

## SETTING ACCOUNT NAMES (SYSTEM MANAGERS)

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 name is displayed when you move the cursor over its account number, or in columns beside its account number.

### To set or change an account name:

1. From the **ADMINISTRATION** menu, select **APPLICATIONS**. The Administration screen is displayed.
2. On the Administration screen, select the **ACCOUNT NAMES** tab.
3. In an account number's **NAME** field, enter the account name to be assigned.
4. Click the **SUBMIT** button to save your selection. A confirmation message is displayed.

## SETTING PASSWORD RETENTION PERIOD (SYSTEM MANAGERS)

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

### To set the password expiration period:

1. From the **ADMINISTRATION** menu, select **APPLICATIONS**. The Administration screen is displayed.
2. On the **ADMINISTRATION** screen, select the **SECURITY** tab.
3. In the **PASSWORD EXPIRATION DAYS** field, enter a number of days.
4. Click the **SUBMIT** button. A confirmation message is displayed, and the setting is updated.  
*[OPTIONAL]* Click the **DEFAULT** button to set the expiration period to the system default.  
*Note: If you click the **DEFAULT** button, you must click the **Submit** button to save the change.*

## ADD A USER PROFILE

You can create entirely new user profiles, or you can base a new user profile upon an existing profile that does not have system manager privileges assigned to it.

*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. From the **ADMINISTRATION** menu, select **APPLICATIONS**. The Administration screen is displayed.
2. Select the **USER SETUP** tab.
3. Click the **CREATE** button, located beneath the Users pane. The Create New User pane is displayed.

4. 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.
5. 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.*

6. Select the checkboxes corresponding to the services the user will be permitted to access (the "user validations"). See the "Validations List" section of this document for information on the validations that may be available for selection.
7. Click the **ADD USER** button. The user is added to the system, and the **USERS** pane is displayed.

### To base a user profile on an existing profile:

1. From the **ADMINISTRATION** menu, select **APPLICATIONS**. The Administration screen is displayed.
2. Select the **USER SETUP** tab.
3. Click the **VIEW** hyperlink associated with the user profile upon which the new profile is to be based. The View User pane is displayed.
4. In the **User ID** field, enter a unique four-character ID for the user. This ID identifies the user to the server.
5. 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.*
6. Click the **ADD USER** button. The user is added to the system, and the Users pane is displayed.  
*Note: The **ADD USER** button is displayed only in association with user profiles that do not have system manager privileges.*
7. Modify the new user profile to customize the services the user will be permitted to access.

## MODIFY A USER PROFILE

### To modify a user profile:

1. From the **ADMINISTRATION** menu, select **APPLICATIONS**. The Administration screen is displayed.
2. Select the **USER SETUP** tab.
3. 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.*

4. Make the necessary changes in the USER NAME fields and select or deselect checkboxes to assign or remove validations to/from the user profile. See the "Validations List" section of this document for information on the validations that may be available for selection.
5. Click the UPDATE button. A confirmation message is displayed.
6. Click the RETURN TO LIST button to return to the Users pane.

### REGENERATE PIC LETTERS FOR FORGOTTEN USER NAMES

If a user name has been forgotten, 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. From the ADMINISTRATION menu, select APPLICATIONS. The Administration screen is displayed.
2. Select the USER SETUP tab.
3. 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.
4. Click the REGENERATE PIC button. The PIC-letter regeneration is confirmed, and the Users pane is displayed.

### DELETE A USER PROFILE

To delete a user profile:

1. From the ADMINISTRATION menu, select APPLICATIONS. The Administration screen is displayed.
2. Select the USER SETUP tab.
3. In the ACTION column, click the DELETE hyperlink associated with the user profile to be modified. A confirmation dialog box is displayed.
4. 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.

### VALIDATIONS LIST

When adding or modifying a user profile, refer to the following

list of user validations when selecting validations to assign services to the user.

*Note: Some of the features described below may not be available to your company or may be available to your company with different names, based on settings instituted by First Federal Bank of California and your agreement with First Federal Bank of California.*

Select this User Validation...	To enable the user to...
BANK ACCT RPT	Access balance and transaction reporting. Reporting is prior day, with optional features of current day, controlled disbursement, and multi-bank reporting depending upon the features available to your company.
RESTRICTED ACCT ACCESS	Access accounts validated as "restricted."
STOP COMPOSE	Access the Stop Payment module and the ability to create, modify, submit, and report on stop payments.
CONTROLLED DISBURSEMENT	Access controlled disbursement reporting. This option should only be chosen if the bank requires and downloads a daily account file for controlled disbursement accounts. If the bank does not download a daily account file, the function is included as a part of the Bank Account Reporting module.
WIRE TRAN COMPOSE	Create, modify, and report on wire transactions. Only users who are validated for WIRE TRAN COMPOSE and WIRE TEMPLATE CREATE can create transactions without using templates, or create a template and transaction together. Users who are creating wire transactions based on templates need not be validated for WIRE TRAN COMPOSE.
WIRE TRAN APPROVE	Approve wire templates and transactions created by another user.
WIRE TRAN DELETE	Delete wire templates and transactions.
WIRE TRAN SUBMIT	Submit wire templates and transactions.
WIRE TEMPLATE CREATE	Create and modify wire templates.
IFT A/M/D	Create, modify, delete, and report on internal funds transfers.
IFT SUBMIT	Submit internal funds transfers.
CC&D COMPOSE	Create Cash Concentration & Disbursement (CC&D) transactions.

