Digital Banking Guide

Policy Administration

CAPITAL BANK

capitalbankmd.com

Member FDIC

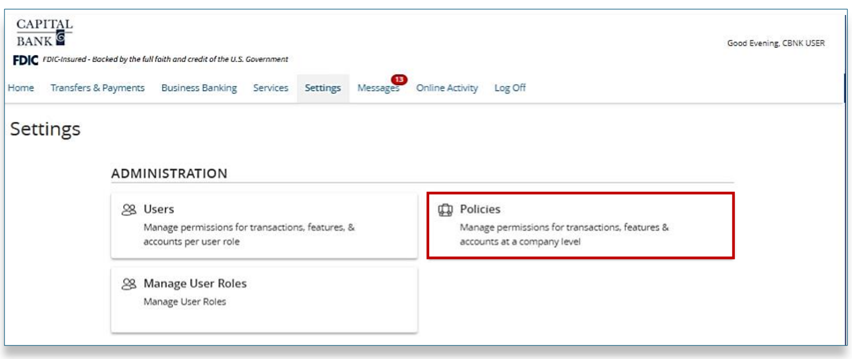
User Guide – Policy Administration

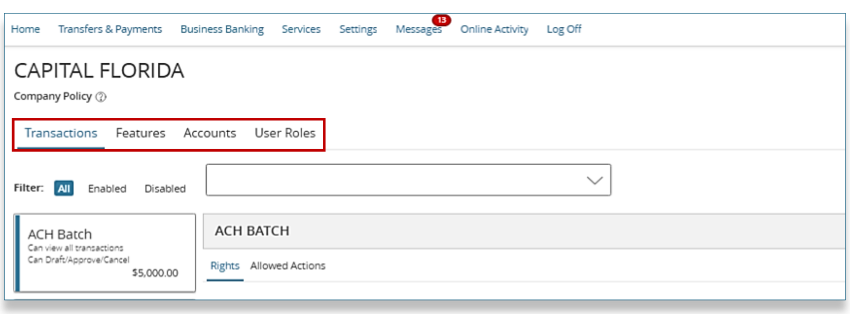
Introduction to Policy Administration

The ‘Company Policy’ feature in Capital Bank’s Digital Banking gives business administrators a centralized way to manage users rights, limits and entitlements at a company level. It can be used to define accounts, transaction types, and features that can be made available along with specific permissions for users at different levels within a company.

Users have administrative rights and ‘Manage Company Policy’ permission can update parts of the policy, such as enabling or disabling transaction types, features and setting transaction limits. However, the policy itself cannot be deleted. This feature is helpful in ensuring consistent and secure activity management for all users in the organization.

Please Note: Based on your company settings, if ‘Dual Action for non-financial transactions’ is enabled, any changes to the policy will require approval from a second authorized user, adding an extra layer of security and control.



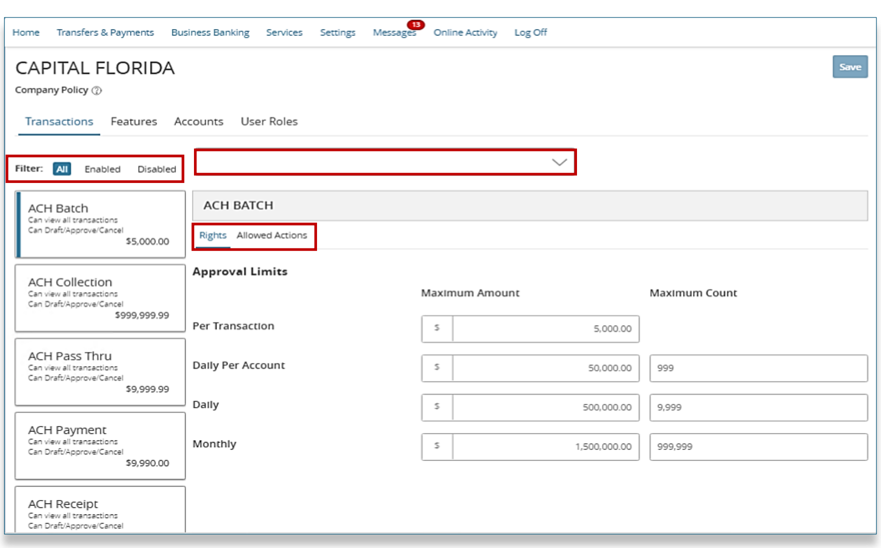


Overview:

This user guide will give an overview of the ‘Company Policy’ features. It also lists the process of managing company-level permissions for transactions, features and accounts.

Company Policy Overview
Navigation:

1. Navigate to the ‘Policies’ tile from the ‘Administration’ section available under the ‘Settings’ tab.
2. Click on the ‘Policies’ tile to further navigate to the ‘Company Policy’ page. This page contains the below given tabs/ sections:
   a. Transactions
   b. Features
   c. Accounts
   d. User Roles



Section 1: Transactions Tab

The ‘Transactions’ tab in the Company Policy section displays a list of all transaction types available to the company, along with their associated ‘Rights’ and ‘Allowed Actions’.

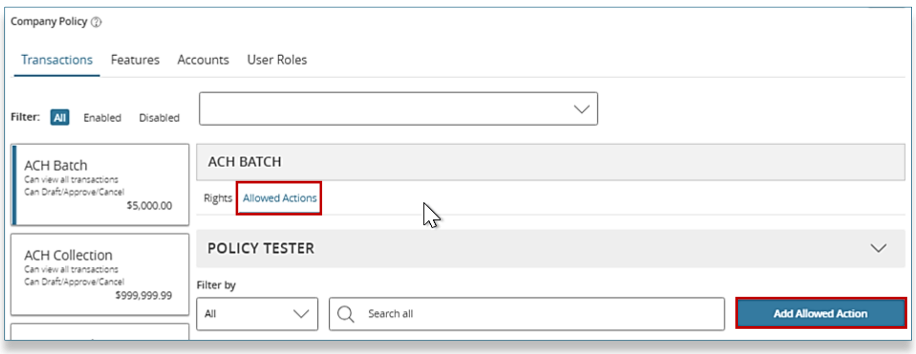
1. *Filter*: You filter for ‘All’, ‘Enabled’ and ‘Disabled’ transaction types using the respective links.

