

# Sage XRT Business Exchange

Versión 11.40.500

Gestión de la contraseña de firma interna



# Índice

|  |          |
|--|----------|
| <b>DESCRIPCIÓN.....</b>                                      | <b>3</b> |
| <b>ADMINISTRACIÓN SAGE .NET. ....</b>                        | <b>4</b> |
| Gestión de los derechos.....                                 | 4        |
| <b>ADMINISTRACIÓN DEL SISTEMA .....</b>                      | <b>7</b> |
| Servicio de firma .....                                      | 7        |
| Entrada de las contraseñas de firma interna.....             | 8        |
| Contraseña no conforme con los requisitos de seguridad ..... | 8        |
| Contraseña válida .....                                      | 8        |
| <b>PUESTO CLIENTE WEB .....</b>                              | <b>9</b> |
| Contraseña no conforme con los requisitos de seguridad ..... | 9        |
| Contraseña válida .....                                      | 9        |

## Descripción

El presente documento describe los elementos que hay que configurar para que la contraseña de la firma interna sea segura, en relación con las reglas de gestión definidas en **Administración Sage .NET**.

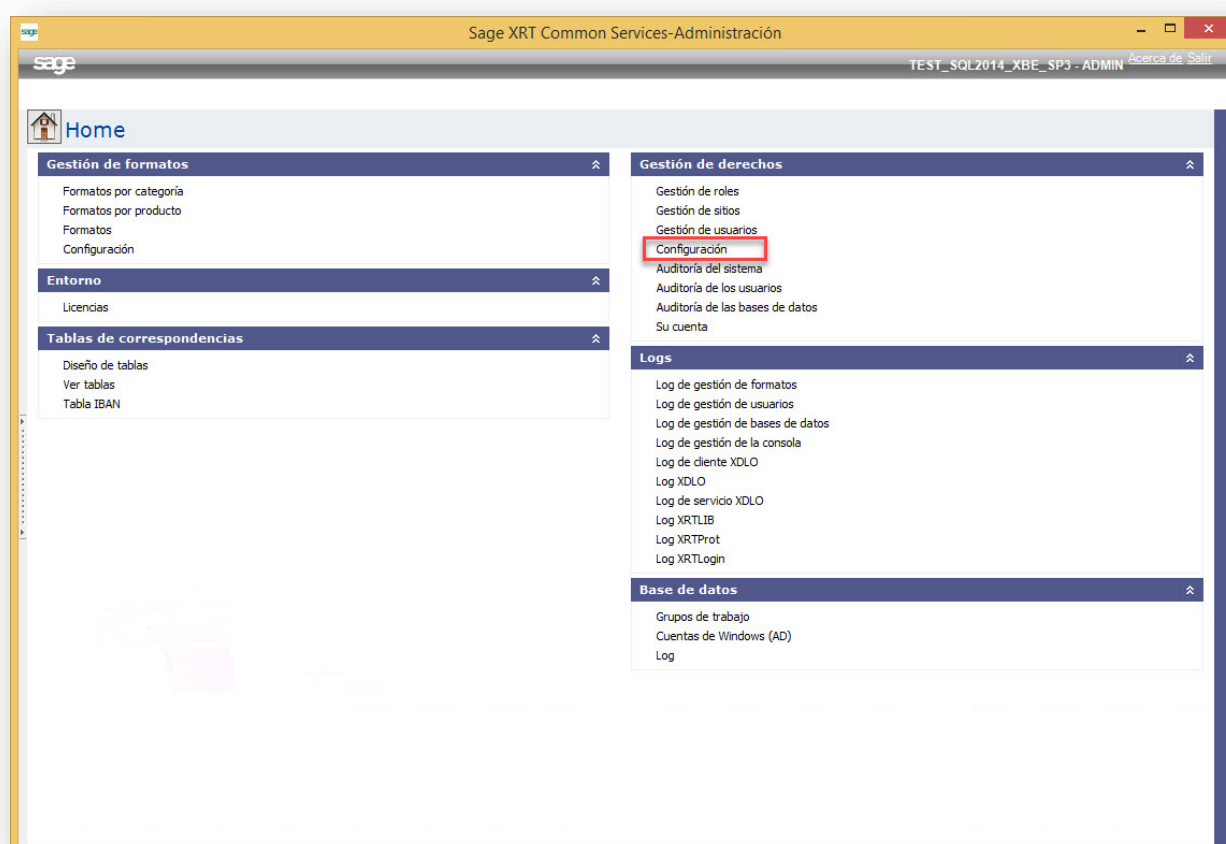
## Administración Sage .NET.

La seguridad de la contraseña de la firma interna está relacionada con la configuración definida en **Administración Sage .NET**. Asimismo, es necesario establecer en este módulo los controles que se desean activar.

