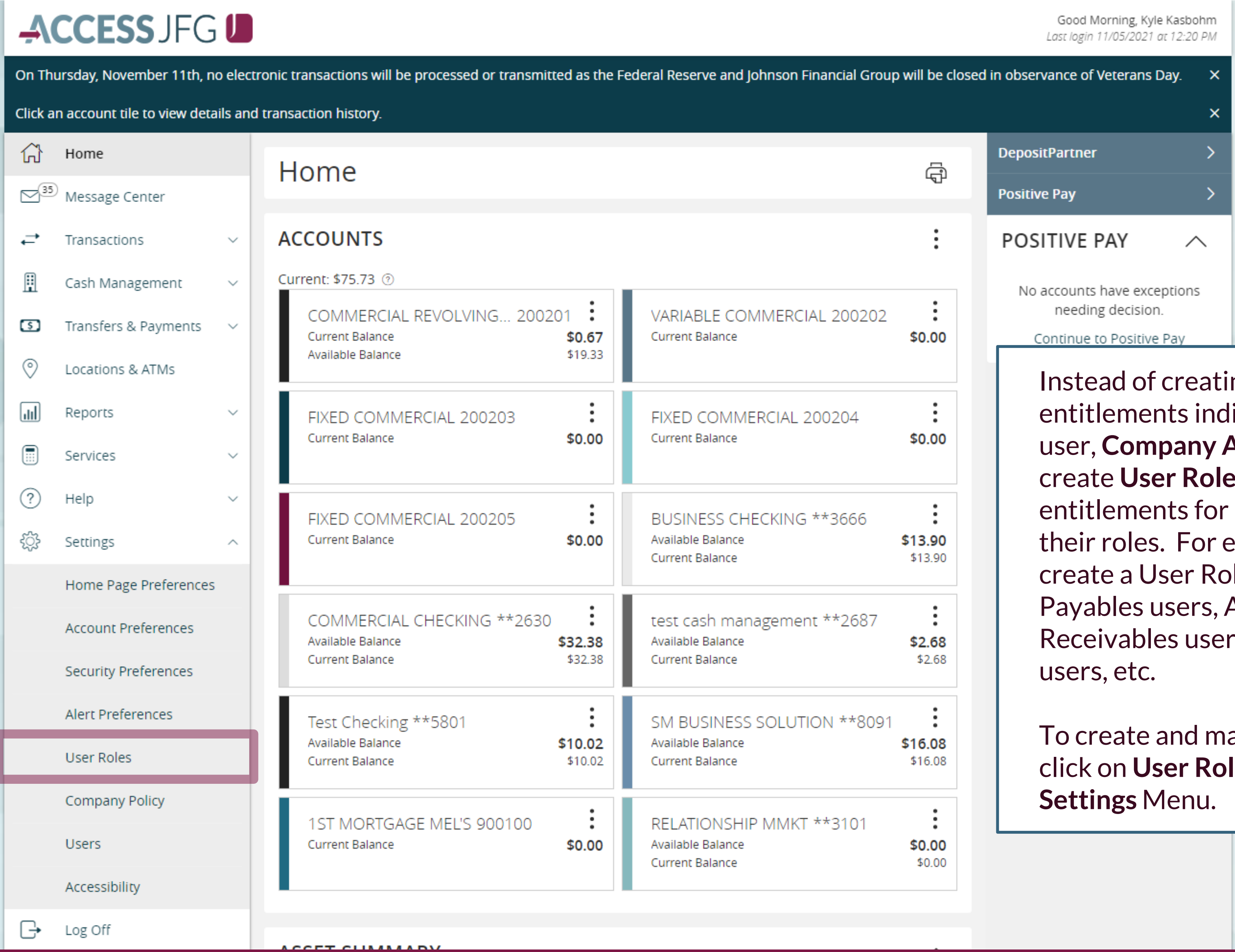
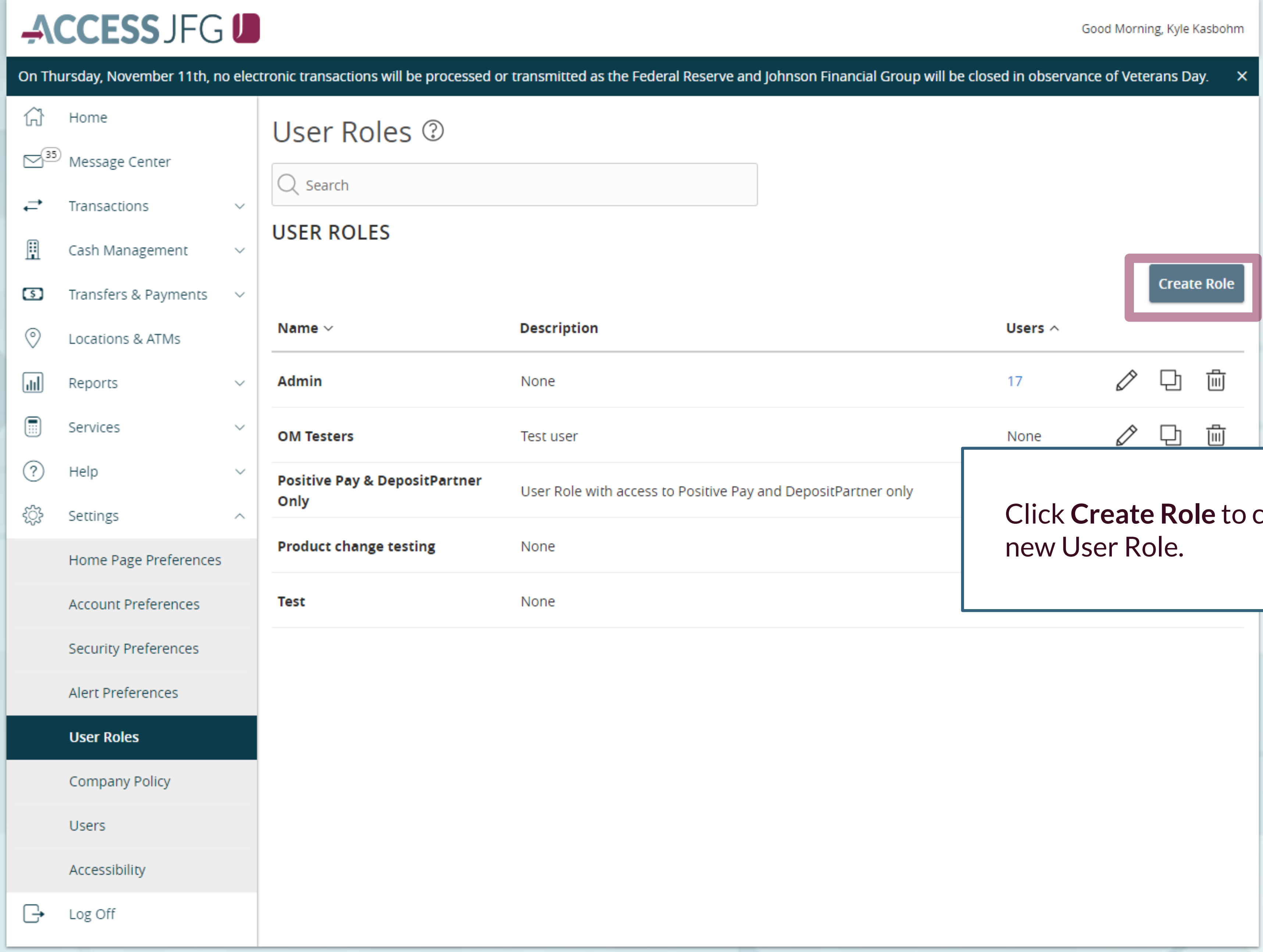
Managing Corporate Users and User Roles

JOHNSON FINANCIAL GROUP®

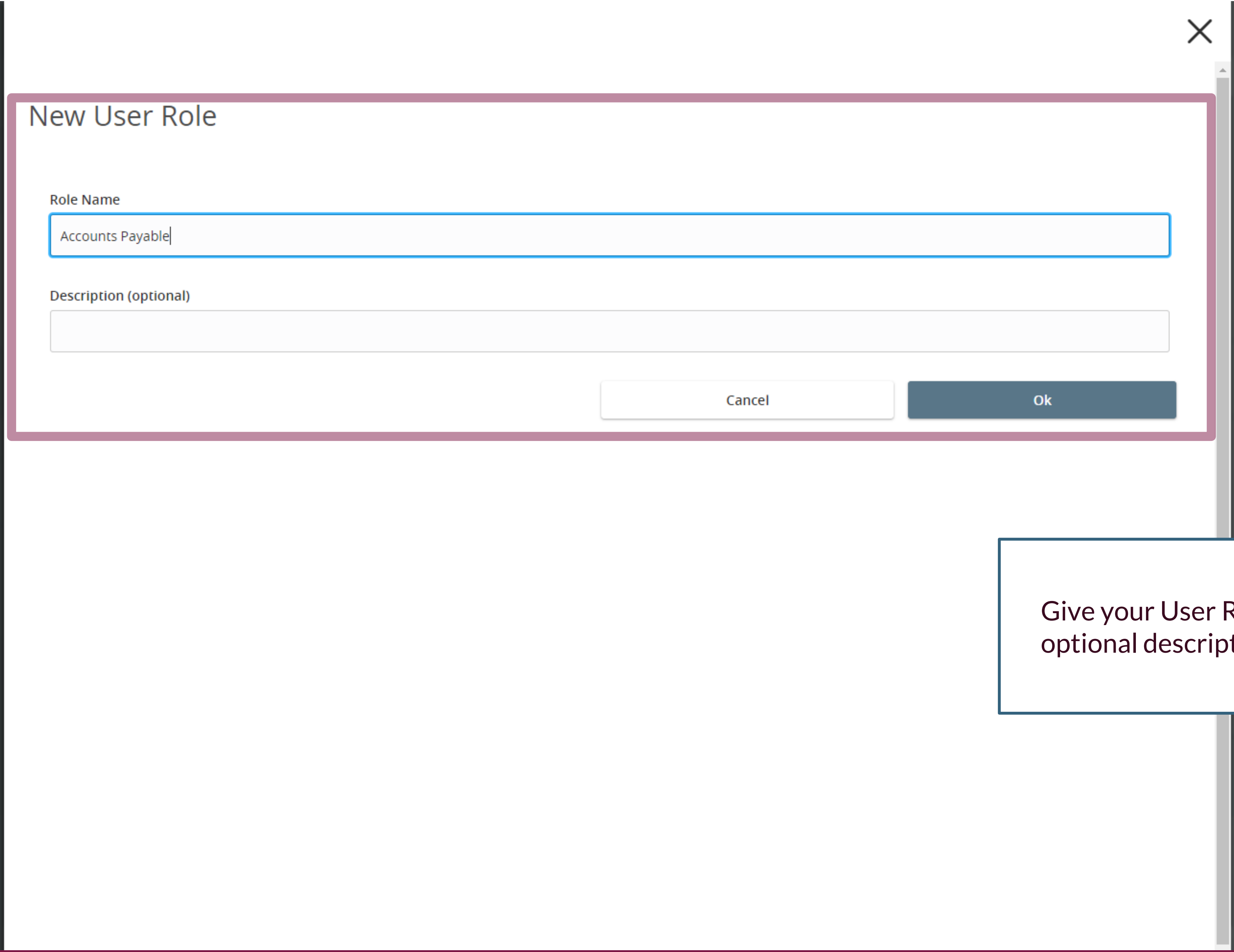


Instead of creating user entitlements individually for each user, **Company Administrators** will create **User Roles** to easily assign entitlements for users based on their roles. For example, you could create a User Role for Accounts Payables users, Accounts Receivables users, View Only users, etc.

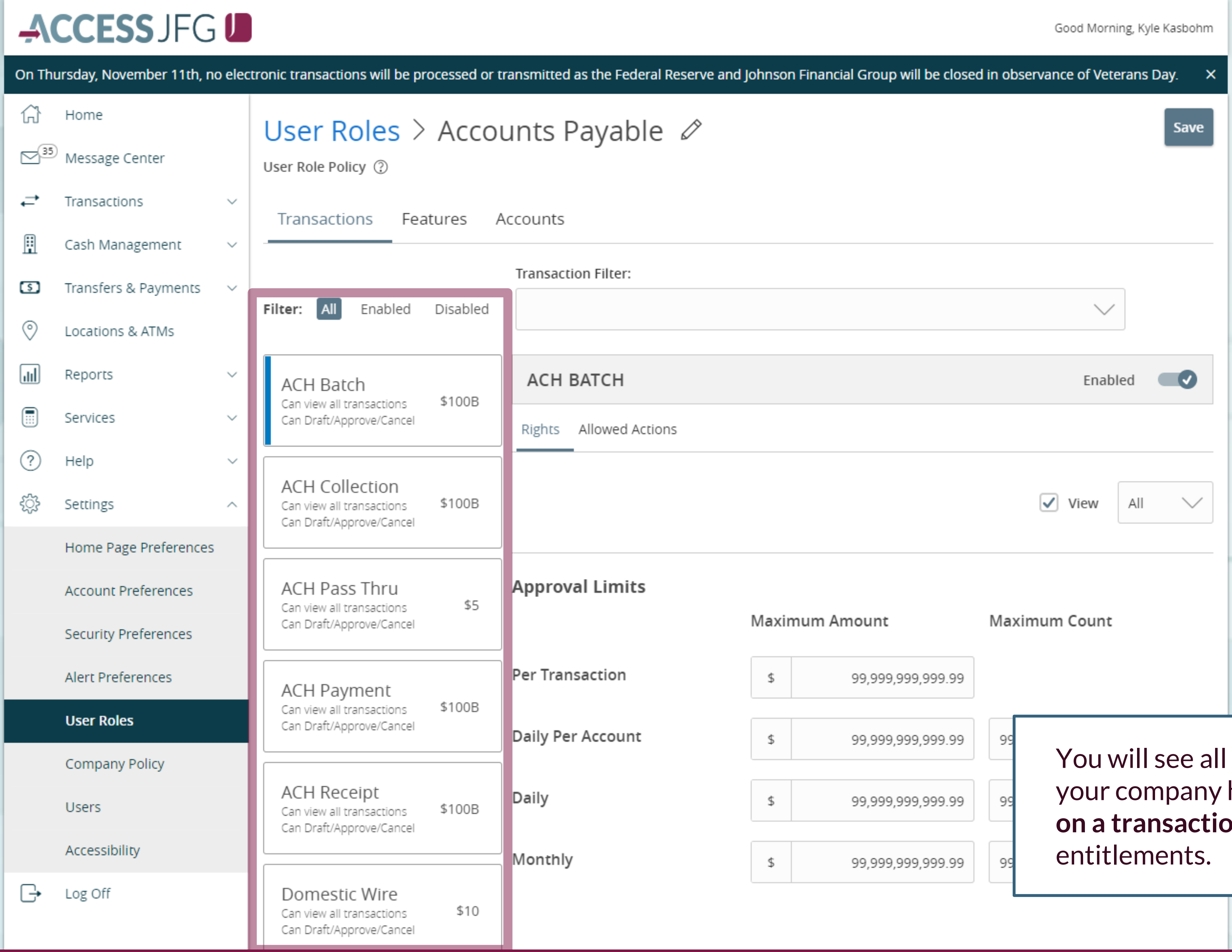
To create and manage User Roles, click on **User Roles** under the **Settings** Menu.



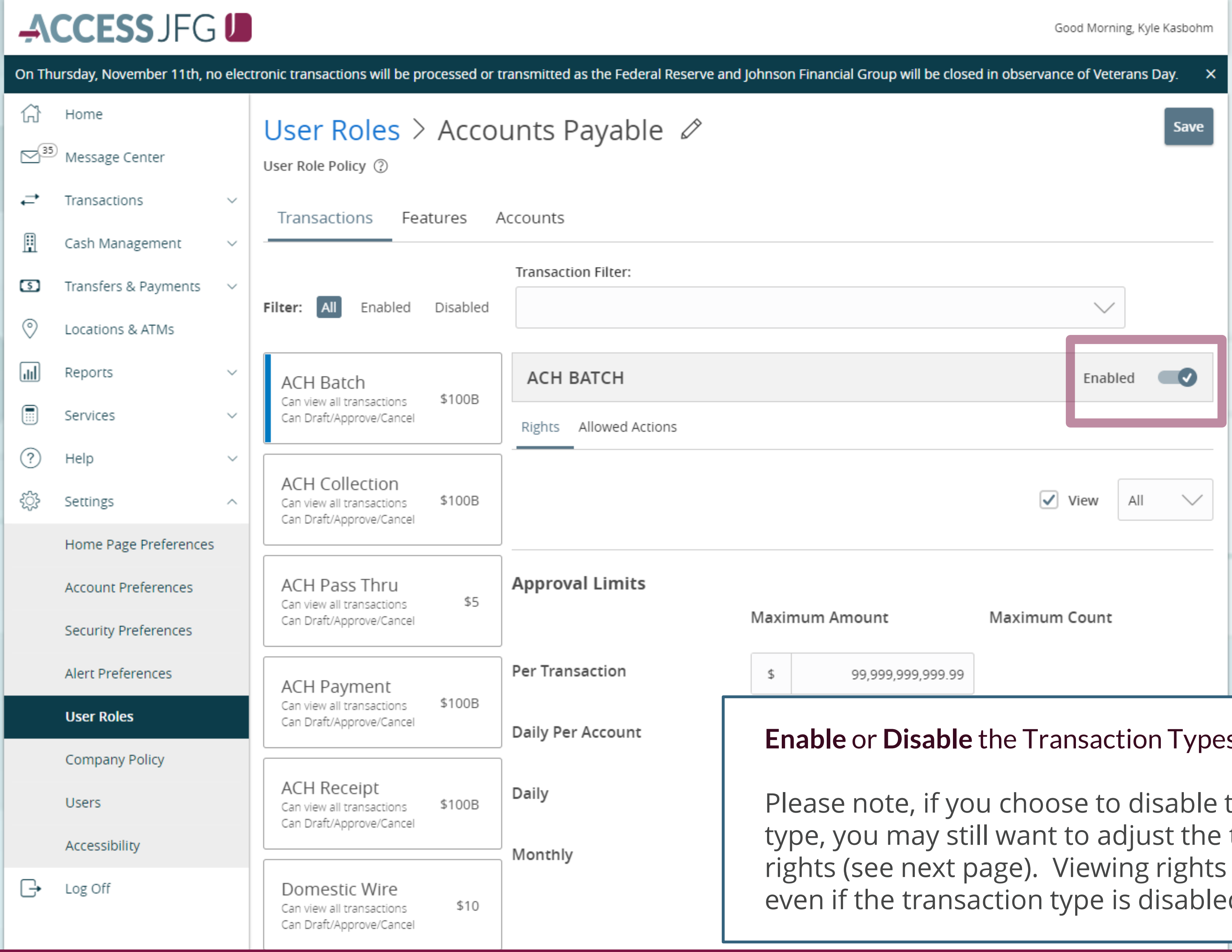
Click **Create Role** to create a new User Role.



Give your User Role a name and an optional description. Click **OK.**

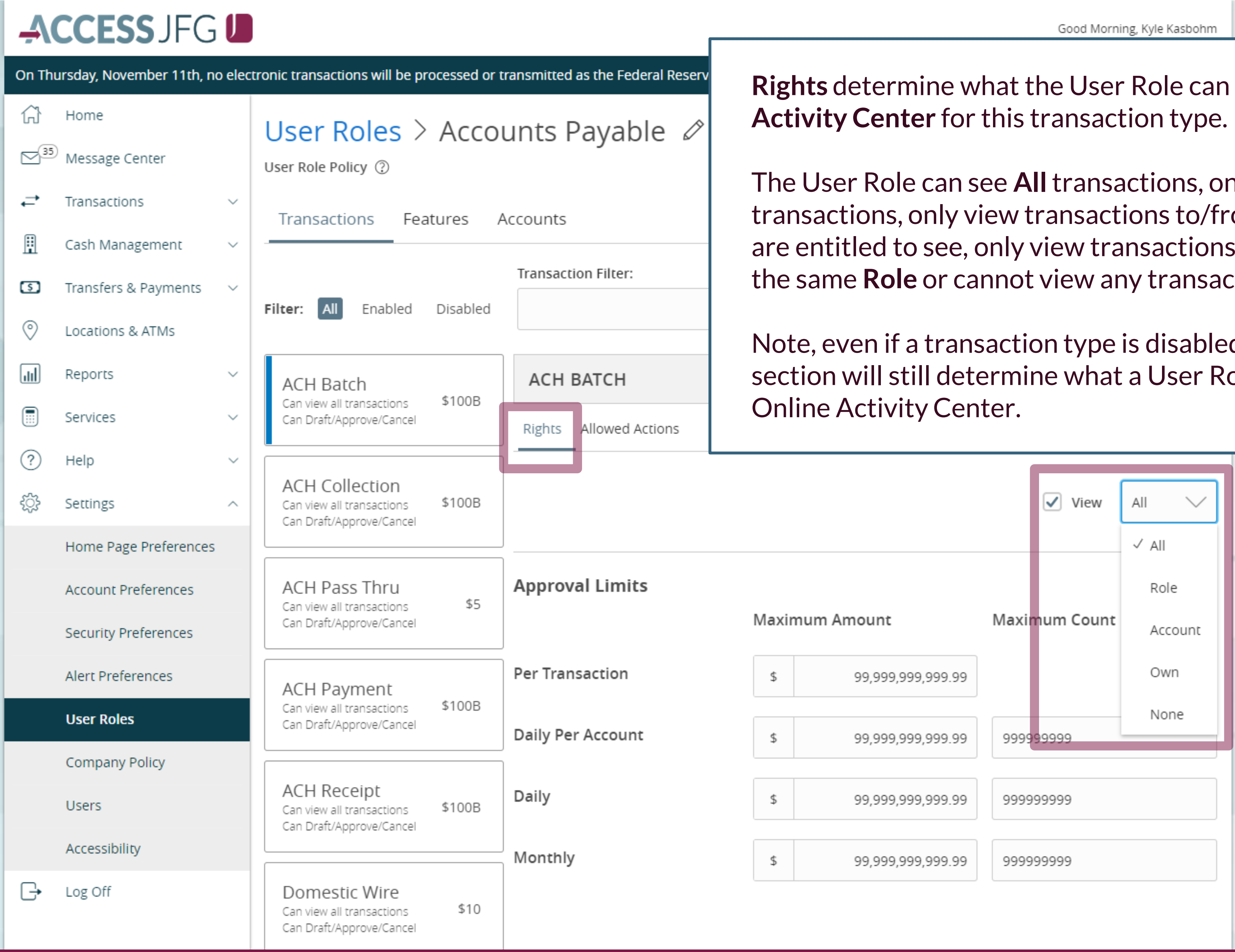


You will see all the transactions your company has access to. **Click on a transaction type** to edit entitlements.



Enable or **Disable** the Transaction Types required.

Please note, if you choose to disable the transaction type, you may still want to adjust the transaction viewing rights (see next page). Viewing rights will still be active even if the transaction type is disabled.



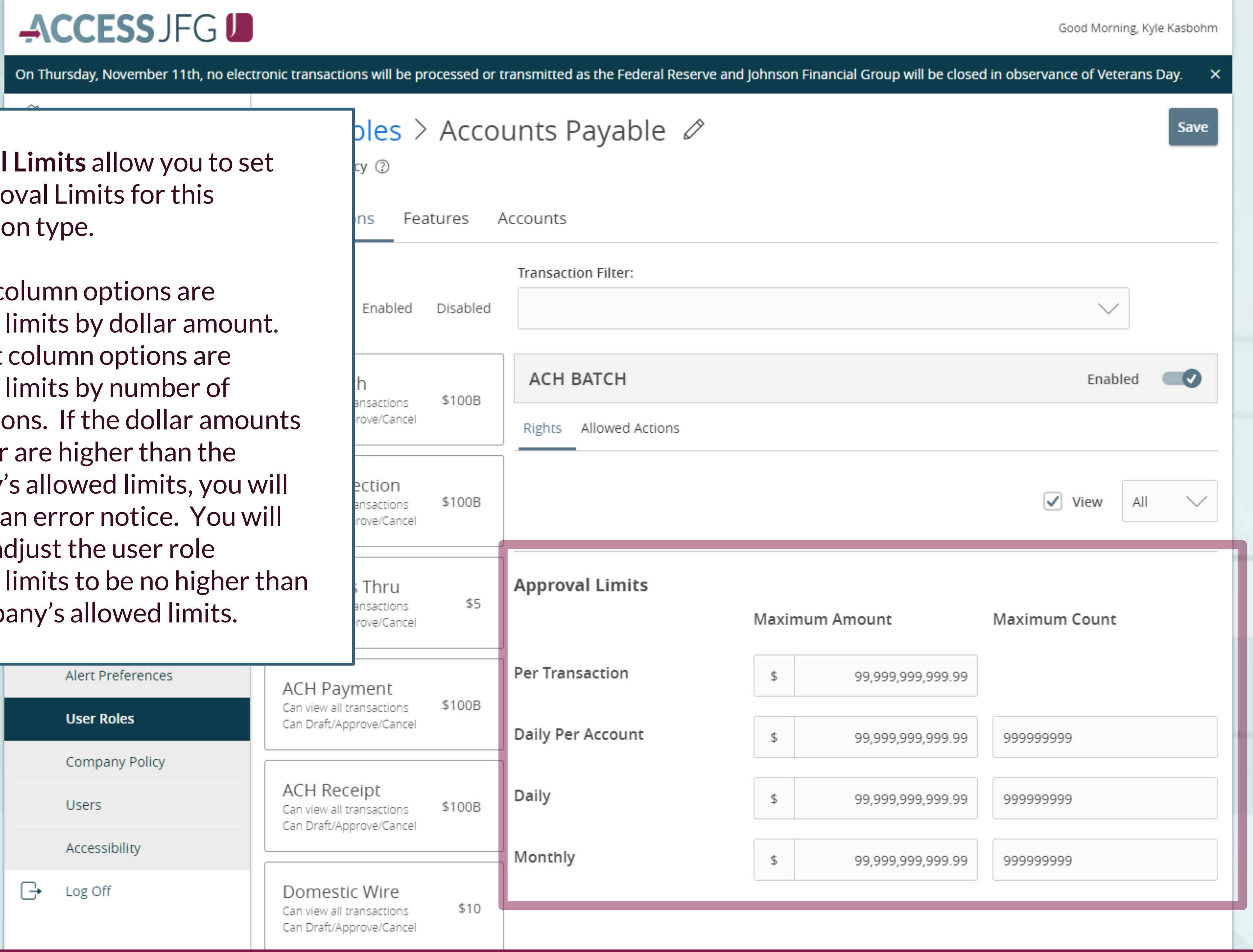
Rights determine what the User Role can see in the **Online Activity Center** for this transaction type.

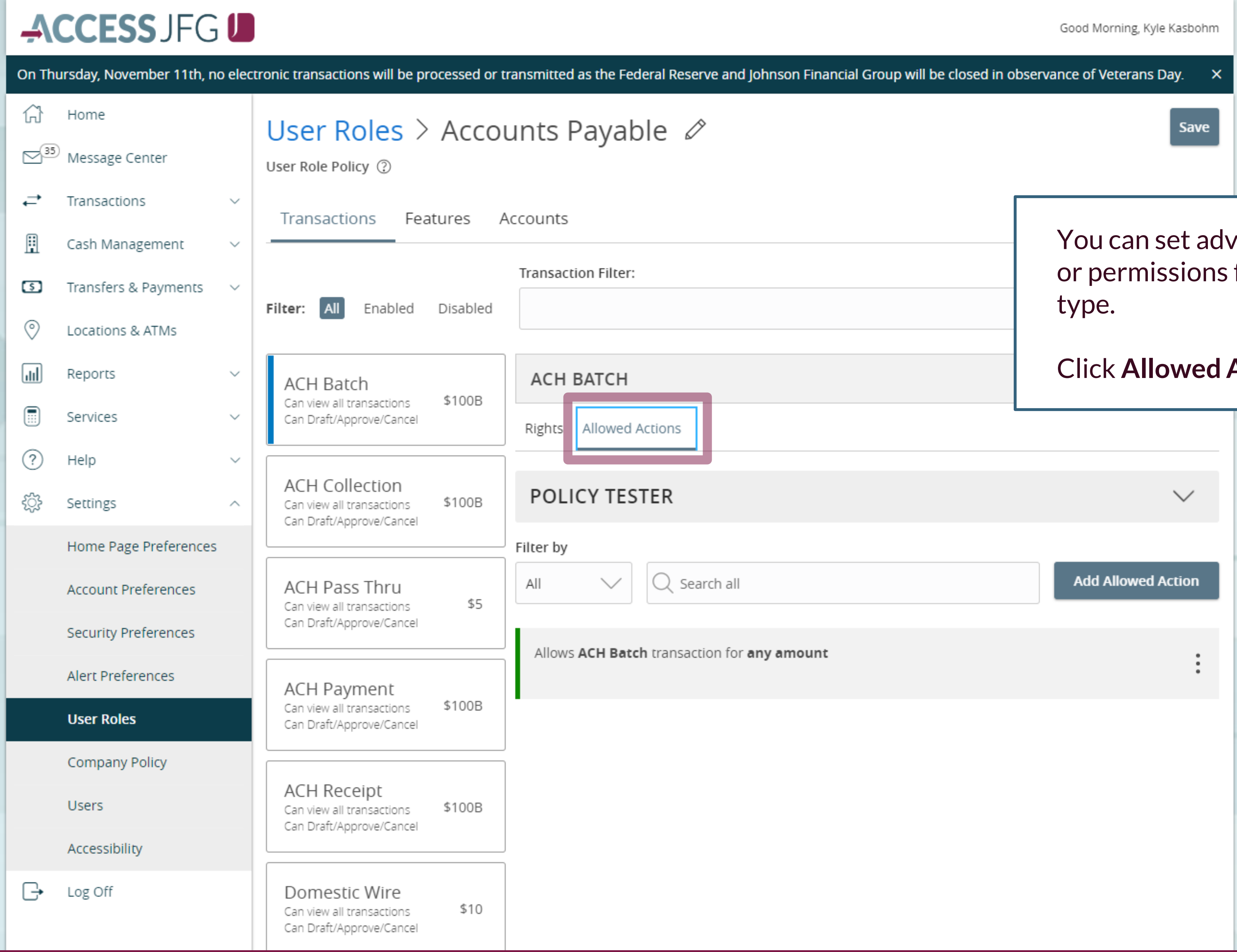
The User Role can see **All** transactions, only view their **Own** transactions, only view transactions to/from **Accounts** they are entitled to see, only view transactions done by others in the same **Role** or cannot view any transactions **(None).**

Note, even if a transaction type is disabled, the Rights section will still determine what a User Role can see in the Online Activity Center.

Approval Limits allow you to set the Approval Limits for this transaction type.

The left column options are approval limits by dollar amount. The right column options are approval limits by number of transactions. If the dollar amounts you enter are higher than the company's allowed limits, you will be given an error notice. You will need to adjust the user role approval limits to be no higher than the company's allowed limits.

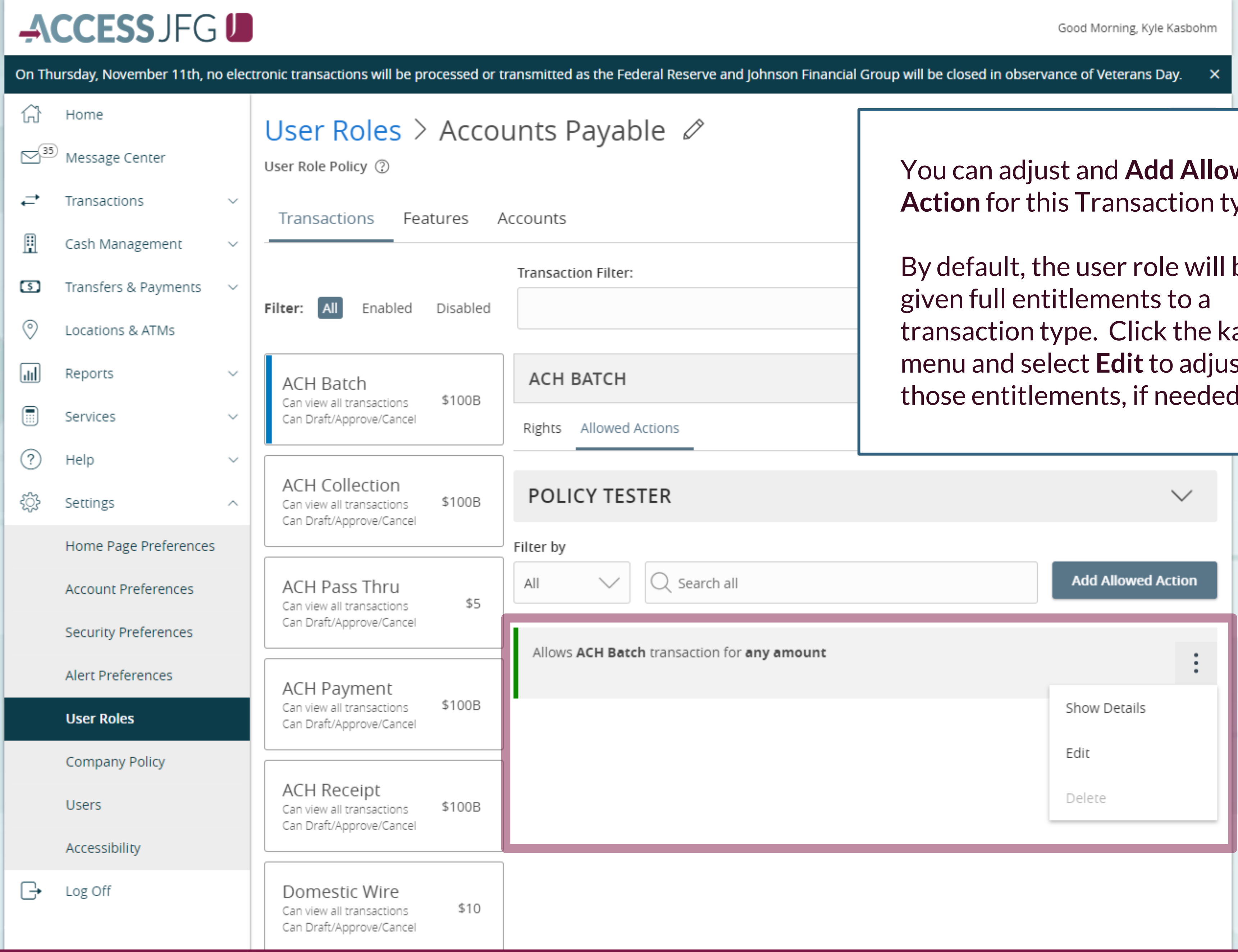




You can set advanced entitlements or permissions for each transaction type.

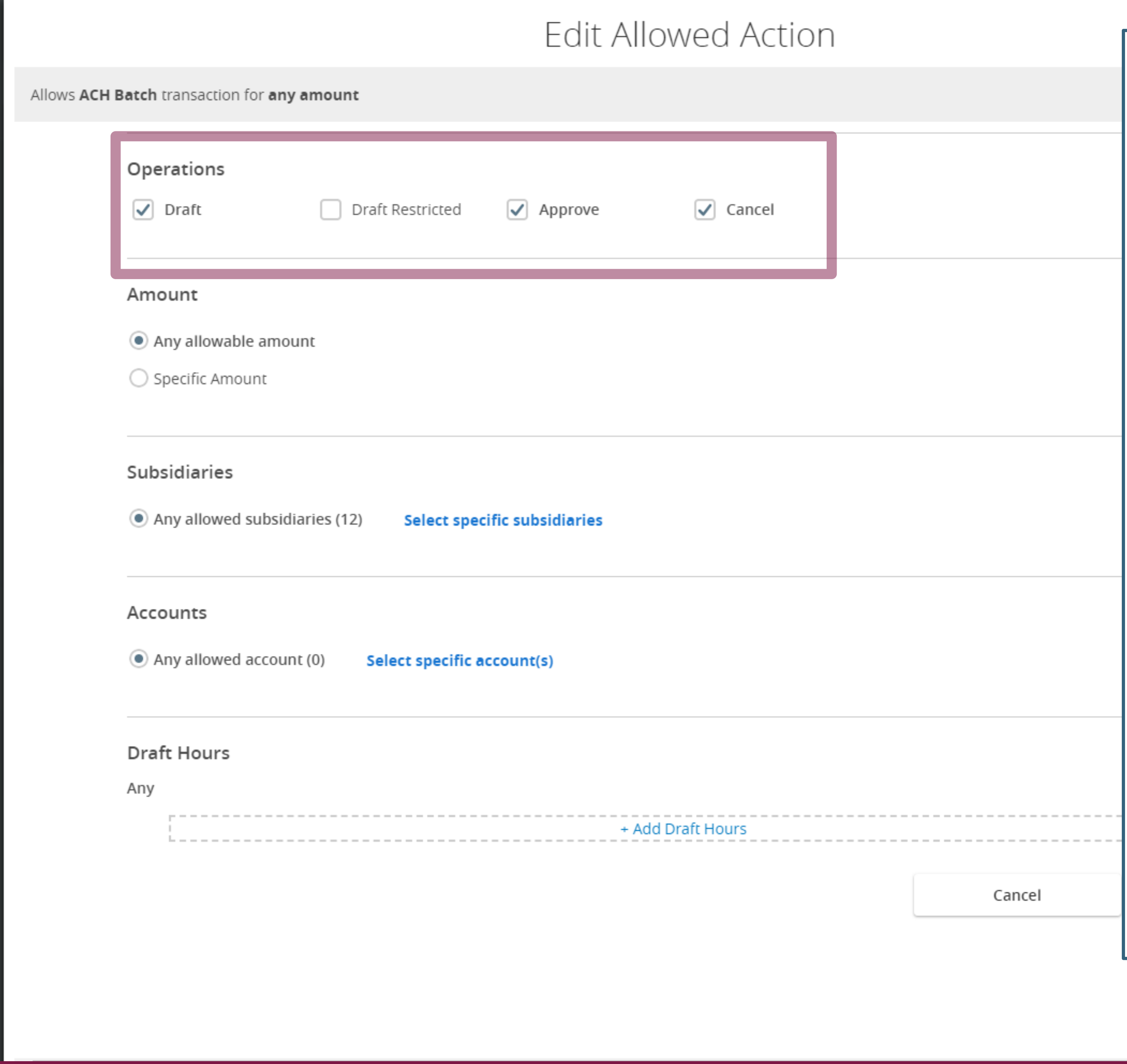
Click **Allowed Actions**

For additional assistance, please call 888.769.3796 or email tmsupport@johnsonfinancialgroup.com.



You can adjust and **Add Allowed Action** for this Transaction type.

By default, the user role will be given full entitlements to a transaction type. Click the kabob menu and select **Edit** to adjust those entitlements, if needed.



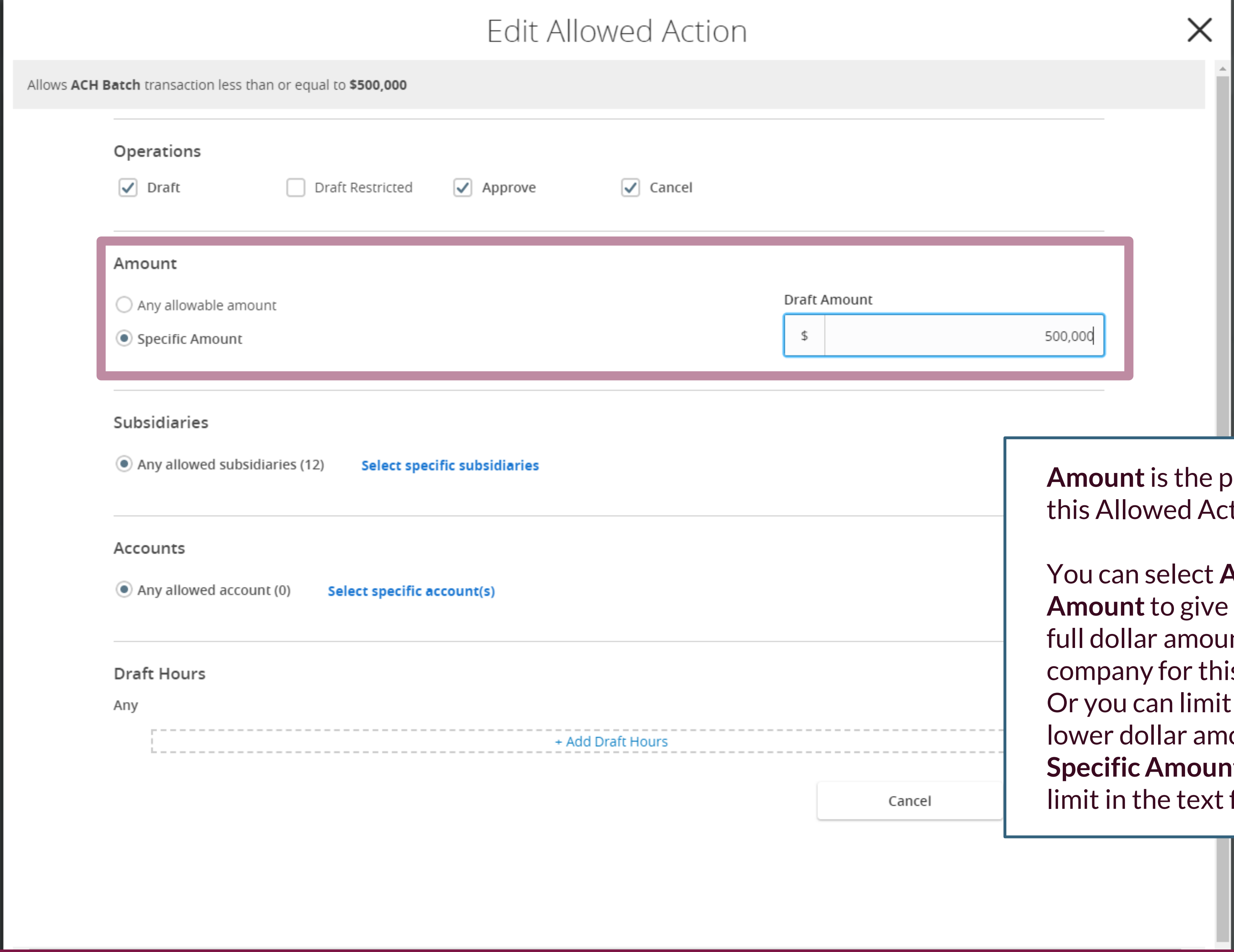
Operations is the ability to Draft, Approve and Cancel transactions. Use the check boxes to enable or disable each option.

Draft is the ability to initiate the transaction.

Draft Restricted is a special permission that only gives the user role access to initiate transactions from templates someone else has setup for them. You cannot have both **Draft** & **Draft Restricted** entitled.

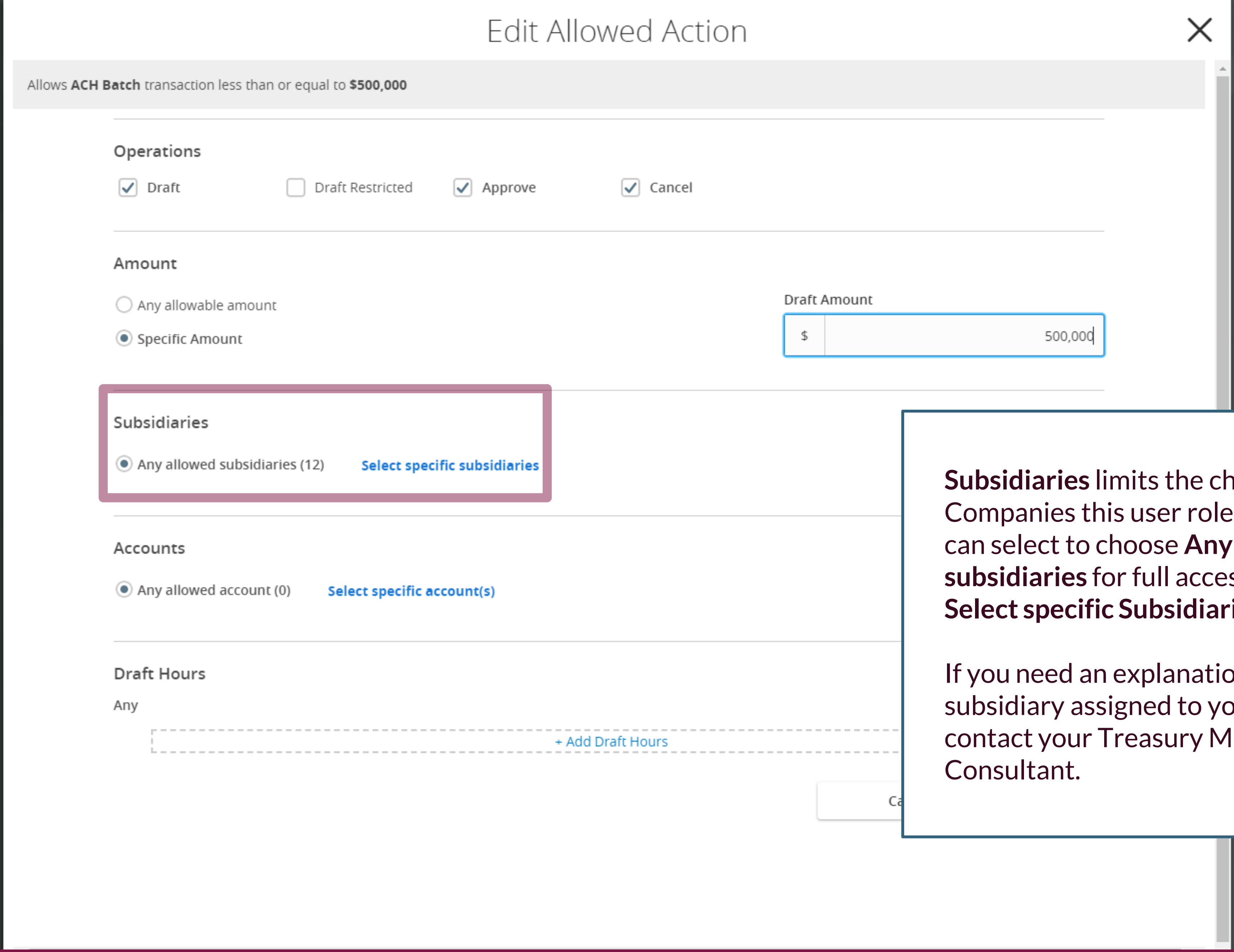
Approve allows the user to approve the transaction type. Please note, if a transaction type requires Dual Control, a user cannot approve a transaction they drafted.

Cancel allows a user to cancel an unprocessed transaction.



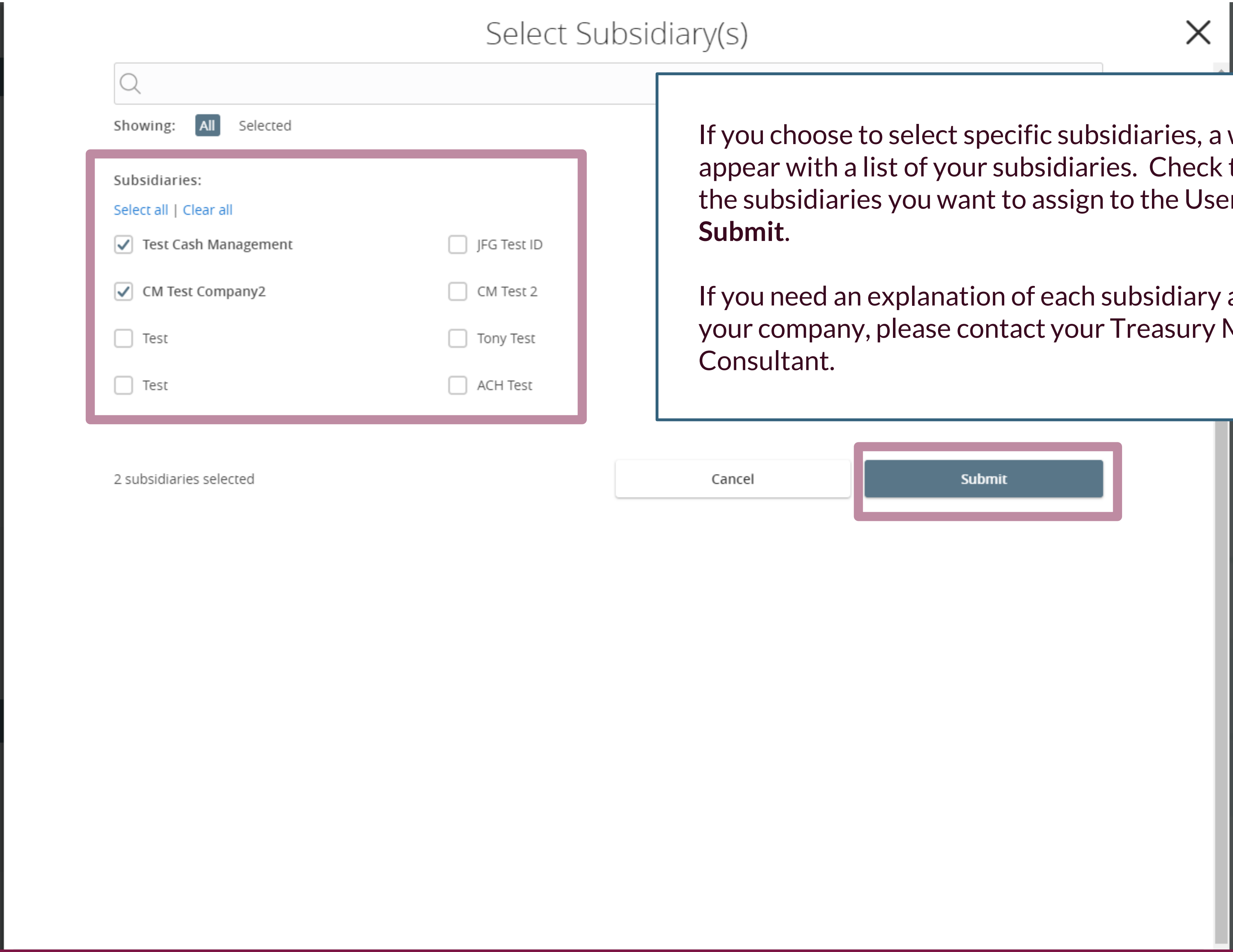
Amount is the payment amount for this Allowed Action.

You can select **Any Allowable Amount** to give this user role the full dollar amount allowed to your company for this transaction type. Or you can limit this user role to a lower dollar amount by choosing **Specific Amount** and entering the limit in the text field.



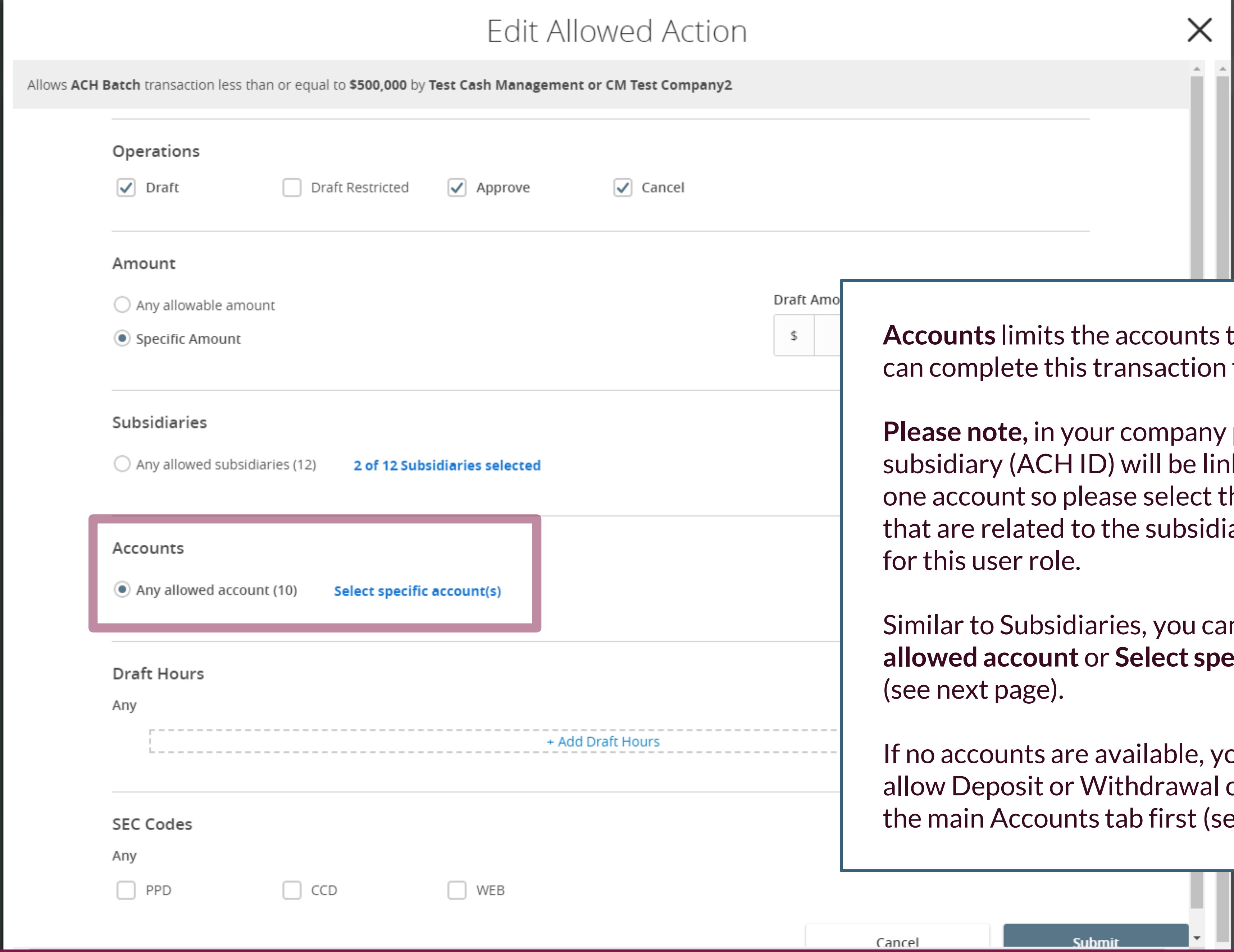
Subsidiaries limits the choice of ACH Companies this user role has access to. You can select to choose **Any allowed subsidiaries** for full access or your can **Select specific Subsidiaries** (see next page).

If you need an explanation of each subsidiary assigned to your company, please contact your Treasury Management Consultant.



If you choose to select specific subsidiaries, a window will appear with a list of your subsidiaries. Check the boxes for the subsidiaries you want to assign to the User Role and click **Submit**.

If you need an explanation of each subsidiary assigned to your company, please contact your Treasury Management Consultant.

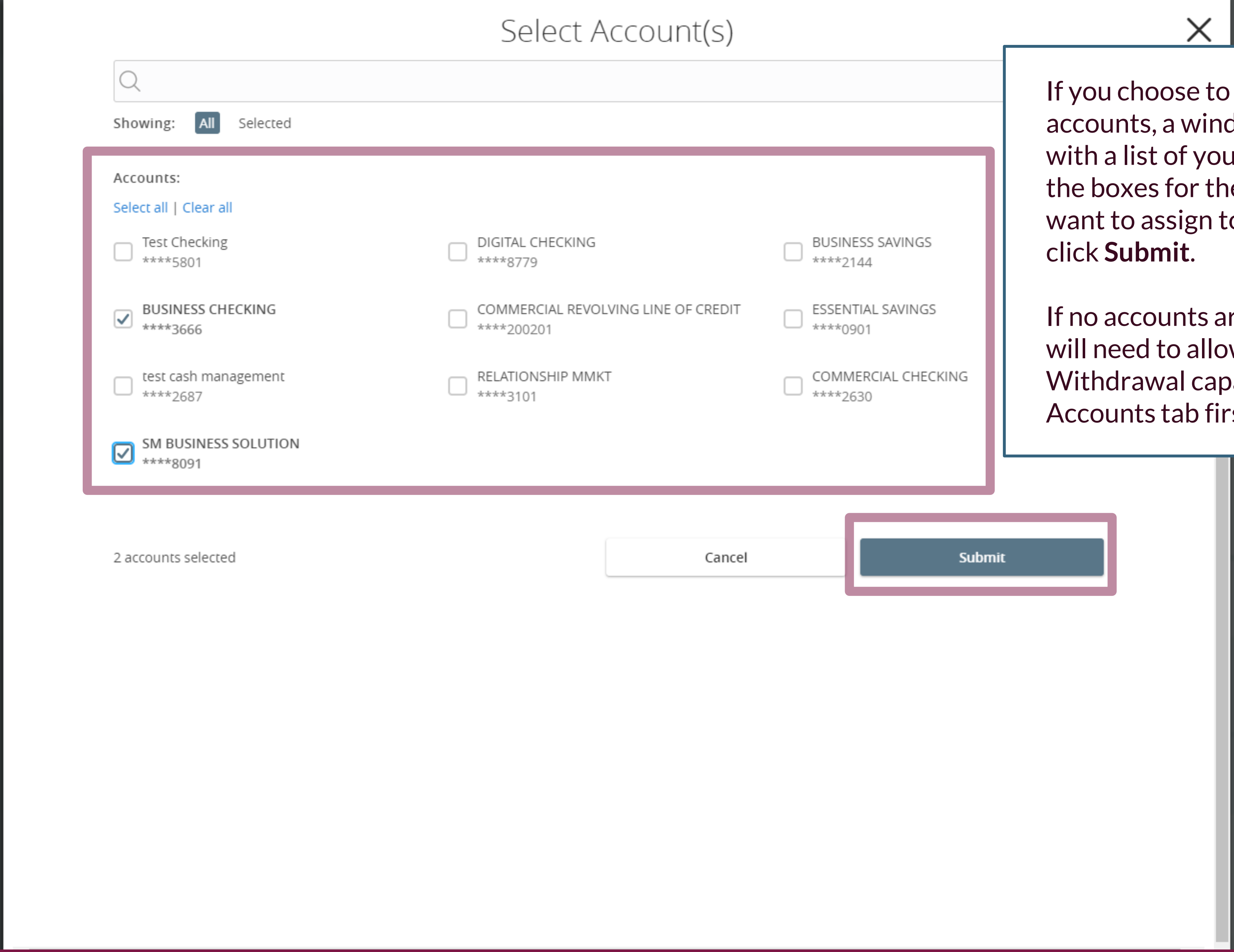


Accounts limits the accounts this user role can complete this transaction from.

Please note, in your company profile, each subsidiary (ACH ID) will be linked to only one account so please select the accounts that are related to the subsidiaries chosen for this user role.

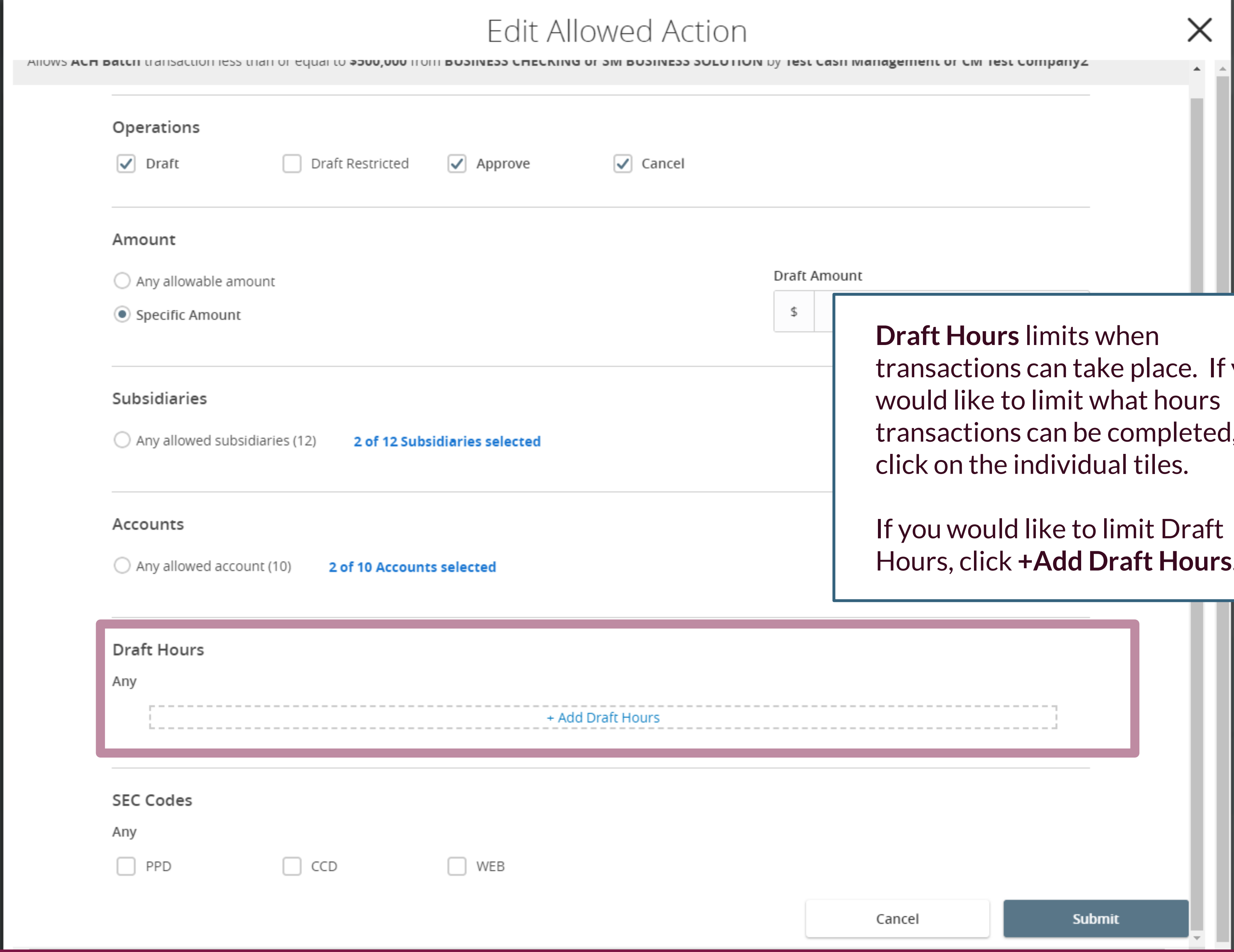
Similar to Subsidiaries, you can select **Any allowed account** or **Select specific accounts** (see next page).

If no accounts are available, you will need to allow Deposit or Withdrawal capabilities in the main Accounts tab first (see page 25).



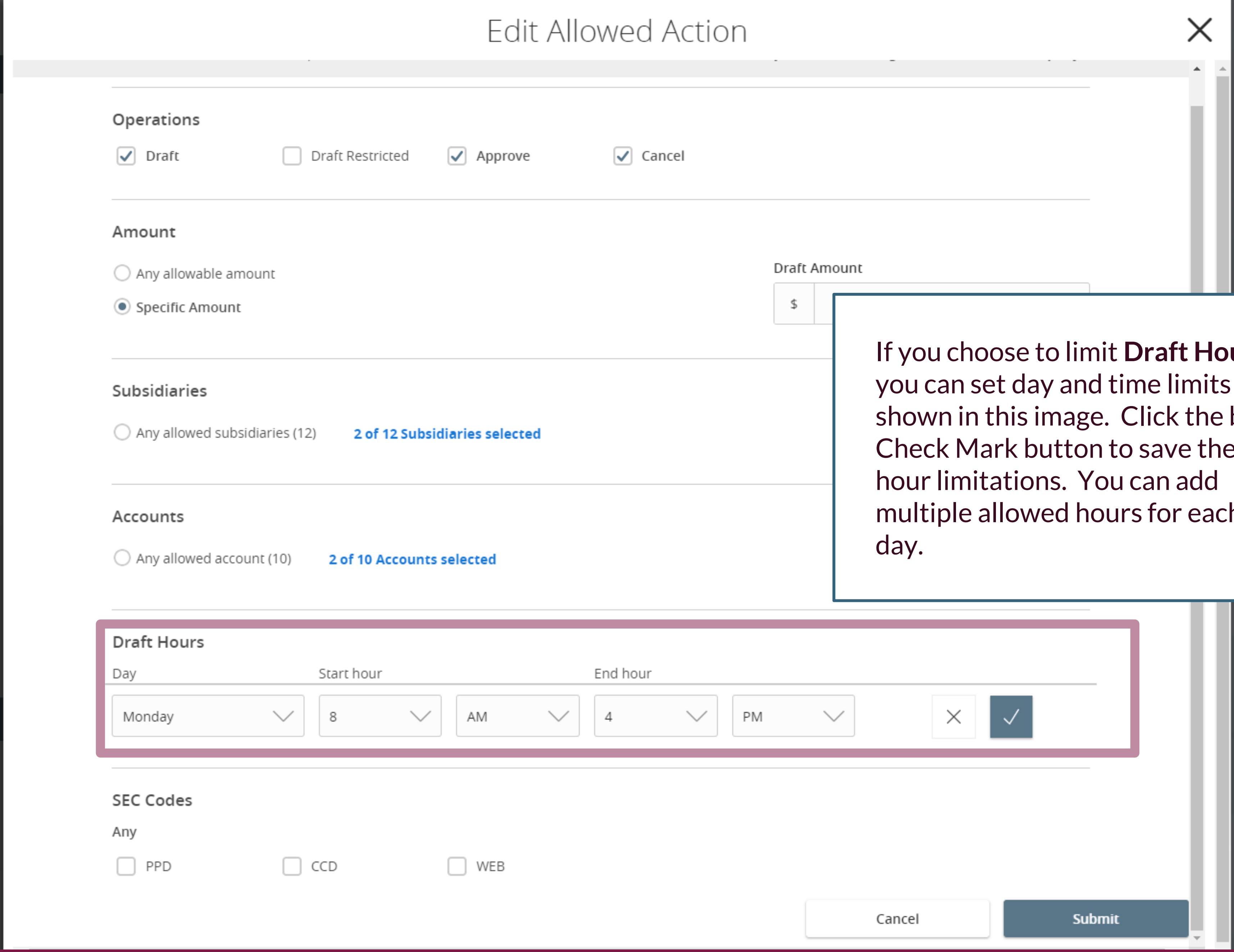
If you choose to select specific accounts, a window will appear with a list of your accounts.. Check the boxes for the accounts you want to assign to the User Role and click **Submit**.

If no accounts are available, you will need to allow Deposit or Withdrawal capabilities in the main Accounts tab first (see page XXX).

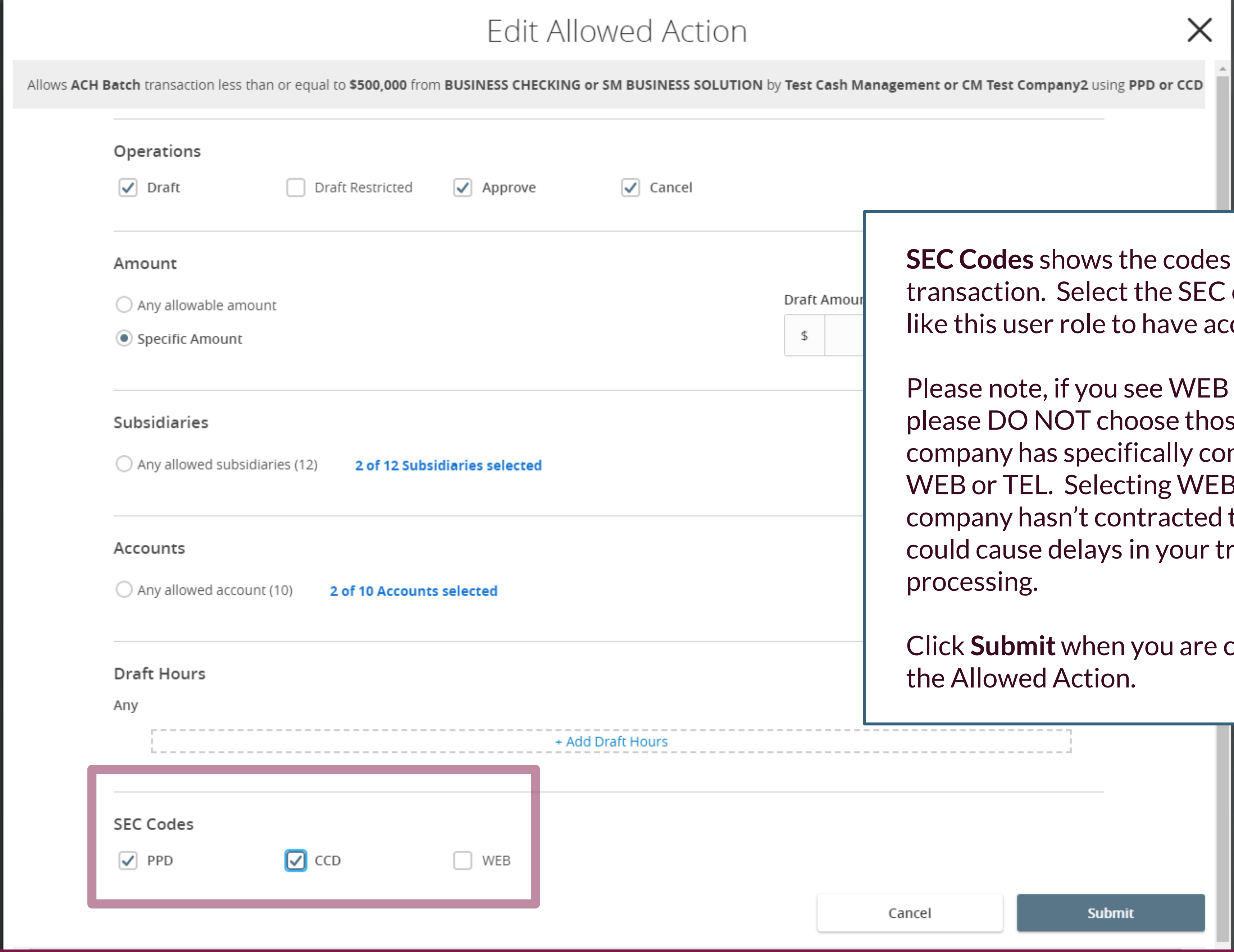


Draft Hours limits when transactions can take place. If you would like to limit what hours transactions can be completed, click on the individual tiles.

If you would like to limit Draft Hours, click **+Add Draft Hours**.