## SETTING ACCOUNT NAMES (SYSTEM MANAGERS) *cont'd*

Select this User Validation...	To enable the user to...
CC&D REPORT ACCESS	View CC&D reports.
CC&D CREATE LOCATION ID	Create CC&D Location IDs.
ACH PAYROLL	Create, modify, and delete ACH payroll templates and transactions. This validation is used in conjunction with the ACH COMPOSE TRAN and ACH CREATE TEMPLATE validations.
ACH CORPORATE	Create, modify, and delete ACH corporate templates and transactions. This validation is used in conjunction with the ACH COMPOSE TRAN and ACH CREATE TEMPLATE validations.
ACH CONSUMER	Create, modify, and delete ACH consumer templates and transactions. This validation is used in conjunction with the ACH COMPOSE TRAN and ACH CREATE TEMPLATE validations.
ACH COMPOSE TRAN	Create ACH transactions.
ACH APPROVE	Approve ACH transactions created by another user.
ACH SUBMIT	Submit ACH transactions for processing.
ACH REPORT ACCESS	ACCESS View the ACH Activity report. <i>Note: This validation does not enable reporting on NACHA pass-thru batches. Enable the ACH PASS-THRU REPORT validation to enable pass-thru reporting.</i>
ACH CREATE TEMPLATE	Create ACH templates.
ACH IMPORT	Import ACH transaction and template files.
ACH PASS-THRU	Upload ACH-ready files to the server for First Federal Bank of California to retrieve.. User must have one or more of ACH PAYROLL, ACH CORPORATE, and/or ACH CONSUMER validations.
ACH PASS-THRU REPORT	View the ACH Activity report for NACHA Pass-thru batches.
SPECIAL REPORTS	Access "special" text-formatted reports provided by First Federal Bank of California (e.g., Lock Box reports and account analysis statements).

Select this User Validation...	To enable the user to...
BILL PAY	Use the Web bill payment module. Users with this validation can: <ul style="list-style-type: none"> <li>• Schedule payments (but scheduled payment must be approved).</li> <li>• Add and edit payment accounts.</li> <li>• Request e-bills.</li> <li>• Add and delete payees.</li> <li>• View payments.</li> <li>• Submit inquiries regarding bill payments to Customer Service via email.</li> </ul>
BILL PAY APPR	Use the Bill Pay online bill payment module in its full capacity. This includes all rights associated with the Bill Pay validation, as well as the ability to approve payments. <i>Note: At least one user must be validated for BILL PAY APPR if any user is validated for the Bill Pay service. Single-user Bill Pay customers must be validated for both BILL PAY and BILL PAY APPR.</i>
LOAN PAY	Make internal loan payments through the loan payment module. <i>Note: If this feature is selected, the INTERNAL TRANSFERS A/M/D feature must also be selected.</i>
LOAN RPT	View loan balance reports. <i>Note: If this feature is selected, the BANK ACCT RPT feature must also be selected.</i>
POS PAY	Use the Positive Pay fraud prevention module, including the ability to create check items, set up check item import templates, and import check items.
POS PAY APPROVE	Approve check release authorizations made by the user or by another individual. <i>Note: At least one user must have POS PAY APPR validation if any user is validated for the Positive Pay service.</i>
POS PAY DECISION	Authorize or withhold payment for a presented check.
POS PAY VIEW	View Positive Pay reports.
CHECK INQUIRY	Access check inquiry functionality. Users can create, modify, submit, and report on requests tracking the status of checks they have issued.
CHECK PHOTOCOPY	Access check copy request functionality. Users can create, modify, submit, and report on requests for copies of paid checks.

## SETTING ACCOUNT NAMES (SYSTEM MANAGERS) *cont'd*

Select this User Validation...	To enable the user to...
STOP CANCEL	Cancel requested stop payments.
REMOTE DEPOSIT	Access the basic remote deposit functionality (the Pending Items and Reports tabs). <i>Note: Users must be validated for RD SCAN in order to scan checks.</i>
RD SCAN	Scan checks for remote deposit. Users with RD SCAN permissions can modify the check type (when available). <i>Note: If this feature is selected, the REMOTE DEPOSIT feature must also be selected.</i>
RD APPROVE	Approve remote deposit check batches that were scanned by users who require approval of their check items. Approval requirements are set by the System Manager. <i>Notes: If this feature is selected, the REMOTE DEPOSIT feature must also be selected.</i> <ul style="list-style-type: none"> <li>If approving users have some or all of the modify permissions (RD SCAN, MICR MOD, or AMT MOD), they can modify the associated portions of check items they are approving. RD SUBMIT Submit remote deposit checks for batching into an X9.37 file.</li> </ul> <i>Notes: If this feature is selected, the REMOTE DEPOSIT feature must also be selected.</i> <ul style="list-style-type: none"> <li>If submitting users have some or all of the modify permissions (SCAN, MICR MOD, or AMT MOD), they can modify the associated portions of check items they are submitting.</li> </ul>
RD MICR MOD	Users with Remote Deposit scanning, approval, or submission permissions can modify the information found on the MICR line of the check. After selecting this checkbox, select Full from the associated drop-down list to grant the user permission to modify all information scanned from the MICR line of the check, or select Partial to grant the user permission to modify only the MICR-line information that caused an error. <i>Note: If this feature is selected, the REMOTE DEPOSIT feature must also be selected.</i>
RD AMT MOD	Users with Remote Deposit scanning, approval, or submission permissions can modify check amount information. <i>Note: If this feature is selected, the REMOTE DEPOSIT feature must also be selected.</i>

Select this User Validation...	To enable the user to...
ACH Transaction Type	Select the checkboxes associated with the transaction types to which the ACH user is to be granted access. <i>Note: User must have one or more of ACH PAYROLL, ACH CORPORATE, and/or ACH CONSUMER validations.</i>
ACH Tax Templates	Select the checkboxes associated with the tax templates to which the ACH user is to be granted access. <i>Note: User must have one or more of ACH PAYROLL, ACH CORPORATE, and/or ACH CONSUMER validations.</i>

The following functions are reserved for future implementation:

- DTS WIRELESS
- IFT APPROVE

### SETTING ACCOUNT PERMISSIONS

System Managers can grant users access permissions to 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.

System Managers may modify their own account access permissions only if they have been given specific permissions to do so by First Federal Bank of California; contact First Federal Bank of California for additional information.

*Important: Users must be assigned account permissions before they can use the system!*

#### To assign user permissions for accounts:

1. From the ADMINISTRATION menu, select APPLICATIONS. The Administration screen is displayed.
2. On the Administration screen, select the ACCOUNT PERMISSIONS tab.
3. From the USER drop-down list, select the ID of the user to whom account access is to be assigned.  
The APPLICATION drop-down list is displayed.
4. 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 the 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.

5. 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.

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

### VIEWING INFORMATION ABOUT USERS AND ACCOUNTS

While all users can view their user privileges and available accounts, System Managers have the additional option of viewing information associated with the user profiles created by System Managers or First Federal Bank of California.

### VIEWING A LIST OF USERS

To access a list of user profiles:

1. Click your User Name, located in the bottom right-hand corner of the system's browser window. A pop-up window is displayed.
2. Select the **USER MAP** tab. A list of user profile is displayed. The following information is provided about each profile:

This Column...	Displays...
User ID	User ID associated with the user profile.
User Name	Name the user chose for purposes of logging on to the system. If the user has not yet performed the first-time log-on procedure, this column is blank.
Name	User's actual name, as provided when the user performs the first-time log-on procedure. If the User has not yet performed the first-time log-on procedure, the column is blank.

3. Close the pop-up window to continue working.

### VIEWING SERVICES AVAILABLE TO USERS

To view a list of the services available to each user:

1. Click your User Name, located in the bottom right-hand corner of the system's browser window. A pop-up window is displayed.

2. Select the **USER PRIVILEGES** tab.

3. From the **USER** drop-down list, select the user ID associated with the profile to be displayed. The user's log-on name is displayed in parentheses next to the user ID, if the user has performed the first-time log-on procedure.

Available services are displayed in the **Available Services** area.

4. Close the pop-up window to continue working.

### REVIEWING USERS' MULTI-FACTOR AUTHENTICATION REGISTRATION STATUS (SYSTEM MANAGERS)

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

To access the Multi-Factor Authentication report:

1. From the **ADMINISTRATION** menu, select **APPLICATIONS**. The Administration screen is displayed.
2. Select the **REPORTING** tab.
3. 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.
4. [OPTIONAL] From the **MFA LOGIN OPTION** drop-down list, make a selection to filter the user list.

User information is displayed in the following columns:

This Column...	Displays...
Line	Identifier for the line, for ease of reference.
Company ID	Identification code for the company.
Site ID	Identification code for the site.
Registered	Date and time at which the user registered for MFA. If the user has not yet registered for MFA, this field is left blank.
Last Login	Date and time the user last accessed the system. If the user has not yet registered for MFA, this field is left blank.