Business online banking user guide

JULY 2017

Contents

Introduction

Welcome to STCU business online banking! This guide includes important information about your account security and an introduction to some of the platform's features.

The "help" button at the top right of your business online banking screen is your friend. It should help you find answers to most of your questions, automatically displaying help files relevant to what you're seeing at the time.

If you have additional questions, please call STCU at (509) 326-1954, (208) 619-4000, or (800) 858-3750. Be sure to ask for an eBusiness representative.

Thank you!

Security tips: Protect your account

STCU's business online banking system is strong and secure. It's also critical for businesses to use tools and strategies to protect themselves against online crooks or internal fraud. One good reason: The federal regulations that protect individuals against online fraud don't extend to businesses.

There's no single surefire way to stop online fraud. However, a combination of diligence, internal checks and balances, and other strategies will help reduce your risk.

Limit access to your business accounts.

- Grant online banking access to as few people and computers as your business really needs. In general, the more people you have doing online banking on more computers, the higher the risk of a virus or malware infection. Those infections can allow fraudsters to access your online accounts.
- Limit employee permissions. For example, limit higher-risk online transactions — such as external transfers— to trusted employees who need the access to complete their normal job duties and limit the dollar amounts for these transactions.
- Consider dual control. Set up certain transactions to require one employee to initiate them and another employee to authorize them.
- Protect against disgruntled or departing employees. If an employee has submitted their resignation, is on probation, or will soon be let go, restrict or turn off their access to your business's accounts.

Log in with care.

- Create individual logins. Each person who accesses your business accounts online must have their own login — no sharing. That makes it easier to track who is doing what with your business's accounts.
- Require strong passwords. Each person authorized to access your business accounts online should choose the strongest password they can remember. It should be eight to 12 characters long and include uppercase and lowercase letters as well as numbers and symbols.
- Make sure you're really logging onto STCU's site. Don't assume a link will take you to STCU's online banking site. Instead, open your browser and type www.stcu.org into the address bar. Your browser should show a padlock icon indicating a secure connection. Your login should include no unexpected steps or extra requests for information.

Keep viruses at bay.

- Update software and operating systems. Software makers issue fixes for security weaknesses in their programs. Regularly check for and install these updates.
- Practice “safe surfing.” Put anti-virus and anti-spyware software on each computer used to access business accounts online, and update the software regularly. Don’t let employees visit websites at high risk for viruses and malware (such as social media sites). Discourage employees from opening attachments in unsolicited emails or that they weren’t expecting. Use firewalls to keep outsiders off your network. And don’t do online banking on public computers or unsecure networks.

Finish strong.

- Click the “Log out” button when you’re done. Every time.
- Review your accounts daily. Look for unexpected or unusual activity.
- Review your risk regularly, and adjust when needed. Have you gained or lost employees? Are you performing new types of business online banking transaction? Are you making more money? Then it’s a good time to audit your internal security measures as well as your employees’ online activity.

Suspect fraud? Call us!

- Minutes matter if you hope to limit losses from online fraud. Call STCU immediately if you suspect any unauthorized activity on your business online banking account. Our numbers: (509) 326-1954, (208) 619-4000, or (800) 858-3750.

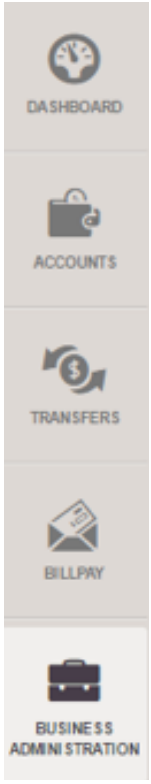
Choose a secure login method

STCU offers multiple ways to log on to your online account. We strongly recommend that business online banking members sign on using our text-security option or one of our token-security options:

- Text security is secure and convenient. When logging in, you receive a random 6-digit security code to your text-enabled phone.
- Soft tokens are digitally generated. They work if you have an iOS, Android, or Windows smartphone. With soft tokens, your stand-alone smartphone security app generates random 10-digit security codes that expire every few minutes.
- Hard tokens appear on a physical key fob. They work if you don't have an iOS, Android, or Windows smartphone but you still want a higher level of security. We can provide security tokens on a physical security key fob.

Visit stcu.org/login_security for more information about our secure-login options.

Business features overview



When you log into business online banking, you'll see a column of icons on the left side of your screen (see left). The top four — Dashboard, Accounts, Transfers, and Billpay — will be familiar to you if you've used STCU online banking before. But here's an introduction to some of the features designed especially for businesses, which you'll find by clicking on "Business administration."