### Gestión de los derechos

Acceda a **Administración Sage .NET**.

En el apartado **Gestión de derechos**, haga clic en **Configuración**:



A continuación, haga clic en **Configuración de directiva de contraseñas:**



Aquí, se pueden activar diversas reglas para validar las contraseñas que se definen para los usuarios de las aplicaciones Sage XRT.

**Parámetros de la gestión de usuarios**

**Modo operativo Autenticación Windows:**

☒ Los usuarios de cuentas de Windows no tienen que introducir su contraseña para iniciar sesión en la aplicación.

☐ Los usuarios de cuentas de Windows tienen que introducir su contraseña para iniciar sesión en la aplicación.

**Parámetros de la contraseña:**

☒ N° obligatorio de caracteres numéricos para las nuevas contraseñas 4

☒ N° obligatorio de mayúsculas para las nuevas contraseñas 1

☒ Longitud mínima de la contraseña 8

☐ Antigua y nueva contraseña deben diferir 4

☐ La nueva contraseña y el nombre de usuario deben diferir

☐ Contraseña predet. para las nuevas cuentas \*\*\*\*

Confirmar contraseña predet. para las nuevas cuentas \*\*\*\*

☐ Bloquear cuenta si la contraseña predeterminada no se cambia en el momento 6 días

☐ Periodo de validez de las nuevas contraseñas 4 semanas

☐ Cta. bloqueada tras unos intentos fallidos de conexión 3

Cuenta bloqueada durante un periodo de 1 minutos

☒ Aceptar

☐ Cancelar

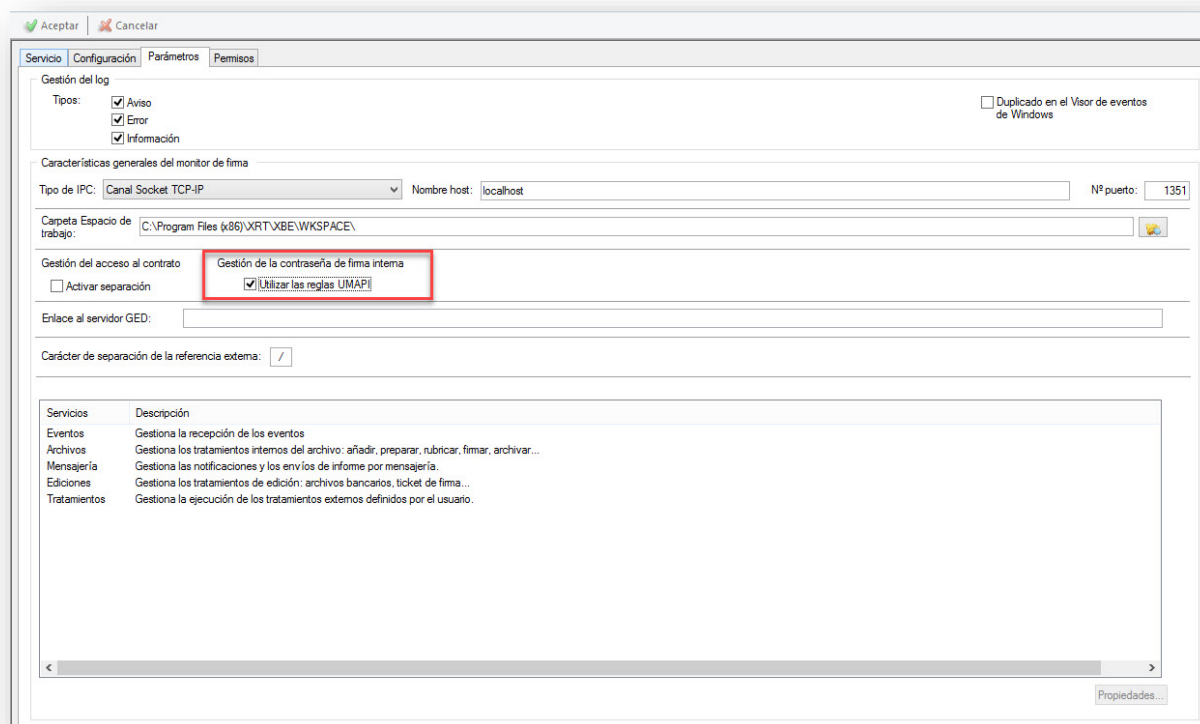


Solo las tres primeras reglas (**N° obligatorio de caracteres numéricos para las nuevas contraseñas**, **N° obligatorio de mayúsculas para las nuevas contraseñas** y **Longitud mínima de la contraseña**) se utilizan para garantizar la seguridad de las contraseñas de firma interna.

