

# Doble Autenticación en 3DEXPERIENCE



## Contenido

<b>Ventajas de la Doble Autenticación en 3DEXPERIENCE.....</b>	<b>3</b>
<b>¿Cómo podemos activar la doble autenticación a los usuarios?.....</b>	<b>4</b>
<b>¿Qué ocurre cuando un usuario desactiva la autenticación en dos Factores? ..</b>	<b>5</b>
<b>¿Cómo acceder cuando se activa la Autenticación en 2 Factores? .....</b>	<b>5</b>

La plataforma 3DEXPERIENCE permite el acceso seguro utilizando el doble factor de autenticación que usa el algoritmo de contraseña de un solo uso basada en el tiempo TOTP app (Time-Based One-Time Password).

En este documento se comentarán las ventajas y diferentes opciones para activar y configurar la doble autenticación en la plataforma 3DEXPERIENCE.

## Ventajas de la Doble Autenticación en 3DEXPERIENCE

La seguridad es un aspecto crucial en cualquier plataforma digital, especialmente cuando se trata de herramientas tan integrales y sofisticadas como 3DEXPERIENCE. La doble autenticación es una **capa adicional de protección** que asegura que solo los usuarios autorizados puedan acceder a los datos y recursos dentro de la plataforma. Algunas de las principales ventajas de implementar la doble autenticación son:

- 1. Mayor protección contra Accesos no autorizados.** La doble autenticación añade un segundo paso en el proceso de inicio de sesión, que generalmente requiere algo que el usuario sabe (como una contraseña) y algo que el usuario tiene (como un dispositivo móvil). Esto dificulta enormemente el acceso para los intrusos, incluso si logran obtener la contraseña del usuario.
- 2. Reducción de riesgo de robo de identidad.** Proporciona una barrera adicional que protege la identidad digital de los usuarios. Este método asegura que incluso si las credenciales de un usuario se ven comprometidas, un atacante no podrá acceder a la cuenta sin el segundo factor de autenticación.
- 3. Protección de datos sensibles.** 3DEXPERIENCE maneja una gran cantidad de datos confidenciales y propiedad intelectual. La doble autenticación asegura que esta información vital esté protegida, minimizando el riesgo de filtraciones de datos y accesos no deseados.
- 4. Cumplimiento normativo.** Muchas industrias están sujetas a regulaciones que requieren medidas estrictas de seguridad de datos. Esto ayuda a cumplir con estos requisitos.



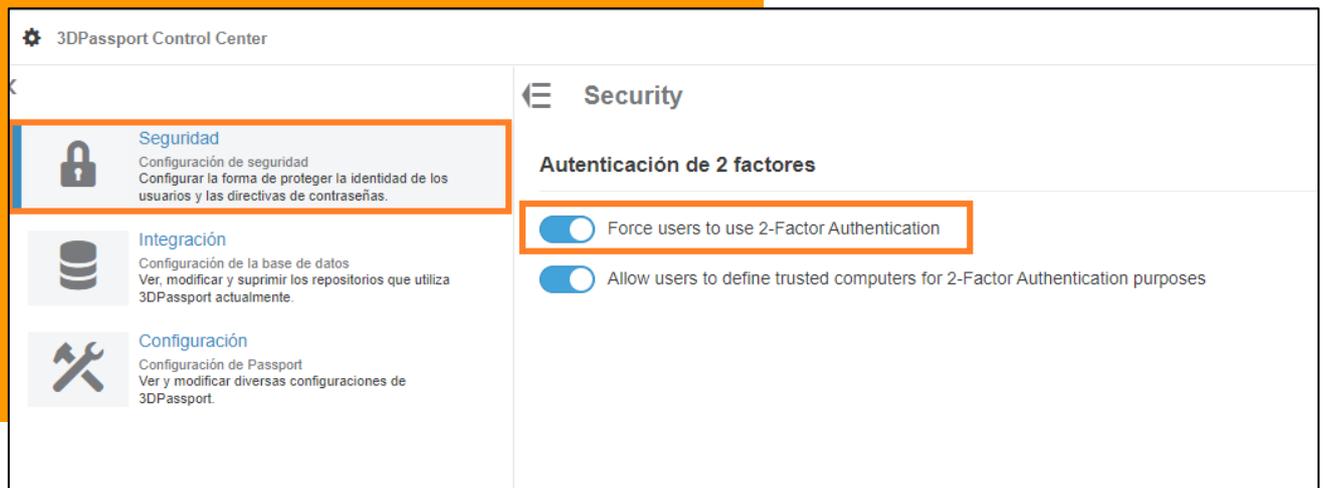
## ¿Cómo podemos activar la doble autenticación a los usuarios?

Si los clientes deciden implementar la seguridad en dos pasos, todos los clientes en ese tenant tendrán que utilizar los códigos TOTP para el acceso.

Esta capacidad está disponible para los administradores en la sección mi perfil. Tendrás que seleccionar mi cuenta, Herramientas de administración.

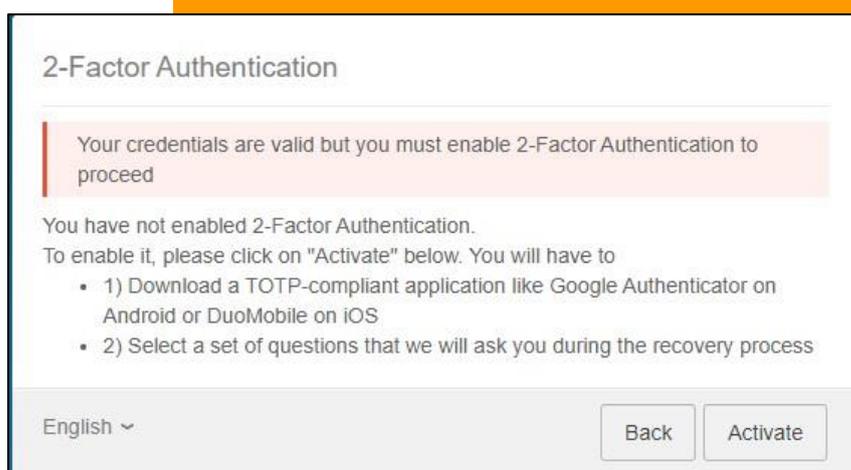


Selecciona Seguridad y activa “Force users to use 2-Factor Authentication”.



## ¿Qué ocurre cuando un usuario desactiva la autenticación en dos Factores?

Si uno de los usuarios desactiva la opción “Force users to use 2-Factor Authentication” que ha sido activada por el administrador de la plataforma, podrá desactivarlo. Pero, la próxima vez que el usuario trate de acceder al tenant, un mensaje aparecerá solicitándole que active la Autenticación de doble factor de nuevo. Sin activarlo no podrá acceder a la plataforma.



## ¿Cómo acceder cuando se activa la Autenticación en 2 Factores?

En el primer inicio de sesión tras la activación de la autenticación en dos factores tendremos que activar la autenticación en dos pasos. Tras acceder a nuestro tenant nos aparecerá un mensaje. Tendremos que seleccionar la opción Activar. Tendremos dos opciones:

1. Descargar una aplicación TOPT como Google Authenticator o DuoMobile en IOS.
2. Seleccionar unas preguntas para asegurar el proceso de recuperación.



## 2-Factor Authentication

Your credentials are valid but you must enable 2-Factor Authentication to proceed

You have not enabled 2-Factor Authentication.

To enable it, please click on "Activate" below. You will have to

- 1) Download a TOTP-compliant application like Google Authenticator on Android or DuoMobile on iOS
- 2) Select a set of questions that we will ask you during the recovery process

Activar

Atrás

Ahora cada vez que introduzcamos nuestro usuario y contraseña tendremos que añadir el código de verificación mediante la aplicación TOPT.



## 3DEXPERIENCE Platform - Control de acceso

Validate 2FA code from paired TOTP application to continue

Code

Trust this computer

Validar

[Recover my account](#)



origen

A través de un código QR podremos vincular nuestra cuenta con un dispositivo móvil. Una vez vinculado podremos desactivar nuestras credenciales de este dispositivo o transferirlas a otro dispositivo.



## 2-Factor Authentication

2-Factor Authentication enabled

You have enabled 2-Factor Authentication.

If you want to disable 2-Factor Authentication, click on "Deactivate".

If you want to use a new device for 2-Factor Authentication, click on "Transfer".

Please note that these actions require you to have access to your mobile application with your TOTP credentials.

Desactivar

Transfer

Atrás

