



# Sage XRT Common Services

Versión 4.3.100

Manual del usuario



# Índice

<b>Presentación general .....</b>	<b>5</b>
Consola Win32 / Consola Web .....	5
<b>Conexión por primera vez .....</b>	<b>6</b>
<b>Consola Web .....</b>	<b>7</b>
Conexión .....	7
Derechos .....	7
Configuración de la autenticación .....	7
Reglas para las contraseñas .....	13
Activación de datos y regla de los 4 ojos .....	14
Cuenta de usuario .....	17
Perfiles .....	19
Creación .....	20
Modificación .....	22
Eliminación .....	22
Activación .....	22
Sitios .....	23
Creación .....	23

Activación .....	24
Modificación .....	24
Eliminación .....	24
Mi cuenta.....	25
Auditorías y Logs .....	25
Configuración .....	25
Auditoría.....	27
Log .....	28
Correspondencias.....	29
Diseño .....	29
Gestión .....	31
<b>Consola Win32 .....</b>	<b>34</b>
Configuración .....	34
Configuración del puesto de administración .....	34
Configuración de la máquina cliente.....	35
Grupo de trabajo .....	36
Creación de un grupo de trabajo.....	36
Añadir un grupo de trabajo .....	43
Actualización de las bases de datos de un grupo de trabajo .....	44
Usuarios de un grupo de trabajo.....	46
Añadir un usuario a un grupo de trabajo .....	46
<b>XDLO.....</b>	<b>49</b>
Destino de los datos .....	49
Dinámica de los intercambios .....	50
<b>Presentación de los servicios de autenticación, presentación y transformación.....</b>	<b>53</b>
Servicio de autenticación (SCAS) .....	54
Servicio de presentación (SCPS) .....	54
Servicio de transformación (SCDTS) .....	55

La información presentada en este documento puede ser objeto de modificaciones sin notificación previa. A menos que se indique lo contrario, las empresas, los nombres y los datos usados en los ejemplos son ficticios. Queda prohibida la copia, reproducción, traducción a cualquier idioma o transmisión de cualquier parte de este documento de forma alguna ni por ningún medio, ya sea electrónico o mecánico, ni bajo ningún concepto, sin la autorización expresa y por escrito de Sage.

© 2019 Sage. Todos los derechos reservados.

El software presentado en este documento se distribuye en virtud de un acuerdo de licencia y solo puede utilizarse o copiarse conforme a los términos de dicho acuerdo. Lea con atención el contrato que define el acuerdo en cuestión.

**Sage XRT Common Services** es una marca registrada de Sage. Se prohíbe cualquier reproducción o desensamblado de las bases de datos o de los algoritmos incorporados.

Word, Excel, WordPad, Notepad, PowerPoint, Explorer, Edit y Access son marcas registradas de Microsoft y MS, MS-DOS, Windows, Windows 2003, Windows 2007, Windows Me y Windows NT son marcas registradas de Microsoft Corporation en los Estados Unidos y en otros países.

Las demás marcas y nombres de productos mencionados en este documento serán marcas registradas por sus respectivos propietarios y se utilizan aquí con fines editoriales, sin intención de infringir ningún derecho.

# Presentación general

La versión **4.3** de **Sage XRT Common Services** presenta los componentes más utilizados en una interfaz web.

Asimismo, esta versión, y las posteriores, incorporan nuevas funcionalidades:

- Posibilidad de gestionar la activación de datos y la política de los 4 ojos.
- Autenticación SAML v2
- Compatibilidad con Crystal Reports 13.0.23
- Servicios de autenticación y de transformación de datos

## Consola Win32 / Consola Web

Desde la versión 4.3, algunas funciones ya no están disponibles vía la interfaz Win32 pues se utilizan vía la interfaz Web de **Sage XRT Common Services**.

Interfaz Win32	Interfaz Web
Gestión de las licencias	Gestión de los derechos (usuarios, perfiles, etc.)
Gestión de los grupos de trabajo ( <i>workgroups</i> )	Gestión de las conexiones (auditorías, <i>logs</i> , etc.)
Gestión de los formatos	Gestión de las correspondencias

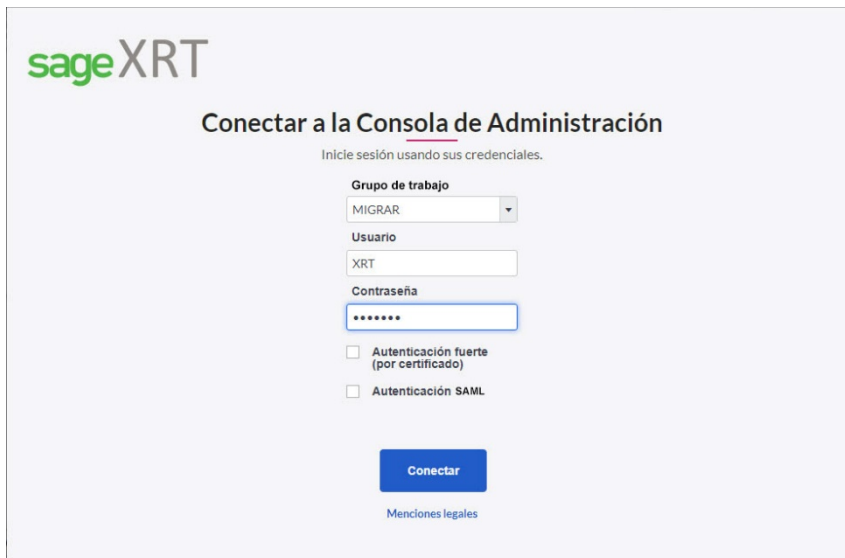
El uso de la interfaz Web vía la URL <http://localhost/SCPS/index.html> exige que se inicien los servicios SCASServer y SCPSServer.

Dicha URL presenta un acceso directo en la interfaz Win32 con el icono  Web .



## Conexión por primera vez

## Conexión por primera vez



The screenshot shows the 'sageXRT' login page. At the top left is the 'sageXRT' logo. The main heading is 'Conectar a la Consola de Administración'. Below it, a subtitle says 'Inicie sesión usando sus credenciales.' The login form includes a 'Grupo de trabajo' dropdown menu with 'MIGRAR' selected, a 'Usuario' text field containing 'XRT', and a 'Contraseña' text field with masked characters. There are two checkboxes: 'Autenticación fuerte (por certificado)' and 'Autenticación SAML', both of which are unchecked. A blue 'Conectar' button is positioned below the password field. At the bottom, there is a link for 'Menciones legales'.

Al conectarse por primera vez, tras crear la base de datos, el usuario puede utilizar:

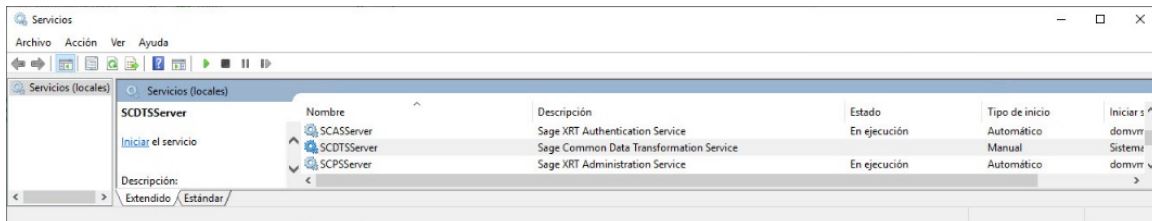
- La cuenta de Windows (AD 'Active Directory') utilizada para instalar el programa.
- El nombre de usuario **XRT** y la contraseña **S3cret#2018** (válida solo por un día).



## Consola Web

### Conexión

La consola Web está disponible vía la URL <http://localhost/SCPS/index.html>. Su uso exige que se inicien los servicios SCASServer y SCPSServer.



### Derechos

En este capítulo se explican los diferentes métodos de autenticación de usuarios que ofrece **Sage XRT Common Services**, así como las acciones que hay que llevar a cabo en relación con la gestión de los usuarios y sus derechos de acceso.

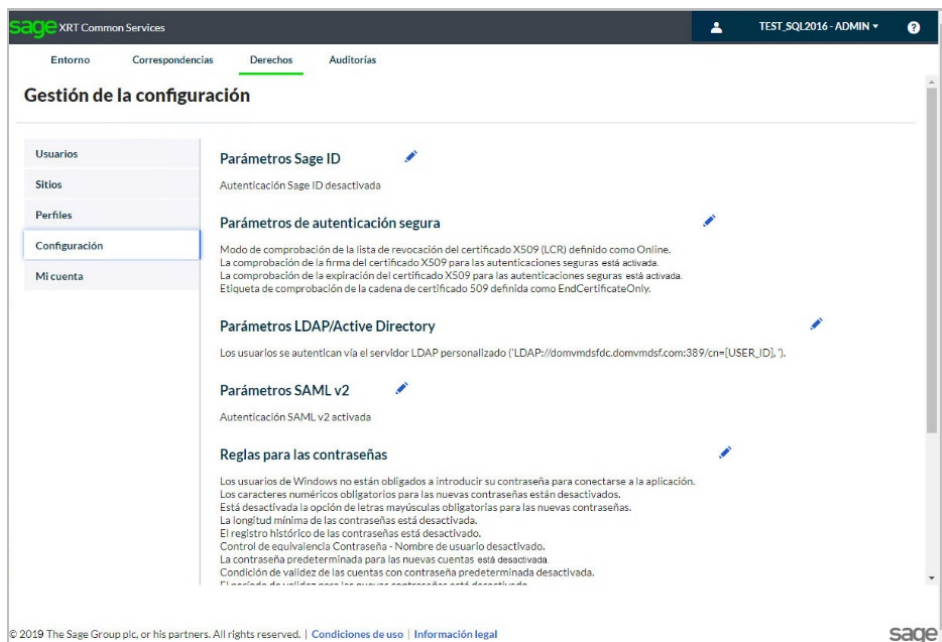
### Configuración de la autenticación

El modelo de *login* UMAPI admite varios métodos de autenticación:

- La autenticación Windows.
- La autenticación UMAPI.
- La autenticación LDAP.
- La autenticación SAML v2.

Antes de asociar estos métodos de autenticación a un usuario, hay que activarlos.

1. Sitúese en el menú **Derechos** y haga clic en **Configuración**.



2. Utilice el icono en forma de bolígrafo para cambiar la configuración de cada método de autenticación.

### Autenticación Windows

La autenticación Windows ofrece las ventajas de la seguridad de Windows (AD) y de su gestión de las cuentas de usuario. Este método de autenticación permite a las aplicaciones **Sage XRT** utilizar las credenciales de los usuarios de Windows (AD).

Las aplicaciones **Sage XRT** ofrecen dos modos de funcionamiento con este tipo de autenticación:

- El modo «*trusted connection*» (conexión de confianza): el usuario no tiene que introducir su contraseña.
- El modo «normal»: el usuario tiene que introducir su contraseña porque el sistema la comprueba vía las API de Windows.

Ventajas del método de autenticación Windows:

- No hay que memorizar credenciales adicionales.
- Si hay un cambio de contraseña, no repercute en UMAPI.
- La gestión de las contraseñas se realiza de acuerdo a las normas de la Ley Sarbanes-Oxley.
- Acceso a otras funcionalidades del sistema, como el cambio periódico de contraseña y la auditoría de los accesos.

**Nota:** El uso de la autenticación Windows exige trabajar en estrecha colaboración con el administrador de Windows durante la creación de los usuarios y de los grupos. La implementación de la autenticación Windows en UMAPI se basa en la biblioteca de clases de bases del *namespace* System.DirectoryServices de Microsoft .NET Framework.



### Autenticación UMAPI

Cuando un usuario se conecta a una aplicación **Sage XRT** y utiliza la autenticación UMAPI, este indicará un nombre de usuario y una contraseña que se comprueban de acuerdo a la información que figura en la base de datos.

Ventajas del método de autenticación UMAPI:

- Gestión de las contraseñas de acuerdo a las normas de la Ley Sarbanes-Oxley.
- Registro de las cuatro últimas contraseñas, las cuales no pueden volverse a utilizar si el sistema solicita un cambio de contraseña (esta funcionalidad se puede configurar).
- Bloqueo de la cuenta de usuario tras tres intentos consecutivos de autenticación fallidos (esta funcionalidad se puede configurar).
- Desbloqueo de la cuenta de usuario bloqueada tras un período de tiempo configurable.
- En la base de datos solo se guardan los códigos *hash* SHA1 de las contraseñas, no las contraseñas.
- La contraseña debe tener un mínimo de seis caracteres e incluir, al menos, una mayúscula y una cifra (esta funcionalidad se puede configurar).
- Cambio periódico de contraseñas (esta funcionalidad se puede configurar).
- Posibilidad para el administrador de bloquear una cuenta de usuario durante un tiempo determinado o de forma permanente.

### Autenticación LDAP

Cuando un usuario se conecta a una aplicación **Sage XRT** y utiliza la autenticación LDAP, este indicará un nombre de usuario y una contraseña que se comprueban de acuerdo a la información que figura en el directorio LDAP.

Ventajas del método de autenticación LDAP:

- Método alternativo para las empresas que no desean utilizar exclusivamente el sistema de autenticación Windows.
- Autenticación de aplicaciones de acuerdo a los productos **Sage XRT**.

La configuración del acceso al directorio se realiza a partir de la pantalla de configuración de la gestión de usuarios. El administrador debe introducir los siguientes parámetros:

- La dirección IP de la máquina que alberga el servidor LDAP.
- El número de puerto para la conexión con el servidor LDAP.
- El parámetro «Base DN» del directorio.
- El atributo ID de usuario (*User ID attribute name*) en el que debe basarse la autenticación del usuario.
- El nombre de la clase «*User*» (Usuario) que hay que utilizar durante la búsqueda de un usuario en el directorio.
- El nombre de la clase «*Group*» (Grupo) que hay que utilizar durante la búsqueda de un grupo de usuarios en el directorio.

- Las credenciales permiten realizar una búsqueda en el directorio (el botón **Probar la conexión** permite comprobar las credenciales en cuestión).

