

Accessing Administration Functions

To work with System Manager features:

1. Click the **Administration** hyperlink, in the upper right-hand corner of the system window. The Administration tabs are displayed.
2. Click the appropriate tab. Submenus are displayed.
3. Click a submenu item to access the feature.

Setting Account Permissions

System managers can grant access permissions to users for specific accounts. These permissions can be given to a user separately for each module in the system, or can be given to a user for all modules.

To assign user access to accounts:

1. From the **Administration** tabs and submenus, click **User Setup**, then **Account Permissions**.
2. From the **User** drop-down list, select the ID of the user to whom account access is to be assigned.

Note: Log-on names are associated with a user's record only after the user performs the first-time sign-on procedure.

The **Application** drop-down list is displayed.

3. Select an application (module) for which permissions are to be assigned. Do one of the following:
 - Select a specific application
From the **Application** drop-down list, select an application name.
 - Select all applications
From the **Application** drop-down list, select **All Applications**.
Accounts available for the application(s) you selected are displayed. The application names are in the left-hand column, and the account numbers, each with their own checkbox, are in the right-hand column.
4. Select the checkbox associated with each account for which permissions are to be granted.

[Optional] Click the **Check All** button to select all checkboxes, or click the **Clear All** button to deselect all checkboxes.

5. Click the **Submit** button. A confirmation message is displayed when your selections have been processed.

Setting Account Names

System managers can set names for accounts. Where the functionality is available in the system, these account names will be displayed in parentheses next to the account numbers (in drop-down lists, for example). Additionally, where available, the account's name is displayed when the user moves the cursor over an account number.

To set or change an account name:

1. From the **Administration** tabs and submenus, click **User Setup**, then **Account Names**. Accounts and the fields used to name them are displayed.
2. In the **Name** fields associated with account numbers, enter the names to be assigned.
3. Click the **Submit** button to save your selection. A confirmation message is displayed.

Account Targets

The Account Targets feature provides feedback to users on how account year-to-date and/or month-to-date average balances compare to a target amount that you specify. You can specify YTD and MTD target balances, and a percentage of permissible variance from that target balance.

To set account targets:

1. Do one of the following:
 - From the Account Targets report
In the **Action** column, click the **modify** hyperlink associated with the account for which targets are to be modified. The Account Targets pane is displayed.
 - From anywhere else in the application
From the **Administration** tabs and submenus, click **Accounts**, then **Account Targets**.
2. If the account to be modified is not already selected, select it from the **Account** drop-down list.
3. In the **MTD Target** and **YTD Target** fields, enter the month-to-date target and/or the year-to-date target.
4. In the **Notification Level** field, enter the acceptable variance as a percentage. Enter only numbers.
5. Select either the **Above** or the **Below** radio button to indicate whether notification should be given to the user if the average balance exceeds or falls short of the target.
6. Click the **Submit** button. A confirmation message is displayed when processing is complete.

System Administration (Cont'd)

Setting Password Retention Period

System managers assigned the appropriate permissions can set the expiration period for all users at their company site.

To set the password retention period:

1. From the **Administration** tabs and submenus, click **Security**, then **Security**.
2. In the **Password Expiration Days** field, enter a number of days.
3. Click the **Submit** button. A confirmation message is displayed.

Account Groups

On the Account Summary report, the Account Groups feature provides the ability to view subtotal information for each group. This information is in addition to the totals information that is already presented for all accounts.

On the Account Targets report, the feature arranges the displayed accounts by group, but does not provide subtotal information.

To organize accounts into groups:

1. From the **Administration** tabs and submenus, click **Accounts**, then **Account Groups**.
2. Do any or all of the following:
 - Create a new group
 1. Click the **Add New** button. A pop-up window is displayed.
 2. In the **Group Name** field, enter a name for the group.
 3. Select the checkboxes associated with the accounts to be added to the group.
 4. Click the **Submit** button. The pop-up window closes, and the new account group is added to the **Groups** list.
 - Modify an existing group
 1. In the **Groups** list, click the name of the group to be modified. Member accounts are displayed on the right-hand side of the screen.
 2. Do either or both of the following:
 - Select the checkboxes associated with the accounts to be added to the group.
 - Deselect the checkboxes associated with the accounts to be removed from the group.
 3. Click the **Submit** button. A confirmation message is displayed.
 - Delete a group
 1. In the **Groups** list, click the name of the group to be deleted.
 2. Click the **Delete Group** button. The group is deleted; the accounts themselves are unaffected.

On the Account Summary report, accounts are arranged into the groups you have configured, with subtotals for each group displaying beneath the last member of the group in each column of the report.

Wire Transfer Administration

The System Manager can authorize individual Wire Transfer users to use one or more templates to create transactions. (Templates can be assigned to a user only if a System Manager has validated the user to use the account with the Wire Transfers module.)

For each type of wire transfer, the System Manager can also set the following limits on each user:

- **Per-Transaction Limit:** Limits maximum value of any wire transfer created in the system.
- **Daily Limit:** Limits maximum value of all wire transfers created in the system each day.
- **Number of Approvals:** Specifies the number of approvals required for both wire transfer transactions and templates.
- **Item Amount Approval Limit:** Limits maximum value of individual transactions the user may approve.

To set wire transfer permissions:

1. From the **Administration** tabs and submenus, click **User Setup**, then **Wire Transfers**.
2. In the **Users** list, click the User ID/log-on name of the user for whom permissions are to be set.
3. Make the necessary setting changes.
4. Click the **Update** button to save the changes. A confirmation message is displayed.
5. Click **OK**.

Note: System Managers may modify their own settings only if ViewPoint Bank has assigned them permissions to do so.

ACH Administration

For each ACH user, the System Manager can set:

- **Included/Excluded Groups:** Limits the template groups to which each user has access.
- **Daily Submission Limit:** Limits the maximum value of any single transaction created in the system.
- **Per-Transaction Submission Limit:** Limits the maximum value of all transactions created in a single batch.
- **Per-Batch Submission Limit:** Limits the maximum value of all transactions submitted in a single batch.

To set ACH limits:

1. From the **Administration** tabs and submenus, click **User Setup**, then **ACH Origination**.
2. In the **Users** list, click the User ID/log-on name of the user for whom permissions are to be set.
3. Make the necessary setting changes.
4. Click the **Update** button to save your changes.
5. Click **OK**.

Note: System Managers may modify their own settings only if the financial institution has assigned them permissions to do so.

System Administration (Cont'd)

Managing Remote Deposit User Settings

For each Remote Deposit user, the System Manager can set:

- **Per-Item Approval Limit:** Limits the maximum value of any single check that a user can approve.
- **Per-Item Submission Limit:** Limits the maximum value of any single deposit ticket that a user can submit in a single day.
- **Per-Deposit Approval Limit:** Limits the maximum value of any single "deposit ticket" that a user can approve.
- **Per-Deposit Submission Limit:** Limits the maximum value of any single "deposit ticket" that a user can submit in a single day.

Additionally, System Managers can allow a user to:

- See items scanned by others.
- Submit deposits without requiring an approval.
- Approve their own deposits.

To set Remote Deposit limits:

1. From the **Administration** tabs and submenus, click **User Setup**, then **Remote Deposit**.
2. In the **Users** list, click the User ID/log-on name of the user for whom permissions are to be set.
3. Make the necessary setting changes.
4. Click the **Update** button to save the changes. A confirmation message is displayed.
5. Click **OK**.

Note: System Managers may modify their own settings only if the financial institution has assigned them permissions to do so.

Managing the Remote Deposit Location List

To simplify deposit tracking, the Remote Deposit module allows the user to associate a transaction batch with an administrator-specified location ID. These IDs must be set up in advance, either by ViewPoint Bank or by the corporate System Manager. Once IDs have been set up, the System Manager assigns users the location IDs with which their deposits will be identified.

Note: If a user has been set up to use location IDs, that user must be assigned one or more location IDs or that user will be unable to use the Remote Deposit module.

