



INFRASTRUCTURE

MINING & METALS

NUCLEAR, SECURITY & ENVIRONMENTAL

OIL, GAS & CHEMICALS

# iSupplier Portal: Autenticación con Multi Factor y Contraseñas de Uso Único

Última Actualización: 4-Jun-18

## Tabla de Contenidos

1	Autenticación con Multi Factor y Claves de Uso Único.....	1
1.1	Autenticación de Two Factor .....	1
1.2	Agregar Google Authentication para Autenticación con Multi Factor .....	2
1.3	Gestión de Dispositivo de Claves de Uso Único .....	5
2	Soporte .....	7
2.1	Información de Contacto .....	7

# 1 Autenticación con Multi Factor y Claves de Uso Único

## 1.1 Autenticación de Two Factor

1. Deberá obtener una **Clave de Uso Único (One-Time Pass-Code, u OTP)** para **cada** ingreso. Esta es una característica de seguridad adicional y no puede obviarse.
2. Si entregó un número de teléfono móvil para completar su registro, podrá recibir su **OTP** mediante **SMS** (mensaje de texto). Si no entregó un número de teléfono móvil, puede recibir su **OTP** mediante **correo electrónico**. También puede descargar la aplicación Microsoft Authenticator a su teléfono móvil para usar Soft Token. Una vez que haya elegido la Opción de Clave de Uso Único y haya hecho clic en “Click here to get the One-Time-Pass-Code”, aparecerá una confirmación.

The screenshot shows the 'Bechtel Partner Access' login page. At the top, there is a red header with the Bechtel logo and a 'Help' button. Below the header, the page title is 'Sign In (multi-factor)'. A yellow disclaimer box contains the following text: 'By Logging on to the system, you agree to the following disclaimer. This system is for authorized Bechtel business purposes. Access is restricted to authorized users. User consents to monitoring and recording of use and agrees to comply with Bechtel policies and procedures. Violation thereof or improper use may result in discipline ranging from withdrawal of access privileges up to and including immediate dismissal. If monitoring reveals evidence of possible criminal activity, the results of such monitoring may be provided to law enforcement officials.' Below the disclaimer, there is a form with the following fields and options: 'E-Mail Address:' with a text box containing a redacted email address followed by '@GMAIL.COM'; 'One-Time Password Options:' with two radio button options: 'SMS/Text: (XXXXXXX-6624)' (which is selected) and 'Email: (XXXXXXXXXX@GMAIL.COM)'; a green button labeled 'Click here to get the SMS/Text One-Time Pass-Code'; 'One-Time Pass-Code:' with a text box; a link 'I forgot my password?'; and a green button labeled 'Click here for Help'.

**Nota:** Tenga paciencia, ya que es posible que las OTP demoren algunos minutos en enviarse. Si envía la OTP más de una vez, asegúrese de usar la clave más reciente.

3. Después de unos minutos, debiera recibir su **OTP**. Ingrese el número de seis dígitos y presione el botón **Sign In**.

Bechtel Partner Access Help

Sign In (multi-factor)

By Logging on to the system, you agree to the following disclaimer.

This system is for authorized Bechtel business purposes. Access is restricted to authorized users. User consents to monitoring and recording of use and agrees to comply with Bechtel policies and procedures. Violation thereof or improper use may result in discipline ranging from withdrawal of access privileges up to and including immediate dismissal. If monitoring reveals evidence of possible criminal activity, the results of such monitoring may be provided to law enforcement officials.

E-Mail Address:  
XXXXXXXXXX@GMAIL.COM

One-Time Password Options:

SMS/Text: (XXXXXXXX-6624)

Email: (XXXXXXXXXX@GMAIL.COM)

Click here to get the SMS/Text One-Time Pass Code

One-Time Pass-Code:  
255532

[Forgot my password ?](#)

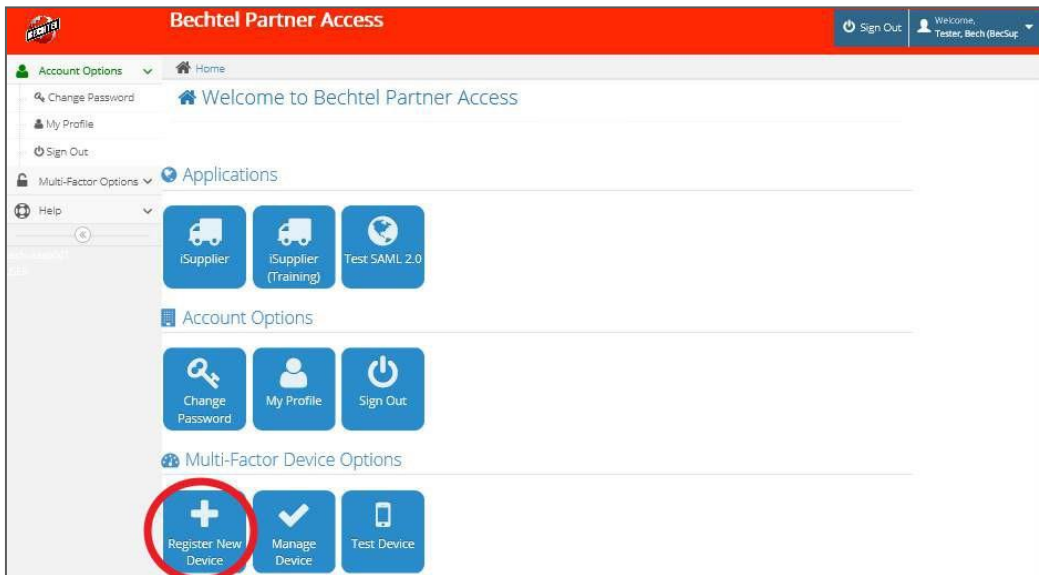
Click here for Help

**Nota:** Si ingresa una OTP errónea, deberá volver a solicitar una nueva clave. No puede volver a ingresar la misma clave de uso único.

## 1.2 Agregar Google Authentication para Autenticación con Multi Factor

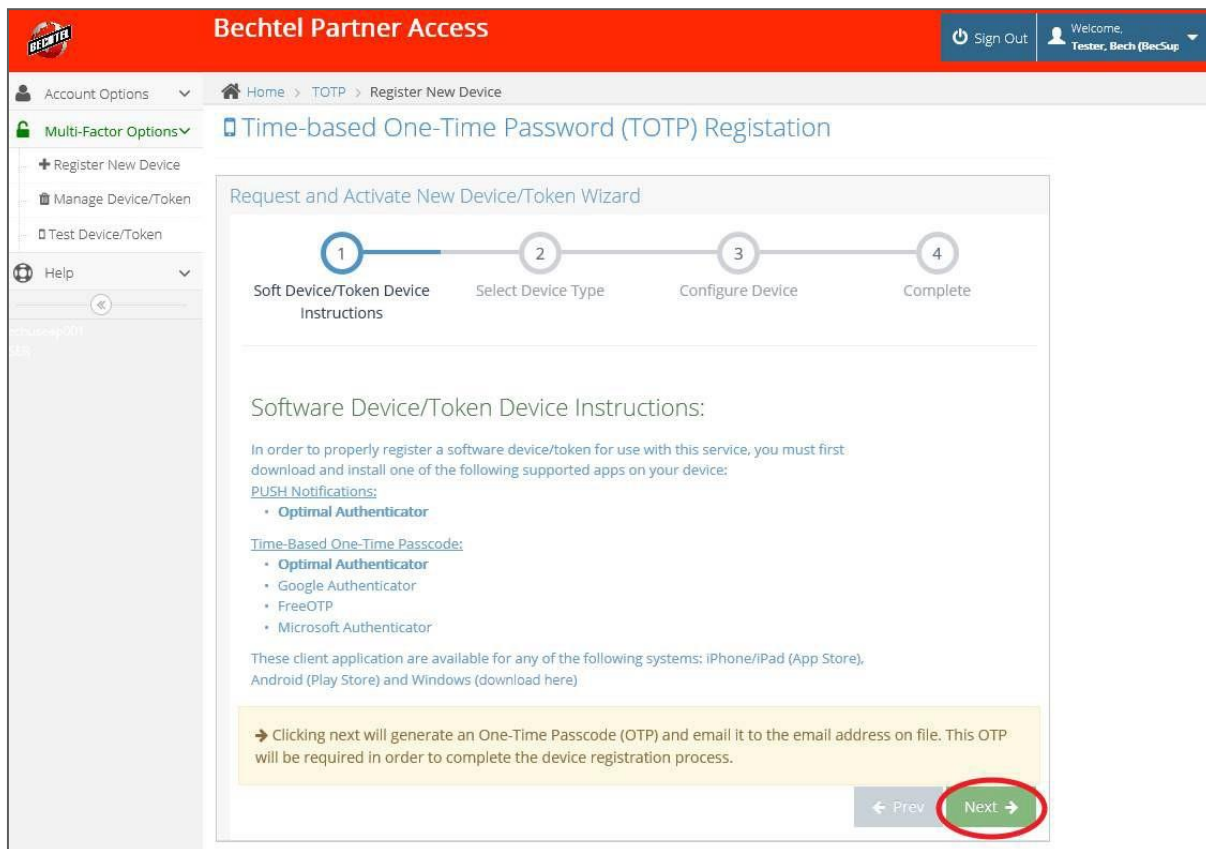
Google Authenticator es otra manera de obtener Autenticación de Two Factor. Si tiene un teléfono inteligente, **recomendamos enfáticamente** este método de autenticación, ya que tiene menos probabilidades de error y retraso que los métodos anteriores. Si experimenta un problema para obtener un código usando un método (SMS o correo electrónico), debiera probar Google Authenticator. Incentivamos la adopción de Google Authenticator para su dispositivo móvil a fin de evitar la dependencia de los códigos enviados por SMS o correo electrónico. Debe esperar hasta **después** de que se haya registrado e ingresado una vez para poder instalar Google Authenticator.

1. Ingrese al **Portal de iSupplier** usando el link: <https://supplier.becpsn.com/>
2. A fin de usar su teléfono móvil para las contraseñas de uso único, seleccione **Register New Device** bajo el encabezado **Multi Factor Device Options**.

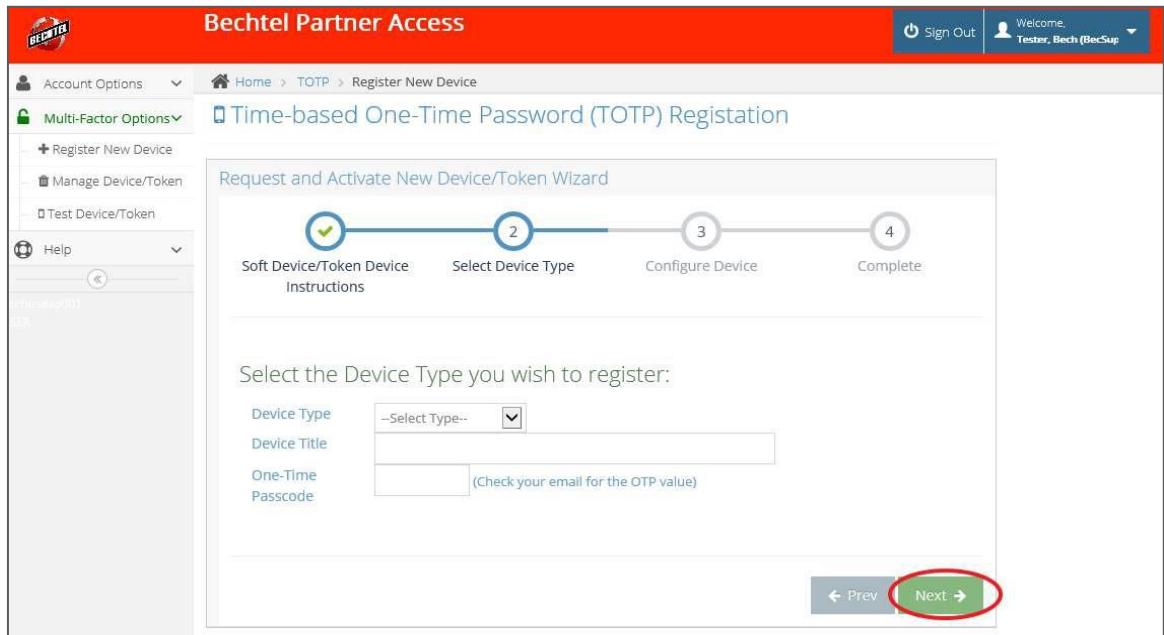


**Nota:** si no llega a esta página después de ingresar, salga y vuelva a ingresar. Si sigue teniendo problemas, contacte al Centro de Servicios IS&T en [istsc@Bechtel.com](mailto:istsc@Bechtel.com).

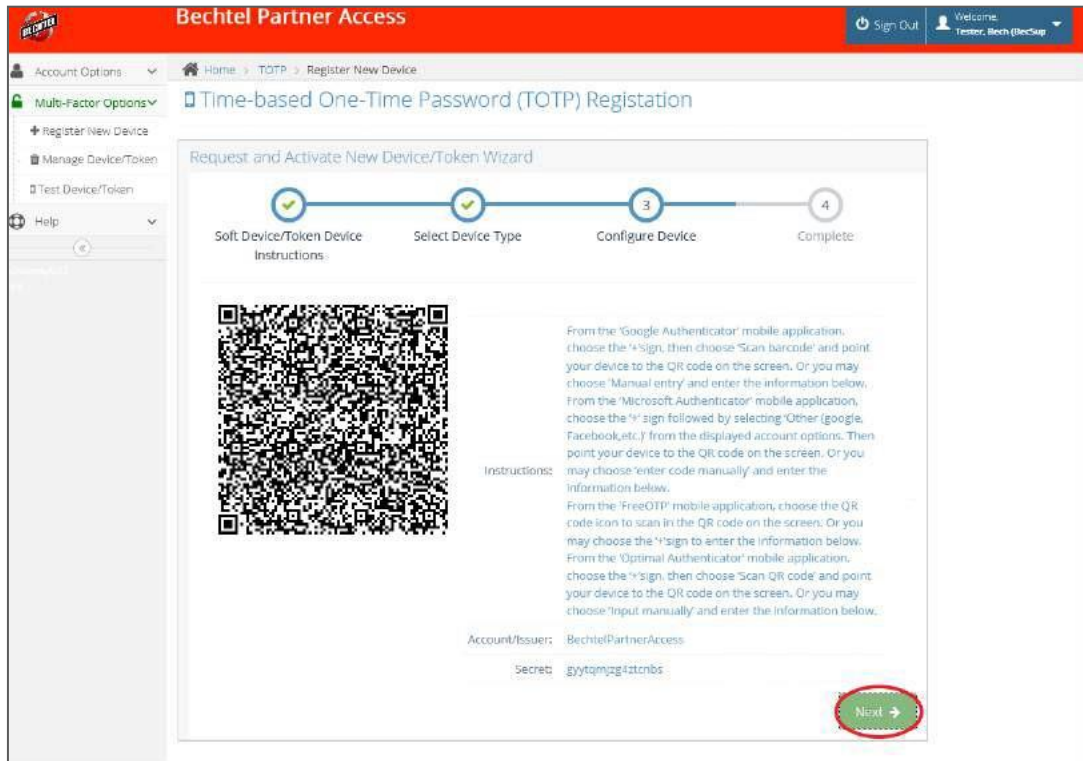
3. Lea las instrucciones y haga clic en el botón **Next** para continuar.



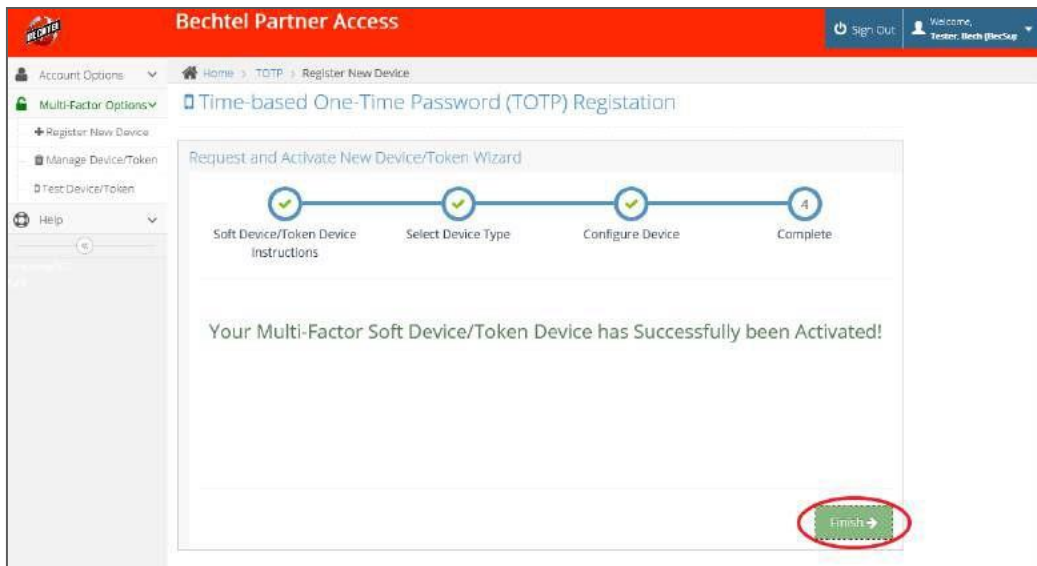
4. Seleccione el tipo de dispositivo, título del dispositivo e ingrese la OTP (que recibió por correo electrónico) luego haga clic en **Next** para continuar.



5. Descargue la aplicación “Google Authenticator” en su dispositivo móvil y siga las instrucciones que reciba para configurar Google Authenticator en su dispositivo. Haga clic en el botón **Next** para continuar.



6. Aparecerá una pantalla confirmando que su **Multi-Factor Soft Device/Token Device** se ha activado con éxito. Haga clic en el botón **Finish** para completar el proceso.



