CITY NATIONAL BANK
AN RBC COMPANY

System Administration User Guide

July 2023

CITY NATIONAL BANK
AN RBC COMPANY

Contents

Overview of Administration 5

Key Features 5

Basic Roles/Terms Defined 6

Additional Roles for Account Services Manager Users 7

Managing Users 7

Overview of Creating a New User 7

To Create a New User 8

Enter User Details 9

Assign Administrative Entitlements 10

Select Bank Services 11

Assign Bank Services Entitlements 12

User Entitlements for Account Services Manager 13

Review 14

Business Suite Service Permissions 16

Assigning Payment Entitlements 16

Assigning Reporting Entitlements 18

Assigning Fraud Control Entitlements 18

Assigning Administration Entitlements 19

Assigning Alerts Entitlements 19

Assigning Accounts 20

Applying Payment Limits 21
Business Bill Pay Service Permissions 23
Single Sign On Service Permission Setup 24
Modify an Existing User 24
Deactivate Users 25
Lock/Unlock Users 26
User Reports 26
User and Audit Reporting 27
Accessing Reports via Business Suite 27
Audit Reporting 28
Results based on selections for Audit Reports 31
User Reporting 33
Audit Activity 36
Account Names 37
Manage Alerts 37
Adding Alerts 37
Deleting or Modifying the Alert 38
Adding an Alert Recipient 38
Add Alerts Recipient Group 39
Add Alerts Recipient Group Assignment 39
Manage Imports 39
Import Files 39

Import Maps 40
Appendix A: Alert Types 44
Appendix B: Administration Quick Reference Guide 48
Create New User 48
Assigning Administration Entitlements 49
Assigning Reporting Entitlements 49
Assign Services 49
Assigning Alerts Entitlements 49
Assigning Reporting Entitlements 50

Overview of Administration

Various treasury management services are accessed through the City National Online portal, and it allows you and other administrators for your company to oversee several critical responsibilities. These include managing how your users access these services, and provides easy toggling between those services, such as City National Business Suite®, E-Deposit, and Business Bill Pay.

Key Features

Users – This feature provides you with the ability to manage your company's users, including creating new users, viewing, modifying, or deleting existing users, updating entitlements and access, resetting passwords and locking/unlocking users.

User Approvals – Client Administrators are responsible for approving new Token activations submitted by users. The approval process requires the client administrator to contact TMS Client Services identify the user(s) who submitted token activations and give verbal approval. TMS Client Services will then record the approval in the portal and then the token becomes activated.

Tokens – Users who are responsible for approving ACH and wire payment transactions must have a security token device (either hard token or soft token), in order to generate and then enter a security passcode before the transaction can be sent. These passcodes are one-time-use. A four-digit Personal Identification Number (PIN) is also required for payment authorization.

Personal Identification Number – A unique four-digit PIN is required to be created before a Token device can be activated. The user creates their own PIN within the My Profile section of the portal. It is an added measure of security to ensure that payments are approved by the authorized user.

Company Details – This function displays company details and information including services enrolled, company users and statuses, banking relationship contacts, and other settings.

User Reports – User Reports allows you to generate various reports for your users that can be filtered by service, role, status, and specific users to help you determine if your users' settings are correct.

Audit Login & Access – This audit report provides you with activity related to when your users logged in or out, and what services (e.g., Business Suite, Bill Pay, E-Deposit, etc.) they accessed while using the system.

Audit Activity – This report provides details on the Business Suite banking activity of your users after login, such as whether they completed a transfer, submitted a wire, approved an ACH template, etc.

Bank Account Setting – This feature gives you the ability to view all basic bank account information. It also allows you to modify the company account name(s) that displays throughout the application for you and all of the company's users.

Alerts Center – For your users who use Business Suite, the Alerts function allows you to configure the system to automatically send alert notifications when certain conditions occur. Alerts are organized by module categories.

Export Maps – Provides self-service mapping of export file formats that can be used for download as well as scheduled exports. NEW Export maps created by a user can be used by all users with appropriate entitlements.

Import Maps – The Import Maps feature allows you to create custom file formats that can be used to import data from your systems, in lieu of the bank's standard file formats.

Import Files – This function displays a historical list of your imported files. The files provide details about each import, including comments on any errors that occurred during the import.

Basic Roles/Terms Defined

Client Admin – The Client Administrator is the bank-authorized administrator for the company and by default has access to all services and all accounts. The Client Admin is responsible for adding and maintaining the company's users and assigning services (e.g., Business Suite, Business Bill Pay, E-Deposit, etc.) to a user.

Service Admin – A Service Administrator is the bank-authorized administrator specifically responsible for maintaining a user's permissions to a particular service that has been assigned by the Client Admin, such as Business Suite or Business Bill Pay. Client Admins may also be Service Admins across one or more services.

Service User – A Service User, set up by a Client Administrator, is the end user of a service and is permissioned for functional use of a service. Typically, a Service User does not administer other users, however, a Client Admin could give a Service User administrator rights to add users and assign services. Also, a Service Admin could give a Service User permission to maintain permissions for other users.

Additional Roles for Account Services Manager Users

With the Account Services Manager (ASM) service, there are four additional levels of roles for users. These include the following:

Non-Approver – This setting enables the user to input requests for deposit accounts and account-related products and services in ASM but requires an approver to review and approve before the request is submitted to City National Bank. These users do not have access to treasury management services. **This is the default setting.**

Non-Approver/TM Maintenance – This setting enables the user to request accounts AND treasury management services, but requires an approver for any requests made.

Approver/TM Maintenance – This setting is for approvers of both deposit account requests and treasury management services requests. Approvers may also initiate new requests and submit them to City National Bank without the review of another approver.

View Only – This setting enables the user to view the requests that have been submitted, with no further permissions in ASM.

Note: The specialized roles established in ASM only apply to ASM. Users may be enabled to perform other functions in any other services used by the firm that are also in the City National Online portal.

Managing Users

Overview of Creating a New User

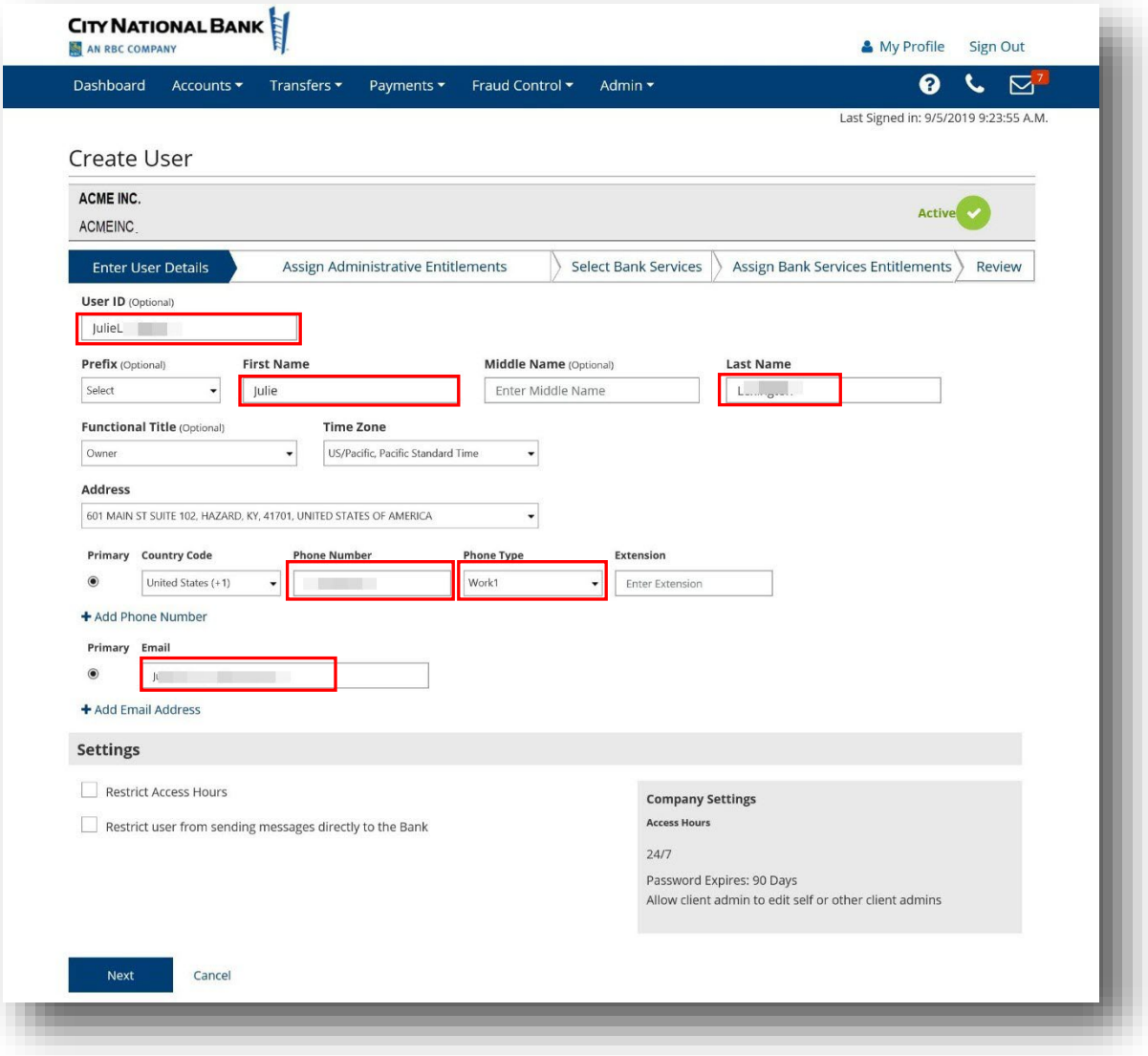
Creating a new user with entitlements is managed through a streamlined workflow process outlined in the following steps:

1. **Enter User Details** - Enter basic user details for the profile and settings information.

2. **Assign Administrative Entitlements** - You may optionally give a user administrative entitlements in order to manage other users in your company.
3. **Select Bank Services** - The Select Bank Services screen allows you to grant the bank services the company has subscribed to and assign those services to the user.
4. **Assign Bank Services Entitlements** - Grant the user functional and account permissions to the services, which is managed in a multi-step process:
    - Set permissions to identify which features and functions to grant the user. This may include payments, reporting, fraud control, administrative and alert functions.
    - Once features and functions for the user are confirmed, assign bank accounts that the user will have access to.
    - You may also apply approval limits that cover transactions the user works with.
5. Review and confirm - Complete a final review to confirm that the profile setup is correct.

To Create a New User

1. Select **Users** from the Admin menu.
2. On the Manage Users page, click **Create User**.
3. The **Create User** page will be displayed.



Enter User Details

The **Enter User Details** section is the first step in the workflow and allows you to add basic information about the user.

1. In the **User ID** section, create a unique User ID. Use only letters and numbers. The User ID should be a minimum of three characters and a maximum of 20 characters long. If you input a User ID that is already in use or taken, the system will show an error message stating, “We couldn’t use that User ID. Please try another one.”

Note: If you do not enter a User ID, the system will automatically create a unique one for you.

2. Enter the user's first name and last name in the **First Name** and **Last Name** fields.
3. Enter the user's phone number and phone type in the **Phone Number** and **Phone Type** fields. To add additional phone numbers, click **Add Phone Number**.
4. Enter the user's email address in the **Email Address** field. To add an additional email address, click **Add Email Address**.
5. (Optional) Select a prefix for the user in the **Prefix** field.
6. (Optional) Enter the user's middle name in the **Middle Name** field.
7. (Optional) Select a time zone for the user in the **Time Zone** field. (If not selected, Time Zone will default to Pacific Time Zone).
8. (Optional) Select a Functional Title for the user in the **Functional Title** field.
9. In the **Settings** section, you can set up some restrictions for the user's profile:
    - **Restrict Access Hours**, which provides day of the week and hours of the day settings for limiting a user's access to the system.
    - **Restrict User from Sending Messages Directly to the Bank**, which will prevent the user from sending messages to the Bank Support team but allow the user to receive important messages from the bank.