**Parámetros LDAP/Active Directory**

☐ Usario Windows Active Directory solamente

☒ Utilizar también el servidor LDAP personalizado

☐ Utilizar un servidor LDAP secundario

Host\* Puerto ☐ SSL

Host Puerto ☐ SSL

Referencias de conexión

Referencias de conexión

Bind DN Contraseña

Bind DN Contraseña

Probar la conexión

DN Base\*

Atributo ID usuario\* objectClass usuario

objectClass grupo Atributo de miembros del grupo

Probar los parámetros

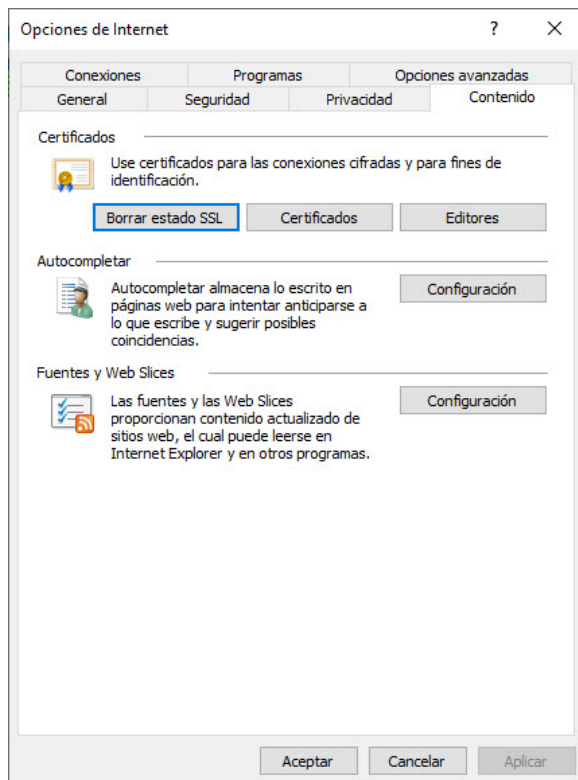
Guardar Cancelar

**Nota:** La implementación en UMAPI de la autenticación LDAP se basa en la biblioteca de clases de bases del *namespace System.DirectoryServices* de Microsoft .NET Framework.

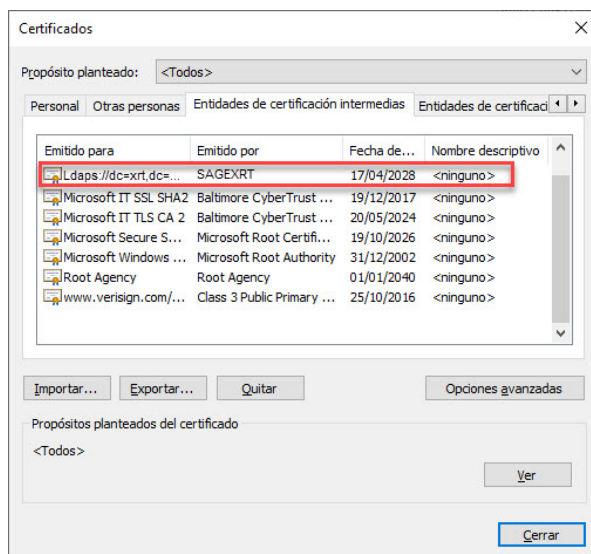
Por regla general, los intercambios LDAP entre los clientes y el servidor transitan por el puerto TCP/IP estándar (puerto 389) de forma cifrada o vía un túnel SSL (puerto 636). La tecnología SSL puede activarse instalando un certificado público de una entidad de certificación aprobada por el controlador de dominio y los clientes de LDAP. La aprobación se establece configurando los clientes y el servidor para aprobar la entidad de certificación raíz a la que está asociada la entidad de certificación emisora.

El certificado instalado se encuentra en el almacén de certificados personal del equipo local, en las opciones de internet del navegador: pestaña **Contenido**, botón **Certificados** y **Entidades de certificación intermedias**.

## Consola Web



Al hacer clic en el botón **Certificados** aparece el siguiente cuadro de diálogo:



## Autenticación SAML v2

SAML (Security Assertion Markup Language) es un protocolo estándar basado en XML para el intercambio de datos de autenticación y autorización.

SAML propone el sistema de inicio de sesión único, o Single Sign-On (SSO), en la web. De esta forma, un usuario puede navegar por diferentes sitios sin tener que autenticarse más de una vez.

En la autenticación SAML participan:

- El proveedor de identidad, o *Identity Provider (IdP)*, que es la entidad que posee las identificaciones: campos **Identity Provider SSO URL** e **Identity Provider Identifiant**).
- Los proveedores de servicios, o *Services Providers (SP)*, que son los servicios que requieren autenticación: campo **Service Provider Identifiant**. Se pueden indicar varios Services Providers (estos conforman el círculo de confianza de los servicios en relación con un IdP).
- El usuario que se identificará vía un dato declarado en los metadatos (por ejemplo: ID o correo electrónico).

### Doble autenticación

La tecnología elegida es la del protocolo TOTP (RFC 6238).

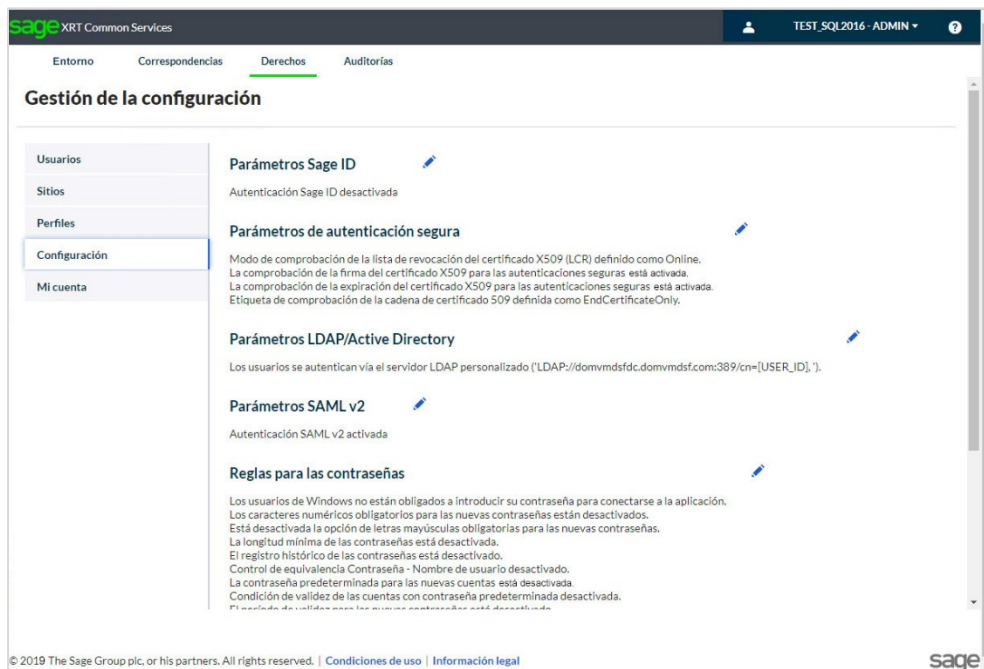
Este protocolo combina una clave secreta con la marca de tiempo (*timestamp*) activa utilizando una función de *hash* criptográfica para generar una contraseña de uso único. Como la latencia de la red y los relojes desincronizados pueden llevar a un intento de autenticación del destinatario de la contraseña, el *timestamp* aumenta por intervalos de 30 segundos, lo que reduce el espacio de búsqueda potencial.

La adopción de este protocolo permite utilizar las aplicaciones móviles que ya están disponibles, como por ejemplo FreeOTP, Microsoft Authenticator o Google Authenticator.

**Nota:** Véase el documento SCS.4.3.DoubleAuthentication.UserGuide\_ES.

## Reglas para las contraseñas

Para crear reglas para las contraseñas, sitúese en el menú **Derechos** y haga clic en **Configuración**.



Utilice el icono en forma de bolígrafo para modificar las reglas de las contraseñas.

Reglas para las contraseñas

☐ Los usuarios de Windows tienen que introducir la contraseña para conectarse a la aplicación

☐ Número obligatorio de caracteres numéricos para las nuevas contraseñas

☐ Número obligatorio de mayúsculas para las nuevas contraseñas

☐ Longitud mínima de la contraseña

☐ La antigua y la nueva contraseña no coinciden

☐ La nueva contraseña y el nombre de usuario no se corresponden

☐ Contraseña predeterminada para las nuevas cuentas

Confirme la contraseña predeterminada para las nuevas cuentas

☐ Bloquear la cuenta si no se cambia la contraseña después

☐ Período de validez de las nuevas contraseñas

☐ Número de intentos de conexión antes del bloqueo de la cuenta

Bloquear la cuenta por un período de

Guardar Cancelar

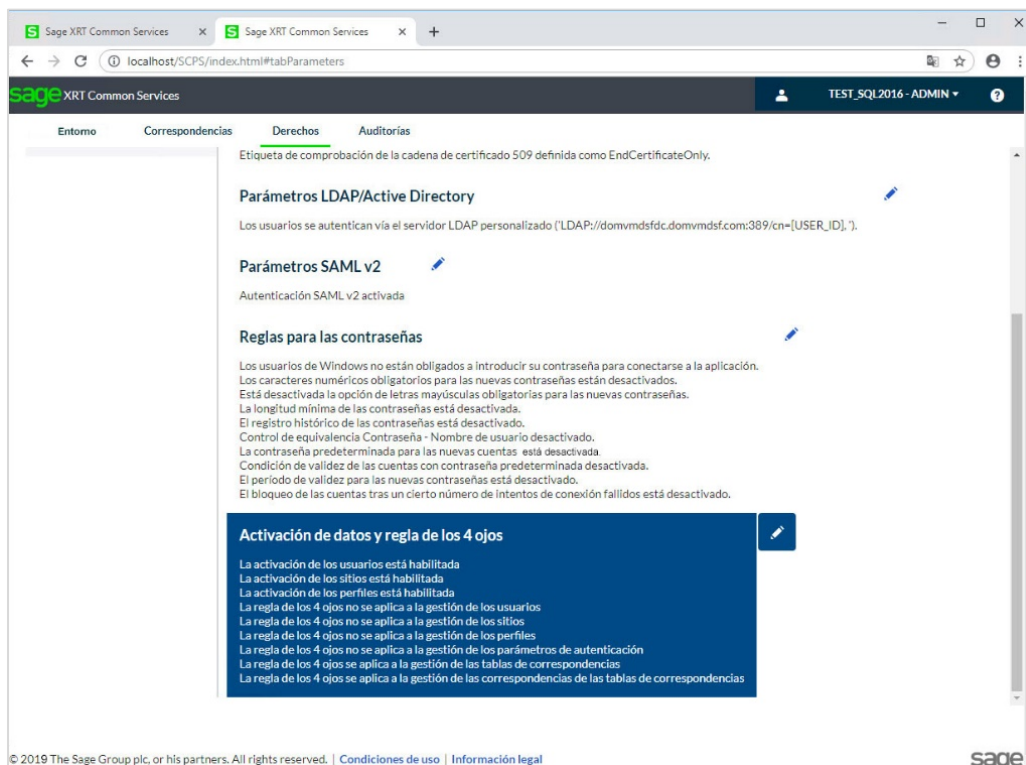
### Activación de datos y regla de los 4 ojos

Nota sobre el principio de activación: un dato con el estado «inactivo» no se puede utilizar. Para poder utilizarlo, se tiene que activar (estado activo).

Nota sobre el principio de la regla de los 4 ojos: un mismo usuario no puede encadenar 2 acciones en un mismo elemento (creación + modificación, creación + eliminación, creación + activación, etc.)

La activación y la aplicación de la regla de los 4 ojos se tienen que solicitar de forma explícita. Por defecto, los datos no deben activarse antes de utilizarlos y la regla de los 4 ojos no se aplica.

Haga clic en Configuración.



Utilice el icono en forma de bolígrafo para modificar la activación de datos y la regla de los 4 ojos.



**Activación de datos y regla de los 4 ojos**

**Activación de datos**

- ☒ Activación necesaria de los usuarios
- ☒ Activación necesaria de los sitios
- ☒ Activación necesaria de los perfiles

No puede desmarcar una activación necesaria de un elemento si todavía hay un elemento inactivo en la lista

**Regla de los 4 ojos**

- ☐ Aplicación en la gestión de los usuarios
- ☐ Aplicación en la gestión de los sitios
- ☐ Aplicación en la gestión de los perfiles
- ☐ Aplicación en la gestión de los parámetros de autenticación
- ☒ Aplicación en la gestión de las tablas de correspondencias
- ☒ Aplicación en la gestión de las correspondencias de las tablas de correspondencias

Guardar Cancelar

Si todavía hay elementos con estado inactivo en la lista, no se podrá desmarcar la activación necesaria para un elemento.

La activación puede solicitarse para:

- Los usuarios
- Los perfiles
- Los sitios

### Perfiles

Si se requiere la activación de perfiles:

- Los perfiles Windows (AD)/LDAP se crean siempre como activos y no se pueden desactivar. Los demás perfiles se crean siempre como inactivos.
- Si un usuario está asociado a un perfil inactivo, no tendrá los derechos asociados al perfil en cuestión.
- Todos los usuarios asociados a un perfil Windows (AD)/LDAP se crean como activos y pueden desactivarse.

Si no se requiere la activación de perfiles:

- Todos los perfiles se crean como activos.

### Sitios

Si se requiere la activación de sitios:

- Los sitios Windows (AD)/LDAP se crean siempre como activos y no se pueden desactivar. Los demás sitios se crean siempre como inactivos.
- Todos los usuarios asociados a un sitio Windows (AD)/LDAP se crean como activos y pueden desactivarse.

Si no se requiere la activación de sitios:

- Todos los sitios se crean como activos.

### Usuarios

Si se requiere la activación de usuarios:

- Todos los usuarios asociados a un perfil Windows (AD)/LDAP se crean como activos y se pueden desactivar.
- Todos los usuarios asociados a un sitio Windows (AD)/LDAP se crean como activos y se pueden desactivar.
- Un usuario «genérico» se crea como inactivo.
- Un usuario no puede autoactivarse.
- Un usuario inactivo no puede conectarse en ningún sitio.

