



# Sage XRT Common Services

Version 4.3.100

Guide Utilisateur



# Sommaire

<b>Présentation Générale.....</b>	<b>5</b>
Console Win 32 / Console Web.....	5
<b>Première connexion .....</b>	<b>6</b>
<b>Console Web .....</b>	<b>7</b>
Connexion.....	7
Droits .....	7
Paramétrage authentification .....	7
Règles des mots de passe.....	13
Activation des données et règle des 4 yeux.....	14
Compte utilisateur.....	17
Profils.....	21
Création .....	22
Modification .....	24
Suppression .....	24
Activation.....	24
Sites .....	25
Création .....	25

Activation.....	26
Modification .....	26
Suppression .....	26
Mon compte .....	27
Audits et logs .....	27
Paramétrage .....	27
Audit .....	29
Log .....	30
Transcodages.....	31
Conception .....	31
Correspondances.....	33
<b>Console Win32 .....</b>	<b>36</b>
Paramétrage.....	36
Paramétrage du poste d'administration .....	36
Paramétrage de la machine cliente.....	37
Groupe de travail.....	38
Création d'un groupe de travail.....	38
Ajout d'un groupe de travail.....	47
Mise à jour des bases de données d'un groupe de travail .....	47
Utilisateurs d'un groupe de travail.....	49
Ajouter un utilisateur à un groupe de travail.....	50
<b>XDLO.....</b>	<b>54</b>
Stockage .....	54
Dynamique des échanges.....	55
<b>Présentation des trois services : Authentification, Présentation et Transformation .....</b>	<b>58</b>
Service d'authentification (SCAS) .....	59
Service de présentation (SCPS) .....	59
Service de transformation (SCDTS) .....	60

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.

© 2019 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 XRT Common Services** à proposer les fonctionnalités les plus utilisées dans une interface Web.

Cette version et suivantes apportent aussi de nouvelles fonctionnalités :

- 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

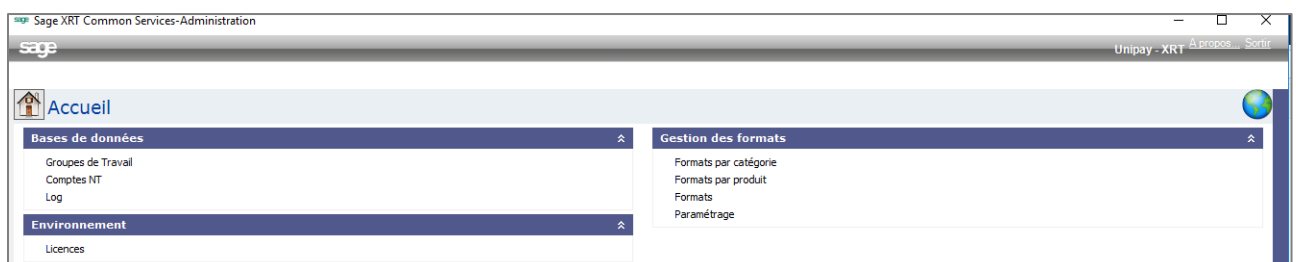
## Console Win 32 / Console Web

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 **Sage XRT Common Services**.


Interface Win 32	Interface Web
Gestion de la licence	Gestion des droits (utilisateurs, profils ...)
Gestion des Groupes de travail	Gestion des connexions (audits, logs ...)
Gestion des formats	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



The screenshot shows the login interface for the Sage XRT administration console. At the top left is the 'sageXRT' logo. The main heading is 'Connexion à la console d'Administration', followed by the instruction 'Connectez-vous en utilisant vos identifiants.' Below this are three input fields: 'Groupe de travail' (a dropdown menu showing 'WEB'), 'Utilisateur' (a text field containing 'WEB1'), and 'Mot de passe' (a masked text field with four dots). A blue 'Me connecter' button is positioned below the password field. At the bottom center, there is a link for 'Mentions légales'.

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

La console Web est disponible via l'url `http://localhost/SCPS/index.html`. Son utilisation nécessite le démarrage des services *SCASServer* et *SCPSServer*.



The screenshot shows the login interface for the Sage XRT Administration Console. At the top left is the 'sageXRT' logo. The main heading is 'Connexion à la console d'Administration'. Below this is a sub-heading 'Connectez-vous en utilisant vos identifiants.' The form contains three input fields: 'Groupe de travail' (a dropdown menu with 'WEB' selected), 'Utilisateur' (a text field containing 'WEB1'), and 'Mot de passe' (a password field with four dots). A blue 'Me connecter' button is positioned below the password field. At the bottom, there is a link for 'Mentions légales'.

### Droits

Ce chapitre présente une description des différentes méthodes d'authentification des utilisateurs proposées par **Sage XRT Common Services** ainsi qu'une description des actions à mener en termes de gestion des utilisateurs et de leurs droits d'accès.

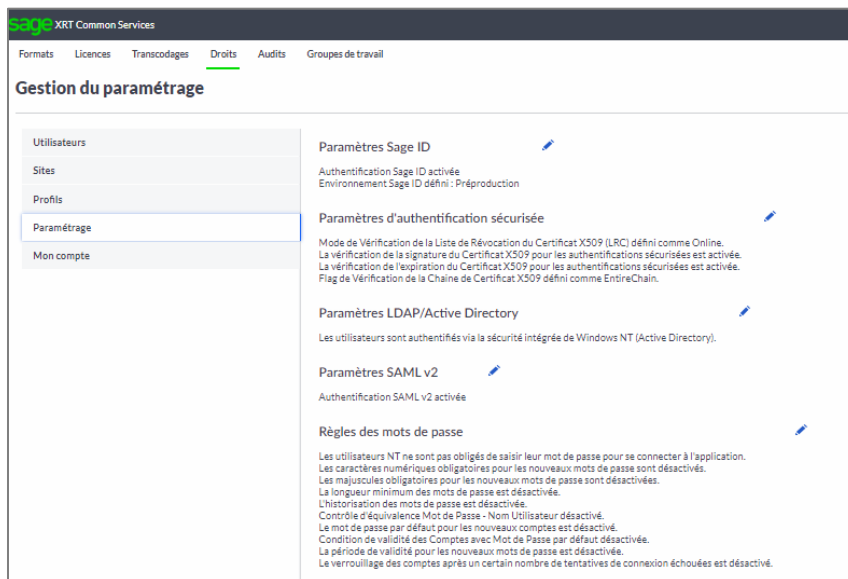
### Paramétrage authentification

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 credentials 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 credentials 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
- 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 **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 crédeniels permettant d'effectuer une recherche sur l'annuaire (le bouton **Test Connection** permet de vérifier ces crédeniels)

Paramètres LDAP/Active Directory

☐ Utiliser Windows Active Directory uniquement

☒ Utiliser aussi le serveur LDAP personnalisé

Hôte: KOKK Port: 389 ☐ SSL

Références de connexion

Bind DN: cn=manager,dc=domain,dc=com Mot de passe

Tester la connexion

DN Base: KOKK

Attribut ID utilisateur: NN

objectClass utilisateur: person

objectClass groupe: groupOfUniqueNames

Attribut membres du groupe: uniqueMember

Tester les paramètres

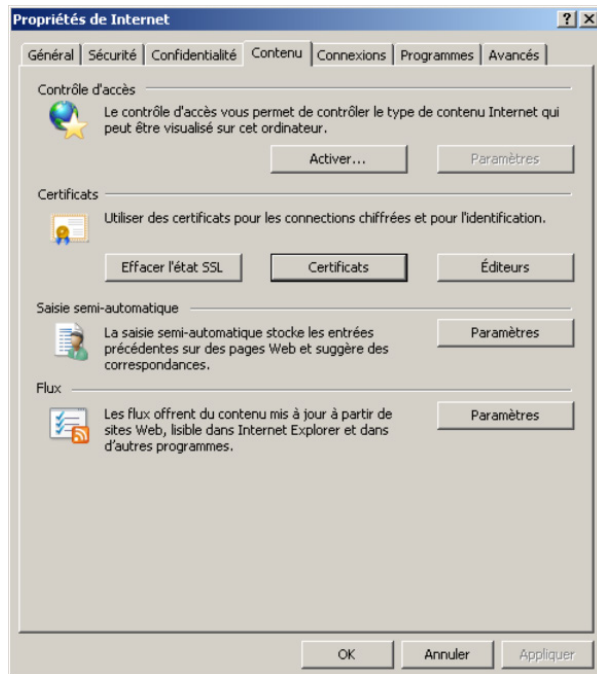
Enregistrer Annuler

**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*.

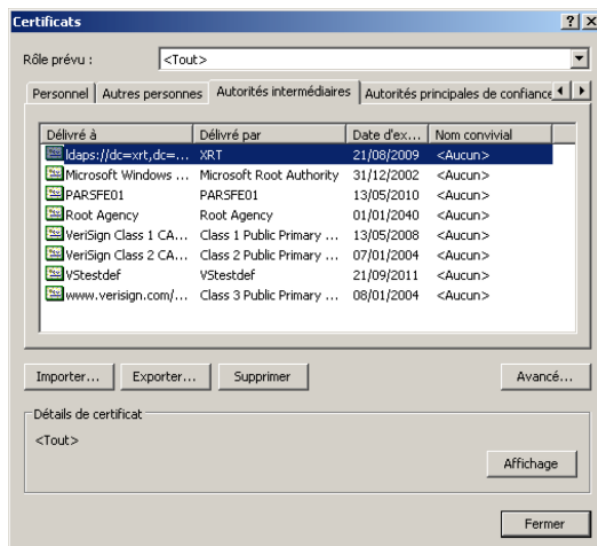
En règle générale, les échanges *LDAP* entre les clients et le serveur transitent par le port *TCP/IP* standard (port 389) sous forme cryptée ou via un tunnel *SSL* (port 636). La technologie *SSL* peut être activée en installant un certificat publié par une autorité de certification approuvée par le 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.

