FULTON BANK

BOSS Online Banking Platform

Admin Controls & User Maintenance Guide

Managing Users, Permissions & Approval Controls

This guide is intended for BOSS Online Banking administrators. It covers how to manage users, assign permissions, configure dual approval entitlements, set transaction limits, manage alerts, and maintain platform preferences.

Administration Overview

The Administration & Settings section of BOSS Online Banking allows authorized administrators to manage users, assign permissions, configure approval controls, set up alerts, and control access to the platform. This guide is intended for company administrators responsible for managing your organization's BOSS environment.

> ⚠ **WARNING**
> Administrative functions are only available to users with the appropriate Administrative Permissions assigned by Fulton Bank. Contact your bank relationship manager if you need administrative access enabled.

User Permission Model

BOSS Online Banking is configured to use a user-based permission model. Under this model, permissions are assigned directly to each individual user rather than through shared roles. This gives administrators precise, per-user control over what each person can see and do within the platform.

How User-Based Permissions Work

When you create or modify a user in BOSS, you assign permissions directly to that individual. You control exactly which payment types they can access, whether they can create payments, approve payments, or both, which accounts they can transact on, and what dollar limits apply to their activity. Because permissions are tied to the individual, each user's access profile is independent — changes to one user's permissions do not affect any other user.

Permission Architecture

User permissions in BOSS are organized into six distinct areas. Understanding each area is essential when building out a new user. All six areas should be reviewed and configured for every user you add to the platform.

Permission Area	What It Controls	Options Available
Payment Permissions	Controls which payment types (ACH, Wire, Book Transfer, etc.) the user can access and what actions they can take.	Create only, Approve only, Create & Approve, or No Access
Reporting Permissions	Determines which reports, account statements, and transaction history the user can view.	View access enabled or disabled per report type
Risk Management Permissions	Grants access to Positive Pay exception decisions, ACH Authorization Rules, and related fraud controls.	Enable or disable per feature (Positive Pay, ACH Rules, etc.)
Administrative Permissions	Allows the user to manage other users, configure alerts, and access system settings.	Enable or disable per admin function

Permission Area	What It Controls	Options Available
	Only assign to users who will serve as administrators.	
Assigned Accounts	The specific bank accounts the user can view and transact on. Users only see accounts explicitly assigned to them.	Select one or more accounts per user
Transaction Limits	Dollar amount caps on what the user can initiate or approve. Limits can be set per transaction, per batch, or per day.	Per-transaction, per-batch, and daily limits

TIP

When onboarding multiple users with similar access needs, use the Copy Permissions feature in User Maintenance to copy an existing user's permission profile as a starting point. This saves time and reduces the chance of missing a permission area.

User Maintenance

User Maintenance is the central workspace for creating and managing the users who have access to BOSS Online Banking. From here you can add new users, modify permissions, assign accounts, apply limits, and manage account status.

Accessing User Maintenance

Step	Action
1	From the top navigation, select Administration & Settings.
2	In the User Maintenance workspace, click the User Maintenance widget.
3	The list of existing users appears with their current status.

Building and Entitling a New Sub-User

Adding a new user to BOSS involves completing each permission area in sequence. Each step below corresponds to a section within the Add User form. Take care to work through every section — skipping a section does not disable access; in some cases it may leave access open by default.

Step 1 — Basic User Information

Step	Action
1	In the User Maintenance widget, click Add User.
2	Enter the user's First Name, Last Name, Email Address, User ID, and Phone Number.
3	Set the Authentication Method as directed by Fulton Bank. Do not change this setting without guidance from your bank contact.
4	Confirm the email address is correct. The user will receive their login invitation at this address once their record is approved.

Step 2 — Payment Permissions

Payment Permissions determine which payment types the user can access and what actions they are allowed to take. Configure this section carefully based on the user's role in your organization.

Step	Action
1	In the Payment Permissions section, locate each payment type (ACH, Wire, Book Transfer, etc.).
2	For each payment type, select the appropriate access level: Create (can initiate payments but not approve), Approve (can approve payments submitted by others but not create), Create & Approve (full access), or leave blank for No Access.
3	If the user will work with ACH payments, expand the ACH settings to configure any ACH-specific options such as payment group access.
4	Review your selections before moving to the next section. Payment permissions directly affect what the user sees on their home dashboard.

TIP

For strong internal controls, it is recommended to separate the Create and Approve functions between different users. Allowing one person to both create and approve their own payments removes an important check. Fulton Bank recommends establishing a dual-control structure for ACH and Wire payments.

Step 3 — Reporting Permissions

Step	Action
1	In the Reporting Permissions section, review the available report types.
2	Enable access to any reports the user needs to perform their job (e.g., account statements, payment history, check images).

Step	Action
3	Restrict reporting access for users who do not need visibility into account balances or transaction history.