## Administración del sistema

### Servicio de firma

En la configuración del Servicio de firma, se ha añadido un nuevo apartado, **Gestión de la contraseña de firma interna**, destinado a la activación de la seguridad de la contraseña:



| Servicios    | Descripción   |
|--------------|---|
| Eventos      | Gestiona la recepción de los eventos  |
| Archivos     | Gestiona los tratamientos internos del archivo: añadir, preparar, rubricar, firmar, archivar... |
| Mensajería   | Gestiona las notificaciones y los envíos de informe por mensajería.                             |
| Ediciones    | Gestiona los tratamientos de edición: archivos bancarios, ticket de firma...                    |
| Tratamientos | Gestiona la ejecución de los tratamientos externos definidos por el usuario.                    |

**Utilizar las reglas UMAP:** Esta opción está desactivada por defecto. Si se activa, tres reglas, y solamente esas, de gestión de la contraseña de los usuarios, configuradas en **Administración Sage .NET**, se utilizan para supervisar las contraseñas de firma interna.

#### Parámetros de la contraseña:

|  |   |
|--|---|
| <input checked="" type="checkbox"/> N° obligatorio de caracteres numéricos para las nuevas contraseñas | 4 |
| <input checked="" type="checkbox"/> N° obligatorio de mayúsculas para las nuevas contraseñas           | 1 |
| <input checked="" type="checkbox"/> Longitud mínima de la contraseña                                   | 8 |

Si se marcan estas opciones en **Administración Sage .NET** y, si además, la opción **Utilizar las reglas UMAPI** está activada, las reglas se aplicarán a la gestión de la contraseña de firma interna.



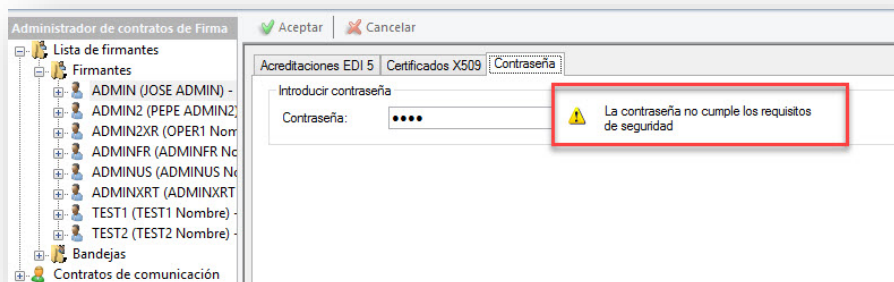
El hecho de aplicar una regla de gestión de la contraseña para la firma interna, activando la opción **Utilizar las reglas UMAPI**, implica que esas reglas se aplicarán también a la contraseña utilizada para la conexión.

## Entrada de las contraseñas de firma interna

En la definición de la contraseña de los firmantes, si la opción **Utilizar las reglas UMAPI** está activada, aparecerá un icono para indicar que se cumplen, o no, las reglas configuradas.

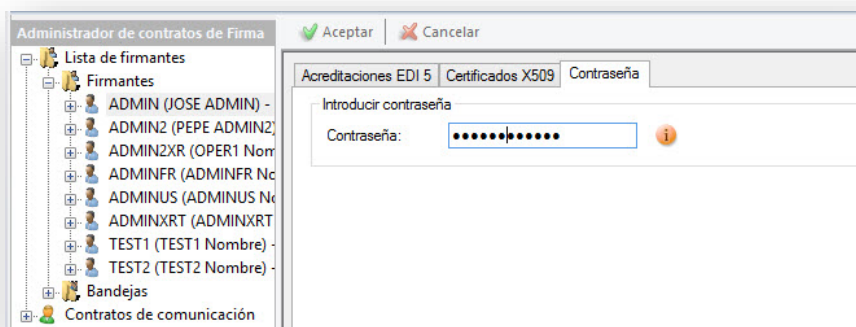
### Contraseña no conforme con los requisitos de seguridad

Hasta que la contraseña introducida no cumpla los requisitos de seguridad, aparecerá el icono acompañado del mensaje «La contraseña no cumple los requisitos de seguridad» al lado del campo de entrada:



### Contraseña válida

Si la contraseña es válida, aparecerá el icono al lado del campo de entrada.





## Puesto cliente Web

En caso de que un usuario modifique su contraseña a través del módulo Web, aparecerá una raya indicando el cumplimiento (o incumplimiento) de las reglas configuradas.

### Contraseña no conforme con los requisitos de seguridad

Hasta que la contraseña introducida no se ajuste a las reglas de seguridad definidas, aparecerá una raya roja con el texto «No conforme» al lado del campo de entrada:

### Contraseña válida

Si la contraseña introducida se ajusta a las reglas de seguridad definidas, aparecerá una raya verde con el texto «Conforme» al lado del campo de entrada: