traitement **SCT_TEST** a été créé par copie du traitement SCT_VISU_DET, en supprimant les types **Traitement permettant de visualiser un fichier** et **Vue permettant la gestion des pouvoirs bancaires**.

Application sage.fcs.pwdencode.exe

Cette application console permet d'encoder le mot de passe d'un utilisateur afin d'éviter qu'il ne circule en clair sur le réseau.

L'encodage peut être effectué en base64 uniquement (par défaut), ou chiffré (avec la clé publique du service d'authentification) puis encodé en base64.

Installation

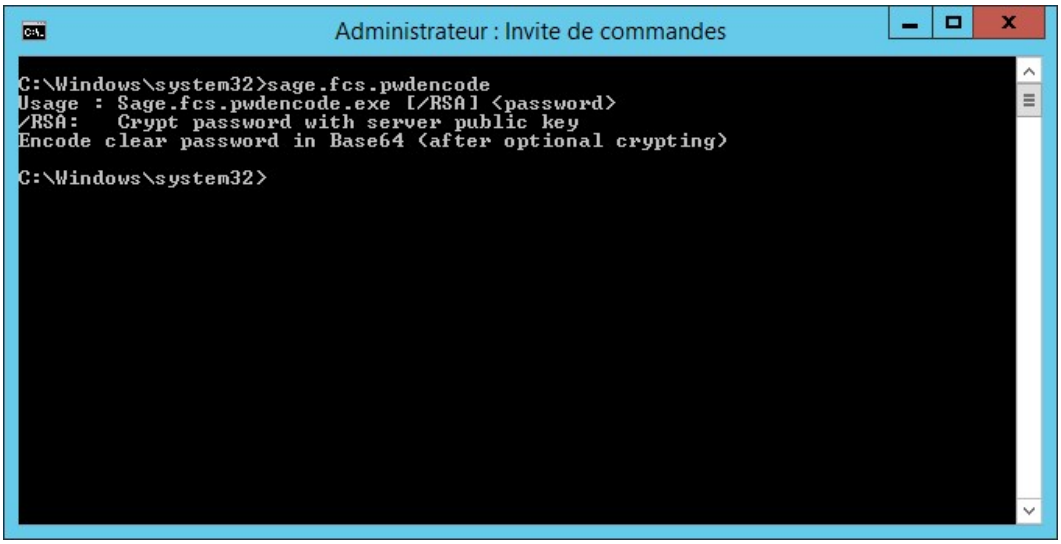
L'installation de cette application est effectuée par l'installation du produit **Sage XRT Solution Common Services**, par la sélection du composant **FCS DLLs** ou du composant **Partie cliente des services SCAS, SCPS et SCDTS**. Hors désélection de ces deux composants lors d'une installation personnalisée, cette application est donc installée par défaut dans toutes les configurations, sauf **Sites Web (SCAS, SCPS, SCDTS et WIDGETS)**.

Deux fichiers sont installés :

- *sage.fcs.pwdencode.exe*
- *sage.fcs.pwdencode.exe.config*

Le fichier de configuration **sage.fcs.pwdencode.exe.config** associé à l'exécutable **sage.fcs.pwdencode.exe** est utilisé pour la déclaration de l'emplacement du service d'authentification dans le cas d'un chiffrement (obtention de la clé publique du certificat).

