



Luther Burbank®

Savings

Business Online User Guide for Administrators

Once your account has been set up, you will be eligible to take advantage of our online banking services. The senior administrator is responsible for managing your company's user access and for setting up templates. The following procedure outlines how to use Business Online to complete senior administrator tasks. If you have any questions about this procedure or wish to report any issues while using Business Online, email onlineaccounthelp@lbsavings.com or call 888.578.4495, Monday – Friday, 9am to 5pm (PT). If emailing, please do not include any sensitive information such as an account number, PIN, password or Online ID.

Managing Users

The senior administrator is responsible for creating basic profiles for new employees requiring access to Business Online. Follow the instructions below to set up a new profile then contact Luther Burbank to complete user access set up for any additional services [Bill Pay, Remote Deposit Capture (RDC)/Mobile Capture (MDC), Automated Clearing House (ACH) or Wires] and to request tokens.

- Adding a New User
 - Navigate to Administration>Employee>Profile & Permissions and a pop up window will appear.
 - Select New Employee then click Submit to complete the following:
 - Employee Name
 - Security Level (user access level)
 - Employee Group (user group)
 - Transaction Export (allows user to export transactions)
 - Contact Methods (email, work number and extension, mobile number)
 - Security
 - Assign a username that is at least six (6) characters long (case sensitive).
 - Click Change Password to assign a temporary password.
 - Note: Once the profile is complete, provide the new user with the username and temporary password.
 - Multifactor Authentication
 - For Token Status, select Pending Enablement.
 - For Token Type, select Go3.
 - Note: New user tokens must be requested from Luther Burbank to be sent by mail. Upon receipt, provide the new token to the user. If you have a token from a previously disabled user profile, contact Luther Burbank to have the token reassigned to the new user.
 - Role Assignment
 - Select the Role Name for the user to determine their access rights. All roles are available to choose from accept the senior administrator. See the Appendix for more information on access rights available for each user role.
 - ACH
 - Check the box if the user will perform ACH transactions then contact Luther Burbank to complete access set up. Unless user-specific limits are requested, limits will default to the approved limits for the business.
 - Accounts
 - Select the accounts the user should have access to as appropriate.
 - Overrides – Skip this field, no changes.
 - Approval Options
 - Review Internal Transfers – Check the box if internal transfers initiated by the user must be approved.
 - Approve Transfers – Select Yes if the user is permitted to approve transfers requiring dual control such as ACH or Wires.
 - Note: This section will not appear for employee users. Approval access rights are only available to administrator and supervisor users.

- Funds Transfer Options
 - Inquire Transfers – Select Yes if the user is permitted to inquire about transfers made by the company.
 - Initiate Transfers – Select Yes if the user is permitted to initiate internal transfers on behalf of the company.
- Merchant Capture Options
 - If the user will be scanning checks:
 - Select Yes for the Merchant Capture Option.
 - Under Role, select Approver.
 - Select Yes for View Client Deposits.
 - If the user will not be scanning checks:
 - Select No for the Merchant Capture Option.
 - Under Role, select Limited.
 - Select No for View Client Deposits.
 - Leave all limit fields blank.
- Stop Payments
 - Inquiry – Select Yes if the user is permitted to inquire about stop payments.
 - New – Select Yes if the user is permitted to request stop payments on behalf of the company.
- Interface Specifications – Skip.
 - Note: To authorize the new user for Bill Pay access or alerts, contact Luther Burbank.
- Electronic Documents
 - Select the appropriate boxes to enable access to view check images or check deposit images.
- Applications Enabled
 - Check the Wires box if the user is permitted to complete wire transactions.
- Once all fields are complete, click Next. The system will add the user to the appropriate accounts (see the green checkmarks under Access Added).
- Click Next.
- If the user is permitted wire access, you will be directed to the Wire User screen. Select the Domestic Wires access rights for each checking account to which the user is granted access. Contact Luther Burbank to complete set up.
- When done, click Finish.
- Changing a User Profile Set Up
 - Navigate to Administration>Employee>Profile & Permissions and a pop up window will appear.
 - Click Change Employee then select Codes from the dropdown.
 - Click Submit then select the user from the list to make changes to their user settings.
 - Click the Save icon to save changes or the Folder icon to ignore changes and return to the previous screen.
- Changing a User ACH Profile
 - Navigate to Administration>Employee>Profile & Permissions and a pop up window will appear.
 - Click Change Employee then select ACH from the dropdown.
 - Click Submit then select the user from the list to make changes to their access rights under permissions.
 - Click the Save icon to save changes.
- Changing a User Wire Profile
 - Navigate to Administration>Employee>Profile & Permissions and a pop up window will appear.
 - Click Change Employee then select Wires from the dropdown.
 - Click Submit then select the user from the list to make changes to their access rights under permissions.
 - Click the Save icon to save changes.
- Changing User Access to Company Accounts
 - Go to Administration>Employee>Accounts and a pop up window will appear.
 - Search for the user by Access ID or Employee Name then click Submit.
 - Click the user's name to access account information.
 - Click the Change icon next to the corresponding account to make changes to the user's account access rights.
 - Click the Save icon to save changes. Repeat for other accounts as necessary. (Refer to the Appendix for access details.)