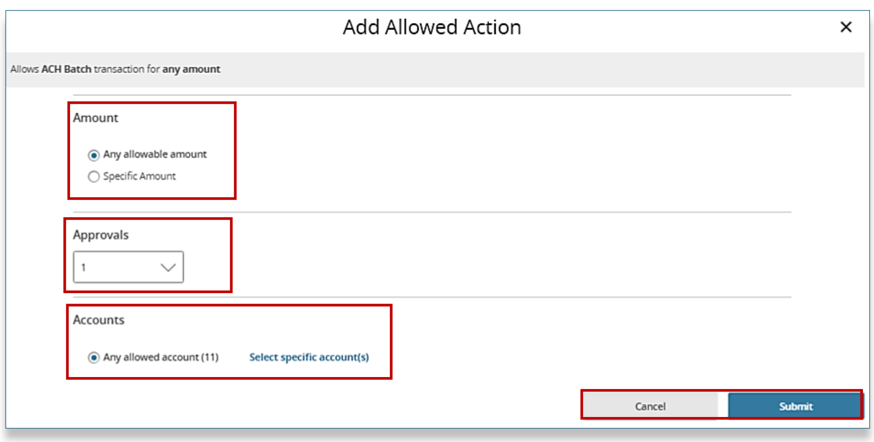
2. Additionally, you can search and select the required transaction type using drop-down.

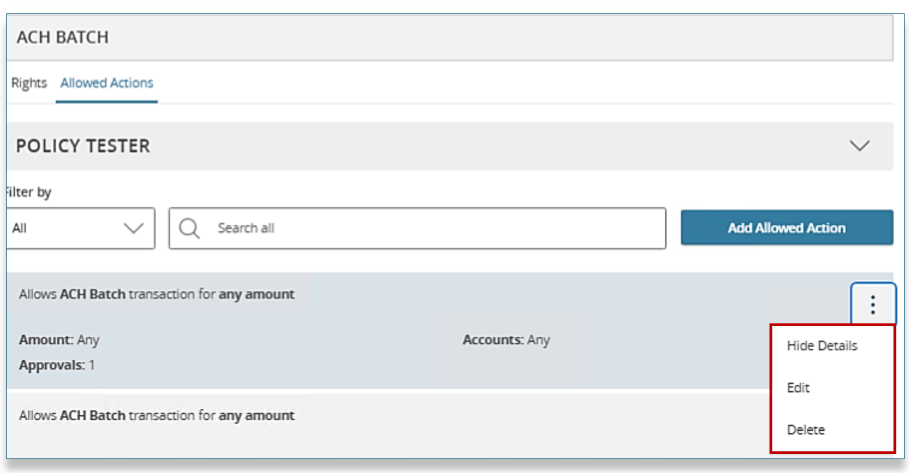
3. The following details will be visible and can be modified for the selected transaction type:

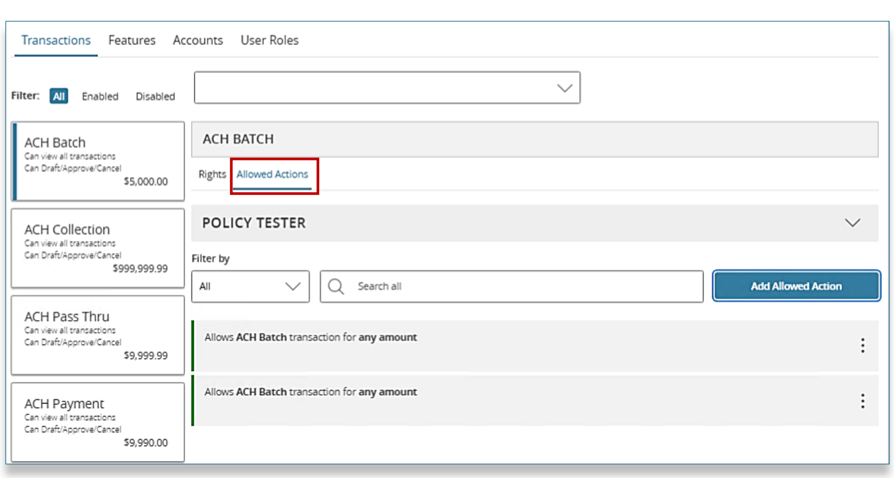
   a. *Rights*: define approval limits at a company level. These limits can be modified as individual user level.
   Approval Limits are defined at ‘Per Transaction’ ‘Daily Per Account’ ‘Daily’ and ‘Monthly’ level and can be assigned as a value - ‘Maximum Amount’ and as a count - ‘Maximum Count’.

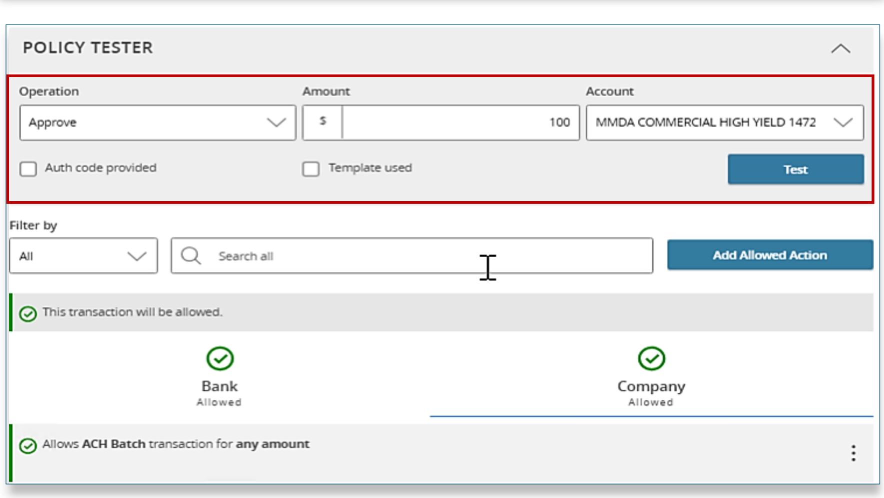
Please Note: The limits defined under the Policies tab are non-editable and displayed for viewing only.

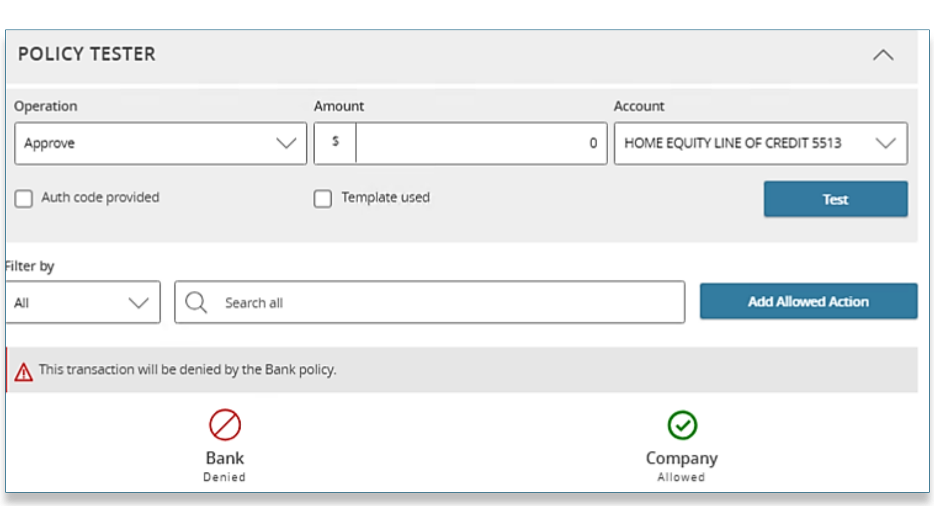












b. *Allowed Actions*: used for assigning actions / operation rights for the selected transaction type.
Based on the transaction type selected, the applicable allowed actions can be viewed by clicking on the 'Add Allowed Action' button.

On the 'Add Allowed Action' overlay, make the required selections and click on 'Submit' to save the changes.

Click the 'Add Allowed Action' button to add a new allowed action

1. *Amount*: You can assign a 'Specific Amount' or select the 'Any Allowable Amount' radio button to enable the action for an unlimited amount.
2. *Approvals* (*Dropdown*): Specify the number of approvals required for each transaction type using the dropdown.
3. *Accounts*: Select the accounts can be made available for the selected transaction type.
   You can 'Select specific account(s)' or assign "Any allowed account".
4. On completing the selections, click 'Submit' to save and return to the Company Policy page

The selected 'allowed Actions' will be displayed in the lower section. Use the ellipsis to perform the following actions:

Edit: Use the 'Edit' option to modify the existing selections.

View / Hide Details: Use the 'View / Hide Details' expand / collapse the Allowed Actions details

Delete: Use the 'Delete' option to delete an existing Allowed Action from a Transaction Type

Policy Tester:

On adding the allowed actions, to review the structure and working of the assigned actions, click on the 'Policy Tester' arrow to view its validity and consistency.

The 'Policy Tester' feature is used to test assigned actions before updating them at the company level.
This helps in ensuring that transaction entitlements align with both Bank and Company Policies.
Use the 'Policy Tester' feature to verify changes made to the 'Allowed Actions' before submitting the changes.

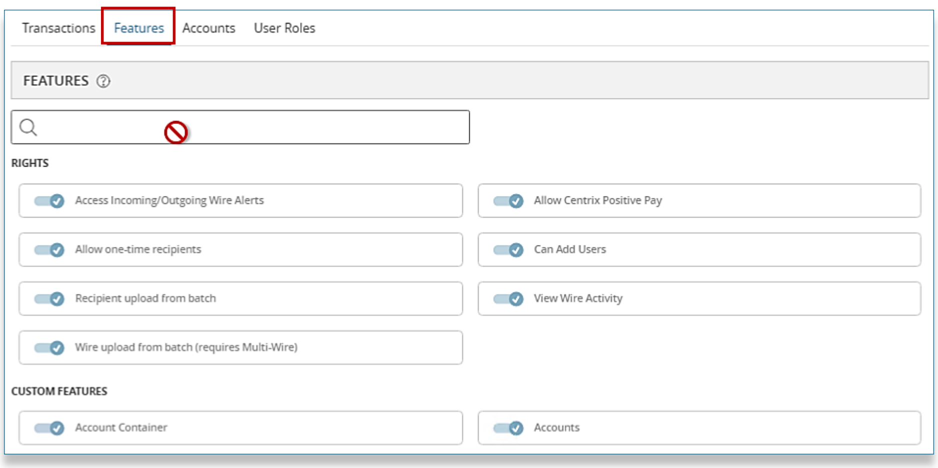
Select the 'Operation' type using the dropdown and update data in the corresponding fields of 'Amount' and 'Account'.

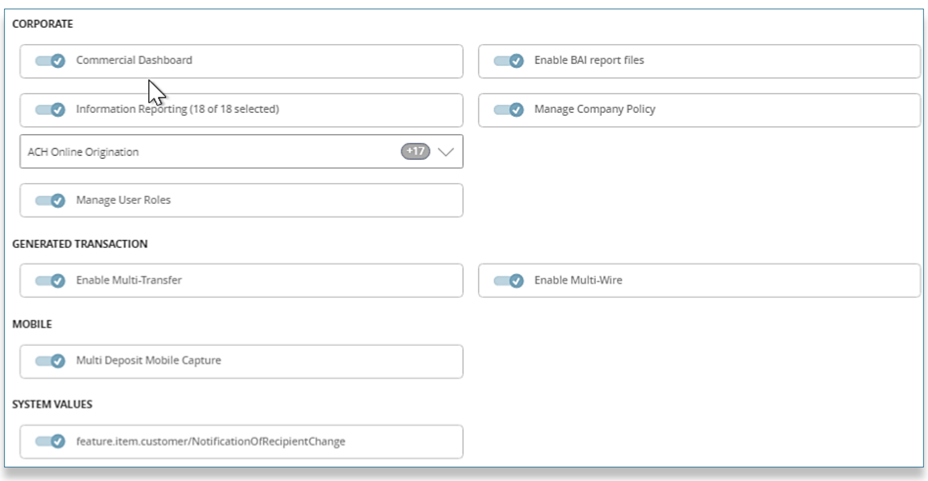
If you wish to add a security layer to the selected operation, select the 'Auth code provided' checkbox. This will require the user to provide an authorization code or code to complete the action.

If you wish to grant access for the selected operation to a 'Drafts Restricted User' select the 'Template used' checkbox.
Click on 'Test' to view the results. The result will display of the company policy settings and bank settings are in sync or not.

In case the policy tester fails, an error message will be displayed highlighting the reason for failure.

The Policy Results appear and indicate whether the Company Policy and FI settings will allow or deny the transaction, depending on your Allowed Actions.





Section 2: Features Tab

The 'Features' tab contains a list of features that have been assigned to your company by the bank.
This is a read-only display and cannot be modified.

Features are categorized as under:

1. Rights: include creation of recipients, alerts, manage users, Positive Pay, upload rights etc.

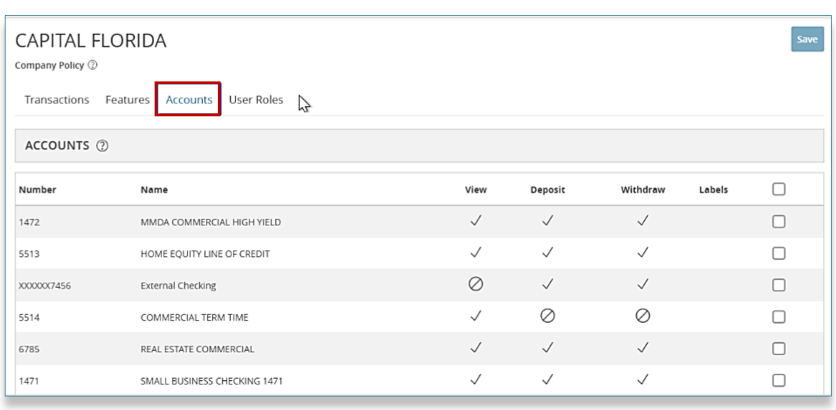
2. Custom Features: include Accounts, Advanced E-statement viewer, Business Enrollment, Address Management etc.

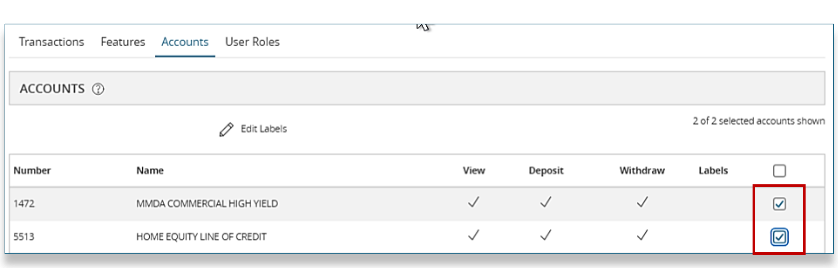
3. Corporate: Commercial Dashboard, Information Reporting options, Manage Company Policy, BAI File Report files, manage User roles etc.

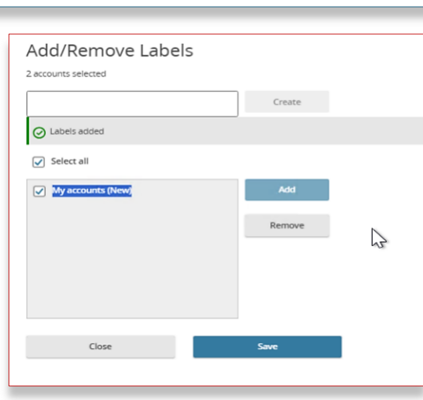
4. Generated Transaction: for enabling multi-payments

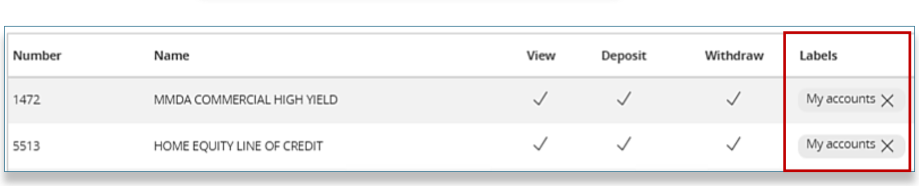
5. Mobile: Multi Deposit Mobile Capture.

6. System Values









Section 3: Accounts Tab

The Accounts tab shows the list of accounts available at the company level.
The accounts list is displayed in a read-only format.
This list also specifies the allowable operations associated with the accounts.

Account Labels: The Account Labels features allows you to combine and group accounts to suit your viewing and usage preferences.
You can club accounts based on their location, purpose or accounting preference by assigning them an Account Label.

To create or edit an 'Account Label':

1. Select the checkbox adjacent to the required 'Accounts' and click on the 'Edit Labels' link to add or modify the label.

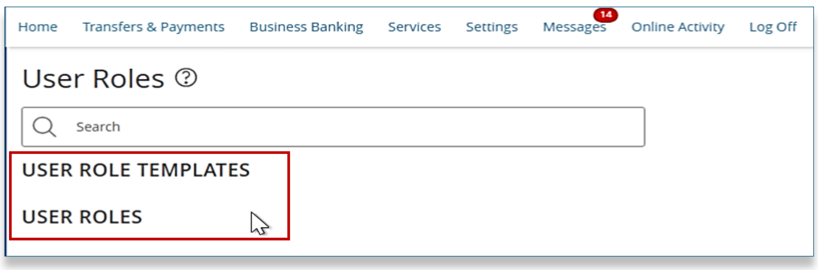
2. On the 'Add / Remove Labels' overlay, enter a new label name and click "Create" to add it.

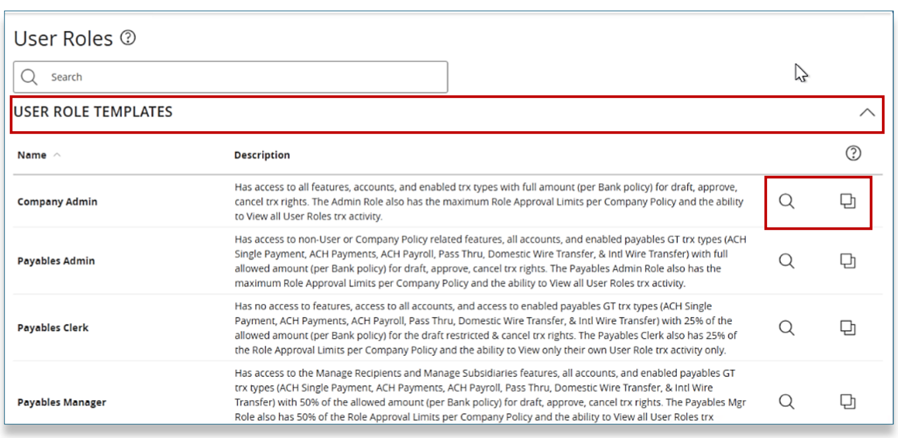
3. The created label name will be displayed in the gray box below.

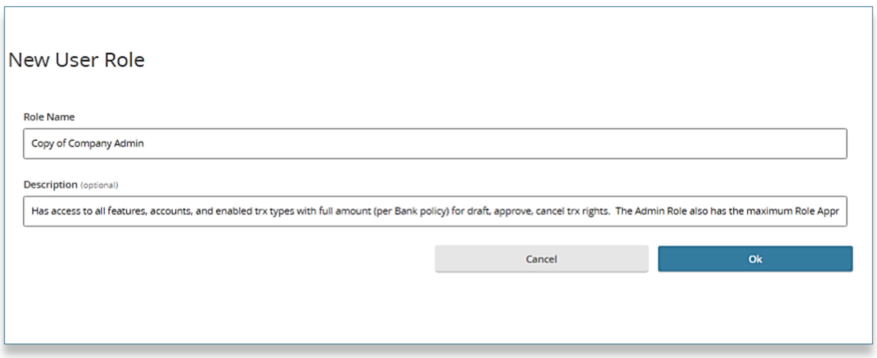
4. Select the label and click on Check the box next to an existing label to apply it to the account and click the 'Add button.

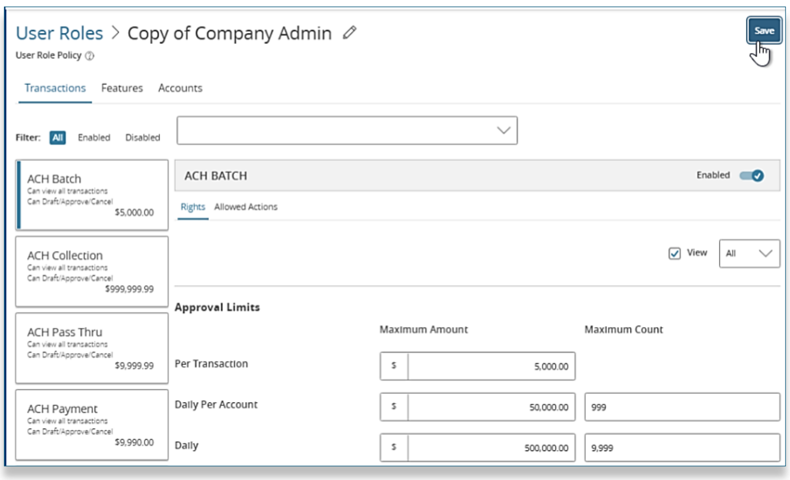
5. Click 'Save' to confirm your changes.

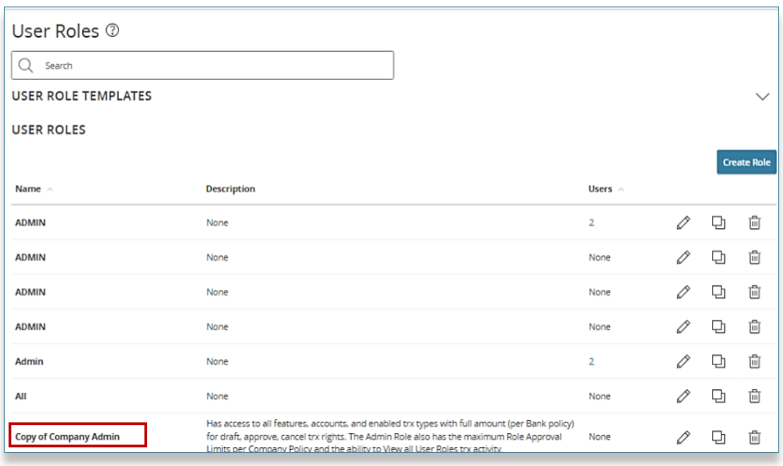
6. Click on 'X' icon in labels column on Accounts tab to remove the label











Section 4: User Roles

The User Role Templates feature can be used to ensure ease and consistency in assigning roles and entitlements to users.

Each corporate end user can be assigned a user role based on their profile, role in the organization and the permissions they may need to perform their roles.
User roles should align with company policy and reflect user responsibilities, such as drafting or approving transactions, without exceeding policy limits. Pre-defined user role templates can be used or modified based on individual organizational needs.

1. User Roles Templates

A default list of user role templates is assigned to each corporate entity based on their bank's settings and group policies.
Entities may choose to map their roles to the existing templates or modify the existing templates as needed.
Existing role templates can be copied and assigned to a user. If needed, user role templates Transaction Types, Accounts, Limits, Rights etc. can be modified for a specific user level.
Any user level modifications need secondary approval and will be available on the user's next login.

1. Click on 'User Role Templates' link to view the list of existing role templates.

2. Use the search bar to type a keyword and locate the required template

3. Use the 'magnifying glass' to view the policy associated with the selected template.

4. To create a new User Role using the template click on Copy icon, give entitlements and save which will list it under User Roles section

The following are a few User role templates which may appear if and where applicable.

- *Admin Role*: Admin has all access in the system like create, approve, cancel transactions, and see all user activity. They have full access and the highest limits allowed by the company.

- *Payables Admin*: Can manage all payment types (ACH, Payroll, Wires, PassThru) with full access to create, approve, and cancel transactions. It has the highest approval limits and can view all user activity.

- *Receivables Admin*: Can manage all incoming payment types (ACH Receipts, Collections, PassThru). Can create, approve, and cancel transactions, view all user activity, and has the highest approval limits.

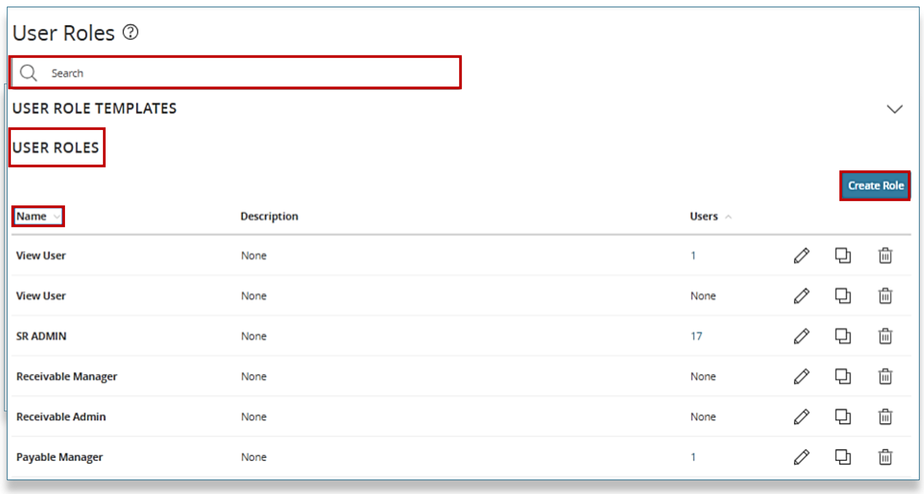
- *Payables/Receivables Admin*: Handles both payments and incoming funds with full access to all transaction types. Can create, approve, and cancel transactions, see all user activity, and has the highest approval limits.

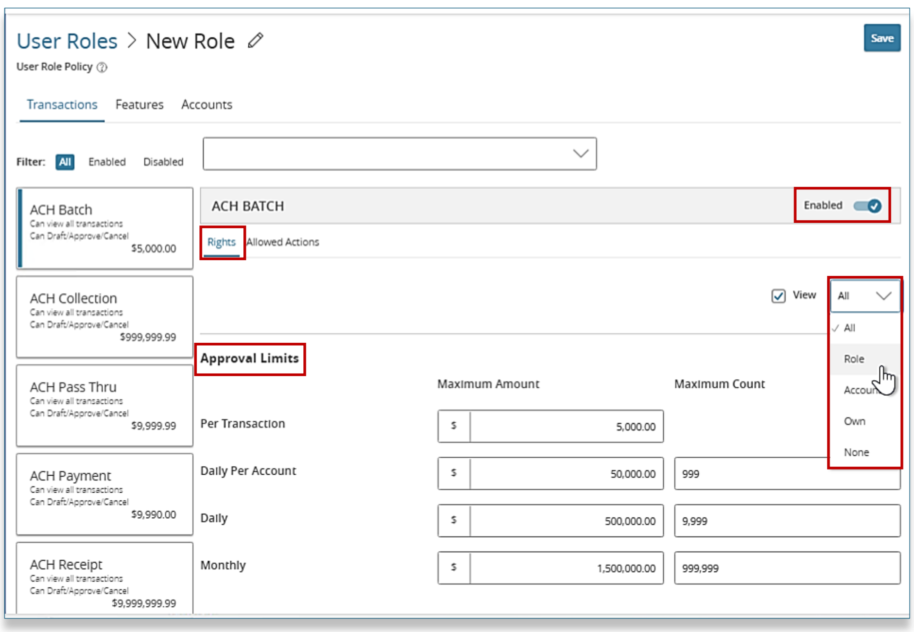
- *Payables Manager*: Manages payment types and recipients with access to accounts and payables. Can create, approve, and cancel transactions up to 50% of the allowed limits. Can see all user activity.

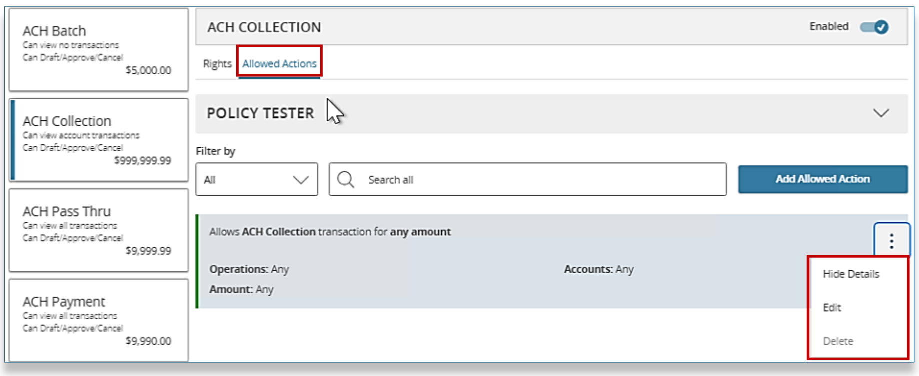
- *Receivables Manager*: Manages incoming payments and recipients. Can create, approve, and cancel receivables up to 50% of the allowed limits. Can view all user activity.

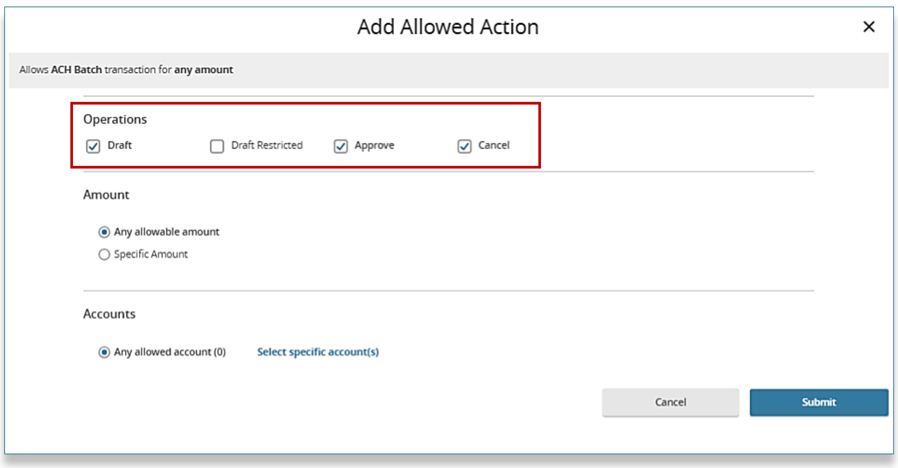
- *Payables Clerk*: Can draft and cancel payment transactions (ACH, Payroll, Wires) up to 25% of the allowed limits. Can only see their own activity. No access to other features.

- *Receivables Clerk*: Can draft and cancel receivable transactions up to 25% of the allowed limits. Can only view their own activity. No access to other features.
- *View Only*: Can view all accounts and receivable transactions (ACH Receipts and Collections). No access to make changes or use features.