In the system, **Location ID** refers to a location's "plain text" identifier, while **Location Code** refers to a unique number assigned to that location. Location ID is used throughout the Remote Deposit module to identify locations.

To manage the location ID list:

1. From the **Administration** tabs and submenus, click **Miscellaneous Setup**, then **Location List**.
2. Do either or both of the following:
 - Add a location
 1. In the **Location ID** field, enter a name for the location. Enter up to 20 alphanumeric characters.
 2. In the **Location Code** field, enter a code for the location. Enter up to 15 characters valid for MICR entries (0-9, "-", and "/").
 3. Click the **Add** button. The location is added to the list.
 - Remove a location
 1. Select the checkbox associated with the location to be removed, or select the checkbox in the header row to select all locations.
 2. Click the **Delete** button. The selected locations are removed from the list.

Managing Remote Deposit Location Permissions

Use the Location Permissions feature to allow users to access location IDs when creating Remote Deposit transaction batches.

To manage location ID permissions:

1. From the **Administration** tabs and submenus, click **User Setup**, then **Location Permissions**.
2. From the **Users** list, select a user.
3. Select the checkboxes associated with the location IDs to be made available to the user.
4. Click the **Update** button. Your changes are saved.

System Administration (Cont'd)

Managing Remote Deposit Endorsement Settings

The Endorsement feature superimposes an endorsement message on the images created from the backs of scanned checks. By marking the permanent record (the electronic version) of the check with this endorsement message, this feature saves users the effort of manually stamping check backs before scanning.

Endorsement messages are placed on the check image when the deposit is saved, and thus will not be visible while the user is scanning checks.

System Managers permitted to administer Remote Deposit settings and validated for access to a particular account may enable Endorsement images for checks scanned for deposit into that account.

To enable Endorsement messages for an account:

1. From the **Administration** tabs and submenus, click **User Setup**, then **Remote Deposit**.
2. At the bottom of the left-hand frame, click the **Virtual Endorsement** button. Accounts validated for Remote Deposit are displayed in the Accounts listbox.
3. Click an account number/name in the **Accounts** listbox. Options are displayed in the right-hand frame.
4. Select the **Enable Virtual Endorsement** checkbox.
5. Click the **Update** button to save your changes.

Note: To return to the Remote Deposit tab's user-limits functionality, either select the **Remote Deposit** tab, or click the **Users** button in the left-hand frame.

Reviewing Users' Multi-Factor Authentication Registration Status

Once a site is configured for Multi-Factor Authentication, System Managers can use the MFA Registration Status report to check the registration status of users at that site.

To access the MFA Registration Status report:

1. From the **Administration** tabs and submenus, click **Security**, then **Reporting**.
2. From the drop-down list at the top of the pane, select **MFA Registration Status**. If this is the only option available, it will be selected for you.
3. [Optional] From the **MFA Login Option** drop-down list, make a selection to filter the user list.

Administering Multi-Factor Authentication Tokens

System Managers validated for MFA token administration can decouple tokens from user profiles, in the event of lost tokens or departed employees. Once decoupled from a user profile, the token may be given to another user and registered as if new.

To de-link a token from a user profile:

1. Access the Multi-Factor Authentication report, as described in the "Reviewing Users' Multi-Factor Authentication Registration Status" section.
2. Click the **delink** hyperlink associated with the user profile whose token is to be de-linked. A confirmation dialog box is displayed.
3. Click the **OK** button. The token is de-linked, and a confirmation dialog box is displayed.
4. Click the **OK** button.

Viewing Tokens Registered to Your Company's Users

The Active MFA Token report identifies the tokens registered to users at your company site.

To access the Active MFA Token report:

1. From the **Administration** tabs and submenus, click **Security**, then **Reporting**.
2. From the drop-down list at the top of the pane, select **Active MFA Token**. The Active MFA Token pane is displayed.

Using the User Audit Report

The User Audit Report displays system activity for your company site's system users. 63 days of Audit history are available.