Step 4 — Risk Management Permissions

Step	Action
1	In the Risk Management Permissions section, enable Positive Pay access if this user will be responsible for making pay/return decisions on exception items.
2	Enable ACH Authorization Rules access if this user will manage authorized debit rules for your accounts.
3	Leave these settings disabled for users who do not participate in fraud control workflows.

Step 5 — Administrative Permissions

Step	Action
1	In the Administrative Permissions section, enable admin functions only if this user needs to manage other users, configure alerts, or access system settings.
2	Common admin permissions include User Maintenance (ability to add/modify users) and Alert Management.
3	Limit the number of users with full administrative access. Most end users should not have Administrative Permissions enabled.

> ⚠ **WARNING**
> Granting Administrative Permissions to a user gives them the ability to modify other users' access, including adding new users and changing approval limits. Only grant admin access to users who genuinely need it.

Step 6 — Assigning Accounts

Step	Action
1	In the Assigning Accounts section, select the bank accounts this user should have access to.
2	Only accounts explicitly assigned here will be visible to the user when initiating or approving transactions.
3	If your organization has multiple accounts, take care to assign only the accounts relevant to this user's job function.
4	Account assignments can be updated at any time by modifying the user record.

Step 7 — Submitting the New User

Step	Action
1	Review all permission sections before submitting.
2	Click Submit. The new user record is placed in Pending Approval status.
3	A second authorized administrator must approve the record before the user can log in.
4	Once approved, the user will receive an email invitation to set up their login credentials.

> **TIP**
> New users will receive their login invitation at the email address entered during setup. Confirm the address is accurate before submitting. If the email is incorrect, the invitation will need to be resent after correcting the user record.

Modifying and Managing Existing Users

Modifying a User's Permissions

Step	Action
1	In the User Maintenance widget, find the user to modify.
2	Click Modify (or select Modify from the Actions menu).
3	Update the user's permissions, account assignments, or limits as needed.
4	Click Submit. Changes require approval from a second administrator before taking effect.

> **TIP**
> When onboarding a new user with a similar access profile to an existing employee, use the Copy Permissions option within User Maintenance to copy permission settings from the existing user. Review and adjust as needed before submitting.

Approving a New or Modified User

Step	Action
1	In the User Maintenance widget, filter for users with a status of Entered or Pending Approval.
2	Select the user to approve.
3	Review the submitted permissions carefully before approving.

Step	Action
4	Click Approve. The user record becomes active.

Disabling a User

If an employee leaves the organization or needs to be temporarily locked out, disable their account immediately. A disabled user cannot log in, but their permission history and transaction records are preserved for audit purposes.

Step	Action
1	In the User Maintenance widget, find the user.
2	Select Disable from the Actions menu.
3	Confirm the action. The user's account is immediately suspended.

> ⚠ **WARNING**
> Disable user accounts promptly when an employee leaves the organization. Do not wait until their official last day if access should be removed sooner. Delayed disabling is one of the most common sources of unauthorized access.

Restoring a Disabled User

Step	Action
1	Filter the User Maintenance list to show Disabled users.
2	Select the user to restore.
3	Click Restore. The account is reactivated and requires approval before the user can log back in.

Dual Approval Entitlements & Limit Approvals

Dual approval is one of the most important fraud prevention controls available in BOSS Online Banking. When properly configured, it requires that a second authorized user approve a payment before it can be processed — no single user can both create and release a payment on their own. This section explains how to set up dual approval at the user level and how to use transaction limits to enforce approval thresholds.

What is Dual Approval?

Dual approval means that for a payment to be processed, it must be submitted by one user and approved by a separate, authorized user. The approver must have the Approve permission (not just Create) for that payment type, and must be a different person than the one who initiated the payment.

Dual approval is configured through the combination of two settings: the payment permissions assigned to each user (Create vs. Approve), and the transaction limits set on those users. Together these controls determine who can initiate payments, who must approve them, and at what dollar amounts approvals are triggered.

> **TIP**
> Fulton Bank strongly recommends enabling dual approval for all Wire payments and for ACH batches above a defined dollar threshold. This provides a critical second line of defense against both external fraud and internal errors.

Setting Up Dual Approval Entitlements

Dual approval is established by how you entitle your users in the Payment Permissions section. The key is to ensure that your creators and approvers are separate individuals and that their permissions are configured accordingly.

Step	Action
1	Identify which users in your organization will serve as payment creators (initiators) and which will serve as approvers. These should be different people.
2	For payment creator users: in the Payment Permissions section, set their access to Create only for the applicable payment types (ACH, Wire, etc.). Do not also enable Approve.
3	For approver users: in the Payment Permissions section, set their access to Approve only (or Create & Approve if they also need to initiate payments themselves, though this reduces control).
4	Make sure at least one user per payment type has Approve access. Without an approver, payments submitted by creators will remain in pending status and cannot be released.
5	Submit and approve each user record as described in the User Maintenance section above.

> **TIP**
> A user set to Create & Approve can approve their own payments, which effectively bypasses dual control. If you want strict dual approval, keep Create and Approve as separate user entitlements assigned to different individuals.