## Console Web

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**)
- 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 *e-mail*)

### Double Authentification

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

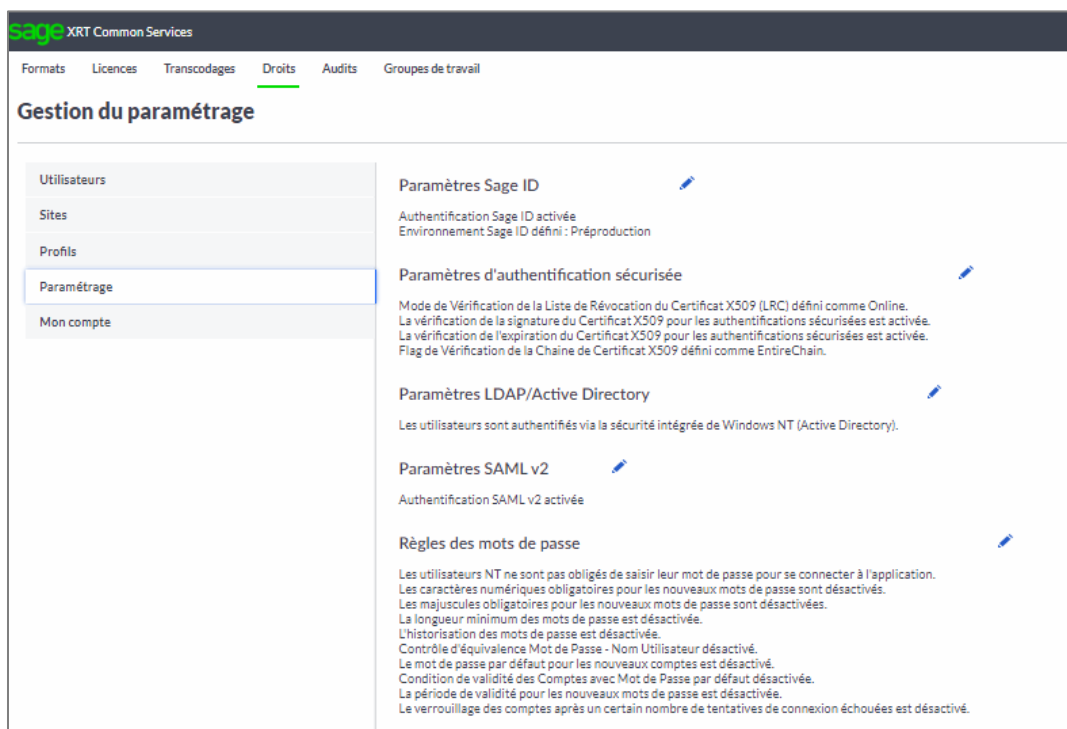
Ce protocole combine une clé secrète avec l'horodatage en cours en utilisant une fonction de hachage cryptographique pour générer un mot de passe à usage unique. Comme la latence du réseau et les horloges désynchronisées peuvent entraîner une tentative d'authentification du destinataire du mot de passe,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

**Note :** Voir le 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.

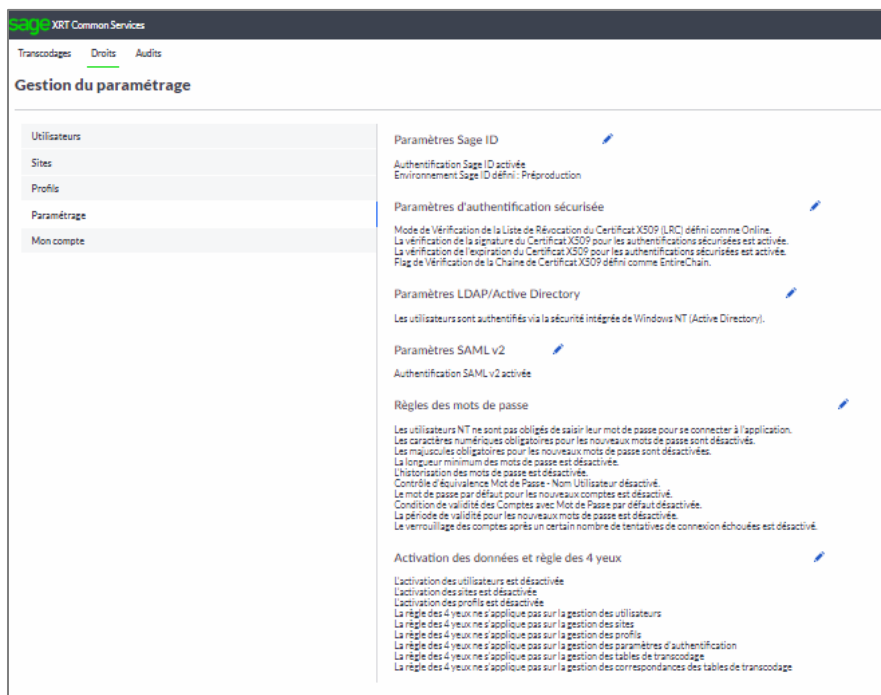
### Activation des données et règle des 4 yeux

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).

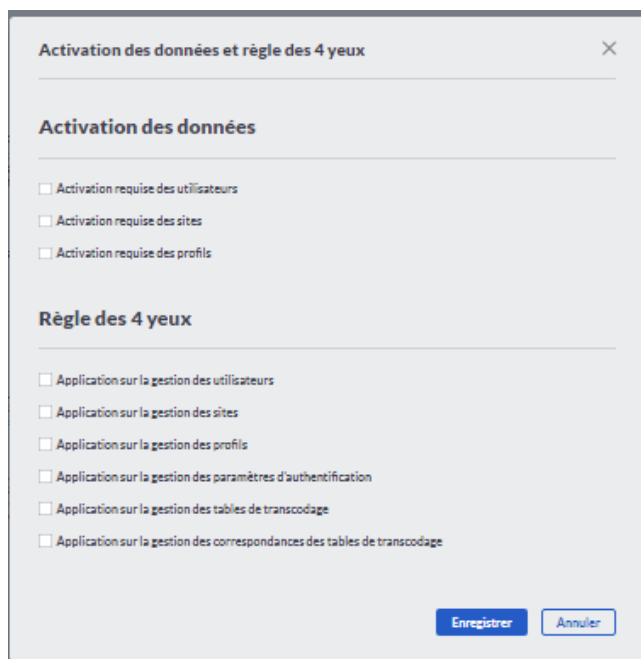
Rappel du principe de la règle des 4 yeux : un même utilisateur ne peut enchaîner 2 actions sur un même élément (création + modification, création + suppression, création + activation...)

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.



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 requise :

- 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 pour envoi des notifications
- 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**.

**Gestion des utilisateurs**

Utilisateurs | Sites | Profils | Paramétrage | Mon compte

<Filtrer par profil> <Filtrer par site> Rechercher le nom contenant... **Nouvel utilisateur**

0 sélectionné(s)

Nom	Description	Type	Profil(s)	Site(s)	Statut
<input type="checkbox"/> ABRILHA		Standard	SIGNATAIRE INTERNE		<b>inactif</b>
<input type="checkbox"/> ADMINISTRATEUR		Niveau 1	<Multiples>		<b>actif</b>
<input type="checkbox"/> AWAGUE		Standard	<Multiples>		<b>actif</b>
<input type="checkbox"/> BDELPR		Standard	SIGNATAIRE BANCAIRE		<b>actif</b>
<input type="checkbox"/> BSARTEL		Standard	SIGNATAIRE BANCAIRE		<b>actif</b>
<input type="checkbox"/> DA		Niveau 1	ADMINISTRATEURS		<b>actif</b>
<input type="checkbox"/> DF		Standard	ADMINISTRATEURS		<b>actif</b>
<input type="checkbox"/> EMACAK		Standard	SIGNATAIRE BANCAIRE		<b>actif</b>
<input type="checkbox"/> ENT1		Niveau 1	ADMINISTRATEURS		<b>actif</b>
<input type="checkbox"/> ENT11		Standard	ADMINISTRATEURS		<b>actif</b>
<input type="checkbox"/> ENT2		Standard	ADMINISTRATEURS		<b>actif</b>
<input type="checkbox"/> FCHATEA		Standard		UTILISATEURS	<b>actif</b>
<input type="checkbox"/> FWILLOT		Standard	SIGNATAIRE BANCAIRE		<b>actif</b>

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

Profil(s)  
 Sites

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

**Enregistrer** **Annuler**

3. 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**.

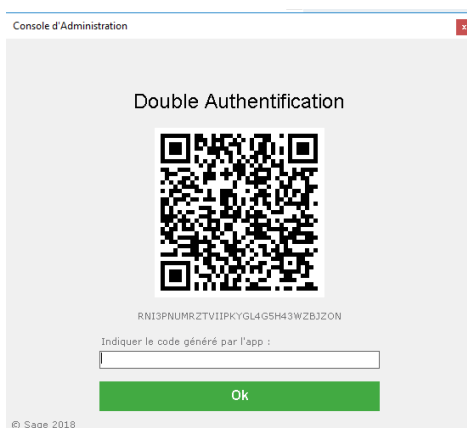
**Authentification standard** : Saisie d'un identifiant unique pour l'utilisateur.

**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 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'a pas été faite, cette option apparaît en orange. Par la suite, elle sera affichée 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.

4. 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.

