Sage XRT Business Exchange

Préconisations Techniques

Version 2024 R1 (16.0.0)

Sage

Sommaire

Environnements **3**

Matrice de compatibilité 3

Ouverture de flux 6

Annexes **7**

View & Sign 7

Virtualisation 7

Installation avec Office 7

SAML V2 8

Mise en place d'un pare-feu logiciel 8

IIS 8

Gestion Unicode base de données 9

Gestion Unicode sous Windows 9

Gestion de la double authentification 10

Java 10

OpenJDK – Azul Zulu 10

Licence Oracle Java 10

Activation du chiffrement de la base de données 11

Microsoft SQL Server 11

Oracle 12

Abandon de l'événement "Unload" sur Chromium 14

Environnements

Matrice de compatibilité

Environnement	Type de prérequis	Prérequis
Logiciels Sage	Ce prérequis concerne les versions suivantes	**Sage XRT Business Exchange** 16.0.0 **Sage XRT Common Services** 6.2.0 **Sage XRT Bank Format Library** 6.2.0 **Sage View & Sign** 3.2.2 **Sage EIDSign** 4.0.0.163
	Numéro de Build	16.0.0.2640
	Langues disponibles	Français – Anglais – Espagnol
Poste Client	Système d'exploitation	Windows 10 64 bits Windows 11 64 bits
	Dimensionnement minimum	Processeur : Bi-pro/Dual Core 2Ghz Mémoire : 8 Go RAM - Espace disque : 2 Go
	Produits tiers nécessaires	Microsoft .NET Framework 4.8 minimum Client SGBD (cf. chapitre *Connectivité Bases de données*) **Provider obligatoire : MSOLEDBSQL** Microsoft.IIS.PowerShell
	Produits tiers optionnels	JRE 8 Update 202 (64 bits). Cf *Licence Oracle Java* ou Azul Zulu 18.30 et supérieures Nécessaire si le poste réalise des traitements sur des fichiers de format XML (édition, conversion, génération)
	Navigateurs validés Microsoft OS	Microsoft Windows 10 et 11 : • Edge 100 et supérieur • Chrome 100 et supérieur • Firefox 100 et supérieur
	Navigateurs validés MAC OS	mac OS Big Sur, Monterey : • Safari • Chrome 100 et supérieur • Firefox 100 et supérieur

Environnement	Type de prérequis	Prérequis
Serveur d'application et de publication	Systèmes d'exploitation	Windows Server 2019 Windows Server 2022 Windows 10 64 bits Windows 11 64 bits
	Composants tiers nécessaires	Microsoft .NET Framework 4.8 minimum Internet Information Service : IIS 10. (Élément <ServerSideInclude> cf. Annexes IIS) JRE 8 Update 202 (64 bits). Cf Licence Oracle Java ou Azul Zulu 18.30 et supérieures
	Composants tiers optionnels	ElasticSearch/Kibana 7.12 minimum
	Dimensionnement minimum	Processeur : 4 vCPU - 2Ghz ou équivalent Mémoire : 8 Go RAM Espace disque : 3 Go (Programmes)
Serveur de base de données	Systèmes d'exploitation	Windows Server 2019 Windows Server 2022
	Dimensionnement minimum	Processeur : 4 vCPU - 2Ghz ou équivalent Mémoire : 8 Go RAM
	Bases de données Microsoft compatibles	SQL Server 2019 SQL Server 2022
	Connectivité Bases de données Microsoft 64 bits	Composants MS-SQL minimum SQL Server 2019 : • Client Connectivity Tools • Complete Management Tools **Provider obligatoire : MSOLEDBSQL**
	Bases de données Oracle compatibles	Oracle 18c Oracle 19c
	Connectivité Oracle 64 bits	Client Oracle (x64) 18.3 pour 18c Client Oracle (x64) 19.3 pour 19c Composants Oracle à installer : • SQL*Plus • Oracle Net • Oracle Connection Manager • Oracle ODBC drivers • Oracle Provider for OLE DB

Environnement	Type de prérequis	Prérequis
Outil de Virtualisation et publication (cf. chapitre *Annexes*)	Remote Desktop Services	Windows Server 2019 et 2022
	XenApp	V6 et supérieur
	vSphere	V5 et supérieur
	Hyper-V	Windows Server 2019 et 2022
Sage View & Sign (smartphone & tablette) (cf. chapitre *Annexes*)	Systèmes d'exploitation	Apple : iOS 12.2 minimum Android : Android 5.1 minimum
	Terminaux validés	Apple : • iPhone 10 • iPhone 11 • iPhone 12

