

# Sage XRT Common Services

Version 4.3.100

Guide Utilisateur



# Sommaire

<b>PRESENTATION GENERALE.....</b>	<b>5</b>
CONSOLE WIN 32 / CONSOLE WEB .....	5
PREMIERE CONNEXION .....	6
<b>CONSOLE WEB .....</b>	<b>7</b>
CONNEXION .....	7
DROITS.....	7
<i>Paramétrage authentication.....</i>	<i>7</i>
Authentification Windows NT .....	8
Authentification UMAPI .....	9
Authentification LDAP .....	9
Authentification SAML.....	11
Double Authentification .....	12
<i>Règles des mots de passe.....</i>	<i>13</i>
<i>Activation des données et règle des 4 yeux.....</i>	<i>14</i>
Profils.....	15
Sites .....	15
Utilisateurs .....	16
<i>Compte utilisateur.....</i>	<i>16</i>
Ajouter un utilisateur .....	17
Activer un utilisateur .....	19
Utilisateur expiré .....	19
Utilisateur bloqué .....	19
PROFILS .....	20
<i>Création .....</i>	<i>20</i>
Gestion des droits du profil .....	21
<i>Modification .....</i>	<i>22</i>
<i>Suppression .....</i>	<i>23</i>
<i>Activation .....</i>	<i>23</i>
SITES.....	23
<i>Création .....</i>	<i>23</i>
<i>Activation .....</i>	<i>24</i>
<i>Modification .....</i>	<i>24</i>
<i>Suppression .....</i>	<i>25</i>
MON COMPTE .....	25
AUDITS ET LOGS .....	25
<i>Paramétrage .....</i>	<i>25</i>
<i>Audit .....</i>	<i>27</i>
<i>Log.....</i>	<i>28</i>
TRANSCODAGES .....	29
<i>Conception.....</i>	<i>29</i>
Création .....	29

Modification .....	30
Suppression .....	30
Import.....	31
Export .....	31
<i>Correspondances</i> .....	31
Création .....	31
Activation .....	33
Modification .....	33
Suppression .....	33
<b>CONSOLE WIN32.....</b>	<b>34</b>
PARAMETRAGE.....	34
Paramétrage du poste d'administration.....	34
Paramétrage de la machine cliente .....	35
GROUPE DE TRAVAIL.....	36
<i>Création d'un groupe de travail</i> .....	36
Atteindre l'assistant de création d'un groupe de travail .....	36
Définir le nom d'un groupe de travail.....	38
Sélectionner un fournisseur .....	39
Sélectionner une base de données.....	40
Configurer les unités logiques .....	41
Créer / Modifier les modèles.....	42
Exécution des opérations .....	42
Sélectionner un produit.....	42
<i>Ajout d'un groupe de travail</i> .....	43
<i>Mise à jour des bases de données d'un groupe de travail</i> .....	43
Sélectionner la base de données à mettre à jour .....	44
Lancer la mise à jour d'une base de données .....	45
UTILISATEURS D'UN GROUPE DE TRAVAIL .....	46
<i>Ajouter un utilisateur à un groupe de travail</i> .....	47
<b>XDLO.....</b>	<b>51</b>
STOCKAGE.....	51
DYNAMIQUE DES ECHANGES .....	51
<b>PRESENTATION DES 3 SERVICES (AUTHENTIFICATION, PRESENTATION ET TRANSFORMATION). ....</b>	<b>54</b>
SAGE.SCPSSERVER.SERVICE.EXE.CONFIG .....	55
SAGE.SCASSERVER.SERVICE.EXE.CONFIG.....	55
SAGE.SCDTSSERVER.SERVICE.EXE.CONFIG.....	56

Les informations contenues dans ce document peuvent faire l'objet de modifications sans notification préalable. Sauf mention contraire, les sociétés, les noms et les données utilisés dans les exemples sont fictifs. Aucune partie de ce manuel ne peut être copiée, reproduite, traduite dans une langue quelconque ou transmise à quelque fin que ce soit ou par n'importe quel moyen électronique ou mécanique, sans permission expresse et écrite de SAGE XRT.

© 2018 SAGE XRT. Tous droits réservés.

Le progiciel décrit dans ce document est diffusé dans le cadre d'un accord de licence et ne peut être utilisé ou copié qu'en conformité avec les termes de cet accord. Veuillez lire attentivement votre contrat définissant cet accord.

**Sage XRT Common Services** est une marque déposée de SAGE. Toute reproduction ou désassemblage de bases de données ou d'algorithmes incorporés est interdit.

Word, Excel, Wordpad, Notepad, Powerpoint, Explorer, Edit et Access sont des marques déposées de Microsoft et MS, MS-DOS, Windows, Windows 2003, Windows 2007, Windows Me et Windows NT sont des marques déposées de Microsoft Corporation aux États-Unis d'Amérique et dans d'autres pays.

Toutes les autres marques et tous les autres noms de produits peuvent être des marques déposées de leurs propriétaires respectifs et sont utilisés ici à des fins éditoriales, sans intention d'enfreindre des droits quelconques.

## Présentation Générale

La version 4.3 est la première version de Sage Common Services à proposer les fonctionnalités les plus utilisées dans une interface Web.

Cette version et suivantes apportent aussi de nouvelles fonctionnalités comme

- La possibilité de gérer une activation des données et une politique des 4 yeux
- L'authentification SAML V2
- Le support de Crystal Report 13.0.23
- Des services d'authentification et de transformation de données

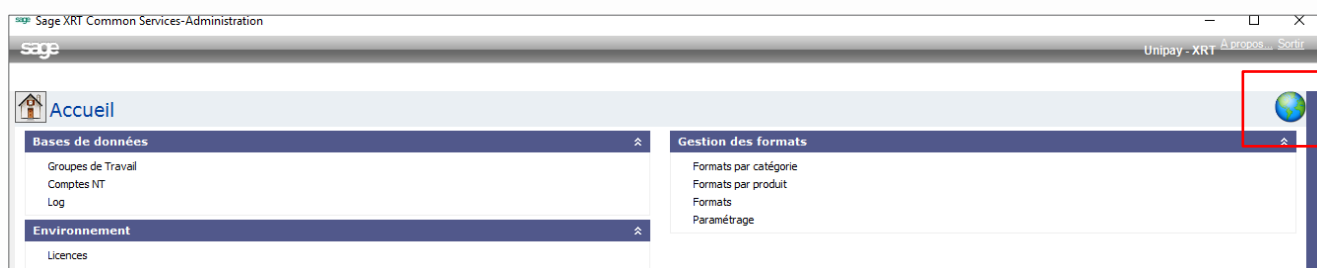
## Console Win 32 / Console Web

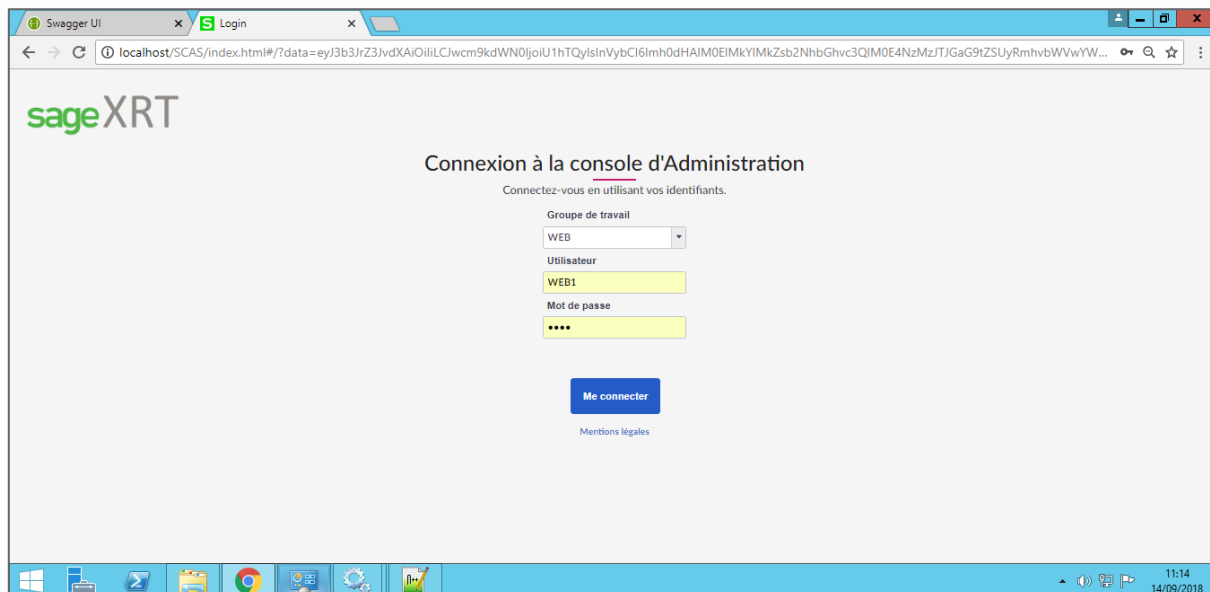
A partir de la version 4.3, certaines fonctions ne sont plus disponibles depuis l'interface Win32 car elles sont utilisables à partir de l'interface Web de XCS.

Interface Win 32	Interface WEB
Gestion de la licence Gestion des workgroups Gestion des formats	Gestion des droits (utilisateurs, profils ...) Gestion des connexions (audits, logs ...) Gestion du transcodage

L'utilisation de l'interface Web via l'url <http://localhost/SCPS/index.html> nécessite le démarrage des services SCASServer et SCPSServer.

Cette url fait l'objet d'un raccourci dans l'interface Win 32





## Première connexion

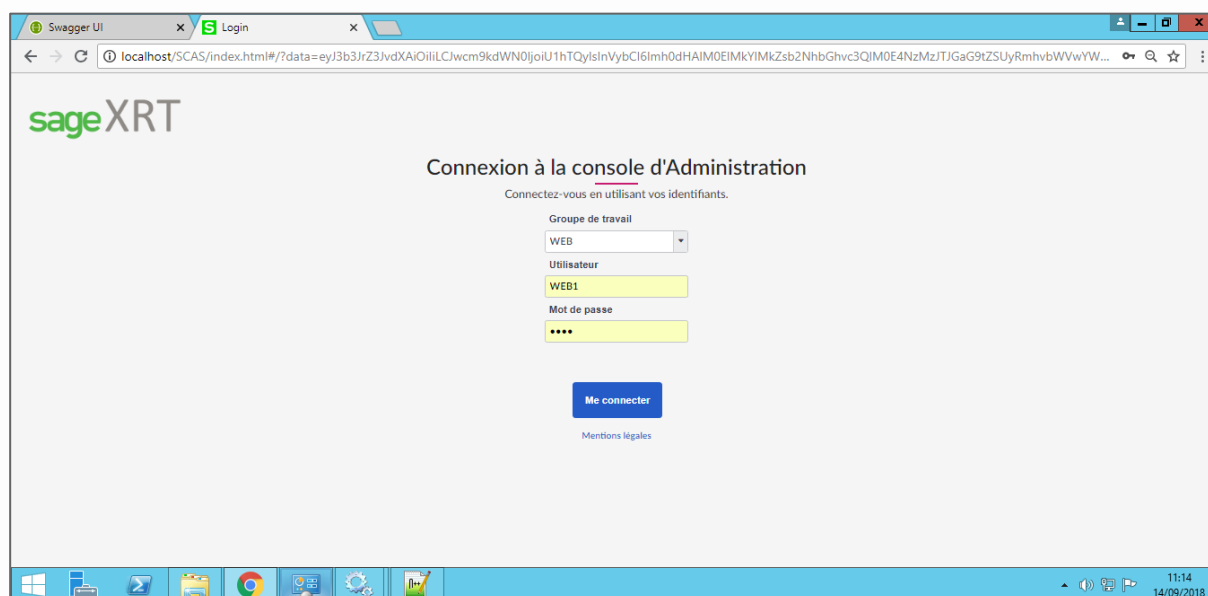
Lors de la première connexion après création de la base de données, l'utilisateur peut utiliser

- Le compte NT utilisé pour installer le produit
- Le login XRT / mot de passe S3cret#2018 (valable seulement 1 journée)

## Console Web

### Connexion

L'utilisation de la console Web se fait via l'url <http://localhost/SCPS/index.html> et nécessite le démarrage des services SCASServer et SCPSServer.



### Droits

Ce chapitre présente une description des différentes méthodes d'authentification des utilisateurs proposées par le module XCS ainsi qu'une description des actions à mener en termes de gestion des utilisateurs et de leurs droits d'accès.

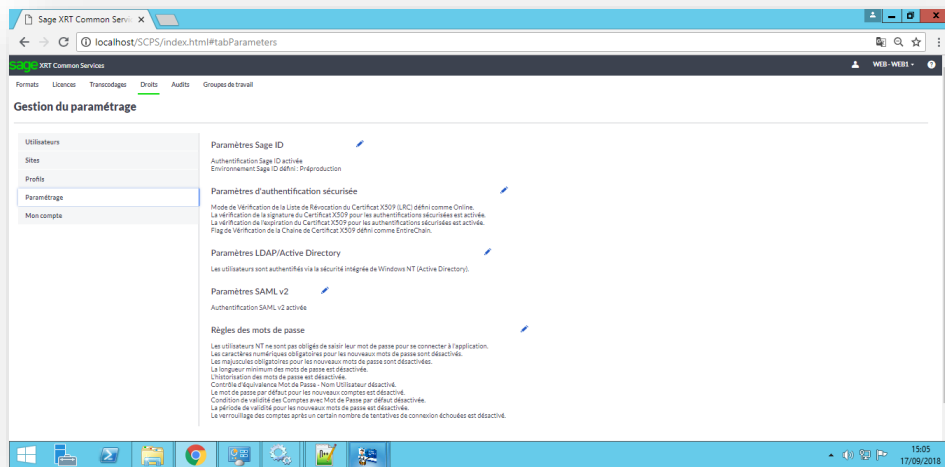
### Paramétrage authentification

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

- L'authentification Windows,
- L'authentification UMAPI
- L'authentification LDAP.
- L'authentification SAML

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

1. A partir du menu Droits, cliquez sur l'entrée Paramétrage.



2. Utilisez l'icône « stylo » 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 XRT d'utiliser les crédeniels des utilisateurs Windows NT.

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

- Le mode "trusted connection" (connexion sécurisée) : l'utilisateur ne doit pas saisir son mot de passe.
- Le mode "normal" : 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 crédeniels 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 Microsoft .NET.