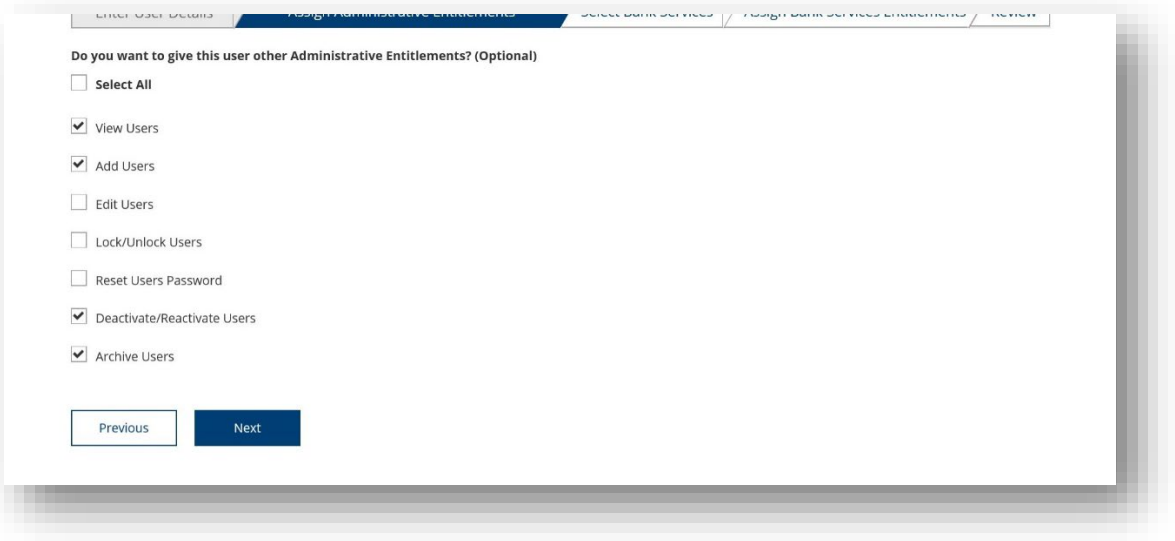
Note: Client Admins always have access to all messages sent to or from anyone in the Company.

10. Click **Next** to proceed to the next step in the workflow to **Assign Administrative Services**. (Note: If a User ID is already in use or taken, the error message in #1 above will appear after clicking **Next.**)

Assign Administrative Entitlements

The **Assign Administrative Entitlements** screen will allow you to grant the user permissions to manage administrative entitlements for other users.

Check the **Select All** or the individual boxes to grant the user access to administrative entitlements including viewing, adding, editing, locking/unlocking users, resetting passwords and/or activating/deactivating and archiving passwords. Selecting All will make the user in effect a "Junior Administrator" or User with Administrator Rights and enables the user to do most all functions of a Client Administrator.



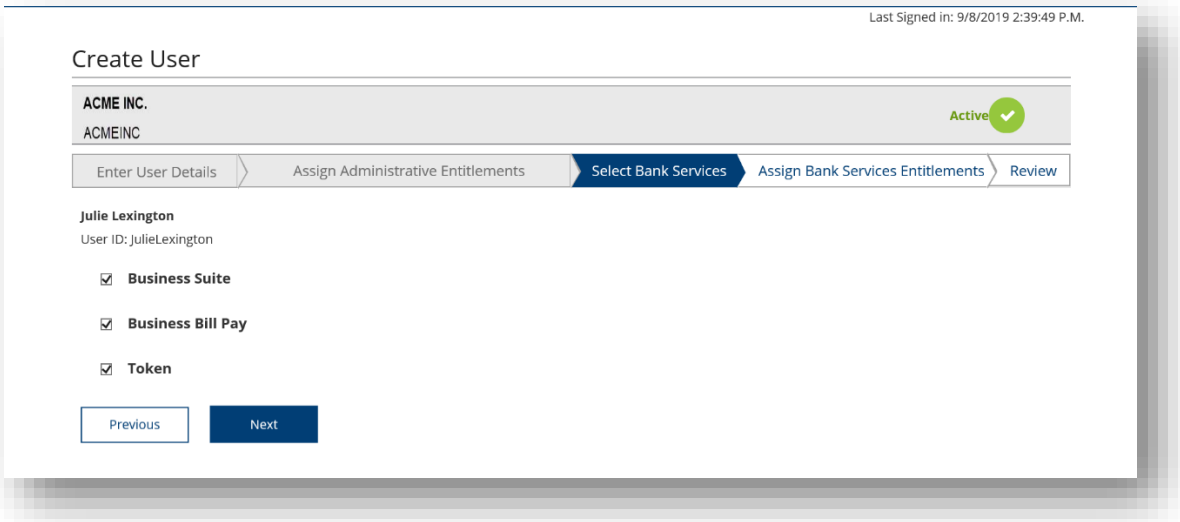
Click **Next** to move to the next step in the workflow to **Select Bank Services.**

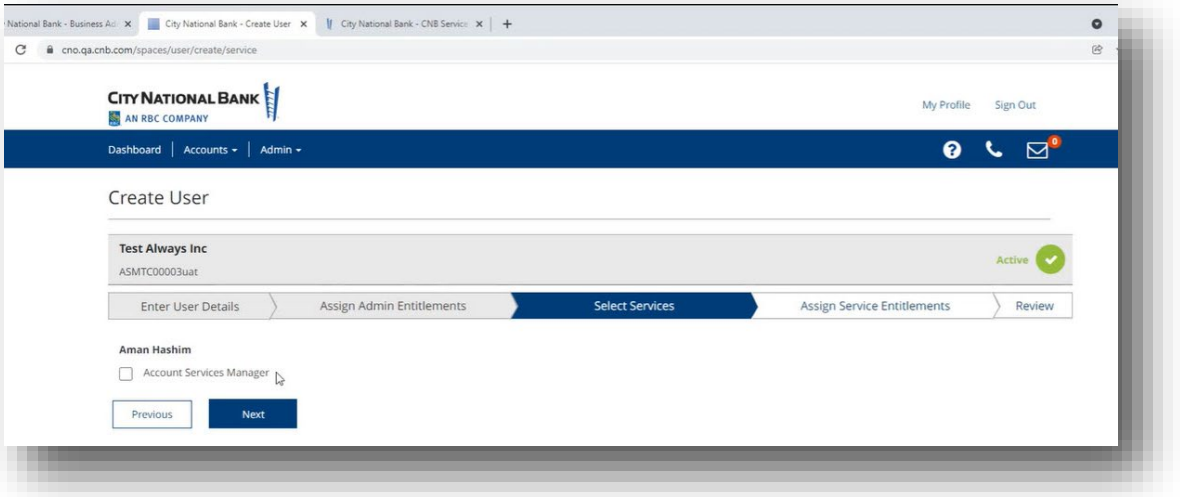
Note: **Archive Users** is an option for requesting a deactivated user to be purged overnight. Otherwise, a Deactivated User will remain in the system for 90 days and then be purged.

Select Bank Services

The **Select Bank Services** screen will allow you to grant the bank services your company has subscribed to and assign those Bank Services to the users as appropriate.

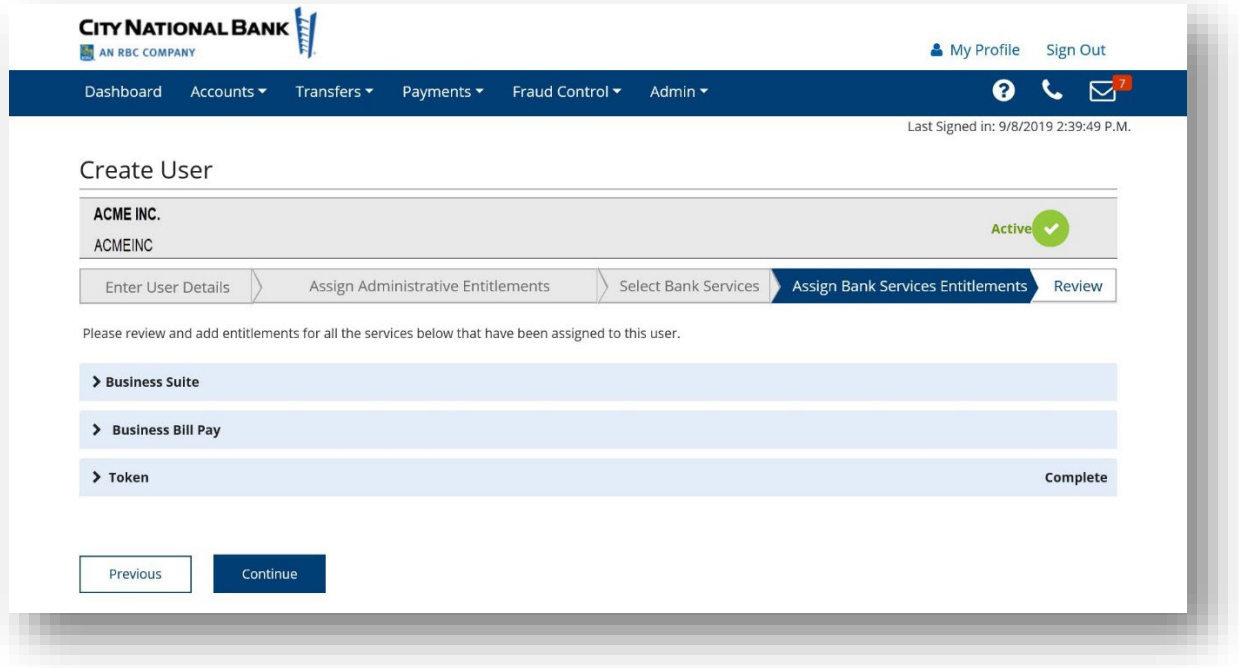
1. Check the box next to each service to which you wish to grant the user access.
2. Click **Next** to continue.





Assign Bank Services Entitlements

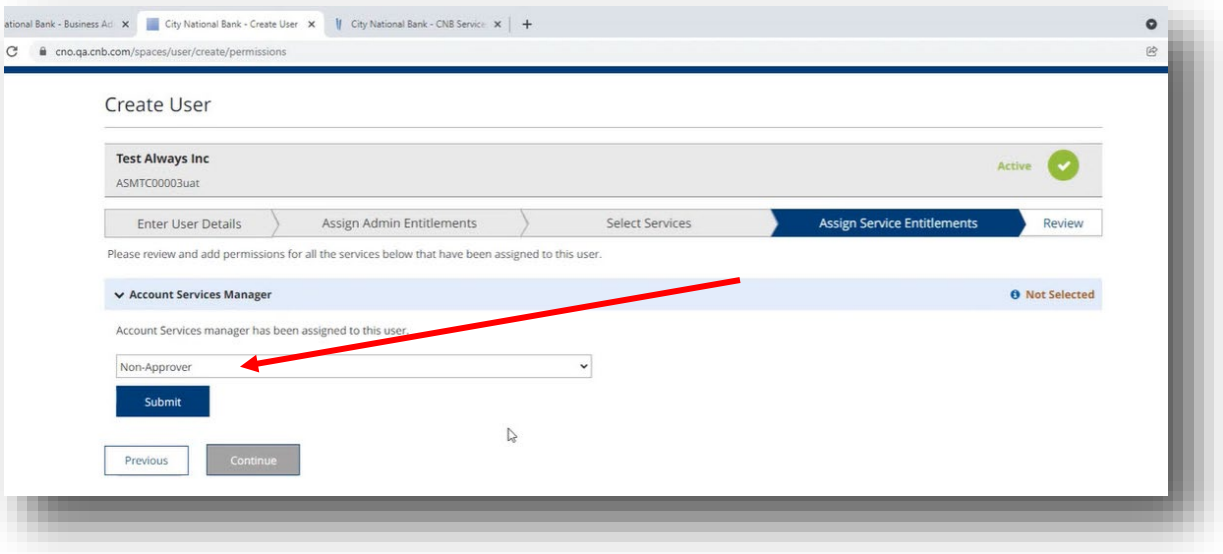
In the **Assign Services Entitlements** screen, you can now grant the user permissions to features and functions such as payments, reporting, fraud control, administration, and alerts. You will also be able to assign accounts and set up approval limits. Click the arrow for the service to expand the section. Select **Continue** to review entitlements, bank services and bank service entitlements assigned to this user.



User Entitlements for Account Services Manager

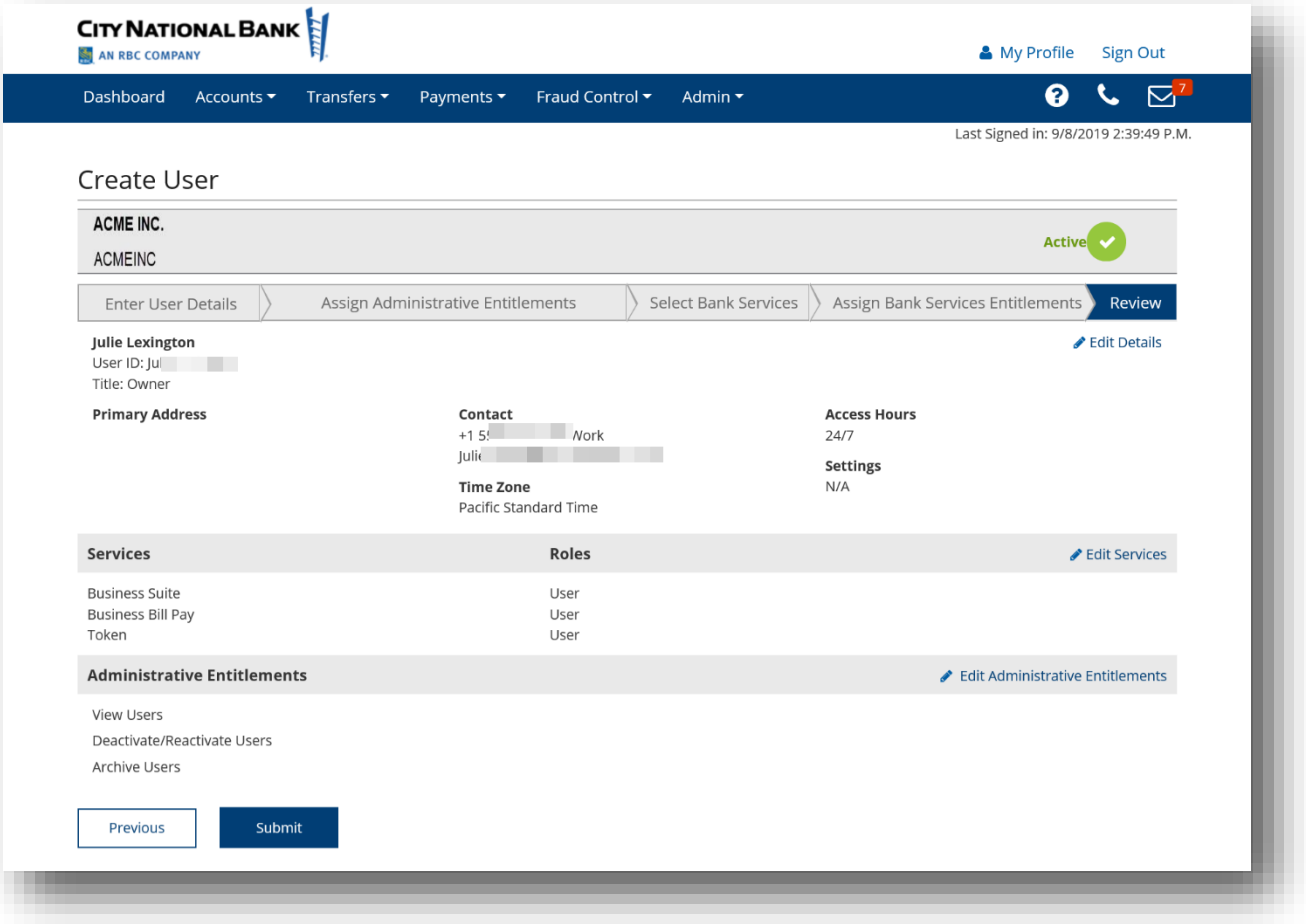
When setting up an Account Services Manager user, you will assign entitlements as follows.

1. Click Account Services Manager on the **Assign Bank Services Entitlements** screen.
2. On the drop-down menu, select which of the four roles apply to the user as shown below. These include the following options as described above:
   - View Only
   - Non-Approver (default)
   - Non-Approver/TM Maintenance
   - Approver/ TM Maintenance

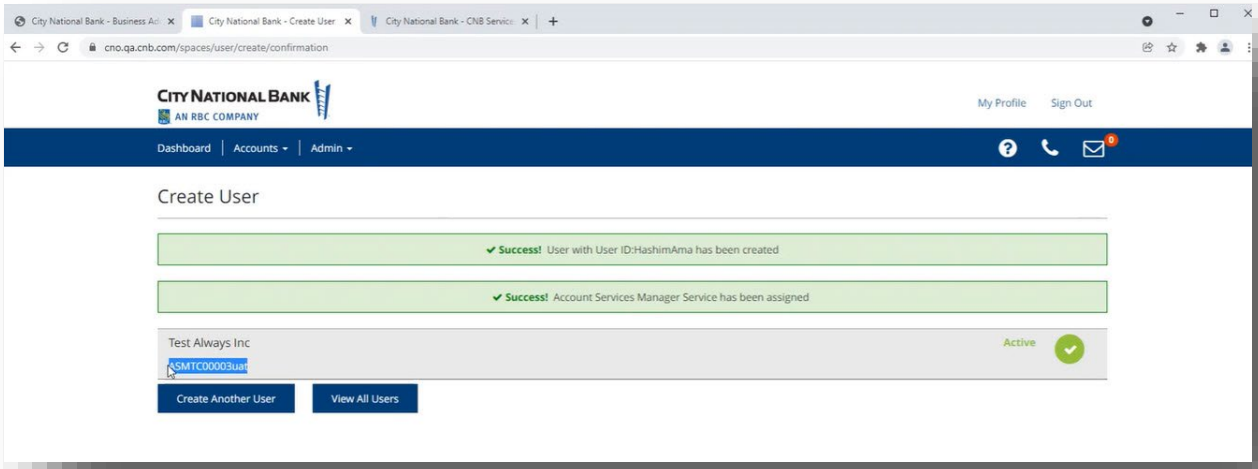


Review

Review the information that has been entered for this user. Validate that the **Administrative Entitlements** and **Bank Services** are correct and that the **Bank Service Entitlements** assigned to this user are also correct. If all information is correct, select **Submit**. The new user is created.

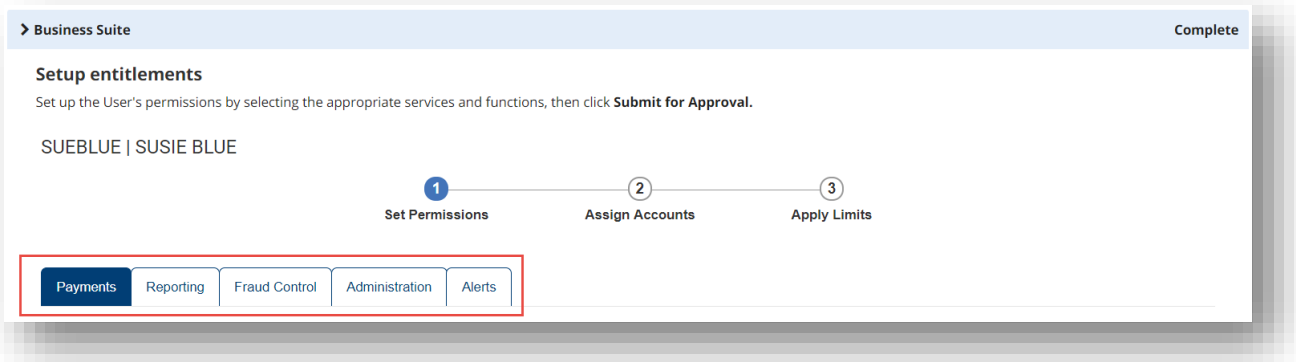


After adding a service for the user, the confirmation screen will appear as shown below.



Business Suite Service Permissions

The steps below highlight the setup for a new user of the **Business Suite** service and the process to set permissions for the user for Payments, Reporting, Fraud Control, Administration and Alerts. Each service has a tab that you will select in order to set permissions for that service. Depending on the features and functions your company has set up, you may not see all service tabs.



Assigning Payment Entitlements

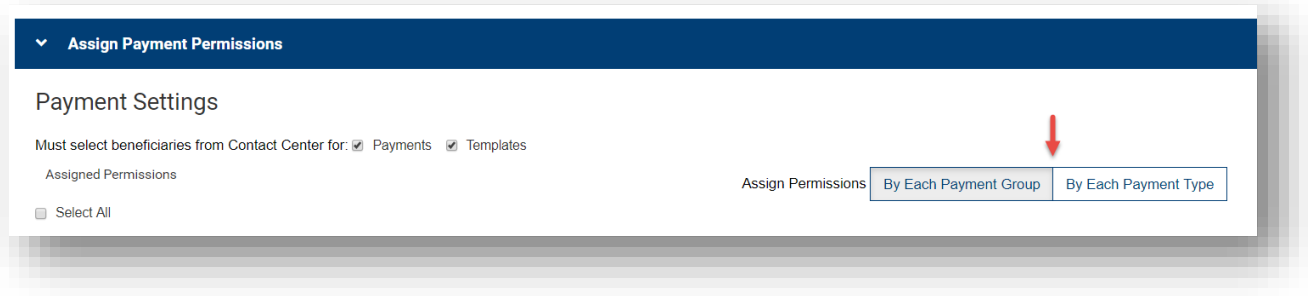
The **Payments** tab allows you to grant access to payment types, assign payment permissions and assign restricted templates.

To assign entitlements by each payment type:

1. The section displays all available payment types. Click the range of permissions you want to apply for each payment type.
2. To assign all permissions for a payment type, check the **Select All** checkbox under the specific payment type.
3. To assign all permissions for all payment settings, check the **Select All** checkbox at the top of the section.

To assign entitlements to payment permissions by each payment type:

1. Click the **By Each Payment Type** button.
   - The screen displays all available payment types.
   - To expand all sections for easy access, click **Expand All**. Otherwise, use the right arrow button to expand each section individually.
2. For each payment type, assign permissions as desired for the user. If you would like to assign all permissions to a payment type for a user, check the **Select All** checkbox.
3. Repeat the process of assigning permissions to payment types or groups for each broad category of payments (for example, **Wires** or **Transfers**) you have assigned to this user. Click the appropriate heading to assign permissions.



To assign entitlements to payment permissions by each payment group:

1. Click the **By Each Payment Group** button.
2. For each category of payment and template permissions (such as **Imports** or **Repetitive Wires**), select the range of permissions you want to apply (for example, **View** or **Manage**). To assign all permissions to payments or templates, check the **Select All** checkboxes.

3. For each category of payments and templates, use the drop-down to select how many approvals are required for each category.

To assign restricted templates entitlements:

1. If you want to assign all templates, whether current or future, to the user, check the **Assign all current & future templates** box. This is an ease-of-use feature since you will not have to assign future templates on an individual basis as they become available.
2. In the grid at the bottom of the section, check the boxes for as many of the available templates as you wish to assign. You can also assign all templates.

Note: At least one restricted template must be in place for this entitlement option to display.

Next, assign reporting entitlements. Click the **Reporting** tab at the top of the screen.

Assigning Reporting Entitlements

The **Reporting** tab allows you to grant the user permission to access various types of balance and transaction data, including **Balance and Transaction** reports, **Statements**, **Payment Reports**, **Checks and Stops Inquiry**, and **Image Search**.

To assign reporting entitlements:

1. To entitle the user to all available reports, check the **Select All** checkbox.
2. Otherwise, select the individual checkboxes for the report or reports (for example, **Balance & Transactions**) you would like to entitle the user to.
3. For each report group, you can choose to entitle the user to all reports or individual reports by checking the appropriate boxes.

Next, assign fraud control entitlements. Click the **Fraud Control** tab at the top of the screen.

Assigning Fraud Control Entitlements

The **Fraud Control** tab allows you to grant access to various types of fraud protection services, including Positive Pay and Stop Payments.

To assign Fraud Control entitlements:

1. To entitle the user to all areas of Fraud Control, which includes Check Services, Positive Pay Processing and Stop Payments, check the **Select All** checkbox.
2. Otherwise, select the checkbox(es) for the permissions you want to grant.

For example, to allow the user to manage check issues/voids, select the **Manage** checkbox in the **Check Issue/Void** row. To allow the user to approve **Positive Pay** decisions, select the **Approve** checkbox in the **Positive Pay Processing row.**

Note: For some areas of **Risk Management**, you can click **Select All** to assign all permissions.