Ouverture de flux

Source vers cible	N° Port	Modifiable	Détail du flux
Client riche vers Base de données	1434 (Oracle)	Oui	La configuration peut être adaptée pour n'avoir qu'un port ouvert, avec une autre valeur que celle par défaut.
	1521 (SQL)		
Client riche vers Serveur de fichiers (fichiers SXBE)	SMB	Non	Exports/imports de données, fichiers au format bancaire à éditer, logs applicatifs Peut contenir les ports suivants : 137, 138, 139 et 445 Peut être utilisé pour les accès aux fichiers distants
Client riche vers Serveur de fichiers (fichiers SXBE)	DFS	Non	Exports/imports de données, fichiers bancaires, fichiers comptables, partages distants Ports pour contrôleur de domaine : 135, 137, 138, 139, 389 et 445 Ports pour autre serveur : 135, 137, 138, 139 et 445
Client riche vers Serveur de fichiers (fichiers tiers)	SMB	Non	Uniquement si des fichiers sont à échanger avec des partages distants Exports/imports de données, fichiers au format bancaire à éditer, logs applicatifs
Client riche vers Active Directory	MS	Non	Authentification des utilisateurs (utilisation de bibliothèques de classes du namespace System.DirectoryServices pour le framework .NET)
Client riche vers Serveur LDAP	389	Oui	En cas d'authentification LDAP uniquement. Ports par défaut, modifiables en absolu
	636	Oui	
Client riche vers Serveurs SXBE (base de registre)	139	Non	Accès aux paramètres du module Administration Système
Client riche vers Serveurs SXBE (Services Windows)	135	Non	Accès aux Services Windows (RPC)
Client riche vers Serveur SCS	80/443	Oui	Requêtes http/https API rest
Serveurs SXBE vers instances ElasticSearch	9243	Oui	Requêtes http/https API rest

Annexes

View & Sign

Pour un fonctionnement avec https (TLS), le serveur web doit utiliser un certificat émis par une autorité de confiance reconnue par le dispositif.

Les certificats autosignés ne sont pas acceptés par les systèmes d'exploitation **Android** et **iOS**.

Virtualisation

Important ! La virtualisation peut avoir un impact significatif sur les temps de traitement des progiciels.

Certaines fonctionnalités liées à l'administration des communications bancaires ne peuvent s'exécuter que sur un serveur d'application.

Avant tout déploiement, il est possible de faire valider l'architecture et le dimensionnement de votre configuration par nos consultants **Sage**.

Les pilotes des *tokens* **EBICS TS** doivent être disponibles en cas de signature électronique pour les envois de fichiers bancaires.

Installation avec Office

Dans le cas d'une installation avec **Office**, il faut tenir compte des versions utilisées pour les pilotes **ACE ODBC**.

Lors de l'installation, la **DSN CERG_TXT** 64 bits est positionnée avec le pilote v°16 **ACE ODBC**.

Après l'installation d'**Office x64**, vérifiez qu'il s'agit bien de cette version du pilote.

Clé de registre :

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\16.0\Access Connectivity Engine\Engines\Text

Format -> Delimited(;)

Le démarrage de **SCDTS** repositionne cette clé sur la bonne valeur.

SAML V2

Les *ID providers* validés sont : **Microsoft ADFS**, **SSO Circle**, **Azure Active Directory**, **Okta**.

Le schéma *SAML* supporté est *IdP-Initiated SSO*. L'URL utilisateur (fournie par l'Idp) doit être accessible.

Par exemple, pour *ADFS*, l'URL est : **https://your_ip/adfs/ls/IDpInitiatedSignOn.aspx**

Mise en place d'un pare-feu logiciel

Depuis plusieurs versions, des mesures de protection ont été prises pour parer les attaques de type *XSS*, *SQL Injection* et *CSRF*.

Néanmoins, il est vivement conseillé de mette en place un pare-feu logiciel destiné à minimiser les attaques de ce type.

Sur cette page, vous trouverez une liste de pares-feux applicatifs :
https://www.iis.net/downloads/category/secure

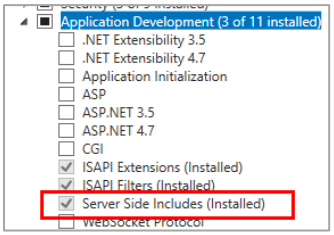
La solution **CloudFlare** ne nécessite aucun déploiement :
https://www.cloudflare.com/fr-fr/lp/waf-a/

IIS

Avec le nouveau tableau de bord, l'élément **<serverSideInclude>** n'est plus requis. Il n'est nécessaire que si vous utilisez l'ancien tableau de bord, et n'est pas installé par défaut. Pour installer ce composant, suivez la procédure **Microsoft** ci-dessous :

WINDOWS SERVER 2016

1. On the taskbar, click Server Manager.
2. In Server Manager, click the Manage menu, and then click Add Roles and Features.
3. In the Add Roles and Features wizard, click Next. Select the installation type and click Next. Select the destination server and click Next.
4. On the Server Roles page, expand Web Server (IIS), expand Web Server, expand Application Development, and then select Server Side Includes. Click Next.



