Latitude®

Printable Help for Administrators

Version 13.0

Last updated November 04, 2019

Abstract

This document is a printable version of Latitude by Genesys help for administrators.

For copyright and trademark information, see https://help.genesys.com/latitude/Liquid/Desktop/Copyright_and_Trademark_Information.htm.

Table of Contents

Introduction to Latitude 13.0 10
What's New in Latitude 13.0 10
Angular upgrade 10
Custom panels 10
Interaction Dialer 10
Payment arrangements 11
Permissions 11
Pool queue 11
Portal redirect 11
Reference panels 11
Log On to Latitude by Genesys 11
Change Your Password 13
Work Form Overview 14
Help Overview 17
Search feature 18
Search syntax 18
Wildcard expressions 18
Boolean operators 19
Nested expressions 19
Screen captures 20
System Administration 20
System Administration 20
Permissions and Policies 20
Scopes 20
Search for a Permission or System Code 21
Set a Permission and Policy 22
Administration Settings 25
Administration Settings 25
System Configuration Permission 25
System Codes and Settings Permission 25

Users, Roles, Permissions, and Policies Permission 25
Application Settings 26
Application Settings 26
AIM Settings 26
AIM Settings 26
Access Reports Permission 26
Access Tools Permission 26
Add/Edit/Delete Account Filters Permission 27
Add/Edit/Delete Agencies Permission 27
Add/Edit/Delete Business Rules Permission 27
Add/Edit/Delete Distribution Templates Permission 28
Run Actions Permission 28
Use AIM Permission 29
View Account Filters Permission 29
View Agencies Permission 29
View Business Rules Permission 30
View Distribution Templates Permission 30
Settings for Auxiliary Products Permission 31
CUBE Server Config Permission 31
Dashboard Settings 32
Dashboard Settings 32
Manage Dashboards Permission 32
View Dashboards Permission 32
Exchange Settings 33
Exchange Settings 33
Modify Client Configuration Permission 33
Use Exchange Permission 33
Use Fusion Permission 34
Liquid Latitude Settings 34
Liquid Latitude Settings 34
Access Accounts Settings 34
Account Actions Settings 40

Account Data Settings 46
Applicable Processes and Stages Permission 73
Dialer Functionality Settings 73
Enable Server Caching of Permissions 75
Work Form Settings 76
Payment Vendor Gateway Settings 78
Payment Vendor Gateway Settings 78
Access Batch Wizard Permission 78
ACH Vendor Information Permission 79
Batch Processor System Permission 80
Credit Card Vendor Information Permission 80
Customer Information Profiles Permission 81
Enable Payment Vendor Gateway Permission 81
Paper Draft Vendor Information Permission 82
Portfolio Manager Settings 83
Portfolio Manager Settings 83
Access Portfolio Manager Permission 83
Access Reports Permission 84
Access Tools Permission 84
Add/Edit/Delete Buyers Permission 84
Add/Edit/Delete Investors Permission 85
Add/Edit/Delete Purchases Permission 85
Add/Edit/Delete Sales Permission 86
Add/Edit/Delete Samples Permission 86
Add/Edit/Delete Sellers Permission 87
View Buyers Permission 87
View Investors Permission 87
View Purchases Permission 88
View Sales Permission 88
View Samples Permission 89
View Sellers Permission 89
Reporting Console Settings 89

Reporting Console Settings 89
Access Reporting Console Permission 89
Manage Reporting Console Permission 90
View Reports Permission 90
Service Request Gateway Settings 91
Service Request Gateway Settings 91
Access Quota Management Application Permission 91
Access SRG Module Installer Permission 92
Credit Report Requests Settings 92
Enable Service Request Gateway Permission 95
Web Access Settings 96
Web Access Settings 96
Account View Client Code Override Policy Permission 96
Website System Policy Permission 96
Website User Client Access Policy Permission 96
Website User Policy Permission 97
WorkFlow Settings 98
WorkFlow Settings 98
Manually Pause WorkFlow Permission 98
Manually Raise Event Permission 99
Manually Release WorkFlow Permission 99
Manually Resume WorkFlow Permission 100
Manually Start WorkFlow Permission 100
Manually Stop WorkFlow Permission 101
WorkFlow Engine Settings Permission 101
Configuration Settings 102
Configuration Settings 102
Delinquency Aging Bucket Labels Permission 102
Payment Processing Settings 103
Payment Processing Settings 103
Configuration for Handling Broken Promises Permission 103
Configuration for Handling NSFs/Reversals Permission 103

Deactivate Automatic Status and Queue Level Permission 104
Override Payment Spread Permission 105
Payment Method Fee Schedule Permission 106
Map a Payment Method to a Fee Schedule 106
Payment Spread Permission 107
Prevent Multiple Account Access Permission 109
SMTP Permission 109
Welcome Web Page Permission 110
Welcome Window Permission 110
Management Tool Settings 111
Management Tool Settings 111
Accounting Settings 111
Accounting Settings 111
Access Invoices Program Permission 111
Access Overpayment Manager Permission 111
Enter AR Payments Permission 113
Enter Bank Transactions Permission 113
Generate Invoices Permission 114
Generate Statements Permission 114
Print Checks Permission 115
Access Credit Reporting Wizard Permission 115
Access Custodian Editor Permission 115
Access Dialer Config Permission 116
Access Goal Manager Permission 116
Archive Settings 116
Archive Settings 116
Access Archive/Restore Functionality Permission 116
Enable Archive of Account Data Permission 117
Letter Console Settings 118
Letter Console Settings 118
Access Letter Console Permission 118
Change Settings Permission 118