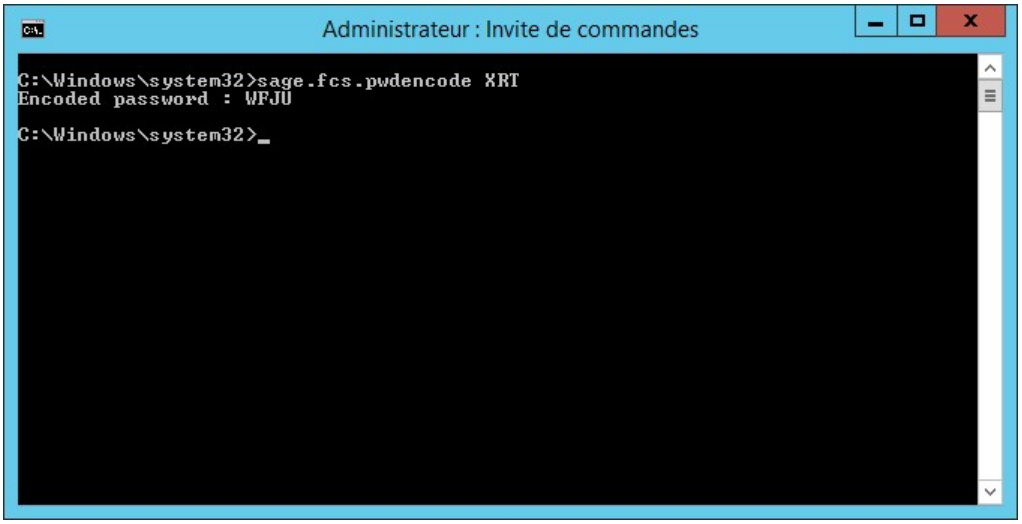
Utilisation



Encodage en base64 uniquement

L'utilisation du fichier de configuration *sage.fcs.pwdencode.exe.config* n'est pas nécessaire dans ce cas puisque l'encodage se fait en local (sans avoir besoin de contacter le service d'authentification).

Le mot de passe : **XRT** est traduit par : **WFJU**.



Chiffrement et encodage en base64

Description du fichier de configuration

Le contenu du fichier est par défaut le suivant :

```
<?xml version="1.0" encoding="utf-8" ?>

<configuration>

  <appSettings>

    <add key="securitylevel" value="http"/>

    <add key="http_servicehost_SCASServer" value="http://localhost:80/Auth" />

    <add key="https_servicehost_SCASServer" value="https://localhost:443/Auth"
/>

  </appSettings>

</configuration>
```

Ce fichier permet d'effectuer la déclaration du service d'authentification qui doit être contacté pour la vérification du mot de passe de l'utilisateur.

Dans le cas où celui-ci fonctionne en mode sécurisé *HTTPS*, il faut apporter la modification à la ligne suivante :

```
<add key="securitylevel" value="https"/>
```

Pour un mode non sécurisé, la ligne suivante est exploitée :

```
<add key="http_servicehost_SCASServer" value="http://localhost:80/Auth" />
```

Pour un mode sécurisé, la ligne suivante est exploitée :

```
<add key="https_servicehost_SCASServer" value="https://localhost:443/Auth" />
```

Vous devez effectuer la modification de *value* pour tenir compte des spécificités de chaque installation.

Rappel :

L'utilisation d'un certificat au niveau du service d'authentification (pour effectuer le déchiffrement du mot de passe) se fait en modifiant le fichier de configuration de ce dernier (*Sage.SCASServer.Service.exe.config*) et en renseignant le numéro de série du certificat sur la ligne suivante :

<add key="serialnumberforpwdcrypt" value="3526df91b8be9ab046a226d0390a764f" />

Si *value* dans cette zone est laissée vide, alors le paramètre **/RSA** ne peut pas être exploité avec ce service d'authentification.

Utilisation de l'exécutable

L'utilisation du chiffrement se fait en ajoutant un paramètre **/RSA** sur la ligne de commande.



Nous vous conseillons de rediriger la sortie de la console dans un fichier afin de récupérer le mot de passe chiffré/encodé pour une exploitation future (ex. : **> pwd.txt**).