Source : **https://docs.microsoft.com/fr-fr/iis/configuration/system.webserver/serversideinclude**

Gestion Unicode base de données

Les versions de **Sage XRT Business Exchange** 14 ont été testées et validées avec les pages de code *AL32UTF8* et *UTF8* sous **Oracle**, *Latin1_CI_AS*, *Modern_Spanish_CI_AS*, *French CI_AS* sous **SQL Server**.

Important ! Toute modification de jeu de caractères doit être encadrée et réalisée par un *DBA* **Oracle** ou un consultant **Sage**, cette modification ayant un impact sur tous les schémas de la base.

Note : Dans le cas de migrations de **Sage XRT Business Exchange** 11 vers la version 14, en raison de la gestion Unicode, la taille de la base de données augmente de manière significative (elle peut doubler, au maximum).

Gestion Unicode sous Windows

Les traitements applicatifs d'édition reproduisant des caractères Unicode (chinois, etc.) nécessitent la présence de la police *ARIAL UNICODE MS*.

Or, cette police n'est pas installée par défaut sous toutes les versions **Windows** de **Microsoft** et son utilisation est soumise à licence.

Son installation peut être réalisée, par exemple, au cours de l'installation de produits **Microsoft Office** 2010 ou 2013 (32 ou 64 bits) ou via un téléchargement individuel.

Cette police peut aussi être installée manuellement (dès lors que l'on dispose de la licence correspondante).

Important ! **Office** 2016 et **Windows** 10 n'intègrent plus cette police nativement.

Gestion de la double authentification

La mise en œuvre de la double authentification nécessite l'utilisation d'une *app* compatible avec **TOTP** (smartphone ou tablette).

Les *apps* testées sont :

- **FreeOTP** (*Android*)
- **Microsoft Authenticator** (*Windows Phone*)
- **Google Authenticator** (*Android*, *iOS*)

Avec cette version de **Sage XRT Business Exchange** / **Sage XRT Common Services**, la double authentification ne nécessite plus que le serveur **SXBE** / **SCS** accède à internet.

Java

OpenJDK – Azul Zulu

La solution **Azul Zulu** est supportée pour l'utilisation des machines virtuelles **Java** *open source*.

Le support de **OpenJDK** n'est plus assuré. En effet, la machine virtuelle **Java** fournie avec **OpenJDK** est totalement instable. Les traitements peuvent cesser de fonctionner aléatoirement à tout moment.

Licence Oracle Java

Pour rappel, la licence **Oracle Java** a été modifiée pour les versions publiées depuis le 16 avril 2019. Le nouveau contrat de licence *Oracle Technology Network* pour **Oracle Java SE** est sensiblement différent des précédentes licences **Oracle Java**.

La nouvelle licence autorise certaines utilisations à titre gratuit, telles qu'une utilisation personnelle ou pour le développement, mais d'autres utilisations peuvent ne plus être disponibles, bien qu'autorisées avec les précédentes licences **Oracle Java**.

Veuillez lire attentivement les conditions avant de télécharger et d'utiliser ce produit. Une FAQ est disponible sur : **https://www.oracle.com/technetwork/java/javase/overview/oracle-jdk-faqs.html**. Le support et la licence commerciale sont disponibles avec un abonnement à **Java SE**.

Cela signifie que toutes les versions de **JRE** postérieures à la version 8 *Update 202* ne sont plus gratuites et doivent être achetées à **Oracle**. La version 8 *Update 202* est disponible ici : **https://www.oracle.com/es/java/technologies/javase/javase8-archive-downloads.html**

Activation du chiffrement de la base de données

Le chiffrement transparent des données (*TDE*) permet de chiffrer les fichiers de données de la base et de protéger les clés utilisées pour chiffrer les données avec un certificat. Cela empêche toute personne qui ne dispose pas des clés d'utiliser les données.

Ce type de protection nécessite d'être planifié, notamment en raison de son impact sur les performances et sur la gestion des sauvegardes (les sauvegardes sont chiffrées). La clé de chiffrement doit être conservée pour d'éventuelles opérations. La perte de cette clé entraine l'impossibilité d'utiliser la base de données correspondante.

Note : Les tests ont été réalisés sur **Microsoft SQL Server 2016 TDE** et **Oracle 12c TDE**.