2. User Roles

The User roles section displays list of created user roles

1. Click on 'User Role' text to expand the section
2. Use the search bar to quickly find specific user roles.
3. Click the 'Sort' icon next to a column to sort roles by name, description, or number of users.
4. The number in the 'Users' column shows how many users are assigned to that role, click it to view the list of assigned users

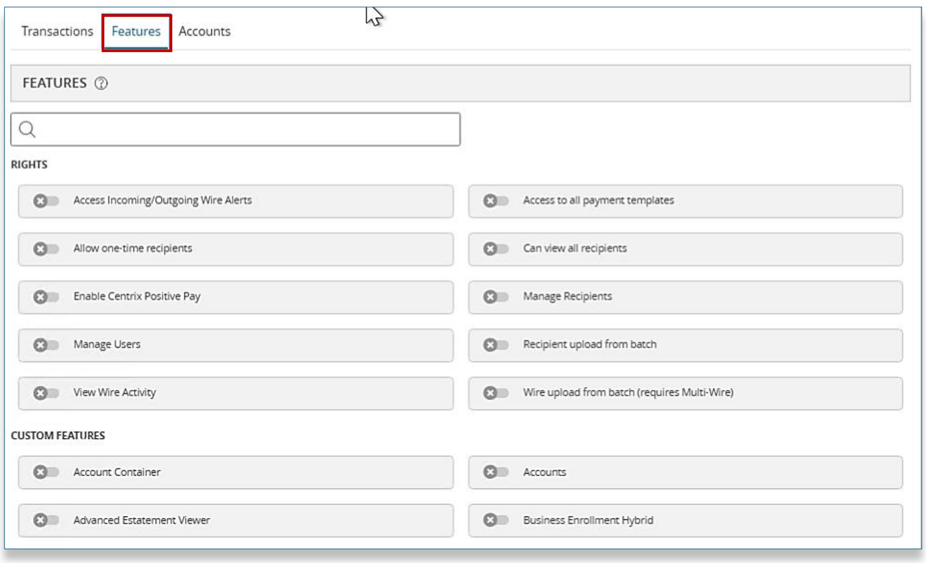
2.1. Create User Role

1. Click on 'Create Role' button and navigate to the 'New User Role' page.
2. Enter a 'Role name' and a brief 'Description' and click on 'Ok' to proceed.
3. You will be navigated to the New Role page which will display tabs for updating entitlements, transactions accesses and limits and other related features.
4. The *'Disabled / Enabled'* toggle on the right hand corner can be used to restrict a user from accessing specific transaction types, such as payroll or international wires.
   a. *Rights*: Use the 'Rights' link to define role specific limits for the selected transaction type.
   b. Select the 'View' checkbox and use the dropdown menu to set transaction view for the user role:
   c. *All*: View all transactions in the company
   d. *Own*: View only their own transactions
   e. *Account*: View transactions involving accounts they have access to
   f. *Role*: View transactions made by others with the same role
   g. *No*: No access to view transactions
   h. *Approval Limits*: User roles can have pre-defined approval limits to monitor the amount and count of transactions they can process. These limits can be set on a daily, monthly, or per-account basis. Modify the required fields and click on 'Save'.

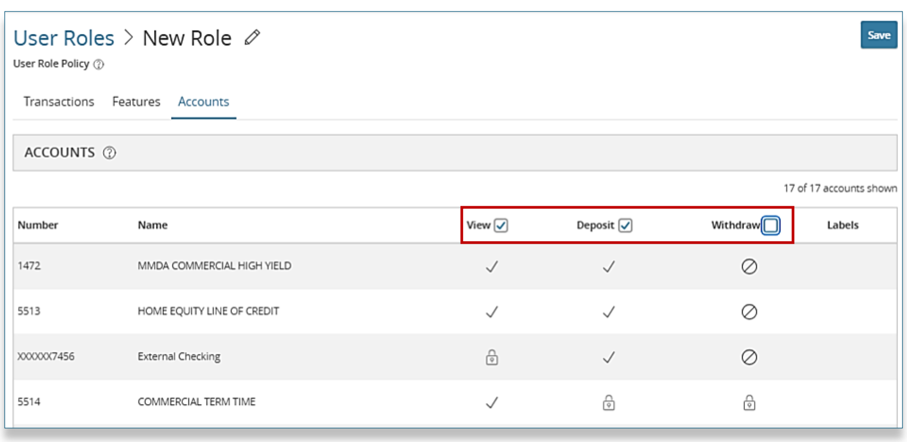
Please Note: Where limits conflict with a higher-level setting, the limit will be highlighted in red.

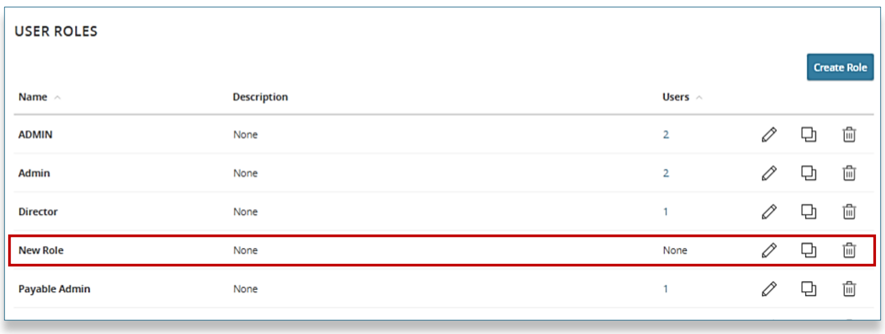
5. *Transactions Tab*: You can view all assigned transaction types along with their approval limits and permitted actions. Use the filter links and dropdown menu to narrow down the list and modify the limits as needed.

   Allowed Actions: used for assigning actions / operation rights for the selected transaction type.
   a. Click on the 'Add Allowed Actions' tab to add or modify the existing allowable actions.
   b. To view or edit existing 'Allowed Actions' click on the ellipsis and select the required operation.
   c. Operations Rights: You can assign the operations a user is allowed to perform on a transaction, such as drafting, approving, or canceling. Simply check or uncheck the boxes to enable or disable specific actions.
   d. *Draft*: Create a transaction or template pending approval.
   e. *Draft Restricted*: Create a drafted transaction from an assigned template, or modify its amount, settlement, date, or description.
   f. *Approve*: Approve or finalize drafted transactions.
   g. *Cancel*: Reject a drafted or unprocessed transaction.

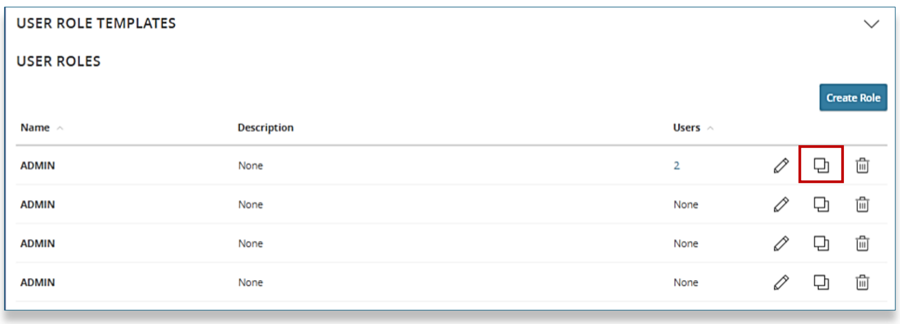


6. *Features in User Role*: The 'Features' tab allows you to manage user permissions for editing templates, managing users, incoming / outcoming wires, recipient upload etc. These permissions vary based on a user's policy or role.
   a. Click the 'edit' icon next to an existing role or select 'Create Role'.
   b. Go to the 'Features' tab.
   c. Toggle features on or off as needed.
   d. Click 'Save' to apply changes.



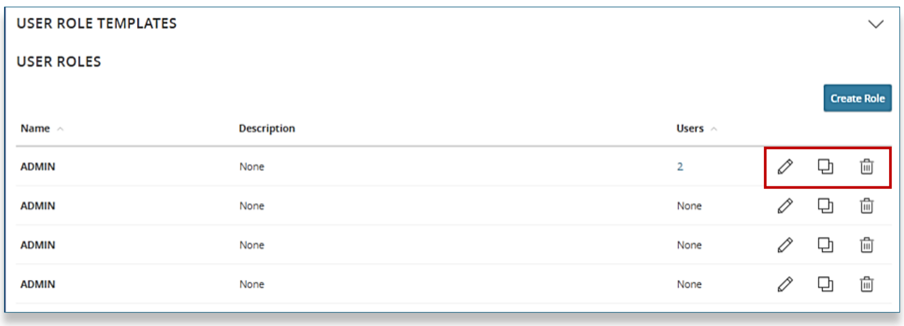


7. *Accounts in User Role*: The 'Accounts' tab allows you to control which users can perform actions on specific accounts, such as viewing account details, accessing transaction history, and making deposits or withdrawals.
   a. Click the 'edit' icon next to an existing role or choose 'Create Role' to create a new role.
   b. Open the 'Accounts' tab.
   c. Adjust each user's permissions to view, deposit to, or withdraw from selected accounts. 'Tick' icon means user rights is active and 'Stop Sign' icon means user rights are disabled.
      View: View balances and history for the account on the Home page, on the Account Details page, and in reports.
      Deposit: Deposit funds into the account. This is applicable to the ACH Receipt and ACH Collections Transaction Types.
      Withdraw: Withdraw funds from the account. This is applicable to the ACH Single Payment, ACH Payments, Payroll, Domestic Wire, International Wire, and Tax Payment Transaction Types.
   d. *Click* 'Save' to finalize your changes.



3. Copy Role

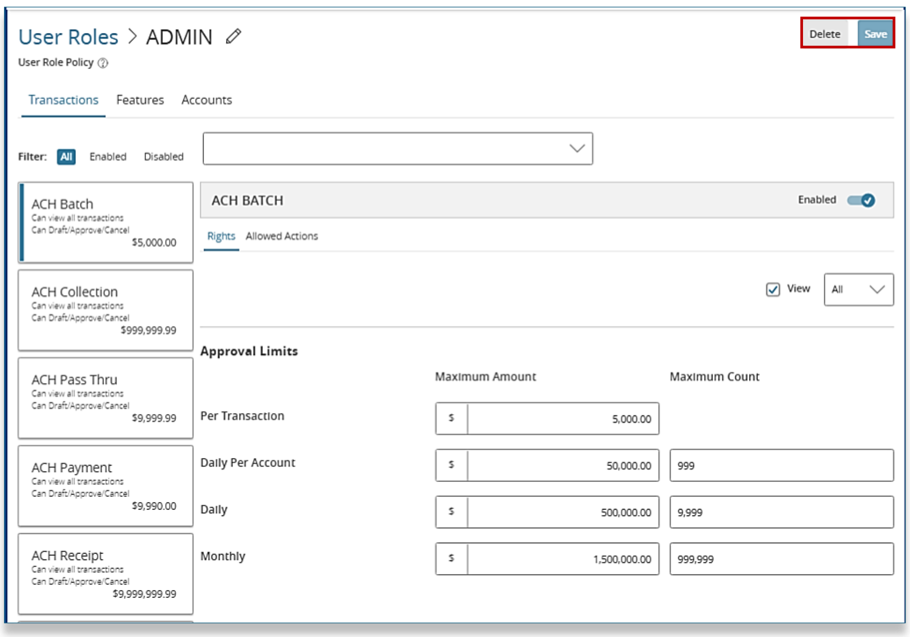
To create a new role based on an existing template or existing user role, click the 'Copy' icon to duplicate a default User Role Template from the user roles list and make any needed adjustments and enter a role name.

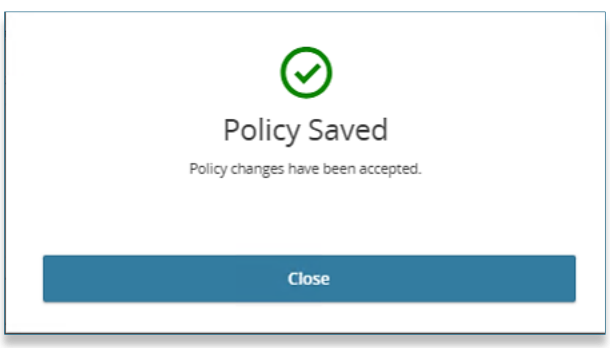


4. Edit User Role

To modify an existing user role, click the 'Edit' icon, system will open a 'User Role' page, make the necessary changes, and click 'Save'.

Please Note: Users with 'Manage User Roles' permissions can select a transaction type to edit at the role level.





5. **Delete User Role**

Users with the ‘Manage Users’ permission can permanently delete user roles that are no longer needed. To do this,

a. Click the delete icon next to the role, then confirm by clicking the ‘Delete’ button.

OR

b. Click on ‘Edit’ icon beside the user role and then click ‘Delete’ button