---



## Authentification UMAPI

Lorsqu'il utilise l'authentification UMAPI, un utilisateur se connectant à une application XRT 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.
- Codes de hachage SHA1 des mots de passe enregistrés dans la base de données. Pas 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 XRT 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 avantageuse lorsqu'une société ne souhaite pas utiliser exclusivement le système d'authentification Windows NT,
- Authentification applicative dans le cadre des produits XRT,

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 créidentiels permettant d'effectuer une recherche sur l'annuaire (le bouton « Test Connection » permet de vérifier ces créidentiels).

Paramètres LDAP/Active Directory

☐ Utiliser Windows Active Directory uniquement

☒ Utiliser aussi le serveur LDAP personnalisé

Hôte\* Port 389 ☐ SSL

Références de connexion

Bind DN Mot de passe

ex: cn=manager, dc=domain, dc=com

[Tester la connexion](#)

DN Base\*

KKK

Attribut ID utilisateur\* objectClass utilisateur

NN ex: person

objectClass groupe Attribut membres du groupe

ex: groupOfUniqueNames ex: uniqueMember

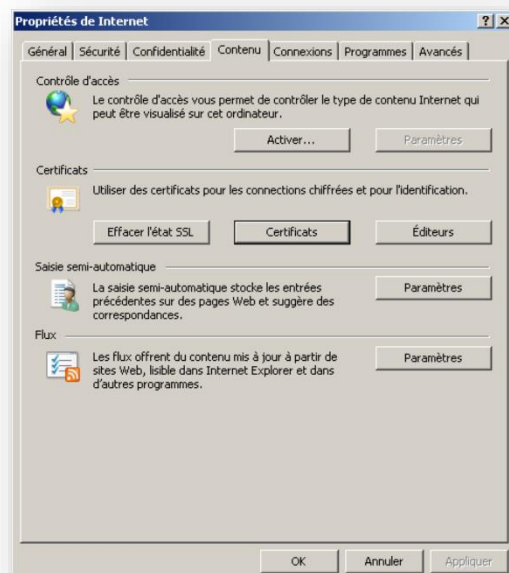
[Tester les paramètres](#)

Enregistrer Annuler

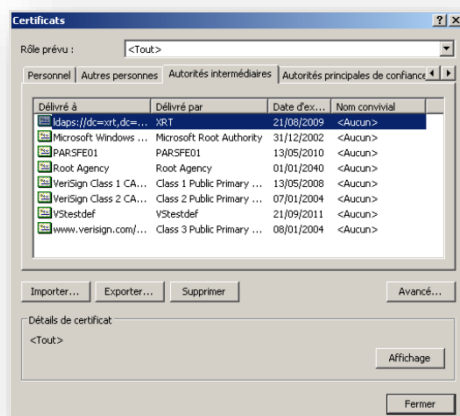
Note : L'implémentation dans UMAPI de l'authentification LDAP est basée sur la librairie de classes de bases du namespace System.DirectoryServices du Framework Microsoft .NET.

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 droit le bouton Certificats. La page 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)
- 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 sera identifié via une donnée déclarée dans les métadonnées (ex : id ou email)

### Double Authentification

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

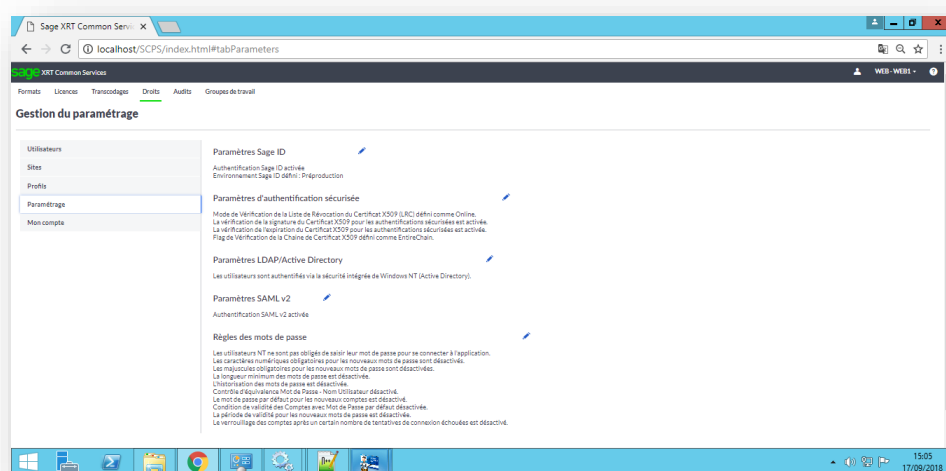
Ce protocole combine une clé secrète avec l'horodatage en cours en utilisant une fonction de hachage cryptographique pour générer un mot de passe à usage unique. Comme la latence du réseau et les horloges désynchronisées peuvent entraîner une tentative d'authentification du destinataire du mot de

se passe, 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.

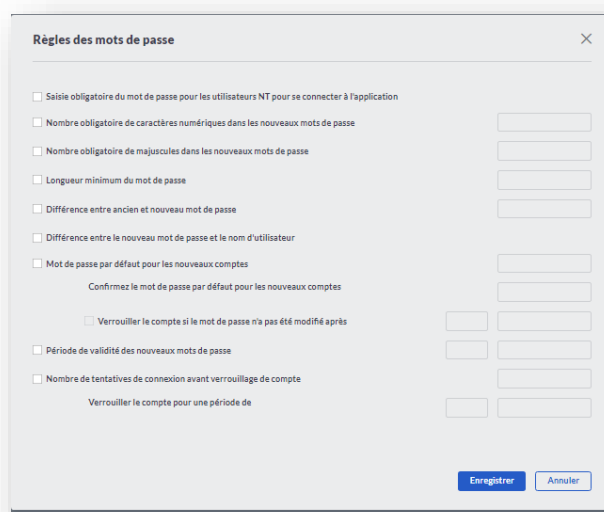
Cf. document « SCS.4.3.DoubleAuthentification.UserGuide\_FR »

## Règles des mots de passe

Ces règles sont définies à partir du menu Droits. Cliquez sur l'entrée Paramétrage.



Utilisez l'icône « stylo » pour modifier les règles des mots de passe.



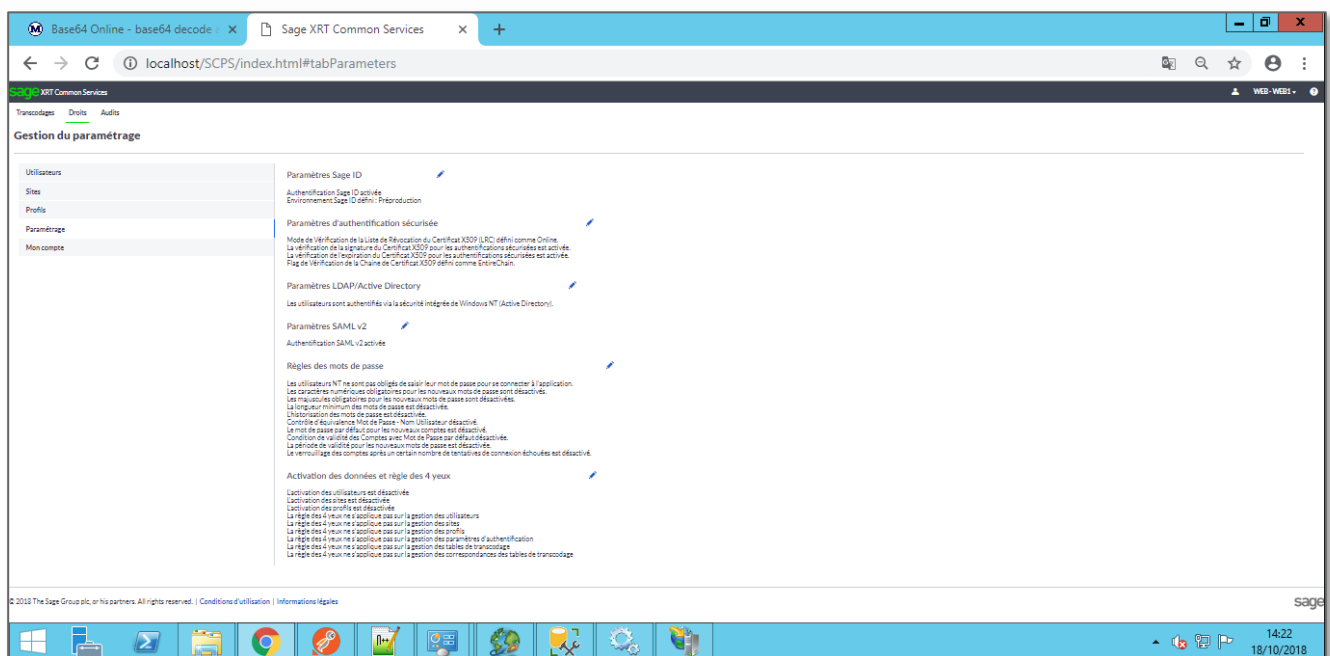
## Activation des données et règle des 4 yeux

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 ...)

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.

Cliquez sur l'entrée Paramétrage



Utilisez l'icône « stylo » pour modifier les règles d'activation des données et des 4 yeux

Activation des données et règle des 4 yeux

**Activation des données**

- ☐ Activation requise des utilisateurs
- ☐ Activation requise des sites
- ☐ Activation requise des profils

**Règle des 4 yeux**

- ☐ Application sur la gestion des utilisateurs
- ☐ Application sur la gestion des sites
- ☐ Application sur la gestion des profils
- ☐ Application sur la gestion des paramètres d'authentification
- ☐ Application sur la gestion des tables de transcodage
- ☐ Application sur la gestion des correspondances des tables de transcodage

Enregistrer Annuler

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

## Profils

*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.

## Sites

*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 requis,*

Tous les sites sont créés actifs.

## Utilisateurs

*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 peut se connecter nulle part.

*En cas d'activation des utilisateurs non requise,*

Tous les utilisateurs sont créés actifs

L'application de la règle des 4 yeux peut être demandée sur

- Les utilisateurs
- Les profils
- Les sites
- La gestion des paramètres d'authentification
- Les tables de transcodage
- Les correspondances des tables de transcodage

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 XRT. Il permet également de gérer les autorisations d'accès de cet utilisateur aux fonctionnalités de l'application.

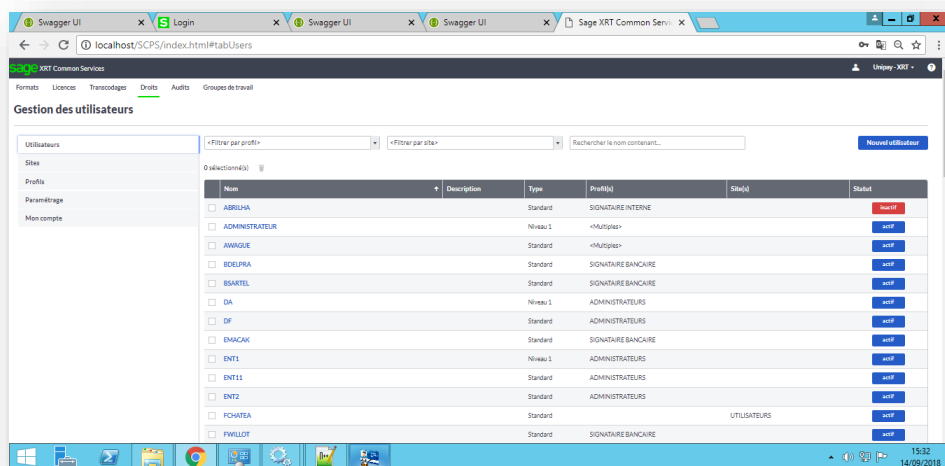
Un compte utilisateur comporte les éléments suivants :

- La langue de l'utilisateur (Français, Anglais, Espagnol, Portugais, Italien, Allemand),
- L'adresse électronique de l'utilisateur à laquelle les notifications doivent être envoyées,
- Une description,
- Le type de l'utilisateur (administrateur ou simple utilisateur).



## Ajouter un utilisateur

1. A partir du menu Droits, cliquez sur l'entrée Utilisateurs.



2. Cliquez sur le bouton « Nouvel utilisateur ». La boîte de dialogue suivante s'affiche :

Création d'un utilisateur

Authentication\*

Nom\*

Niveau de sécurité\*

Langue\*

Adresse mail

Description

☐ Activer la période de validité
 ☐ Double authentification
 ☐ Réinitialiser la double authentification

Profils

Sites

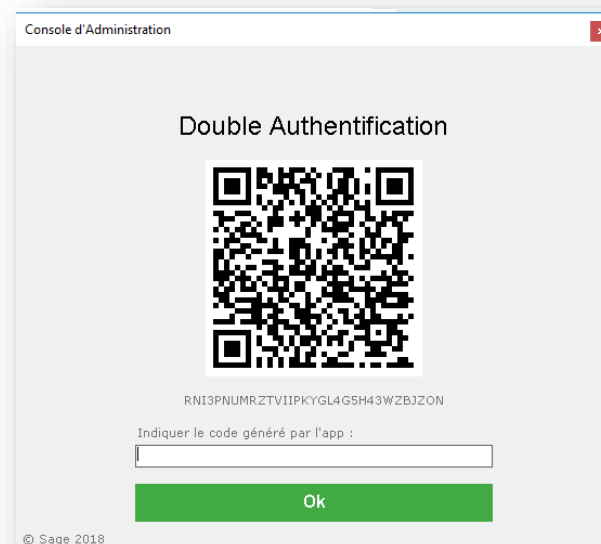
☐ UTILISATEURS  
☐ PAIE  
☐ DRH  
☐ SIGNATAIRE BANCAIRE  
☐ INFORMATIQUE  
☐ SIGNATAIRE INTERNE  
☐ STAGIAIRE  
☐ TRESORERIE  
☐ ADMINISTRATEURS  
☐ TESTEUR

Enregistrer

Annuler

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, ...). Si cette option est cochée, lors de sa première connexion, l'utilisateur devra initialiser cette authentification via la saisie d'un code secret obtenu après scan du QR Code (ou saisie du code équivalent) via une application compatible avec le protocole TOTP 6 digits (FreeOTP par exemple). Tant que cette initialisation n'aura pas été faite, cette option apparaîtra en orange, par la suite, elle sera verte.



Si un utilisateur perd (ou change) 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 dans la liste des utilisateurs sera présente

3. Choisissez le type d'utilisateur à créer :

- Administrateur de sécurité de niveau 1 : gère les droits d'accès des utilisateurs du groupe de travail.
- Administrateur de sécurité de niveau 2 : valide les permissions d'accès accordées par l'administrateur de sécurité de niveau 1. Ce type d'utilisateur ne peut être créé que si l'administrateur système a créé un groupe de travail dont les permissions sont régies par 2 administrateurs de sécurité (l'un validant les permissions accordées par l'autre).
- Utilisateur standard : utilisateur n'ayant aucun droit d'écriture ou de modification.

4. Complétez les autres informations :

Nom du champ	Description
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.