- Changing User Access to Complete Internal Transfers
 - Navigate to Administration>Employee>Change Fund Transfer Access.
 - Search by Employee Name then click Submit.
 - Click the user's name to view current access and make changes by selecting the appropriate option from the dropdown.
 - Click Submit to save changes.
 - Note: For view-only access, navigate to Administration>Employee>Inquire Fund Transfer Access.

Managing Display Groups

Display groups are used to organize accounts, employee access and transactions types within Business Online. To customize or add new display groups to suit your business needs, contact Luther Burbank.

Managing Internal Transfer Templates

Employee users who have been granted access to perform internal transfers for the company can use templates for one-time or recurring internal transfers.

- Adding a New Template
 - Navigate to Administration>Fund Transfer>Add Template.
 - Select the Funds Transfer Type – Internal Transfer (the default and only option).
 - Enter the Transfer Description.
 - Assign a Fund Transfer Group, if applicable.
 - Identify whether review of the transfer is required, and if so, indicate who should approve the transfer.
 - Enter the appropriate account information in the From and To sections.
 - Use the Defaults section to select defaults such as the maximum or minimum transfer amounts.
 - If this template will be used for automated recurring payments, select the Frequency option and set the number of recurrences.
 - In the Instructions section, include any instructions regarding the template.
 - Click Submit to set up the template.
- Changing an Existing Template
 - Navigate to Administration>Funds Transfer>Change Template.
 - Search for the template under Transfer Description.
 - Click Transfer Description/Template Name to update the template.
 - Click Submit to save changes.
- Deleting an Existing Template
 - Navigate to Administration>Fund Transfer>Delete Template.
 - Search for the template under Transfer Description.
 - Check the box next to the template you wish to delete.
 - Click Submit to delete the template.

Managing the Account Display Group or Nicknames

The default display group and account nicknames (account titles that appear in Business Online) can be modified to suit your business' needs.

- Updating the Account Display Group or Nicknames
 - Navigate to Administration>Business>Accounts and a pop up window will appear.
 - Click the Change icon for the account that you wish to change.
 - Update the display group and/or nicknames as necessary.
 - Click Submit to save changes.

APPENDIX

Security Levels and Access Rights

The table below shows access rights available to each security level assignment.

Access Rights	Senior Administrator	Administrator	Supervisor	Employee
View Account and Balances	x	x	x	x
View Transactions	x	x	x	x
View eStatements	x	x	x	x
24-Hour Business Online Access	x	x	x	x
Change Secret Question/Security Challenge	x	x	x	x
Change PIN (for token user)	x	x	x	x
Change Password (for non-token user)	x	x	x	x
Maintain Employee Profiles (setup, change and delete users)	x	x		
Monitor Employee Profiles (view user set up only)	x	x	x	
Export Data	x	x	x	x
Create Reports	x	x	x	x
Maintain Company Accounts (change nicknames and assign display groups)	x			
Create Templates (recurring transfers: ACH, wire or internal)	x	x		
Internal Transfer Access (view, initiate and send; no approval necessary)	x	x	x	x
Initiate ACH/Wire Transfers	x	x	x	
Approve ACH/Wire Transfers	x	x		
View ACH/Wire Transfer Details	x	x	x	
Positive Pay	x			
Mobile Deposit	x	x	x	x
Scan RDC Check(s) with Viewing (ability to see account balances)	x	x	x	x
Scan RDC Check(s) with No Viewing (ability to create deposits/batches only)				x*
Initiate Bill Payments	x	x	x	x
Approve Bill Payments	x	x		

*The option to only scan checks with no ability to see account balances is available.

Note: The senior administrator must have all access rights as listed in the above table. Other users may only view or maintain user profiles/records that have a security level below their own. (Ex.: An administrator can only see profiles for a supervisor or employee, not of other administrators or the senior administrator.)