

WebLink Multi-Factor Authentication (MFA) User Guide and Registration Process

Table of Contents

About WebLink Multi-Factor Authentication (MFA).....	1
Accessing WebLink.....	1
OTP via SMS Authentication/Voice Callback.....	2
Register Device on First Sign-In.....	2
Subsequent Login Instructions	7
Forgot your password?.....	8
Resetting your OTP device from the User Login page.....	10
Steps to follow when you “Don’t know your One-Time-PIN device”	12
OTP via the FIS Authenticator Application.....	14
FIS Authenticator App Mobile Phone Version	14
FIS Authenticator App Desktop Version.....	19

About WebLink Multi-Factor Authentication (MFA)

WebLink uses multi-factor authentication (MFA) to keep your login secure and prevent unauthorized users from accessing your account(s).

MFA is a security process that will prompt you for an additional method of identification to verify your identity during the User Login process. MFA requires you to provide not only Login credentials (User ID and password) but to submit a second form of authentication during Login.

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

WebLink allows the following three MFA methods to receive your One-time PIN (OTP)

- Short Message Service (SMS) authentication which delivers an OTP via text message.
- Voice Callback authentication which delivers a spoken OTP via your mobile or land device.
- FIS Authenticator application which can be loaded to your mobile phone or installed on your computer. It's another way to verify your identity and get an OTP on the fly without the need for a network or cellular connection.

Accessing WebLink

Go to [First Mid Bank & Trust | Homepage](#)

Hover over Wealth Management

Click on Trust Services Login

The screenshot shows the First Mid Bank & Trust website navigation menu. At the top left is the First Mid logo. To the right are icons for location and search, a dropdown menu for "CHOOSE ANOTHER LOGIN", and buttons for "Personal" and "Business" under the heading "LOG IN TO ONLINE BANKING". Below this is a horizontal navigation bar with categories: PERSONAL BANKING, COMMERCIAL BANKING, MORTGAGE, INSURANCE, AG SERVICES, WEALTH MANAGEMENT, and ABOUT FIRST MID. The WEALTH MANAGEMENT category is expanded, showing a list of services: TRUSTS (About Trusts, Revocable Living Trusts, Charitable Trusts, Directed Trusts, Life Insurance Trusts, Special Needs Trusts, Estate Administration, Meet our Trust Representatives), FARM SERVICES (Farmland Sales & Auctions, Farm Management, Real Estate Appraisals), INVESTMENT SERVICES (About Investment Services, Charitable Investments, Education Planning, Asset Management, Investment Strategies, Financial Planning, Meet our Financial Advisors), RETIREMENT PLANNING (Personal Retirement Planning, Employer Retirement Services), and LEARN MORE (About First Mid Wealth Management, Wealth Management Locations, Financial Advisor Opportunities, Personal Document Locator, Scholarship Applications, WebLink 3.0 User Guide, Trust Services Login).

On the WebLink login screen, enter the login credentials provided by your system administrator.

Note: For security purposes, you must login to WebLink within 10 days of receiving your login credentials. Additionally, login every 90 days to keep your access active. Inactivity will cause your access to be systematically disabled and you will be forced to resubmit your access request to your system administrator.

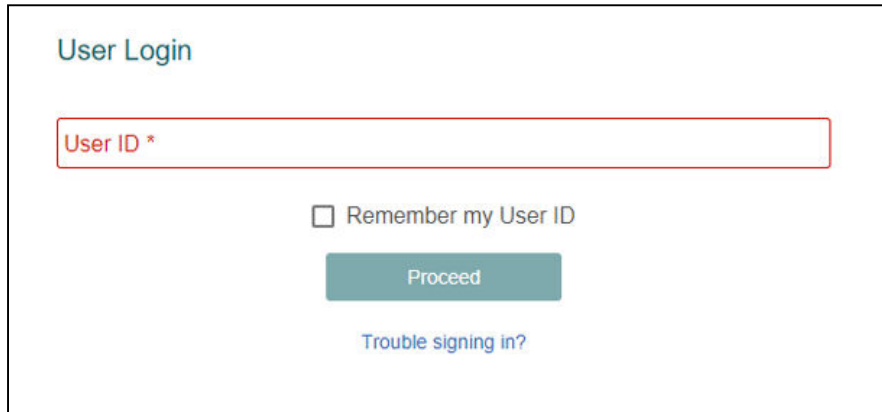
OTP via SMS Authentication/Voice Callback

Register Device on First Sign-In

NOTE: Please clear browser cache before first login.

Step 1 - User Login – User ID

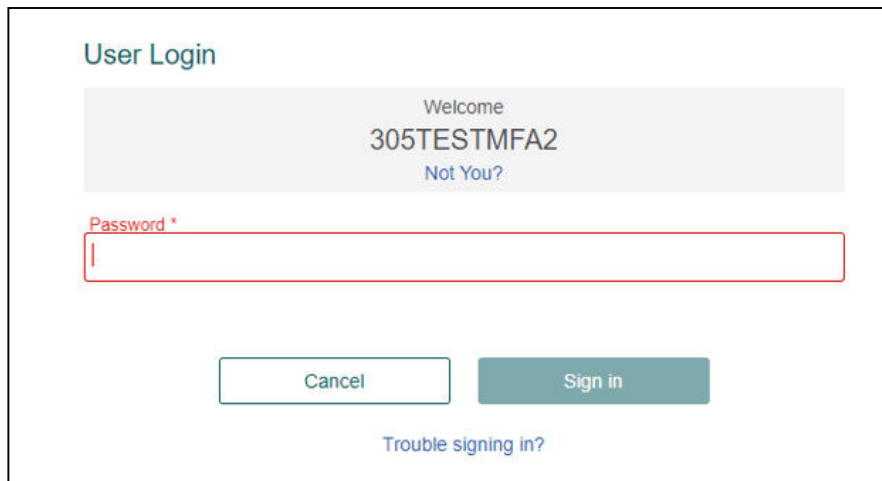
Enter **User ID** and click **Proceed**.



The screenshot shows a 'User Login' form. At the top left is the title 'User Login'. Below it is a text input field with the label 'User ID *'. Underneath the input field is a checkbox labeled 'Remember my User ID'. Below the checkbox is a teal button labeled 'Proceed'. At the bottom of the form is a blue link labeled 'Trouble signing in?'.

Step 2 – User Login – Password

Enter **Password** and click **Sign In**. This is the **temporary password** received from your system administrator.



The screenshot shows a 'User Login' form. At the top left is the title 'User Login'. Below it is a grey rectangular box containing the text 'Welcome 305TESTMFA2' and a blue link 'Not You?'. Below this box is a text input field with the label 'Password *'. At the bottom of the form are two buttons: a white button labeled 'Cancel' and a teal button labeled 'Sign in'. Below the buttons is a blue link labeled 'Trouble signing in?'.

Step 3 - Change Password

The next step is to change your **temporary password**. The **Old Password** is the **temporary password** sent to you by your system administrator. This is the same password you entered on the previous screen.

You will now need to choose a new password by following the Password Rules shown in the blue box at the top of the screen.

Click **Proceed** after you have entered the Old Password field, the New Password field and the Confirm New Password field. On the screen, you will be notified if the new password you have chosen is strong and if the values you entered in the “New Password” and “Confirm New Password” fields match.

First screen before your passwords are entered:

Change Password

i This page allows you to update your password.
The following rules apply when changing passwords:

Passwords must contain at least 8 characters, one uppercase character, one lowercase character, one number and one special character (!@#%&^*()_+}{":;"/><.,).
The new password must be different from the last 10 previously created password or passwords.
The new password cannot contain your Login Name, in forward or reverse order.
The new password cannot contain your first, middle or last name, in forward or reverse order.

Old Password: *

New Password: *

Confirm New Password: *

Screen after your passwords are entered:

Change Password

i This page allows you to update your password.
The following rules apply when changing passwords:

Passwords must contain at least 8 characters, one uppercase character, one lowercase character, one number and one special character (!@#%&^*()_+}{":;"/><.,).
The new password does not meet the defined password criteria.
The new password must be different from the last 10 previously created password or passwords.
The new password cannot contain your Login Name, in forward or reverse order.
The new password cannot contain your first, middle or last name, in forward or reverse order.

Old Password: *

New Password: *

Confirm New Password: * Strong

Step 4 - Select OTP method

As detailed on page 1, you must choose the MFA method to receive your one-time pin (OTP). To have a PIN sent to your mobile phone, click on **Send PIN to my phone** and then on **Add a New Device**.

Note: If choosing to use a software app, refer to the FIS Authenticator Application detailed later in this document.

Two options are available when choosing to receive your OTP on your mobile phone. You will need to choose **ONE** of the two options:

- SMS/Text Message to your mobile phone
- Voice Callback (to your mobile phone or house phone)

Step 5 - Add a New Device

The following screen appears for you to complete the device detail fields. Complete the fields and click **Save**.

- **Device Name** - You can enter any text e.g. Mobile, My Mobile, etc.
- **Device Profile** - choose either SMS Text or Voice Callback
- **Country Code** – select the Country Code from the drop-down list provided
- **Mobile Number** – enter your Mobile number; enter as: 2165551212; no spaces are needed.

Keep in mind, some countries may have restrictions and block incoming calls. For example, China is one of the most restrictive locations globally regarding receipt of international SMS. They are known to block most messages, even if they are financial-related.

We cannot be responsible if messages are not making it to users in countries that employ blocking technology.

Step 6 - Select OTP Device

Click on the radio button beside the mobile number and click on **Proceed**.

Select OTP method

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

Send a PIN to my phone

Let me use a software app

Select OTP Device

Test Device + Add a New Device

Step 7 – Validate your One-Time-PIN setup

Enter the **OTP code** received either as a text message or through the voice callback feature and click on **Validate OTP**. After entering the OTP code, you will gain access to WebLink.

Note: The OTP texted to your mobile phone will be either an alphabetic code that must be entered in uppercase letters when logging into WebLink or a sequence of numbers. The voice callback that you receive may come over as Spam. There will be a recording saying: “This is your bank. Your one-time pin code is xxxxxx (a six digit code will be supplied at this time). Press 1 to repeat this message or hang up the phone.”

Validate your One-Time-PIN setup

i An OTP code has been sent to your mobile device ****2513**. Please enter it below to complete the OTP device registration process.

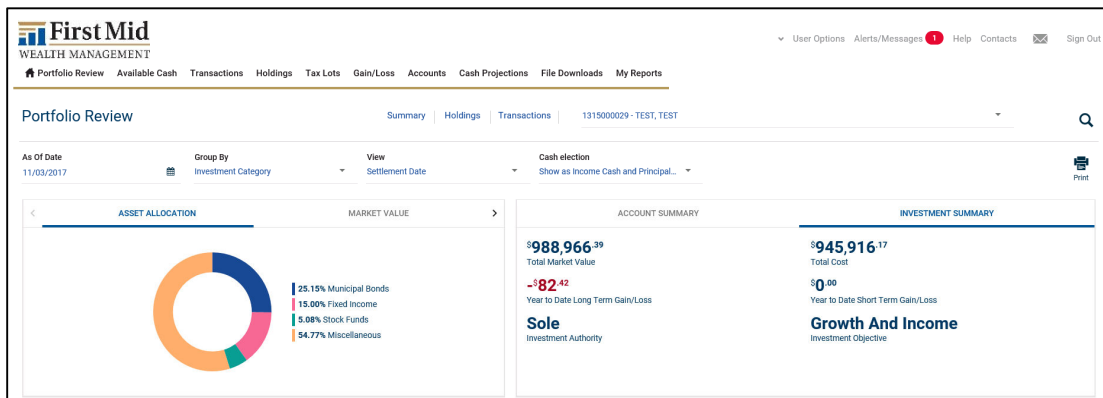
OTP Code *

If you did not receive the OTP code, please wait a minute or try reconfiguring your device.

Cancel
Validate OTP

[Reconfigure OTP Device](#)

You are now successfully logged into WebLink. The WebLink Portfolio Review report is displayed. All subsequent logins will now prompt you to enter a PIN code. You must enter the PIN code retrieved from your mobile device and click **Sign In**.

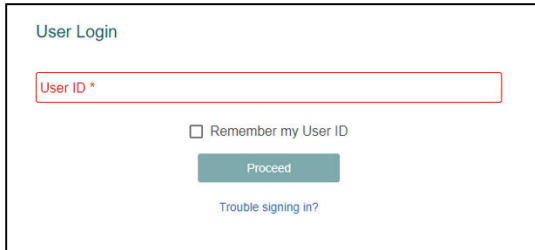


Subsequent Login Instructions

Step 1 – Initial log in screen – User ID:

Enter your **User ID** and hit **Proceed**.

Note: All passwords are case sensitive.



User Login

User ID *

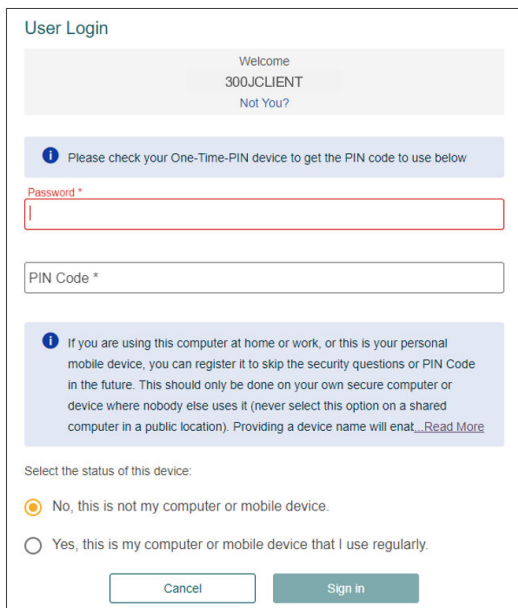
Remember my User ID

Proceed

[Trouble signing in?](#)

Step 2 – Password and PIN Code:

Enter your **Password** and the **PIN Code** (OTP) received via text message, voice callback or the FIS Authenticator app and click on **Sign in**.



User Login

Welcome
300JCLIENT
Not You?

Please check your One-Time-PIN device to get the PIN code to use below

Password *

PIN Code *

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 enat...[Read More](#)

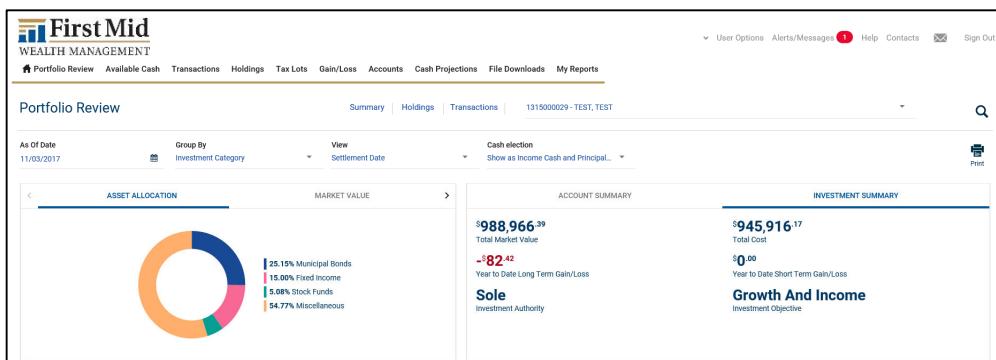
Select the status of this device:

No, this is not my computer or mobile device.

Yes, this is my computer or mobile device that I use regularly.

Cancel Sign in

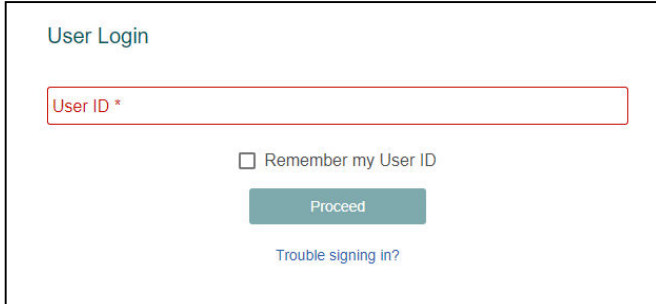
You are now successfully logged into WebLink. The Portfolio Review report will be displayed.



Forgot your password?

Step 1 – User Login:

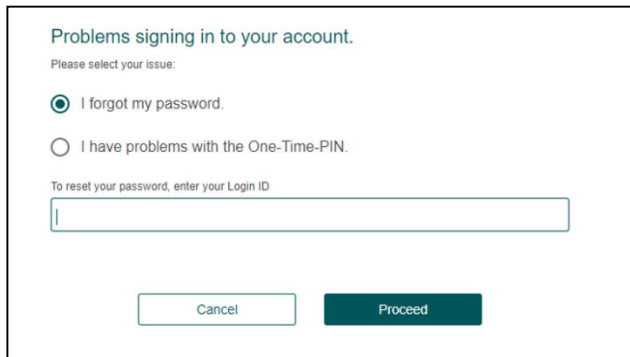
Click the “**Trouble signing in?**” link.



The screenshot shows a 'User Login' form. It features a text input field labeled 'User ID *'. Below the field is a checkbox labeled 'Remember my User ID'. A teal 'Proceed' button is centered below the checkbox. At the bottom of the form, there is a blue link that says 'Trouble signing in?'.

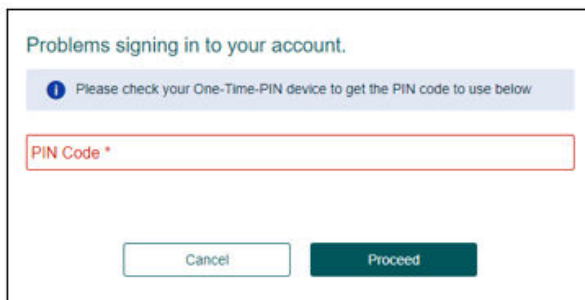
Step 2 – Problems signing in to your account:

Click on the radio button beside “I forgot my password” and enter your **User ID** (Login ID) then click on **Proceed**.

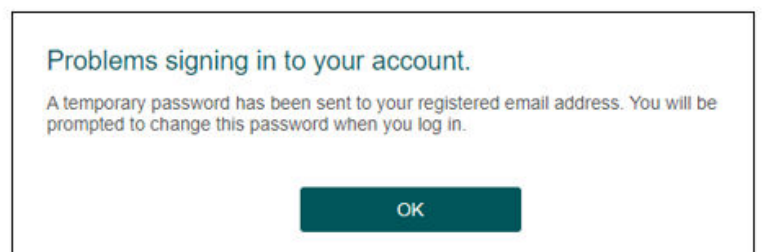


The screenshot shows a 'Problems signing in to your account' form. It asks the user to 'Please select your issue:' with two radio button options: 'I forgot my password.' (which is selected) and 'I have problems with the One-Time-PIN.'. Below the options, it says 'To reset your password, enter your Login ID' followed by a text input field. At the bottom, there are 'Cancel' and 'Proceed' buttons.

Enter your PIN Code (OTP) received via text message, voice callback or the FIS Authenticator app and click on **Proceed** and then **OK**.



The screenshot shows the 'Problems signing in to your account' form with a blue information banner at the top that says 'Please check your One-Time-PIN device to get the PIN code to use below'. Below the banner is a text input field labeled 'PIN Code *'. At the bottom, there are 'Cancel' and 'Proceed' buttons.

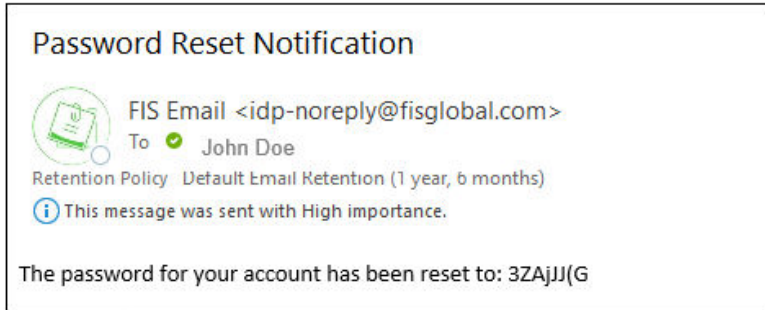


The screenshot shows a confirmation message: 'Problems signing in to your account. A temporary password has been sent to your registered email address. You will be prompted to change this password when you log in.' Below the message is a teal 'OK' button.

Step 3 – Password Reset Notification:

You will receive a “Password Reset Notification” email, from idp-norply@fisglobal.com, which will provide you with a temporary password. Use this temporary password the next time you log into WebLink and you will be instructed at that time to setup a new password.

Note: *If you do not see this email, please check your spam folder.*



Resetting your OTP device from the User Login page

Step 1 – User Login

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

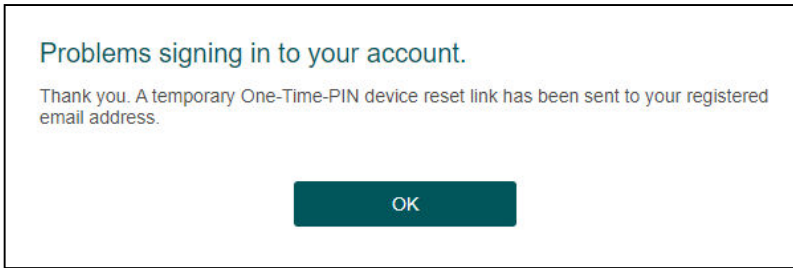
Step 2 – Problems signing in to your account:

Click on the radio button beside **“I have problems with the One-Time-PIN”** and enter your **User ID** (Login ID) then click on **Proceed**.

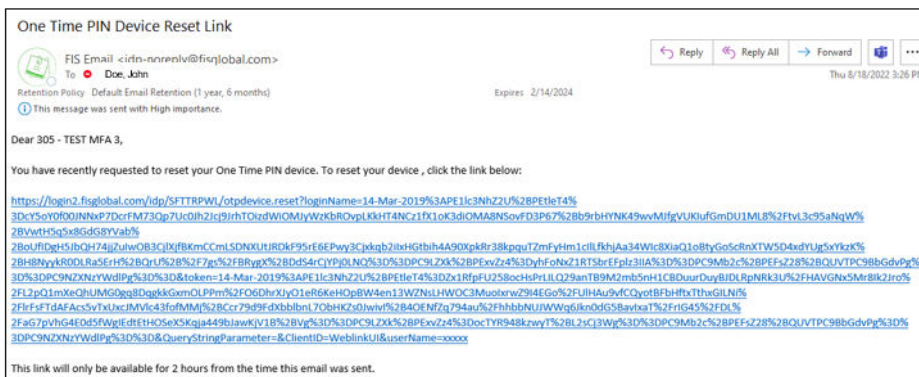
The following screen appears for you to select your problem. In this example, select **“I want to reset my One-Time-PIN device”**, enter your **Password** and click **Proceed**.

FIS Authenticator and OTP via SMS

The following message appears notifying you that an OTP device reset link was sent to your registered email address. Click **OK**.

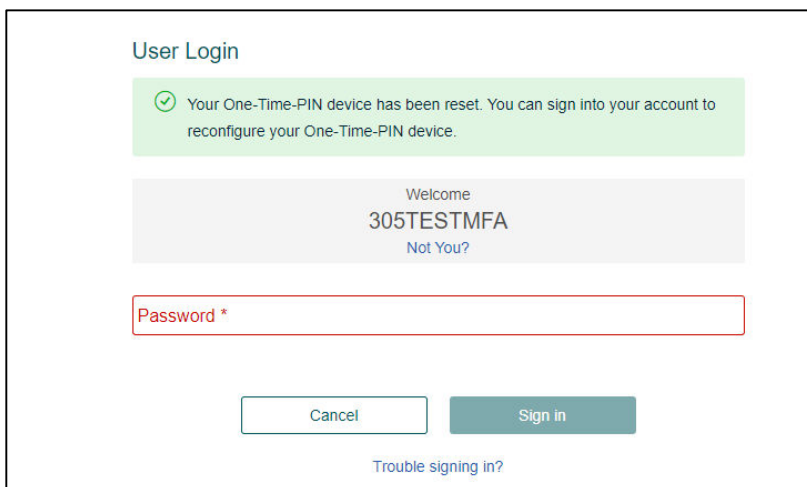


You will receive a “One Time PIN Device Reset Link” email, from ldap-norply@fisglobal.com, which will provide you with a link to reset your OTP device.



Step 3 – User Login:

Now you are able to reset your One-Time-PIN device. Enter your **Password** and click on **Sign In**.



Step 4 – Complete the process to reset your One-Time-PIN device

Follow the steps outlined earlier in this document to setup your OTP device either using the SMS/Voice Callback method or the FIS Authenticator app.

Steps to follow when you “Don’t know your One-Time-PIN device”

Step 1 – User Login:

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

User Login

User ID *

Remember my User ID

Proceed

[Trouble signing in?](#)

Step 2 – Problems signing in to your account:

Click on the radio button beside “**I have problems with the One-Time-PIN**” and enter your **User ID** (Login ID) then click on **Proceed**.

Problems signing in to your account.

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.

Cancel Proceed

The following screen appears for you to select your problem. In this example, select “**I don’t know my One-Time-PIN device**”, enter your **Password** and click **Proceed**.

Problems signing in to your account.

Select your problem:

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

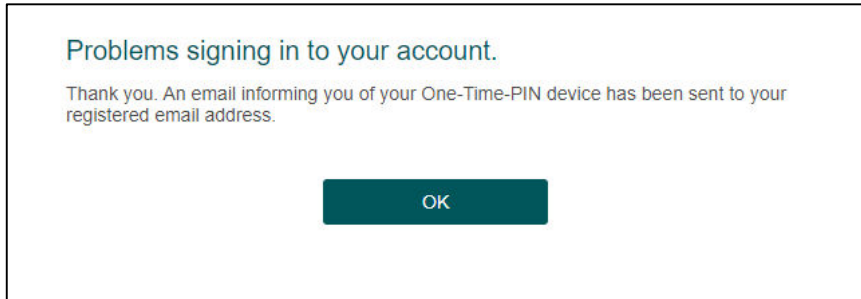
I want to reset my One-Time-PIN device.

Password *

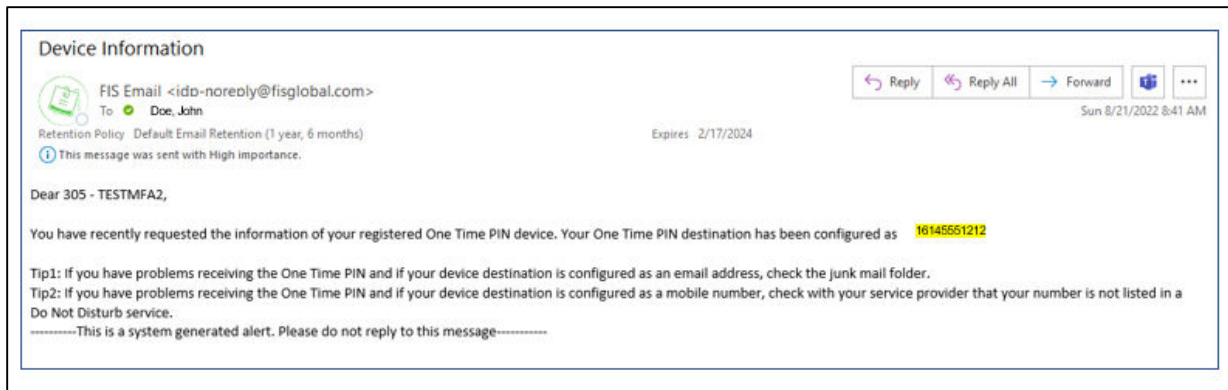
Cancel Proceed

FIS Authenticator and OTP via SMS

The following message appears notifying you that an email informing you of your One-Time-PIN device has been sent to your registered email address. Click **OK**.



The “Device Information” email message provides you with the phone number that has been registered as your One-Time-PIN device. Tips are also provided as to why you may not be receiving your OTP.



Step 3 – User Login:

Now that your registered device has been identified, proceed to the User Login screen and follow the steps to complete the login process.

OTP via the FIS Authenticator Application

The FIS Authenticator app can be set up to send an OTP to your mobile phone using the Android or iOS (Apple) operating system. It provides second-factor authentication for registered users and is also available as a desktop-friendly version.

Using the FIS Authenticator app is an even more secure method because it does not utilize your phone/data carrier to transmit access codes. The app codes also expire in 30 seconds; another measure that increases security.

FIS Authenticator App Mobile Phone Version

To install the FIS Authenticator on your Mobile phone, first login to WebLink as outlined below.

Step 1 - User Login – User ID

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

The screenshot shows a web form titled "User Login". It features a text input field labeled "User ID *". Below the field is a checkbox labeled "Remember my User ID". A teal "Proceed" button is centered below the checkbox. At the bottom of the form, there is a blue link that says "Trouble signing in?".

Step 2 – User Login – Password

Enter **Password** and click **Sign In**.

Note: If this is the first time you are logging into WebLink, this is the temporary password received from your system administrator.

The screenshot shows the "User Login" page after the first step. A grey box displays a "Welcome" message with the temporary password "305TESTMFA2" and a "Not You?" link. Below this is a "Password *" input field. At the bottom, there are two buttons: a white "Cancel" button and a teal "Sign in" button. A blue link "Trouble signing in?" is located at the very bottom of the form.

Step 3 – User Login - Password

Complete the login process, creating a new password if needed and setting up a security image. See the detailed instructions provided earlier in this document.

Step 4 - Select OTP method

As explained on page 1, you must choose the MFA method to receive your one-time pin (OTP). To have a PIN sent to an app on your mobile phone, click on **“Let me use a software app”** and then on **“Use a Software Authenticator App”** and click on **Proceed**.

The following screen will appear during first login after you enter your **User ID** and **Password**.

Select OTP method

Send a PIN to my phone

Let me use a software app

Select Token Generator

Use a Software Authenticator App ?

Cancel Proceed

Step 5 – Configure Software Authenticator App

If you already have the FIS Authenticator app installed on your mobile device, choose **“I’ve already installed the app”**. If you need to install the app, choose **“Email me a download link”** and click **Proceed**.

Configure Software Authenticator App

i An Authenticator is a software app installed on your mobile device. You can download the FIS Authenticator app from iTunes or Google Play. Once downloaded, simply open the app and add your account by pointing your mobile device's camera at the QR code shown on next page. Alternatively, you can manually enter the Secret Key.

I've already installed the app

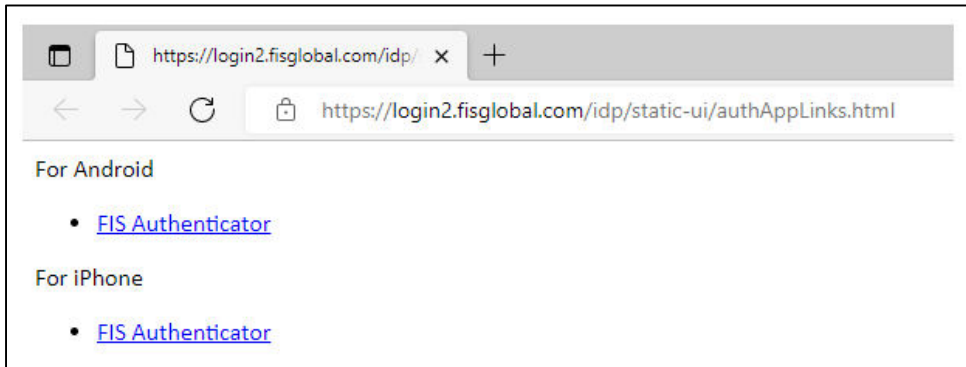
Email me a download link

Back Proceed

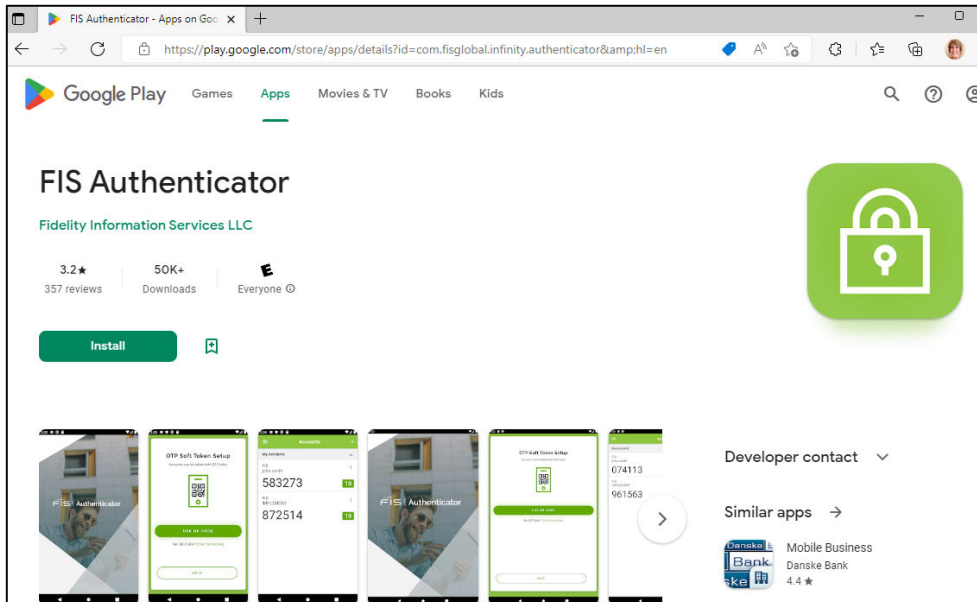
If you selected “**Email me a download link**”, you receive the following email.



Click on the link in the email to open the following page with links for downloading the FIS authenticator.

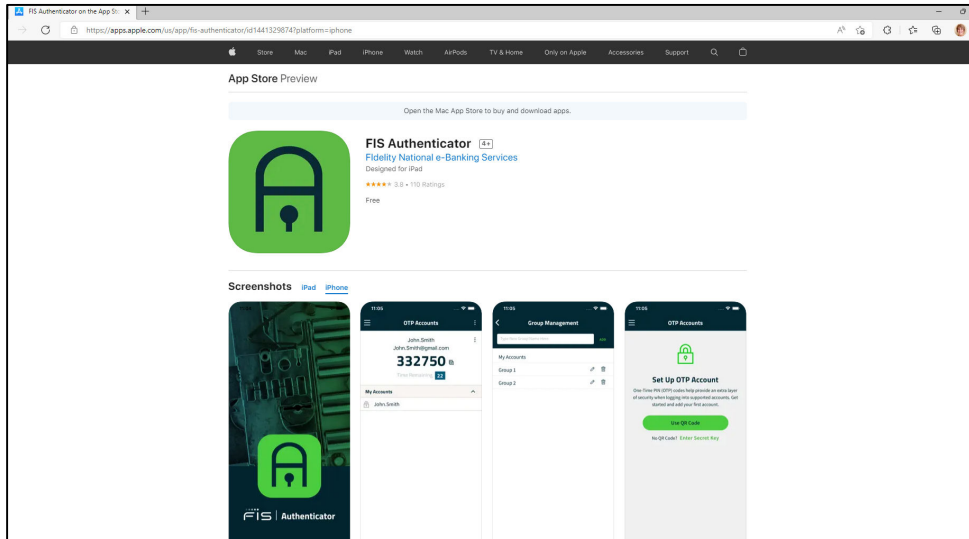


Authenticator for android devices:



FIS Authenticator and OTP via SMS

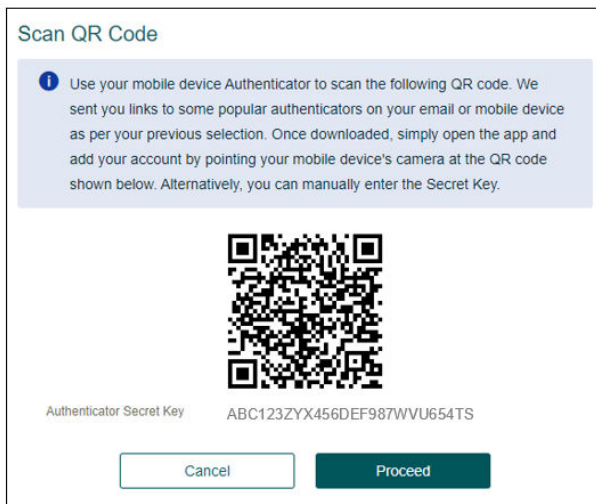
Authenticator for IOS (Apple) devices:



Download the FIS Authenticator on your mobile device and then go back to WebLink to scan in the QR code.

Step 6 – Scan QR Code

The following screen will appear. Open the **Authenticator** app on your mobile device and either scan in the QR code onto your phone by holding your phone up to your computer to scan in the QR code or manually enter the Authenticator Secret Key and click **Proceed**.



Step 7 – Validate your One-Time-PIN setup

Enter the code from your FIS Authenticator app and click on **Validate OTP**.

Validate your One-Time-PIN setup

i Please enter the OTP code generated in the authenticator app to complete the OTP device registration process.

OTP Code *

Cancel Validate OTP

Reconfigure OTP Device

Step 8 – Device Registration

After entering the OTP code, you are able to register your device and then click **Proceed**.

Device Registration

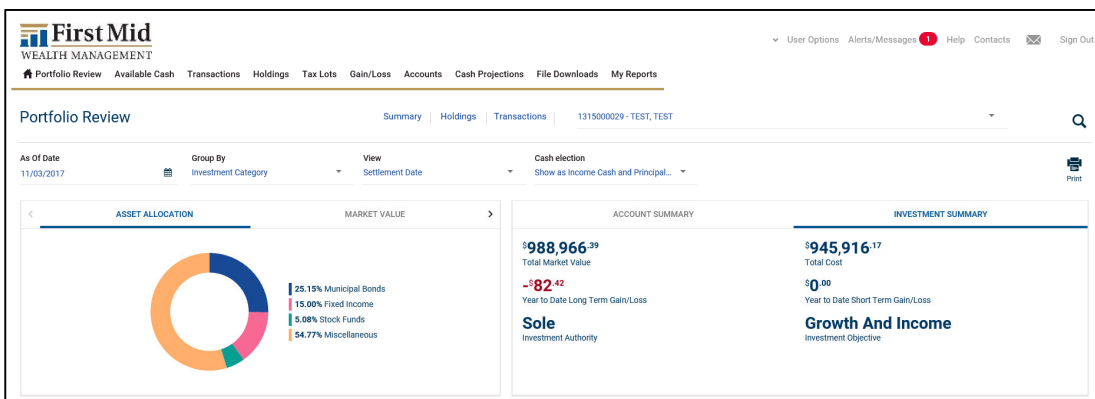
i If you are using this computer at home or work, or this is your personal mobile device, you can register it to skip the security questions or PIN Code in the future. This should only be done on your own secure computer or device where nobody else uses it (never select this option on a shared computer in a public location). Providing a device name will ena...[Read More](#)

No, this is not my computer or mobile device.

Yes, this is my computer or mobile device that I use regularly.

Cancel Proceed

You are now successfully logged into WebLink. The WebLink Portfolio Review report is displayed. All subsequent Logins will now prompt you to enter a PIN. You must enter the PIN generated in Authenticator app and click Sign In.



FIS Authenticator App Desktop Version

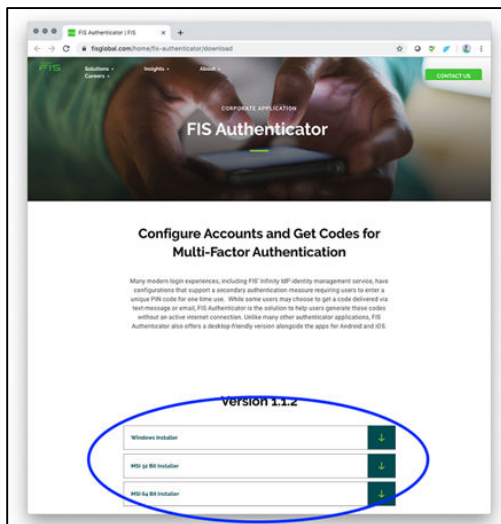
FIS Authenticator for Desktop is available as an alternative to the mobile version to help keep your accounts more secure. This section provides FIS Authenticator installation and configuration guidance for Desktop users.

Open your internet browser, type the URL for WebLink in the URL address field and press **Enter**. As an alternative, you can save the URL in your browser or on your desktop as a shortcut and begin your session by clicking one of these. Some systems may initially display a Security Alert; if so, click **Yes** to proceed.

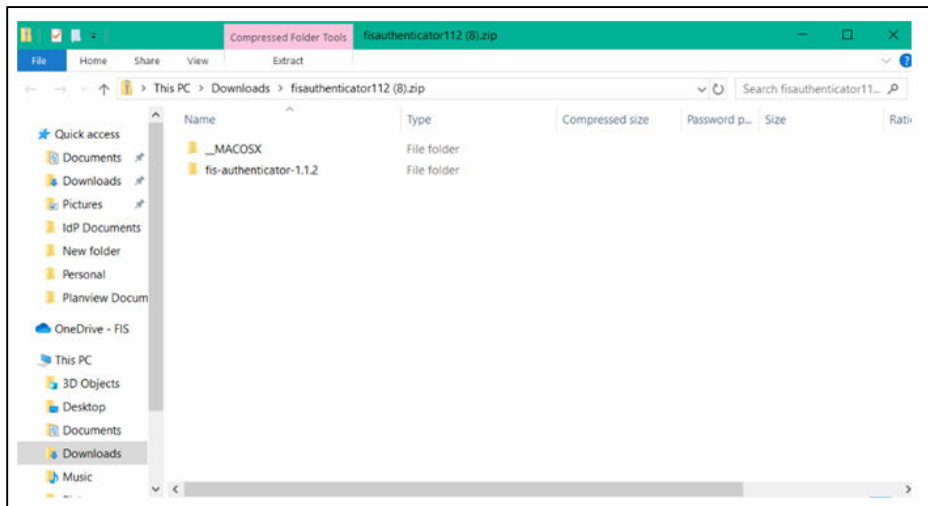
When the Login screen appears, enter your **User ID** and **Password**, then click **Sign-In**. If this is your first session, you will need to change your password as detailed above.

Step 1 - Download the FIS Authenticator for Desktop

From your web browser, go to <https://www.fisglobal.com/home/fis-authenticator/download> to download the **FIS Authenticator** for Desktop. On the FIS Authenticator download page, select the appropriate file to download based on your machine's platform. The version number that appears is the latest available version.

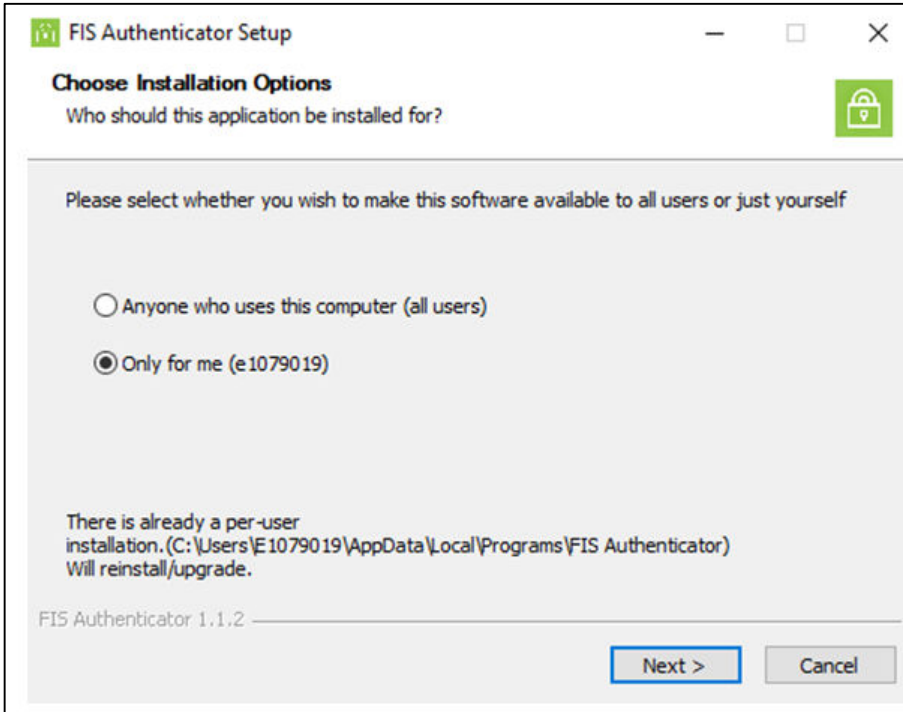


Navigate to the FIS Authenticator .exe file in your Downloads folder.

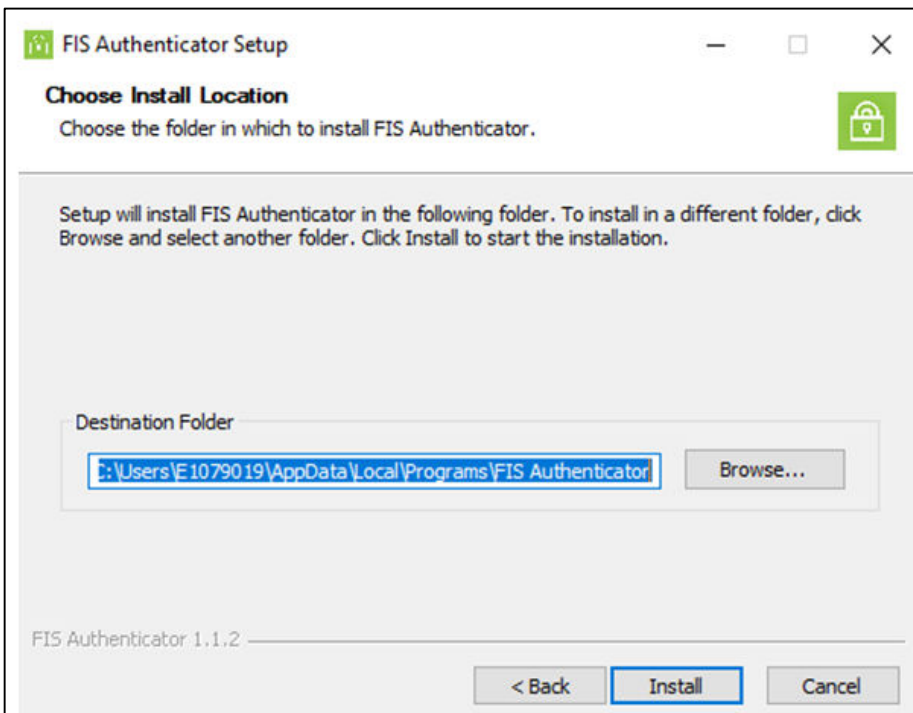


Step 2 - Install the FIS Authenticator for Desktop

Double click the .exe file to install it. The FIS Authenticator Setup wizard appears. Select the **Only for me (User ID/Name)** option and click **Next**.