5. Rattachez éventuellement l'utilisateur à un profil et/ou site déjà existant.

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

### Activer un utilisateur

Un utilisateur ne peut pas s'auto-activer.

### Utilisateur expiré

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

### Utilisateur bloqué

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.

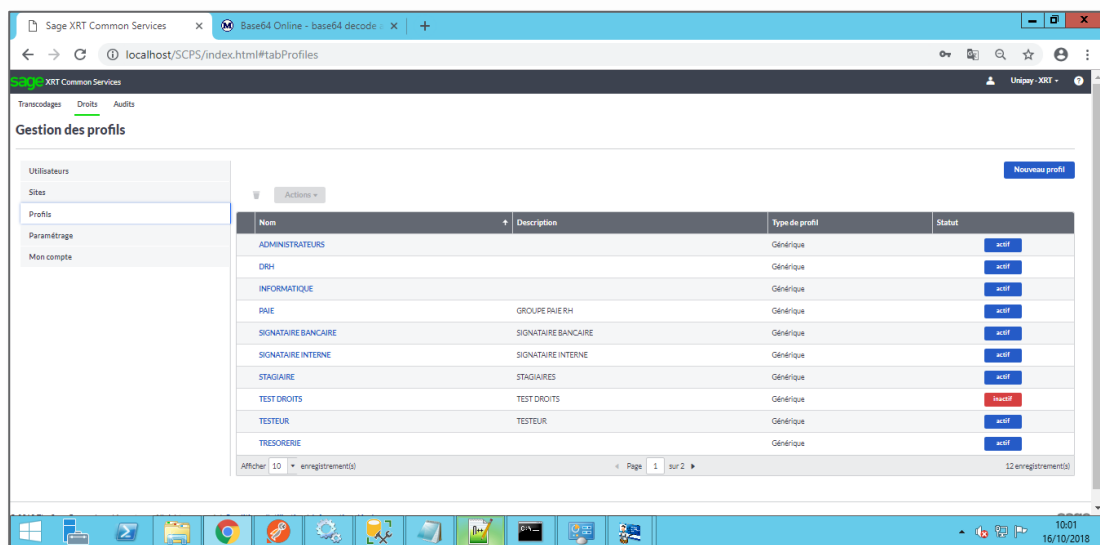
Ce mode de fonctionnement permet d'associer un profil à un groupe de personnes ayant les mêmes activités.

Un profil « standard » est décrit par les propriétés suivantes :

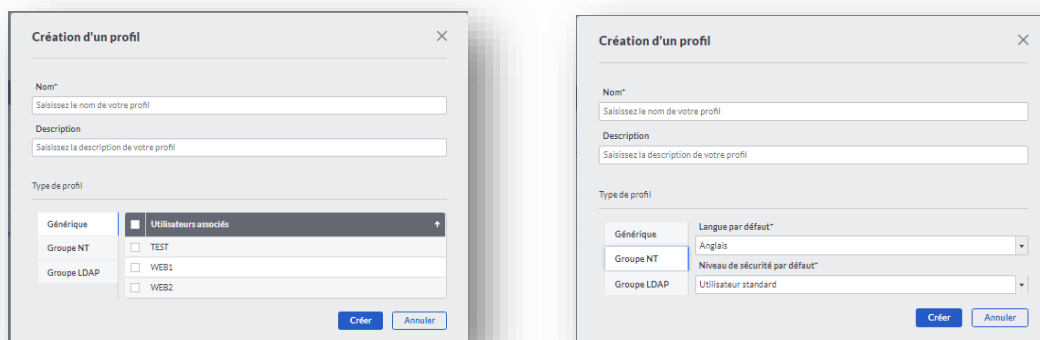
- Un code qui identifie le profil (sans espaces).
- Une description.

## Création

- A partir du menu Droits, cliquez sur l'entrée Profils.



- Cliquez sur le bouton « Nouveau profil ». La page suivante s'affiche :



- Pour créer un profil, renseignez les informations :
  - Nom : saisissez un nom pour le profil. Ce champ doit être renseigné obligatoirement.
  - Description : saisissez une description pour le profil.
- Sélectionner le type de profil :
  - Générique : sélectionnez les utilisateurs existants à associer au profil
  - Groupe AD : tout utilisateur membre du groupe est automatiquement enregistré dans la base de données comme utilisateur des applications 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.  
Note : 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.

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 XRT.

- Cliquez sur le bouton Créer pour valider la création du profil ou sur Annuler pour annuler l'action précédente.

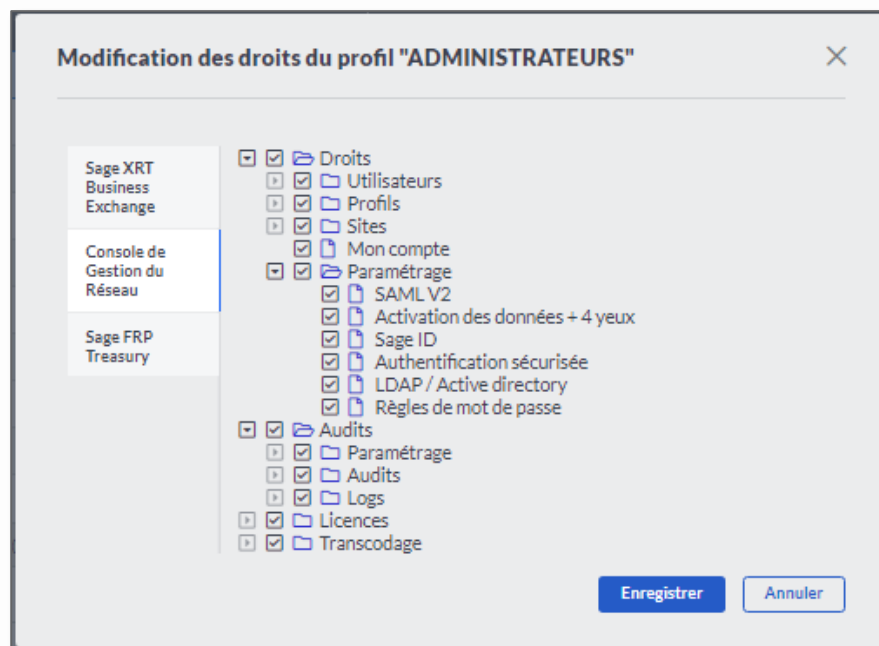
### Gestion des droits du profil

1. A partir de la liste des profils, sélectionnez un profil et sélectionnez l'action « Gérer les droits du profil »

Nom	Description	Type de profil
ADMIN	ADMIN	Générique
ROLE1	ROLE1	Générique
ROLE2	Rôle 2	Générique
ROLE3	ROLE 3	Générique

La page Attribution des droits permet de gérer les droits d'accès d'un profil aux différents produits XRT installés sur le serveur.

2. Cliquez sur l'onglet Console de Gestion du réseau. La page suivante s'affiche :



3. Cochez les droits accordés.
4. Répétez l'opération pour les produits SAGE FRP Treasury et XRT Business Exchange si vous souhaitez attribuer des droits d'accès à ces deux produits pour le profil.
5. Cliquez sur Enregistrer pour enregistrer les modifications effectuées ou sur Annuler pour annuler les modifications.

## Modification

- A partir du menu Droits, cliquez sur l'entrée 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

- A partir du menu Droits, cliquez sur l'entrée Profils.

La liste des profils existants s'affiche. Pour supprimer un profil, sélectionnez la case à cocher correspondante et utilisez l'icône « Poubelle ».

## Activation

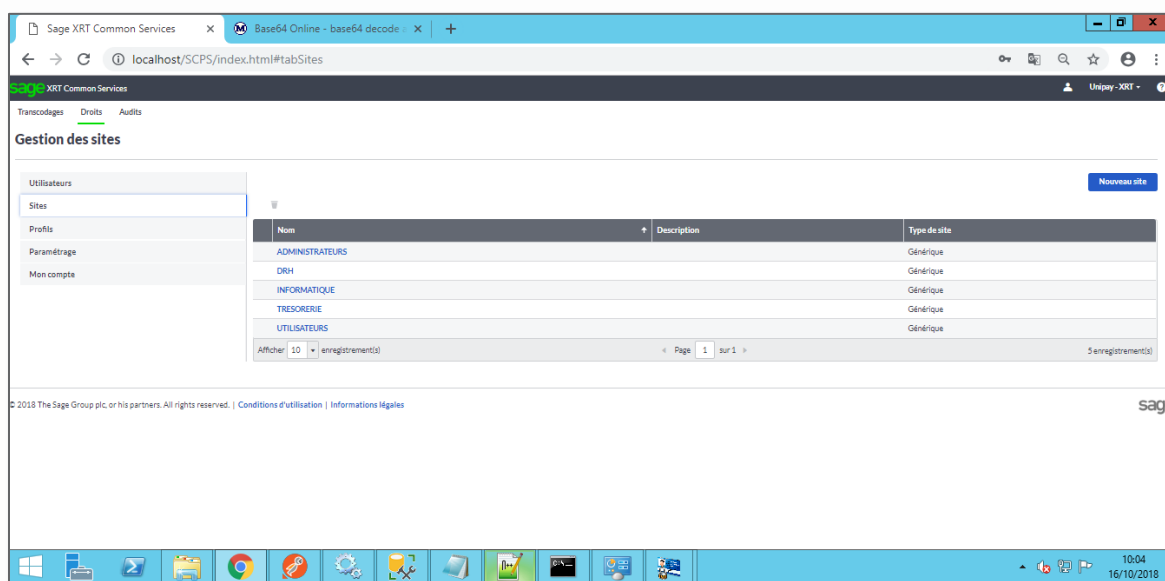
Tout profil créé obtient le statut « inactif » et devra faire l'objet d'une activation par un autre utilisateur de niveau Administrateur.

## Sites

### Création

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

- A partir du menu Droits, cliquez sur l'entrée Site.



- Cliquez sur le bouton « Nouveau site ». La page suivante s'affiche :

Création d'un site

Nom\*

Saisissez le nom de votre site

Description

Saisissez la description de votre site

Type de site

Générique

Groupe NT

Groupe LDAP

Utilisateurs associés

TEST

WEB1

WEB2

Créer Annuler

- Pour créer un site, renseignez les informations :
  - Nom : saisissez un nom pour le site. Ce champ doit être renseigné obligatoirement.
  - Description : saisissez une description pour le site.
- Sélectionner 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 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.  
Note : 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 ou sur Annuler pour annuler l'action précédente.

## Activation

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

## Modification

- A partir du menu Droits, cliquez sur l'entrée 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

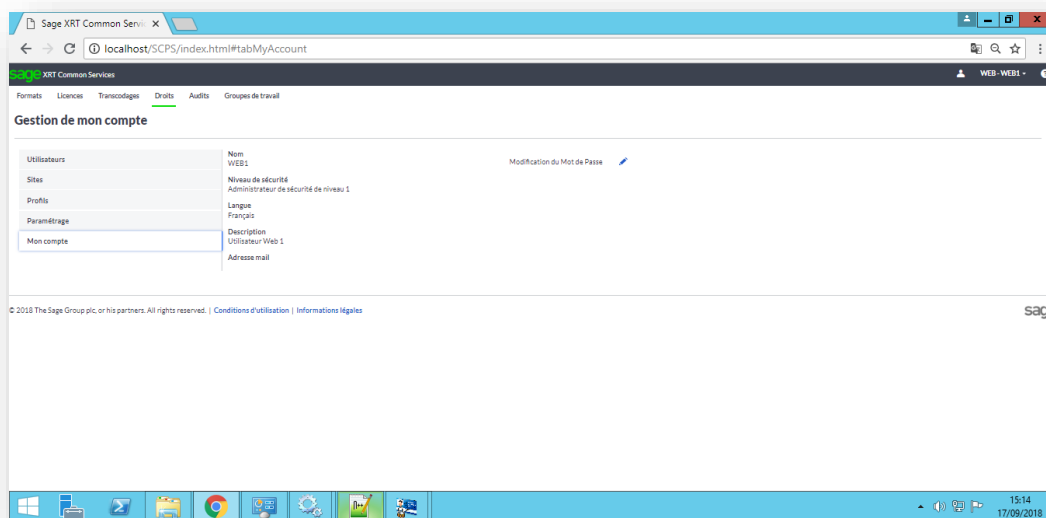
- A partir du menu Droits, cliquez sur l'entrée Site.

La liste des sites existants s'affiche. Pour supprimer un site, sélectionnez la case à cocher correspondante et utilisez l'icône « Poubelle ».

## Mon compte

Cette fonction est accessible aux utilisateurs de type Standard. Elle permet de modifier le mot de passe de l'utilisateur connecté.

- A partir du menu Droits, cliquez sur l'entrée Mon compte.



Les informations de l'utilisateur sont rappelées : nom, niveau de sécurité, langue, description, adresse mail.

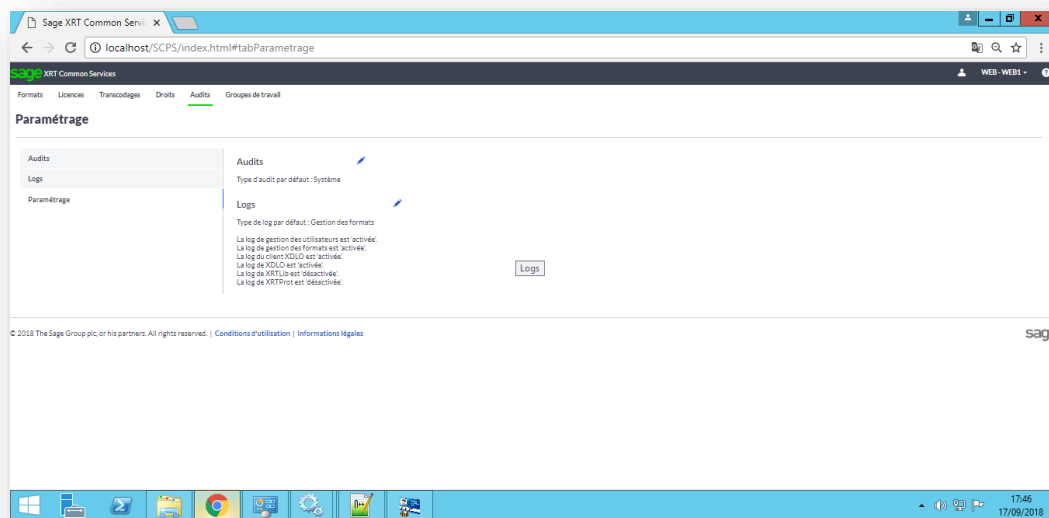
Seul le mot de passe peut être modifié en utilisant l'icône « stylo ».

