Multi-factor authentication for U.S. Bank Access® Online frequently asked questions

What is MFA?

Multi-factor authentication (MFA) requires a user to provide two or more verification factors to confirm their identity before gaining access to an app or digital resource. The goal of MFA is to create a layered defense that makes it more difficult for an unauthorized person to gain system access. One of the most common MFA methods that users encounter is one-time passcodes (OTP) that are sent via SMS, email, or app.

Why is MFA important?

MFA is a core component of a strong identity and access management policy and is used to ensure that digital users are who they say they are. Asking for an additional verification factor, beyond username and password, decreases the likelihood of a successful cyber incursion.

Will this new step make it harder for my users to log into Access Online?

By default, the system will remember a user + device combination to decrease the frequency of this prompt, unless you disable this feature. (The "Prompt me for enhanced security during login instead of remembering my device" option should be disabled in User Preferences if shared devices are used to access the system.)

How does a user enroll in MFA?

After the August release, unenrolled users will be automatically prompted to enroll in MFA at login.

Are there occasions after initial login when users will need to MFA, regardless of device recognition?

Once the user has enrolled to the enhanced security, they will be prompted to use enhanced authentication at the following times:

- If they are logging in from a device (machine/browser combination) that has not been previously used for that ID.
- If "Always prompt user for additional verification at login" is enabled at the **relationship level**. (This is not the default setting.)
- If the device has not been used to log into Access Online in the last 60 days.
- If the user's password is expired and needs to be updated during login.
- If the **user** has selected to "Always Prompt me for Enhanced Security" during login instead of remembering my device history.

What happens if I get my one-time passcode wrong?

A user can enter 5 invalid OTPs before they are locked out of Access Online. Once locked out, the user must follow the Forgot Password workflow to reset their User ID. If a user is unable to enroll in MFA, even after resetting their password, please call the Help Desk for assistance.

What if I don't receive my OTP?

Please call the Help Desk for assistance.

Why am I getting an error message when I enter my OTP?

OTPs are only valid for 10 minutes. If the OTP expires, you may request another via Access Online.

Does MFA impact the Access Online mobile app?

Yes, MFA will be required for all users, regardless of device type.

What if I use biometrics on my phone?

If the mobile user is enrolled in biometrics, they will log in using their fingerprint/face ID and will not be prompted for mobile or email.

How can I update my MFA contact information before this change takes effect?

The email address used for MFA is found on the **My Personal Information >> Contact Information screen**. Contact information found in other areas of Access Online will not have an impact on the delivery of the MFA OTP.

Can I run a report of my user's email addresses to confirm accuracy?

To run a report of user email addresses to confirm accuracy, you can run the System User List Detail report found at: **Reports >> Administration >> System User List Detail report** and select **Contact Information** under **Additional Detail.**

I have a user who cannot enroll in MFA. Why?

User profiles in Access Online must be active and in good standing. Expired, Admin Locked, or Failed Self Service profiles must be reset to allow for MFA registration.

If I need assistance, what information will I need to provide to the Help Desk when I call?

If you call the Help Desk, be prepared to provide the answers to your authentication questions, your User ID, and organization short name.

What can the Technical Help Desk NOT assist with?

- The Help Desk cannot reactivate users who have been removed or are in an Admin Locked status. This task must be completed by the Program Administrator.
- Removed profiles cannot be reactivated; the Program Administrator must build an entirely new User ID profile.
- Profiles in an Admin Locked status may not be unlocked by the Help Desk; the Program Administrator must reset the profile before MFA can be established.
- Any confirmation of employee validity must be handled by the Program Administrator.

What are common things the Technical Help Desk CAN assist with?

- Authentication questions that need to be updated.
- All information looks accurate but still no success with sign on.
- Cardholder account issues after MFA sign in.

- Same device used for sign in but no success with MFA.
- Expired OTPs.
- Assistance with Enhanced Security set-up.

What other resources are available?

Access Online web-based training provides information about managing profile information and can be found at **Access Online Home page > Training > Type "Profiles" in the Search box.**