5. Complétez les informations suivantes.

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

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

7. Cliquez sur **Enregistrer** ou **Annuler** pour sortir de la boîte de dialogue et 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

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

**Gestion des profils**

Utilisateurs Sites Profils Paramétrage Mon compte

Nouveau profil

Nom	Description	Type de profil	Statut
ADMINISTRATEURS		Générique	actif
DRH		Générique	actif
INFORMATIQUE		Générique	actif
PAIE	GROUPE PAIE RH	Générique	actif
SIGNATAIRE BANCAIRE	SIGNATAIRE BANCAIRE	Générique	actif
SIGNATAIRE INTERNE	SIGNATAIRE INTERNE	Générique	actif
STAGIAIRE	STAGIAIRES	Générique	actif
TEST DROITS	TEST DROITS	Générique	inactif
TESTEUR	TESTEUR	Générique	actif
TRESORERIE		Générique	actif

Afficher 10 enregistrements(s) Page 1 sur 2 12 enregistrements(s)

2. Cliquez sur le bouton **Nouveau profil**. La page suivante s'affiche.

**Création d'un profil**

Nom\*  
Saisissez le nom de votre profil

Description  
Saisissez la description de votre profil

Type de profil

Générique ☒ Utilisateurs associés

Groupe NT ☐ TEST

Groupe LDAP ☐ WEB1 ☐ WEB2

Créer Annuler

**Création d'un profil**

Nom\*  
Saisissez le nom de votre profil

Description  
Saisissez la description de votre profil

Type de profil

Générique ☒ Langue par défaut\*  
Anglais

Groupe NT ☐ Niveau de sécurité par défaut\*  
Utilisateur standard

Groupe LDAP ☐

Créer Annuler

3. Pour créer un profil, renseignez les informations suivantes :
  - **Nom** : saisissez un nom pour le profil. Ce champ doit être renseigné obligatoirement.
  - **Description** : saisissez une description pour le profil.

### 4. Sélectionner le type de profil :

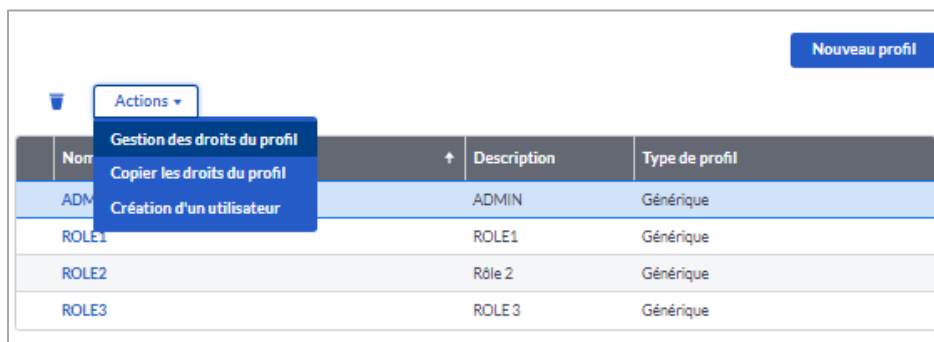
- **Générique** : sélectionnez les utilisateurs existants à associer au profil
- **Groupe AD** : tout utilisateur membre du groupe est automatiquement enregistré dans la base de données comme utilisateur des applications **XRT**. Le profil de type *Groupe AD* s'appuie sur les données relatives aux comptes 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. 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**.

5. 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**.

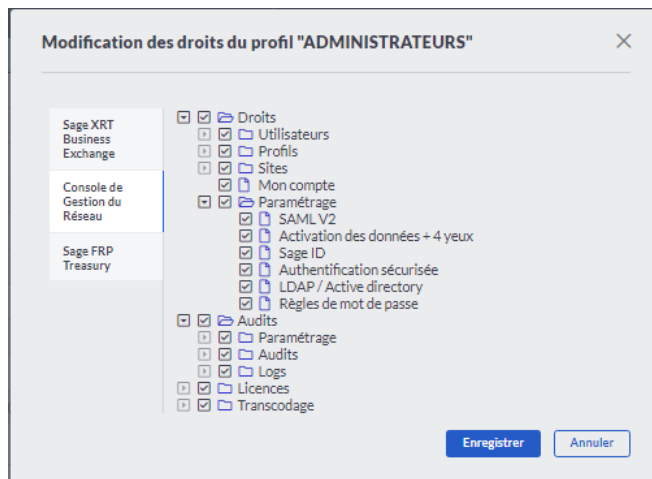


The screenshot shows a web interface for managing profiles. At the top right is a button labeled "Nouveau profil". Below it is a table with columns: "Nom", "Description", and "Type de profil". The table contains four rows: "ADM", "ROLE1", "ROLE2", and "ROLE3". An "Actions" dropdown menu is open over the "ADM" row, showing three options: "Gestion des droits du profil", "Copier les droits du profil", and "Création d'un utilisateur".

Nom	Description	Type de profil
ADM	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**.



3. Activez les droits à accorder.
4. Répétez l'opération pour les produits **Sage XRT Treasury** et **Sage 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

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

La liste des profils existants s'affiche.

2. Pour modifier un profil, utilisez le lien disponible sur le nom du profil.
3. Procédez aux modifications souhaitées et cliquez sur le bouton **Enregistrer**.

## Suppression

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

La liste des profils existants s'affiche.

2. Pour supprimer un profil, sélectionnez la case à cocher correspondante et cliquez sur 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.

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

The screenshot shows the 'Gestion des sites' (Site Management) page. On the left, a sidebar contains links for 'Utilisateurs', 'Sites' (selected), 'Profils', 'Paramétrage', and 'Mon compte'. The main area displays a table of sites with columns 'Nom', 'Description', and 'Type de site'. The table lists five sites: ADMINISTRATEURS, DRH, INFORMATIQUE, TRESORERIE, and UTILISATEURS, all with the type 'Générique'. A 'Nouveau site' button is located in the top right corner. At the bottom, there is a pagination bar showing 'Page 1 sur 1' and '5 enregistrement(s)'.

Nom	Description	Type de site
ADMINISTRATEURS		Générique
DRH		Générique
INFORMATIQUE		Générique
TRESORERIE		Générique
UTILISATEURS		Générique

2. Cliquez sur le bouton **Nouveau site**. La page suivante s'affiche.

The screenshot shows the 'Création d'un site' (Create Site) form. It has a title bar with a close button. The form contains three main sections: 'Nom' with a text input field, 'Description' with a text input field, and 'Type de site' with a dropdown menu. The dropdown menu is open, showing options: 'Générique', 'Groupe NT', 'Groupe LDAP', and 'Utilisateurs associés'. The 'Utilisateurs associés' option is selected, and a sub-menu is displayed with checkboxes for 'TEST', 'WEB1', and 'WEB2'. At the bottom right, there are two buttons: 'Créer' and 'Annuler'.

3. Pour créer un site, renseignez les informations suivantes :
  - **Nom** : saisissez un nom pour le site. Ce champ doit être renseigné obligatoirement.
  - **Description** : saisissez une description pour le site.
4. 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 **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.
5. 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

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

La liste des sites existants s'affiche.

2. Pour modifier un site, utilisez le lien disponible sur le nom du site.
3. Procédez aux modifications souhaitées et cliquez sur le bouton **Enregistrer**.

## Suppression

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

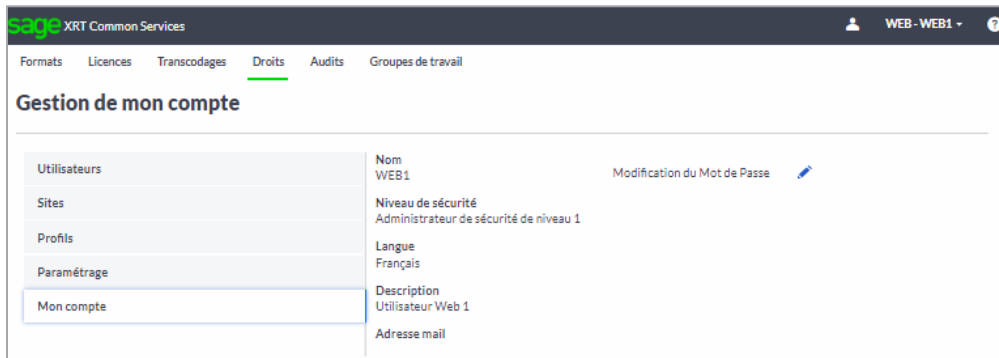
La liste des sites existants s'affiche.

2. 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 E-mail**.

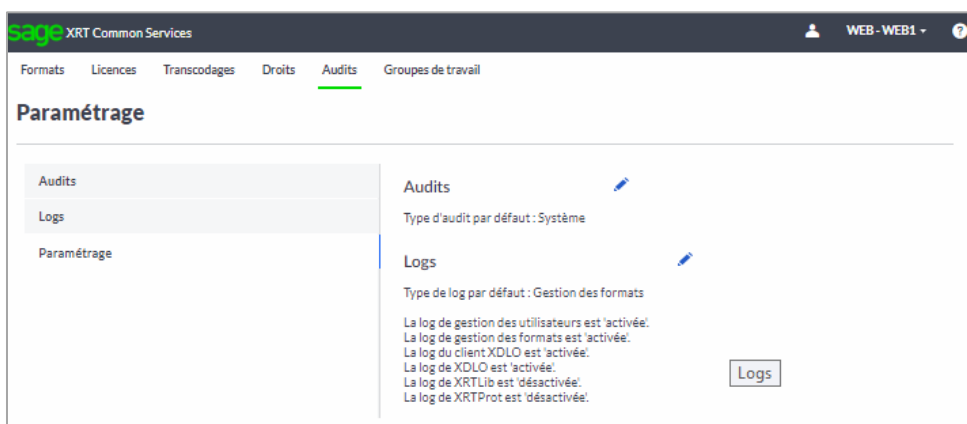
Seul le mot de passe peut être modifié en utilisant l'icône *Styl*o.

### 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.

1. 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*.

2. Sélectionnez le type d'audit qui sera proposé par défaut à l'appel de la fonction **Audit** :
  - Système
  - Base de données
  - Utilisateurs
3. Sélectionnez le type de log qui sera proposé par défaut à l'appel de la fonction **Log** :
  - Gestion des formats
  - Gestion des utilisateurs
  - Gestion base de données
  - Gestion de la console
  - Client XDLO
  - XDLO
  - Service XDLO
  - XRTProt
  - XRTPLogin
  - XRTPLib
4. Cochez les logs à activer.
5. 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 XRTPLib

☒ Activer la log client XDLO    ☐ Activer la log XRTProt

Enregistrer Annuler

### Audit

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

Le type d'audit défini par défaut s'affiche.