Si no se requiere la activación de usuarios:

- Todos los usuarios se crean como activos.
- La aplicación de la regla de los 4 ojos puede solicitarse en:
  - Los usuarios
  - Los perfiles
  - Los sitios
  - La gestión de los parámetros de autenticación
  - Las tablas de correspondencias
  - La gestión de las tablas de correspondencias

La configuración de la activación de datos y de la aplicación de la regla de los 4 ojos se rige siempre por la regla de los 4 ojos.

### Cuenta de usuario

Una cuenta de usuario permite al usuario en cuestión autenticarse en una aplicación **Sage XRT**. Asimismo, permite gestionar los permisos de acceso de dicho usuario a las funcionalidades de la aplicación.

La cuenta de usuario consta de los siguientes elementos:

- El idioma del usuario (idiomas disponibles: español, alemán, francés, inglés, italiano y portugués).
- El correo electrónico del usuario para las notificaciones.
- Una descripción.
- El tipo de usuario (administrador o usuario común).

### Añadir un usuario

1. En el menú **Derechos**, haga clic en **Usuarios**.

Nombre	Descripción	Tipo	Perfiles	Sitios	Estado
ADMIN		Nivel 1	<Múltiples>	<Múltiples>	activo
ADMIN2	Nada es un usuario de test	Nivel 1	<Múltiples>	<Múltiples>	activo
ADMIN3	Nada	Nivel 1	<Múltiples>	<Múltiples>	activo
ADMINA2333		Estándar	<Múltiples>	<Múltiples>	inactivo
ADMINFR	ADMINFR	Nivel 1	<Múltiples>	<Múltiples>	activo
ADMINUS		Nivel 1	ADMIN	<Múltiples>	activo
ADMIN_INICIAL		Estándar	<Múltiples>	<Múltiples>	activo

2. A continuación, haga clic en el botón **Nuevo usuario**. Aparecerá el siguiente cuadro de diálogo:

**Creación de un usuario**

Autenticación\*

Nombre\*

Nivel de seguridad\*

Idioma\*

Dirección de email

Descripción

☐ Activar el periodo de validez

☐ Doble autenticación

Perfiles

- ☐ ADMIN2
- ☐ ADMTEC
- ☐ APODERADO
- ☐ FIRMANTE

**Guardar** **Cancelar**

3. Seleccione un método de autenticación e introduzca el nombre del usuario:

**Autenticación Windows:** Hay dos formas de añadir un usuario Windows (AD):

- Seleccionándolo en la lista que figura en el cuadro de diálogo. Antes, hay que haber establecido los accesos a la base de datos para cada usuario.
- Buscándolo en el directorio de la empresa. El usuario hereda el acceso a la base de datos de tipo XRTUsers.

**Autenticación LDAP:** Se realiza la búsqueda y selección de los usuarios que pertenecen al directorio creado en la configuración de la autenticación LDAP, al que se accede por el botón **Búsqueda**.

**Autenticación estándar:** Esta autenticación consiste en introducir un identificador único para el usuario.

**Importante:** Es necesario aplicar una gestión de los accesos que se base en las cuentas Windows (AD).

**Autenticación SAML:** Entrada de un identificador SSO obligatorio, proporcionado por el Identity Provider.

### Autenticación Sage ID

Casilla **Doble autenticación:** Esta opción se puede marcar o desmarcar al crear el usuario y también al modificarlo, sea cual sea el tipo de autenticación (estándar, Windows, Sage ID, etc.). Si está marcada, cuando el usuario se conecte por primera vez, tendrá que resetear la autenticación correspondiente introduciendo un código secreto que obtenga al escanear el código QR (o introduciendo el código equivalente) vía una aplicación compatible con el protocolo TOTP 6 dígitos (FreeOTP, por ejemplo). Hasta que no se resetee, la opción aparecerá en naranja. Después, aparecerá en verde.



Si un usuario pierde (o cambia) su *smartphone*, o desinstala la aplicación de autenticación, habrá que restablecer su estado para que pueda volver a crear el enlace.

Para ello, existe la opción **Resetear la doble autenticación** en la lista de usuarios.

4. Seleccione el tipo de usuario que desee crear:
  - **Administrador de seguridad:** gestiona los derechos de acceso de los usuarios del grupo de trabajo.
  - **Usuario estándar:** usuario sin permisos de escritura o modificación.
5. Indique la siguiente información:
  - **Idioma:** En la lista desplegable, seleccione el idioma utilizado por el usuario.
  - **Descripción:** Introduzca una descripción para el usuario.
  - **Dirección de email:** Introduzca el correo electrónico del usuario.
  - **Período de validez:** Marque la casilla para activar los tres campos que permiten definir el período de validez del usuario.
6. Asocie, en su caso, el usuario a un perfil y/o a un sitio ya existente.
7. Haga clic en **Guardar**, o en **Cancelar** si no desea guardar los cambios, para salir del cuadro de diálogo y volver a la lista de usuarios.

### Activar un usuario

Un usuario no puede autoactivarse.

### Usuario expirado

Un usuario recibe el estado «expirado» cuando vence su período de validez.

### Usuario bloqueado

Un usuario recibe el estado «bloqueado» cuando, tras aplicar las reglas para las contraseñas, no consigue conectarse.

## Perfiles

Llegados a este punto, la consola de administración está activada. Ahora puede crear uno o varios perfiles para los usuarios.

Por defecto, un usuario no puede acceder a ninguna funcionalidad del producto. El administrador debe intervenir para definir los derechos de acceso de los usuarios.

Un perfil está constituido por usuarios que comparten los mismos derechos. Los derechos permiten autorizar o denegar el acceso de un usuario a las funciones de un producto.

**Importante:** Un usuario puede pertenecer a varios perfiles.

Un usuario está autorizado a acceder a una función de un producto si se le ha concedido el permiso correspondiente en, como mínimo, uno de los perfiles a los que pertenece.

UMAPI ejecuta una operación de tipo OU en los permisos. Este modo de funcionamiento permite asociar un perfil a un grupo de usuarios que desarrollan las mismas actividades.

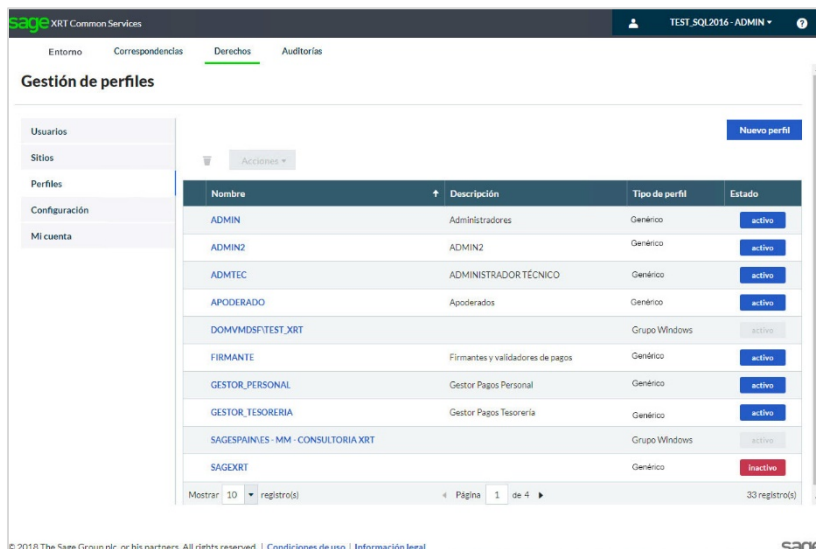
## Consola Web

Un perfil «estándar» queda descrito por las siguientes propiedades:

- Un **código** que identifica el perfil (sin espacios).
- Una descripción.

## Creación

1. Sitúese en el menú **Derechos** y haga clic en **Perfiles**.



2. A continuación, haga clic en el botón **Nuevo perfil**. Aparecerán las siguientes pantallas:

3. Indique la siguiente información:

- **Nombre:** Introduzca un nombre para el perfil. Es obligatorio completar este campo.
- **Descripción:** Introduzca una descripción para el perfil.



### 4. Seleccione el tipo de perfil:

- **Genérico:** Seleccione los usuarios existentes que desee asociar al perfil.
- **Grupo Windows:** Cualquier usuario que pertenezca al grupo se guarda, de forma automática, en la base de datos como usuario de las aplicaciones **Sage XRT**. El perfil de tipo Grupo Windows (AD) se basa en los datos relativos a las cuentas de usuarios de Windows (AD). Seleccione el idioma y el nivel de seguridad predeterminados.
- **Grupo LDAP:** El perfil de tipo Grupo LDAP se basa en los datos relativos a un directorio de empresa. La creación de un grupo LDAP solo es efectiva si se ha configurado el acceso al directorio de empresa. Seleccione el idioma y el nivel de seguridad predeterminados.

Al crear un perfil Windows (AD) o LDAP, cualquier usuario que pertenezca al grupo se guarda, automáticamente, en la base de datos como usuario de las aplicaciones **Sage XRT**.

5. Haga clic en **Crear** para confirmar la creación del perfil, o en **Cancelar** para salir sin guardar los cambios.

## Gestión de los derechos del perfil

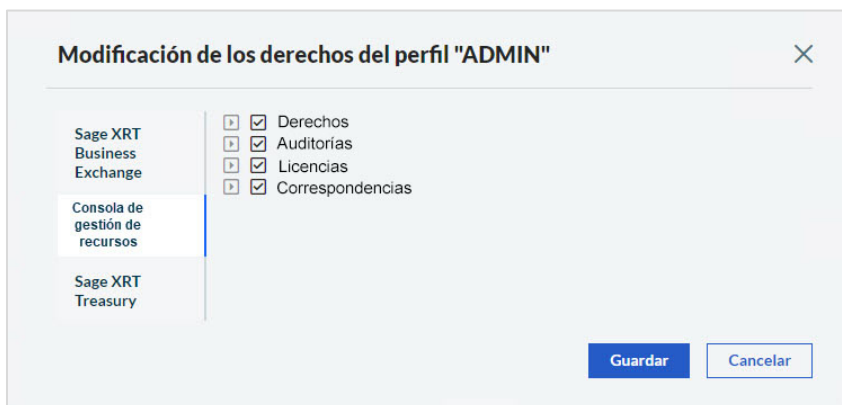
1. En la lista de perfiles, seleccione un perfil y haga clic en **Gestionar los derechos del perfil**.



Nombre	Descripción	Tipo de perfil	Estado
ADMIN	Administradores	General	activo
ADMIN2	ADMIN2	General	activo
ADMTEC	ADMINISTRADOR TÉCNICO	General	activo
APODERADO	Apoderados	General	activo
DOMVMSFTTEST_XRT		Grupo Windows	activo

La página **Modificación de los derechos del perfil** permite gestionar los derechos de acceso de un perfil a los diferentes productos **Sage XRT** instalados en el servidor.

2. Haga clic en la pestaña Consola de gestión de recursos.



**Modificación de los derechos del perfil "ADMIN"**

Sage XRT Business Exchange

Consola de gestión de recursos

Sage XRT Treasury

☒ Derechos

☒ Auditorías

☒ Licencias

☒ Correspondencias

Guardar

Cancelar

## Consola Web

3. Active los derechos que se vayan a conceder.
4. Repita los mismos pasos para los productos **Sage XRT Treasury** (SXT) y **Sage XRT Business Exchange** (SXBE), si desea asignar al perfil derechos de acceso a estos dos productos.
5. Haga clic en **Guardar** para guardar los cambios realizados, o en **Cancelar** para salir sin tenerlos en cuenta.

## Modificación

1. Sitúese en el menú **Derechos** y haga clic en **Perfiles**.

Aparecerá la lista de los perfiles existentes.

2. Para modificar un perfil, utilice el enlace disponible en el nombre del perfil.
3. Realice los cambios que considere oportunos y haga clic en **Guardar**.

## Eliminación

1. Sitúese en el menú **Derechos** y haga clic en **Perfiles**.

Aparecerá la lista de los perfiles existentes.

2. Para eliminar un perfil, marque la casilla que le corresponda y haga clic en el icono en forma de papelera.

## Activación

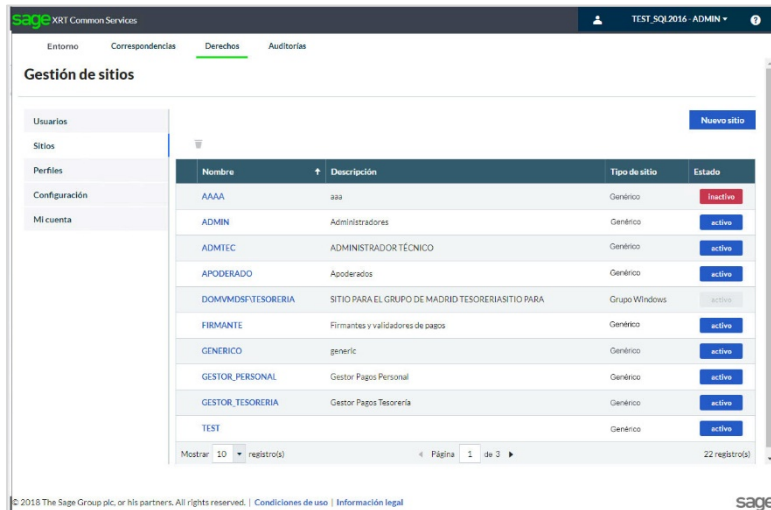
Todo perfil creado recibe el estado «inactivo». El usuario con derechos de administrador tendrá que activarlo.

## Sitios

### Creación

La creación de los sitios sigue las mismas pautas que la de los perfiles.

