



# Sage XRT Business Exchange

Versión 12.4

Indicaciones técnicas



# Índice

<b>Entornos .....</b>	<b>3</b>
Tabla de compatibilidad .....	3
Esquema de los flujos .....	6
<b>Anexos .....</b>	<b>7</b>
View & Sign.....	7
Virtualización .....	7
Instalación con Office .....	7
SAML V2 .....	7
Instalación de un cortafuegos de software .....	7
IIS .....	8
Gestión Unicode de base de datos.....	8
Gestión Unicode en Windows .....	9
Gestión de la doble autenticación.....	9
Activación del cifrado de la base de datos .....	9
Microsoft SQL Server .....	10
Oracle .....	11

## Entornos

### Tabla de compatibilidad

Entorno	Tipo de requisito	Requisito
<b>Software Sage</b>	Este requisito se aplica a las siguientes versiones	<b>Sage XRT Business Exchange 12.4</b> <b>Sage XRT Common Services 5.1</b> <b>Sage XRT Bank Format Library 4.6</b> <b>Sage View &amp; Sign 3.1</b> <b>Sage EIDSign 3.0</b>
	Build	12.3.4.1881
	Idiomas disponibles	Español, francés e inglés
<b>Puesto cliente</b>	Sistema operativo	Windows 10 64 bits
	Recursos mínimos	Procesador: Bi-pro/Dual Core 2Ghz Memoria: 8 GB RAM - Espacio en disco: 2 GB
	Productos de terceros necesarios	Microsoft .NET Framework 4.8 como mínimo Cliente SGBD (v. <i>Conectividad de Bases de datos</i> ) Microsoft.IIS.PowerShell
	Productos de terceros opcionales	JRE 8.0.1410 (64 bits) u OpenJDK 13 (v. documento dedicado a la implementación) Necesario si el puesto realiza tratamientos en archivos de formato XML (edición, conversión, generación)
	Navegadores validados en sistemas operativos Microsoft	Microsoft Windows 8 y 10: <ul style="list-style-type: none"> <li>• Edge</li> <li>• Chrome 70 y posterior</li> <li>• Firefox 63 y posterior</li> </ul>
	Navegadores validados en sistemas operativos MAC	MAC OS X Mojave, Catalina: <ul style="list-style-type: none"> <li>• Safari</li> <li>• Chrome 70 y posterior</li> <li>• Firefox 63 y posterior</li> </ul>

Entorno	Tipo de requisito	Requisito
<b>Servidor de aplicaciones y de publicación</b>	Sistemas operativos	Windows Server 2016 Windows Server 2019 Windows 10 64 bits
	Componentes de terceros necesarios	Microsoft .NET Framework 4.8 como mínimo Internet Information Service: IIS 10. Hay que instalar el componente <ServerSideInclude> (v. <i>Anexos IIS</i> ). Entorno de ejecución Java: JRE 8.0.1410 (64 bits) u OpenJDK 13 (v. documento dedicado a la implementación)
	Recursos mínimos	Procesador: 4 vCPU - 2Ghz o equivalente Memoria: 8 GB RAM Espacio en disco: 3 GB (Programas)
<b>Servidor de base de datos</b>	Sistemas operativos	Windows Server 2016 Windows Server 2019
	Recursos mínimos	Procesador: 4 vCPU - 2Ghz o equivalente Memoria: 8 GB RAM
	Bases de datos de Microsoft compatibles	SQL Server 2016 SQL Server 2017 SQL Server 2019
	Conectividad de Bases de datos Microsoft 64 bits	Componentes MS-SQL como mínimo SQL Server 2016: <ul style="list-style-type: none"> <li>Client Connectivity Tools</li> <li>Complete Management Tools</li> </ul>
	Bases de datos de Oracle compatibles	Oracle 12c Oracle 18c  <b>Importante:</b> Hay que señalar que la versión <b>12.1.0.2</b> tiene bastantes regresiones que impiden el correcto funcionamiento de algunas opciones de SXBE 12.0, sobre todo por lo que se refiere a la optimización del puesto de firma.
	Conectividad de Oracle 64 bits	Client Oracle (x64) 12.2.0.1.0 como mínimo para 12c Client Oracle (x64) 18.0 para 18c Componentes Oracle que hay que instalar: <ul style="list-style-type: none"> <li>SQL*Plus</li> <li>Oracle Net</li> <li>Oracle Connection Manager</li> <li>Oracle ODBC drivers</li> <li>Oracle Provider for OLE DB</li> </ul>