### 1.3 Gestión de Dispositivo de Claves de Uso Único

Puede gestionar los dispositivos usados para obtener su OTP una vez que ha ingresado. A fin de remover un dispositivo existente, primero deberá obtener una OTP nueva.

1. Para borrar un dispositivo existente, haga clic en **Manage Device/Token** en el lado izquierdo de la página.

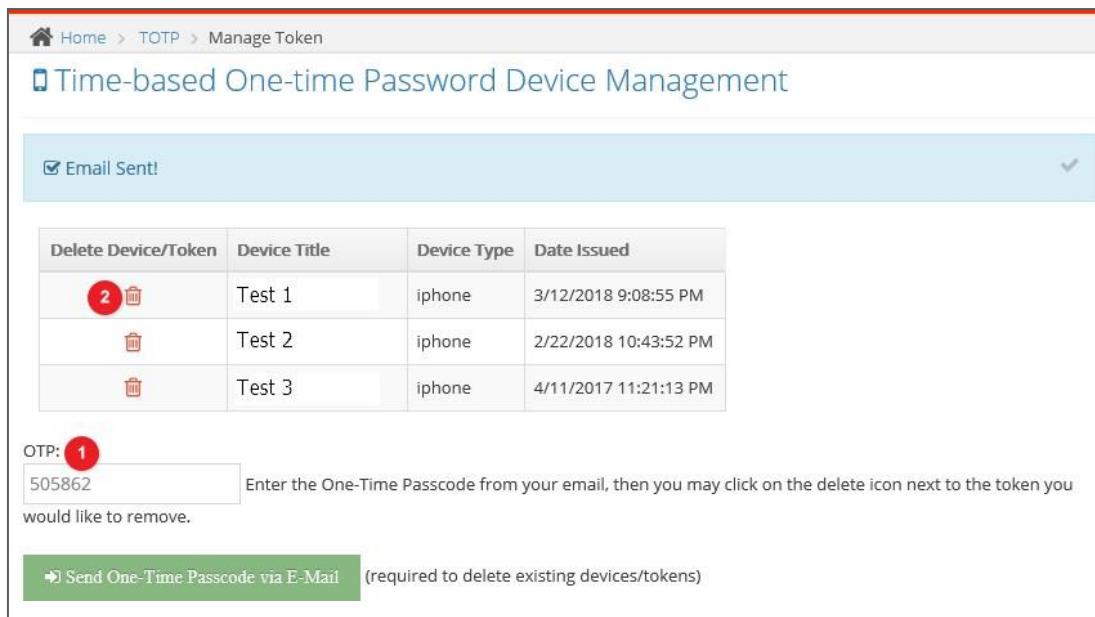




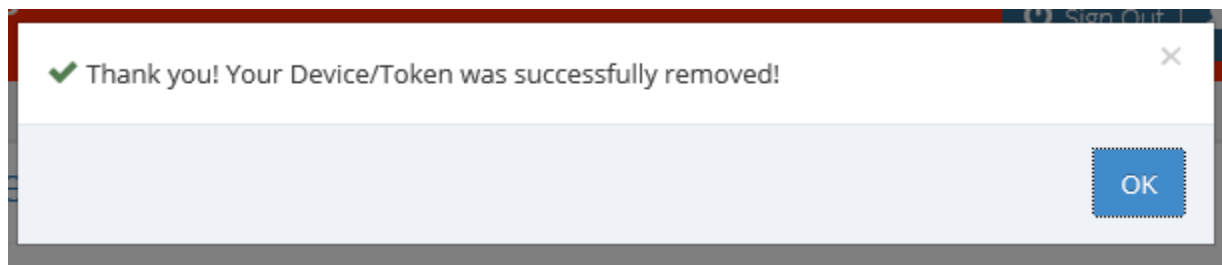
- Luego presione Send One Time Passcode via E-mail



- Ingrese la OTP y haga clic en el ícono del basurero al lado del dispositivo que desea borrar



- Recibirá un mensaje de confirmación cuando el dispositivo haya sido borrado con éxito





## 2. Soporte

### 2.1 Información de Contacto

Para solucionar los problemas de ingreso con Claves de Uso Único, contáctese con el Centro de Servicios IS&T en [istsc@Bechtel.com](mailto:istsc@Bechtel.com).

Puede encontrar Información de Contacto adicional para el Centro de Servicios IS&T haciendo clic en el botón verde “**Click here for Help**” que se ve en la página de ingreso.



Al hacer clic en este botón se abrirá una ventana nueva con la Información de Support Contact