**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-C2QPQHDOQB2	
18/10/2018 14:13:13	Login	Echec	CS	FCS Web	WEB1	Administrateur	WIN-C2QPQHDOQB2	Une exception de type 'UMAPILib.UMAPIException' a été levée.
18/10/2018 14:13:12	Login	Echec	CS	FCS Web	WEB1	Administrateur	WIN-C2QPQHDOQB2	Une exception de type 'UMAPILib.UMAPIException' a été levée.
18/10/2018 14:12:51	Login	Echec	CS	FCS Web	WEB1	Administrateur	WIN-C2QPQHDOQB2	Une exception de type 'UMAPILib.UMAPIException' a été levée.
18/10/2018 12:03:48	Login	Succès	CS	FCS Web	WEB1	Administrateur	WIN-C2QPQHDOQB2	
18/10/2018 11:27:27	Login	Succès	CS	FCS Web	WEB1	Administrateur	WIN-C2QPQHDOQB2	
18/10/2018 11:00:17	Login	Succès	CS	FCS Web	BROBOAM@DOMVMDSF.COM	Administrateur	WIN-C2QPQHDOQB2	
18/10/2018 10:32:39	Login	Succès	CS	FCS Web	WEB1	Administrateur	WIN-C2QPQHDOQB2	
18/10/2018 10:30:07	Login	Echec	CS	FCS Web	WEB1	Administrateur	WIN-C2QPQHDOQB2	Invalid password.
18/10/2018 10:29:16	Login	Echec	CS	FCS Web	WEB1	Administrateur	WIN-C2QPQHDOQB2	Invalid password.

Afficher 10 enregistrements(s) Page 1 sur 3 24 enregistrements(s)

2. Pour modifier le type par défaut, sélectionnez une option dans la liste déroulante **Type d'audit**.
3. Pour filtrer les informations affichées, sélectionnez une option dans liste déroulante **Période** :
  - Aujourd'hui
  - Semaine courante
  - Mois courant
  - Année courante

D'autres critères de sélection sont disponibles en utilisant le bouton **Rechercher**. Les critères de filtre appliqués sont rappelés au-dessus de la liste.

4. Cliquez sur le bouton **Purger** pour supprimer ou exporter des événements de la liste.

### Suppression d'évènements de l'audit 'Utilisateurs'

Evènements antérieurs au :

Nombre d'évènements à supprimer :

ExporterSupprimerAnnuler

## Log

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

Le type de log défini par défaut s'affiche.

Sage XRT Common Services

Unipay -XRT

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:FMtdDisconnect
16/10/2018 08:51:00	DEBUG	return_S_OK

Afficher 10 enregistrement(s) Page 1 sur 1 2 enregistrement(s)

2. Pour modifier le type par défaut, sélectionnez une option dans la liste déroulante **Type de log**.
3. Pour filtrer les informations affichées, sélectionnez une option dans liste déroulante **Période** :
  - Aujourd'hui
  - Semaine courante
  - Mois courant
  - Année courante

D'autres critères de sélection sont disponibles en utilisant le bouton **Rechercher**. Les critères de filtre appliqués sont rappelés au-dessus de la liste.

## Transcodages

### Conception

#### Création

1. 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.

**Conception des tables de transcodage**

Conception | Correspondances

<Filtrer par nom> <Filtrer par description> Rechercher le nom contenant...

0 sélectionné(s) Actions

Nom	Description	Nombre de colonnes en entrée	Nombre de colonnes en sortie
acsaebdv.dat	Correspondance Code Devise AEB <-> Code ISO	1	1
ACSAFBDV.DAT	Correspondance Code Devise AFB <-> Code ISO	2	1
ACSAFBPA.DAT	Table des partenaires	1	1
ACSAFBVE.DAT	Taux de change de l Euro par devise	1	1
ACSAFB_TO_MT		1	1
acsfinstapa.dat	Parametres d'intégration FINSTA	2	1
ACSMT_OP.DAT	Traduction des codes opération SWIFT	1	1
ACSMT_OP_DIR		2	1
AEB43_PARAM		1	1
AFB120RT_PARAM	Parametrage de l'AFB 120	1	1

Afficher 10 enregistrement(s) Page 1 sur 6 56 enregistrement(s)

2. Cliquez sur le bouton **Nouvelle table** pour créer une table.

**Création d'une table**

Nom\*

Description

0 sélectionné(s) Nouvelle colonne

Nom	Type de colonne
-----	-----------------

Annuler

3. Renseignez obligatoirement un **Nom** pour la table et éventuellement une **Description**.
4. Cliquez sur 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

5. Pour chaque colonne, renseignez obligatoirement un Nom et sélectionnez le Type de colonne (Entrée ou Sortie).
6. 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 supprimée 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

7. Cliquez sur le bouton **Enregistrer** pour enregistrer la création de la table.

La table s'inscrit alors dans la liste.

### Modification

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

La liste des tables existantes s'affiche.

2. Pour modifier une table, utilisez le lien disponible sur le nom de la table.
3. Procédez aux modifications souhaitées et cliquez sur le bouton **Enregistrer**.

### Suppression

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

La liste des tables existantes s'affiche.

2. Pour supprimer une table, sélectionnez la case à cocher correspondante et utilisez l'icône *Poubelle*.

### Import

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

La liste des tables existantes s'affiche.

2. Pour importer des tables de transcodage, cliquez sur le bouton **Importer**.

Une boîte de dialogue pour sélectionner le fichier à importer s'ouvre.

3. Sélectionnez un fichier et cliquez sur **Ouvrir**.

### Export

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

La liste des tables existantes s'affiche.

2. Pour exporter une table, activez la case à cocher correspondante, puis sélectionnez **Exporter** dans la liste déroulante **Actions**.

### Correspondances

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

### Création

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

La table **RIBS-Table IBAN** est sélectionnée par défaut dans la liste déroulante **Table** pour l'affichage des correspondances.

2. Sélectionnez dans la liste déroulante la table pour laquelle les correspondances doivent être créées.

La structure de la table s'affiche

sage XRT Common Services

Formats Licences **Transcodages** Droits Audits Groupes de travail

Correspondances dans les tables de transcodage

Conception  
Correspondances

Table  
DOC

Nouvelle correspondance

0 sélectionné(s)

ENTREE 1 (E)	ENTREE 2 (E)	SORTIE (S)
--------------	--------------	------------

Afficher 10 enregistrement(s) Page 1 sur 1 0 enregistrement(s)

3. Cliquez sur le bouton **Nouvelle correspondance**.

Création d'une correspondance

ENTREE 1 (E)\*

ENTREE 2 (E)\*

SORTIE (S)

Enregistrer Annuler

4. Renseignez pour chaque correspondance, la ou les valeurs d'entrée et la ou les valeurs de sortie.
5. 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**.

**Correspondances dans les tables de transcodage**

Table: ACSAFB\_TO\_MT

0 sélectionné(s)

	Code_AFB (E)	Code_Swift (S)
<input type="checkbox"/>	01	NCHK
<input type="checkbox"/>	02	NCLR
<input type="checkbox"/>	03	NRTI
<input type="checkbox"/>	04	NMSC
<input type="checkbox"/>	05	NTRF
<input type="checkbox"/>	06	NTRF
<input type="checkbox"/>	07	NBOE
<input type="checkbox"/>	08	NDDT
<input type="checkbox"/>	09	NDDT
<input type="checkbox"/>	10	NRTI

Afficher 10 enregistrement(s) Page 1 sur 11 103 enregistrement(s)

### Modification

1. A partir du menu **Transcodages**, cliquez sur l'entrée **Correspondances**.
2. Sélectionnez la table de travail.

La liste des correspondances existantes s'affiche.

3. Pour modifier une correspondance, utilisez le lien disponible sur la première colonne de la table.
4. Procédez aux modifications souhaitées et cliquez sur le bouton **Enregistrer**.

### Suppression

1. A partir du menu **Transcodages**, cliquez sur l'entrée **Conception**.
2. Sélectionnez la table de travail.

La liste des correspondances existantes s'affiche.

3. 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.

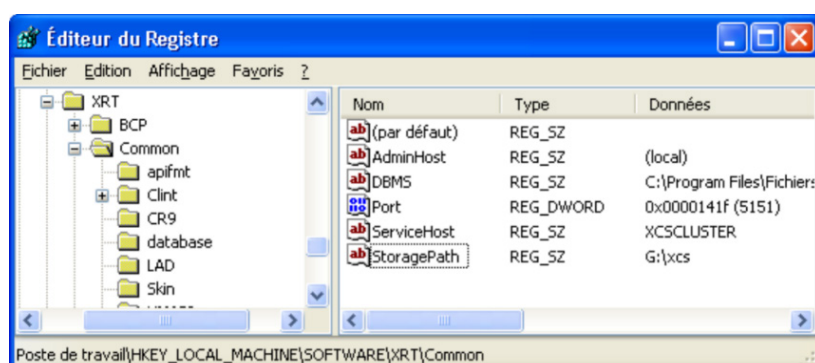
#### Paramétrage du poste d'administration

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*.

Cette clé contient les valeurs suivantes :

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



Les paramètres optionnels de XDLO sont définis dans la clé de registre `HKEY_LOCAL_MACHINE\SOFTWARE\XRT\Common\XDLO`.

Cette clé contient la valeur suivante :

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

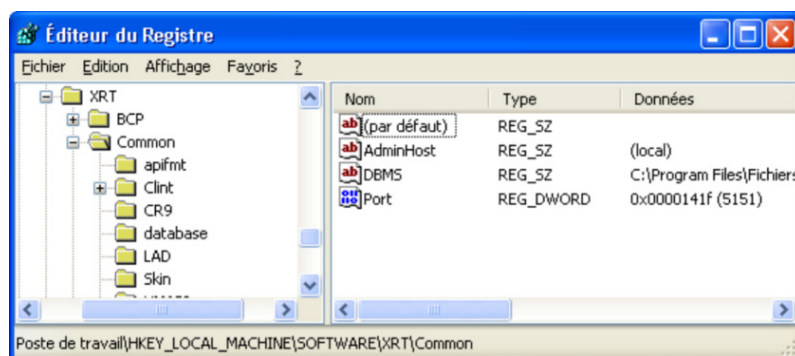
### Paramétrage de la machine cliente

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`.

