



Fifth Third Direct®

How Do I Log In to Fifth Third Direct for the First Time?

Use this guide to learn more about **logging in to Fifth Third Direct**.

For questions about this guide, please reach out to your Fifth Third relationship team or contact our Commercial Support Center at 866-475-0729, Monday through Friday, 7 a.m. to 10 p.m., ET.

August 2026

Getting Started

Welcome to Fifth Third Direct. Learn how to sign on to the Fifth Third Direct portal, change your password, activate your security device, and more.

Initial Log In for Fifth Third Direct

1. Navigate to **express.53.com** using your browser's address bar.
2. Click **Start Here** at the call-out under the login screen.
3. Type your Comerica CBC User ID.
4. Type your **Primary Email Address**; this will be the same email that was set up on CBC.
5. Click **Continue**.



Welcome Comerica Bank customer!
First time logging in? [Start here.](#)

2

Create a Fifth Third Direct Password

To ensure your Fifth Third Direct experience is as secure as possible, **we are requiring you to change your password**. Please enter your **Comerica CBC User ID** and **primary email address** to log in and change your password.

Comerica CBC UserID:

Primary Email Address:

5

Continue

[Login Help \(pdf\)](#)

Don't know your Comerica CBC User ID or email? Call **866-475-0729** to have your email address updated and/or User ID provided.



Resetting a Password

6. You will receive an email with your temporary password.
7. Return to the FTD login screen. Enter your **User ID** (CBC ID) and **Temporary Password** you received in your email. Click **Log In**.
8. At the Change Your Password screen, enter your **Temporary Password** from the email, then **Create New Password** and **Verify New Password**.
9. Click **Submit**.

Note: When requesting a password reset or TAC, clients should **click the button once** and wait to receive the email. The code ID is generated almost immediately, but please note it could take up to 30 minutes to arrive. Fifth Third is sending the password and TAC emails promptly but due to Outlook and firewall issues, they may take time to arrive.

Change Your Password - Reset

You have requested to reset your password.

* Required

Password

Your new Fifth Third Direct Password must meet the following criteria:

- Must be 8-64 characters in length
- May not contain more than two of the same character in a row (aaa, 222, etc.)
- May not contain your username or custom user ID
- The two passwords must match
- May not contain commonly used passwords or password patterns (qwerty, password, abc123, etc.)
- May not be one of your last 6 passwords [OR] May not be a password you used within last year
- Must contain at least one upper case, one lower case and one numeric character



10. Enter your **User ID** (CBC ID) and your new **Password**.

11. Click **Log In**.

Fifth Third **DIRECT**

Your password has been successfully changed. Please log in below to get started.

10 User ID

Password

11 Log In

[Forgot Your Password?](#) [Login Help \(pdf\)](#)

Comerica Bank

Welcome Comerica Bank customer!
First time logging in? [Start here.](#)



Initial Login Flow

Note: If you require a token, skip to step 16

12. Set your security questions and answers.
13. Review your phone number for awareness. Updates should not be made here. Please contact your administrator or your relationship team to make any updates.
14. Verify your Primary Email Address.
15. Click **Continue** and then click **Confirm** on the next screen.

Note: Users who are required to set up a security token may not be prompted to set up security questions and answers during the initial login but will be prompted to set up security questions and answers during subsequent login.

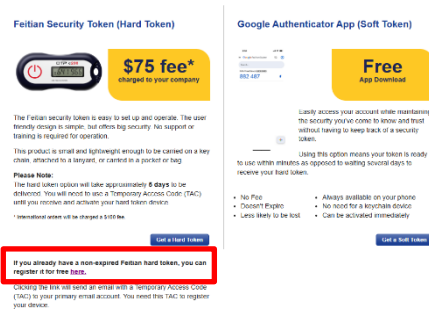


Secure Tokens

A secure token provides a 6-digit code as an additional measure of security. Fifth Third Direct requires users with payment capabilities to set up a security token. Depending on the entitlements you've been assigned by your Administrator, you may be provided with either a soft token or a hard token for your login to Fifth Third Direct. Please note that only one token type can be active at a time. If you have been issued a token, follow the steps in "Activating your token" below.

- Tokens were delivered to the Comerica CBC Administrator or primary contact for Comerica at your organization.
- **If you did not receive a token but believe you should have, please check with your Administrator.**

If prompted, click the "here" link to activate/re-activate your hard token device:



Activating Your Hard Token

16. Enter the **Temporary Access Code** that was sent in your email.
17. From your physical token enter the **Credential ID** found on the back of the device.
18. Enter the **Security Device Code** from your device.
19. Click **Continue**.

Enhanced Online Protection

Security Device Activation

If you received your Feitian security token, please activate it now by following the instructions below. If you have not received your security device, you can skip to the next screen to enter your Temporary Access Code (TAC) and activate your device later.

Step 1: Enter your Temporary Access Code

Temporary Access Code:

16

We just sent an email to the primary email address associated with your Fifth Third Direct Account. It contains the new Temporary Access Code (TAC) you need to complete the device registration process. [Can't find your Temporary Access Code \(TAC\)?](#)

Step 2: Enter your security device serial number from the back of the device

Credential ID:

17



Step 3: Enter your Security Device Code

Enter the security code from your new device.

Security Device Code:

18



19

[Activate Later](#) [Continue](#)

Important: Once you activate your Security Device, you will need to use it every time you log in to your account.



Activating Your Soft Token

20. Install an authenticator application on your mobile device (we recommend Google Authenticator).
21. Enter the **Temporary Access Code** that was sent in your email.
22. From your authenticator application scan the **QR Code** found on the activation screen in FTD.
23. Enter the **Security Device Code** from the application on your mobile device.
24. Click **Continue**.

Obtaining your Soft Token

Follow the directions below to get the app for your smartphone.

1. Install the Google Authenticator app from the App Store or Google Play Store
2. When the installation is completed, open the app
3. Allow the Google Authenticator to access your camera.
4. Click the **Continue** button below

Google Authenticator



20

DO NOT store your login information (user ID and password) on the same device that you use for your soft token. This prevents someone from logging in with your user ID if they have access to your phone.

If none of these options work for you, you can order a hard token [here](#).

Continue

Enhanced Online Protection

Your access to sensitive functionality requires you to register for a security device.

Security Device Activation

Activate your new Google authenticator app by following the steps below:

Step 1: Enter your Temporary Access Code

21

Temporary Access Code:

Required



We just sent an email to the primary email address associated with your Fifth Third Direct Account. It contains the new Temporary Access Code (TAC) you need to complete the device registration process. [Can't find your Temporary Access Code \(TAC\)?](#)

Step 2: Scan the QR Code



22

1. Scan this QR code.
2. * If prompted for a passphrase
3. The app will begin displaying the 6-digit security code, as shown below.

Step 3: Enter your Security Device Code

Enter the security code from your new device.

23

Security Device Code:

Fifth Third Direct: Q0000000

882 487

24

Continue

Important: Once you activate your Security Device, you will need to use it every time you log in to your account.



25. Click **I Agree** to accept the Enhanced Online Protection agreement.

26. You will be brought to your Fifth Third Direct Overview screen.

Enhanced Online Protection

Using your mobile device to check the balances of your accounts, to process simple transactions, or to manage online access is convenient and can save you time, but how do you make sure it is also secure?

What Are The Risks?

- Data loss
- Unauthorized access
- Mobile malware
- Falling victim to [phishing](#) or other types of social engineering
- Accessing fraudulent web sites
- Downloading fraudulent applications
- Weak or no passwords
- Failure to update the device

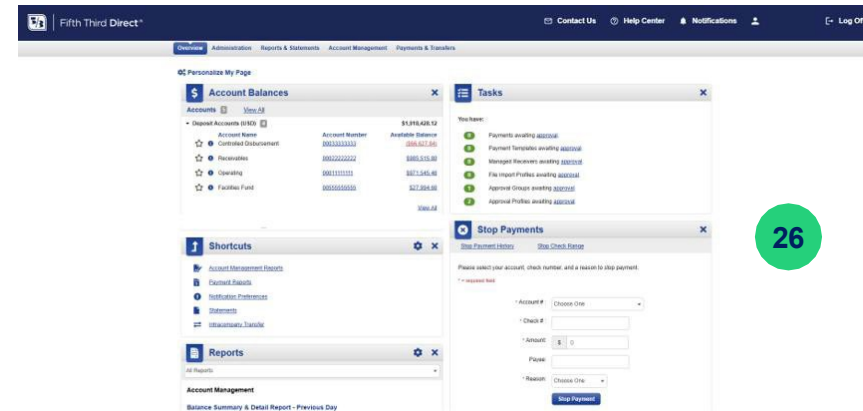
What You Can Do to Protect Your Information?

- Treat your mobile device with the same level of care as you would a credit card. If it is lost or stolen and you have not protected it adequately, you may be at risk.
- Password-protect your mobile device.
- Store your mobile device in a safe place.
- Do not send confidential information in e-mail or text messages (e.g., account numbers). It is important to understand that text messages are not encrypted the same way your mobile device information is. If someone gains access to your phone, they will be able to view any text messages sent or received that have not yet been deleted.
- Delete messages that contain account information, including account balances, and any alerts you receive on a regular basis.
- Only download information (photos, ring tones, video clips, etc.) from trusted sources.
- Follow the same rules you use on your computer with respect to opening e-mail and attachments. Similar to [phishing](#) attacks on your computer, SMiShing attacks involve fraudsters using text messages with links in them on your mobile device. The fraudsters will use these text messages in an attempt to:
 - Get you to download unsuspecting software containing viruses. Never open or respond to a text message from someone you do not know, and proceed with caution even if it comes from someone you do know.
 - Take you to a "spoofed" or fake Web site that is masquerading as a Fifth Third Bank site and request your account credentials (e.g., password, user ID, etc.)
- Install antivirus software on your mobile device. Contact your carrier for specific information on available antivirus software for your device.
- If you are concerned about the sites you are accessing from your mobile device, turn on the "show URL" or "show address bar" option so that you can see the actual site addresses to ensure they start with "https." Check the information that came with your device for specific instructions.

Cancel

I Agree

25



26

Have a question? Contact your relationship team or call our Commercial Support Center at 866-475-0729, Monday through Friday, 7 a.m. to 10 p.m., ET.