Next, assign administration entitlements. Click the **Administration** tab at the top of the screen.

Assigning Administration Entitlements

The **Administration** tab allows you to grant access to administrative functions on the client application.

To assign administrative entitlements:

1. To entitle the user to all areas of administration, check the **Select All** checkbox.
2. Otherwise, select the checkbox(es) for the permissions you want to grant. For example, to allow the user to view users but not manage or approve them, click *only* the **View** checkbox under **User Administration**.

Note: For some areas of Administration, you can click **Select All** to assign all permissions.

Next, assign alerts entitlements. Click the **Alerts** tab at the top of the screen.

Note: Alert types are defined in Appendix A – Alert Types.

Assigning Alerts Entitlements

The **Alerts** tab allows you to grant permission for alerts.

To assign alerts entitlements:

1. To entitle the user to all alerts, check the **Select All** checkbox.
2. Otherwise, select the checkboxes for the alerts you want to grant access to.

You are now ready to assign bank accounts to the user. Click **Continue** or **Assign Accounts** at the top of the screen.

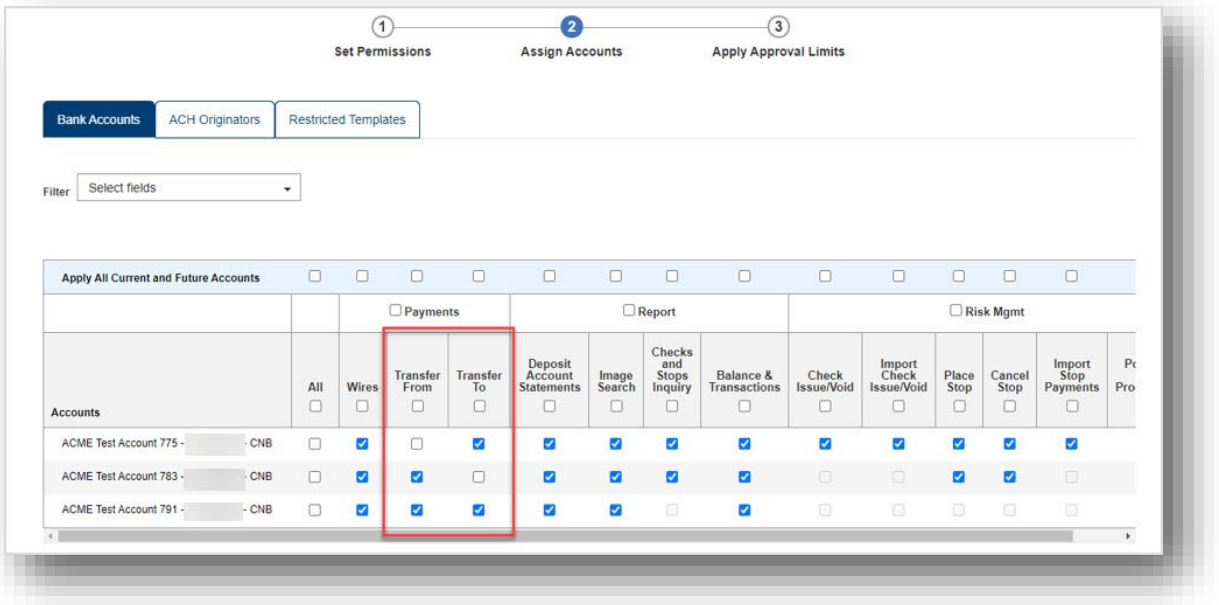
Assigning Accounts

The Accounts section of the Setup Entitlements screen allows you to assign the bank accounts that the current user can work with.

To assign bank accounts to the user:

With the **Bank Accounts** tab selected, check the boxes corresponding to the reports and functions you want the user to be able to use with the specified account.

- You can assign all accounts and all reports and functions to the user by checking the **All** checkbox. Alternatively, you can choose to assign all accounts to a user for a particular payment type (for example, Wires) by checking the box at the top of the column corresponding to the payment type.
- You can assign all accounts for all payment types by checking the **Payments** checkbox.
- You can assign all current and future accounts to each of the assigned payment types by checking the appropriate checkbox in the **Apply All Current & Future Accounts** row. You can also choose to assign *all* current and future accounts to the user by checking all checkboxes in the row.



To assign ACH originators to the user:

Click the **ACH Originators** tab at the top of the screen.

- You can assign all accounts to the user by checking the **All** checkbox. Alternatively, you can choose to assign all ACH accounts by checking the **Payments** box.
- You can assign all current and future accounts for payment types by checking the **Apply All Current & Future Accounts** row.

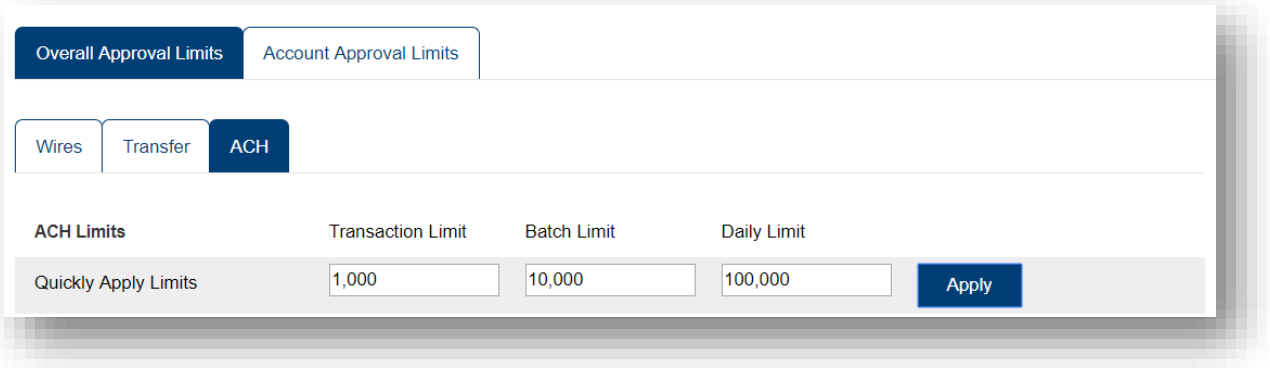
Finally, you may apply approval limits for the transactions the user is entitled to approve. Click **Continue** OR **Apply Limits** at the top of the screen.

Applying Payment Limits

The **Apply Limits** section of the Setup Entitlements screen allows you to assign overall approval limits and limits associated with individual bank accounts assigned to the user. Overall approval limits indicate the maximum value of payments the user can approve. Values in this section are expressed in the default currency of your company.

There are three types of limits: Transaction, Batch (ACH only) and Daily.

- A transaction approval limit indicates the maximum amount of a single transaction. This limit applies to both wire and batch payments.
- A batch approval limit is the maximum amount of all ACH items in a batch. This limit is not applicable to wire payments.
- A daily approval limit is the maximum total value of all payments that can be approved on a given value date.



To apply overall approval limits to the user:

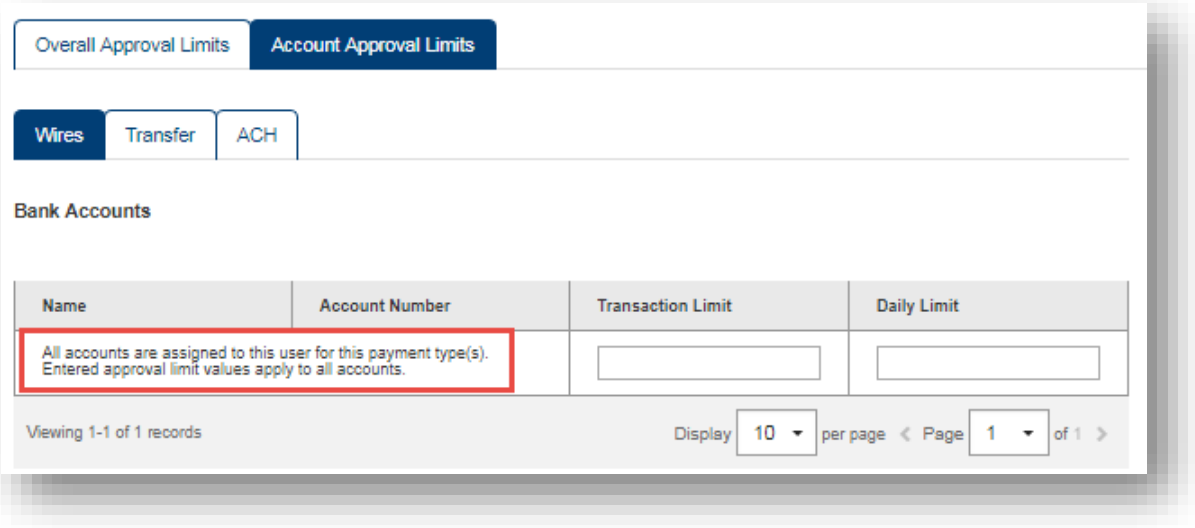
1. With **Overall Approval Limits** selected, enter the transaction, batch, and daily limits for each payment type in the selected payment group.
2. To apply these limits to all payment types in the group, enter the transaction, batch, and daily limit in the **Quickly Apply Limits** row, and then click **Apply**.
3. To assign approval limits to another payment group, click the group name tab (**Wires**, **Transfer**, **ACH**).
4. Repeat the actions in step 1 for the remaining payment types and groups assigned to this user.

To assign account approval limits to the user:

1. Click **Account Approval Limits** at the top of the screen.
2. Set approval limits by entering the limit in the appropriate text box. If you assigned permissions by each payment type, the types will be listed in separate sections. Click the arrow to expand a section.
3. You can set limits for multiple accounts by clicking the **Quickly Apply limits** link. The limits entered in this window will be applied to all accounts the user is assigned to. However, you can edit the limit for individual accounts.

4. By default, the user can perform any action on an account that was assigned in the **Set Permissions** section. However, actions can be restricted for an account by clicking the **Show** button next to **Advanced Account Permissions**.
5. After clicking the **Show** button, icons appear on the far-right side of the screen. Clicking a checkbox allows you to assign the actions a user can perform on payments or templates originating from the account. A check in the box indicates that the action can be performed on the account.
6. Repeat steps 2-5 for each payment type and payment group assigned to this user. You can navigate to the next payment group by clicking the appropriate link.
7. When you have finished granting all permissions to the user, click **Add User**.
8. The user record will be displayed on the User Maintenance widget. A user record must be approved before it can be used.

Note: If **Apply All Current & Future Accounts** is checked under Assign Accounts, limits applied to a payment type will apply to all accounts.



Business Bill Pay Service Permissions

The steps below cover how to set up a user for Business Bill Pay.

Click **Submit** to be taken to the **Review** screen to verify user profile settings.

1. Select the accordion fold for Business Bill Pay to access the user's service permissions.
2. Assign **Administrative** entitlement to Add/Modify Bill Pay users.

3. Assign which accounts the user will have access to.
4. Assign which functions the user will have access to, such as **Make Payments**, **Approve Payments,** and **Access Reports**.
5. If appropriate, set a user's Bill Pay transaction limits. The bank's default limits are $50,000 per day and per transaction, so a user's limits can be set lower than that, but not higher.

Once all Service Permissions are correct for each service, click **Submit** to move to the **Review** screen. If there are errors in the user's profile, you can update it by clicking the **Edit Details** or **Edit Services** link.