1. Sitúese en el menú **Derechos** y haga clic en **Sitios**.



2. A continuación, haga clic en **Nuevo sitio**. Aparecerá la siguiente pantalla:

**Creación de un sitio**

**Nombre\***  
Introduzca el nombre de su sitio

**Descripción**  
Introduzca la descripción de su sitio

**Tipo de sitio**

- ☒ Genérico
- ☐ ADMIN\_INICIAL
- ☐ ADMTEC
- ☐ AMDIN\_TEST222
- ☐ APOD1
- ☐ APOD2
- ☐ CASHMNGR
- ☐ DEMO
- ☐ DFIN
- ☐ DIRECTOR TESORERIA

**Crear** **Cancelar**

3. Indique la siguiente información:

- **Nombre:** Introduzca un nombre para el sitio. Es obligatorio completar este campo.
- **Descripción:** Introduzca una descripción para el sitio.

4. Seleccione el tipo de sitio:

- **Genérico:** Seleccione los usuarios que se vayan a asociar al sitio.
- **Grupo Windows:** Cualquier usuario que pertenezca al grupo se guarda, de forma automática, en la base de datos como usuario de las aplicaciones **Sage XRT**. El sitio de tipo **Grupo Windows (AD)** se basa en los datos relativos a las cuentas de usuarios de Windows (AD).
- **Grupo LDAP:** El sitio de tipo **Grupo LDAP** se basa en los datos relativos a un directorio de empresa. La creación de un grupo LDAP solo es efectiva si se ha configurado el acceso al directorio de empresa.

5. Haga clic en **Crear** para confirmar la creación del sitio, o en **Cancelar** para salir sin guardar los cambios.

## Activación

Todo sitio creado recibe el estado «inactivo». El usuario con el nivel de derechos de administrador tendrá que activarlo.

## Modificación

1. En el menú **Derechos**, haga clic en **Sitios**.

Aparecerá la lista de los sitios existentes.

- 2. Para modificar un sitio, utilice el enlace disponible en el nombre del sitio.
- 3. Realice los cambios que considere oportunos y haga clic en **Guardar**.

## Eliminación

1. En el menú **Derechos**, haga clic en **Sitios**.

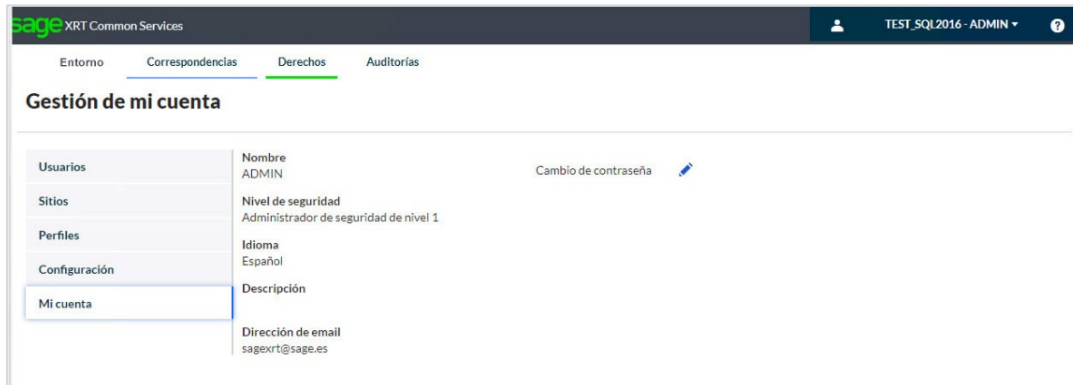
Aparecerá la lista de los sitios existentes.

- 2. Para eliminar un sitio, marque la casilla que le corresponda y haga clic en el icono en forma de papelera.

### Mi cuenta

Esta función está disponible para los usuarios de tipo «estándar». Desde ella, se puede modificar la contraseña del usuario conectado.

En el menú **Derechos**, haga clic en **Mi cuenta**.



Aparecen los datos del usuario: Nombre, Nivel de seguridad, Idioma, Descripción, Dirección de email.

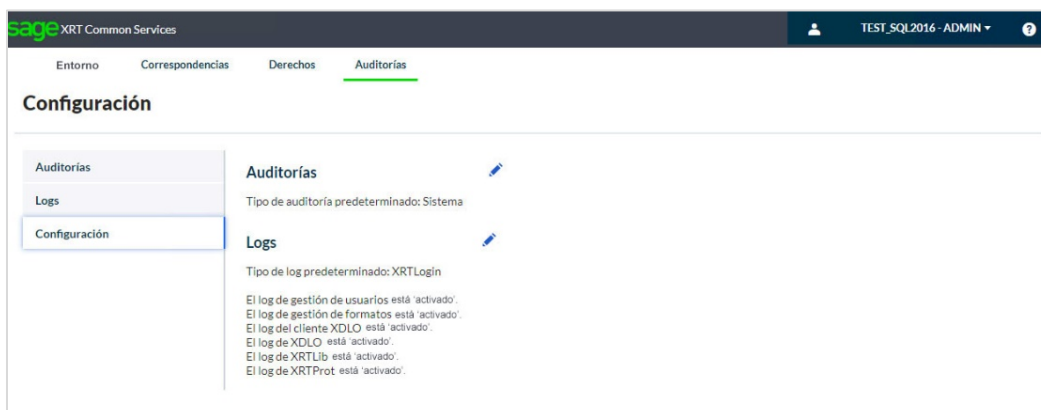
Solo se puede modificar la contraseña, con ayuda del icono en forma de bolígrafo.

### Auditorías y Logs

#### Configuración

Antes de consultar los datos, hay que definir el tipo de auditoría propuesta al usuario, así como la activación de *logs*.

1. En el menú **Derechos**, haga clic en la opción **Configuración**.



La configuración aparece resumida. Se puede modificar haciendo clic en el icono en forma de bolígrafo.

2. Seleccione el tipo de auditoría que se propondrá por defecto al utilizar la función **Auditorías**:
  - Sistema
  - Base de datos
  - Usuarios
3. Seleccione el tipo de *log* propuesto por defecto al utilizar la función **Logs**:
  - Gestión de formatos
  - Gestión de usuarios
  - Gestión de bases de datos
  - Gestión de la consola
  - Cliente XDLO
  - XDLO
  - Servicio XDLO
  - XRTProt
  - XRTPLogin
  - XRTPLib
4. Marque los *logs* que desee activar.
5. Haga clic en **Guardar** para guardar los cambios, o en **Cancelar** para no tenerlos en cuenta y volver a la página de resumen de la configuración.

The screenshot shows a configuration window titled "Parámetros de auditorías y logs". It is divided into two main sections: "Auditorías" and "Logs".

**Auditorías section:**

- "Tipo de auditoría seleccionado por defecto": A dropdown menu with "Sistema" selected.
- "Idioma": A dropdown menu with "Español" selected.

**Logs section:**

- "Tipo de log seleccionado por defecto": A dropdown menu with "XRTPLogin" selected.
- A grid of six checkboxes, all of which are checked:
  - Activar el log de la gestión de usuarios
  - Activar el log de XDLO
  - Activar el log de la gestión de formatos
  - Activar el log de XRTPLib
  - Activar el log del cliente XDLO
  - Activar el log de XRTProt

At the bottom right, there are two buttons: "Guardar" (highlighted in blue) and "Cancelar".



## Auditoría

1. En el menú **Auditorías**, haga clic en **Auditorías**.

Aparecerá el tipo de auditoría seleccionado como predeterminado.

2. Para modificarlo, seleccione una de las opciones de la lista desplegable **Tipo de auditoría**.
3. Para filtrar la información mostrada, seleccione una de las opciones de la lista desplegable **Período**:
  - Hoy
  - Semana actual
  - Mes actual
  - Año actual

Para acceder a otros criterios de selección disponibles, haga clic en el botón **Buscar**. Los criterios de búsqueda aplicados figuran en la parte superior de la lista.

4. Haga clic en el botón **Purgar** para eliminar o exportar eventos de la lista.

## Log

1. En el menú **Auditorías**, haga clic en **Logs**.

Aparece el tipo de *log* seleccionado como predeterminado.

The screenshot shows the 'Gestión de logs' (Log Management) interface in Sage XRI Common Services. The interface includes a sidebar with 'Auditorías', 'Logs', and 'Configuración'. The main area has filters for 'Tipo de log' (set to 'Gestión de formatos') and 'Período' (set to 'Ninguno'). A table displays log entries with columns for 'Fecha y hora', 'Nivel', and 'Mensaje'. The table shows several entries with a 'DEBUG' level and timestamps from 02/04/2019 9:08:38. The bottom of the table shows 'Mostrar: 10' and '656 registros'.

Fecha y hora	Nivel	Mensaje
02/04/2019 9:08:38	DEBUG	CGTTestRunFMTDisconnect
02/04/2019 9:08:38	DEBUG	return S_OK
02/04/2019 9:08:38	DEBUG	CAdoTransactionsRollback
02/04/2019 9:08:38	DEBUG	CAdoTransactions-CAdoTransaction
02/04/2019 9:08:38	DEBUG	Commit Transaction
02/04/2019 9:08:38	DEBUG	FMT_FORMATS table cleanup
02/04/2019 9:08:38	DEBUG	return S_OK
02/04/2019 9:08:38	DEBUG	ID=256539
02/04/2019 9:08:38	DEBUG	execute (INSERT INTO FMT_WORKS (WORK_ID, PROJECT_ID, ORIGIN_ID, NO_ITEMS, ITEM_RANK, EXE_NAME, WORK_TYPE, NAME, PARAM, REPEAT, COMMENTS, TIME_STAMP, VERSION) VALUES (256537, 403, 1, 1, 1, 'CLINTEXE', 17, 'XMLVDDOM03', 'X0MLVDDOM03.dtl - translate SQL', 'X0MLVDDOM', '2019-04-02 09:08:38'))
02/04/2019 9:08:38	DEBUG	ID=256536

2. Para modificarlo, seleccione una de las opciones de la lista desplegable **Tipo de log**.
3. Para filtrar la información mostrada, seleccione una de las opciones de la lista desplegable **Período**:
  - Hoy
  - Semana actual
  - Mes actual
  - Año actual

Para acceder a otros criterios de selección disponibles, haga clic en el botón **Buscar**. Los criterios de búsqueda aplicados figuran en la parte superior de la lista.

# Correspondencias

## Diseño

### Creación


1. En el menú **Correspondencias**, haga clic en **Diseño**.

Aparecerá en pantalla la lista de las tablas entregadas por defecto para garantizar el funcionamiento de los productos **Sage XRT**.

2. Para crear una tabla, haga clic en **Nueva tabla**.

3. Es obligatorio que complete el campo **Nombre**, y, si lo desea, el campo **Descripción**.
4. Para definir las columnas de entrada y de salida de la tabla, haga clic en **Nueva columna**.

## Consola Web



Creación de una nueva columna

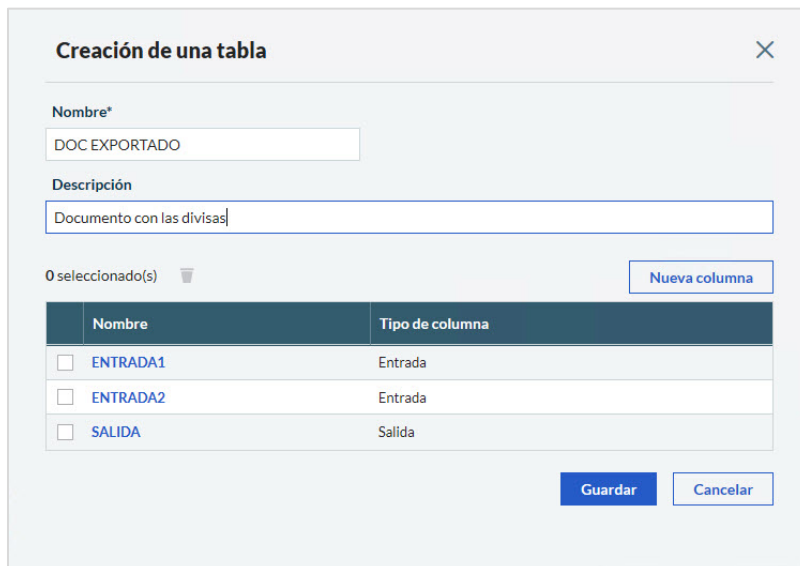
Tipo de columna\*

Nombre\*

Validar Cancelar

5. Es obligatorio que complete el campo **Nombre** y seleccione el tipo de columna (entrada o salida) para cada columna.
6. Haga clic en **Validar** para confirmar la creación de la columna.

La columna creada figurará en la lista de columnas que conforman la tabla. Para modificar una columna, haga clic en el enlace que aparece en su nombre o, si desea eliminarla, marque la casilla correspondiente y haga clic en el icono en forma de papelera.



Creación de una tabla

Nombre\*

DOC EXPORTADO

Descripción

Documento con las divisas

0 seleccionado(s) Nueva columna

	Nombre	Tipo de columna
<input type="checkbox"/>	ENTRADA1	Entrada
<input type="checkbox"/>	ENTRADA2	Entrada
<input type="checkbox"/>	SALIDA	Salida

Guardar Cancelar

7. Haga clic en **Guardar** para guardar los cambios y confirmar la creación de la tabla.

La tabla figurará en la lista de tablas.

## Modificación

1. En el menú **Correspondencias**, haga clic en **Diseño**.

Aparecerá en pantalla la lista de las tablas existentes.

2. Para modificar una tabla, haga clic en el enlace disponible en el nombre de la tabla.
3. Realice los cambios que considere oportunos y haga clic en **Guardar**.

### Eliminación

1. En el menú **Correspondencias**, haga clic en **Diseño**.

Aparecerá en pantalla la lista de las tablas existentes.

2. Para eliminar una tabla, marque la casilla correspondiente y haga clic en el icono en forma de papelera.

### Importación

1. En el menú **Correspondencias**, haga clic en **Diseño**.

Aparecerá en pantalla la lista de las tablas existentes.

2. Para importar tablas de correspondencias, haga clic en el botón **Importar**.

Se abrirá un cuadro de diálogo para que seleccione el archivo que desee importar.

3. Seleccione el archivo en cuestión y haga clic en **Abrir**.

### Exportación

1. En el menú **Correspondencias**, haga clic en **Diseño**.

Aparecerá en pantalla la lista de las tablas existentes.