Annexes

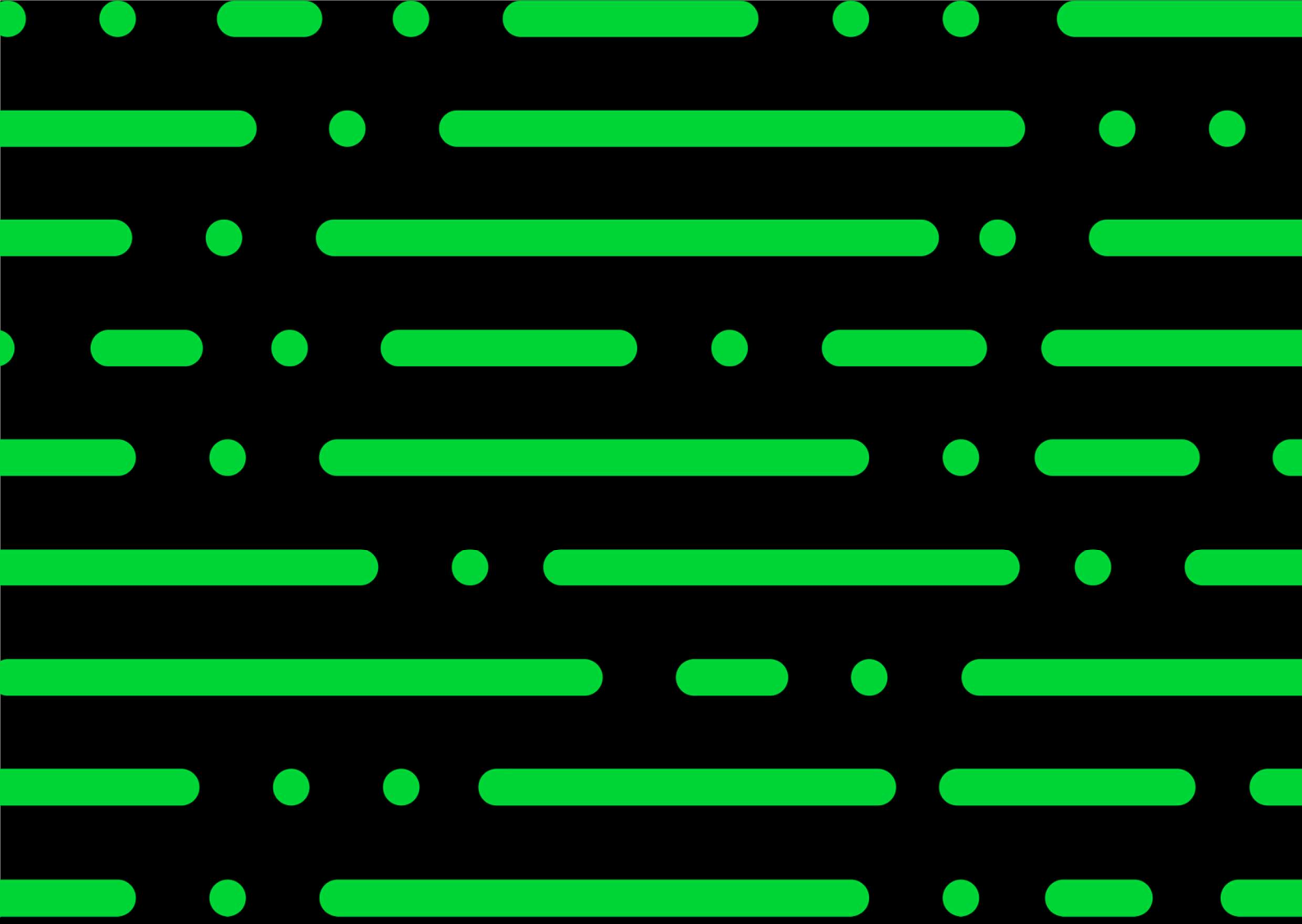
Configuration SCAS

Configuration SCPS

Configuration SCDTS

Configuration SXABCP

Configuration SXAPDS



sage.com
0191 479 5911

Sage

©2022 THE SAGE GROUP PLC OR ITS LICENSORS. SAGE, SAGE LOGOS,SAGE PRODUCT AND SERVICE NAMES MENTIONED HEREIN ARE THE TRADEMARKS OF THE SAGE GROUP PLC OR ITS LICENSORS. ALL OTHER TRADEMARKS ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS.