Contents

What is MFA?

Multi-factor authentication (MFA) is a method of confirming a user's claimed identity in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something the user and only the user knows), possession (something the user and only the user has), and inherence (something the user and only the user is)

Did the URL change for accessing the Portal?

No, the login URL remains the same https://portal.fisglobal.com/***firm***

******Do not bookmark the re-direct URL to the identity provider (IdP) or you will encounter improper browser cookies handling and receive invalid credentials errors attempting to login. If you have bookmarked the redirect URL you will need to update the bookmark properties URL to the original https://portal.fisglobal.com/firm.***

What is an authenticator?

An authenticator is a software token that implements two-step verification services using a time-based one-time password algorithm by generating a six to eight-digit one-time password (OTP) which users must enter in addition to their usual login details.

What methods can I use to authenticate on the Portal?

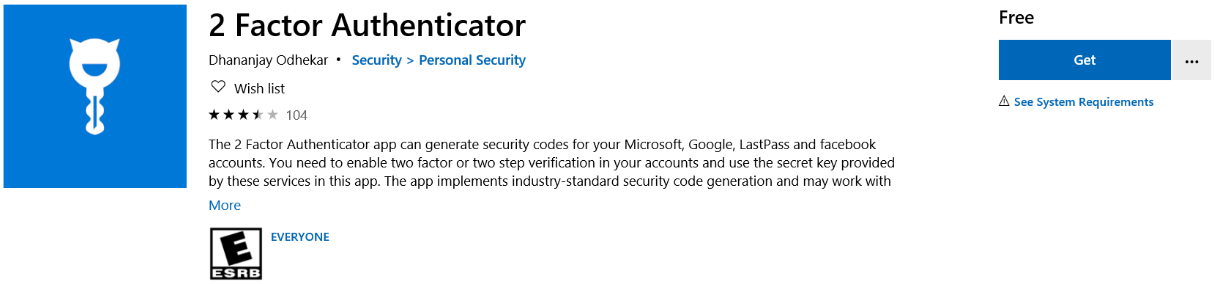
3 options:

1. Install an authenticator application on your smart device (smart phone, tablet)
2. Install a desktop authenticator application on your computer
3. Use text messaging/SMS

Is there a desktop authenticator application so I don’t have to use my mobile device?

Yes, desktop authenticator application called **2 Factor Authenticator** found in the Microsoft Store:

https://www.microsoft.com/en-us/p/2-factor-authenticator/9nblggh5k7jn?&activetab=pivot:overviewtab



2 Factor Authenticator

Dhananjay Odhekar • Security > Personal Security

♡ Wish list

★★★★★ 104

The 2 Factor Authenticator app can generate security codes for your Microsoft, Google, LastPass and facebook accounts. You need to enable two factor or two step verification in your accounts and use the secret key provided by these services in this app. The app implements industry-standard security code generation and may work with

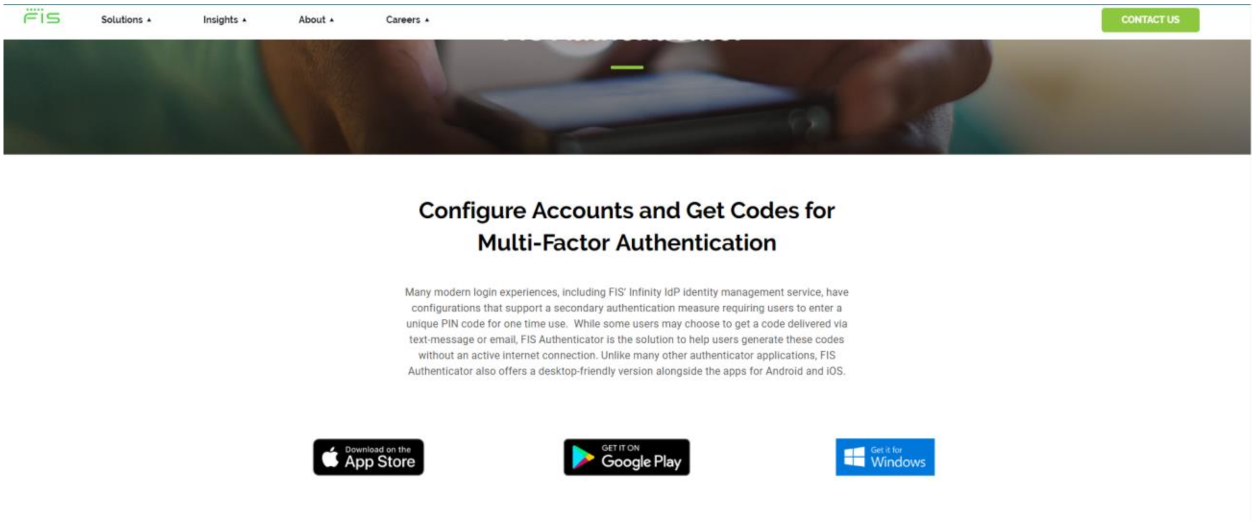
More

EVERYONE

Free

Or the **FIS Authenticator Desktop and Mobil**:

https://www.fisglobal.com/fis-authenticator/



Configure Accounts and Get Codes for Multi-Factor Authentication

Many modern login experiences, including FIS’ Infinity IdP identity management service, have configurations that support a secondary authentication measure requiring users to enter a unique PIN code for one time use. While some users may choose to get a code delivered via text-message or email, FIS Authenticator is the solution to help users generate these codes without an active internet connection. Unlike many other authenticator applications, FIS Authenticator also offers a desktop-friendly version alongside the apps for Android and iOS.

Do I have to have a smart phone?

If you want to use a mobile device (smart phone or tablet) to generate your One-Time-PIN (OTP), it must be able to download an authenticator application from your device’s app store. Otherwise you need to install a desktop authenticator application. You may use text messaging/SMS with your smart phone too.

How do I get an authenticator application on my mobile device?

Look in the App Store on your smart phone or tablet and search for Google Authenticator, Microsoft Authenticator, or FIS Authenticator. These are available for both android and iOS phones. It does not matter which one you choose to use as they all will generate the same OTP.

I'm receiving "CC0193 Invalid Credentials" message on initial login to Portal

Make sure you did not enter or copy and paste an extra space at the end of the password that was emailed to you from the IdP.

I keep getting "CC0316 Invalid Credentials" message using a desktop authenticator

The OTP generated by the authenticator application is using a time-based algorithm. The time on your computer/device must be in-sync with the world clock https://www.timeanddate.com/worldclock/

If your time is off by only a few seconds you will continue to have difficulties trying to authenticate. Choose the SMS/Text messaging option for receiving your OTP if you are not able to change the time on your computer/device. Click the "**Trouble signing in?**" link on the login page and "**I have problems with the One-Time-PIN**" option. After entering your password select "**I want to reset my One-Time-PIN device**". You will receive an email with a link to reset your OTP device. Click the link and continue to log into the Portal, the select the SMS/Text option for receiving your OTP.

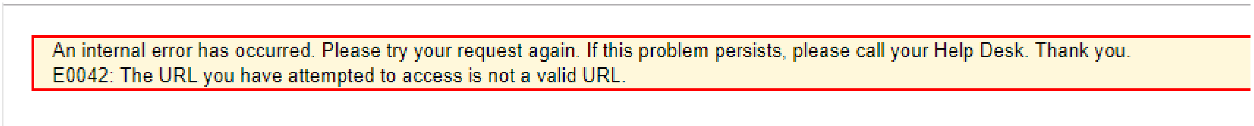
I replaced my mobile device and need to re-establish my authenticator account

Click on the "**Trouble signing in**" link on the login page and select the "**I have problems with the One-Time-PIN**". After entering your password select "**I want to reset my One-Time-PIN device**". You will receive an email with a link to reset your device. Delete your account from the authenticator app. Click the link in the email and proceed to log into the Portal. You will enter your login ID and password, then select the option for how you want to receive your OTP.   If you choose an authenticator app, you will receive a new QR code / Key code to re-establish your authenticator account. If you have any problems, contact your lead institution to have them reset your OTP device.

Can I change my authenticator from mobile device to desktop or vice versa?

Yes, click on the "**Trouble signing in**" link on the login page and select the "**I have problems with the One-Time-PIN**". After entering your password select "**I want to reset my One-Time-PIN device**". You will receive an email with a link to reset your device. Delete your account from the authenticator app. Click the link in the email and proceed to log into the Portal. You will enter your login ID and password, then select the option for how you want to receive your OTP. If you choose an authenticator app, you will receive a new QR code / Key code to re-establish your authenticator account. If you have any problems, contact your lead institution to have them reset your One-Time-PIN device.

I received "An internal error has occurred. E0042: The URL you have attempted to access is not a valid URL" message



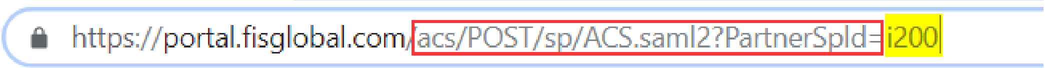
An internal error has occurred. Please try your request again. If this problem persists, please call your Help Desk. Thank you.
E0042: The URL you have attempted to access is not a valid URL.

You may receive this message if:

- Your Portal session has timed out and after a period of time you are attempting to login again, your original session cookie has expired
- You encountered an error while attempting to change your password
- You encountered an error while attempting to register your device

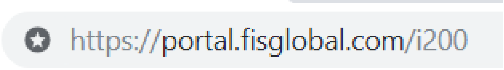
You can click on your original browser Portal bookmark or favorite and you should be directed to the Portal. Otherwise, close the browser session and launch a new session to authenticate to the Portal.