2. Para exportar una tabla, marque la casilla correspondiente a la tabla que desee exportar y seleccione la opción **Exportar** en la lista desplegable **Acciones**.

### Gestión

Una vez creada la tabla, se deben completar las correspondencias que se vayan a registrar.

### Creación

1. En el menú **Correspondencias**, haga clic en **Gestión**.

La tabla **CCC-Tabla IBAN (RIBs)** aparece seleccionada por defecto en la lista desplegable **Tabla** para mostrar correspondencias.

2. Seleccione en la lista desplegable la tabla para la que se deben crear las correspondencias.

Aparecerá en pantalla la estructura de la tabla.

The screenshot shows the Sage XRT Common Services web interface. The top navigation bar includes 'Entorno', 'Correspondencias', 'Derechos', and 'Auditorías'. The 'Correspondencias' tab is active. The main heading is 'Gestión de las tablas de correspondencias'. On the left, there's a sidebar with 'Diseño' and 'Gestión' tabs. The 'Gestión' tab is selected. The main content area shows a 'Tabla' dropdown menu with 'DOC EXPORTADO' selected. Below the dropdown, it says 'Documento con las divisas'. To the right of this is a button labeled 'Nueva correspondencia'. Below that, it says '0 seleccionados'. A table structure is displayed with three columns: 'ENTRADA1 (E)', 'ENTRADA2 (E)', and 'SALIDA (S)'. The table is currently empty, showing 'Mostrar 10 registro(s)' and 'Página 1 de 1'.

## Consola Web

3. Haga clic en el botón **Nueva correspondencia**.

**Creación de una correspondencia** ✕

**ENTRADA1 (E)\***

**ENTRADA2 (E)\***

**SALIDA (S)**

**Guardar** **Cancelar**

4. Indique, para cada correspondencia, el o los valores de entrada y de salida.
5. Haga clic en **Guardar** para guardar los cambios y confirmar la creación de la correspondencia, que figurará en la lista de correspondencias de la tabla.

Sage XRT Common Services

TEST\_SQL2016 - ADMIN

Entorno **Correspondencias** Derechos Auditorías

**Gestión de las tablas de correspondencias**

**Diseño**  
Gestión

Tabla  
ACSAFB\_TO\_MT

**Nueva correspondencia**

0 seleccionado(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

Mostrar 10 registro(s) ◀ Página 1 de 11 ▶ 103 registro(s)

## Modificación

1. En el menú **Correspondencias**, haga clic en **Gestión**.
2. Seleccione la tabla de trabajo.

Aparecerá en pantalla la lista de correspondencias existentes.

3. Para modificar una correspondencia, utilice el enlace disponible en la primera columna de la tabla.
4. Realice los cambios que considere oportunos y haga clic en **Guardar**.



### Eliminación

1. En el menú Correspondencias, haga clic en Diseño.
2. Seleccione la tabla de trabajo.

Aparecerá en pantalla la lista de correspondencias existentes.

3. Para eliminar una correspondencia, marque la casilla situada al lado de la correspondencia que desee eliminar y haga clic en el icono en forma de papelera.

# Consola Win32

## Configuración

En este capítulo se presenta la descripción del puesto de administración y de la máquina cliente.

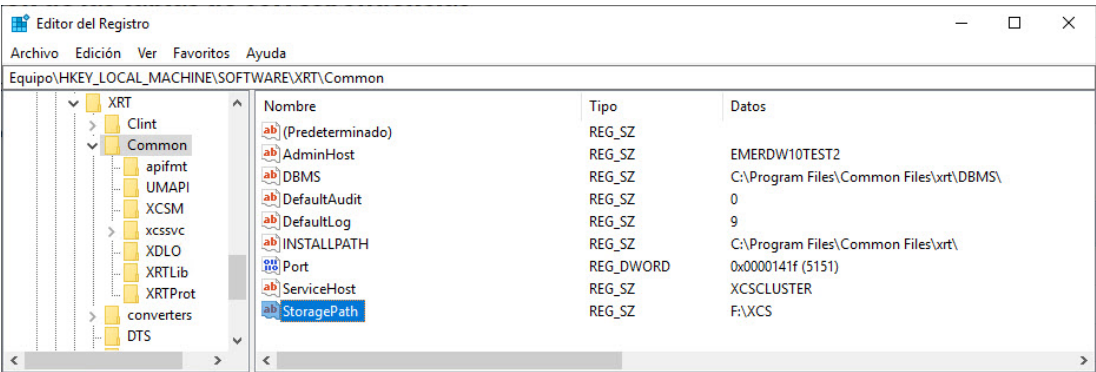
### Configuración del puesto de administración

El puesto de administración se refiere a la máquina en la que se ejecuta el servicio XDLO.

La configuración principal de XDLO para el puesto de administración se define en la clave del Registro de Windows `HKEY_LOCAL_MACHINE\SOFTWARE\XRT\Common`.

En dicha clave figuran los siguientes valores:

Valor	Descripción
Port	Puerto TCP/IP en el que el servicio se encuentra en escucha de las llamadas de clientes. Durante la instalación de <b>Sage XRT Common Services</b> , este parámetro recibe, por defecto, el valor <b>5151</b> .
StoragePath	Indica la ruta de acceso al archivo <code>xdlo_storage.xml</code> . Este parámetro permite cambiar la ruta de acceso del archivo <code>xdlo_storage.xml</code> cuando XDLO se instala en modo clúster. Cada nodo del clúster debe tener un acceso de escritura en el archivo compartido.
ServiceHost	Permite especificar el nombre o la dirección IP de la máquina de administración, o el nombre virtual o la dirección IP virtual asociada al puesto de administración. Si el servicio XDLO se instala en modo clúster, este valor permite especificar el nombre virtual del clúster. Dicho nombre puede asociarse a cualquier nodo del clúster que viene después del nodo activo.



Los parámetros opcionales de XDLO se definen en la clave del Registro de Windows `HKEY_LOCAL_MACHINE\SOFTWARE\XRT\Common\XDLO`.

## Consola Win32

En esta clave figura el siguiente valor:

Valor	Descripción
Debug	El valor <b>Y</b> activa el modo <i>debug</i> para <i>xdlo_service.exe</i> y <i>xdlo_com.dll</i> , los cuales generan los archivos de <i>log</i> <i>xdlo-service.log</i> y <i>xdlo.log</i> .

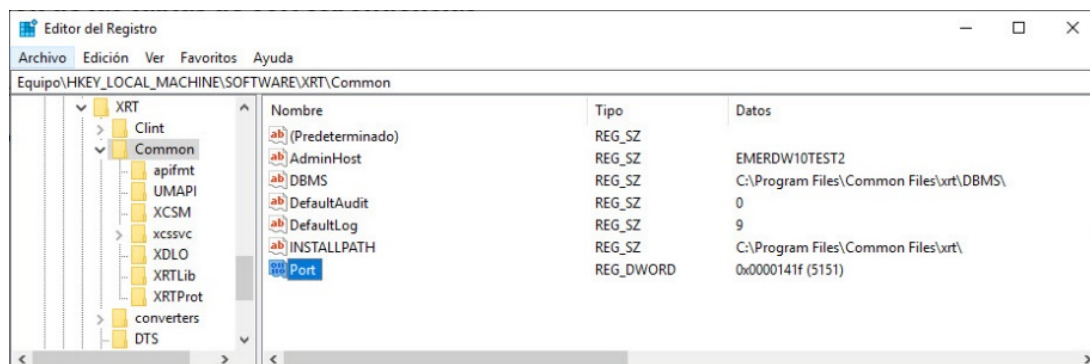
## Configuración de la máquina cliente

La máquina cliente hace referencia al equipo en el que se ejecutan las aplicaciones **Sage XRT** y el cliente XDLO.

Los principales parámetros de la parte cliente de XDLO se definen en la clave del Registro de Windows *HKEY\_LOCAL\_MACHINE\SOFTWARE\XRT\Common*.

En esta clave figuran los siguientes valores:

Valor	Descripción
AdminHost	Nombre o dirección IP de la máquina en la que se ejecuta el servicio XDLO. El valor predeterminado de este parámetro es <b>local</b> .
Port	Número de puerto IP en el que el servicio XDLO se encuentra en escucha de las llamadas de clientes. El valor predeterminado de este parámetro es <b>5151</b> .



Los parámetros opcionales de la parte cliente de XDLO se definen en la clave del Registro de Windows *HKEY\_LOCAL\_MACHINE\SOFTWARE\XRT\Common\XDLO*.

En esta clave figuran los siguientes valores:

Valor	Descripción
DebugRC	Este valor activa el modo <i>debug</i> del componente cliente que genera un archivo de <i>log xdlo_remclient.log</i> si tiene asignado el valor <b>Y</b> . El archivo de <i>log</i> se genera en la carpeta <User>\Application Data\XRT\XCS.
Cache_lease	Este valor define el plazo en segundos durante el que XDLO utiliza la caché para encontrar una cadena de conexión. Cuando el plazo « <i>cache lease</i> » expira, XDLO llama al servicio.

## Grupo de trabajo

Al instalar **Sage XRT Common Services** por primera vez, no hay ningún grupo de trabajo creado. Por lo tanto, el primer paso consiste en crear uno o varios grupos de trabajo.

En este capítulo se explica cómo crear un grupo de trabajo en función del tipo de base de datos que se utilice: SQL Server u Oracle.

Asimismo, figura la descripción detallada de las primeras acciones que hay que llevar a cabo tras la creación de un grupo de trabajo: actualizar una base de datos, añadir un grupo de trabajo y gestionar los usuarios de un grupo de trabajo.

## Creación de un grupo de trabajo

### Asistente para la creación de un grupo de trabajo

1. En el menú Inicio, seleccione **Programas > Sage > Administration XRT .NET**.

Aparecerá la pantalla de conexión.

Sage XRT Common Services

**Sage XRT**  
Sage XRT Common Services  
Consola de administración

☐ Gestionar grupos de trabajo  
☒ Administrar el grupo de trabajo:

TEST\_SQL2016

☐ Utilizar la seguridad integrada de Windows  
☐ Conectar con SageID

Usuario:  
ADMIN

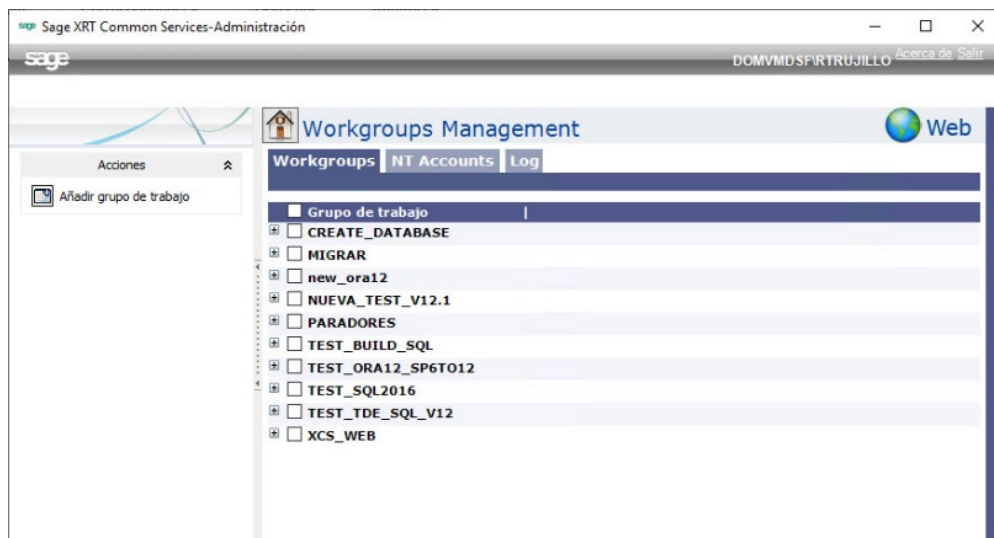
Contraseña:

**Conectar**

© Sage 2018

## Consola Win32

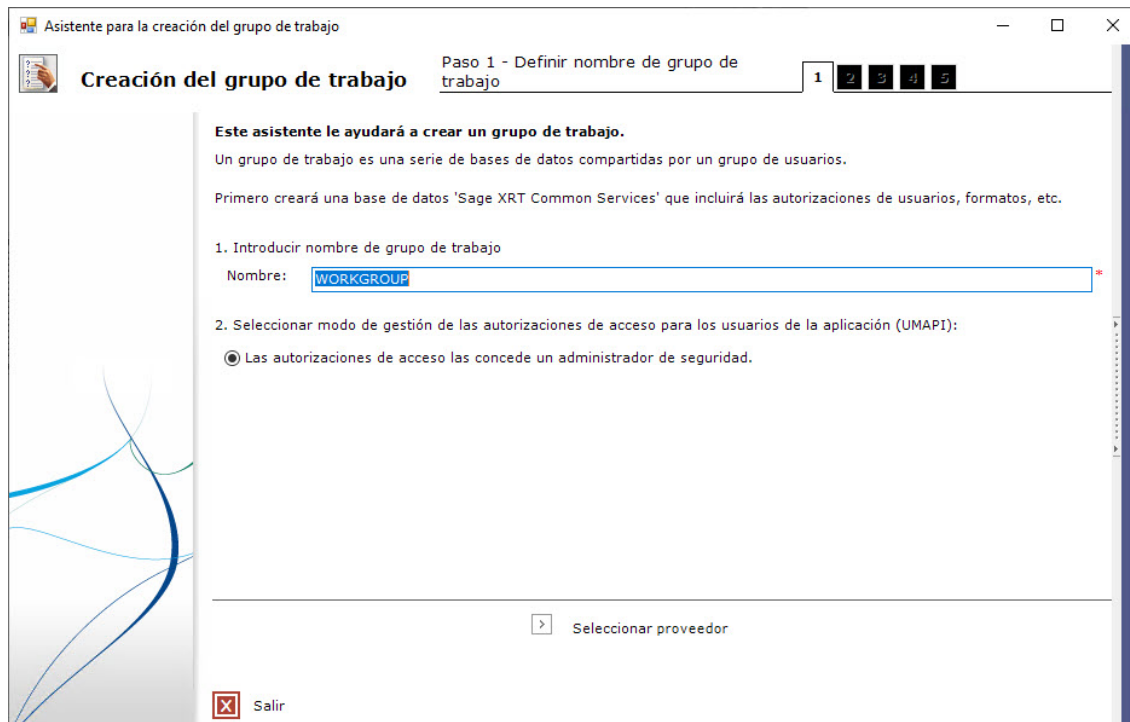
2. Seleccione la opción **Gestionar grupos de trabajo**.
3. A continuación, haga clic en **Conectar**.