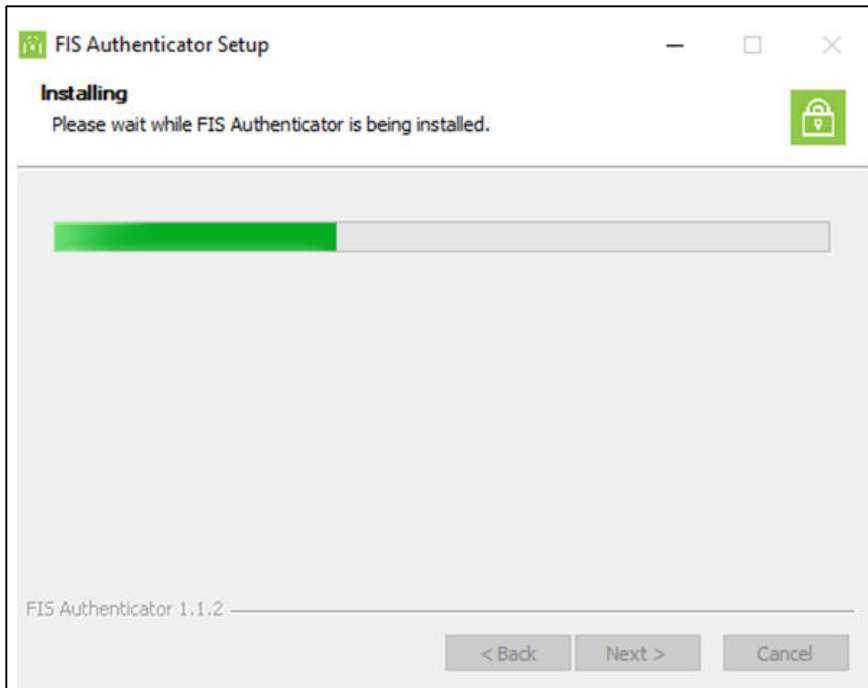


Keep the default **Destination Folder** as the location and click **Install**.

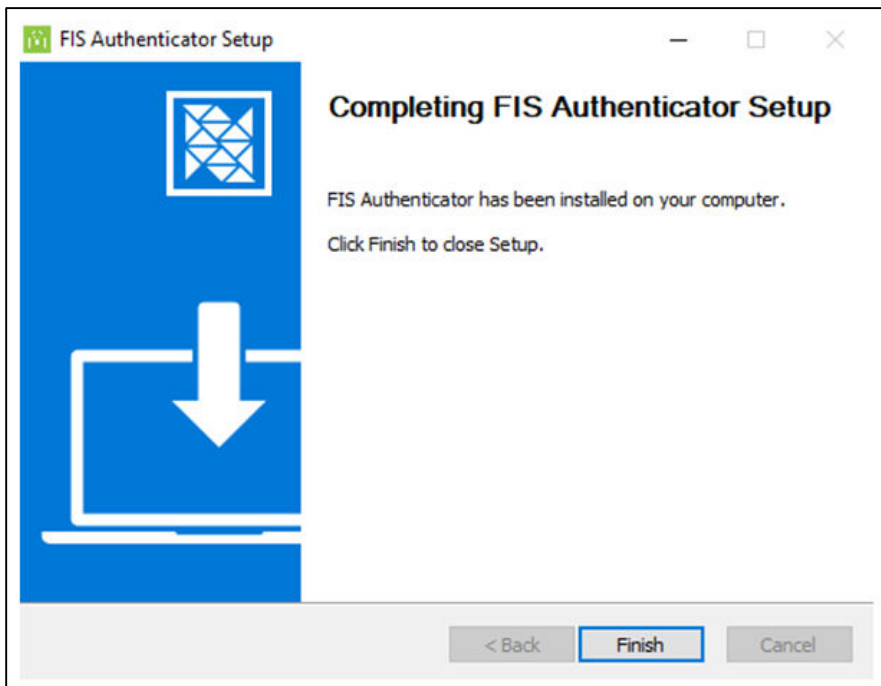


FIS Authenticator and OTP via SMS

NOTE: Installation can take a few minutes to complete.

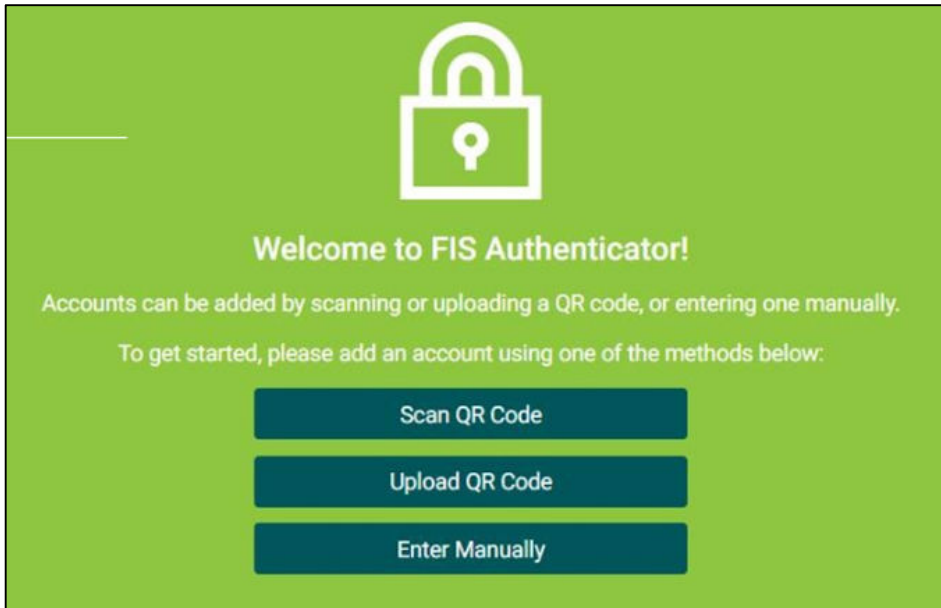


Click **Finish**, once loading process is complete.



Step 3 - Configure FIS Authenticator

Once the **FIS Authenticator** app is installed, open the app on your computer. The FIS Authenticator Welcome Page appears for you to select the method to use to add an account.



Step 4 – Manually add an account to the FIS Authenticator

Click **Enter Manually** (recommended for desktop) to begin the OTP (One-Time-PIN) setup. The Add Account screen appears.

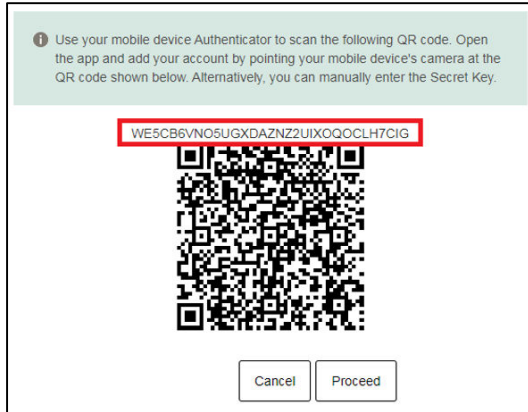
Complete Issuer, Key Code and Username fields and click **Save**.

The Issuer is the name of your banking institution where your WebLink account is being serviced. The Key Code is app-generated and shown above the QR code (see example below). The Username is your WebLink User ID.

VALUABLE information regarding Key Codes:

- The Key Code is a 26-character alphanumeric string that looks like this:
WE5CB6VNO5UGXDAZNZ2UIXOQOCLH7CIG
- It cannot be copied and pasted into the FIS Authenticator app
- All letters are UPPER CASE
- There are no zeros (0) or ones (1) in the Key Code
- Only the following numbers are valid: 2, 3, 4, 5, 6, 7 – **numbers 0,1, 8 and 9 are never used**

FIS Authenticator and OTP via SMS



Once the Add Account step is complete, you will see the Accounts screen and a new PIN code will be generated every 30 seconds to be used for all subsequent sign-ins.