Single Sign On Service Permission Setup

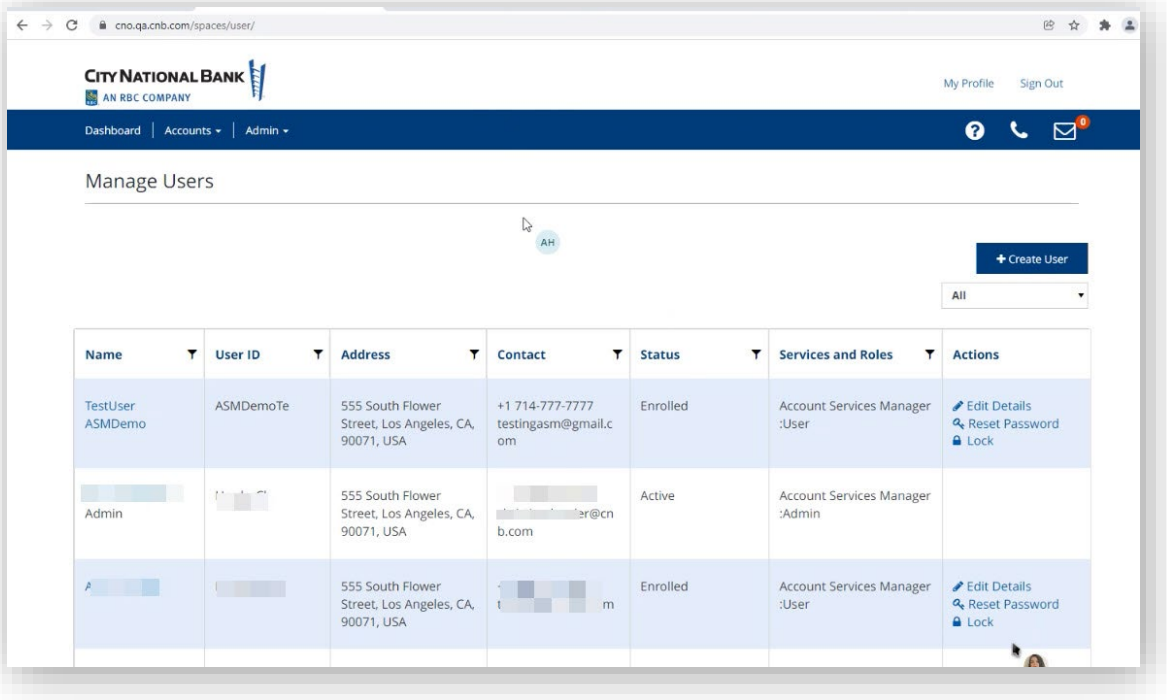
Users who will use other Treasury Management Services in City National Online will also need to be set up on CNO before being set up in the single sign on service(s).

- ACH Positive Pay
- Account Reconcilements Processing/Reporting
- E-Deposit
- Account Services Manager

Modify an Existing User

To edit the profile information or user entitlements for an existing user.

1. Select **Users** from the **Admin** menu. The Manage Users screen will be displayed, as shown below.



2. Locate the user you wish to modify and click **Edit Details** in the row where their profile information is displayed. The Edit User screen will be displayed.
3. The **Edit User Details** tab will allow you to make updates to any contact information related to the user's profile. You can also update the **Settings** boxes for the user.
4. The **Assign Services** tab will allow you to make updates to the user's entitlements. If you want to add or remove a service and all permissions from the user, you can check/uncheck the box for that service. If you want to update entitlements for the products and services set up for the user, click **Set Specific Service Permissions**. This will take you through the process to edit their entitlements. For information on this process, see **Service Permissions**.
5. If you want to update the user's administrative permissions, click **Edit Specific Administration Permissions**. Update selections and click **Save**.

Deactivate Users

This function will allow you, as an administrator, to deactivate a user and prevent the user from accessing the system.

To deactivate a user:

1. Select **Users** from the **Admin** menu. The **Manage Users** screen will be displayed.
2. Locate the user you wish to modify and click their name in the row where their profile information is displayed. The **View User** screen will be displayed.
3. Click **View Details** at the top right of the screen.
4. Click **Deactivate** at the top right of the screen.
5. Select **Reason for Deactivating User** from the drop-down.
6. Click Deactivate User.

Lock/Unlock Users

This function will allow you, as an administrator, to temporarily prevent a user from accessing the system or restore a user who has been locked out of the system (for example, if a user is locked out due to exceeding the maximum number of login attempts).

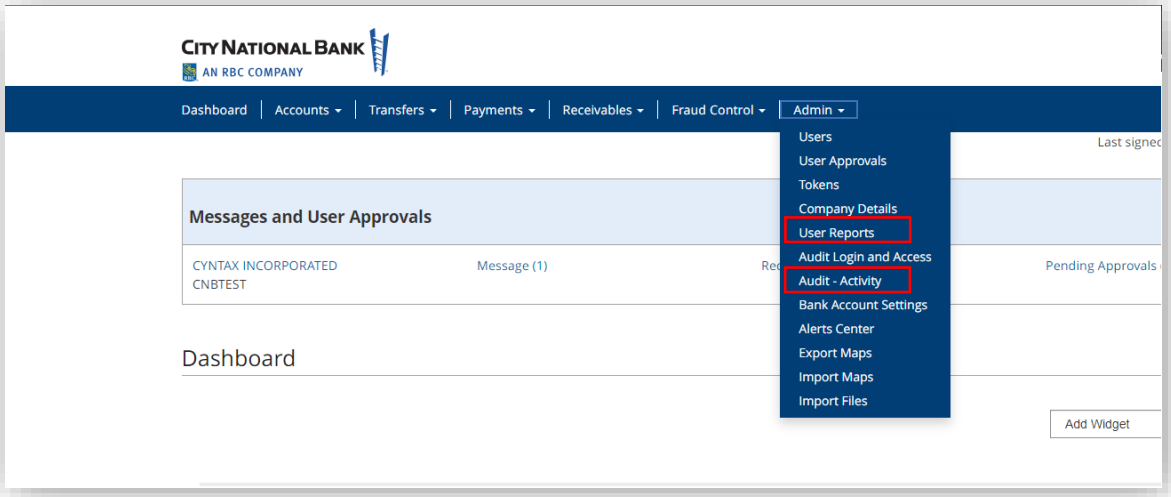
To lock or unlock a user:

1. Select **Users** from the **Admin** menu. The Manage Users screen will be displayed.
2. Locate the user you wish to update and confirm in the **Status** column that they are showing as **Locked** (if you want to unlock the user) or **Active** (if you want to lock the user).
   - If the user is in a Locked status, click **Unlock**
   - If the user is in an Active status, click **Lock**.
3. Select the reason for locking or unlocking the user from the drop-down.
4. Click **Lock User** to lock the user or Click **Unlock User** to unlock the user.

User Reports

The User Reports feature allows you to generate various reports on your users that can be filtered by service, role, or status, and specific users to help you determine if your users' settings are correct.

Under the Reporting menu, client administrators have the option to see User Reports, and Audit Report.

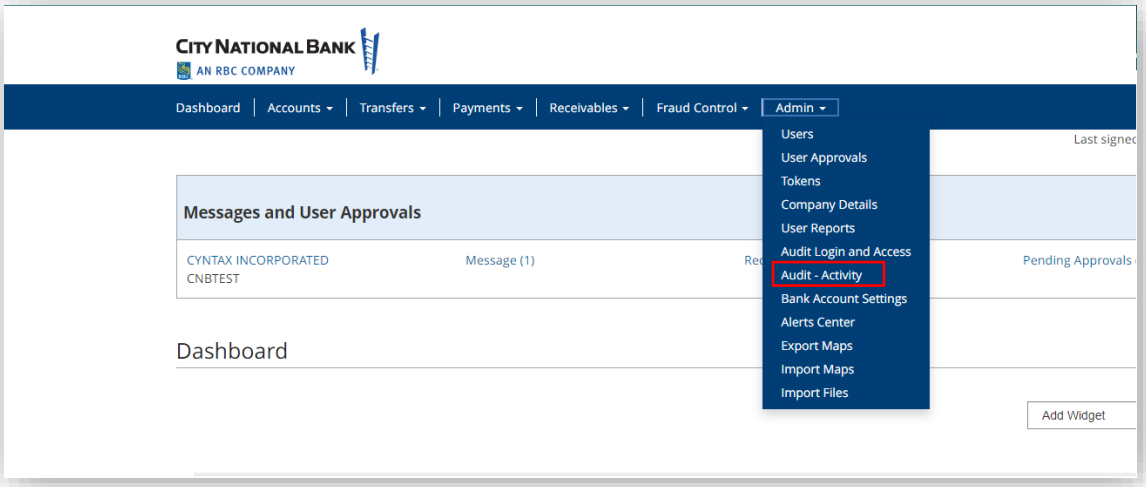


User and Audit Reporting

Audit and user reports provide client administrative users with dynamic, flexible report creation. Users have the option to view searchable fields directly on the screen or export them to csv files.

Accessing Reports via Business Suite

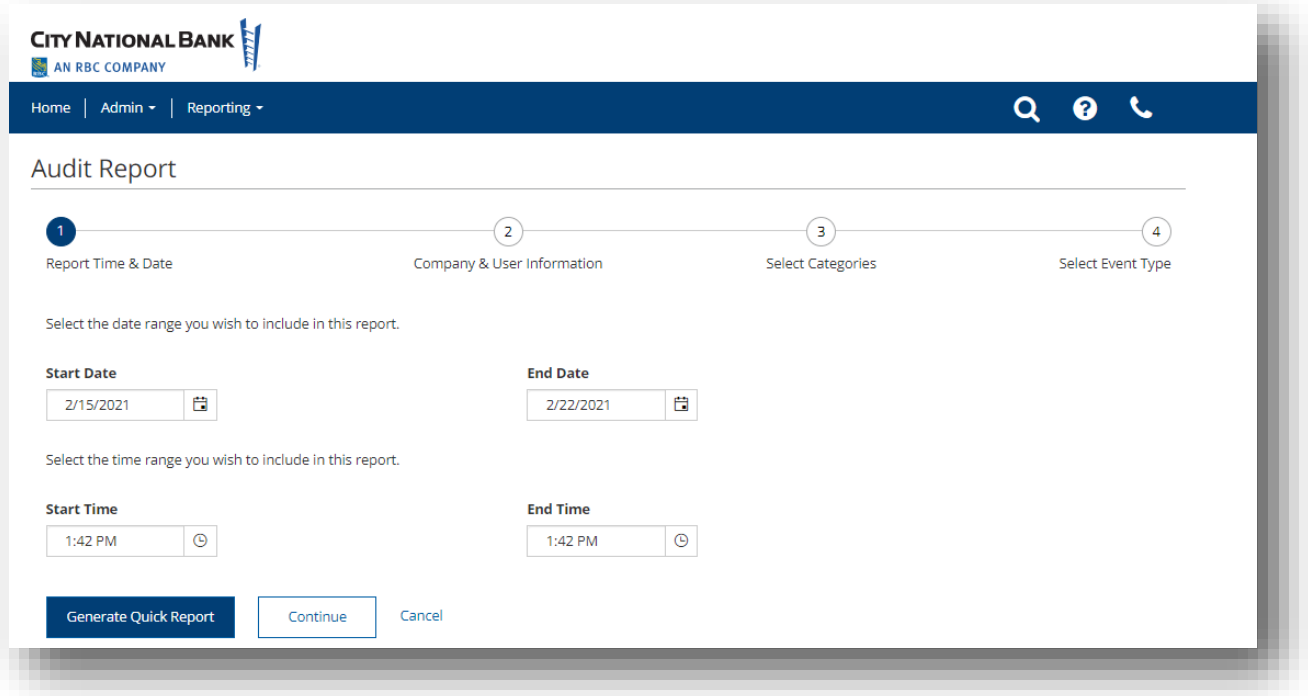
Within the Business Suite, under the Admin menu, Client Administrators have the option to see User Reports and the Audit Report.



