



Sage XRT Common Services

Versión 4.2

Doble autenticación



Índice

Introducción.....	3
Tecnología	3
Proceso de implementación.....	3
Configuración de usuarios	4
Creación de enlaces.....	5
Creación del enlace (conexión vía el sitio web)	5
Creación del enlace (conexión en el puesto cliente).....	6
Uso de la doble autenticación.....	7
Conexión por el sitio web	7
Conexión en el puesto cliente	7
Recuperación	8

Introducción

El objetivo de este documento es explicar el uso de la funcionalidad de **doble autenticación** disponible a partir de la versión 4.2 de **Sage XRT Common Services**.

La doble autenticación se podrá utilizar para la autenticación segura de los usuarios en todos los productos que utilicen **Sage XRT Common Services** 64 bits (en las versiones 4.2 y posteriores). Esta funcionalidad no está disponible en **Sage XRT Common Services** 32 bits (en versiones 3.x).

Tecnología

La tecnología utilizada para la doble autenticación se basa en el protocolo TOTP (Time-based One-time Password, RFC 6238).

Este protocolo combina una clave secreta con la marca de tiempo (*timestamp*) activa mediante una función de *hash* criptográfica para generar un código de uso único. Como la latencia de la red y los relojes no sincronizados pueden llevar a un intento de autenticación en un intervalo de tiempo diferente, el *timestamp* aumenta por intervalos de 30 segundos, lo que reduce el espacio de búsqueda potencial.

La adopción de este protocolo permite utilizar todas las aplicaciones móviles compatibles con dicho protocolo, como por ejemplo Microsoft Authenticator, Google Authenticator o FreeOTP.

Proceso de implementación

Para que un usuario puede utilizar la doble autenticación, es necesario lo siguiente:

- Que la opción **Doble autenticación** esté activada para dicho usuario en **Sage XRT Common Services**.
- Que el usuario haya instalado en su dispositivo móvil una aplicación TOTP compatible.

Funcionamiento: el usuario introduce sus credenciales (nombre de usuario y contraseña) para autenticarse. Si todo es correcto, el servidor genera una clave secreta que el usuario introducirá en la aplicación TOTP de su *smartphone*, o escaneará el código QR obtenido. La aplicación móvil genera automáticamente un código de uso único (de 6 cifras) que se comprobará en el servidor. Si el código es correcto, el usuario se autentica de dos formas, con sus credenciales (nombre de usuario y contraseña) y con un código de acceso único, y puede empezar a utilizar la aplicación correspondiente.

Para las siguientes autenticaciones, el usuario introducirá su nombre de usuario y contraseña. Si todo es correcto, el servidor solicitará al usuario que introduzca su actual código de uso único (de 6 cifras). Para ello, el usuario irá a la aplicación TOTP de su móvil para consultar el código generado. Si es correcto, el usuario se autentica de dos formas, con sus credenciales (nombre de usuario y contraseña) y con un código de acceso único, y puede empezar a utilizar la aplicación correspondiente.

Importante: Para que esto funcione, los relojes del dispositivo del usuario y del servidor tienen que estar prácticamente sincronizados (por lo general, el servidor acepta los códigos de uso único generados por marcas de tiempo (*timestamp*) que difieran en ± 1 intervalo de tiempo respecto a la hora del cliente).

Configuración de usuarios

Para que un usuario pueda utilizar la doble autenticación, antes hay que activar dicha opción para el usuario correspondiente en **Sage XRT Common Services**.

De modo que, al crear o modificar un usuario, se activará o desactivará la opción de doble autenticación.

Crear usuario

Usuario: Buscar...

Roles Sitios

☐ ADMIN

Autenticación

☐ Autenticación Windows ☐ Autenticar usuario con certificado x.509

☐ Autenticación LDAP ☒ Doble autenticación

☐ Autenticación estándar ☐ Contraseña predet.

☐ Autenticación SageID

Contraseña

Confirmar contraseña

Tipo de usuario

☐ Administrador de seguridad de nivel 1

☒ Usuario estándar

Varios

Idioma

Descripción

E-mail

☐ P. de validez 0 años (hasta 03/10/2019)

☒ Aceptar

☐ Cancelar

Creación de enlaces

Creación del enlace (conexión vía el sitio web)

Un usuario introduce sus credenciales (nombre de usuario y contraseña) en el sitio web.

A continuación, se comprueba que dicho usuario esté correctamente autenticado.

Si se ha activado la opción de doble autenticación para dicho usuario, el servidor generará una clave secreta que el usuario introducirá en la aplicación TOTP de su *smartphone*, o escaneará el código QR obtenido.

Después, el usuario introducirá el código generado por la app de autenticación (de 6 cifras), que el servidor comprobará.

Si el código es correcto, significa que la app de autenticación del usuario está vinculada y este puede utilizar la doble autenticación (sin escaneo de código QR para las sesiones posteriores).

El usuario solo podrá acceder a la aplicación si ha introducido el código correcto y si se ha autenticado correctamente.

Importante: Si el usuario ya ha vinculado su aplicación de autenticación en el sitio web, no tendrá que volverlo a hacer en el puesto cliente, lo único que se le solicitará es su actual código de uso único (de 6 cifras).

Nota: En la consola de **Sage XRT Common Services**, si la opción **Doble autenticación** de la pantalla para la modificación del usuario está marcada, el color que esta tenga indicará el estado de la doble autenticación:

Naranja: El usuario todavía no ha vinculado su app de autenticación.