Cette clé contient les valeurs suivantes :

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



Les paramètres optionnels de la partie cliente de *XDLO* sont définis dans la clé de registre *HKEY\_LOCAL\_MACHINE\SOFTWARE\XRT\Common\XDLO*.

Cette clé contient les valeurs suivantes :

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

## Groupe de travail

Dans le cas d'une première installation de **Sage XRT Common Services**, 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*.

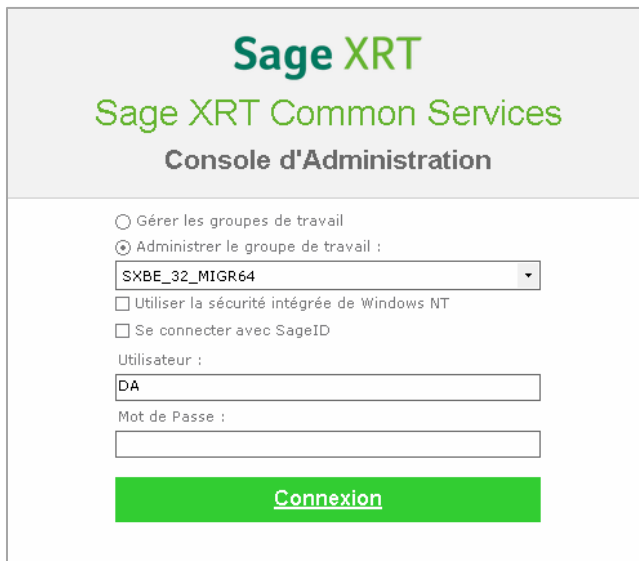
Vous trouverez également la description détaillée des premières actions à entreprendre après la création d'un groupe, à savoir la mise à jour d'une base de données, l'ajout d'un groupe de travail ou encore la gestion des utilisateurs d'un groupe.

## Création d'un groupe de travail

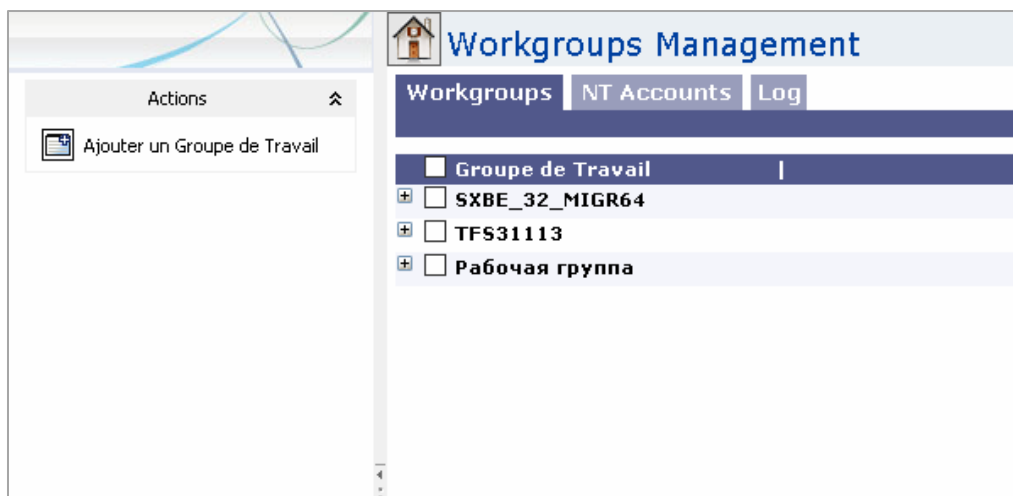
### Assistant de création d'un groupe de travail

1. A partir du menu Démarrer, sélectionnez **Programmes > Sage > Administration XRT .NET**.

L'écran de connexion s'affiche.



2. Sélectionnez l'option **Gérer les groupes de travail**.
3. Cliquez sur **OK**.



4. Cliquez sur le lien **Ajouter un groupe de travail** pour lancer l'assistant Création d'un **Groupe de travail**.

**Note :** Lorsqu'aucun groupe de travail n'est défini, l'écran **Création d'un groupe de travail** s'affiche immédiatement, sans passer par les étapes 2 et 3.

## Définir le nom d'un groupe de travail

Assistant Création d'un Groupe de Travail

Création d'un Groupe de Travail

Etape 1 - Définir le nom d'un Groupe de Travail

Cet assistant va vous aider à créer un groupe de travail.

Un groupe de travail est un jeu de bases de données partagées par un groupe d'utilisateurs.

Vous devrez tout d'abord créer une Base de Données 'Sage XRT Common Services' qui contiendra les permissions utilisateur, les formats, etc.

1. Saisir un nom de groupe de travail

Nom :

2. Sélectionner un mode de gestion des droits d'accès pour les utilisateurs de l'application (UMAPI) :

☒ Les droits d'accès sont accordés par un administrateur de sécurité.

☐ Les droits d'accès sont accordés par un administrateur de sécurité de niveau 1 puis validés par un administrateur de sécurité de niveau 2.

[Sélectionner un Fournisseur](#)

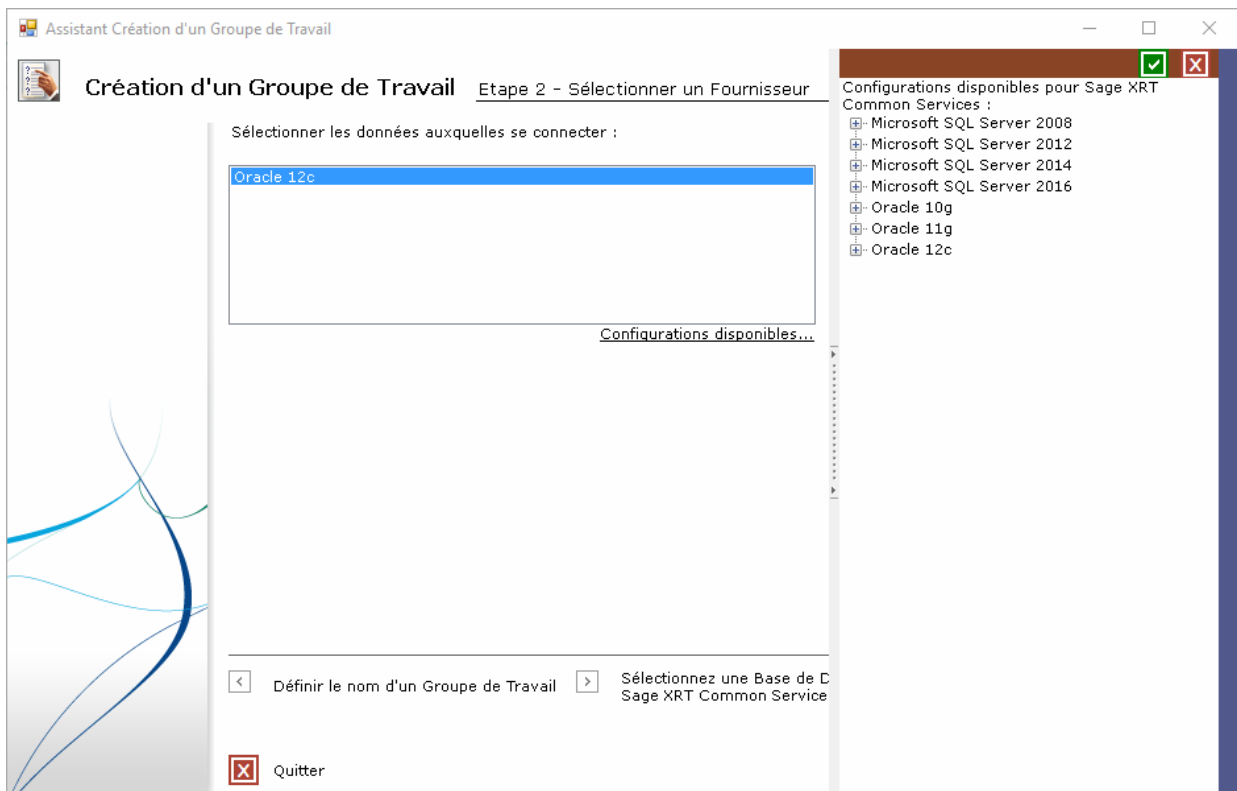
[Quitter](#)

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, avec un seul administrateur de sécurité, sélectionnez l'option **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 l'option **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.

## 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).



3. Cliquez sur l'icône **Quitter** pour fermer la page et revenir à l'écran de sélection des fournisseurs d'accès aux bases de données.
4. Cliquez sur **Sélectionner une base de données**.

## Sélectionner une base de données

Assistant Création d'un Groupe de Travail

Création d'un Groupe de Travail

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

1. Sélectionner un service Oracle :

Sélectionner les informations nécessaires à la connexion aux données Oracle :

CALYPSO2  
ORACLR\_CONNECTION\_DATA

2. Saisir les créditsiels de l'administrateur de base de données :

Nom : system \*

Mot de Passe : \*

3. Saisir les créditsiels du propriétaire du schéma de base de données :

☒ Sélectionner le schéma : Version du modèle XRT :  
☐ Créer le schéma :  
 Nom : \* Mot de Passe : \*  
 Utilisateurs : XRTUSERS \* Mot de Passe : \*\*\*\*\* \*

< Sélectionner un Fournisseur > Produits

Quitter

Tester la connexion DBA  
 Tester la connexion DBO  
 Tester la connexion USERS

1. Saisissez le nom du serveur sur lequel la base de données doit être créée. Les valeurs disponibles 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 une des options suivantes :
  - **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 créden-  
tiels 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* 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. 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 créden-  
tiels 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 créden-  
tiels 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 conservez celle proposée par défaut, *French\_CI\_AS* (pas de distinction entre majuscule et minuscule).
4. Cliquez sur **Produits**.

### Configurer les 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 *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 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 cible n'existent pas (par exemple, *XCS\_DATA* et *XCS\_INDEX*), ceux-ci sont automatiquement créés par l'assistant.

Cliquez sur Créer / Modifier les modèles.

### Créer / Modifier les modèles

La liste intitulée **Scripts à exécuter** contient l'ensemble des scripts utilisés pour la création du modèle *XRT 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 sera 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*.