Audit Reporting

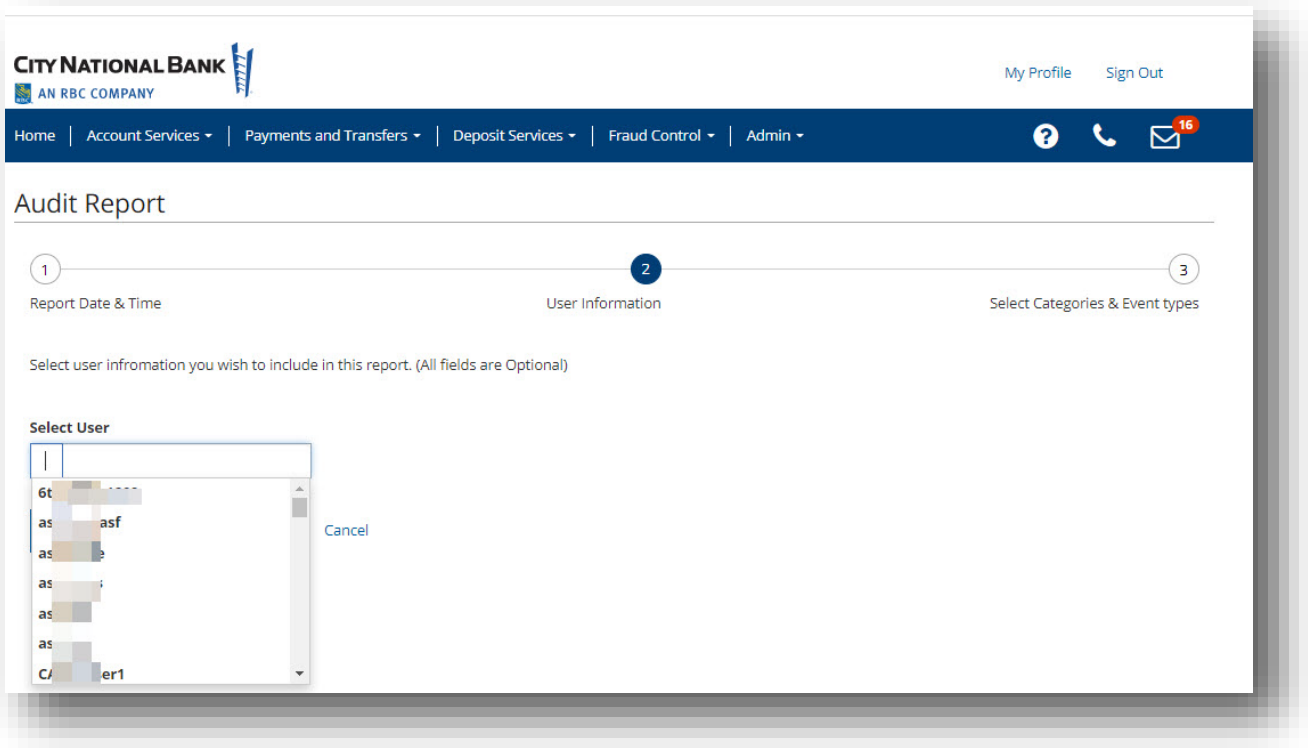
The Audit reporting page is divided up into four different sections that only Client Administrators are able to search by:

- Report Time and Date
- User Information
- Categories
- Event Type

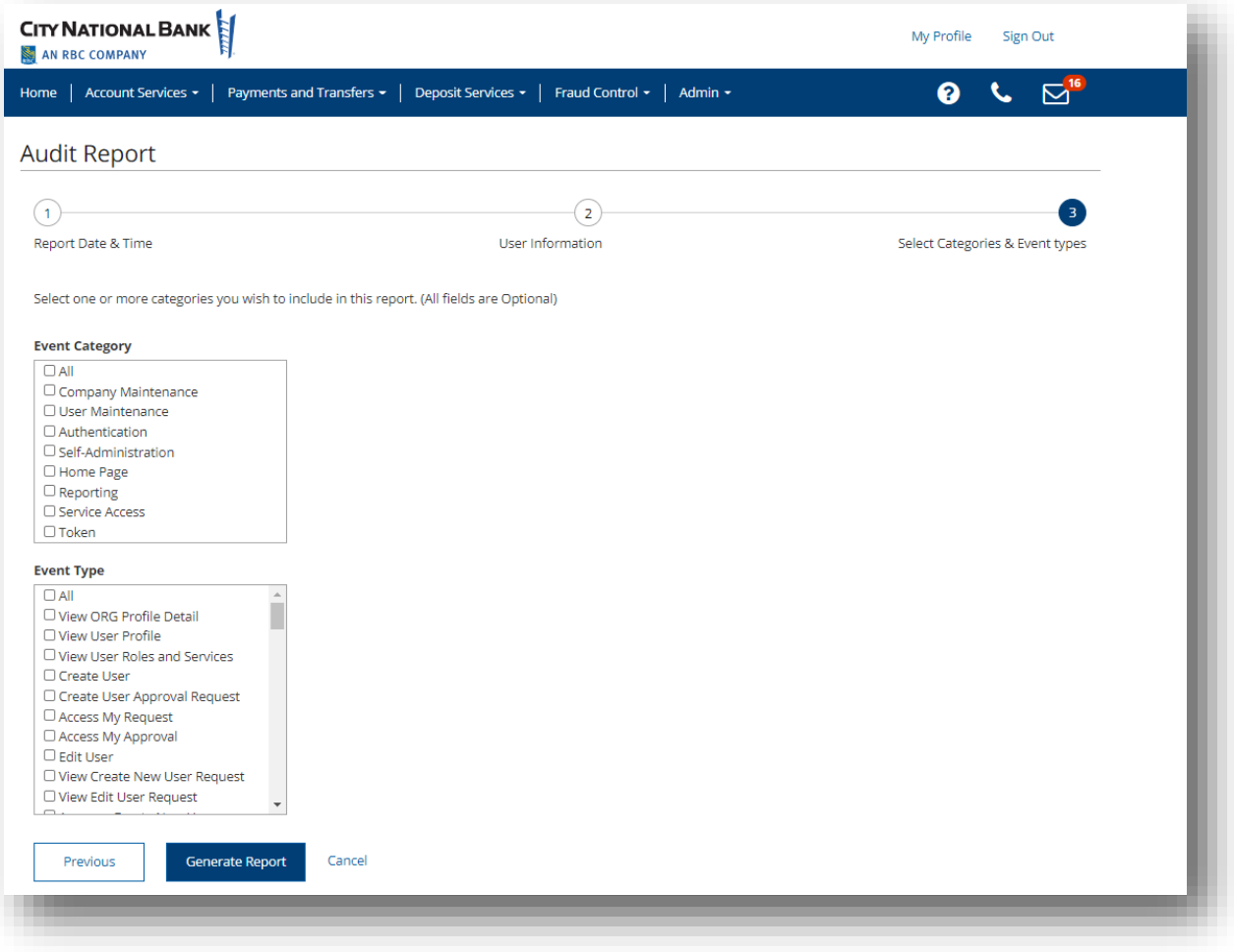


With the Generate Quick Report option, Client Administrators can run reports with just a Start Date and End Date, within a seven-day range. This can include a range of times you would like to have included in your report, or continue to the following sections for more defined results.

Click **Continue** to move to the next section.



Your company's user list will appear to help drill down the report to the level you are looking for. If no user is selected, all will be included in the report.



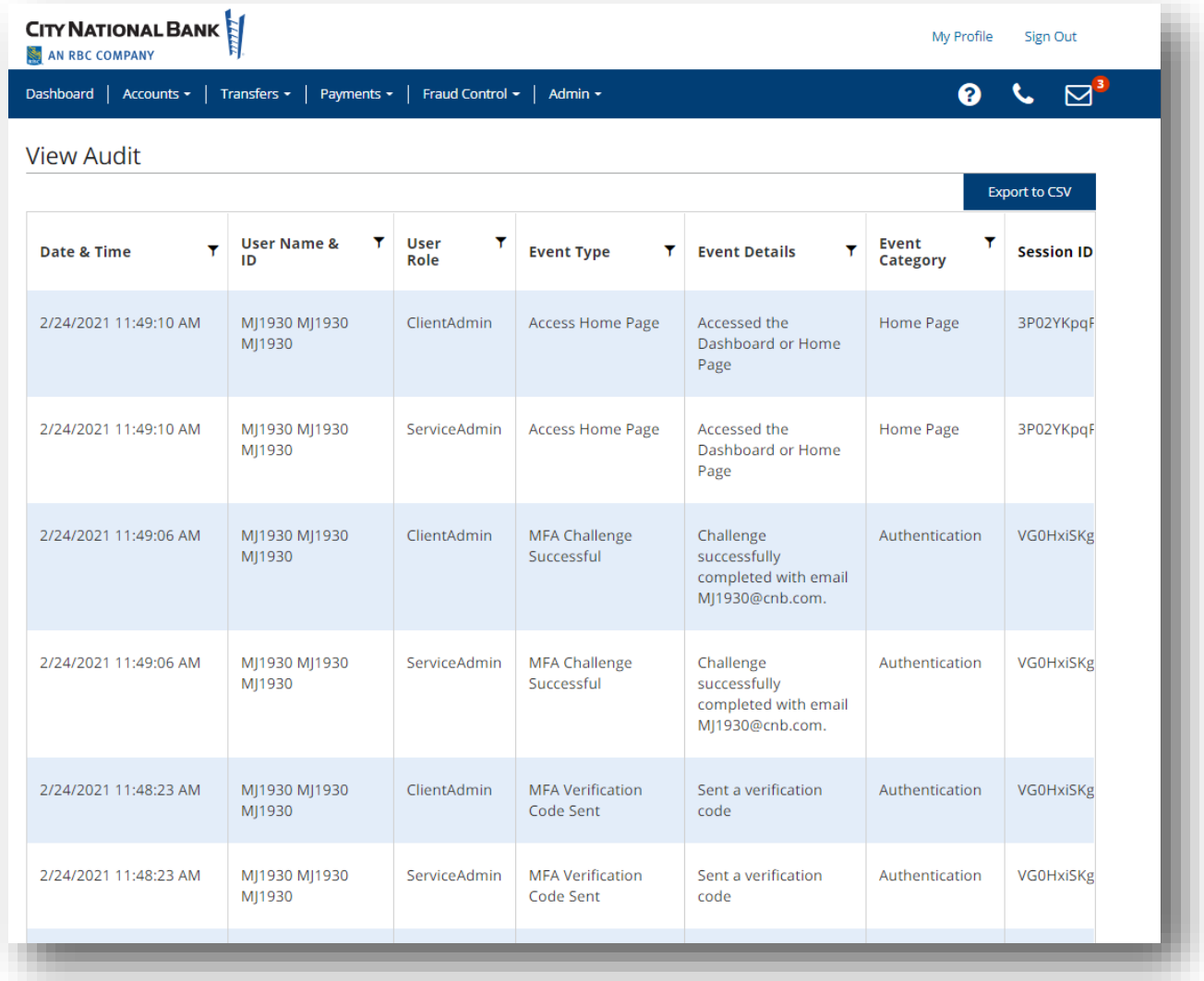
Under the Event Category and Event Type sections, select options to customize the report into more targeted results. Or, click Continue and Generate Report, to include the default setting of all fields within your report.

Results based on selections for Audit Reports

The following columns will appear on the screen, for your reference, based on the selections you selected to the prior screens. This information can either be viewed directly on the screen or exported in a CSV format file.

- Created Date & Time
- User Name & ID
- User Role

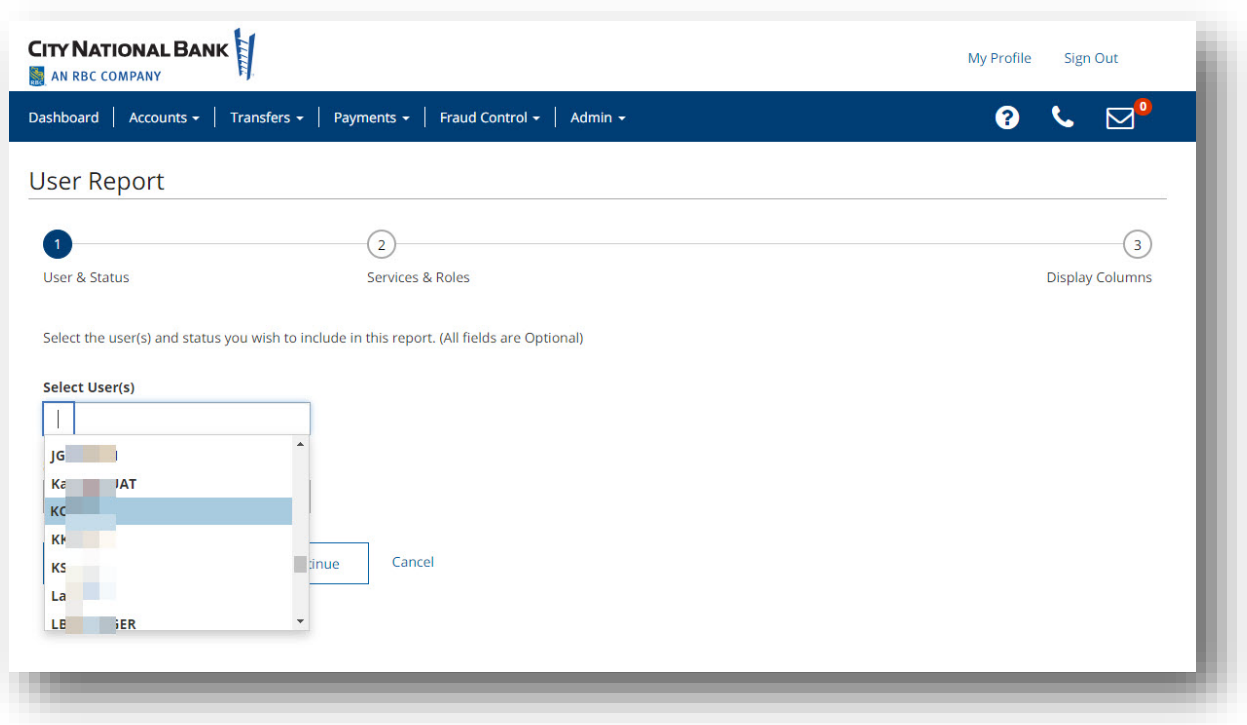
- Event Type
- Event Details
- Event Category
- Session ID
- IP Address
- Device Type & OS Version
- Browser Version