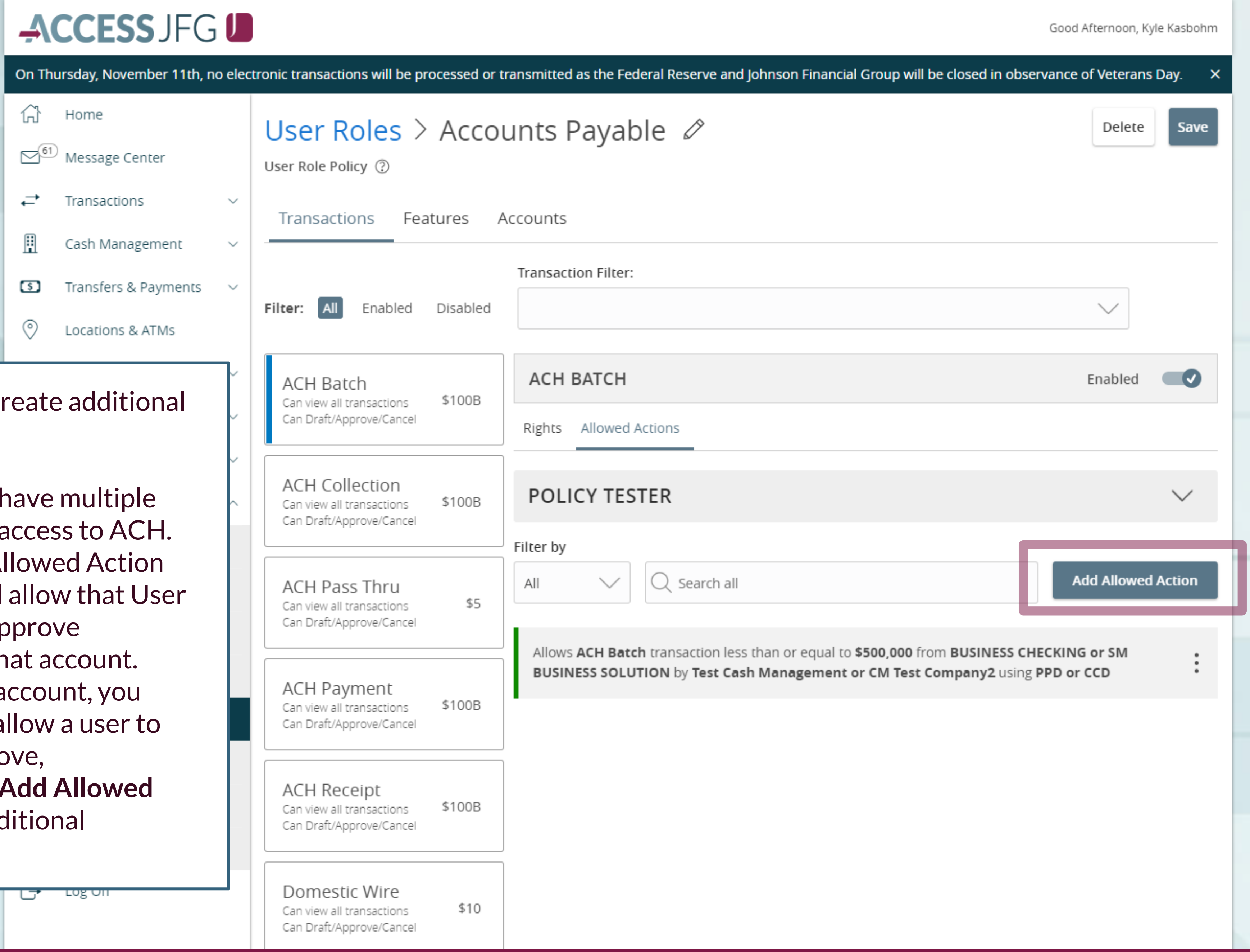
If you choose to limit **Draft Hours** you can set day and time limits as shown in this image. Click the blue Check Mark button to save the hour limitations. You can add multiple allowed hours for each day.



SEC Codes shows the codes allowed with this transaction. Select the SEC codes you would like this user role to have access to.

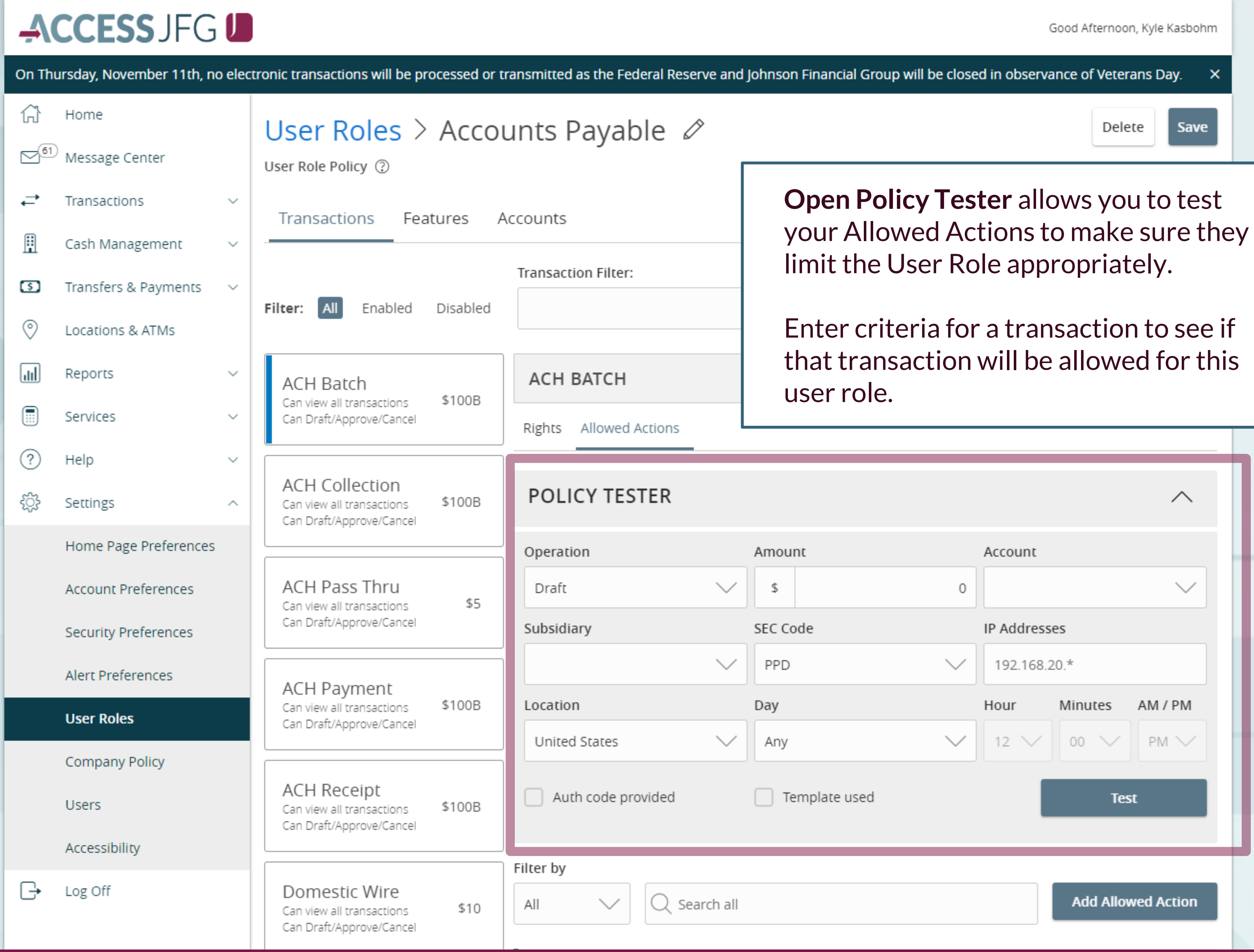
Please note, if you see WEB or TEL as options, please DO NOT choose those unless your company has specifically contracted to use WEB or TEL. Selecting WEB or TEL if your company hasn't contracted to use those codes could cause delays in your transaction processing.

Click **Submit** when you are completed updating the Allowed Action.



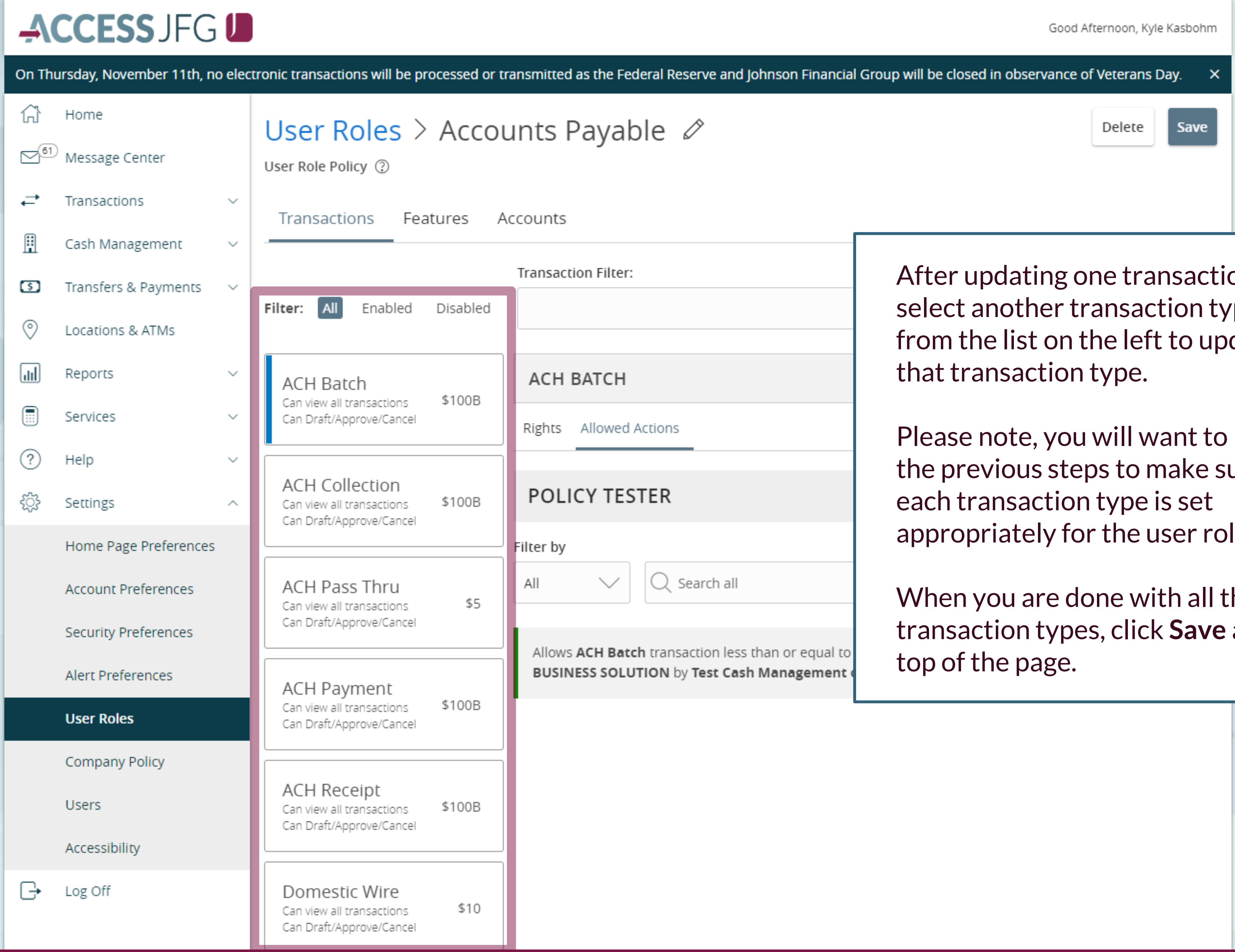
If needed, you can create additional Allowed Actions.

For example, if you have multiple accounts that have access to ACH. You can create an Allowed Action for one account and allow that User Role to Draft and Approve transactions from that account. But, for a different account, you can choose to only allow a user to Draft, but not Approve, transactions. Click **Add Allowed Action** to create additional Allowed Actions.



Open Policy Tester allows you to test your Allowed Actions to make sure they limit the User Role appropriately.

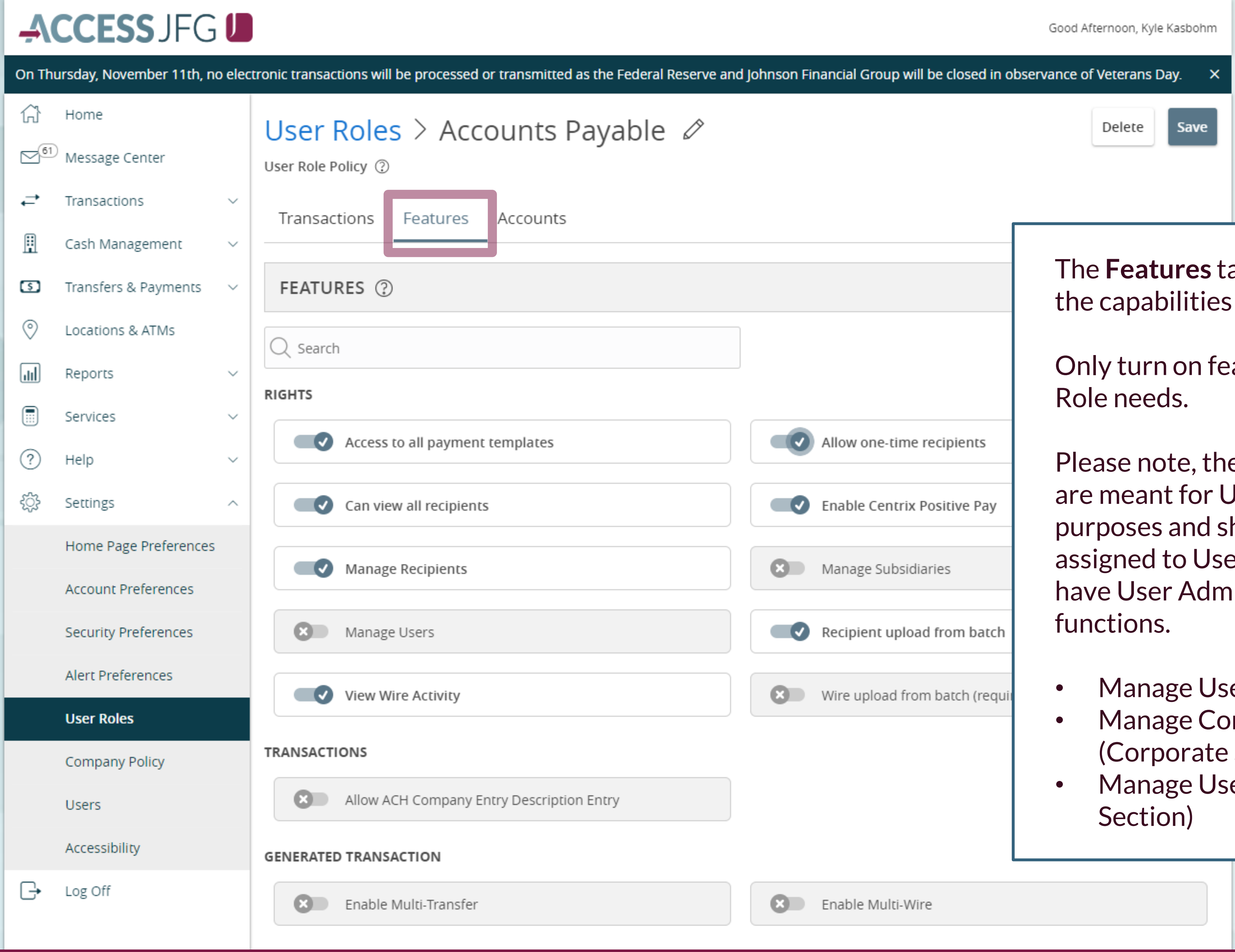
Enter criteria for a transaction to see if that transaction will be allowed for this user role.



After updating one transaction, select another transaction type from the list on the left to update that transaction type.

Please note, you will want to repeat the previous steps to make sure each transaction type is set appropriately for the user role.

When you are done with all the transaction types, click **Save** at the top of the page.

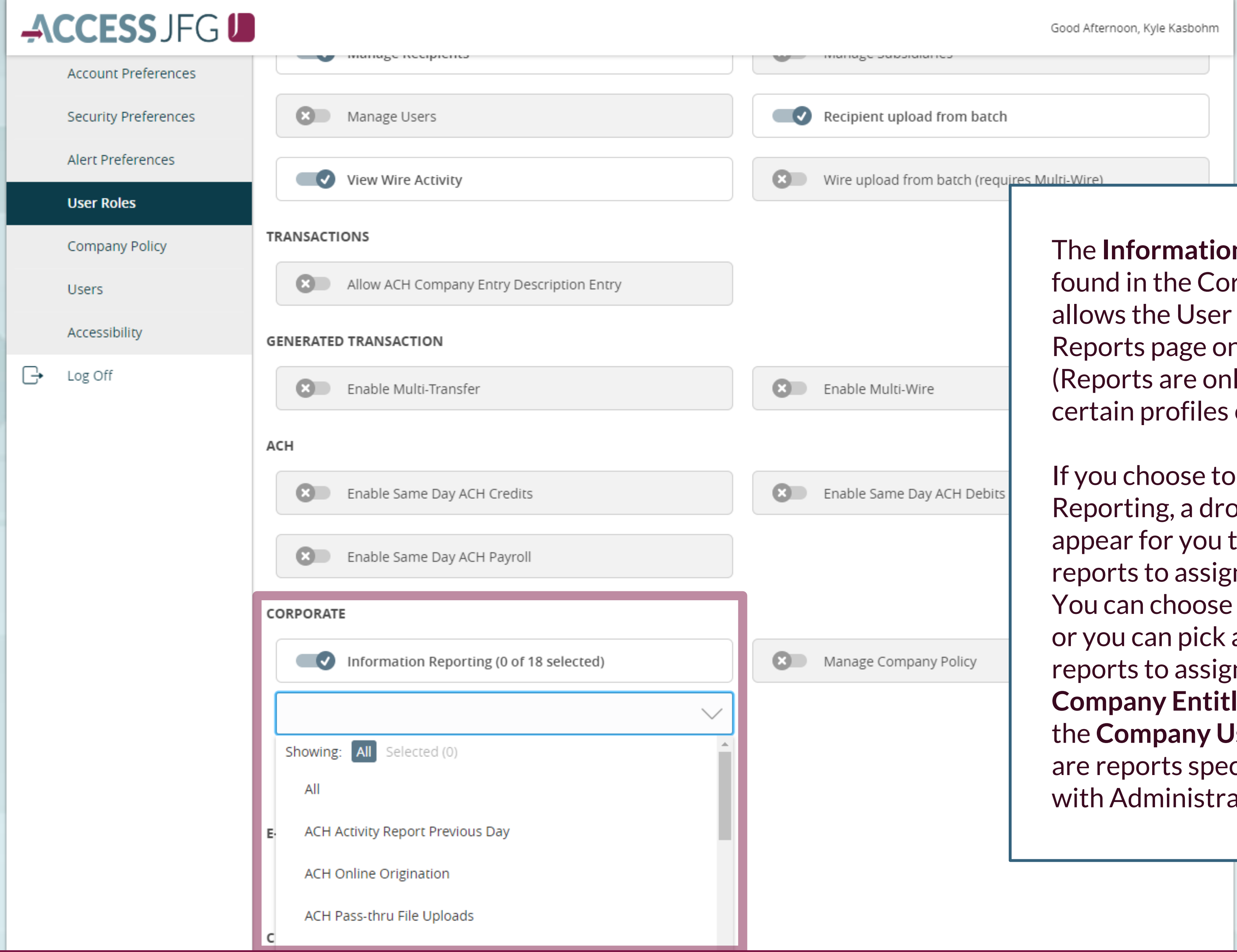


The **Features** tab allows you to set the capabilities the User Role has.