## Entornos

Entorno	Tipo de requisito	Requisito
<b>Herramienta de virtualización y publicación</b>  v. <i>Anexos</i>	Remote Desktop Services (Servicios de Escritorio remoto)	Windows Server 2016 y 2019
	XenApp	V6 y posterior
	vSphere	V5 y posterior
	Hyper-V	Windows Server 2016 y 2019
<b>Sage View &amp; Sign</b>  <i>(smartphones y tablets)</i>  v. <i>Anexos</i>	Sistemas operativos	Apple: iOS 12.2 como mínimo Android: Android 5.1 como mínimo
	Terminales validados	Apple: <ul style="list-style-type: none"> <li>• iPhone 6</li> <li>• iPhone 7</li> <li>• iPhone 10</li> </ul>



## Esquema de los flujos

De origen a destino	N.º de puerto	Se puede modificar	Detalle del flujo
De cliente a base de datos	1434 (SQL)	Sí	Para solo tener un puerto abierto, en la configuración se puede reemplazar el valor propuesto por defecto por otro.
	1521 (Oracle)		
Cliente a Servidor de archivos (archivos SXBE)	SMB	No	Exportación/Importación de datos, archivos con el formato bancario que hay que editar, <i>log</i> de aplicaciones. Puede incluir los siguientes puertos: 137, 138, 139 y 445.  Se puede utilizar para el acceso a los archivos remotos.
De cliente a servidor de archivos (archivos SXBE)	DFS	No	Exportación/Importación de datos, archivos bancarios, archivos contables, unidades remotas compartidas.  Puertos para el controlador de dominios: 135, 137, 138, 139, 389 y 445  Puertos para otros servidores: 135, 137, 138, 139 y 445
De cliente a servidor de archivos (archivos de terceros)	SMB	No	Solo si hay que intercambiar archivos con unidades remotas  Exportación/Importación de datos, archivos con el formato bancario que hay que editar, <i>log</i> de aplicaciones.
De cliente a Active Directory	MS	No	Autenticación de usuarios (uso de bibliotecas de clases de base del <i>namespace</i> System.DirectoryServices del Framework.NET).
Cliente a Servidor LDAP	389	Sí	En caso de autenticación LDAP solamente. Puertos predeterminados, modificables en términos absolutos.
	636	Sí	
De cliente a servidores SXBE Base de registro	139	No	Acceso a los parámetros del módulo Administración del sistema.
De cliente a servidores SXBE Servicios Windows	135	No	Acceso a los servicios Windows (RPC).

## Anexos

### View & Sign

Para el funcionamiento con HTTPS (TLS), el servidor web debe usar un certificado emitido por una autoridad de certificación reconocida por el dispositivo.

Los certificados autofirmados no son aceptados por sistemas operativos Android e iOS.

### Virtualización

**Importante:** La virtualización puede repercutir notablemente en los tiempos de tratamiento de los programas.

Algunas funcionalidades asociadas a la administración de las comunicaciones bancarias solo se pueden ejecutar en un servidor de aplicaciones.

Antes de realizar cualquier implementación, debe pedir que los consultores de Sage validen la arquitectura y el dimensionado de su configuración.

Sujeto a la disponibilidad de los *drivers* de los **tokens EBICS TS** en caso de firma electrónica para el envío de archivos bancarios.

### Instalación con Office

Para la instalación con **Office**, hay que tener en cuenta las versiones utilizadas para los drivers ACE ODBC.

Durante la instalación, la cadena **DSN CERG\_TXT** para 64 bits se declara con el driver v<sup>o</sup>14 ACE ODBC.

Después de instalar **Office x64**, compruebe que esa sea la versión del driver.

### SAML V2

Los ID de proveedores validados son los siguientes: *Microsoft ADFS*, *SSO Circle*.

### Instalación de un cortafuegos de software

Ya desde anteriores versiones, se han tomado medidas de seguridad para bloquear los ataques de tipo XSS, SQL Injection y CSRF.

En todo caso, lo ideal es instalar un cortafuegos de software destinado a minimizar ataques de este tipo.

A continuación, encontrará una lista de aplicaciones de cortafuegos:

<https://www.iis.net/downloads/category/secure>

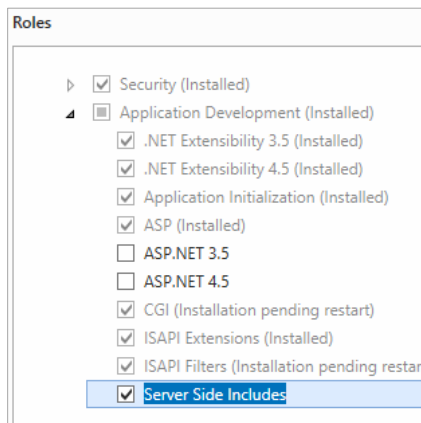
La aplicación **CloudFlare** no requiere ninguna implementación (<https://www.cloudflare.com/es-es/lp/waf-a/>).

