FULTON BANK

BOSS Online Banking Platform

Admin Controls & User Maintenance Guide

Administering Users and Permissions in BOSS Online Banking

This guide is intended for Company Administrators responsible for setting up and managing BOSS Online Banking users. It covers the user permission model, adding and entitling new users, modifying existing users, managing approvals, and configuring alerts.

> **NOTE**
> Access to Administration & Settings menus is restricted to users with Administrative permissions. Contact Fulton Bank if you believe you should have administrator access but do not see these menus.

Admin Overview

As a Company Administrator on BOSS Online Banking, you are responsible for:

- Creating and managing sub-users for your company
- Assigning permissions and entitlements to each user based on their role
- Assigning accounts each user can access
- Setting transaction limits for payment users
- Approving new users and user changes (when dual approval is enabled)
- Configuring alerts and notifications

Administrators access user management functions through Administration & Settings in the main menu.

User Permission Model

Permissions in BOSS are organized into six functional areas. Each area is configured independently when you build or edit a user.

Permission Area	What It Controls
Payments	Access to payment functions: ACH, wires, transfers, templates, real-time payments, and check issuance.
Reporting	Access to account reporting, balance reports, transaction history, and legacy reports.
Risk Management	Access to positive pay decisions, ACH authorization rules, and check fraud controls.
Administration	Access to user management, alert configuration, and company-wide system settings.
Assigned Accounts	Which accounts the user can view and transact on.
Transaction Limits	Per-transaction and daily limits for payment initiation.

> **TIP**
> A user does not need all permission areas. For example, a view-only user for account reporting would only need Reporting and Assigned Accounts permissions, with no payment or admin access.

User Maintenance

User Maintenance is accessed through Administration & Settings in the main menu. The User Maintenance list shows all sub-users for your company along with their status.

Accessing User Maintenance

Step	Action
1	From the top menu, click Administration & Settings.
2	Select User Maintenance.
3	The User Maintenance list displays all sub-users. Use the Filter or search options to locate a specific user.

Building and Entitling a New Sub-User

Adding a new sub-user in the 26.05 interface uses a tabbed design with numbered segments at the top of the screen. You will move through four stages: (1) basic user information, (2) permissions, (3) assigned accounts, and (4) transaction limits.

Step 1 — Enter Basic User Information

Step	Action
1	From the User Maintenance list, click Add New User.
2	Select the company for the new user and click Continue.
3	Enter the User ID (the login name the user will use).
4	Enter the user's name, temporary password, and email address.
5	Complete any other required fields on the basic information screen.
6	Click Set Permissions at the top of the screen to advance to the permissions stage.

> **TIP**
> The user will receive a system-generated email prompting them to log in for the first time and complete their security question setup.

Step 2 — Grant Permissions

The permissions stage displays tabs at the top of the User Maintenance screen. Each tab represents a permission area. Click the tab name to open and configure that area.

Permission Tab	What to Configure
Payments	Select which payment types the user can initiate, approve, or view. Options include ACH, Wires, Transfers, Real-Time Payments, and Templates.

Permission Tab	What to Configure
Reporting	Enable access to balance reporting, transaction detail, and legacy report types.
Risk Management	Enable positive pay decision authority and ACH rules management.
Administration	Grant administrative access such as user management or alert configuration. Use carefully.
Alerts	Assign the user as a recipient for one or more alert types.
Ancillary Business Services	Enable access to additional services if applicable to your company agreement.

NOTE
You do not need to configure every tab. Leave a tab's permissions blank (or leave the area toggled off) if the user does not need access to that area.

Step 3 — Assign Accounts

After setting permissions, click the Assign Accounts button at the top of the screen. Select the accounts from your company's account list that this user should be able to access. You can assign individual accounts or assign all accounts.

Step 4 — Apply Transaction Limits (if applicable)

If the user has payment initiation permissions, you may also set transaction limits. Limits control the maximum dollar amount the user can initiate per transaction and per day for each payment type.

Submitting the New User

After completing all applicable stages, review the configuration and submit the new user. If your company has dual approval enabled, a second administrator will need to approve the new user before they can log in.

WARNING
Always assign the minimum permissions required for the user's role. Granting broad permissions to all users creates risk. Review user permissions regularly and remove access that is no longer needed.

Modifying and Managing Existing Users

Editing a User

Step	Action
1	From the User Maintenance list, locate the user you want to modify.
2	Click the user's name to open their User Maintenance record.
3	The same tabbed interface used for adding a user is available for editing. Click the appropriate tab to modify permissions, accounts, or limits.
4	Save your changes. If dual approval is enabled, a second administrator will need to approve the changes.

Copying Permissions from an Existing User

When creating a new user with a similar role to an existing user, you can use the Copy Permissions option to replicate the permission set. After selecting Copy Permissions and choosing the source user, review the copied permissions on each tab and adjust as needed before submitting.

> **TIP**
> Copying permissions is a starting point, not a final configuration. Always review each tab after copying to ensure the permissions are appropriate for the new user's specific role.

Resetting a User's Password

Administrators can trigger a password reset for any sub-user directly from the User Maintenance list. The Reset Password option sends a system-generated email to the user with a link to complete the reset using their security questions.

Step	Action
1	From the User Maintenance list, locate the user.
2	Use the action menu (three-dot ⋯ or right-click) for that user row and select Reset Password.
3	The system sends a password-reset email to the user's email address on file.