Only turn on features that the User Role needs.

Please note, the following **Features** are meant for User Administration purposes and should only be assigned to User Roles who should have User Administration functions.

- Manage Users (Rights Section)
- Manage Company Policy (Corporate Section)
- Manage User Roles (Corporate Section)



The **Information Reporting** feature found in the Corporate section allows the User Role to access the Reports page on AccessJFG (Reports are only available to certain profiles of AccessJFG).

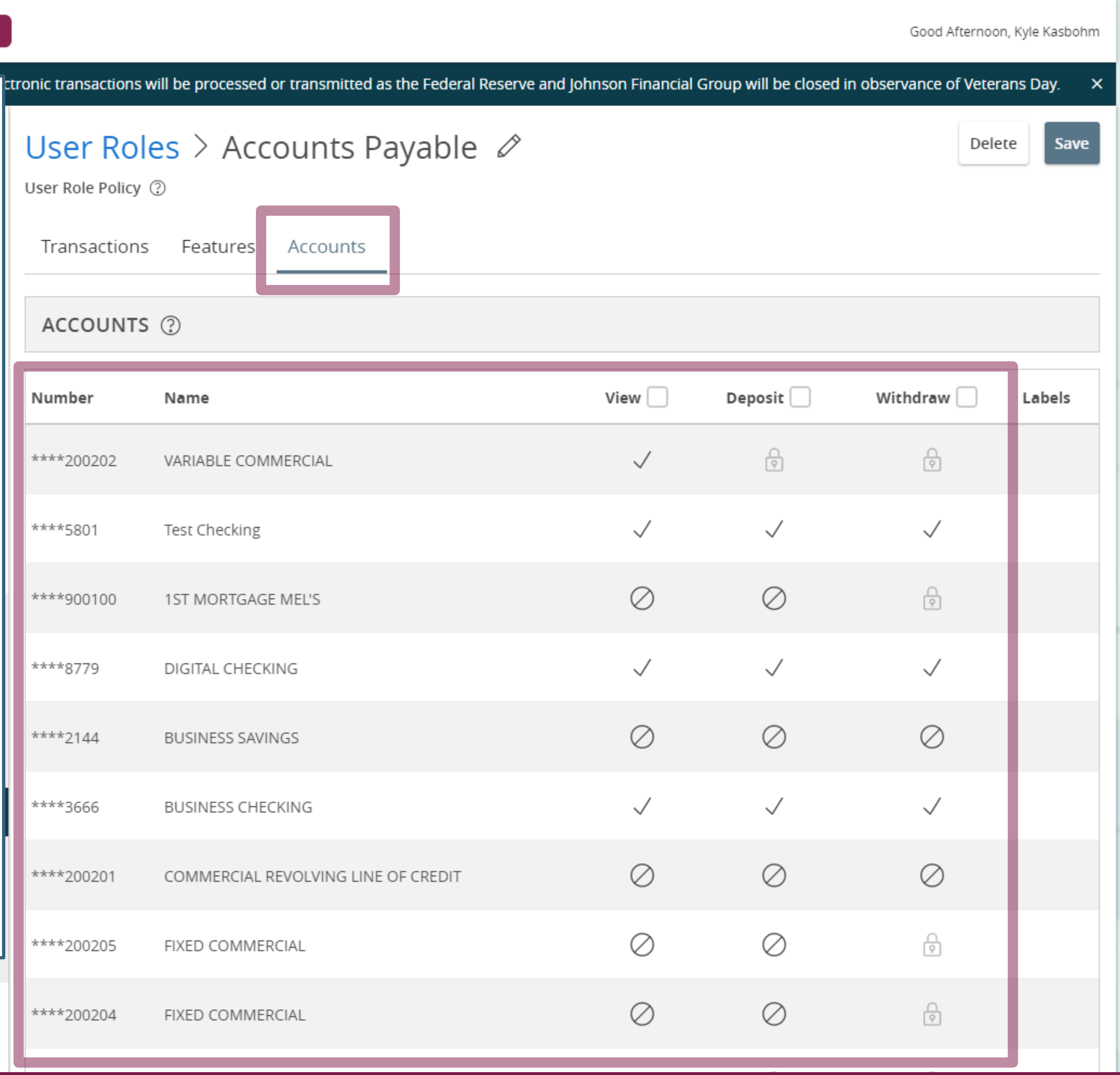
If you choose to enable Information Reporting, a drop-down menu will appear for you to choose which reports to assign to the User Role. You can choose to assign **All** reports or you can pick and choose which reports to assign. Please note, the **Company Entitlements Report** & the **Company User Activity Report** are reports specifically for Users with Administration functionality.

By clicking the **Accounts** tab, you can select which accounts the User Role can View, Deposit into, or Withdraw from. Deposit/Withdraw functionality refers to transactions within AccessJFG only (internal transfers & ACH/Wire transactions). For example, if a user role should be able to submit an ACH Batch Payment out of an account, they must be given Withdraw functionality for that account.

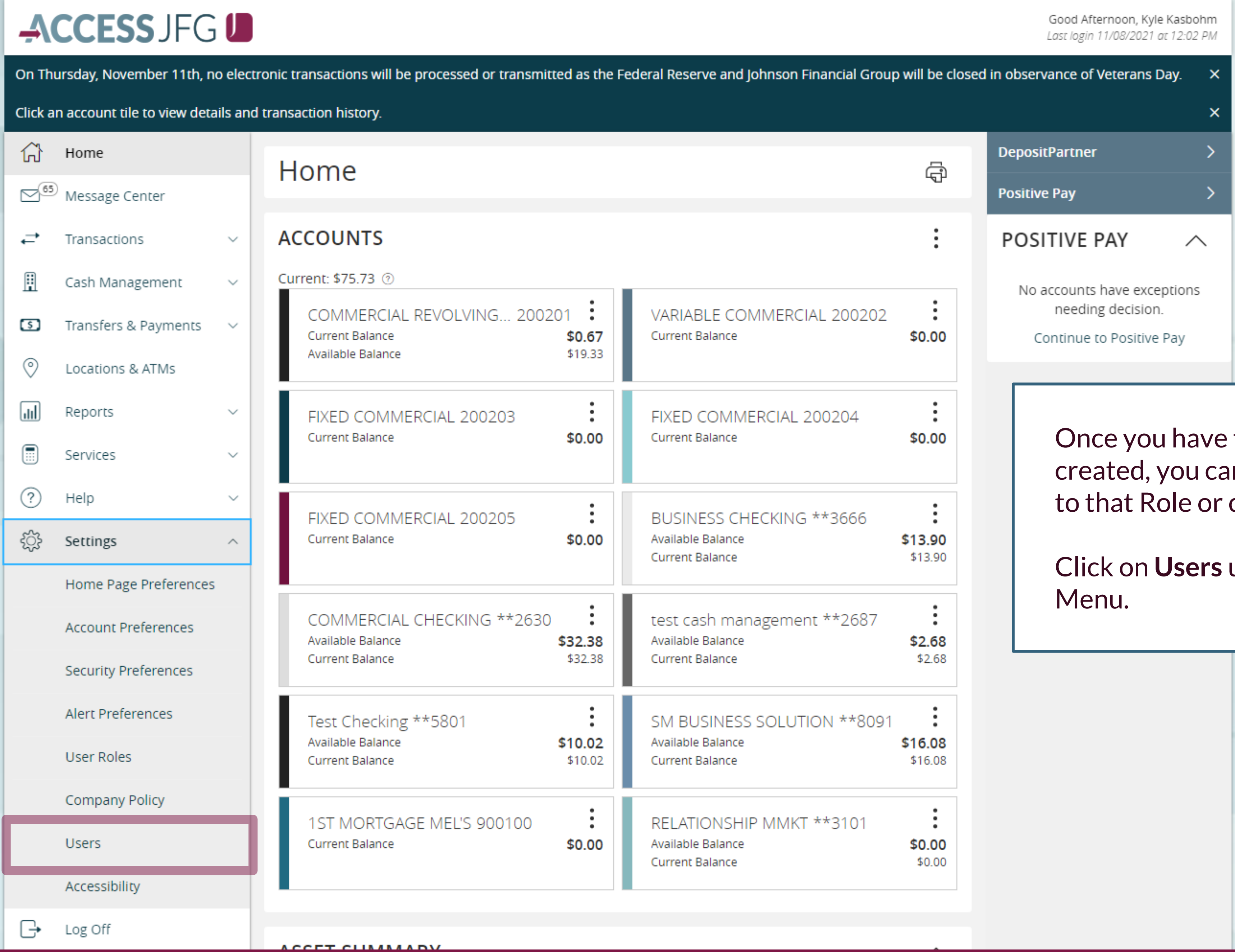
Withdraw entitlements refer only to online transactions; this does not give a user authority to sign checks or make in-person withdrawals.

A padlock indicates that transaction type is restricted from that account.

Click **Save** when finished.

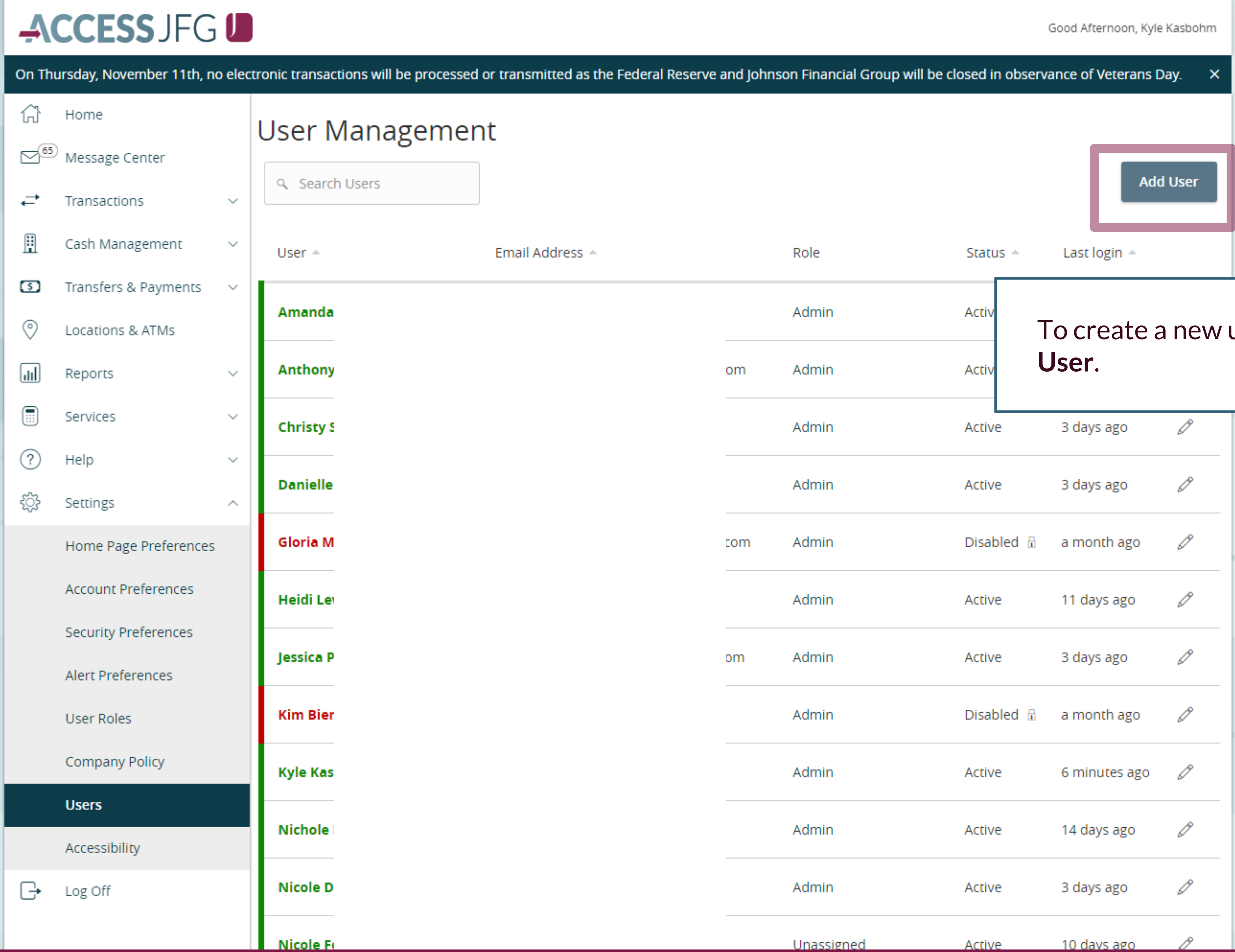


Log Off



Once you have the User Role created, you can **add** existing users to that Role or create a new user.

Click on **Users** under the **Settings** Menu.



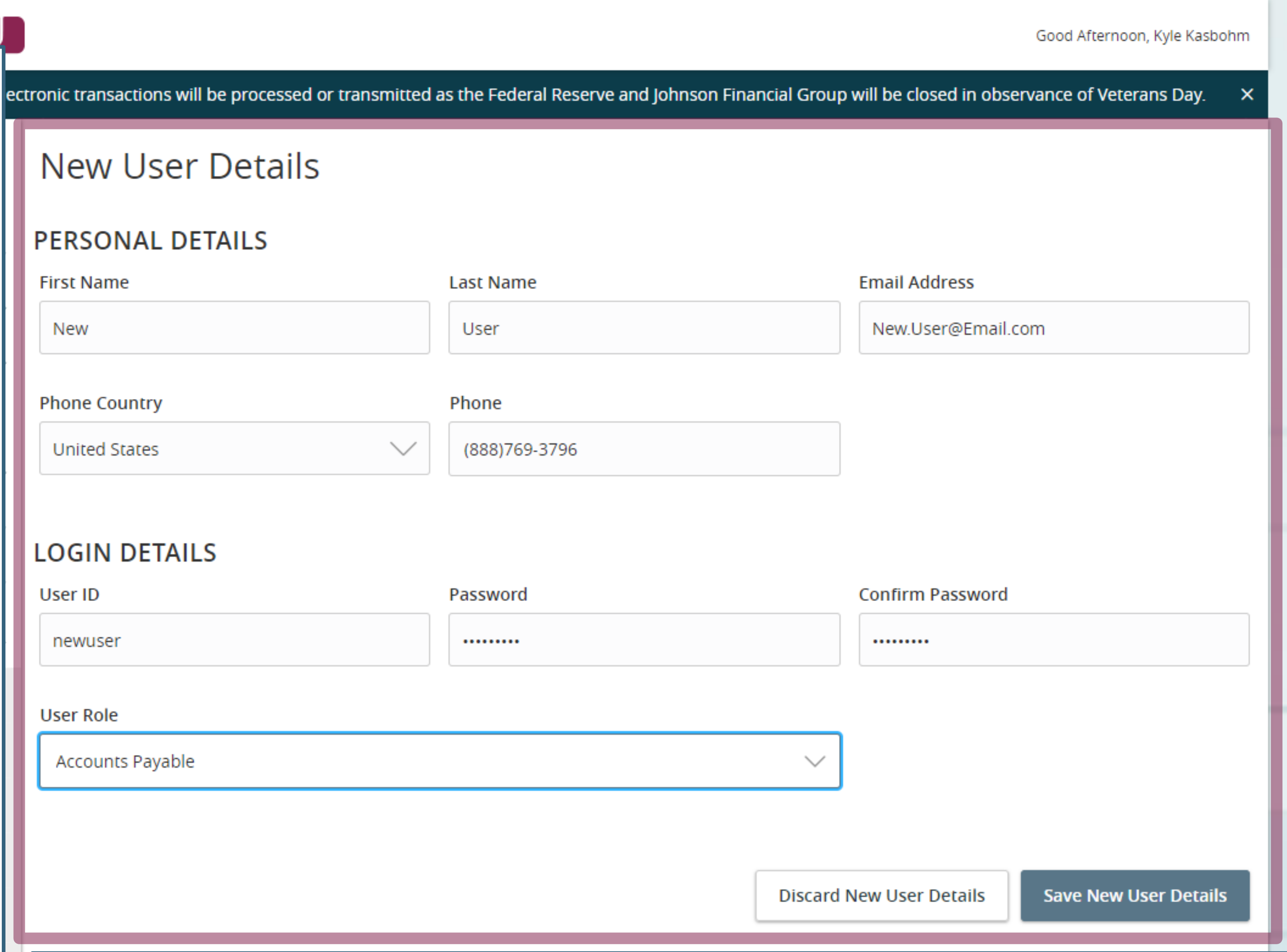
To create a new user, click **Add User**.

Fill in the information of your new user.