## Audits et logs

### Paramétrage

Le type d'audit présenté à l'utilisateur ainsi que l'activation des logs sont à définir préalablement à la consultation des informations.

- A partir du menu Audits, cliquez sur l'entrée Paramétrage.



Le paramétrage est ici résumé. Il peut être modifié en cliquant sur l'icône « stylo ».

- Sélectionnez le type d'audit qui sera proposé par défaut à l'appel de la fonction « Audit ». Les choix possibles sont :
  - Système
  - Base de données
  - Utilisateurs
- Sélectionnez le type de log qui sera proposé par défaut à l'appel de la fonction « Log ». Les choix possibles sont :
  - Gestion des formats
  - Gestion des utilisateurs
  - Gestion base de données
  - Gestion de la console
  - Client XDLO
  - XDLO
  - Service XDLO
  - XRTProt
  - XRTLogin
  - XRTLib
- Cochez les logs à activer.
- Cliquez sur le bouton « Enregistrer » pour enregistrer le paramétrage ou « Annuler » pour retourner à la page de résumé en ignorant les modifications.

Paramètres audits et logs

Audits

Type d'audit sélectionné par défaut

Système

Logs

Type de log sélectionné par défaut

Gestion des formats

☒ Activer la log sur la gestion des utilisateurs

☒ Activer la log XDLO

☒ Activer la log sur la gestion des formats

☐ Activer la log XRTLib

☒ Activer la log client XDLO

☐ Activer la log XRTProt

Enregistrer

Annuler

## Audit

- A partir du menu Audits, cliquez sur l'entrée Audit.

Le type d'audit défini par défaut s'affiche. Les autres audits sont accessibles en modifiant ce choix dans la combo. L'utilisateur a la possibilité de filtrer les informations listées en utilisant la combo « Période », par défaut renseignée sur « Aujourd'hui » (autres choix : semaine courante, mois courant, année courante).

D'autres critères de sélection sont disponibles via le bouton « Rechercher ». Les critères de filtre appliqués sont rappelés au-dessus de la liste.

Base64 Online - base64 decode

Sage XRT Common Services

localhost/SCPS/index.html#audits

Transcodages

Droits

Audits

Gestion des audits

Audits

Logs

Paramétrage

Type d'audit

Utilisateurs

Période

Aujourd'hui

Rechercher

Purger

Critères de recherche appliqués

Date du 18/10/2018 au 18/10/2018 inclus

Effacer la recherche

Date/Heure	Catégorie	Statut	Produit	Composant	Utilisateur	Compte utilisateur	Machine	Description
18/10/2018 14:13:18	Login	Succès	CS	FCS Web	WEB1	Administrateur	WIN-C2QRQHDOO82	
18/10/2018 14:13:13	Login	Echec	CS	FCS Web	WEB1	Administrateur	WIN-C2QRQHDOO82	Une exception de type 'UMAPILib.UMAPIException' a été levée.
18/10/2018 14:12:12	Login	Echec	CS	FCS Web	WEB1	Administrateur	WIN-C2QRQHDOO82	Une exception de type 'UMAPILib.UMAPIException' a été levée.
18/10/2018 14:12:51	Login	Echec	CS	FCS Web	WEB1	Administrateur	WIN-C2QRQHDOO82	Une exception de type 'UMAPILib.UMAPIException' a été levée.
18/10/2018 12:03:48	Login	Succès	CS	FCS Web	WEB1	Administrateur	WIN-C2QRQHDOO82	
18/10/2018 11:27:27	Login	Succès	CS	FCS Web	WEB1	Administrateur	WIN-C2QRQHDOO82	
18/10/2018 11:00:17	Login	Succès	CS	FCS Web	BROBOAM@DOMVMD5F.COM	Administrateur	WIN-C2QRQHDOO82	
18/10/2018 10:32:39	Login	Succès	CS	FCS Web	WEB1	Administrateur	WIN-C2QRQHDOO82	
18/10/2018 10:30:07	Login	Echec	CS	FCS Web	WEB1	Administrateur	WIN-C2QRQHDOO82	Invalid password.
18/10/2018 10:29:16	Login	Echec	CS	FCS Web	WEB1	Administrateur	WIN-C2QRQHDOO82	Invalid password.

Afficher

10

enregistrement(s)

Page

1

sur 3

24 enregistrement(s)

© 2018 The Sage Group plc, or his partners. All rights reserved. | Conditions d'utilisation | Informations légales

sage

- L'utilisation du bouton « Purger » permet de supprimer ou d'exporter des évènements de la liste.

Suppression d'événements de l'audit 'Utilisateurs'

Evénements antérieurs au :

18/10/2018

Nombre d'événements à supprimer :

28

Exporter

Supprimer

Annuler

## Log

- A partir du menu Audits, cliquez sur l'entrée Log.

Le type de log défini par défaut s'affiche. Les autres logs activées sont accessibles en modifiant ce choix dans la combo. L'utilisateur a la possibilité de filtrer les informations listées en utilisant la combo « Période », par défaut renseignée sur « Aujourd'hui » (autres choix : semaine courante, mois courant, année courante).

D'autres critères de sélection sont disponibles via le bouton « Rechercher ». Les critères de filtre appliqués sont rappelés au-dessus de la liste.

Sage XRT Common Services

Transcodages Droits Audits

### Gestion des logs

Audits  
Logs  
Paramétrage

Type de log : Gestion des formats

Période : Aujourd'hui

Rechercher

Critères de recherche appliqués

Date du 16/10/2018 au 16/10/2018 inclus

Effacer la recherche

Date/Heure	Niveau	Message
16/10/2018 08:51:00	DEBUG	CCFFmtRun:FMTDconnect
16/10/2018 08:51:00	DEBUG	return 5_OK

Afficher 10 enregistrement(s)

Page 1 sur 1

2 enregistrement(s)

© 2018 The Sage Group plc, or its partners. All rights reserved. | Conditions d'utilisation | Informations légales

sage

VERR MAJ : ACTIVE  
10/10/2018

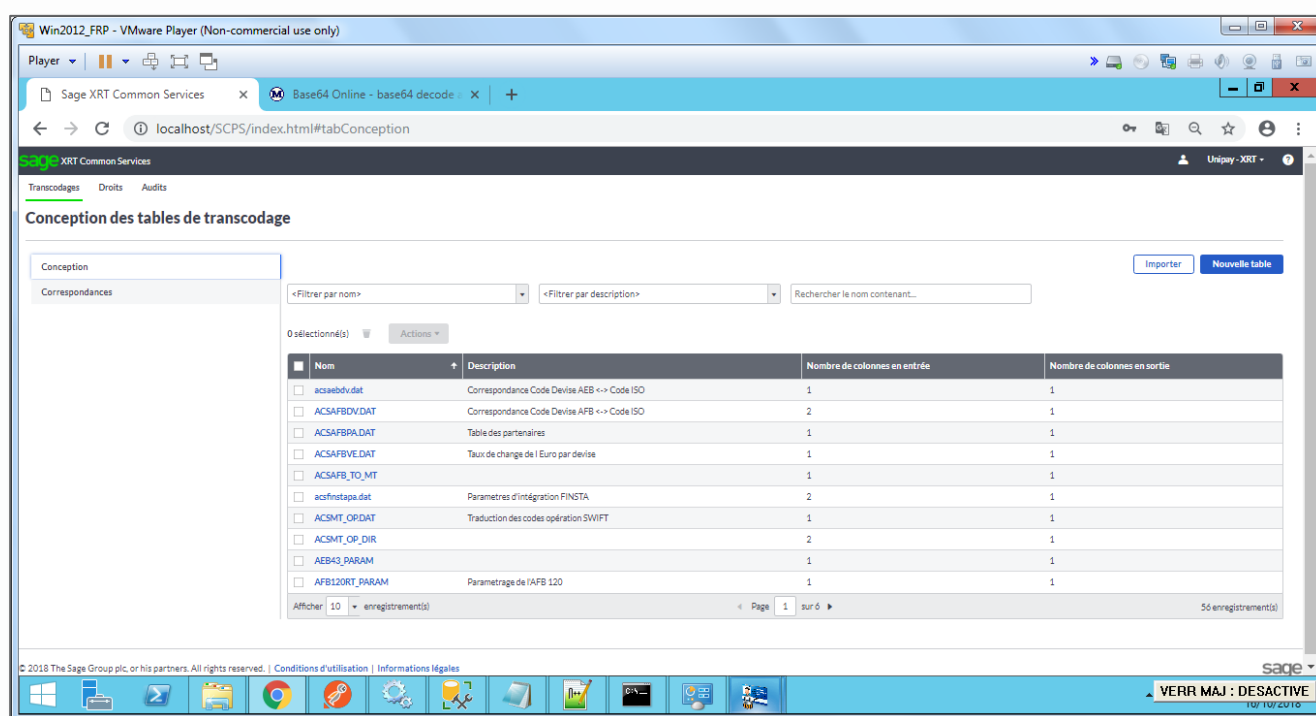
## Transcodages

### Conception

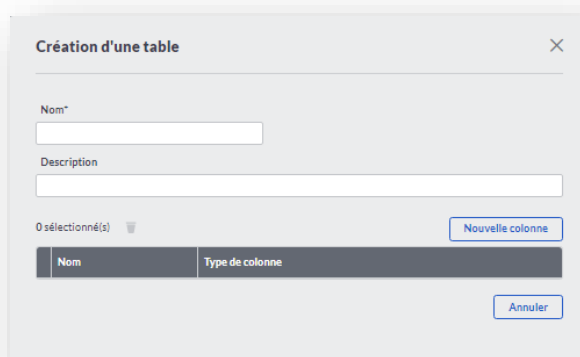
#### Création

- A partir du menu Transcodages, cliquez sur l'entrée Conception.

La liste des tables livrées par défaut pour assurer le fonctionnement des produits XRT s'affiche.



- Cliquez sur le bouton « Nouvelle table » pour créer une table.



- Renseigner obligatoirement un nom pour la table et éventuellement une description. Utilisez ensuite le bouton « Nouvelle colonne » pour définir les colonnes d'entrée et de sortie de la table.
- Renseigner obligatoirement un nom pour la table et éventuellement une description. Utilisez ensuite le bouton « Nouvelle colonne » pour définir les colonnes d'entrée et de sortie de la table.

Création d'une nouvelle colonne

Type de colonne\*

Nom\*

Valider Annuler

- Pour chaque colonne, renseignez obligatoirement un nom et un type (entrée ou sortie). Cliquez sur « Valider » pour enregistrer la création de la colonne. La colonne créée s'inscrit dans la liste de colonnes constituant la table. Une colonne peut être modifiée en utilisant le lien sur son nom ou supprimer en la sélectionnant (case à cocher) et en utilisant l'icône « Poubelle ».

Création d'une table

Nom\*

DOC

Description

0 sélectionné(s)

Nouvelle colonne

Nom	Type de colonne
<input type="checkbox"/> ENTREE 1	Entrée
<input type="checkbox"/> ENTREE 2	Entrée
<input type="checkbox"/> SORTIE	Sortie

Enregistrer Annuler

- Cliquez sur le bouton « Enregistrer » pour enregistrer la création de la table. Elle s'inscrit alors dans la liste des tables.

### Modification

- A partir du menu Transcodages, cliquez sur l'entrée Conception.

La liste des tables existantes s'affiche. Pour modifier une table, utilisez le lien disponible sur le nom de la table. Procédez aux modifications souhaitées et cliquez sur le bouton « Enregistrer »

### Suppression

- A partir du menu Transcodages, cliquez sur l'entrée Conception.

La liste des tables existantes s'affiche. Pour supprimer une table, sélectionnez la case à cocher correspondante et utilisez l'icône « Poubelle ».

### Import

- A partir du menu Transcodages, cliquez sur l'entrée Conception.

La liste des tables existantes s'affiche. Pour importer des tables de transcodage, cliquez sur le bouton « Importer ». Une boîte de dialogue pour sélectionner le fichier à importer s'ouvre. Sélectionner un fichier et cliquez sur « Ouvrir ».

### Export

- A partir du menu Transcodages, cliquez sur l'entrée Conception.

La liste des tables existantes s'affiche. Pour exporter une table, sélectionnez la case à cocher correspondante et utilisez l'action « Exporter » disponible dans la combo « Actions ».

## Correspondances

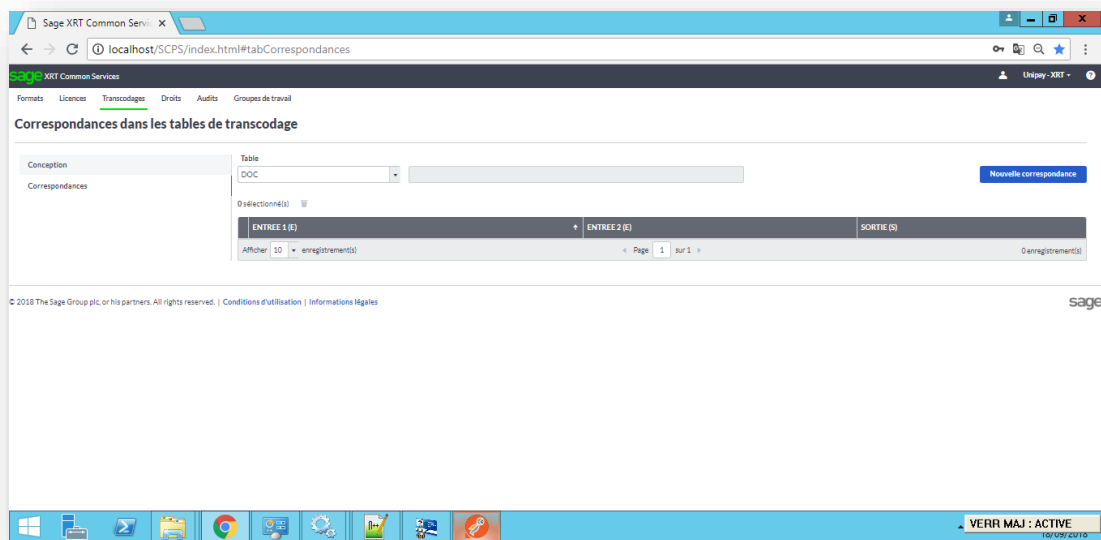
Une fois la table créée, les correspondances à appliquer doivent être renseignées.

### Création

- A partir du menu Transcodages, cliquez sur l'entrée correspondances.

La table « RIBS-Table IBAN » est positionnée par défaut dans la combo de sélection de la table pour affichage des correspondances.

Sélectionnez dans la combo « Table », la table pour laquelle les correspondances doivent être créés. La structure de la table s'affiche.