4. Para abrir el asistente de creación de un **grupo de trabajo**, haga clic en el enlace **Añadir grupo de trabajo**.

**Nota:** Si no hay ningún grupo de trabajo, aparecerá directamente la pantalla **Creación del grupo de trabajo** sin pasar por las etapas 2 y 3.

## Definir el nombre del grupo de trabajo



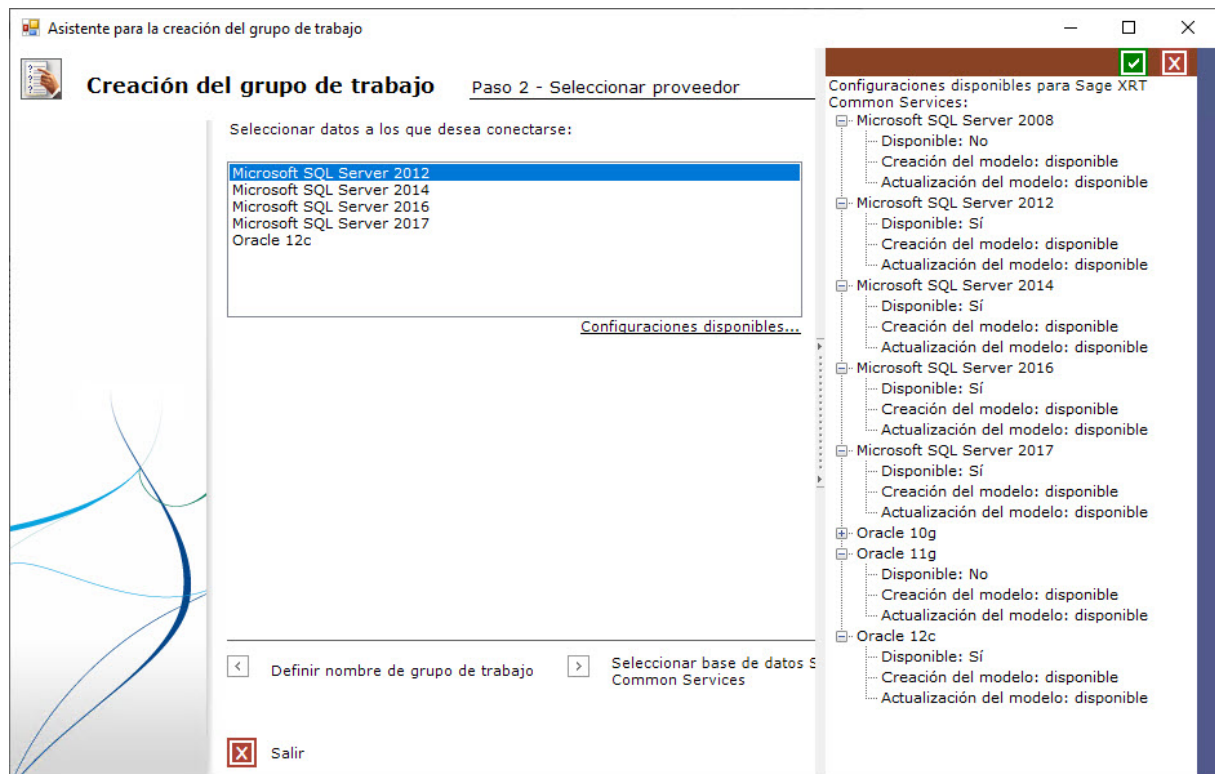
## Consola Win32

1. Introduzca un nombre para el grupo de trabajo en el campo **Nombre**. El nombre que figura por defecto es *WORKGROUP*.
2. Las autorizaciones de acceso de los usuarios a las aplicaciones **Sage XRT** las concede un administrador de seguridad.
3. Haga clic en el enlace **Seleccionar proveedor**.

### Seleccionar proveedor



1. En la lista, seleccione el servidor o cliente de base de datos instalado.
2. Haga clic en **Configuraciones disponibles...** para conocer el detalle de los servidores o clientes de bases de datos instalados en la máquina, así como las operaciones admitidas (creación y actualización).



3. Haga clic en el icono en forma de cruz **Salir** para cerrar la página y volver a la pantalla de selección de los proveedores de acceso a las bases de datos.
4. A continuación, haga clic en **Seleccionar base de datos Sage XRT Common Services**.

## Seleccionar base de datos Sage XRT Common Services

Asistente para la creación del grupo de trabajo

**Creación del grupo de trabajo** Paso 3 - Seleccionar base de datos Sage XRT Common Services

Especificar la siguiente información para conectarse a los datos de SQL Server:

1. Seleccionar o introducir nombre de servidor:
2. Introducir credenciales del administrador del servidor:
 

☐ Utilizar seguridad integrada de Windows  
☒ Utilizar un nombre de usuario y una contraseña:  
 Nombre usuario:   
 Contraseña:  ☐ Sin contraseña
3. Seleccionar o crear base de datos en el servidor:
 

☐ Seleccionar base de datos: ☐ Usar ODBC Driver ☐ Grupo de disponibilidad  
☒ Crear base de datos:  
 Nombre:   
 DBO:  Contraseña:   
 Usuario:  Contraseña:   
 Collation string:  ☐ Base de datos incluida

[Probar conexión DBA](#)  
[Probar conexión DBO](#)  
[Probar conexión USERS](#)

1. Introduzca el nombre del servidor en el que debe crearse la base de datos. Los valores disponibles para indicar el servidor son los siguientes:
  - (local)
  - (LOCAL)
  - .
  - Nombre del servidor

El botón **Actualizar** permite obtener la lista de los servidores Microsoft SQL Server conectados a la red de la empresa.

2. Según el tipo de autenticación utilizado por el DBA para conectarse al servidor de bases de datos, seleccione una de las siguientes opciones:
  - **Utilizar seguridad integrada de Windows:** el DBA se autentica por su cuenta de Windows (AD).
  - **Utilizar un nombre de usuario y una contraseña:** el usuario se autentica mediante un nombre de usuario y una contraseña.

**Nota:** Haga clic en el enlace **Probar conexión DBA**, situado en la parte inferior de la página, para comprobar las credenciales del DBA.



3. Seleccione o cree una base de datos en el servidor:

- Marque la opción **Seleccionar base de datos** si desea trabajar en una base de datos existente:
  - Seleccione la base de datos (la lista de las bases de datos existentes se actualiza al consultarla por primera vez).
  - Introduzca la contraseña correspondiente al nombre del DBO que aparece en el campo **DBO**. La contraseña propuesta por defecto por el asistente es **password#2005** (si el usuario selecciona una base de datos en la lista, el asistente busca automáticamente el nombre del propietario de esa base de datos. El asistente utiliza la cuenta DBA para realizar esta operación).
  - Introduzca la contraseña de la cuenta **XRTUSERS**. Por defecto, el asistente propone la contraseña **password#2005**.

**Nota:** Haga clic en el enlace **Probar conexión DBO**, situado en la parte inferior de la página, para comprobar las credenciales del propietario de la base de datos (DBO).

- Marque la opción **Crear base de datos** si desea crear una nueva base de datos:
  - Introduzca el nombre de la base de datos: el asistente comprueba que ninguna base tenga ese nombre cuando el usuario hace clic en **Propiedades de la base de datos**.

**Nota:** El nombre de la base de datos no debe incluir espacios ni caracteres especiales (\*, ?, \, /, etc.).

- Introduzca las credenciales del propietario de la base de datos: el asistente propone, por defecto, la cuenta **XRT** y la contraseña **XRT**. El asistente también se encarga, en su caso, de crear la cuenta y de asignarle el rol de *db\_owner* en la base.
- Seleccione la *collation string* o deje por defecto **Modern\_Spanish\_CI\_AS** (no existe distinción entre mayúsculas y minúsculas).

4. Haga clic en Versión del modelo XRT.

### Configuración de las unidades lógicas

Por defecto, el asistente propone un escenario en el que las tablas (*filegroup DATA*) y los índices (*filegroup INDEX*) del modelo se crean en el *filegroup PRIMARY* (*filegroup* predeterminado al crear una base de datos SQL Server).

En el panel de las propiedades puede realizar las siguientes acciones:

- Modificar el escenario propuesto e instalar las tablas y los índices en dos *filegroups* diferentes (ejemplo: *XCS\_DATA* y *XCS\_INDEX*)
- Modificar los parámetros de creación de los *filegroups* (carpeta de destino, tamaño inicial, tamaño máximo, tasa de crecimiento). Para que la creación se realice correctamente, debe existir la carpeta de destino.

**Importante:** Los *scripts* modelo de **Sage XRT Common Services** hacen referencia a un *filegroup* «lógico» *DATA* para las tablas y un *filegroup* «lógico» *INDEX* para los índices.

Durante la ejecución de las operaciones de creación del modelo, el asistente reemplaza estos nombres lógicos por los valores introducidos en la pantalla de propiedades (*PRIMARY* para el escenario predeterminado).

Si no existen los *filegroups* de destino (por ejemplo, *XCS\_DATA* y *XCS\_INDEX*), el asistente los crea automáticamente.

Haga clic en Crear/Actualizar modelos.

### Crear/Actualizar modelos

La lista **Scripts a ejecutar** incluye todos los scripts utilizados para crear el modelo *XRT Common Services* (XCS):

- createlogicalunits.sql

Script de creación de las unidades lógicas (una unidad lógica representa un *filegroup* correspondiente a la creación de una base de datos Microsoft SQL Server).

- xl\_configuration createxl\_configuration.sql

Script de creación de la tabla en la que se guardará la versión del modelo.

- registerlogicalunits.sql

Script de registro de las unidades lógicas.

A continuación, se tratarán los scripts «producto». Según sea su tipo, los *scripts* se ejecutan con la cuenta del DBA o del DBO.

1. Marque la casilla **Seleccionar datos a importar** y seleccione uno de los idiomas de la lista.

Esta importación corresponde a los datos (formato XML) para APIFMT, TRANSCO y UMAPI.

2. Haga clic en **Confirmar todas las etapas** para proceder a la ejecución de las operaciones configuradas en los pasos 1, 2, 3, 4 y 5 del asistente.

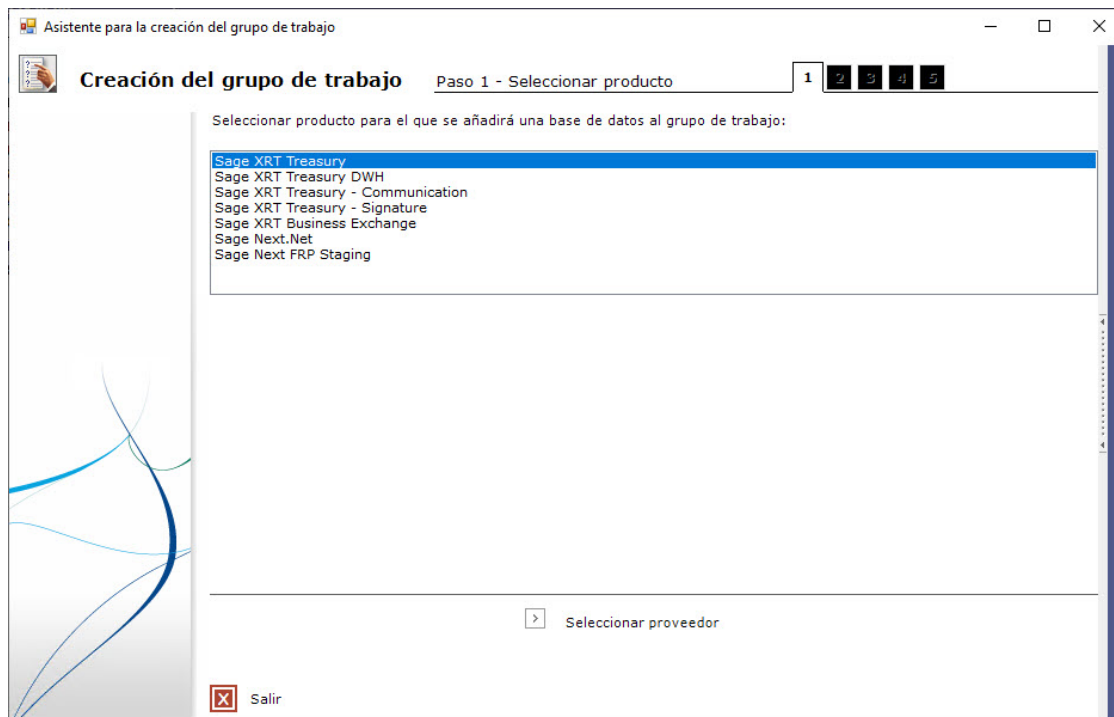
### Ejecución de las operaciones

La ejecución de las operaciones puede tardar algunos minutos. En esta etapa se crea el modelo XCS.

Puede salir del asistente para la creación de un grupo de trabajo haciendo clic en el icono en forma de cruz **Salir** e iniciar la consola de administración o añadir un modelo de producto.

Haga clic en **Añadir base de datos del producto**.