1. Activez la case **Sélectionner les données à importer** et sélectionnez une langue dans la liste.

Cette importation concerne les données (format *XML*) pour *APIFMT*, *TRANSCO* et *UMAPI*.

2. 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.

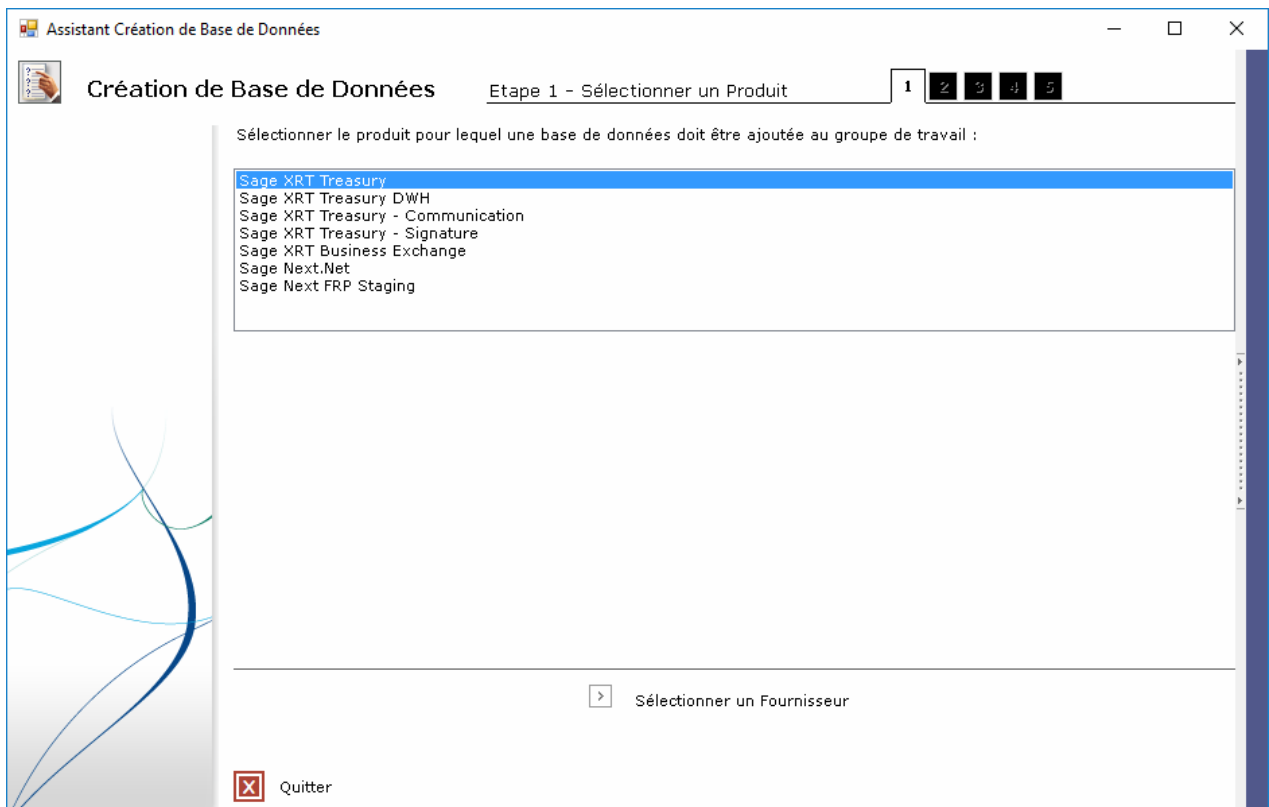
### Exécution des opérations

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 **Quitter** et lancer la Console d'Administration ou ajouter un modèle de Produit.

Cliquez sur **Ajouter une base de données Produit**.

### Sélectionner un produit

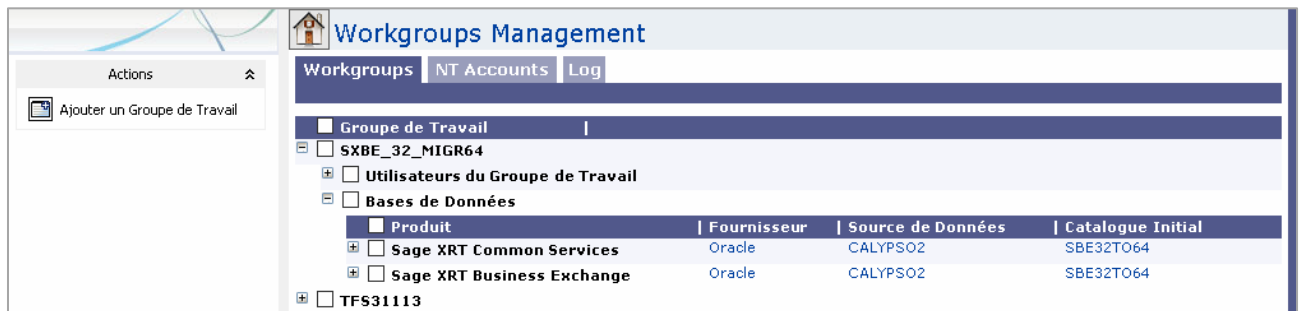


1. Sélectionnez un produit dans la liste.
2. Cliquez sur le lien **Sélectionnez un fournisseur**.

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

## Ajout d'un groupe de travail

L'espace de travail de la Console d'administration, lorsque celle-ci est ouverte en mode **Gérer les groupes de travail**, se présente de la façon 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**.

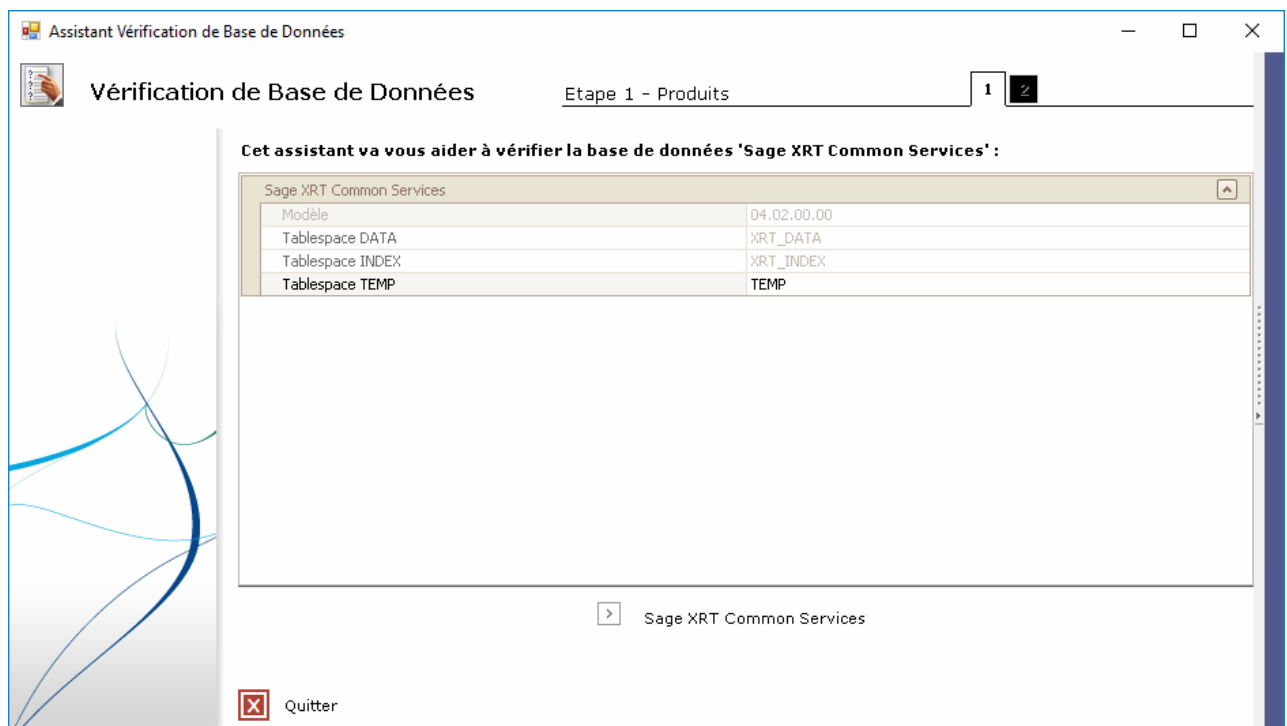
## Mise à jour des bases de données d'un groupe de travail

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 ses données au préalable.

1. A partir de la page d'accueil, ouvrez l'arborescence **Groupe de travail** et déployez l'entrée correspondant au nom du groupe de travail, puis la sous-entrée **Bases de données**.
2. 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.

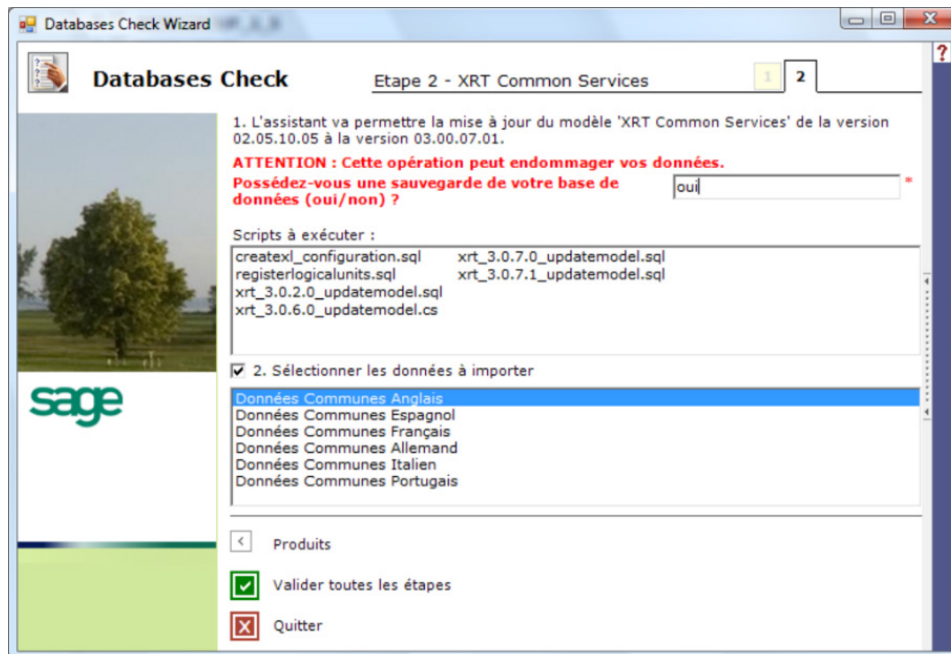


L'assistant **Vérification de Base de Données** s'affiche.



**Note :** Si l'utilisateur *Windows* n'est pas enregistré en tant que *DBO* dans le 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 le lien *Produit* ne sera pas affiché.

3. Cliquez sur le nom de 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, l'écran suivant s'affiche.



4. Répondez à la question **Possédez-vous une sauvegarde de votre base de données ?** par oui ou non.
5. Activez l'option **Sélectionner les données à importer** si les données de la base ne sont pas à jour.
6. Cliquez sur le lien **Valider toutes les étapes**.

## Utilisateurs d'un groupe de travail

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

**Sage XRT Common Services** propose un assistant permettant de gérer les utilisateurs au sein des groupes de travail.

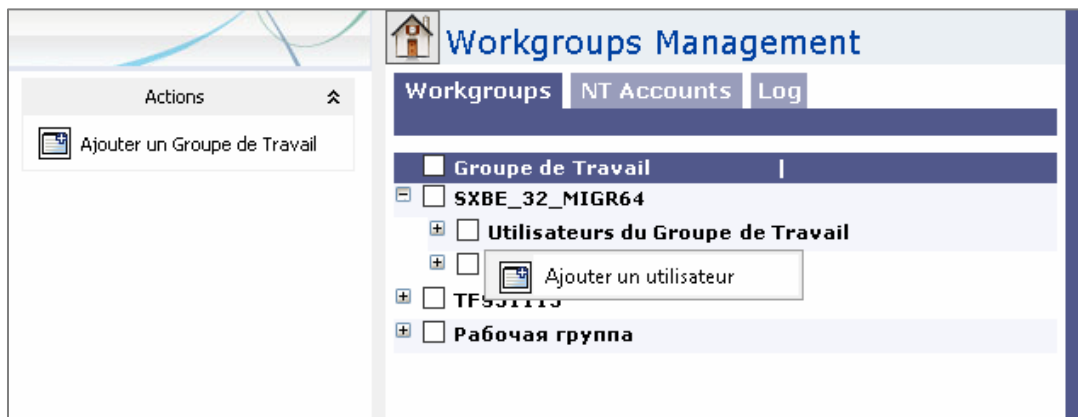
Cet assistant regroupe les actions suivantes :

- **Ajouter 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*.

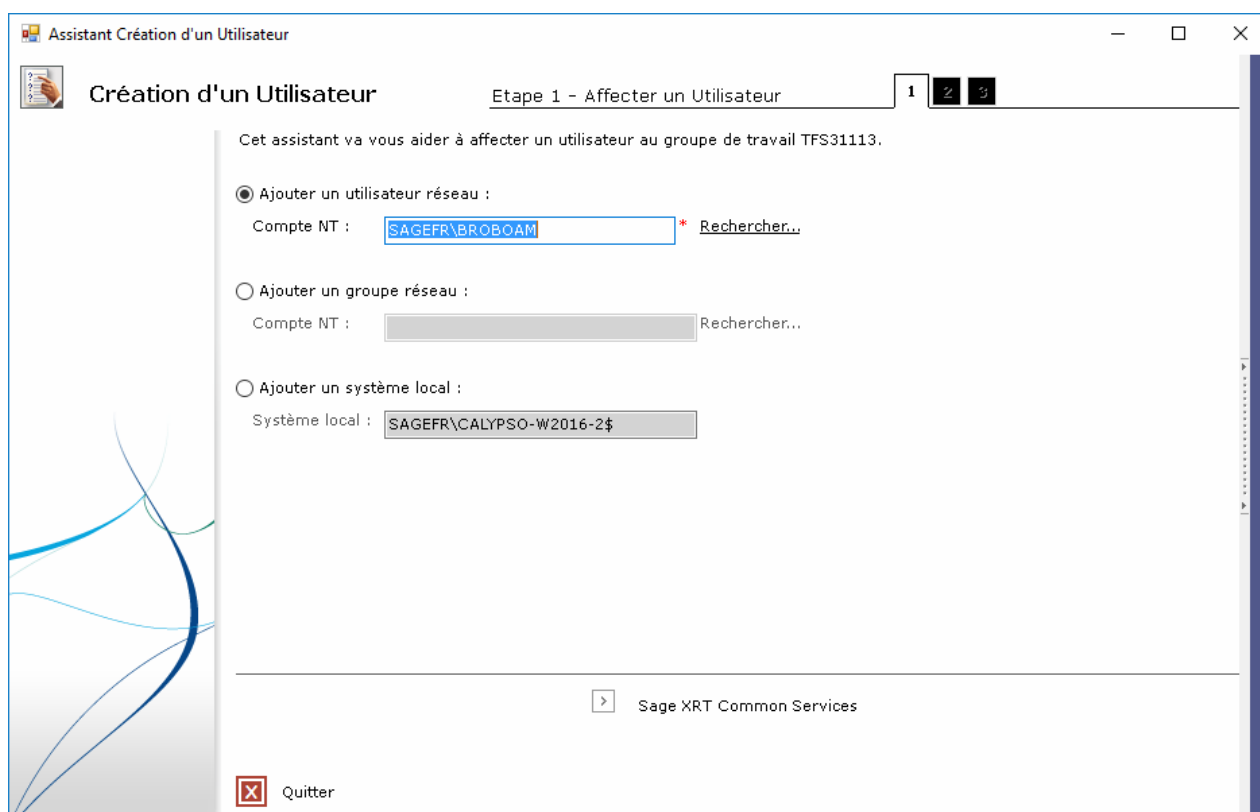
- **Ajouter un groupe réseau** : cette option vous permet d'associer un groupe d'utilisateurs *Windows NT* à un groupe de travail. Pour réaliser cette association, cliquez sur **Rechercher...**. L'outil *Microsoft* de recherche d'un groupe *Windows NT* vous permet de retrouver le groupe d'utilisateur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

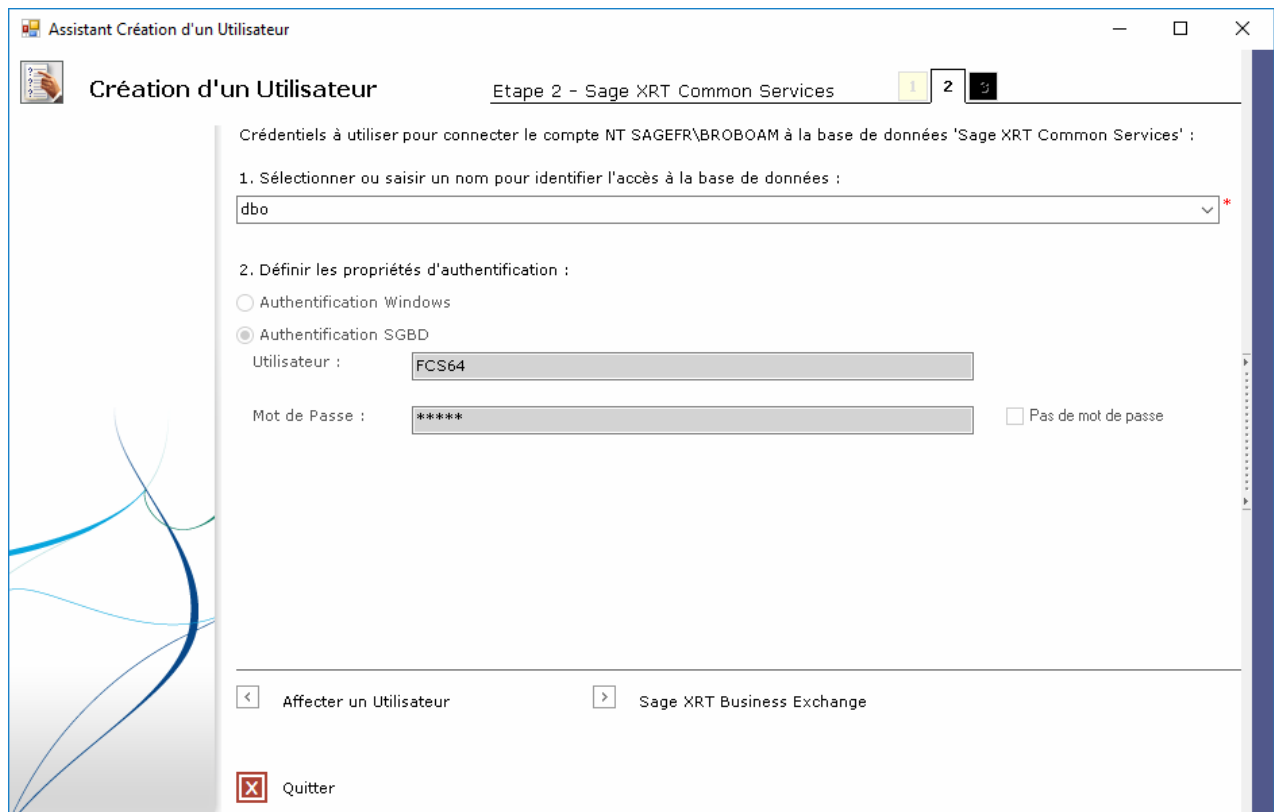
1. Pour assigner un utilisateur au groupe de travail, développez l'élément **Groupe de travail**.
2. Sélectionnez un groupe de travail dans la liste, et effectuez un clic droit sur le niveau **Utilisateurs**.



3. Sélectionnez l'opération **Ajouter un utilisateur** pour lancer l'assistant **Création d'un utilisateur**.



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



5. 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 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.