- Cliquez sur le bouton «Nouvelle correspondance »

Création d'une correspondance

ENTREE 1 (E)\*

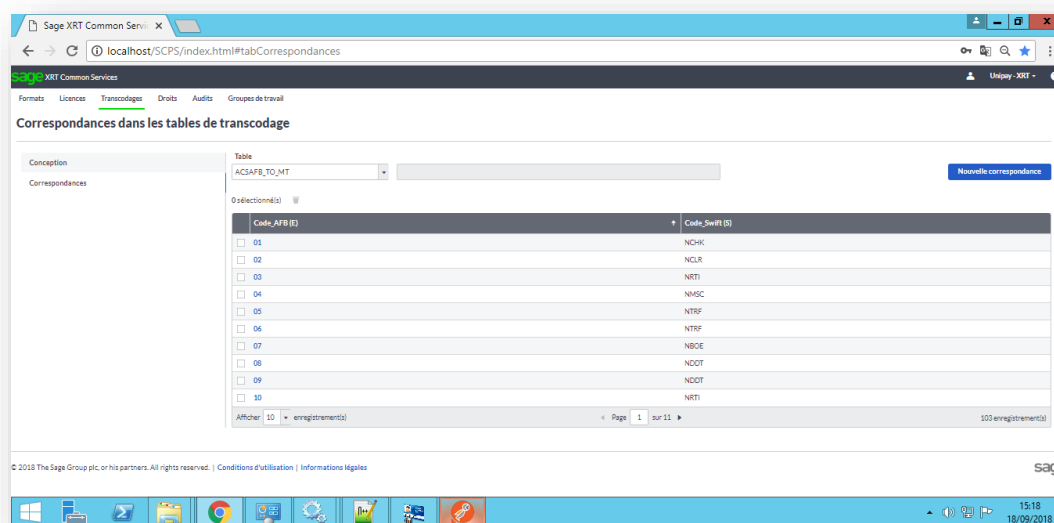
ENTREE 2 (E)\*

SORTIE (S)

Enregistrer Annuler

- Renseignez pour chaque correspondance, la ou les valeurs d'entrée et la ou les valeurs de sortie. Cliquez sur « Enregistrer » pour enregistrer la création de la correspondance qui s'inscrit dans la liste des correspondances de la table. La table est créée en statut « inactif »





## Activation

## Modification

- A partir du menu Transcodages, cliquez sur l'entrée Correspondances.

Sélectionnez la table de travail : la liste des correspondances existantes s'affiche. Pour modifier une correspondance, utilisez le lien disponible sur la première colonne de la table. Procédez aux modifications souhaitées et cliquez sur le bouton « Enregistrer »

## Suppression

- A partir du menu Transcodages, cliquez sur l'entrée Conception.

Sélectionnez la table de travail : la liste des correspondances existantes s'affiche. Pour supprimer une correspondance, sélectionnez la case à cocher correspondante et utilisez l'icône « Poubelle ».

## Console Win32

### Paramétrage

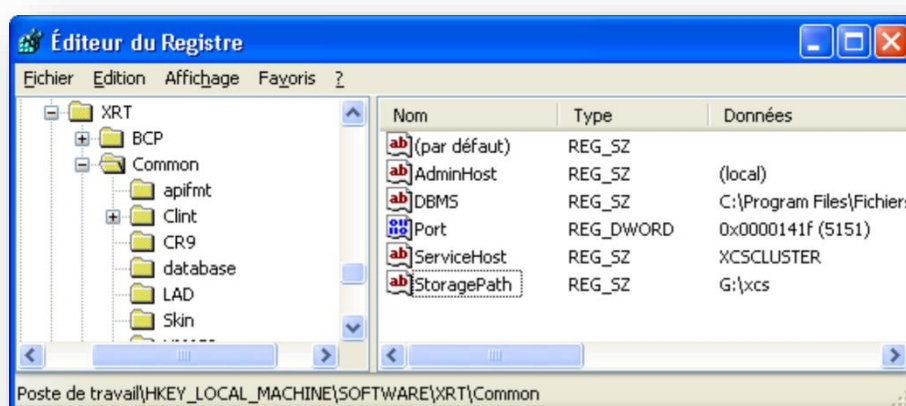
Ce chapitre comporte une description du poste d'administration et de la machine cliente.

#### Paramétrage du poste d'administration

Le poste d'administration désigne la machine sur laquelle s'exécute le service XDLO.

Le paramétrage principal de XDLO pour le poste d'administration est défini dans la clé de registre HKEY\_LOCAL\_MACHINE\SOFTWARE\XRT\Common. Celle-ci contient les valeurs suivantes :

Valeur	Description
Port	Port TCP/IP sur lequel le service est en écoute des appels clients. Durant l'installation d'XCS ce paramètre reçoit la valeur par défaut 5151.
StoragePath	Définit le chemin d'accès au fichier xdlo_storage.xml. Ce paramètre permet de changer le chemin d'accès du fichier xdlo_storage.xml quand XDLO est installé en mode cluster. Chaque nœud du cluster doit avoir un accès en écriture sur le fichier partagé.
ServiceHost	Permet de spécifier le nom ou l'adresse IP de la machine d'administration ou le nom virtuel ou l'adresse IP virtuelle attachée au poste d'administration. Lorsque le programme XDLO est installé en mode cluster. Cette valeur permet de spécifier le nom virtuel du cluster. Ce nom peut être attaché à n'importe quel nœud du cluster suivant le nœud actif.



Les paramètres optionnels de XDLO sont définis dans la clé de registre HKEY\_LOCAL\_MACHINE\SOFTWARE\XRT\Common\XDLO. Celle-ci contient la valeur suivante :

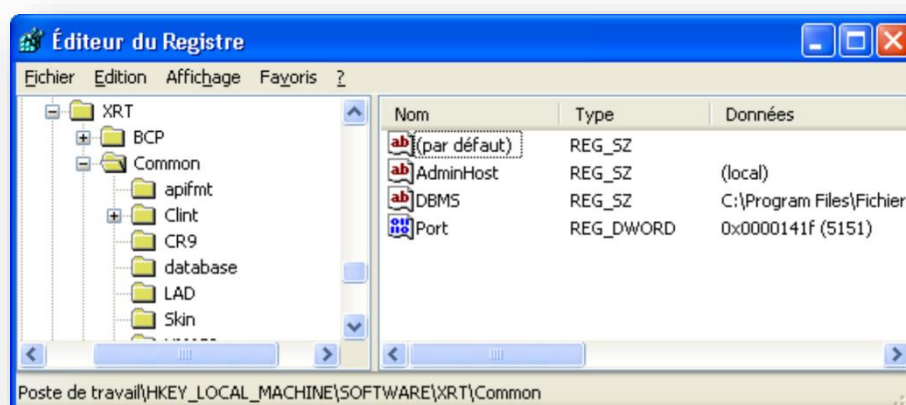
Valeur	Description
Debug	La valeur Y active le mode debug pour xdlo_service.exe et xdlo_com.dll qui génèrent les fichiers de log xdlo-service.log et xdlo.log.

### Paramétrage de la machine cliente

La machine cliente fait référence à l'ordinateur sur lequel s'exécutent les applications XRT et le client XDLO.

Les principaux paramètres de la partie cliente de XDLO sont définis dans la clé de registre HKEY\_LOCAL\_MACHINE\SOFTWARE\XRT\Common. Elle contient les paramètres suivants :

Valeur	Description
AdminHost	Nom ou adresse IP de la machine sur laquelle s'exécute le service XDLO. La valeur par défaut de ce paramètre est "(local)".
Port	Numéro de port IP sur lequel le service XDLO est en écoute des appels des clients. La valeur par défaut de ce paramètre est 5151.



Les paramètres optionnels de la partie cliente d'XDLO sont définis dans la clé de registre HKEY\_LOCAL\_MACHINE\SOFTWARE\XRT\Common\XDLO. Celle-ci contient les valeurs suivantes :

Valeur	Description
DebugRC	Active le mode debug du composant client qui génère un fichier de log xdlo_remclient.log lorsque la valeur "Y" lui est affectée. Le fichier de log est généré dans le dossier <User>\Application Data\XRT\XCS.
Cache_lease	Définit le délai en secondes pendant lequel XDLO s'appuie sur le cache pour retrouver une chaîne de connexion. Quand le délai "cache lease" expire, XDLO appelle le service.

## Groupe de travail

Dans le cas d'une première installation de XCS, aucun groupe de travail n'existe. Ainsi, la première étape consiste à créer un ou plusieurs groupes de travail.

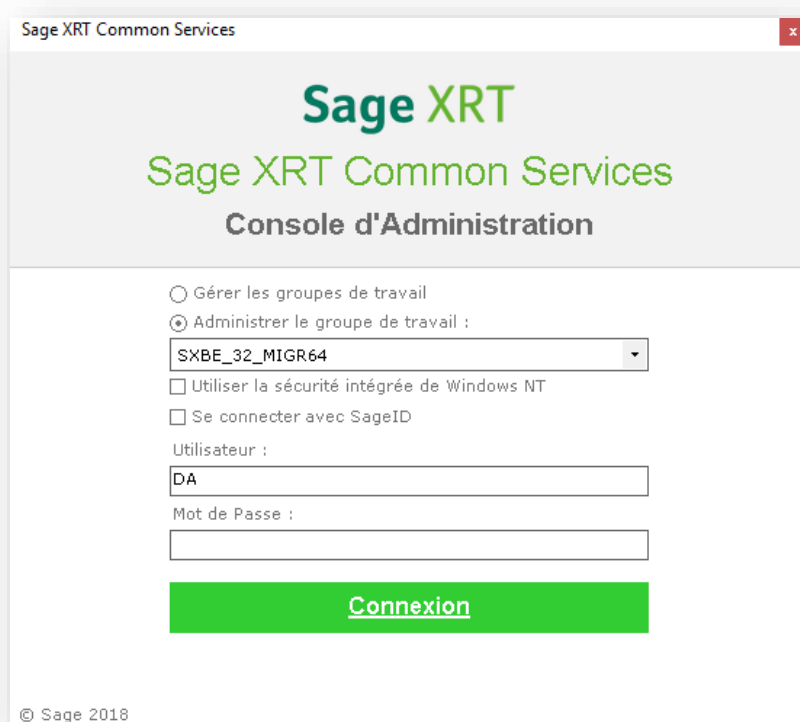
Ce chapitre présente la marche à suivre pour créer un groupe de travail en fonction du type de base de données utilisée : SQL Server ou Oracle.

Vous trouverez également la description détaillée des premières actions à entreprendre après la création d'un groupe, à savoir la mise à jour d'une base de données, l'ajout d'un groupe de travail ou encore la gestion des utilisateurs d'un groupe.

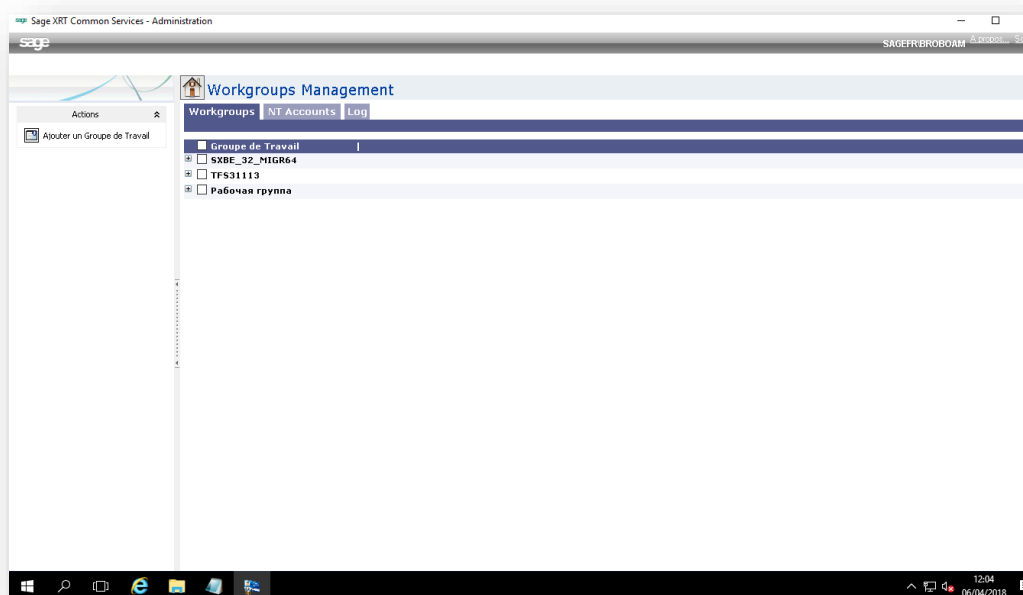
## Création d'un groupe de travail

### Atteindre l'assistant de création d'un groupe de travail

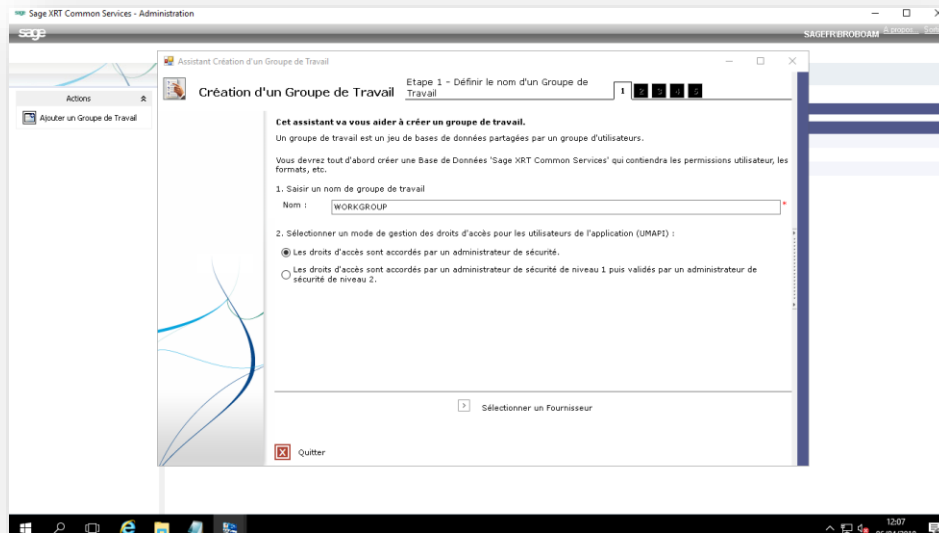
1. A partir du menu Démarrer, sélectionnez **Programmes > Sage > Administration XRT .NET**. La page suivante s'affiche :



2. Sélectionnez l'option **Gérer les groupes de travail**.
3. Cliquez sur **OK**. La page suivante s'affiche :



4. Cliquez sur le lien Ajouter un groupe de travail pour lancer l'assistant Création d'un Groupe de travail. La page suivante s'affiche :

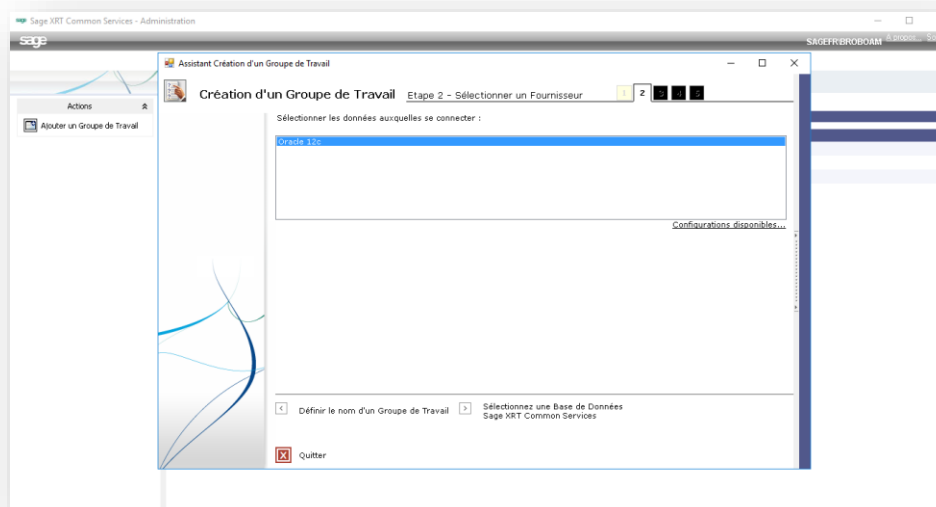


Remarque

lorsqu'aucun groupe de travail n'est défini, la page Création d'un groupe de travail s'affiche immédiatement à l'écran, sans passer par les étapes 2 et 3.