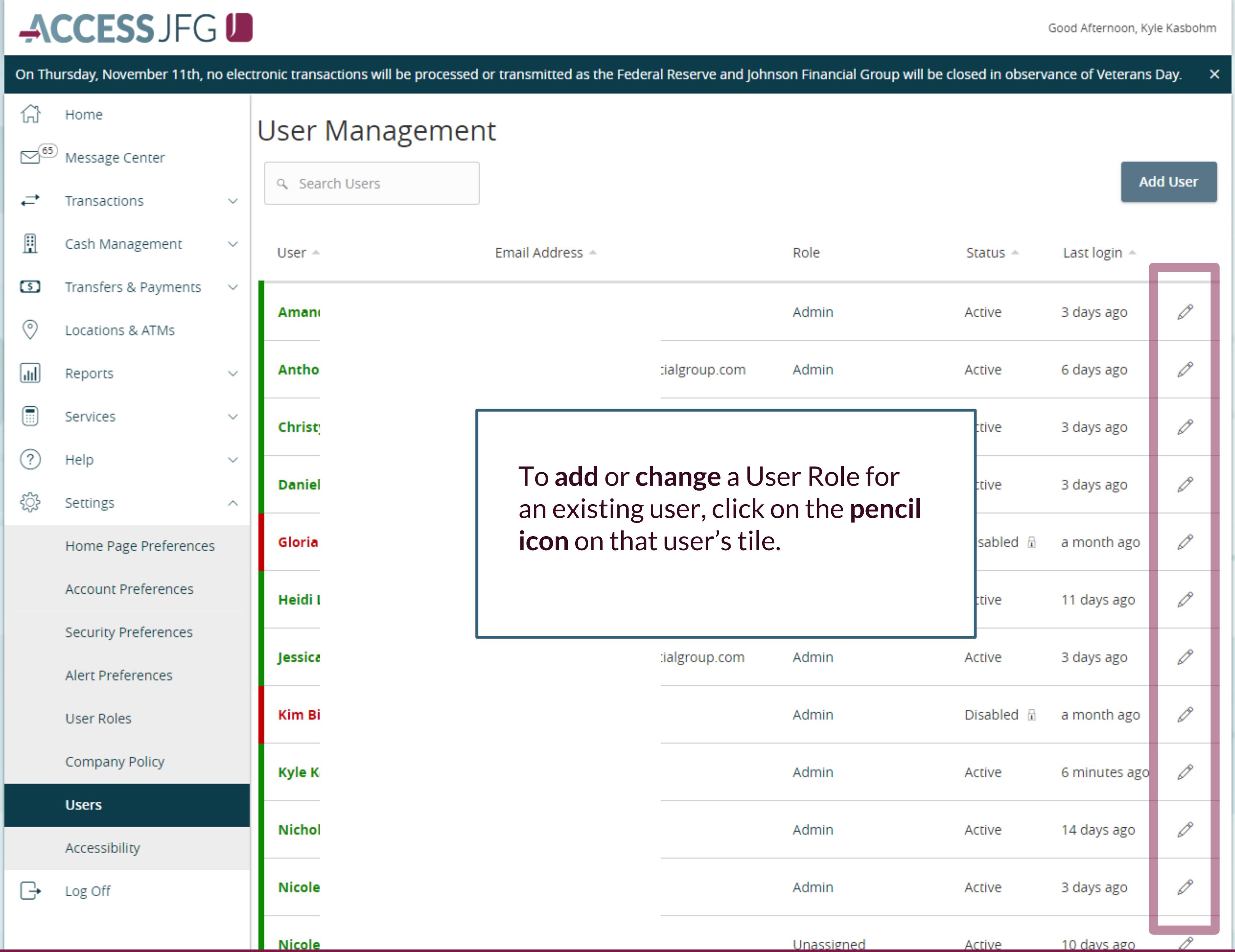
In the top section, enter the personal information (name, email, and direct phone number) of your new user.

In the bottom section, enter the Login Details of the new user. For **User ID**, if you are creating a user who will also use Positive Pay and/or DepositPartner, please do your best to keep the User ID consistent across all three platforms. **Password** requirements will show on the screen when you are in the Password text field. Select the proper **User Role** from the dropdown menu. Click **Save New User Details** when finished.

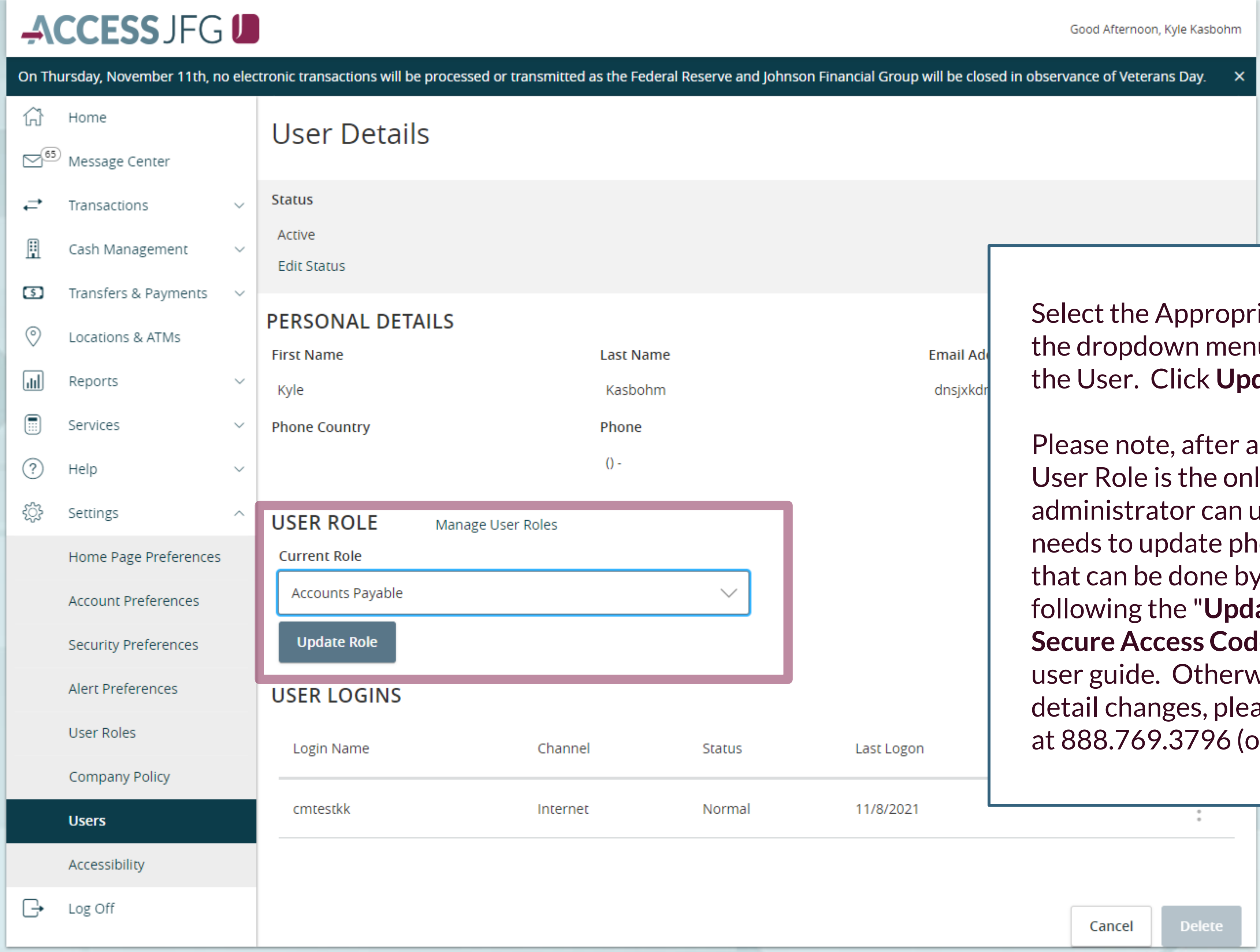
The system will not send an automatic email to the new user. It is the responsibility of the administrator to provide the new user with their User ID and logon instructions.



Please note, if you are creating a user who will also use DepositPartner and/or Positive Pay, that user will need to have user profiles in those systems as well. When you have the user built in AccessJFG as well as DepositPartner and/or Positive Pay, please email tmsupport@johnsonfinancialgroup.com with your company name and the usernames for Access JFG & DepositPartner and/or Positive Pay so they can enable the Single Sign On.

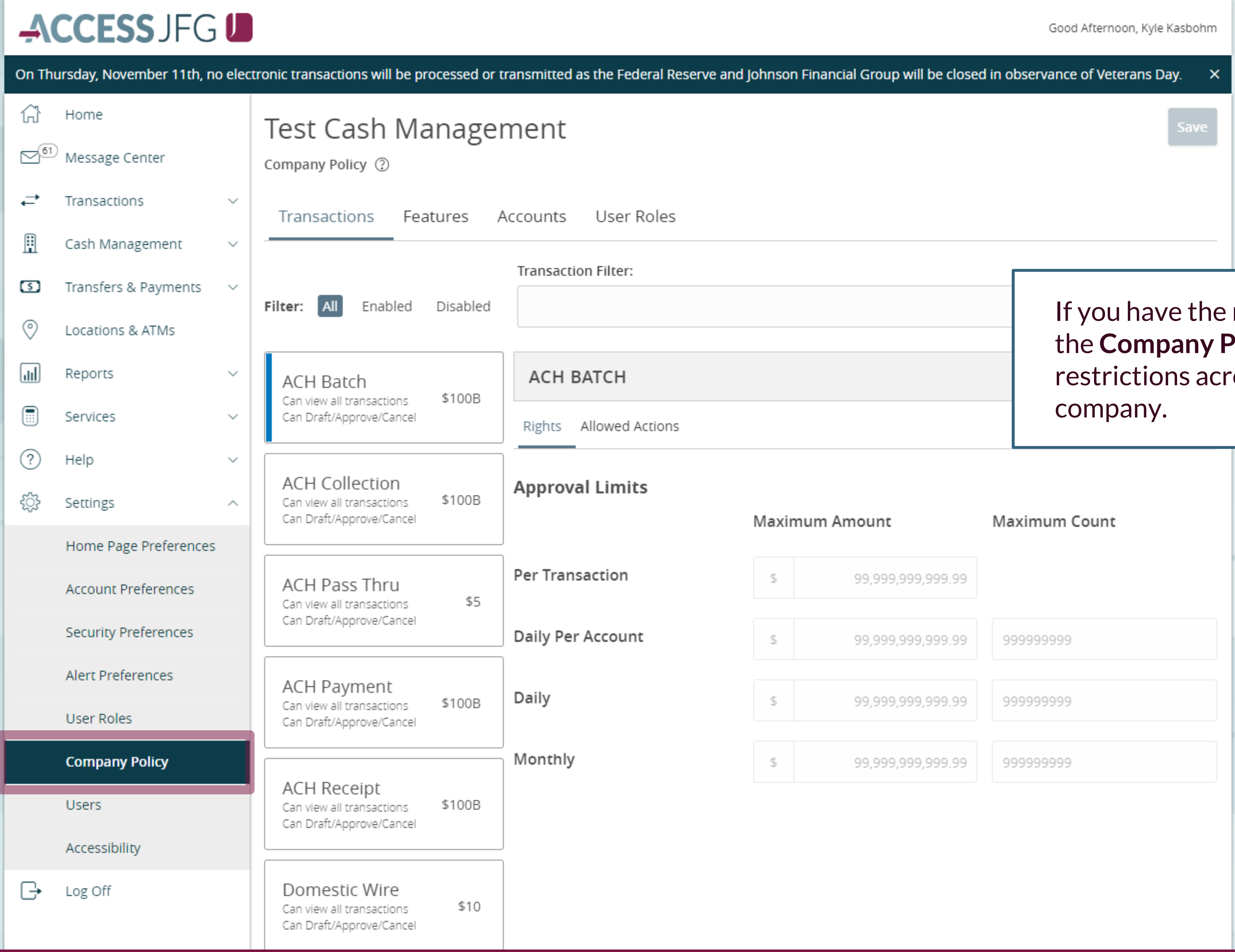


To **add** or **change** a User Role for an existing user, click on the **pencil icon** on that user's tile.

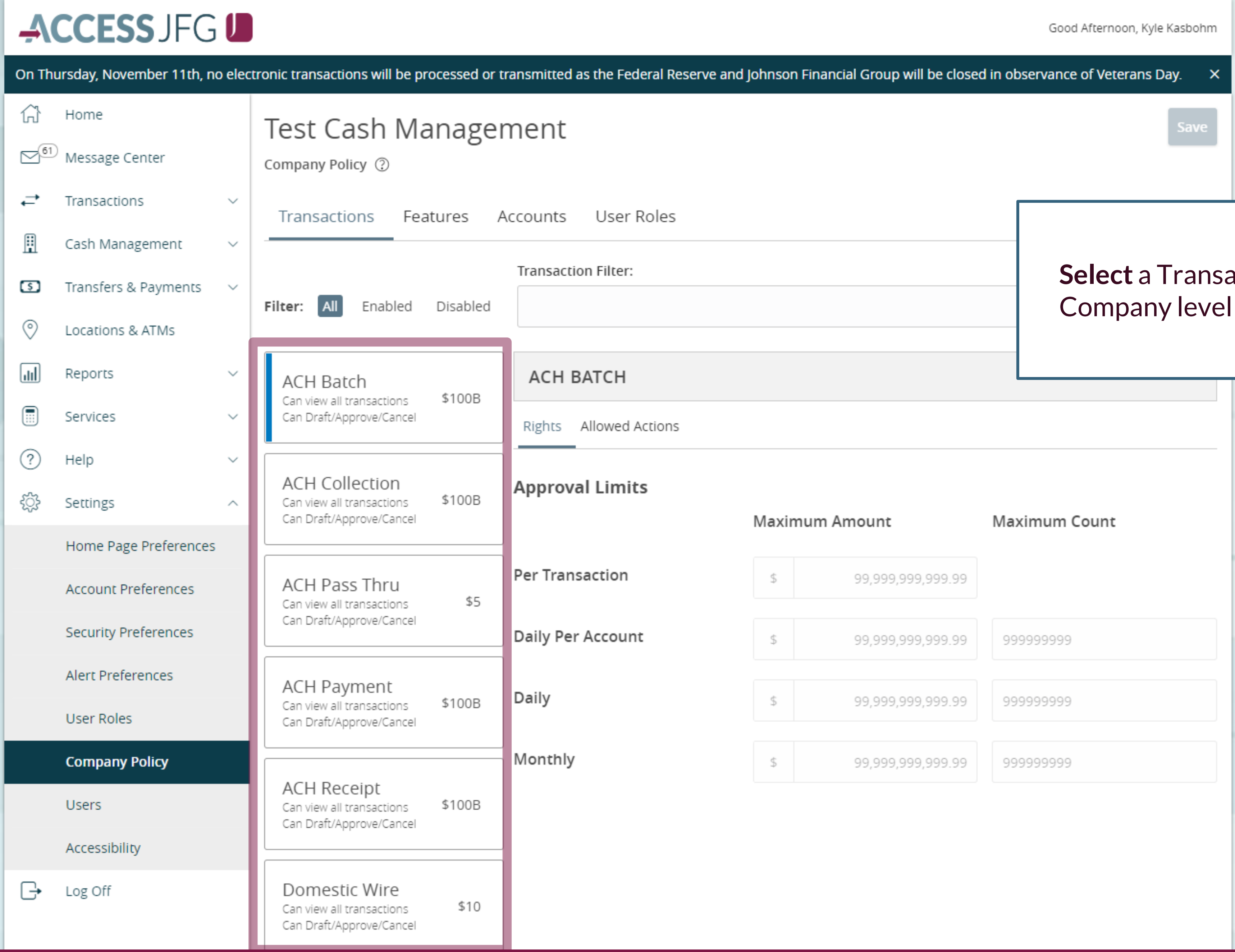


Select the Appropriate User Role from the dropdown menu and assign it to the User. Click **Update Role** to Save.

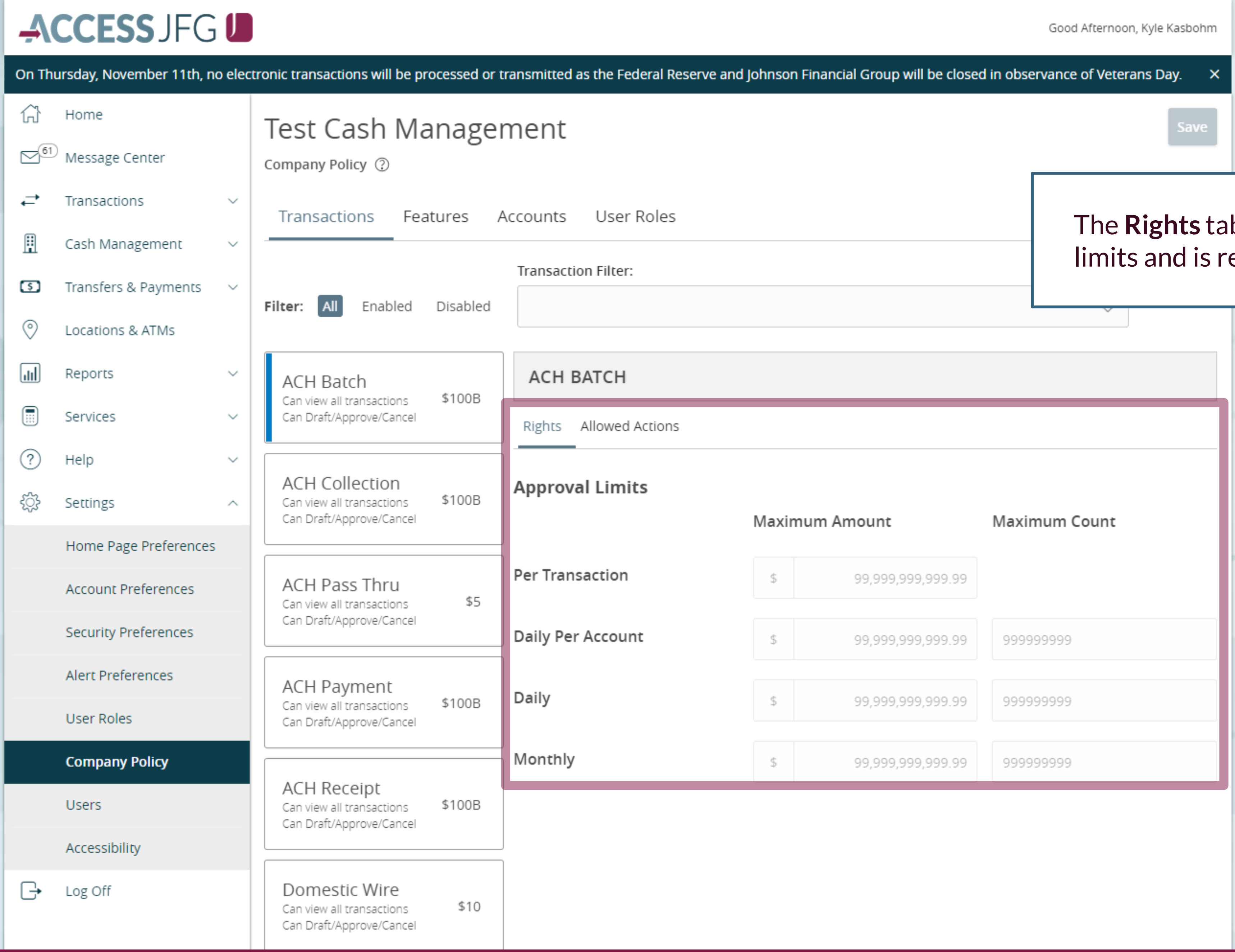
Please note, after a user is created, the User Role is the only information an administrator can update. If the user needs to update phone information, that can be done by the user by following the "**Updating Password & Secure Access Code Phone Numbers**" user guide. Otherwise, for all other detail changes, please contact support at 888.769.3796 (option 2).



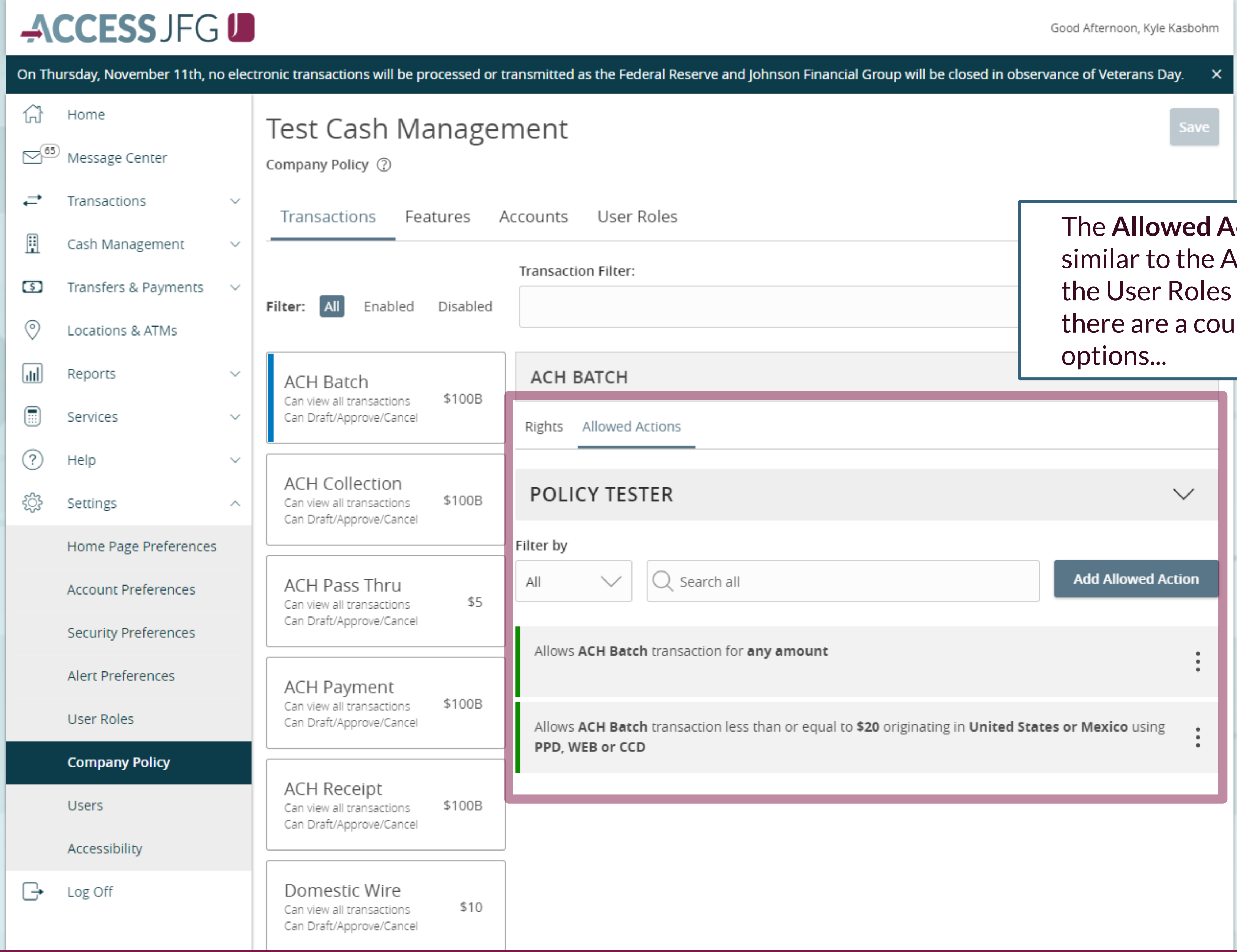
If you have the rights to manage the **Company Policy**, you can add restrictions across all users in the company.



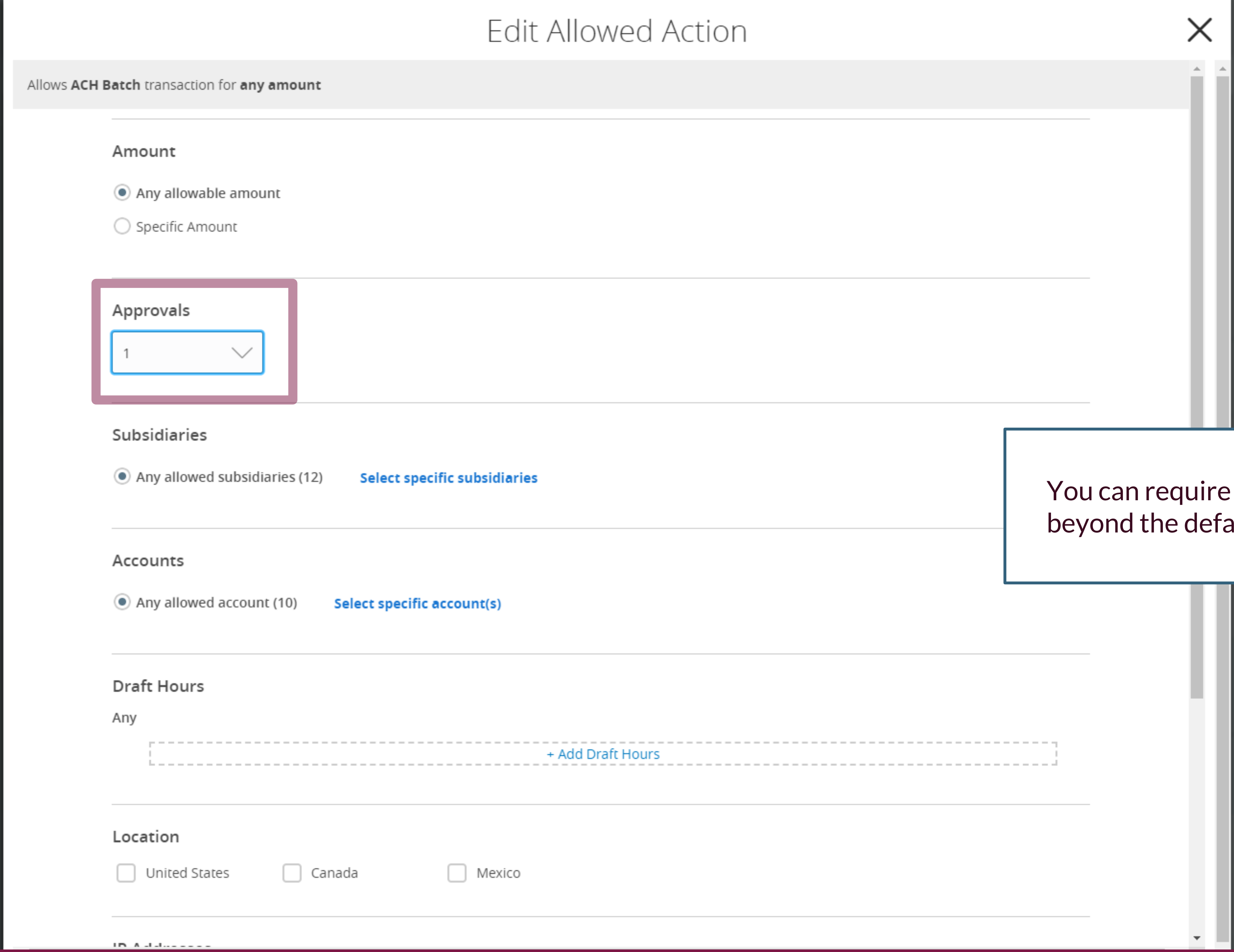
Select a Transaction Type to add Company level restrictions.



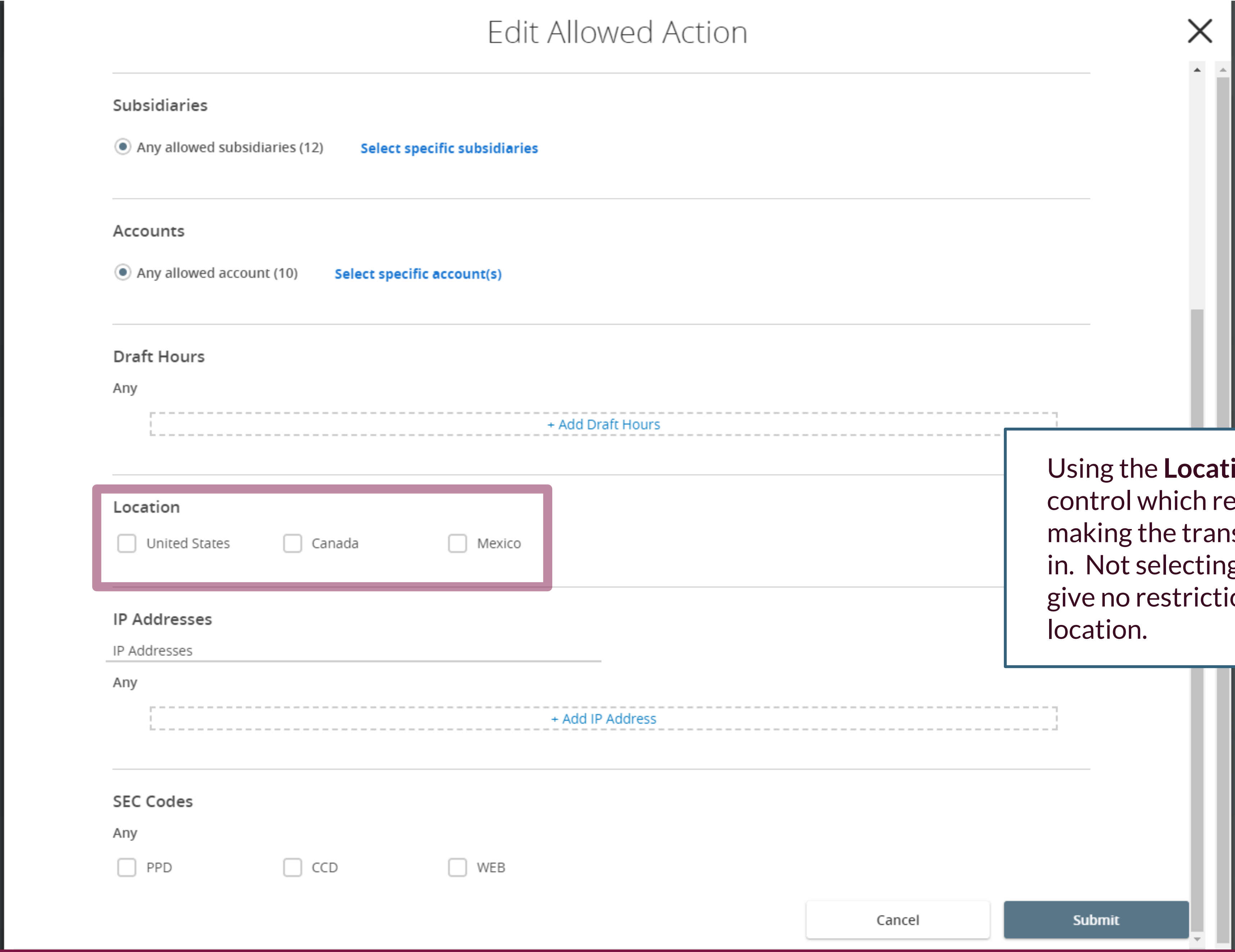
The **Rights** tab will show company limits and is read only.



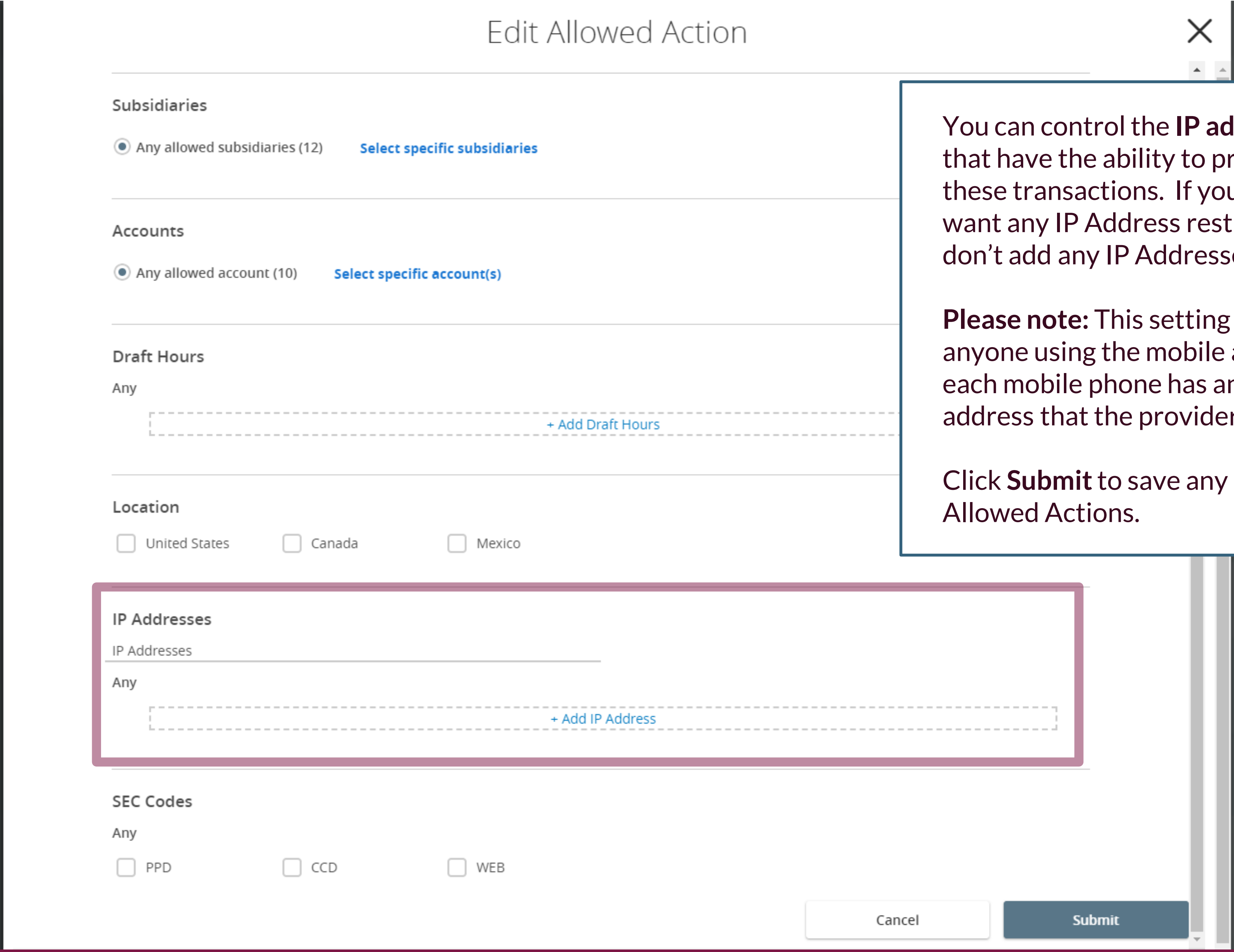
The **Allowed Actions** tab is very similar to the Allowed Actions on the User Roles page. However, there are a couple extra Action options...



You can require extra **Approvals** beyond the default single Approval.



Using the **Location** option, you can control which region the IP address making the transaction may reside in. Not selecting any options will give no restrictions based on location.



You can control the **IP addresses** that have the ability to process these transactions. If you don't want any IP Address restrictions, don't add any IP Addresses.

Please note: This setting will stop anyone using the mobile app, as each mobile phone has an IP address that the provider supplies.

Click **Submit** to save any edits to Allowed Actions.

Thank You

Additional Resources and Support

For additional resources, including “how-to” guides, please visit our online Client Resources page at https://www.johnsonfinancialgroup.com/client-resources

If further support is needed, please call our Treasury Management Support Center at 888.769.3796 or by email at tmsupport@johnsonfinancialgroup.com.