**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 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 *Sage XRT Treasury*, avec un compte *SQL Server* spécifique intitulé *TRESO*.

7. Cliquez sur **Valider toutes les étapes.**



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

## XDLO

*XDLO* est une architecture orientée services (*SOA* pour *service oriented architecture*) 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 Groupe de travail
- Un utilisateur peut facilement changer de Groupe de travail, 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 connexion 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 **Sage XRT Common Services**).
- 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 modifié si nécessaire. Ce fichier peut être installé sur un répertoire partagé dans le cas d'un déploiement en *clusters*.

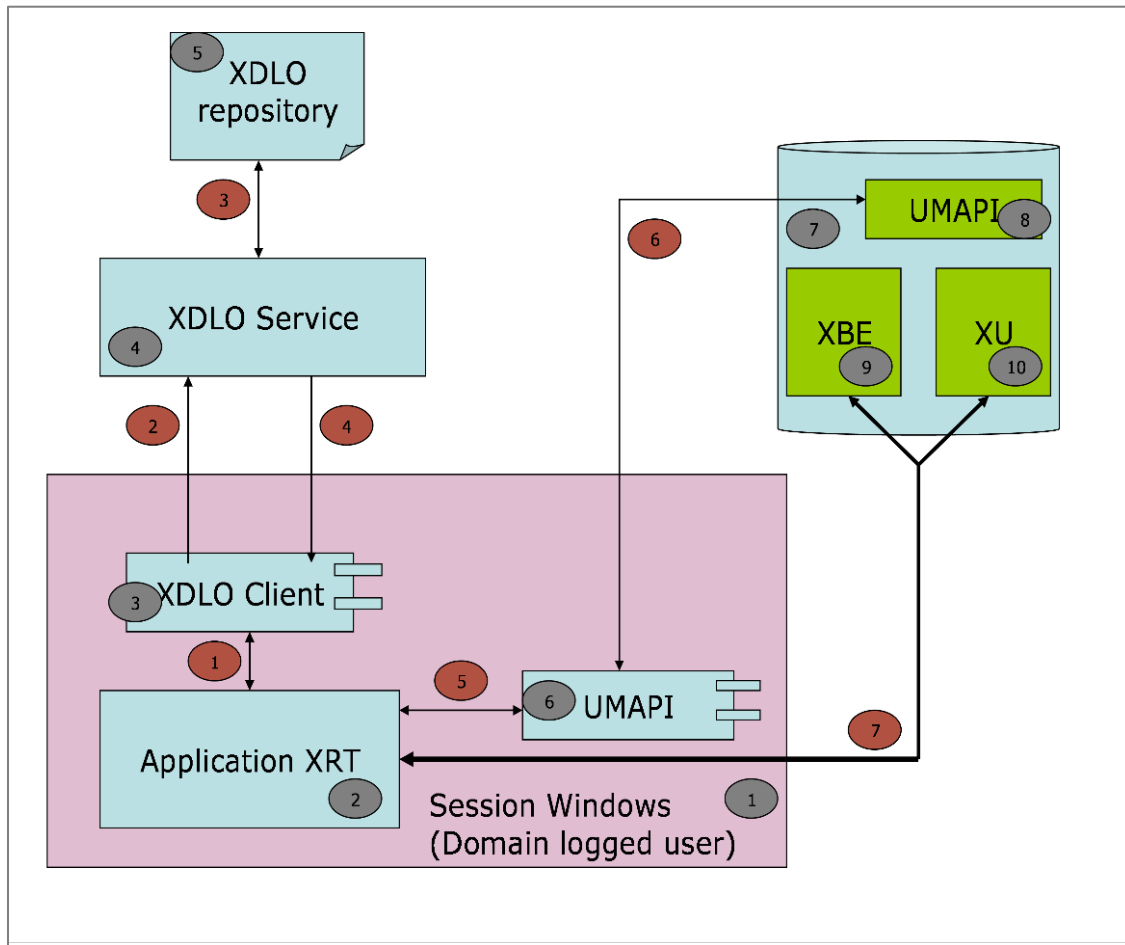
Le fichier *XML* est protégé par l'algorithme de chiffrement *3DES* et ne peut être modifié directement par les utilisateurs.

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 : 
- les interactions entre ces composants : 

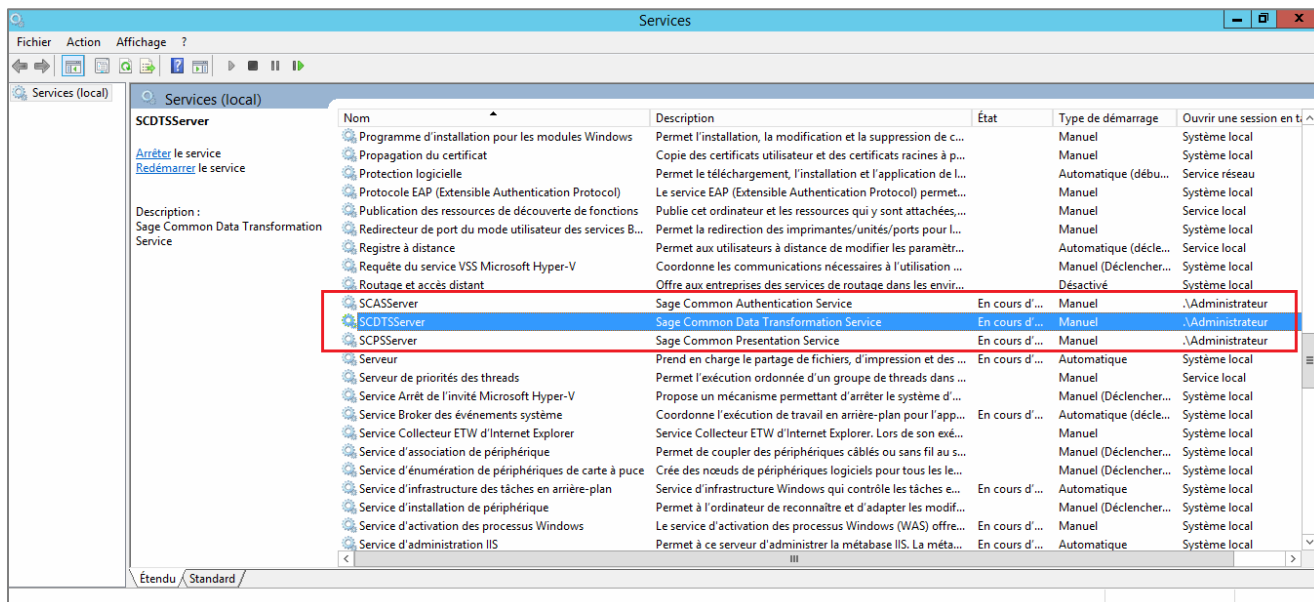


Composant	Description
1	Session <i>Windows</i> d'un utilisateur du domaine <i>NT</i> . Cette session est ouverte et la connexion à l'application <b>XRT</b> est effectuée avec le compte <i>NT</i> de l'utilisateur connecté.
2	L'utilisateur <i>NT</i> exécute une application <b>XRT</b> ( <b>SXT</b> , <b>SXBE</b> , etc.).
3	L'application utilise le composant client <i>XDLO</i> installé par le setup de <b>Sage XRT Common Services</b> pour obtenir la chaîne de connexion à la base de données.
4	Le composant client <i>XDLO</i> se connecte au service <i>XDLO</i> qui s'exécute sur le poste d'administration. La communication entre le client et le service est effectuée via <i>DCOM</i> .
5	Le fichier <i>XDLO</i> contient la définition des groupes de travail et les chaînes de connexion associées. Le service <i>XDLO</i> recherche les informations dans le fichier <i>XDLO</i> .
6	Si l'application obtient une chaîne de connexion, elle démarre le composant <i>UMAPI</i> pour vérifier que l'utilisateur est habilité à utiliser le logiciel et pour obtenir ses permissions d'accès au produit.
7	L'application se connecte à la base de données <i>SQL server</i> ou <i>Oracle</i> avec une chaîne de connexion obtenue via <i>XDLO</i> .
8	La base de données contient les droits <i>UMAPI</i> des applications <b>XRT</b> .
9	La base de données peut contenir les tables <b>SXBE</b> et les données de <b>SXBE</b> .
10	La base de données peut contenir les tables <b>SXT</b> et les données de <b>SXT</b> .

Interaction	Description
1	L'application <b>XRT</b> exécute le client <i>XDLO</i> avec les crédeniels <i>NT</i> de l'utilisateur connecté.
2	Le client <i>XDLO</i> se connecte au service sur le port <i>TCP/IP</i> et initie une communication via <i>DCOM</i> .
3	Le service <i>XDLO</i> interroge le référentiel <i>XDLO</i> pour retrouver les groupes de travail configurés pour l'utilisateur <i>NT</i> connecté.
4	Le service <i>XDLO</i> retourne l'information au client <i>XDLO</i> . 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 <i>UMAPI</i> pour obtenir les droits de l'utilisateur sur l'application.
6	Le composant <i>UMAPI</i> interroge les tables <i>UMAPI</i> 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 trois 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, etc.), **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 processus.



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

Le lien vers le fichier JSON est inscrit dans le fichier *\*.config* de chaque service dans le répertoire **C:\Program Files\Common Files\lxt**.

## Service d'authentification (SCAS)

Fichier de configuration **Sage.SCASServer.Service.exe.config**

[...]  
<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" />  
<!--

Définition de l'emplacement du site web, des ports d'écoute et des hosts de service

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

URL de document et  
URL d'exportation  
Désactivable

## Service de présentation (SCPS)

Fichier de configuration **Sage.SCPSServer.Service.exe.config**

[...]  
<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="syncprofilesitereuser" value="XRT"/>  
<add key="syncprofilesiterefrequency" value="3600"/>  
<!--

Définition de l'emplacement du site web, des ports d'écoute et des hosts de service

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

URL de document et  
URL d'exportation  
Désactivable

## Service de transformation (SCDTS)

Fichier de configuration **Sage.SCDTSServer.Service.exe.config**

