Midland Wealth Management

Secure Sign In Frequently Asked Questions

What is Secure Sign In?

Secure Sign In is a service to help protect you from fraudulent online activity. We use multiple layers and factors beyond access ID and password before allowing access to your account. If we suspect unauthorized account activity, we will ask for additional authentication before permitting access to your account. Secure Sign In provides you with a secure website, ensuring that only authorized individuals have access to their financial information online.

How does Secure Sign In work?

When you access the site for the first time, using the credentials provided by your financial institution, you are required to change your password, and establish a delivery method to receive your One-Time PIN (OTP). The OTP is available through one of the following:

- SMS Text Message.
- Software Authenticator through a supported app. The supported apps include:
  - FIS Authenticator.
  - Google ™ Authenticator.
  - Microsoft ® Authenticator.
- Voice Callback.

How do I sign in for the first time and establish my OTP method?

The OTP method is established during your initial sign in. If your institution converted from a different Secure Sign In method to Identity Provider (IdP), your first sign in with IdP is treated as your initial sign in.

1. Enter your Access ID and the new password you received via email.
2. After the product has validated your access ID and password, you are required to change your password. Your new password must meet the strong password requirements provided.
3. You are then asked how you would like to receive your OTP. You must select the OTP method from the following choices:
   - Send a PIN to my phone.
   - Let me use a software app.
   - Voice Callback to my phone.
4. You are authenticated into the product after your password has been reset and the OTP method established.

What is the format for my phone number if I choose Send a PIN or Voice Callback to my phone?

When this OTP method is selected, the PIN is delivered only to your phone, as email delivery is not supported for your institution. You need to enter the following:

- Device Name – Provide a name that identifies the device to you. You can register multiple OTP method devices, and the name helps you determine which number is which. This field is required.
- Device Profile – Select either SMS Text or Voice Callback from the drop-down list, only one option is offered. You will not receive a PIN if you do not select a profile option.
- Route to Number – Enter the phone number, using the international format. For example, your US phone number is (888) 555-1212. The number must be entered as +18885551212. You will receive an error if you enter the number in a format other than that provided in the example.

What if I select the authenticator app?

If you choose the authenticator app, you can either install an app in advance, or have a link to an app emailed to you. If you choose the email option, you receive a link to download the FIS Authenticator app. If you have already installed an app, you are prompted to scan the QR Code or manually enter the string of characters above the QR Code provided in your OTP method set up.

Please note that the FIS Authenticator app does not have any account requirement, but if you use the Google Authenticator or Microsoft Authenticator you will need to sign into the app with your Google or Microsoft sign in information.

What happens if I cancel during the Secure Sign In process?

If you do any of the following during the sign in or OTP method set up, the information entered is discarded and you will be required to complete the processes the next time you attempt to sign in.

- Click the Cancel button on any page in the process.
- Are inactive on any of the enrollment pages for an extended period of time.
- Exit your browser window before the final step is completed.

Should I register my device in the Desktop Registration page?

It is recommended that you register your device on the Desktop Registration page. To register your, select Yes, this is my computer or mobile device that I use regularly. IdP remembers your device, and you will not be prompted to authenticate with a PIN on subsequent sign ins. The option is available to enter a Device Name. This is helpful if you want to register multiple devices.

If you do not choose to register your device, you will be prompted to enter a PIN with each subsequent sign in.

Should I register every computer or personal device I use?

The registration is device specific, so we recommend registering each device you regularly use.

Does my device registration expire?

Yes, as a security measure, your device registration periodically expires – generally every 60 days - unless your institution chooses a custom range. When this happens, you will need to enter a PIN when you sign in and have the option to again register the device.

Why am I prompted for a PIN on a device I have registered?

You may be prompted for a PIN on a registered device if the browser or location used on sign in is different than the browser or location used when the device was registered.

Is my PIN case sensitive?

Yes, your PIN is case sensitive. Enter your PIN in the format in which you receive it. However, the PIN is typically all numeric in which case it is not case sensitive.

What can I do to protect my accounts?

You are the first line of defense for your online account security. We have taken numerous steps to keep your accounts secure, but you also play a role in maintaining the security of your account information.

Here is what you can do:

- Never provide your access ID and password to anyone.

- Memorize your password. Your online password authenticates you when you begin an online session. You should memorize this password and never write it down anywhere.
- Create a password that consists of letters, numbers, and/or special characters. It should be a combination that cannot be easily guessed by others.
- Change your password regularly**.** It is important to change your password regularly, which can be accomplished within the product.
- Remember to sign out. You may not always be at your own computer when you access your account. It is important to sign out by clicking the Sign Out link in the top-right corner of the page. If you forget to do so, we automatically sign you off after 15 minutes of inactivity.
- Use your browser's built-in security features. It is recommended that you use the built-in security features that browsers provide. Choosing certain security settings and options will help protect the privacy of your accounts and personal information. To learn how to maximize your online security, review the security features of your web browser.

How often can I change my password?

You may change your password often as needed; however, it is recommended that you make no more than one password change per day.

What can I do if I forget my password or need to change my password?

Use the 'Trouble signing in?' link, and select 'I forgot or need to change my password.' You need to enter your email or access ID and are prompted to also enter a PIN to verify your identity. You will receive an email that includes a link you must use to change your password.

What can I do if I forget my Access ID?

Use the 'Trouble signing in?' link, and select 'I forgot my Access ID.' You then need to enter your email and are prompted to also enter a PIN to verify your identity. An email is sent that includes your access ID.

How can I unlock my account if I have trouble signing in?

Use the 'Trouble signing in?' link, and select 'I think my account is locked.' You need to enter your email or access ID and are prompted to also enter a PIN to verify your identity. You will receive an email that includes a link to unlock your account.

What can I do if I am having problems with my OTP?

Use the 'Trouble signing in?' link, and select 'I have problems with my One-Time PIN.' You need to select one of the following options, and must enter your password to verify your identity:

- 'I don't know my One-Time PIN device.' When selected, an email is sent that includes the detailed information for your OTP device.
- 'I want to reset my One-Time PIN device.' When selected, an email is sent with a link to establish an OTP device. When you use the link, you can either establish a new OTP device, or select one of the devices previously established.

How can I change my access ID?

If you need to change your access ID, contact customer support for assistance.

What can I do if I forget my access ID?

If you have forgotten your access ID, contact customer support for assistance.

What if I have tried all the 'trouble signing in' options and still can't sign in?

If you need additional assistance, contact customer support for assistance.

Do I have to change any Internet browser settings to access the product?

Your Internet browser must be set to accept permanent cookies. Most browsers accept cookies as a default setting. If you have not customized this setting, you should not need to make any changes. If you need to change the Internet cookie setting to accept permanent cookies, follow the instructions provided in the Internet browser's help file. If you do not make the change to accept permanent cookies, you will be able to sign in; however, moving throughout the product will be difficult and may lead to unexpected errors.

Why doesn't my browser's Auto Complete feature pre-fill my password?

Once you set up Secure Sign On, your password will not pre-fill. Secure Sign On uses a process that does not allow your browser to anticipate your password entry. While the Auto Complete feature may be helpful for some things, it can also seriously compromise your security and privacy. If a password is saved in the browser on a public computer, that information is available to others for use or theft.

What security measures are taken to prevent sensitive information from being intercepted online?

From the moment account information leaves your computer to the time it reaches us; all online sessions are encrypted. That means your password as well as all information relating to you and your accounts employ some of the best forms of cryptography that are commercially available for use over the Internet. If for any reason your secure session ends, your online session automatically terminates.

What is Phishing?

Phishing is an Internet fraud technique that is used by criminals to trick you into giving them personal information. Phishing occurs when a criminal sends you an e-mail message with a link to what may appear to be your institution's website but is actually a fake. On this fake website, you will be asked to enter personal information such as your social security number, account number, or credit card number. Phishing is a fraudulent act aimed at stealing your identity and private account information.

Phishers set up a phony website that looks like the site of a trusted company to trick you into disclosing your access ID and password.

What is a cookie?

A cookie is a small text file that a web server can store on a user's computer. The cookie your institution stores on your computer is only used by your institution when you access your account information online. It is not used to track your Internet activity and cannot be used by others to access your information.

Are cookies dangerous to my computer?

No. These websites cannot look at any other cookie or anything else on your machine. The cookie your institution stores on registered computers are only used to ensure that an authorized location is accessing your account information. It is not used to track your Internet activity and cannot be used by others to access your information.

Does anti-spyware and firewall software affect registration of a personal computer?

It is recommended that you use anti-spyware and firewall software on all your computers. However, some anti-spyware and firewall software do not allow cookies to be stored on a computer. Some anti-spyware software may give you an option to remove cookies. If this product site's cookie is removed, upon future sign in, you may be required to validate your identity.