## Seleccionar producto

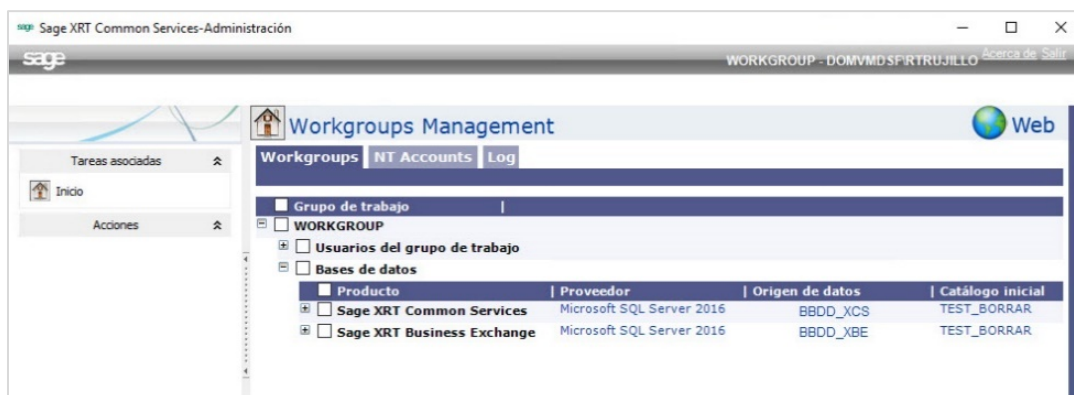


1. Seleccione uno de los productos de la lista.
2. Haga clic en el enlace **Seleccionar proveedor**.

**Nota:** Para más información sobre cómo seleccionar un proveedor, consulte al apartado **Seleccionar proveedor**.

## Añadir un grupo de trabajo

El espacio de trabajo de la consola de administración, cuando se abre en modo **Gestionar grupos de trabajo**, tiene el siguiente aspecto:



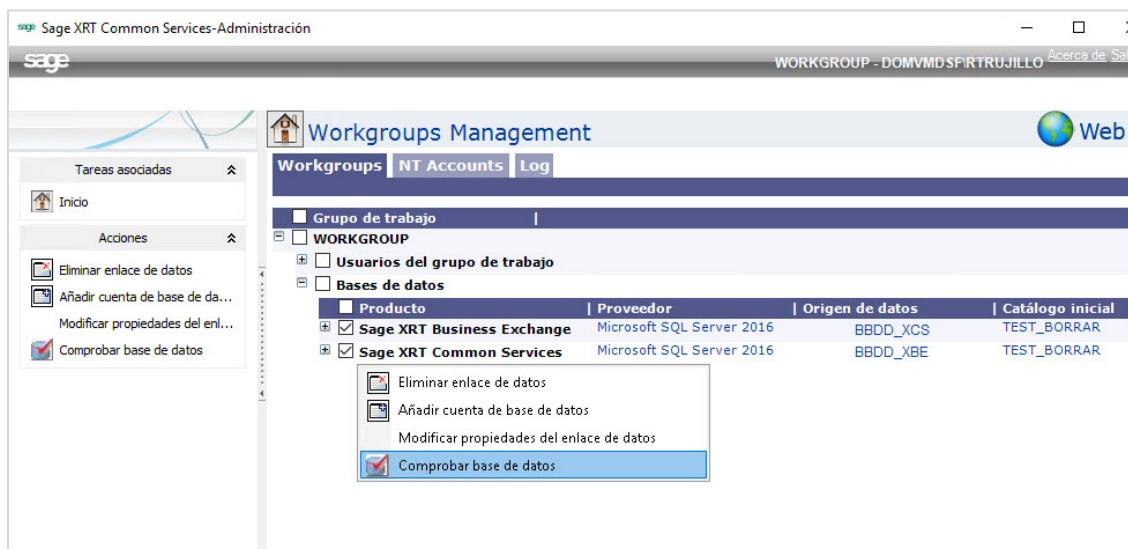
Haga clic en el enlace **Añadir grupo de trabajo**.

Para añadir un grupo de trabajo repita los pasos seguidos para su creación. Puede consultar el apartado **Creación de un grupo de trabajo** para obtener más información.

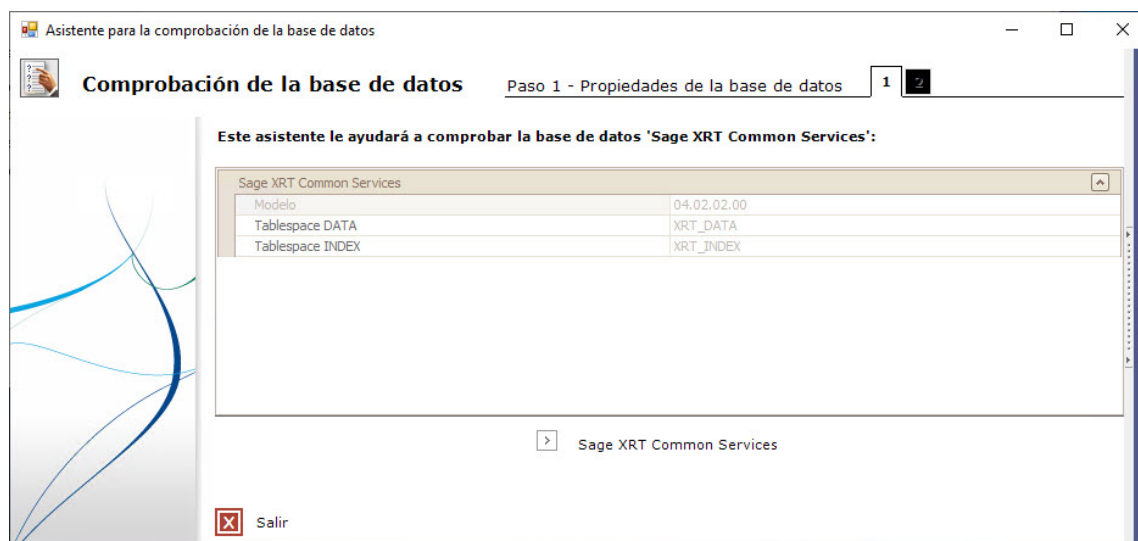
### Actualización de las bases de datos de un grupo de trabajo

La actualización de una base de datos puede conllevar ciertos riesgos para los datos del usuario. Por lo tanto, antes de ejecutar este tipo de operación, asegúrese de haber realizado una copia de seguridad de los datos del usuario.

1. En la página de inicio, seleccione **Grupo de trabajo** y expanda la categoría correspondiente al nombre del grupo de trabajo y, a continuación, la subcategoría **Bases de datos**.
2. Sitúese en la línea correspondiente a la base de datos que vaya a actualizar y haga clic en el botón secundario del ratón y seleccione **Comprobar base de datos** en el menú contextual.



Aparecerá en pantalla el asistente para la comprobación de bases de datos.



**Nota:** Si el usuario Windows no está registrado como DBO en el grupo de trabajo correspondiente, no podrá actualizar la base de datos. El asistente no propondrá ninguna actualización de la base de datos y no aparecerá el enlace correspondiente al producto.

1. Haga clic en el nombre del producto. Si el asistente encuentra alguna incoherencia entre las versiones, reenviará al usuario al proceso de actualización de la base de datos. En caso contrario, aparecerá la siguiente pantalla:



2. Responda **Sí** o **No** a la pregunta «¿Tiene una copia de seguridad de su base de datos?».
3. Si los datos de la base no están actualizados, marque la opción **Seleccionar datos a importar**.
4. Haga clic en el enlace Confirmar todas las etapas.

## Usuarios de un grupo de trabajo

Durante la creación de un grupo de trabajo, los grupos locales *Windows (AD) Administrators* y *XRTDBAdministrators* se declaran automáticamente como administradores del nuevo grupo de trabajo.

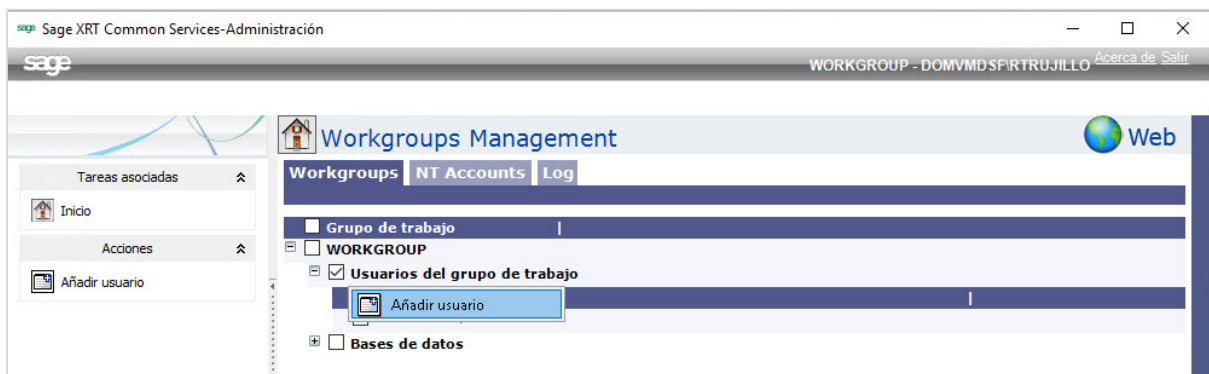
**Sage XRT Common Services** ofrece un asistente que permite gestionar los usuarios de los grupos de trabajo.

Dicho asistente reúne las siguientes operaciones:

- **Añadir usuario de red:** Para añadir un usuario, introduzca la cuenta Windows (AD) de un usuario de red o haga clic en **Búsqueda...** para acceder a la herramienta de búsqueda de un usuario Windows (AD) de Microsoft.
- **Añadir grupo de red:** Esta opción permite asociar un grupo de usuarios Windows (AD) a un grupo de trabajo. Para realizar esta asociación, haga clic en **Búsqueda...** La herramienta de Microsoft de búsqueda de un grupo Windows (AD) permite encontrar el grupo de usuarios apropiado.
- **Añadir sistema local:** Este tipo de cuenta es utilizada por un servicio del sistema que se ejecuta en la cuenta del sistema local y con acceso a una base de datos.

## Añadir un usuario a un grupo de trabajo

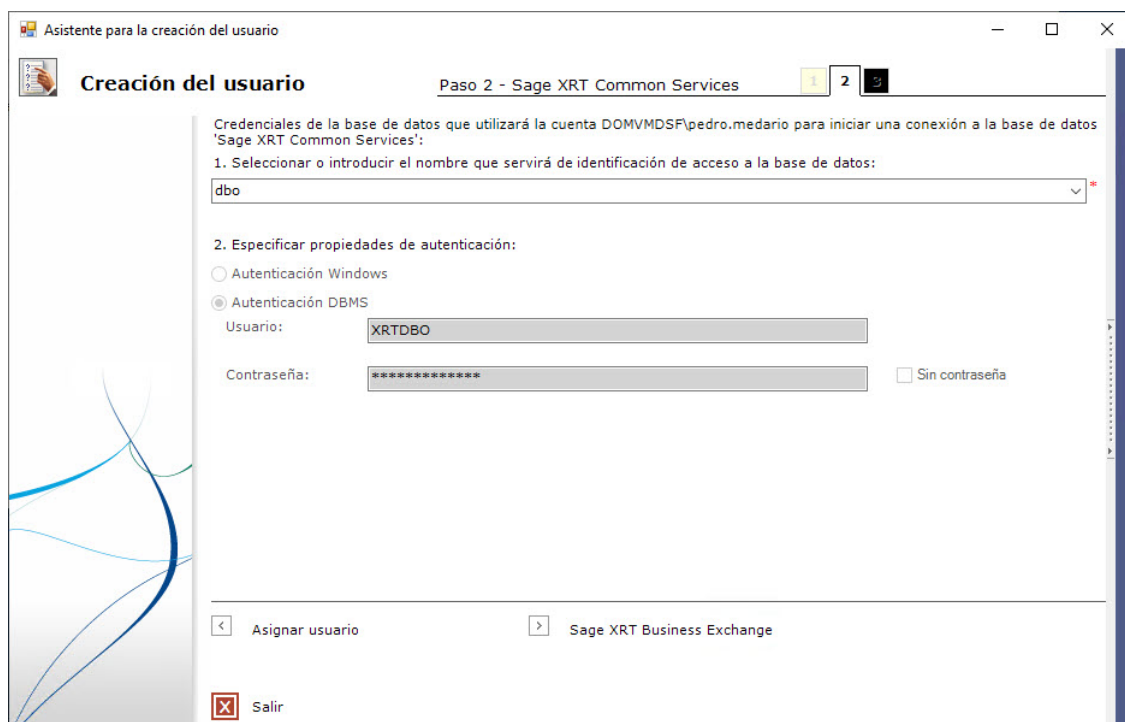
1. Para añadir un usuario al grupo de trabajo, expanda la categoría **Grupo de trabajo**.
2. Seleccione uno de los grupos de trabajo de la lista, sitúese en **Usuarios** y haga clic en el botón secundario del ratón.



