

**PAL and PAL Admin
Multi-Factor Authentication (MFA)
User Guide**

Table of Contents

About PAL Multi-Factor Authentication	1
OTP via SMS Authentication/Voice Call	2
Register Device on First Sign-In.....	3
Reset OTP Device from Sign-In Page.....	8

About PAL Multi-Factor Authentication

FIS provides multi-factor authentication (MFA) in PAL to keep your Sign Ins secure and prevent unauthorized users from accessing your PAL account.

MFA is a security process that prompts a user for additional methods of identification to verify the user's identity during Sign-In. MFA requires a user to provide not only Sign-In credentials (username and password) but to submit a second form of authentication during Sign-In.

If one factor is compromised, the additional factor is not easy for a hacker to obtain or duplicate.

PAL facilitates the following MFA methods:

- Short Message Service (SMS) authentication which delivers a one-time password (OTP) via text message.
- Voice Call which delivers a spoken OTP via the phone.

OTP via SMS Authentication/Voice Call

The OTP is sent through Short Message Service (SMS) authentication via a text message to a registered mobile phone. Alternatively, users can also receive an OTP via Voice, where the password is received through a call on the user's registered phone number.

Register Device on First Sign-In

Note – Please clear browser cache before first login.

You can register your mobile number during first sign in to PAL, so you can receive the OTP (via either SMS or Voice Call) on the registered mobile number going forward.

1. Enter User ID and click **Proceed**.

* User ID

Trouble signing in?

2. Enter **Password**.

User ID SHIV

* Password

Trouble signing in?

3. Click **Sign In**. The following screen will appear for you to add the device.

4. Click **Add a New Device**.

i Your Out-of-Band PIN Device is the delivery destination where you will receive time-limited passcodes (PINs) during the login process. The same device will also be used for Trouble Signing In. When prompted to enter your PIN, you will use that device to retrieve your PIN.

Select your Out-of-Band PIN device

 Test Device

+ Add a New Device

Cancel

Proceed

5. Click **OK**. The following screen appears for you to complete the device details fields.

Add a New Device x

* Device Name:

Device Profile:

SMS Text ▼
SMS Text
Voice Callback

* Route to Number:

*Format: +(Country Code)(Mobile Number)
e.g. +18005551212*

Cancel

OK

6. Complete the device detail fields.

- Assign a Device Name. You can enter any text such as Mobile, MyMobile, etc.
- Select one of the Device Profile options.
- Enter the Route to Number. This is the Mobile number in +(Country Code) (Mobile Number) format, e.g. +18005551212.
- Click OK

Add a New Device



* Device Name:

Cell

Device Profile:

SMS Text

* Route to Number:

+18005551212

*Format: +(Country Code)(Mobile Number)
e.g. +18005551212*

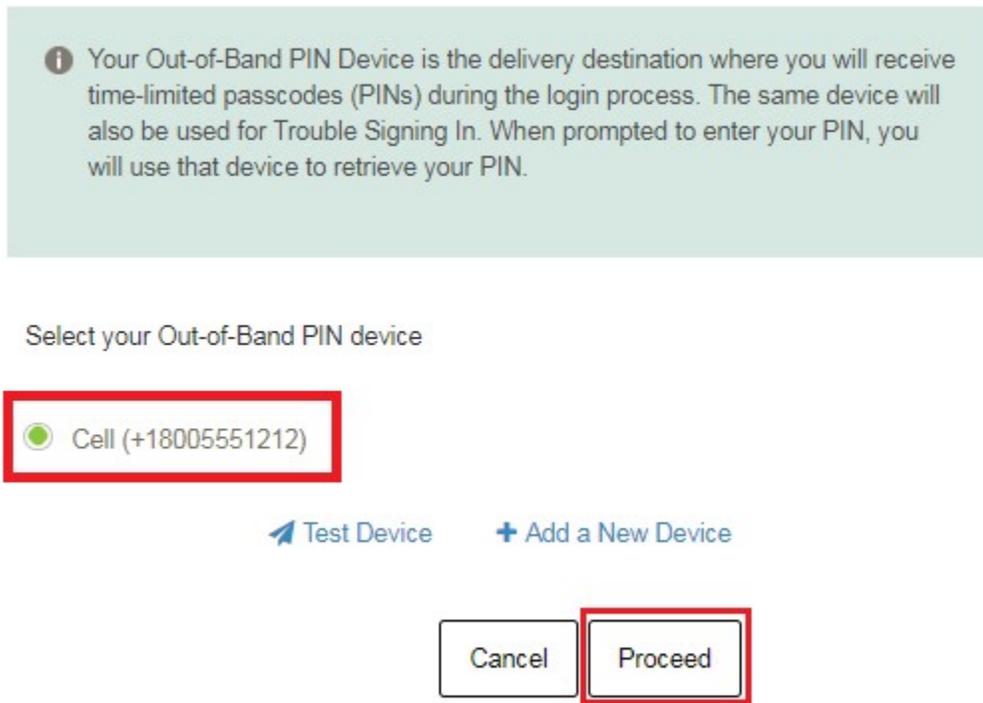
Cancel

OK

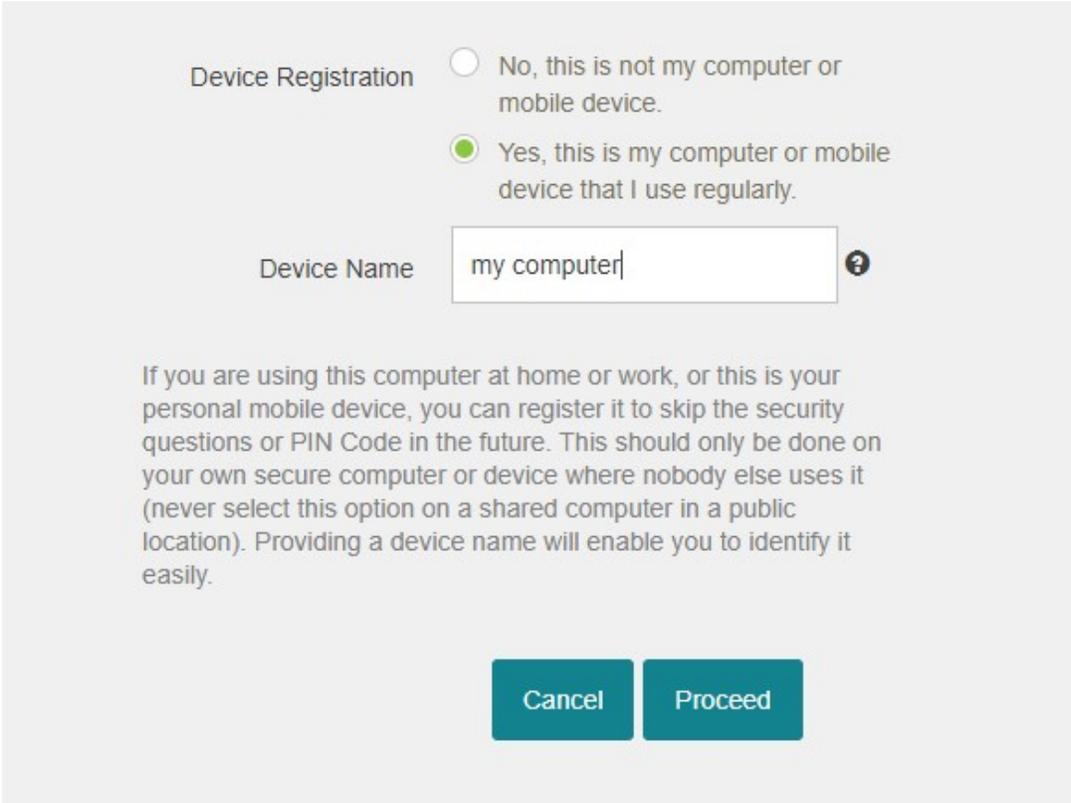
7. Test the device by selecting your Out-of-Band Device and click **Test Device**.



8. Click Proceed to log in



To avoid having to enter a PIN on the next login, select Yes, this is my computer. If you are using a public computer, do not select this option.



The screenshot shows a 'Device Registration' form. It has two radio button options: 'No, this is not my computer or mobile device.' (unselected) and 'Yes, this is my computer or mobile device that I use regularly.' (selected). Below the options is a text input field labeled 'Device Name' containing the text 'my computer|'. To the right of the input field is a small question mark icon. Below the input field is a paragraph of explanatory text: 'If you are using this computer at home or work, or this is your personal mobile device, you can register it to skip the security questions or PIN Code in the future. This should only be done on your own secure computer or device where nobody else uses it (never select this option on a shared computer in a public location). Providing a device name will enable you to identify it easily.' At the bottom of the form are two buttons: 'Cancel' and 'Proceed'.

Once registration process is complete, the PAL dashboard appears. For subsequent Sign-Ins, OTP via SMS or Voice Call is sent to this registered number when required.

Reset OTP Device from Sign-In Page

You can reset your OTP device from the PAL Sign-In page. For instance, if you want to change the mobile number used for OTP delivery.

1. Click **Trouble Signing In?** link.

* User ID

The following screen appears for you to select your issue.

2. Select **I have problems with the One-Time-PIN** and enter your **Sign-In ID**.

Please select your issue:

I forgot my password.

I have problems with the One-Time-PIN.

Enter the email address, username or alias that you use to sign in.

3. Click **Proceed**.

The following screen appears for you to select your problem.

4. Select **I want to reset my One-Time-PIN device** and enter your **Sign-In password**.

Select your problem:

I don't know my One-Time-PIN device.

I want to reset my One-Time-PIN device.

Password

.....

Cancel

Proceed

5. Click **Proceed**.

The following message appears notifying you that an OTP device reset link was sent to the registered email address.

6. Click **OK**.

Thank you. A temporary One-Time-PIN device reset link has been sent to your registered email address.

OK

- 7. Click the link in the email received to reset the device.

Dear SHIV P,

You have recently requested to reset your One Time PIN device. To reset your device , click the link below:

<https://login2-uat.fisglobal.com/idp/TRTAXWL/otpdevice.reset?loginName=14-Mar-2019%3APE1c3NhZ2U%2BPETleT4%3DQLGvO50s%2F%2FUBzNmbJbST84ujoworBII6BpZPPgrBhd4B8AObMenxXm3vq1tYceGHnMqhm%2FEhOT%2FTHMVLwD02y3swT2QnTP99XZnM4YjhDu%2F95YeaLQGgQwSsktb6YY3cDirmVF6KzM8MOaEUQxadxabJSBbHGIIJgGlx1Z9MczSa7wl2nMtWFm%2BQRNtI5TVBzGhZy11DmyOlgGOIVOH2AC8wT39WRIB7t9Jm8jEZ%2Bknp48Scizj8NcEI24q1dObUCIbM4wIORIuMis06ynrU%2B%2F0%2B8XzeWUBHX655w4aspqj1%2FVmLg4f2LOK1BGjfMibdgvkQT0HvxRMxne4BgdPUQ%3D%3DPC9LZXk%2BPEXvZz4%3DUb3n6gs6hFORo0ar1vusMQ%3D%3DPC9Mb2c%2BPEFsZ28%2BQUVTPC9BbGdvPg%3D%3DPC9NZXNzYwdlPg%3D%3D&token=14-Mar-2019%3APE1c3NhZ2U%2BPETleT4%3DaG%2BfuAMCBITkBbw2ppC5YCRCPXbWOHDMUFhra6GvsPYKWecYirZFqywFMHrSckfFYuEpd4E1DQXmKl4wzjMc6mRlw2k8xero8bi9nFyit57cAXUX8halCyGtYXp7rgCfAQQ3McL1CP%2F4JudtPNBRjdD13JpqqdRbHOQE%2FetCz5LQ6%2FwiDahOBOKZrg7IlgV%2FZLGPcrfag3XhbhmPayCthz4tc4eoJqwOoeAXqCDPnnCjXDej1IMcw9Oy5fb8NdbzrfvpOqouta4b0ySyBYwkUiWU3ZcCa3h%2FOA5hITDfFogwSR008Gr%2BM9i5UjgubCJgOYJ%2F1RIZnB6lOrpcUm6XQ%3D%3DPC9LZXk%2BPEXvZz4%3DMgQRi%2FpjpCsiSmgTa6wnQQ%3D%3DPC9Mb2c%2BPEFsZ28%2BQUVTPC9BbGdvPg%3D%3DPC9NZXNzYwdlPg%3D%3D&QueryStringParameter=&ClientID=TrustUI&userName=xxxx>

This link will only be available for 2 hours from the time this email was sent.

If you did not request this or need assistance, please contact your site administrator. If you do not wish to have your One Time PIN device reset, do not click the link above, and your current selection will not be affected.

-----This is a system generated alert. Please do not reply to this message-----

- 8. The PAL Sign-In page appears, enter **Password**.

User ID SHIVP

* Password

Trouble signing in?

- 9. Click **Sign In**. The following screen appears for you to reset your OTP device.

10. Select already added device or add new device. If adding a new device, follow steps shown in the First Sign In section above.

i Your Out-of-Band PIN Device is the delivery destination where you will receive time-limited passcodes (PINs) during the login process. The same device will also be used for Trouble Signing In. When prompted to enter your PIN, you will use that device to retrieve your PIN.

Select your Out-of-Band PIN device

Cell (+18005551212)

[↗ Test Device](#)

[+ Add a New Device](#)

Cancel

Proceed

11. Click **Proceed**. PAL dashboard page appears.