



Sage XRT Business Exchange

Versión 12.4.300

Indicaciones técnicas



Índice

Entornos	4
Tabla de compatibilidad	4
Esquema de flujos	7
Anexos.....	8
View & Sign.....	8
Virtualización.....	8
Instalación con Office.....	8
SAML V2	8
Instalación de un cortafuegos de software	9
IIS.....	9
Gestión Unicode de base de datos.....	10
Gestión Unicode en Windows.....	10
Gestión de la doble autenticación.....	10
JAVA.....	11
OpenJDK – Azul Zulu.....	11
Licencia Oracle Java.....	11

Activación del cifrado de la base de datos	11
Microsoft SQL Server	12
Oracle	13

Entornos

Tabla de compatibilidad

Entorno	Tipo de requisito	Requisito
Software Sage	Este requisito se aplica a las siguientes versiones:	Sage XRT Business Exchange 12.4.300 Sage XRT Common Services 5.3 Sage XRT Bank Format Library 4.8 Sage View & Sign 3.1 Sage EIDSign 3.2
	Build	12.4.300.2162
	Idiomas disponibles	Español, francés e inglés
Puesto cliente	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 8.202 (64 bits) ver <i>Licencia Oracle Java o Azul Zulu 17.28.13</i> y posteriores Necesario si el puesto realiza tratamientos en archivos de formato XML (edición, conversión, generación)
	Navegadores validados en sistemas operativos Microsoft	Microsoft Windows 10 y 11: <ul style="list-style-type: none"> • Edge 89 y posterior • Chrome 89 y posterior • Firefox 86 y posterior
Navegadores validados en sistemas operativos MAC (v. <i>nota sobre Mac OS</i>)	macOS Big Sur, Monterey: <ul style="list-style-type: none"> • Safari • Chrome 89 y posterior • Firefox 86 y posterior 	

Entornos

Entorno	Tipo de requisito	Requisito
Servidor de aplicaciones y de publicación	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>) JRE 8.202 (64 bits) ver Licencia Oracle Java o Azul Zulu 17.28.13 y posteriores
	Componentes de terceros opcionales	ElasticSearch/Kibana 7.12 como mínimo
	Recursos mínimos	Procesador: 4 vCPU - 2Ghz o equivalente Memoria: 8 GB RAM Espacio en disco: 3 GB (Programas)
Servidor de base de datos	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"> Client Connectivity Tools Complete Management Tools
	Bases de datos de Oracle compatibles	Oracle 18c Oracle 19c
	Conectividad de Oracle 64 bits	Client Oracle (x64) 18.3 para 18c Client Oracle (x64) 19.3 para 19c Componentes Oracle que hay que instalar: <ul style="list-style-type: none"> SQL*Plus Oracle Net Oracle Connection Manager Oracle ODBC drivers Oracle Provider for OLE DB

Entornos

Entorno	Tipo de requisito	Requisito
Herramienta de virtualización y publicación (v. «Anexos»)	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
Sage View & Sign (smartphones y tablets) (Ver Anexos)	Sistemas operativos	Apple: iOS 12.2 como mínimo Android: Android 5.1 como mínimo
	Terminales validados	Apple: <ul style="list-style-type: none"> • iPhone 10 • iPhone 11 • iPhone 12

Esquema de 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.
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 (Registro de Windows)	139	No	Acceso a los parámetros del módulo Administración del sistema .
Cliente a Servidor(es) SXBE (Servicios Windows)	135	No	Acceso a los servicios Windows (RPC).
Cliente a Servidor SCS	80/443	Sí	Consultas http/https API rest
Servidores SXBE hacia instancias ElasticSearch	9243	Sí	Consultas http/https API rest

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 sistemas operativos Android y iOS no admiten los certificados autofirmados.

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°16 ACE ODBC.

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

Clave del Registro de Windows:

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

Format -> Delimited(;)

Al iniciar SCDTS, la clave se restablece en su valor correcto.