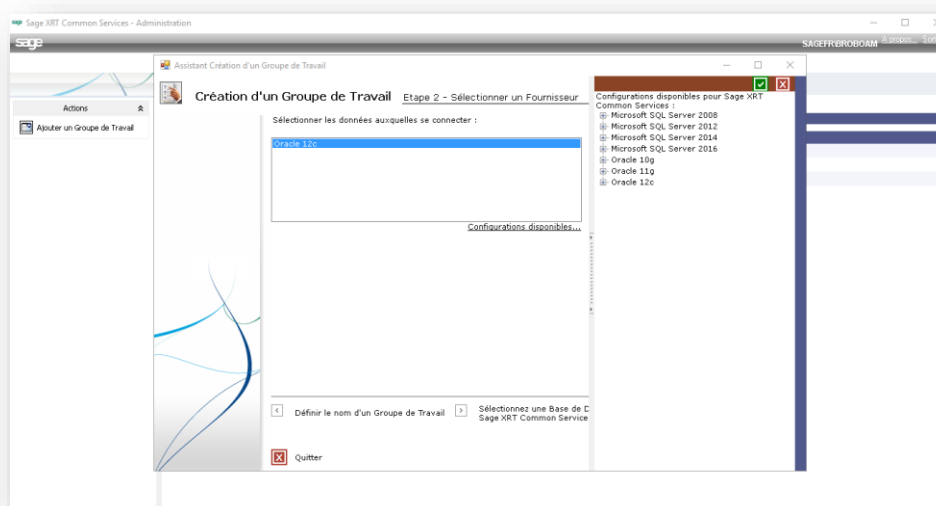
### Définir le nom d'un groupe de travail


1. Saisissez un nom de groupe de travail dans le champ **Nom**. Le nom par défaut est **WORKGROUP**.
2. Définissez le mode de fonctionnement de la gestion des droits d'accès des utilisateurs aux applications XRT. Vous devez sélectionner le mode d'affectation des permissions.
  - Si vous souhaitez mettre en place une gestion simple des droits d'accès aux applications, qui ne fait intervenir qu'un seul administrateur de sécurité, sélectionnez Les droits d'accès sont accordés par un administrateur de sécurité.
  - Si vous souhaitez mettre en place une gestion des droits d'accès aux applications dans laquelle toute opération effectuée par un administrateur de sécurité doit être validée par un deuxième administrateur de sécurité, sélectionnez Les droits d'accès sont accordés par un administrateur de sécurité de niveau 1 puis validés par un administrateur de sécurité de niveau 2.
3. Cliquez sur le lien **Sélectionner un fournisseur**. La page suivante s'affiche :

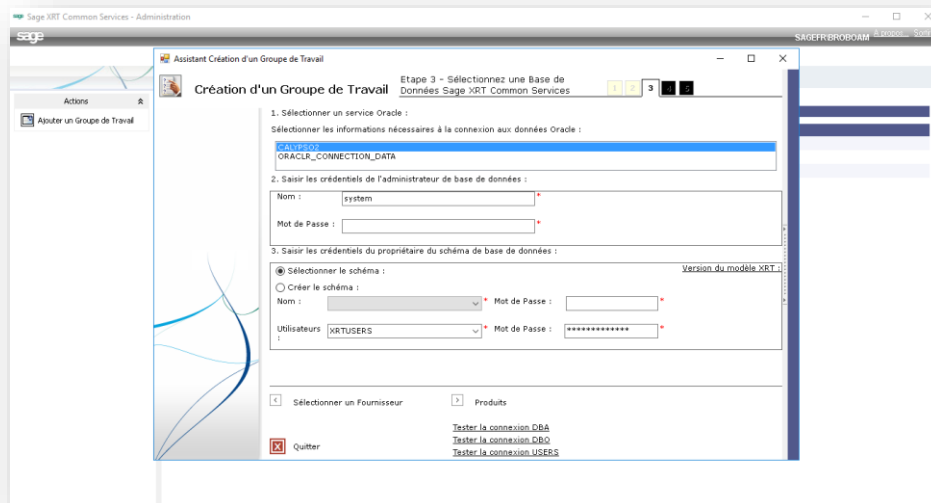


## Sélectionner un fournisseur

1. Sélectionnez dans la liste le serveur ou client de base de données installé.
2. Cliquez sur Configurations disponibles pour visualiser le détail des serveurs ou clients de base de données installés sur la machine et les opérations admises (création et mise à jour). La page suivante s'affiche :



3. Cliquez sur  pour fermer la page et revenir à la page de sélection des fournisseurs d'accès aux bases de données.
4. Cliquez sur Sélectionner une base de données. La page suivante s'affiche :



### Sélectionner une base de données

1. Saisissez le nom du serveur sur lequel la base de données doit être créée. Les caractères possibles pour indiquer le 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.
2. Suivant le type d'authentification utilisé par le DBA pour se connecter au serveur de bases de données, sélectionnez :
  - **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** en bas de page pour vérifier les identifiants du DBA.

3. Sélectionnez ou créez une base de données sur le serveur :
  - Choisissez **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 qui est affiché dans le champ **DBO**. Le mot de passe proposé par défaut par l'assistant est password#2005 (lorsque l'utilisateur sélectionne une base de données dans la liste, l'assistant



recherche automatiquement le nom du propriétaire de celle-ci. L'assistant utilise le compte DBA pour effectuer cette opération).

- Saisissez le mot de passe du compte XRTUSERS. 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 crédeniels du propriétaire de la base de données (DBO).

- Choisissez **Créer la base de données** si vous souhaitez créer une nouvelle base de données :
  - Saisissez un nom de base de données : l'assistant vérifie qu'aucune base ne porte ce nom lorsque l'utilisateur clique sur **Créer/Modifier les modèles**.

Note : Le nom de la base de données ne doit pas comprendre d'espaces, ni de caractères spéciaux (\*, ?, \, / ...).

- Saisissez les crédeniels du propriétaire de la base de données : l'assistant propose le compte **XRT** avec le mot de passe **XRT** par défaut. L'assistant se charge également, si nécessaire, de créer le compte et de lui affecter le rôle de db\_owner sur la base.
- Sélectionnez la chaîne d'interclassement (Collation string) ou laissez par défaut French\_CI\_AS (pas de distinction entre majuscule et minuscule).

4. Cliquez sur Produits.

### Configurer les unités logiques

1. L'assistant propose par défaut un scénario dans lequel les tables (**Groupe de fichiers DATA**) et les index (**Groupe de fichiers INDEX**) du modèle sont créés dans le filegroup **PRIMARY** (Groupe de fichiers par défaut lors de la création d'une base de données SQL SERVER). Via ce panneau de propriétés, vous pouvez :
  - Modifier le scénario proposé et installer les tables et les index dans deux groupes de fichiers différents (exemple XCS\_DATA et XCS\_INDEX).
  - Modifier les paramètres de création des groupes de fichiers (répertoire de stockage, taille initiale, taille limite, taux de croissance): attention le répertoire de stockage doit exister pour que l'opération de création fonctionne correctement.


Important : Les scripts modèle de XCS 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 cible n'existent pas (par exemple XCS\_DATA et XCS\_INDEX), ceux-ci sont automatiquement créés par l'assistant.

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

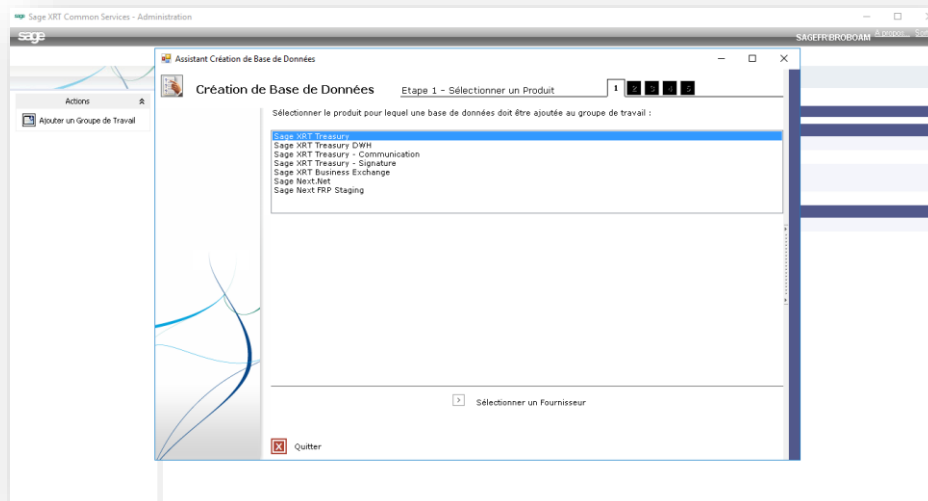
## Créer / Modifier les modèles

1. La liste intitulée **Scripts à exécuter** contient l'ensemble des scripts à exécuter pour créer le modèle « XRT Common Services ». Il comprend le script de création des unités logiques **createlogicalunits.sql** (une unité logique représente un filegroup dans le cas de la création d'une base de données Microsoft SQL Server), le script de création de la table **xl\_configuration createxl\_configuration.sql** dans laquelle sera enregistrée la version du modèle, et le script d'enregistrement des unités logiques **registerlogicalunits.sql**.
2. Les scripts « produit » sont traités par la suite. Suivant leur type, les scripts sont exécutés avec le compte du DBA ou du DBO.
3. Activez la case **Sélectionner les données à importer** et sélectionnez une langue dans la liste. Ces données représentent les données (XML) pour APIFMT, TRANSCO et UMAPI.
4. 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 groupe de travail en cliquant sur l'icône  et entrer dans la Console d'Administration ou ajouter un modèle de Produit.

Cliquez sur Ajouter une base de données Produit; la page suivante s'affiche :



## Sélectionner un produit

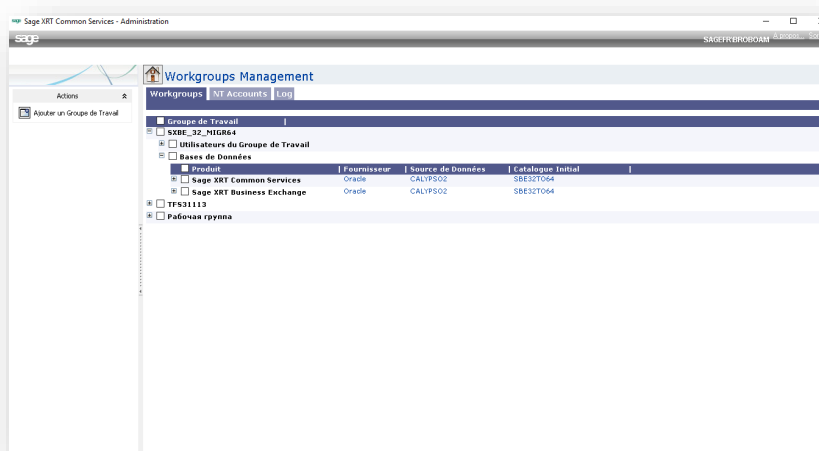
1. Sélectionnez un produit dans la liste.

## 2. Cliquez sur le lien **Sélectionnez un fournisseur.**

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

## Ajout d'un groupe de travail

L'espace de travail de la console d'administration, lorsqu'il est ouvert en mode « Gérer les groupes de travail », se présente de la manière suivante :



Cliquez sur le lien **Ajouter un Groupe de Travail.**

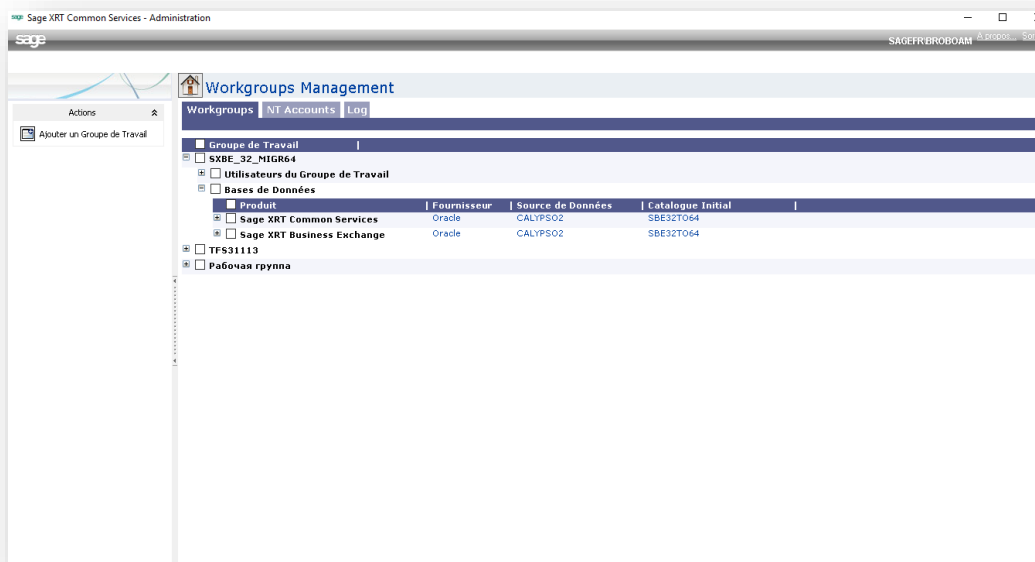
Le processus d'ajout d'un groupe de travail respecte le même principe que celui de la création d'un groupe de travail. Reportez-vous à la section "Création d'un groupe de travail".