You can also correct the URL by deleting part of it. In the following example the Portal Firm is i200:



https://portal.fisglobal.com/acs/POST/sp/ACS.saml2?PartnerSpId=i200

Place your cursor at the = sign before the Firm identifier, and using your backspace key erase the part of the URL that is in the box, so that your URL appears as follows:

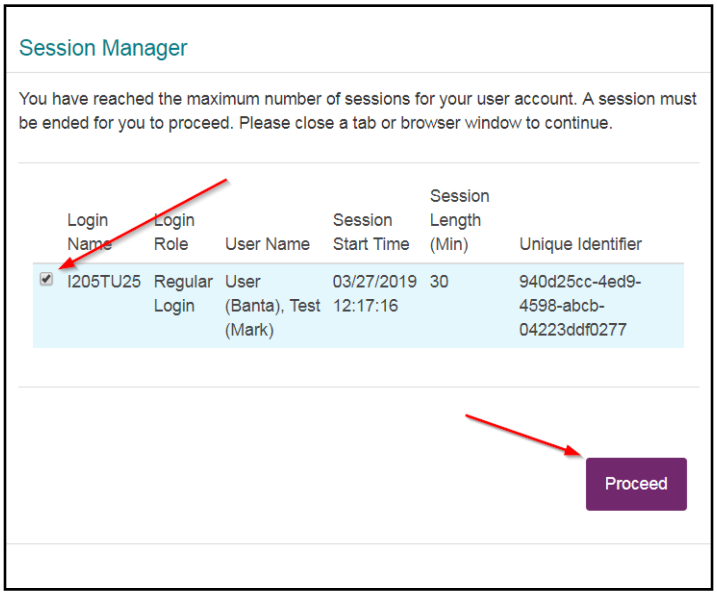


https://portal.fisglobal.com/i200

Hit "Enter" or refresh your browser window and you should be directed to the Portal. The above URL should be the same URL as your browser bookmark or favorite.

Session Manager – "You have reached the maximum number of sessions for your user account"

This message will appear if the IdP recognizes that you have been previously logged into the Portal and may have forgotten to sign out and just closed your browser. Now you are attempting to login again. You can click on the box next to your Login Name and "Proceed" to end your prior session and gain access to the portal:



Session Manager

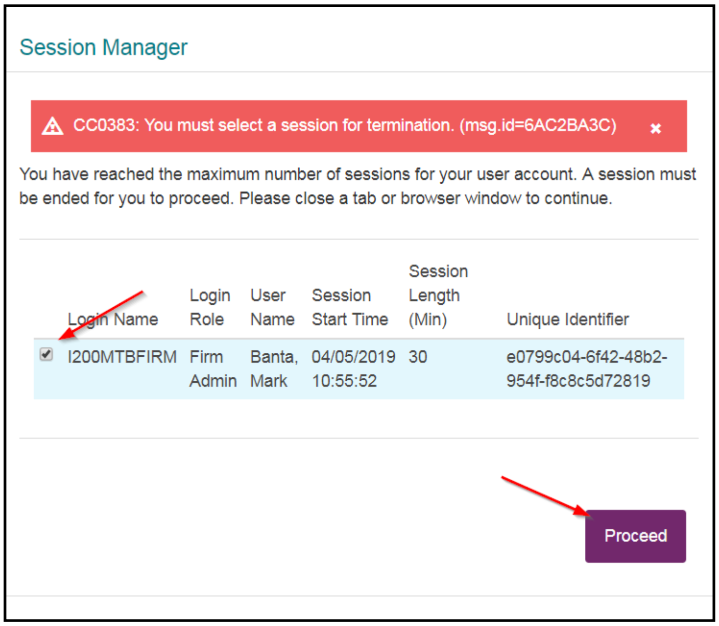
You have reached the maximum number of sessions for your user account. A session must be ended for you to proceed. Please close a tab or browser window to continue.

	Login Name	Login Role	User Name	Session Start Time	Session Length (Min)	Unique Identifier
☑	I205TU25	Regular Login	User (Banta), Test (Mark)	03/27/2019 12:17:16	30	940d25cc-4ed9-4598-abcb-04223ddf0277

If you are not able to click the “Proceed” button to land on the Portal, contact your firm administrator to have them end your IdP session.

Session Manager – “CC0383: You must select a session for termination”

You have reached the maximum number of sessions (1) for your account. You need to click the box next to your Login Name and click “Proceed” to end your prior session:



Session Manager

CC0383: You must select a session for termination. (msg.id=6AC2BA3C)

You have reached the maximum number of sessions for your user account. A session must be ended for you to proceed. Please close a tab or browser window to continue.

	Login Name	Login Role	User Name	Session Start Time	Session Length (Min)	Unique Identifier
☑	I200MTBFIRM	Firm Admin	Banta, Mark	04/05/2019 10:55:52	30	e0799c04-6f42-48b2-954f-f8c8c5d72819