### IIS

El componente **<serverSideInclude>** (inclusión del lado del servidor) no se instala por defecto. Para instalarlo, siga los siguientes pasos:

#### WINDOWS SERVER 2016

1. En la barra de tareas, haga clic en **Administrador del servidor (Server Manager)**.
2. A continuación, haga clic en el menú **Administrar (Manage)** y en **Agregar roles y características (Add Roles and Features)**.
3. En el asistente **Agregar roles y características (Add Roles and Features)**, haga clic en **Siguiente (Next)**. Seleccione el tipo de instalación y haga clic en **Siguiente (Next)**. Después, seleccione el servidor de destino y haga clic en **Siguiente (Next)**.
4. En la página **Roles de servidor (Server Roles)**, expanda **Servidor web Web Server (IIS) > Servidor Web (Web Server) y Desarrollo de aplicaciones (Application Development)**, y seleccione **Inclusión del lado servidor (Server Side Includes)**. Por último, haga clic en **Siguiente (Next)**.



Origen: <https://docs.microsoft.com/es-es/iis/configuration/system.webserver/serversideinclude>

## Gestión Unicode de base de datos

La versión 12.0 de **Sage XRT Business Exchange** se ha validado con las páginas de código **AL32UTF8** y **UTF8** en **Oracle**, y **Latin1\_CI\_AS**, **Modern\_Spanish\_CI\_AS** y **French\_CI\_AS** en **SQL Server**.

**Importante:** Cualquier modificación del juego de caracteres la tiene que realizar y supervisar un administrador de base de datos (DBA) de Oracle o un consultor de Sage, ya que dicha modificación repercute en todos los esquemas de la base.

**Nota:** En caso de migración de la versión 11 a la 12 de **Sage XRT Business Exchange**, el tamaño de la base de datos aumente considerablemente por la gestión Unicode (como máximo, se duplica).



### Gestión Unicode en Windows

Los procesos de aplicaciones de edición que reproducen caracteres Unicode (el chino, por ejemplo) requieren que esté instalado el tipo de letra Arial Unicode MS.

No obstante, este tipo de letra no viene instalado por defecto en todas las versiones de **Windows** y para usarlo se requiere una licencia.

Su instalación se puede realizar, por ejemplo, instalando productos Microsoft Office 2010 o 2013 (en 32 o en 64 bits), o descargándose por separado este tipo de letra.

**Importante:** Office 2016 y Windows 10 no incluyen este tipo de letra de forma nativa.

### Gestión de la doble autenticación

Para aplicar la doble autenticación es necesario utilizar una Aplicación compatible con **TOTP** (smartphone o tablet).

Las aplicaciones que se han probado son las siguientes:

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

### Activación del cifrado de la base de datos

El cifrado transparente de datos (**TDE**) se refiere a los archivos de datos de la base, y protege las claves utilizadas para cifrar los datos con un certificado. Ello impide que cualquier persona pueda utilizar los datos si no dispone de las claves necesarias. En todo caso, la activación por este tipo de protección tiene que configurarse por anticipado.

De hecho, repercute en el rendimiento y la gestión de las copias de seguridad (las copias de seguridad, o *backups*, se cifrarán). Hay que guardar de forma segura la clave de cifrado para realizar las operaciones. Si se pierde dicha clave no se podrá utilizar la base de datos correspondiente.

**Nota:** Se han realizado pruebas en **Microsoft SQL Server 2016 TDE** y **Oracle 12c TDE**. Solo las versiones **Enterprise** en **SQL Server** disponen de **TDE**.

### Microsoft SQL Server

#### Ejemplo de aplicación de TDE en Microsoft SQL Server

```
// nos situamos en MASTER
```

```
USE master;
```

```
GO
```

```
// creamos una contraseña (passphrase)
```

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

```
GO
```

```
// creamos un certificado que sirva para cifrar la clave de cifrado simétrica
```

```
CREATE CERTIFICATE MyTDECert WITH SUBJECT = 'MyTDECert Certificate';
```

```
GO
```

```
// nos situamos en nuestra base SBE
```

```
USE SBE;
```

```
GO
```

```
// creamos la clave de cifrado de la base (por ejemplo en AES 128) y se cifra dicha clave con el certificado creado en MASTER
```

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

```
GO
```

```
// activamos el cifrado
```

```
ALTER DATABASE TDE SET ENCRYPTION ON;
```

```
GO
```

Más información en

<https://docs.microsoft.com/es-es/sql/relational-databases/security/encryption/transparent-data-encryption>

### Oracle

Ejemplo de aplicación de **TDE** en **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';
```

## Anexos

```
        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;

/
```