Approving Users

If your company has dual approval enabled for user maintenance, a second Company Administrator must approve new users and certain user changes before they take effect.

Step	Action
1	Log on as a Company Administrator with approval authority (not the same administrator who submitted the user).
2	Review pending approvals in the Notifications drawer (Bell icon). Users awaiting approval appear under Needs Approval.

Step	Action
3	Click View next to Users Awaiting Approval, or navigate to User Maintenance and filter for users in Pending Approval status.
4	Review the user's information and permissions.
5	Click Approve to activate the user, or Reject to send it back with comments.

> **NOTE**
> The administrator who submitted the user and the administrator who approves them must be different individuals. A user cannot approve their own submissions.

Disabling and Restoring Users

Disabling a User

Disabling a user immediately prevents them from logging into BOSS Online Banking. Any payments that user has submitted and that are still pending will not be affected — those remain in the system and must be handled by another administrator or approver.

Step	Action
1	From the User Maintenance list, locate the user to disable.
2	Open the user's record.
3	Click Disable (or use the action menu for that user row).
4	Confirm the action when prompted.

Alert Deletion Notifications (26.05 New)

Beginning with the 26.05 release, if the user you are deleting or disabling has created any alerts in the system, BOSS will notify administrators about those "stranded" alerts — alerts that were set up by that user and may no longer function properly without them.

Additionally, if the user being deleted is the last or only recipient of an alert, the system will block the deletion and display an error message:

> **SYSTEM MESSAGE**
> "Selected recipient(s) cannot be deleted. Please update the following alerts to assign a new Recipient or delete the alert(s)."

If you receive this message, take the following steps before completing the deletion:

Step	Action
1	Navigate to Administration & Settings → Alerts Center.
2	Locate the alert(s) listed in the error message.
3	Update each alert to assign a new recipient, or delete the alert if it is no longer needed.

Step	Action
4	Return to User Maintenance and complete the user deletion.

> ⚠ **WARNING**
> Leaving unmanaged alerts without a valid recipient means those alerts will not fire when triggered. Always reassign or delete orphaned alerts promptly when removing a user.

Restoring a Disabled User

Step	Action
1	From the User Maintenance list, filter for disabled users (Status: Disabled).
2	Open the user's record.
3	Click Restore to reactivate the user's access.
4	If dual approval is required for your company, the restore action will need approval before taking effect.

Dual Approval Entitlements & Limit Approvals

Companies can require a second administrator to approve changes to user permissions and limits, adding an extra layer of control. When dual approval is enabled:

- Any new user, permission change, or limit change submitted by one administrator must be approved by a second administrator before taking effect.
- Pending approvals appear in the Notifications drawer under Needs Approval.
- The submitting administrator cannot also be the approving administrator.

Approval Workflow

Step	Action
1	Administrator A submits a new user or a change to a user's permissions/limits.
2	Administrator B logs in and reviews the pending approval in the Notifications drawer or the User Maintenance list.
3	Administrator B reviews all details and approves or rejects with comments.
4	If approved, the change takes effect immediately. If rejected, Administrator A is notified and can revise and resubmit.

> ℹ **TIP**
> If your company has only one administrator and dual approval is enabled, you will need to contact Fulton Bank to process changes that require a second approver.

Managing Alerts

BOSS Online Banking can send automated alerts to notify users about key account activities. Alerts are configured in the Alerts Center, accessible from Administration & Settings.

Alert Types

Alert Type	Trigger
Large Credit	A credit above a specified dollar amount posts to an account.
Large Debit	A debit above a specified dollar amount posts to an account.
Insufficient Funds	Account balance falls below a specified threshold.
Payment Approval Required	A payment is submitted and awaiting approval.
Payment Approved	A submitted payment has been approved.
Payment Rejected	A submitted payment has been rejected.
Positive Pay Items Loaded	Next-day positive pay items are loaded and ready for review.
Suspect Item Decision Required	A positive pay suspect item requires a pay/return decision.
ACH Exception	An ACH transaction is flagged for review against your authorization rules.
New User Added	A new sub-user has been added to your company.
User Locked Out	A user has been locked out due to failed login attempts.

Configuring Alerts

Step	Action
1	Navigate to Administration & Settings → Alerts Center.
2	Click the Alerts tab to see all available alert types.
3	Click an alert name to open its configuration.
4	Enable the alert and select one or more recipients.
5	Set any applicable thresholds (for example, the dollar amount for a Large Credit alert).
6	Save the alert configuration.

> **NOTE**
> Positive Pay-related alerts (Positive Pay Items Loaded and Suspect Item Decision Required) are automatically assigned to users with positive pay decision permissions. These do not need to be manually configured.

Preferences & Passcode Maintenance

Changing Your Password

Administrators can change their own password at any time through the Utilities menu at the top right of the screen.

Step	Action
1	Click the Utilities menu (below your login name, upper right).
2	Select Change Password.
3	Enter your current password and then your new password twice to confirm.
4	Click Save.

Unlocking a Locked User

If a user is locked out after too many failed login attempts, an administrator can unlock them from User Maintenance. Locate the user, open their record, and click Unlock (or Restore if the account shows as disabled).

> **TIP**
> Remind users to contact an administrator rather than repeatedly attempting incorrect passwords. Multiple failed attempts will lock the account and require administrator intervention to restore access.

Need Help?

If you need assistance, please reach out to the Fulton Bank Cash Management team. We're happy to help.