Limit Approvals — Controlling What Each User Can Approve

Transaction limits allow you to set dollar-based thresholds on what a user can initiate or approve. Limits are configured in the Limits section of each user record and work in combination with payment permissions to define the full scope of a user's authority.

Limit Type	What It Controls	Example Use Case
Per-Transaction Limit	The maximum dollar amount for a single payment this user can create or approve.	A payment clerk limited to $25,000 per transaction.
Per-Batch Limit	The maximum total dollar amount for a single ACH batch this user can submit or approve.	An ACH operator limited to $100,000 per batch submission.
Daily Limit	The maximum total dollar amount this user can initiate or approve across all transactions in a single business day.	An approver capped at $500,000 in total daily approvals.

Setting Transaction and Approval Limits on a User

Step	Action
1	In the User Maintenance widget, open the user record (Add User or Modify User).
2	Scroll to the Limits section at the bottom of the user form.
3	For each payment type (ACH, Wire, etc.), enter the applicable per-transaction limit. Leave blank to apply no limit for that payment type.
4	Enter a Per-Batch limit for ACH users if your organization wants to cap the total size of any single batch submission.
5	Enter a Daily limit to cap the total volume a user can process or approve in a single business day.
6	Click Submit. Limit changes require approval from a second administrator before taking effect.

⚠ **WARNING**

Limits apply to both Create and Approve functions based on how the user is entitled. If a user has a $50,000 per-transaction limit, they cannot approve a payment above $50,000 even if another user submitted it. Ensure your approvers have limits appropriate for the payments they will be reviewing.

Recommended Dual Approval Configuration

The following is a recommended starting framework for establishing dual approval controls. Adjust based on your organization's specific needs and transaction volumes.

User Type	Payment Permission	Suggested Limits
Payment Clerk / Initiator	Create only — ACH and/or Wire	Per-transaction limit set at your normal payment ceiling; no daily limit required if approver controls are in place.
Payment Approver	Approve only (or Approve + Create if dual role)	Per-transaction limit at or above your highest expected payment; daily limit set to your organization's maximum daily exposure threshold.
Senior Approver / Admin	Create & Approve (or Approve only)	Higher limits for elevated approvals; consider a separate senior approver for payments above a defined large-dollar threshold (e.g., wires over $500,000).

TIP

Contact your Fulton Bank relationship manager if you need guidance on setting appropriate limit thresholds for your organization. Getting this configuration right at setup is much easier than correcting it after users are live.

Managing Alerts

BOSS Online Banking can send email or SMS alerts to notify users and administrators of important events — such as payments pending approval, positive pay exceptions ready for review, or new users added to the system. Alerts are configured from the Alerts Center within Administration & Settings.

Adding an Alert for a User

Step	Action
1	From Administration & Settings, navigate to the Alerts Center.
2	Click Add Alert.
3	Select the Alert Type from the list (see common types below).

Step	Action
4	Select the account(s) or condition(s) that trigger the alert.
5	Select the recipient: enter their email address or select from existing contacts.
6	Click Save.

Common Alert Types

Alert Type	When It Fires
Payment Pending Approval	Notifies approvers when a payment has been submitted and is waiting for their review.
Positive Pay Suspect Items Loaded	Notifies reviewers when positive pay exception items are available for pay/return decisions.
New User Added	Alerts administrators when a new user record has been created and is pending approval.
User Approved	Alerts administrators when a user record has been approved and the user is now active.
ACH Authorization Rule Pending Approval	Notifies when a new ACH authorization rule has been submitted and requires approval.
Check Issue Management File Loaded	Alerts when a check issue file has been imported successfully and is ready for review.

TIP

Set up payment pending approval alerts for all users who have Approve permissions. This ensures approvers are notified in real time rather than having to check the platform manually. Timely approvals are especially important for same-day ACH and wire payments where deadlines apply.

Preferences & Passcode Maintenance

The Preferences Workspace, accessible from Administration & Settings, contains administrative settings for the platform. Most preference options are pre-configured by Fulton Bank at implementation. The primary area you will interact with regularly is Passcode Maintenance.

Passcode Maintenance

Passcodes are used as part of multi-factor authentication workflows in BOSS. Administrators can view and manage user passcodes from the Passcode Maintenance widget in the User Maintenance workspace.

Step	Action
1	From Administration & Settings, navigate to the User Maintenance workspace.
2	Click the Passcode Maintenance widget.
3	Locate the user whose passcode needs to be reset or reviewed.
4	Select the appropriate action (reset, unlock, or view status).
5	Confirm the action. The user will receive instructions for setting a new passcode.

TIP

If a user is locked out due to failed authentication attempts, an administrator can reset their access from the Passcode Maintenance or User Maintenance areas. Users do not need to call Fulton Bank for routine lockout resets — this can be handled directly by your organization's administrator.

For additional assistance with administration, user setup, or entitlement configuration, contact your Fulton Bank relationship manager or client support team.