Il est à noter que seules les versions *Enterprise* de **SQL Server** disposent du *TDE*.

Il est également possible de chiffrer le canal de communication entre le client et le serveur de bases de données. Cela fonctionne de manière transparente pour les applications.

https://docs.microsoft.com/fr-fr/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine

https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-network-data-encryption-and-integrity.html

Microsoft SQL Server

Exemple de mise en place de **TDE** sur **Microsoft SQL Server**

```
// on se place sur MASTER

USE master;

GO


// on créé un passphrase

CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'MyPassword saisi dans SCS';

GO


// on crée un certificat servant à chiffrer la clé de chiffrement symétrique

CREATE CERTIFICATE MyTDECert WITH SUBJECT = 'MyTDECert Certificate';

GO
```

```
// on se place sur notre base SBE

USE SBE;

GO



// on créé la clé de chiffrement de la base (par exemple en AES 128) et on chiffre cette clé avec le certificat créé dans MASTER

CREATE DATABASE ENCRYPTION KEY WITH ALGORITHM = AES_128  ENCRYPTION BY SERVER CERTIFICATE
MyTDECert;

GO



// on active le chiffrement

ALTER DATABASE TDE SET ENCRYPTION ON;

GO
```

Plus d'informations sur **https://docs.microsoft.com/fr-fr/sql/relational-databases/security/encryption/transparent-data-encryption**

Oracle

Exemple de mise en place de **TDE** sur **Oracle**

```
orapki wallet create -wallet "C:\app\your_user\admin\your_service\wallet" -auto_login -pwd "P@ssword"



ALTER SYSTEM SET ENCRYPTION KEY IDENTIFIED BY "MyPassword saisi dans SCS";

/



CREATE TABLESPACE ENC_XRT_DATA DATAFILE 'C:\app\your_user\oradata\your_service\ENC_XRT_DATA.dbf' SIZE 150 M
AUTOEXTEND ON NEXT 100

ENCRYPTION using 'AES192'

DEFAULT STORAGE(ENCRYPT);

/



CREATE TABLESPACE ENC_XRT_INDEX DATAFILE 'C:\app\your_user\oradata\your_service\ENC_XRT_INDEX.dbf' SIZE 150
M AUTOEXTEND ON NEXT 100 M

ENCRYPTION using 'AES192'

DEFAULT STORAGE(ENCRYPT);

/



ALTER USER SCS QUOTA UNLIMITED ON ENC_XRT_DATA;

/
```

```
ALTER USER SCS QUOTA UNLIMITED ON ENC_XRT_INDEX;

/


DECLARE

   strStatement varchar2(512);

   recCount INTEGER:=-1;

   CURSOR code_objects IS select object_name,object_type from all_objects where owner='your_schema' and object_type =
'TABLE' and temporary='N';

   code_object_rec code_objects%rowtype;

BEGIN

  FOR code_object_rec IN code_objects

  LOOP

    strStatement :=  'ALTER TABLE your_schema.' || code_object_rec.object_name || ' MOVE TABLESPACE ENC_XRT_DATA';

    DBMS_OUTPUT.PUT_LINE (strStatement);

    EXECUTE IMMEDIATE strStatement;

  END LOOP;

END;

/


DECLARE

   strStatement varchar2(512);

   recCount INTEGER:=-1;

   CURSOR code_objects IS select object_name,object_type from all_objects where owner='your_schema' and object_type =
'INDEX' and temporary='N';

   code_object_rec code_objects%rowtype;

BEGIN

  FOR code_object_rec IN code_objects

  LOOP

    strStatement :=  'ALTER INDEX your_schema.' || code_object_rec.object_name || ' REBUILD TABLESPACE ENC_XRT_INDEX';

    DBMS_OUTPUT.PUT_LINE (strStatement);

    EXECUTE IMMEDIATE strStatement;

  END LOOP;

END;

/
```

Abandon de l'événement "Unload" sur Chromium

Sur les navigateurs basés sur la technologie **Chromium**, l'événement *Unload* est abandonné de façon progressive. La valeur par défaut est graduellement modifiée, afin que les gestionnaires *Unload* cessent de se déclencher sur les pages, sauf si celles-ci les réactivent explicitement.

L'évènement *Unload* est utilisé à plusieurs endroits sur **Sage XRT Online Banking**. Une désactivation de cet abandon est donc nécessaire sur les navigateurs pour lesquels l'option serait activée par défaut.

Vous pouvez désactiver l'abandon avec l'option **`chrome://flags/#deprecate-unload`** définie sur **`disabled`**.

https://developer.chrome.com/docs/web-platform/deprecating-unload