SAML V2

Los ID de proveedores validados son los siguientes: Microsoft ADFS, SSO Circle, Azure Active Directory.

El esquema SAML admitido es IdP-Initiated SSO. La URL de acceso del usuario (proporcionada por el IdP) debe estar habilitada.

Por ejemplo, para ADFS, la URL es la siguiente:
https://your_ip/adfs/ls/IDpInitiatedSignOn.aspx

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, se muestra una lista de aplicaciones de cortafuegos:

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

La aplicación **Cloudflare** no requiere ninguna implementación:

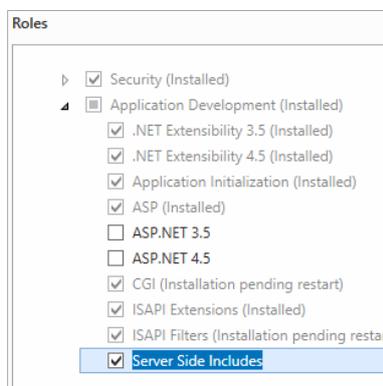
<https://www.cloudflare.com/es-es/lp/waf-a/>

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** y en **Agregar roles y características**.
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)**. A continuación, 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

Las versiones 12 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: Para las migraciones de SXBE V11 a SXBE V12, y debido a la gestión Unicode, el tamaño de la base de datos aumenta considerablemente (como máximo el doble).

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 Microsoft 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.

Dicho tipo de letra también se puede instalar de forma manual (siempre y cuando se cuente con la licencia correspondiente).

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 *app* 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)

A partir de la versión 5.3 de **Sage XRT Common Services**, ya no es necesario tener acceso a internet para generar el código QR.

JAVA

OpenJDK – Azul Zulu

La solución Azul Zulu es compatible con las máquinas virtuales (MV) Java Open Source.

La compatibilidad con OpenJDK no está garantizada. De hecho, la Máquina Virtual de Java con OpenJDK es totalmente inestable. Los procesos pueden dejar de funcionar, aleatoriamente, en cualquier momento.

Licencia Oracle Java

Cabe recordar que la licencia Oracle Java se ha modificado para las versiones publicadas a partir del 16 de abril de 2019. El nuevo contrato de licencia Oracle Technology Network para Oracle Java SE es algo diferente de las licencias Oracle Java. La nueva licencia permite algunos usos de forma gratuita, como, por ejemplo para uso personal o para desarrollos; pero otros, puede que ya no estén disponibles, aunque se permitan con las anteriores licencias Oracle Java. Hay que leer con atención las condiciones de uso antes de descargar y utilizar este programa. Existe un documento de preguntas frecuentes (en inglés) en la siguiente dirección: <https://www.oracle.com/technetwork/java/javase/overview/oracle-jdk-faqs.html>. La suscripción a Java SE da acceso al soporte y a la licencia comercial.

Esto quiere decir que cualquier versión de JRE posterior a la versión 8 Update 202 ya no es gratuita y se debe adquirir a Oracle.

Para acceder a la versión 8 Update 202 de JRE, está disponible el siguiente enlace: <https://www.oracle.com/es/java/technologies/javase/javase8-archive-downloads.html>

Activación del cifrado de la base de datos

El cifrado transparente de los datos (**TDE**) permite cifrar los archivos de datos de la base y proteger 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, 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**.

Hay que señalar que solo las versiones **Enterprise** en **SQL Server** disponen de **TDE**.

También se puede cifrar el canal de comunicación entre el cliente y el servidor de bases de datos. Esto funciona de forma transparente para las aplicaciones.

<https://docs.microsoft.com/es-es/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-ver15>

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

Anexos

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 introducida en SCS';
GO

// creamos un certificado que sirva para cifrar la clave de cifrado simétrico
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>

Anexos

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 introducida en 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
```

Anexos

```
    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;

/
```