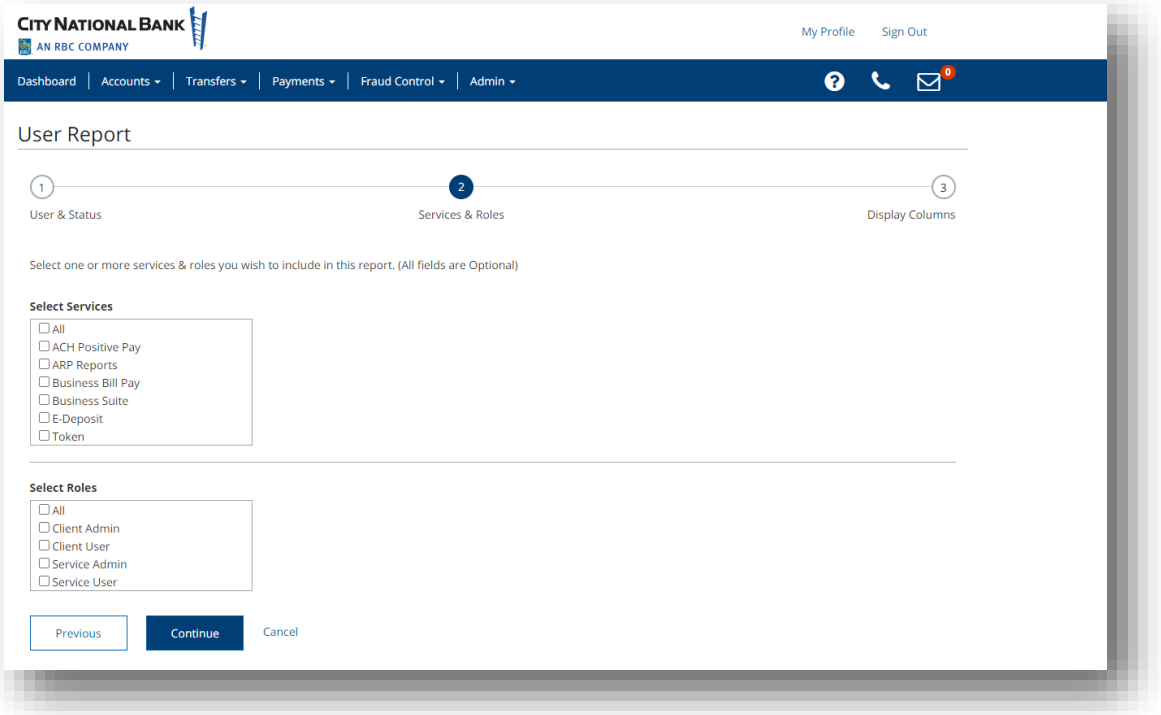
User Reporting

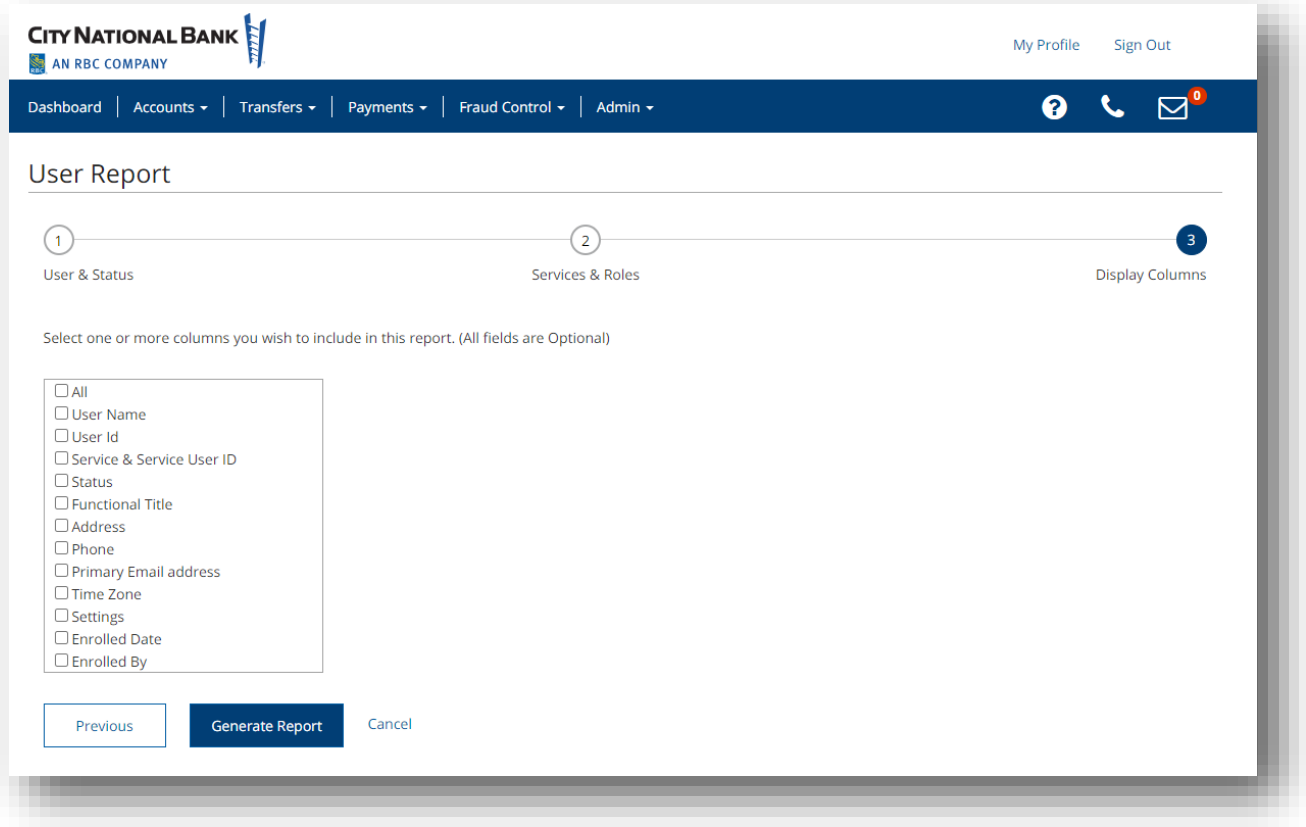
The user reporting page is divided up in three different sections:

- User & Status
- Services & Roles
- Display columns



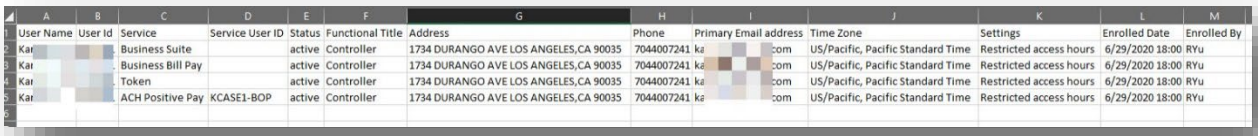
CITY NATIONAL BANK
AN RBC COMPANY





You can click on Generate Report to generate a report that provides you the following information:

- User Name
- User ID
- Status
- Functional Title
- Address
- Phone
- Primary Email
- Time Zone
- Settings
- Enrolled Date
- Enrolled By



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	User Name	User Id	Service	Service User ID	Status	Functional Title	Address	Phone	Primary Email address	Time Zone	Settings	Enrolled Date	Enrolled By
2	Kar		Business Suite		active	Controller	1734 DURANGO AVE LOS ANGELES,CA 90035	7044007241	ka com	US/Pacific, Pacific Standard Time	Restricted access hours	6/29/2020 18:00	RYu
3	Kar		Business Bill Pay		active	Controller	1734 DURANGO AVE LOS ANGELES,CA 90035	7044007241	ka com	US/Pacific, Pacific Standard Time	Restricted access hours	6/29/2020 18:00	RYu
4	Kar		Token		active	Controller	1734 DURANGO AVE LOS ANGELES,CA 90035	7044007241	ka com	US/Pacific, Pacific Standard Time	Restricted access hours	6/29/2020 18:00	RYu
5	Kar		ACH Positive Pay	KCASE1-BOP	active	Controller	1734 DURANGO AVE LOS ANGELES,CA 90035	7044007241	ka com	US/Pacific, Pacific Standard Time	Restricted access hours	6/29/2020 18:00	RYu
6													

Once the report has been generated, the user may choose to print and/or export it.

Audit Activity

The Audit Activity widget supplies a variety of information for your company, allowing you to filter the information that appears, as well as export and print it.

To perform an audit activity search:

1. Select **Audit – Activity** from the Admin menu. The Audit Activity screen will be displayed.
2. In the **Date/Time**, **Product Code**, **Function Code**, **Type Code**, **Action Mode**, **Entry Method, Description, User** and **Affected User** fields, select the type of audit records you want to search for. You can select a single field or multiple fields. For example:
   - To return all the available audit records for **ACH**, select **ACH** from the **Product Code** list.
   - To return all audit records for August 4, 2023, for Jane Smith, select:
     - 08/04/2023 from the Date/Time field.
     - **Jane Smith** from the User list.
   - To return all audit records for approved wire payments created from a template, select all of the following:
     - Wire – Payments from the Function Code list.
     - Approve from the Action Mode list.
     - Template from the Entry Method list.
3. Click **Search**. The relevant search information appears at the bottom of the screen.

Account Names

The Account Names feature is automatically available to Client Admins and provides a list of company bank accounts. From here, you can view details of each account as well as print or export the list. The Account Names feature also gives you the opportunity to change the existing account name for all the company's users, if desired.

To modify an account:

1. Select Account Names from the Admin menu.
2. Select the account you want to change, and then click **Modify**. The system displays the Bank Account Settings for the account selected.
3. Change the name in the **Company Account Name** field.
4. Click **Save**.

The new Company Account Name will now appear throughout the service for all the company's users.

Manage Alerts

The Alerts feature configures the system to automatically send alerts when certain conditions occur. For example, a Closing Available Balance alert can be sent when a day's closing account balance falls below a certain threshold, or an alert can be sent when a positive pay suspect file is received from the bank. Although you can specify the recipient directly on the alert screen, we recommend that you set up recipients or recipient groups before creating alerts.

Adding Alerts

To add an alert:

1. Select **Alerts** from the Admin menu. Alerts are available to all Client Admins and any user who has been given permission for alerts. The **Alerts Center** screen appears. The Alerts Center allows you to:
   - Create and manage alerts.
   - Add new recipients for these alerts.
2. Click the Alerts tab in the Alerts Center, then click add New Alert.
3. In the **Alert Name** field, enter a name for the alert.

4. From the **Alert Type** list, select the appropriate group for this alert: for example, *Payments and Transfers*.
5. In the **Alert** field, select the type. For example, if you chose the Payments alert type, you might choose *Payment & Transfers Processed* as the alert.
6. In the **Alert Subject Line** field, a sample subject line appears based on the alert type you have chosen. If you would like to use a different subject line, write the desired information in the field. This is the subject line that will appear on the email notification sent to the recipient.
7. From the **Recipient** list, enter or select a recipient or recipient group.
8. In the **Contact Methods** section, check the checkboxes for the appropriate contact method or methods. Check the **All** box for each contact method to have the alert sent through all contact methods.
9. When you have entered all the necessary fields, click **Save**.

Now, when the criteria specified in the alert are met, the recipient will be contacted using the specified method.