To access the User Audit Report:

1. From the **Administration** tabs and submenus, click **Security**, then **User Audit**. The User Audit criteria screen is displayed.
2. From the **User ID** drop-down list, select an individual user by user name/ID, or accept the default selection of **All**.
3. From the **Activity Type** drop-down list, do one of the following:
 - To view system activity such as user logon, use of modules, etc.
 1. Select **Routine User Activity**.
 2. From the **Category** drop-down list, select the module or functionality for which activity is to be tracked.
 - To view administrative activity such as user setup or PIC letter resets
Select **Administrative Activity**.
4. In the **From Date** and **To Date** fields, enter start and end dates for the search. Use mm/dd/yyyy format.
5. Click the **Submit** button. Audit information is displayed beneath the parameters pane.

System Administration: User Profiles

[Contact Us](#) | [Preferences](#) | [Administration](#) | [Sign Out](#)

Accessing the User Setup Utility

To access the User Setup utility:

1. Click the **Administration** hyperlink in the top right-hand corner of the application window. The Administration tabs are displayed.
2. Click the **User Setup** tab. The Security submenu is displayed beneath the tab.
3. Click the **User Setup** submenu item.

Adding a User Profile

Important: Once you have created a user profile, you must assign account access to the user in order for the user to access the system.

To create a user profile:

1. Access the User Setup feature.
2. Click the **Create** button, located beneath the Users pane. The Create New User pane is displayed.
3. In the **User ID** field, accept the generated ID or enter a unique four-character ID for the user. This ID identifies the user to the server.
4. In the **User Name** fields, enter the user's first name, middle initial, and last name.

Note: User names are displayed on the Users pane after the user generates a permanent log-on ID during first-time log-on.

5. Select the checkboxes corresponding to the services the user will be permitted to access (the "user validations").
6. *[Optional]* Click the **Auto-account Permission** checkbox to automatically assign access to accounts validated for features to which the user will be given access.
Note: Selection of this checkbox is valid only during the current operation; if you later modify the user profile, the checkbox will be de-selected.
7. Click the **Create** button. The user is added to the system, and the Users pane is displayed.

Modifying a User Profile

To modify a user profile:

1. Access the User Setup feature.
2. In the **Action** column, click the **modify** hyperlink associated with the user profile to be modified. The Modify User pane is displayed.

Note: You may not modify your own user profile or the user profile of any other system manager. If a user is a system manager, a **Y** is displayed in the **Sys Mgr** column of the Users pane in that user's row, and no **modify** hyperlink is available for the user.

3. Make the necessary changes in the **User Name** fields and select or deselect checkboxes to assign or remove validations to/from the user profile.
4. *[Optional]* Click the **Auto-account Permission** checkbox to automatically assign access to accounts validated for features to which the user will be given access.

Note: Selection of this checkbox is valid only during the current operation; if you later modify the user profile, the checkbox will be de-selected.

5. Click the **Update** button. A confirmation message is displayed.
6. Click the **Return to List** button to return to the Users pane.

Regenerating PIC Letters for Forgotten User Names

If a user has forgotten their user name, you can generate a new PIC letter to allow the user to access the system using the first-time log-on procedures. The user will need to create a new permanent user name. For security purposes, system managers may not regenerate PIC letters for other system managers.

Note: This feature is not intended to address forgotten passwords or "locked" status due to multiple unsuccessful log-on attempts or a user who has closed the browser window without logging off. For help with these issues, please contact the Customer Service Center.

To regenerate a user's PIC letters:

1. Access the User Setup feature.
2. In the **Action** column, click a **modify** hyperlink associated with the user whose PIC letters are to be regenerated. The Modify User pane is displayed.
3. Click the **Regenerate PIC** button. The PIC-letter regeneration is confirmed, and the Users pane is displayed.

Deleting a User Profile

To delete a user profile:

1. Access the User Setup feature.
2. In the **Action** column, click the **delete** hyperlink associated with the user profile to be modified. A confirmation dialog box is displayed.
3. Click the **OK** button. The list of user profiles is refreshed, and a confirmation message is displayed.

[Optional] Click the **Cancel** button to discard the deletion request.



ViewPoint Bank.
ePoint Business