Business Administration

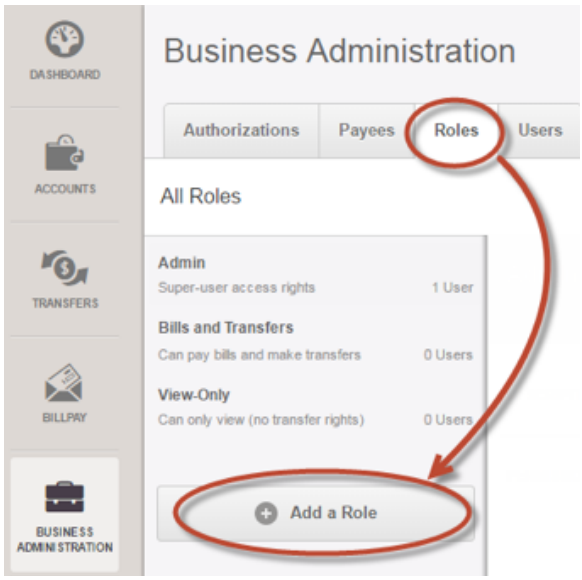
As the account owner, you are the “master user.” STCU business online banking lets you decide who else should get access to your accounts, and what the limitations of that access should be for each person. You can authorize multiple account users with very specific levels of access.

Roles

A “role” is a combination of permissions and transaction limits that you’ll define for one or more of your “subusers.” Roles can be applied to more than one subuser. Details on each of the available permissions, account types, and transaction limits can be found by clicking “help” at the top right-hand corner of the online banking screen.

You must create a role before you can place a subuser in that role. To start creating roles, click “Business Administration,” then “Roles.”

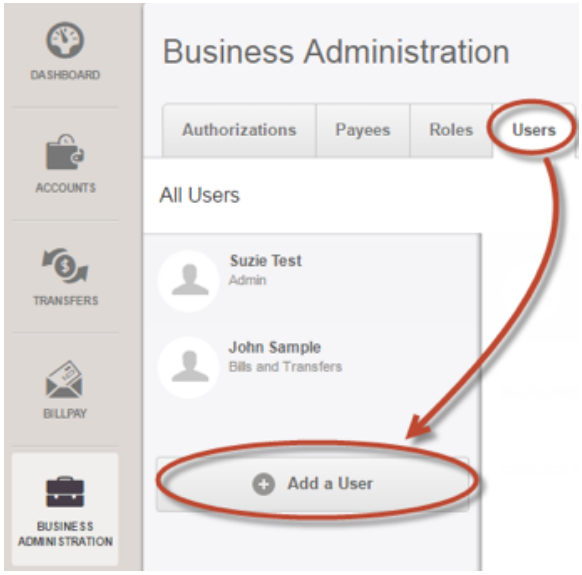
Keep in mind: You must log out and log back in to business online banking before new permissions are applied, but changes to transaction limits are applied in real time.



Users

Once roles have been created, you can add, edit, and delete subusers to fill those roles. The account's master user is responsible for all subusers. This includes creating their usernames, resetting their passwords, and managing their permissions.

To start placing subusers within roles, click "Business Administration," then "Users."



To add a new user, provide their unique username, first and last name, and email address — and specify which role they'll be placed in. The system automatically emails the new user a temporary password, but it's up to you to tell them their username. When the new user sets up their account for the first time, they'll be asked to complete a full user setup. (Please note that temporary passwords expire in 24 hours.)

For detailed instructions on setting up your subusers, click "Help" at the top right-hand corner of the online banking screen in business administration.

Authorizations

Here's where you can review and approve transfers.

You can set up notifications (alerts) for whenever a transfer request is submitted for approval. See the "Notifications" screen in "Settings" to set these up.

For detailed instructions, click "Help" at the top right-hand corner of the online banking screen in business administration.

A note about authorizations: Even after you delete a subuser from your account, all scheduled transactions created by that user will remain active and will be submitted to STCU for processing unless you delete them or take another action to stop them.

Tell us what you think

Your feedback will be critical as we continue to improve business online banking. To report a flaw with business online banking or to share other specific feedback, please call our Contact Center at (509) 326-1954, (208) 619-4000, or (800) 858-3750.

When reporting a problem, please let us know what you were doing when something went wrong, including details such as which browser you were using. Let us know what you expected to happen — and what actually happened. For example, a great problem report might sound like this:

> I was logged in to business online banking in Firefox, in the Business Administration screen, editing users. I clicked on Maria, who I have set up with all permissions as a super-user. I tried to add a mobile phone number. When I clicked "save changes," I expected the change to save and the screen to display her new number. Instead, the save changes button changed to "Saving ..." and did not refresh for at least 3 minutes. When I clicked "refresh" in my browser, the new mobile phone number did not display.

If you need support with your regular (nonbusiness) account, or have basic questions about transactions, feel free to contact us.

- Call (509) 326-1954, (208) 619-4000, or (800) 858-3750.
- Use our online LiveChat tool from 8 a.m. to 5 p.m. Monday through Friday. (To find LiveChat, go to stcu.org and click on "Contact us.")
- Stop by any STCU branch location.
- Send a secure message in online banking or via the STCU mobile app.

Thank you!

We hope you enjoy using STCU business online banking, and we look forward to building our relationship with you and your business.