Deleting or Modifying the Alert

Once created, an alert can be modified or deleted by selecting such options from the Action drop-down for each alert. Alternatively, you can delete multiple alerts at once by selecting multiple alerts and selecting the Delete button at the bottom of the page.

Adding an Alert Recipient

To add an alert recipient:

1. Select **Alerts** from the Admin menu. The Alert Center screen will be displayed. Click the Recipients tab in the Alert Center.
2. Scroll to the Recipients list and click **Add**.
3. Enter the recipient's name and email address.
4. If you want to add a different method of contact for this recipient, click Add **Another Contact Method**.
5. Use the drop-down to select a contact method.
6. Enter the secondary contact information.
    - If you are entering a phone number, note that you can also enter an extension and pause indicator: for example, a **9** when dialing out of a business office. In addition, check the appropriate checkbox indicating whether the contact should be sent a voice or text message.

- The value entered in the **Contact Method Name/Alias** field will be displayed on the alert creation screen.

7. To add another contact method, repeat steps 3 through 5.
8. Click **Save**.

Add Alerts Recipient Group

To add a recipient group:

1. From the Alerts Center, click the **Recipients** tab. The Alert Recipients screen will be displayed. Scroll to the Recipient Groups list and click **Add**. The system displays the Recipient Group Settings screen.
2. Enter a name for the recipient group in the **Name** field.
3. Click **Save**.

Add Alerts Recipient Group Assignment

To add a recipient to a recipient group:

1. From the Alerts Center, click the **Recipients** tab. The Alert Recipients screen displays.
2. Scroll to the Recipient Group Assignments list and click **Add**.
3. Select the desired recipient group from the **Group Name** drop-down list.
4. Select the recipient from the **Recipient Name** drop-down list.
5. Click **Save**.

Manage Imports

Import Files

The Import Files feature displays a list of imported files, one file to a row. Each file is identified by file name, date of import, import type and job ID.

To view file import history:

1. Select **Import Files** from the Admin menu. The Import Files screen will be displayed and will list all imported files.

2. Scroll to the right to see a listing of the number of items successfully created from the imported file, as well as the number of rejected items and errors associated with the import.

To view file import details:

1. Select **View** from the **Actions** drop-down list or drill down on one of the items in the list. A table corresponding to the item type is displayed. It lists pertinent details about the import, including explanatory comments on any errors that occurred during import.
2. The detail screen will display both failed records and successful imports. Click the right arrow to see details of either type.

Note: The **Import Files** list and **File Import Details** can be exported or printed, if desired, by clicking on the appropriate icon for each.

Import Maps

This feature allows you to create custom import maps that can be used to import data from your systems. This tool provides you with the ability to define the file layout, field mapping and rules for importing files. Import maps are typically used in lieu of standard bank file formats.

Note: The following instructions outline the steps for creating an import map. The fields you see in the window will be different depending on the map and payment type you choose.

To add an import map:

1. Select **Import Maps** from the Admin menu. The Import Maps screen will be displayed.
2. Click Add Import Map.
3. Select the **Map Type** from the drop-down list. The map type represents the file format of the files that you will import.
    - Select **Delimited** if imported files will use a delimiter, such as a comma, semicolon, or other indicator to separate the records.
    - Select **Fixed** if the imported files will be fixed-width text files.
    - Select **NACHA** if the imported files are in NACHA format.
4. Select the payment type that you are creating a map for.

5. If necessary, use the **Import As** drop-down to choose whether files should be imported as payments or templates.
6. If necessary, select a clearing method (applies to ACH Payments only).
7. If the payment type requires additional details, an additional section will appear beneath the **Clearing Method** field. For example, the child support payment type requires the selection of a child support agency. Use the drop-down menu to make your selection.

Additional fields will appear for the payment type you selected. Note that the fields are different depending on the payment type and map type you select.

8. In the **Format Name** field, enter a name for the import map.
9. In the **Description** field, enter a description for the import map.
10. For batch payment types, the **File Process** field is used to indicate how records will be processed. This field does not appear for single-beneficiary payment types. Select the appropriate process.
    - **Append All –** This setting will add all transactions in the file to the batch.
    - **Append New –** This setting will compare the records in the file with the transactions already in the batch. Transaction details that exist in the file that do not already exist in the batch will be added.
    - **Match and Update –** This setting will compare the records in the file with the transactions already entered in the batch. The matching transactions will be updated with the data from matching records in the file.
    - **Replace All –** This setting will replace all the transaction details in the batch with the details in the file.
11. For batch payment types, in the **Match Failure** field, choose how you would like to handle records from the file that cannot be matched to an existing transaction in the batch. This setting is only applicable if you select **Append New** or **Match and Update** in the **File Process** field.
    - **Append to Batch –** Choose this setting to add records to the batch if they cannot be matched to an existing record.
    - **Fail Record –** Choose this setting to fail any records that cannot be matched. The file will continue processing.
    - **Fail File –** Choose this setting if the entire file should fail if any records cannot be matched.
12. In the **Start Import at Row** field, choose the row in the file that the import should start at. For example, if your import file contains three rows of header data, and the records start at row 4, enter **4** in the field. Note that this field does not appear for a NACHA map type.

13. In the **String Delimiter** field, select the delimiter used to indicate a string in the file. The default section is “Double Quote.” Note that this field is not visible for map types of fixed or NACHA.
14. In the **Field Delimiter** field, select the delimiter used to indicate the end of a field in the file. The default selection is “Comma.” Note that this field is not visible for map types of fixed or NACHA.
15. In the **Record Delimiter** field, select the delimiter used to indicate the end of a record in the file. The default selection is **[CR] [LF]**, which corresponds to carriage return or line feed. Note that this field is not visible for single-beneficiary or NACHA map types.
16. In the **Date Format** field, select the date format used in the file. The default selection is **MMDDYY**.
17. In the **Date Separator** field, if needed, choose how dates are separated.
18. The **Implied Number of Positions** field is an optional field that can be used to designate the implied number of decimals in a numeric value in the file. For example, you would choose 3 if the number 1000000 should be interpreted as 1000.000. If a decimal separator is defined below, you can leave this field blank.
19. In the **Decimal Separator** field, enter the character used to indicate a decimal in the file.
20. The values shown in the **Credit**, **Checking**, **Debit**, **Savings**, **Yes/True**, **No/False**, **General Ledger**, **Loan Account**, **Issue**, **Void**, **Header Indicator**, **Body Indicator** and **Trailer Indicator** fields are the abbreviations used to represent these values in the file. These fields are case sensitive. If needed, you can change the default values.
21. The table at the bottom of the screen is used to indicate how the fields in your file map to fields in the applicable screen in the application.

An explanation of the fields in the table is included below.

- **Active –** A check mark in this field indicates that a field in the file should either be imported or matched against existing data in the application.
- **Field Name –** The name of the field in the application. The values in this column vary by payment type.
- **Field Number –** For delimited map types, indicates which field in the file maps to a field on the application screen.
- **Start Position –** For fixed map types, indicates the starting point of the field (in characters, measured from the start of the file).
- **End Position –** For fixed map types, indicates the ending point of the field (in characters, measured from the start of the file).

- **Match –** Check the checkbox if the value in the file should be matched against the value in the application. This column is only used for batch payment types and when the file process is *Match and Update* or *Append New*.
- **Default Value –** Used to indicate the default if a value is not supplied in the file.

22. Complete the screen as appropriate. Once you have finished entering the values for the import map, click **Save**.

Appendix A: Alert Types

Service	Alert Type	Description
Administration	Beneficiary Address Book Maintenance	Email is generated when changes are made to and/or approved for Contact Center/ Beneficiary Address Book records.
Check Management	Positive Pay Cutoff Time Is Approaching	If a positive pay item requires a decision, an alert email is generated stating that a cutoff time is approaching in X number of minutes.
	Positive Pay Decision Pending Approval	Alert email is generated when a positive pay decision is ready to be approved.
	Positive Pay No Suspect Items	Alert email is generated when there are *no* suspect items for the selected accounts.
	Positive Pay Suspect Item Alert	Alert email is generated when a positive pay suspect file is received.

Service	Alert Type	Description
	File Import Confirmation For Check Issues and Voids	Alert notifies user when a file of check issues or voids have been successfully imported to Business Suite.
	Transactions Processing Status Changed For Issues and Voids	Alert notifies user of each status change for the file uploaded, i.e., changes from “submitted” to “approved” and several other.
Balances and Transactions	Balance/Amount Threshold	Email is generated when an account balance meets the specified criteria.
	Transaction Notification	Email is generated when a transaction is posted and clears that meets specified criteria
	Wire Activity	Email is generated in real time for incoming and outgoing posted wires.
Payments	Approver Rejected Payments	Notifies you of any payments rejected during the approval process.

Service	Alert Type	Description
	Payments Automatically Generated	Notifies you of payments automatically created based on scheduled payment settings.
	Payment Processed	Email is generated if a payment is received by the bank, confirmed by the bank, or rejected by the bank.
	Payments Awaiting Approval	Email is generated when a payment is awaiting approval.
	Payments Rejected Today	Email is generated when a payment is rejected.
	Payment Cutoff Time Warning	Warning of a payment that has been submitted but still requires approvals or other actions to meet the payment cutoff time.
	File Import confirmation For Payments and Transfers	When you import a file of payment transactions to be processed, this alert notifies you when you when the import has successfully completed.

Service	Alert Type	Description
	Transactions Processed Status Changed for Payments and Transfers	This alert tells users when a submitted payment or transfer has had a status changed. This includes an email when a transaction has been approved, or when it has been processed.

Appendix B: Administration Quick Reference Guide

The Administration function allows management of users as follows:

- Enter basic user details for the profile and settings information.
- Assign services to the user and/or grant access to perform administrative permissions.
- Grant functional and account permissions for the services:
    - Features and functions, including payments, reporting, fraud control, administrative, and alert functions.
    - Bank accounts that the user will have access to.
    - Approval limits that cover transactions the user works with.

Create New User

1. Select **Users** from the Admin menu.
2. On the Manage Users page, click **Create User**.
3. The Create User page will display.
4. In the **User ID** section, create a unique user ID for the user.
    - Use only letters and numbers. Minimum 3 characters and maximum 20 characters long.
4. Enter user's first name and last name in the **First Name**/**Last Name** fields.
5. Enter user's **Phone Number** and **Phone type** in appropriate fields. To add additional phone numbers, click **Add Phone Number**.
6. Enter user's email in the **Email Address** field.
7. (optional) Select a prefix for the user in the **Prefix** field.
8. (optional) Select a time zone for the user in the **Time Zone** field.
9. (optional) Select a Functional Title for the user in the **Functional Title** field.
10. In **Settings** you can add restrictions for the user's profile:
    - Restrict Access limiting a user's access hours to the days/times they should be accessing the system.
    - Restrict User from Sending Messages Directly to the Bank
11. Click Continue to proceed to Assign Services.

Assign Services

1. Check the box next to each service you wish to grant the user.
2. To provide the user with administrative permissions, click **Manage Administrative Permissions**. Check the box for the permissions you want to assign to the service (**Select All** check box, if desired).
3. Click **Save** to return to the previous screen.
4. Click **Next** to move to the step in the workflow to assign **Service Permissions**.

Assigning Alerts Entitlements

The **Alerts** tab allows you to grant permission to alerts.

1. To entitle the user to all alerts, check the **Select All** checkbox.
2. OR, select the checkbox(es) for the alerts you want to grant access to.

Assigning Administration Entitlements

The **Administration** tab allows you to grant access to administrative functions on the client application.

Assigning Reporting Entitlements

1. To entitle the user to all areas of administration, check **Select All** box.
2. OR select the checkbox(es) for the permissions you want to grant. Example: To allow the user to view users but not manage or approve them, click *only* the **View** check box next to **User Administration**.

Assigning Reporting Entitlements

The **Reporting** tab allows you to grant permission to access balance and transaction data (i.e., Balance and Transaction reports, Statements, Payment Reports, Checks and Stops Inquiry, and Image Search).

To assign reporting entitlements:

1. To entitle the user to all available reports, check the **Select All** box.
2. ALTERNATIVELY, select the individual checkbox(es) for the reports (for example, Balance & Transactions) that you would like to entitle the user to.
3. For each report group, you can choose to entitle all reports or individual reports by checking the appropriate boxes.