Verde: El usuario ha vinculado su app de autenticación correctamente.

Creación del enlace (conexión en el puesto cliente)

Este proceso es similar al de creación del enlace en el sitio web. Un usuario introduce sus credenciales (nombre de usuario y contraseña) en el cuadro de diálogo de inicio de sesión (*login*).

Se comprueba que dicho usuario esté correctamente autenticado.

Si se ha activado la opción de doble autenticación para dicho usuario, el servidor generará una clave secreta que el usuario introducirá en la aplicación TOTP de su *smartphone*, o escaneará el código QR obtenido.



Después, el usuario introducirá el código generado por la app de autenticación (de 6 cifras), que el servidor comprobará.

Si el código es correcto, significa que la app del usuario está vinculada y puede utilizar la doble autenticación (sin escaneo de código QR para las sesiones posteriores).

El usuario solo podrá acceder a la aplicación si ha introducido el código correcto y si se ha autenticado correctamente.

Importante: Si el usuario ya se ha vinculado vía el puesto cliente, no tendrá que volverlo a hacer en el sitio web, lo único que se le solicitará es su actual código de uso único (de 6 cifras).

Nota: En la consola de **Sage XRT Common Services**, si la opción **Doble autenticación** de la pantalla para la modificación del usuario está marcada, el color que esta tenga indicará el estado de la doble autenticación:

Naranja: El usuario todavía no ha vinculado su app de autenticación.

Verde: El usuario ha vinculado su app de autenticación correctamente.

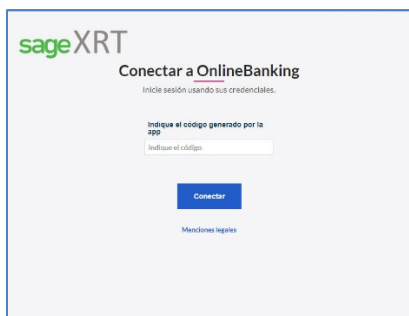
Uso de la doble autenticación

Conexión por el sitio web

Un usuario introduce sus credenciales (nombre de usuario y contraseña) en el sitio web.

A continuación, se comprueba que dicho usuario esté correctamente autenticado.

Si se ha activado la opción de doble autenticación para el usuario, y este ya ha vinculado su app de autenticación, se le solicitará que introduzca el código de uso único (de 6 cifras) que haya generado la app TOTP de su móvil.



The screenshot shows the SageXRT Online Banking login interface. At the top, the logo 'sageXRT' is displayed. Below it, the text 'Conectar a OnlineBanking' is shown, followed by a smaller instruction: 'Inicie sesión usando sus credenciales.' There are two input fields: the first is labeled 'Indique el código generado por la app' and the second is labeled 'Indique el código'. A blue 'Conectar' button is positioned below the input fields. At the bottom, there is a link that says 'Manténgase logueado'.

El usuario solo podrá acceder a la aplicación si ha introducido el código correcto y si se ha autenticado correctamente.

Conexión en el puesto cliente

Un usuario introduce sus credenciales (nombre de usuario y contraseña) en el cuadro de diálogo de inicio de sesión (login).

Se comprueba que dicho usuario esté correctamente autenticado.

Si se ha activado la opción de doble autenticación para el usuario, y este ya ha vinculado su app de autenticación, se le solicitará que introduzca el código de uso único (de 6 cifras) que haya generado la app TOTP de su móvil.



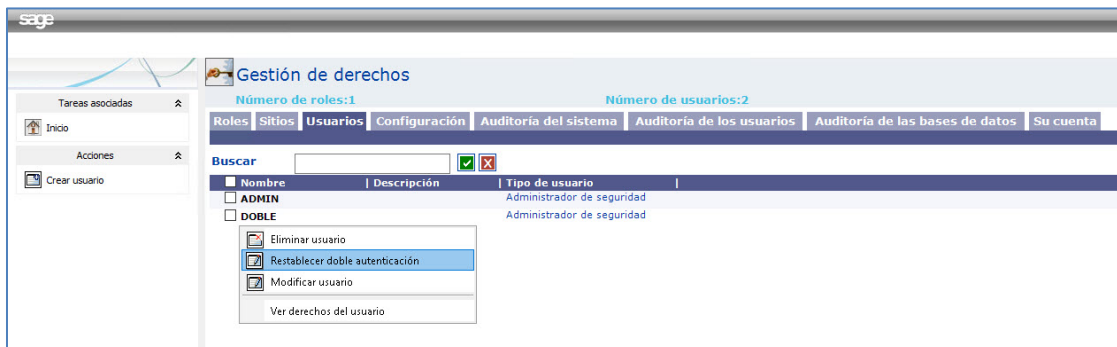
The screenshot shows a 'Console de administración' window titled 'Doble Autenticación'. It contains a single input field with the placeholder text 'Introduzca el código generado por la app:'. Below the input field is a green 'Aceptar' button. In the bottom left corner, there is a small copyright notice: '© Sage 2018'.

El usuario solo podrá acceder a la aplicación si ha introducido el código correcto y si se ha autenticado correctamente.

Recuperación

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 **Restablecer doble autenticación** en la lista de usuarios.



En la pantalla correspondiente a la modificación del usuario, el color de la opción **Doble autenticación** indicará su estado:

- **Naranja:** El usuario todavía no ha vinculado su app de autenticación.
- **Verde:** El usuario ha vinculado su app de autenticación correctamente.