## Mise à jour des bases de données d'un groupe de travail

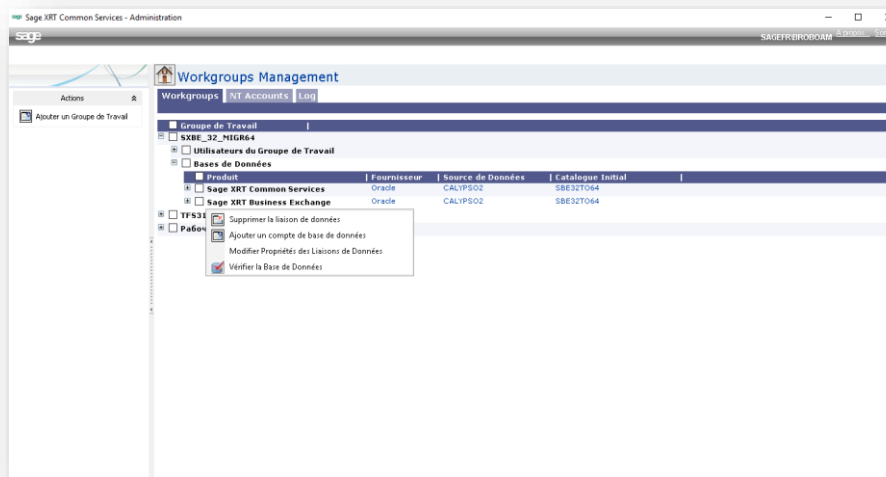
La mise à jour d'une base de données n'est pas sans risque pour les données de l'utilisateur. Il est donc impératif de sauvegarder ces données au préalable.

## Sélectionner la base de données à mettre à jour

1. A partir de la page d'accueil, ouvrez l'arborescence **Groupe de travail**, déployez l'entrée correspondant au nom du Workgroup, puis la sous-entrée **Bases de données**. La page suivante s'affiche :



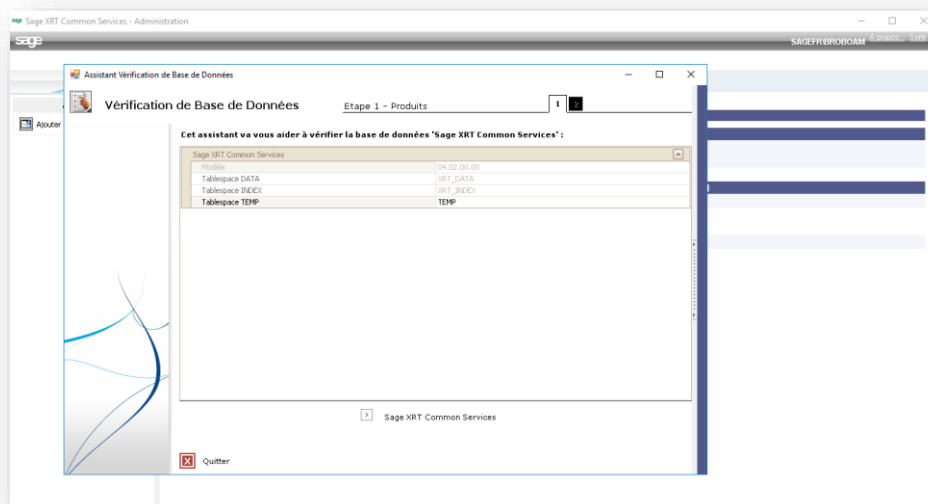
2. Cliquez droit sur une Base de données produit. Le menu contextuel suivant s'affiche :



## Lancer la mise à jour d'une base de données

Après avoir cliqué sur un groupe de travail ou une base de données produit, une fenêtre contextuelle est affichée, présentant une liste d'actions à accomplir.

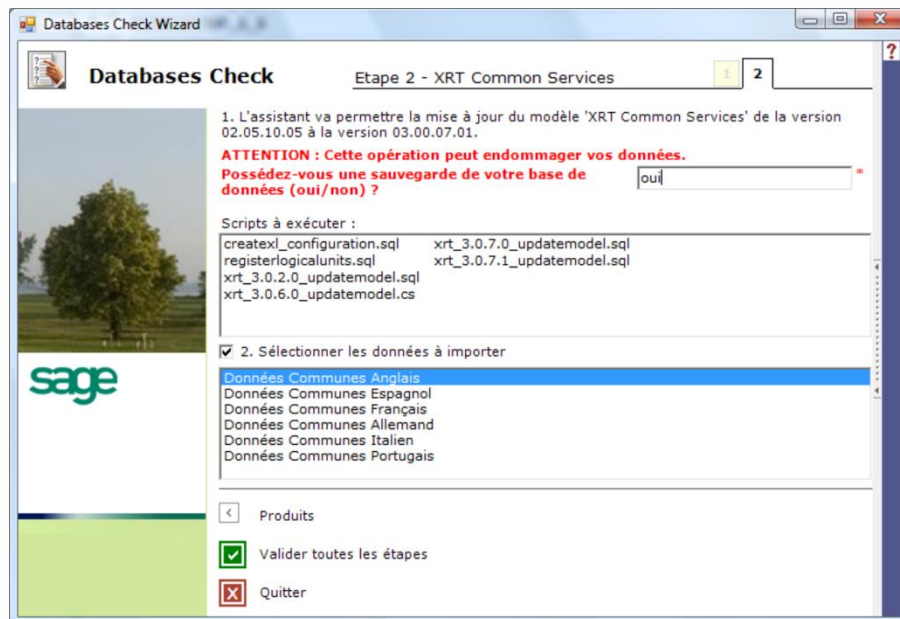
1. Sélectionnez **Vérifier la base de données**. L'assistant de Vérification de Base de Données s'affiche :



Remarque :

Si l'utilisateur Windows n'est pas enregistré en tant que DBO dans le groupe de travail approprié, il ne sera pas autorisé à mettre à jour la base de données. L'assistant ne proposera aucune mise à jour de base de données et à l'écran, le lien XRT Common Services ne sera pas affiché.

2. Cliquez sur le produit. Si l'assistant détecte une incohérence dans les versions, l'utilisateur est renvoyé sur le processus de mise à jour de base de données. Dans le cas contraire, la page suivante s'affiche :



3. Répondez par oui ou par non à la question : Possédez-vous une sauvegarde de votre base de données ?
4. Cochez Sélectionner les données à importer si les données de la base XRT Common Services ne sont pas à jour
5. Cliquez sur le lien Valider toutes les étapes.

## Utilisateurs d'un groupe de travail

Lors de la création d'un WORKGROUP les groupes locaux Windows NT Administrators et XRTDBAdministrators sont automatiquement déclarés comme administrateurs de celui-ci.

Le module XCS propose un assistant permettant de gérer les utilisateurs au sein des groupes de travail.

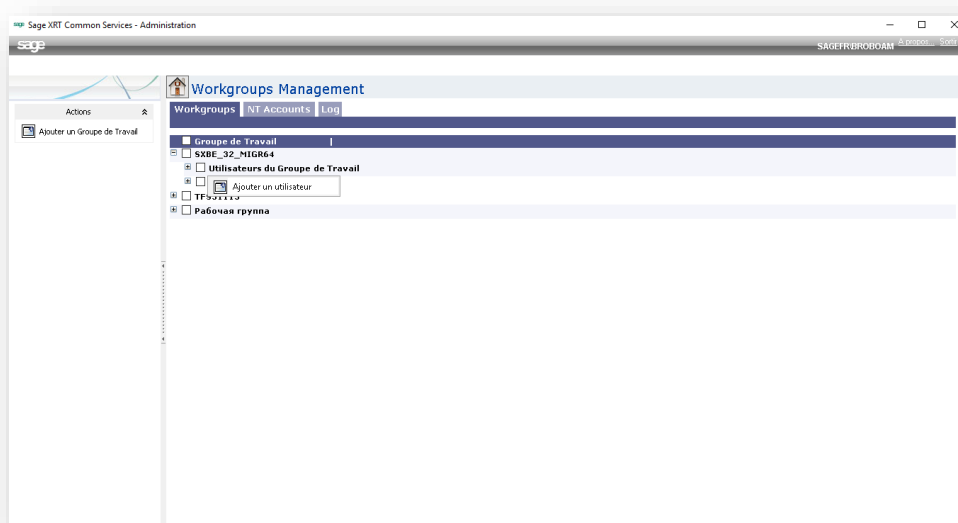
Cet assistant propose les actions suivantes :

- **Ajouter un utilisateur réseau** au groupe de travail. 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 NT.
- **Ajouter un groupe réseau** au groupe de travail. Cette option vous permet d'associer un groupe d'utilisateurs Windows NT à un groupe de travail. Pour réaliser cette association, cliquez sur **Rechercher....** L'outil Microsoft de recherche d'un groupe Windows NT vous aidera à retrouver le groupe d'utilisateur approprié.

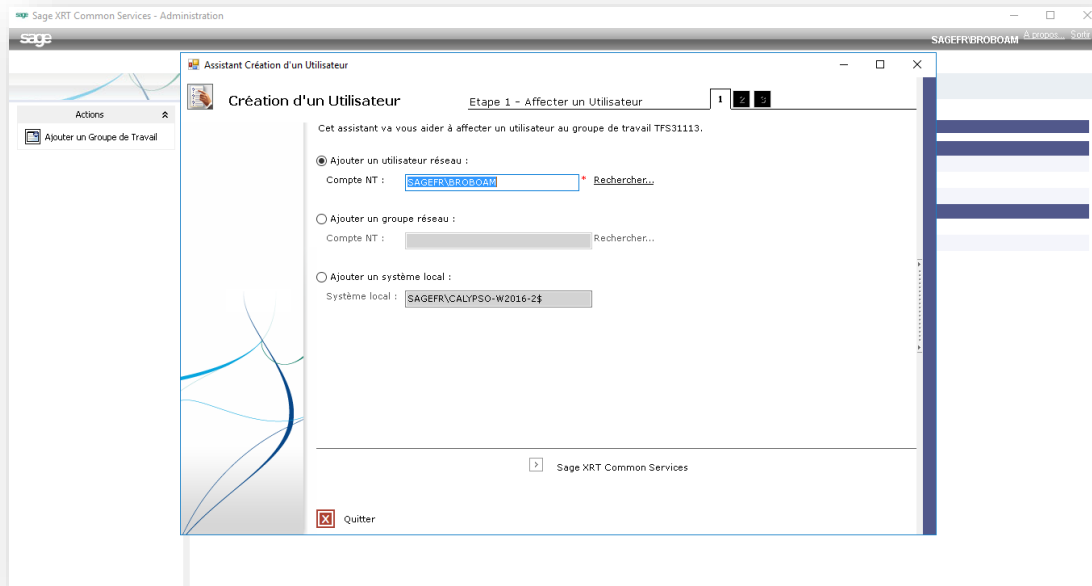
- **Ajouter un compte système local** au groupe de travail. Ce type de compte est utilisé par un **service système** qui est exécuté au compte du **système local** et doit accéder à une base de données.

## Ajouter un utilisateur à un groupe de travail

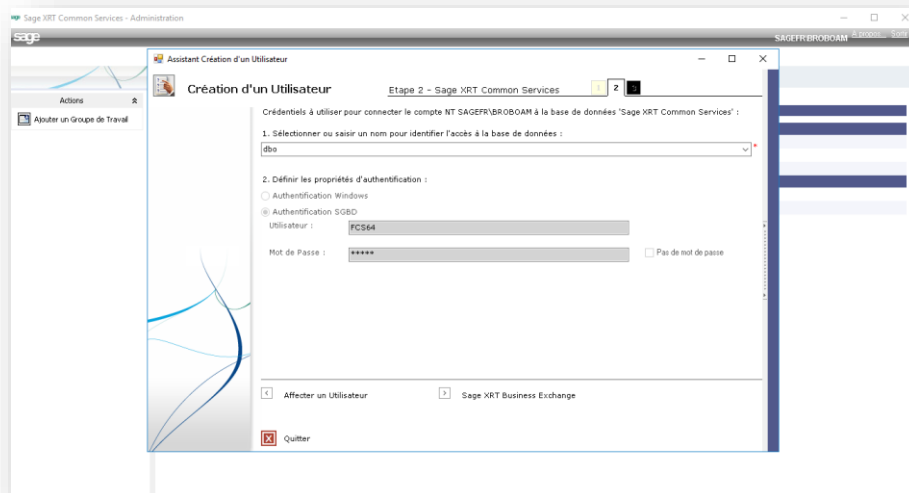
1. Pour assigner un utilisateur au groupe de travail, développez l'élément Groupe de travail.
2. Sélectionnez un groupe de travail dans la liste et cliquez droit sur le niveau Utilisateurs. La page suivante s'affiche :



3. Sélectionnez l'opération **Ajouter un utilisateur**. L'assistant **Création d'un utilisateur** s'affiche :



4. Cliquez sur **XRT Common Services**. La page suivante s'affiche :



5. Sélectionnez par son nom un accès aux données existant 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 utilisateurs « sans pouvoir ».



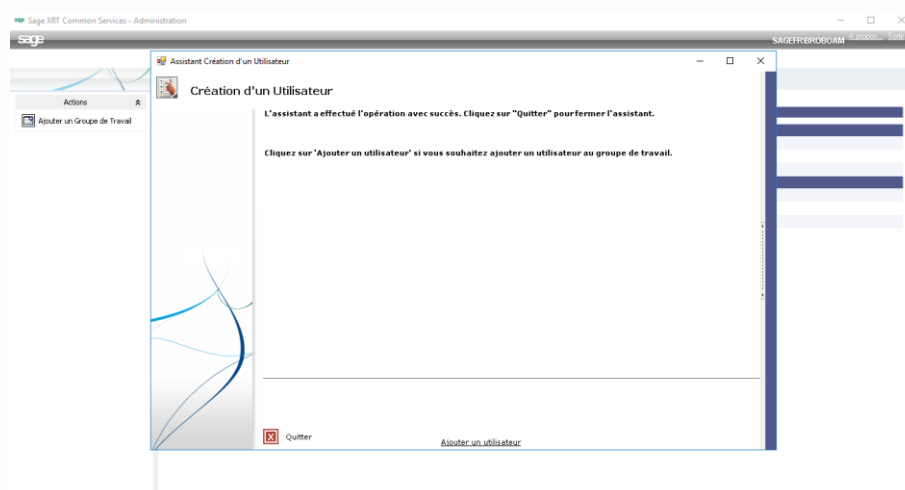
6. Sélectionnez le mode d'authentification de l'utilisateur sur le serveur de bases de données:

- **Authentification Windows** : l'utilisateur est authentifié 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.

**Avertissements** : 1 - 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.

2 - Il est possible de créer un nouveau nom d'accès pour un groupe d'utilisateurs donné. Ce nouvel accès sera de type User. Exemple : définition d'un accès "TRESORIER" pour la base FRP Treasury, avec un compte SQL Server spécifique intitulé TRESO.

7. Cliquez sur Valider toutes les étapes. La page suivante s'affiche :



**Note** : Il est également possible de gérer les utilisateurs du produit SAGE FRP Treasury en répétant l'opération effectuée pour accéder à la base XRT Common Services.



## XDLO

XDLO est un SOA qui gère les chaînes de connexion aux bases de données pour les applications XRT. Avec XDLO,

- Les chaînes de connexion sont stockées dans un référentiel sécurisé partagé par un groupe d'utilisateurs,
- Les chaînes de connexion sont définies par les administrateurs système,
- Chaque utilisateur appartient à un "Workgroup",
- Un utilisateur peut facilement changer de Workgroup à condition que l'administrateur ait configuré les chaînes de connexion appropriées.

En outre, XDLO comporte deux éléments principaux :

- Les objets XDLO, détenus par le composant COM XDLO\_COM.dll et exposés aux clients par le service NT xdlo\_service.exe qui s'exécute sur le poste d'administration, et répond aux demandes de chaînes de connexions effectuées par les clients. Ce service NT écoute les appels sur le port TCP/IP 5151 (cette valeur par défaut peut être changée durant l'installation de XCS).
- Le client (rem\_client.dll) utilisé par les applications XRT pour envoyer des requêtes au service XDLO. Ce composant s'appuie sur les sockets TCP/IP et DCOM pour l'échange de données.

Le nom du poste d'administration est configuré durant l'installation des machines clientes.



## Stockage

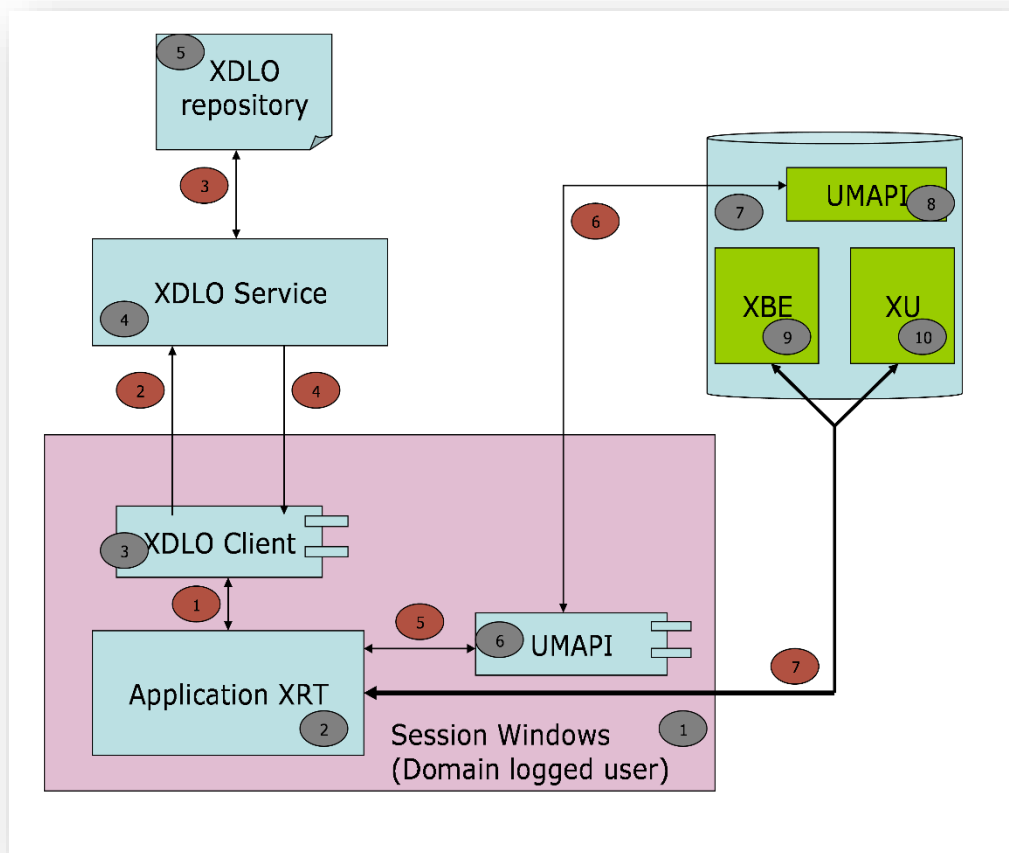
Les objets XDLO sont maintenus dans un fichier XML stocké dans le dossier <All Users>\Application Data\XRT du poste d'administration. L'emplacement de ce fichier peut être changé si nécessaire. Ce fichier peut être installé sur un répertoire partagé dans le cas d'un déploiement en clusters.

Le fichier XML est protégé par l'algorithme de chiffrement 3DES et ne peut être modifié directement par les utilisateurs.

Sur un système de fichiers NTFS, le panneau "sécurité" permet à l'administrateur de configurer des permissions avancées pour restreindre les accès au fichier de stockage de XDLO.

## Dynamique des échanges

Le graphique suivant est une représentation rapide des échanges entre les composants XDLO dans une application XRT. Il représente les différents composants des processus  et les interactions entre ces composants, .



## Composants :

- 1 Session Windows d'un utilisateur du domaine NT. Cette session est ouverte et la connexion à l'application XRT est effectuée avec le compte NT de l'utilisateur connecté.
- 2 L'utilisateur NT exécute une application XRT (SXT, SBE, ...).
- 3 L'application utilise le composant client XDLO installé par le setup d'XCS pour obtenir la chaîne de connexion à la base de données.
- 4 Le composant client XDLO se connecte au service XDLO qui s'exécute sur le poste d'administration. La communication entre le client et le service est effectuée via DCOM.
- 5 Le fichier XDLO contient la définition des groupes de travail et les chaînes de connexion associées. Le service XDLO recherche les informations dans le fichier XDLO.

- 6 Si l'application obtient une chaîne de connexion, elle démarre le composant UMAPI pour vérifier que l'utilisateur est habilité à utiliser le logiciel et obtenir ses permissions d'accès au produit.
- 7 L'application se connecte à la base de données SQL server ou Oracle avec une chaîne de connexion obtenue via XDLO.
- 8 La base de données contient les droits UMAPI des applications XRT.
- 9 La base de données peut contenir les tables SBE et les données de SBE.
- 10 La base de données peut contenir les tables SXT et les données de SXT.

#### Interactions :

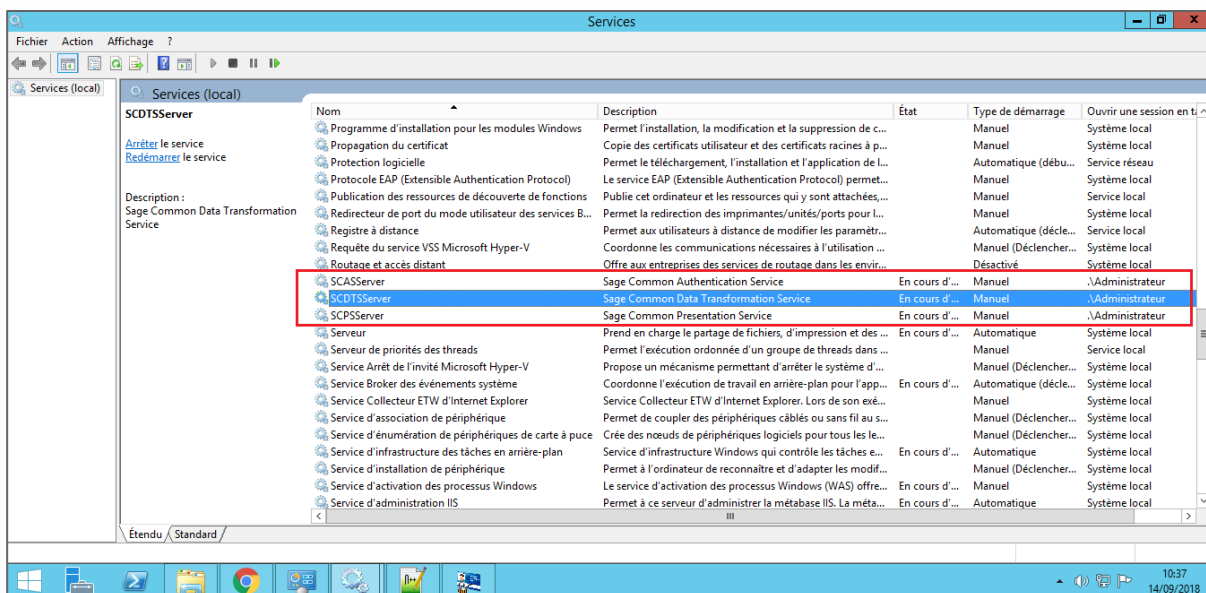
- 1 L'application XRT exécute le client XDLO avec les crédeniels NT de l'utilisateur connecté.
- 2 Le client XDLO se connecte au service sur le port TCP/IP et initie une communication via DCOM.
- 3 Le service XDLO interroge le référentiel XDLO pour retrouver les groupes de travail configurés pour l'utilisateur NT connecté.
- 4 Le service XDLO retourne l'information au client XDLO. Cette donnée permet à l'application de constituer la liste des groupes de travail pour la fenêtre de connexion.
- 5 L'application instancie le composant UMAPI pour obtenir les droits de l'utilisateur sur l'application.
- 6 Le composant UMAPI interroge les tables UMAPI dans la base de données pour obtenir les droits de l'utilisateur. Cette information est retournée à l'application qui peut ainsi finaliser l'initialisation de son environnement d'exécution.
- 7 L'application peut se connecter à son référentiel et l'utilisateur commencer son travail.

## Présentation des 3 services (authentification, présentation et transformation).

Le service d'authentification (SCASServer) permet de valider l'authentification des utilisateurs.

Le service de présentation (SCPSServer) permet de gérer les parties Droits (Utilisateurs, Profils, Sites ...), Audits (Audits, Logs) et Transcodages (Conception et correspondances).

Le service de transformation (SCDTSServer) assure la conversion d'un fichier d'un format A vers un format B et la mise à disposition des informations de suivi du process.



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

Accès 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

## Sage.SCPSServer.Service.exe.config

### Service de Présentation (SCPS) – Fichier de configuration



**Sage.SCPSServer.Service.exe.config** sous C:\Program Files\Common Files\xrt

```
[...]
<system.diagnostics>
<diagnostics>
[...]
```

Possibilité d'activer des logs

```
<add key="websitehost" value="http://localhost"/>
  <add key="httpservicehost" value="http://localhost:8733"/>
  <add key="httpsservicehost" value="https://localhost:8734"/>
  <add key="syncprofilesuser" value="XRT"/>
  <add key="syncprofilesfrequency" value="3600"/>
<!--
  Call http://localhost:8735/api-docs/index.html?url=/api-docs/swagger.json for online help
  Call http://localhost:8735/api-docs/swagger.json to download swagger.json file
```

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

Compte et fréquence (sec) de synchronisation des groupes NT/LDAP

URL de document et URL d'exportation  
**DESACTIVABLE**

12/20/2018

© 2018 The Sage Group plc or its licensors. All rights reserved.

9

## Sage.SCASServer.Service.exe.config

### Service d'Authentification (SCAS) – Fichier de configuration



**Sage.SCASServer.Service.exe.config** sous C:\Program Files\Common Files\xrt

```
[...]
<system.diagnostics>
<diagnostics>
[...]
```

Possibilité d'activer des logs

```
<ApplicationSettings>
  <add key="websitehost" value="http://localhost" />
  <add key="httpservicehost" value="http://localhost:8760/Auth" />
  <add key="httpsservicehost" value="https://localhost:8761/Auth" />
<!--
  Call http://localhost:8762/api-docs/index.html?url=/api-docs/swagger.json for online help
  Call http://localhost:8762/api-docs/swagger.json to download swagger.json file
```

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

URL de document et URL d'exportation  
**DESACTIVABLE**

12/20/2018

© 2018 The Sage Group plc or its licensors. All rights reserved.

5

## Sage.SCDTSServer.Service.exe.config

### Service de Transformation (SCDTS) – Fichier de configuration



Sage.SCDTSServer.Service.exe.config sous C:\Program Files\Common Files\xrt

```
[...]
<system.diagnostics>
<diagnostics>
[...]
```

Possibilité d'activer des logs

```
<ApplicationSettings>
  <add key="websitehost" value="http://localhost" />
  <add key="httpservicehost" value="http://localhost:8740" />
  <add key="httpservicehost" value="https://localhost:8741" />
  <add key="apifmtasyncuser" value="XRT" />
  <add key="apifmtsyncfrequency" value="3600" />
  <add key="payasyncuser" value="XRT" />
  <add key="payasyncfrequency" value="30" />
  <add key="payasyncthreadtaskl" value="10" />
  <add key="payasyncthreadtaskil" value="10" />
```

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

Compte et fréquence (sec) de dépilement des jobs APIFMT

Compte et fréquence (sec) de dépilement des jobs DTS

Nb de threads utilisés pour dématérialiser Flux vers BdD

Nb de threads utilisés pour rematérialiser Flux depuis BdD

12/20/2018

© 2018 The Sage Group plc or its licensors. All rights reserved.

32

### Service de Transformation (SCDTS) – Fichier de configuration



Sage.SCDTSServer.Service.exe.config sous C:\Program Files\Common Files\xrt

```
<ApplicationSettings>
<add key="payasyncexception" value="[WORKGROUP]"/>
```

Id Workgroups à exclure lors du dépilement des jobs

```
<!-- let you follow the payment status file after generation -->
  <add key="payfollowfilepostgen" value="[SXA:FollowSbeSignFile.ps1 -url
  &#34;http://WIN-I8LGUGG6C31:9090/sra/v1/pdssa/getstatus&#34; -idjobext
  &#34;$idjobext&#34; -action &#34;YES&#34;]" />
```

Paramétrage du lien de suivi avec un autre produit (ici sra)

```
<!--
  Call http://localhost:8742/api-docs/index.html?url=/api-docs/swagger.json for
  online help
  Call http://localhost:8742/api-docs/swagger.json to download swagger.json file
```

URL de document et URL d'exportation  
**DESACTIVABLE**

12/20/2018

© 2018 The Sage Group plc or its licensors. All rights reserved.

33