3. Seleccione **Añadir usuario** para abrir el asistente para la creación de un usuario.



4. A continuación, haga clic en el enlace **Sage XRT Common Services** para pasar a la segunda etapa del asistente.

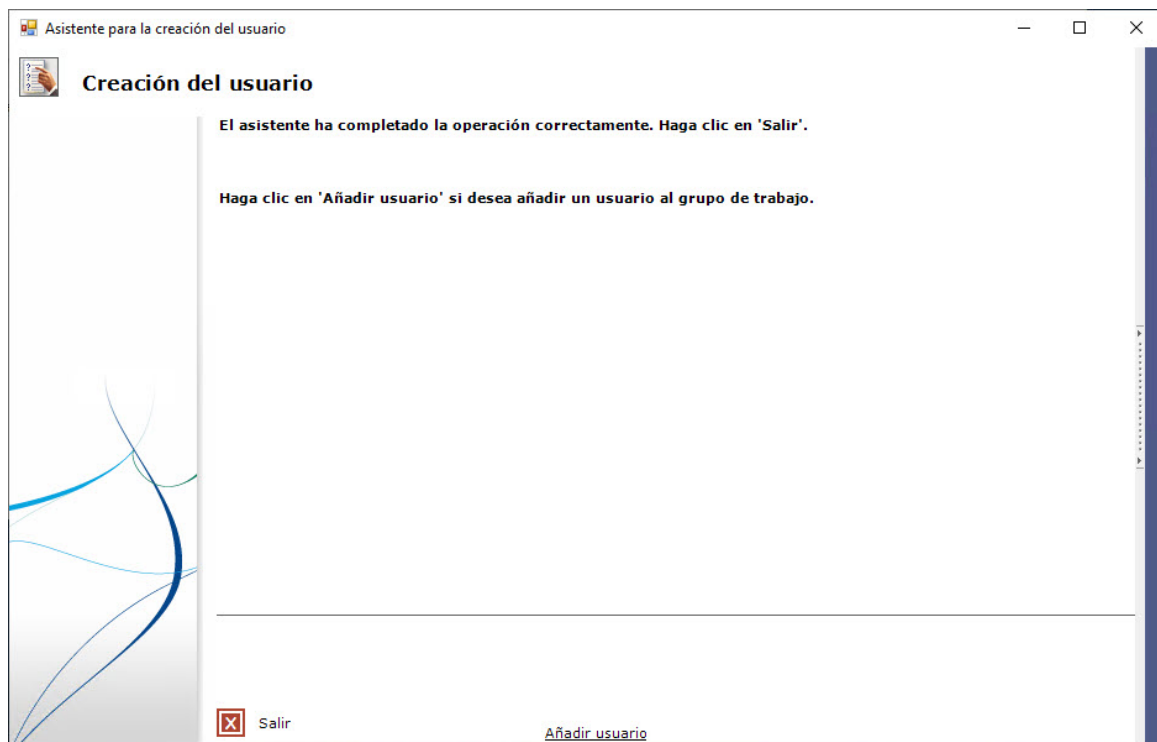


5. Seleccione un tipo de acceso a los datos en la lista desplegable, o introduzca un nombre nuevo. Por defecto, el asistente propone dos tipos de acceso predefinidos:
  - **DBO:** Este tipo de acceso debe reservarse al propietario de la base de datos.
  - **Users:** Este tipo de acceso lo deben utilizar los usuarios «sin poderes».
6. Seleccione el método de autenticación del usuario en el servidor de base de datos:
  - **Autenticación Windows:** El usuario se autentica mediante su cuenta de Windows (AD).
  - **Autenticación DBMS (SGBD):** El usuario se autentica mediante una cuenta que el administrador del servidor de bases de datos le ha asignado.

**Importante:** Se recomienda definir el acceso con una cuenta SQL Server pues el uso de la autenticación Windows (AD) no permite el *pooling* (agrupación) de conexiones.

Se puede crear un nuevo nombre de acceso para un grupo de usuarios determinado. Este nuevo acceso será de tipo *User*. Ejemplo: Definición de un acceso «Tesorero» para la base Sage XRT Treasury (SXT), con una cuenta SQL Server específica denominada TRESO.

7. Haga clic en Confirmar todas las etapas.



**Nota:** También existe la posibilidad de gestionar los usuarios de **Sage XRT Treasury** repitiendo los mismos pasos seguidos para acceder a la base **Sage XRT Common Services**.



## XDLO

XDLO es un arquitectura orientada a servicios (SOA, siglas del inglés Service Oriented Architecture) que gestiona las cadenas de conexión a las bases de datos para las aplicaciones **Sage XRT**. Con XDLO:

- Las cadenas de conexión se almacenan en un repositorio seguro, compartido por un grupo de usuarios.
- Los administradores del sistema definen las cadenas de conexión.
- Cada usuario pertenece a un grupo de trabajo.
- Un usuario puede cambiar con facilidad de grupo de trabajo, siempre y cuando el administrador haya configurado las cadenas de conexión apropiadas.

Asimismo, XDLO incluye dos elementos principales:

- Los objetos XDLO componente *COM XDLO\_COM.dll* y presentados a los clientes por el servicio de Windows (AD) *xdlo\_service.exe*, que se ejecuta en el puesto de administración y responde a las solicitudes de cadenas de conexión que realizan los clientes. Dicho servicio de Windows (AD) escucha las llamadas en el puerto *TCP/IP 5151* (este valor predeterminado puede cambiarse durante la instalación de **Sage XRT Common Services**).
- El cliente *rem\_client.dll* que utilizan las aplicaciones **Sage XRT** para enviar consultas al servicio XDLO. Este componente utiliza los *sockets* TCP/IP y DCOM para el intercambio de datos.

El nombre del puesto de administración se configura durante la instalación de las máquinas clientes.

## Destino de los datos

Los objetos XDLO se conservan en un archivo XML que se encuentra en la carpeta **<All Users>\Application Data\XRT** del puesto de administración. Si fuera necesario, se puede cambiar la ubicación de este archivo. Para una implementación en modo clúster, el archivo en cuestión se puede instalar en una carpeta compartida.

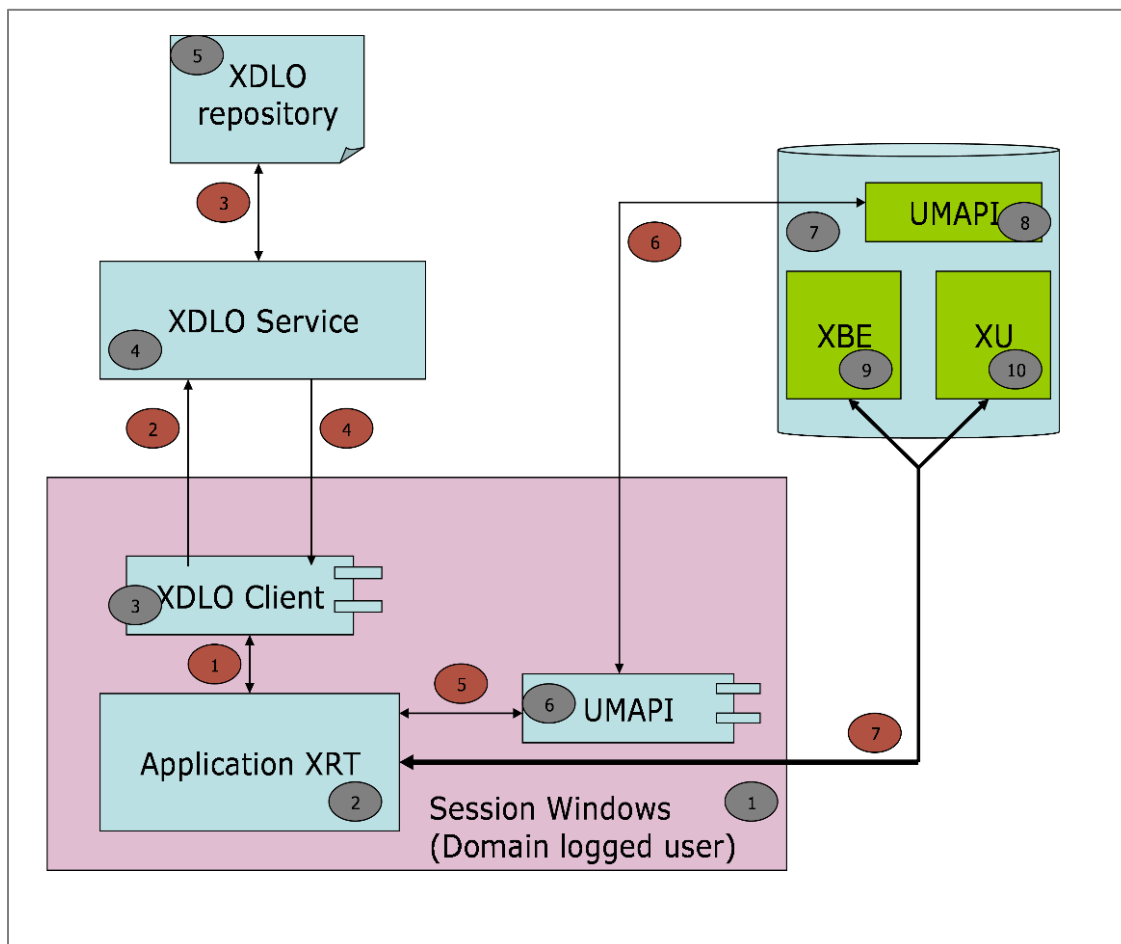
El archivo XML está protegido por el algoritmo de cifrado 3DES, de forma que los usuarios no pueden modificarlo.

En un sistema de archivos NTFS, el panel **Seguridad** permite al administrador configurar permisos avanzados para restringir los accesos al archivo de destino de los datos de XDLO.








## Dinámica de los intercambios

El siguiente gráfico es una representación esquemática de los intercambios entre los componentes XDLO en una aplicación **Sage XRT**. Representa:

- Los diferentes componentes de los procesos: 1
- Las interacciones entre los componentes: 1

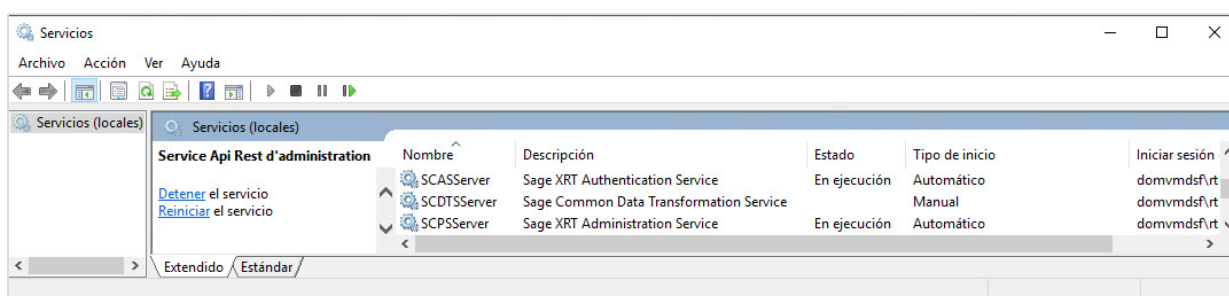


Componente	Descripción
1	Sesión Windows de un usuario del dominio AD. Esta sesión está abierta y la conexión a la aplicación <b>Sage XRT</b> se realiza con la cuenta Windows (AD) del usuario conectado.
2	El usuario Windows (AD) ejecuta una aplicación <b>Sage XRT</b> ( <b>SXT</b> , <b>SXBE</b> , etc.).
3	La aplicación utiliza el componente cliente XDLO instalado por el ejecutable de <b>Sage XRT Common Services</b> para obtener la cadena de conexión a la base de datos.
4	El componente cliente XDLO se conecta al servicio XDLO que se ejecuta en el puesto de administración. La comunicación entre el cliente y el servicio se realiza vía DCOM.
5	El archivo XDLO incluye la definición de los grupos de trabajo y sus correspondientes cadenas de conexión. El servicio XDLO busca la información en el archivo XDLO.
6	Si la aplicación obtiene una cadena de conexión, inicia el componente UMAPI para comprobar si el usuario está habilitado para utilizar el programa y obtener los permisos de acceso al producto.
7	La aplicación se conecta a la base de datos SQL Server u Oracle con una cadena de conexión obtenida mediante XDLO.
8	La base de datos incluye los derechos UMAPI de las aplicaciones <b>Sage XRT</b> .
9	La base de datos puede incluir las tablas <b>SXBE</b> y los datos de <b>SXBE</b> .
10	La base de datos puede incluir las tablas <b>SXT</b> y los datos de <b>SXT</b> .

Interacción	Descripción
	La aplicación <b>Sage XRT</b> ejecuta el cliente XDLO con las credenciales de Windows (AD) del usuario conectado.
	El cliente XDLO se conecta al servicio en el puerto TCP/IP e inicia una comunicación vía DCOM.
	El servicio XDLO busca en el repositorio XDLO para encontrar los grupos de trabajo configurados para el usuario de Windows (AD) conectado.
	El servicio XDLO devuelve la información al cliente XDLO. Este dato permite a la aplicación crear la lista de grupos de trabajo para la ventana de conexión.
	La aplicación crea una instancia del componente UMAPI para obtener los derechos del usuario en la aplicación.
	El componente UMAPI consulta las tablas UMAPI en la base de datos para obtener los derechos del usuario. Esta información se devuelve a la aplicación que, de esta forma, puede concluir la inicialización de su entorno de ejecución.
	La aplicación puede conectarse al repositorio y el usuario empezar a trabajar.

## Presentación de los servicios de autenticación, presentación y transformación

- El **servicio de autenticación** (SCASServer) permite validar la autenticación de los usuarios.
- El **servicio de presentación** (SCPSServer) permite gestionar la parte correspondiente a **Derechos** (usuarios, perfiles, sitios, etc.), **Auditorías** (auditorías y logs) y **Correspondencias** (diseño y gestión).
- El **servicio de transformación** (SCDTSServer) garantiza la conversión de un archivo de un formato A a otro B, y la disponibilidad de la información de seguimiento de la operación.



La documentación de estas API la genera Swagger. El archivo *swagger.json* corresponde a una exportación de la documentación en formato JSON.

El enlace al archivo JSON figura en el archivo *\*.config* de cada servicio en el directorio **C:\Program Files\Common Files\xrt**.

## Servicio de autenticación (SCAS)

Archivo de configuración Sage.SCASServer.Service.exe.config

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

Posibilidad de activar *logs*

```
<ApplicationSettings>
  <add key="websitehost" value="http://localhost" />
  <add key="httpservicehost" value="http://localhost:8760/Auth" />
  <add key="httpsservicehost" value="https://localhost:8761/Auth" />
<!--
```

Definición de la ubicación del sitio web,  
de los puertos de escucha y de los *hosts*  
de servicio

```
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 documento y  
URL de exportación  
Se puede desactivar

## Servicio de presentación (SCPS)

Archivo de configuración Sage.SCPSServer.Service.exe.config

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

Posibilidad de activar *logs*

```
<add key="websitehost" value="http://localhost"/>
<add key="httpservicehost" value="http://localhost:8733"/>
<add key="httpsservicehost" value="https://localhost:8734"/>
<add key="syncprofilesiteuser" value="XRT"/>
<add key="syncprofilesitefrequency" value="3600"/>
<!--
```

Definición de la ubicación del sitio web, de  
los puertos de escucha y de los *hosts* de  
servicio

```
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 documento y  
URL de exportación  
Se puede desactivar

## Servicio de transformación (SCDTS)

Archivo de configuración Sage.SCDTSServer.Service.exe.config