Create/Delete Permission 118
Merge Using Microsoft Word Permission 119
Link Console Settings 119
Link Console Settings 119
Access Link Console Permission 119
Link Accounts Permission 120
Payment Entry Settings 120
Payment Entry Settings 120
Access Payment Entry Permission 120
Remove Other Users Batch Locks Permission 121
Query Designer Settings 121
Query Designer Settings 121
User Restrictions by Conditions Permission (Account Analysis) 121
Access Condition Builder Permission 122
Access Custom Queue Manager Permission 122
Access List Builder Permission 122
Access Management Suite Extension Wizard Permission 123
CBR Requester Settings 123
Desk Mover Settings 127
Letter Requester Settings 128
Restrict Conditions Permission 129
Status Changer Settings 129
Use Literal Conditions Permission 130
Security Settings 131
Security Settings 131
Account Lockout Permission 131
API Key Manager 131
API Key Manager 131
Add an API Key 132
Revoke an API Key 132
Password Complexity Permission 133
Password Expiration Permission 133

Access Services Permission 134
System Codes and Settings 134
System Codes and Settings 134
Account Codes 134
Account Codes 134
Anchor Cards 134
Anchors 138
Care Types 143
Claim Types 145
Classes of Business 148
Clients 150
Complaint Categories 184
Courts 186
Custom Panel Mapping 190
Desks 194
Dispute Types 204
Documentation Categories 207
Extra Data Codes 210
Fee Schedules 215
Hardship Types 223
Legal Court Case Statuses 226
Letter Types 230
List Codes 233
Manual Process Stages 239
Note Action Codes 240
Note Result Codes 244
Process Stages 249
Queue Levels 260
Responsible Party Codes 274
Status Codes 277
System Configuration 282
Financial Codes 303

Financial Codes 303
ABA Routing Numbers 303
Banks 308
Credit Card Types 313
Legal Ledger Types 316
Payment Methods 319
Payment Sub-Batch Types 323
Salesman Codes 325
General Settings 328
General Settings 328
Law Lists 328
State Restriction 331
Organization Groups 336
Organization Groups 336
Branches 336
Departments 339
Roles 341
Teams 343
Users 346
Party Codes 351
Party Codes 351
Asset Types 351
Language Codes 354
Data Grids 357
Data Grids 357
Sort Data in a Data Grid 357
Filter Data in a Data Grid 358
Move Between Pages of a Data Grid 358

Introduction to Latitude 13.0

The Latitude 13.0 collections solution has comprehensive debt collection and recovery capabilities for managing all pre- and post-charge-off accounts and workflow processes. It provides collectors and agents with the tools to manage the debt collection and recovery process. It also provides supervisors, managers, administrators, and support staff with the tools to manage Latitude.

Latitude provides the full functionality for the collector's or agent's desktop and deploys as a true zero-footprint, browser-based environment.

Latitude 13.0 allows you to:

- Maintain account and contact information.
- Track account activities.
- Record account notes.
- Set account reminders and follow-up dates.
- Schedule and process payments.

What's New in Latitude 13.0

The initial release of Latitude 13.0 introduced the following enhancements.

Angular upgrade

Latitude by Genesys upgraded the Agent Desktop to the most recent Angular technology. This upgrade improves overall performance, supportability, and scalability as we continue to transition the Latitude product suite to a minimal footprint deployment strategy.

Custom panels

Added ability to create custom anchor cards and reference panels to display in the **Work Form**. You map the custom anchor card or reference panel to a query that specifies the data to display in the card or panel. You create the query using the **Custom Panel Query Creator** tool in Latitude Console and create the mapping in the **Custom Panel Mapping** panel in Latitude. For more information, see Custom Panel Query Creator in the *Latitude Console* documentation and Custom Panel Mapping in the *Latitude* documentation.

Interaction Dialer

- Added integration to Interaction Dialer to allow users to process campaign calls in call lists that your organization creates using List Builder. For more information, see Dialer Agent Interface
- Added ability to log on to Interaction Dialer automatically when logged on to Latitude. For more information, see Add a User and Modify a User.
- Added ability to map disposition codes from your Dialer server to result codes in Latitude. For more information, see Map a Disposition Code to a Result Code.
- Added ability to dial phone numbers manually from the **Contact Information** tab or the **Phones** panel. For more information, see Dial a Phone Number.

Payment arrangements

Added ability to create a single payment arrangement for an amount that exceeds the account balance when proposing a payment arrangement in the **Payment Negotiator** card. You can create the arrangement for a single, non-joined account or for one or more joined accounts. The amount cannot exceed the maximum overpayment amount configured in the **Allow Overpayments** permission.

Permissions

- Added Access Redirect Portal permission for specifying the web site to open in a new browser tab when a user clicks the link on the account toolbar.
- Added Allow Overpayments permission for specifying whether to allow payment arrangements that exceed the account balance. If allowing overpayments, specify the maximum percentage of the account balance that users are allowed to increase the payment by when scheduling overpayments. For example, if the account balance is $100 and the maximum overpayment percentage allowed is 10%, you cannot create an overpayment arrangement for more than $110.
- Added Dialer permission for specifying whether to display the **Dialer Agent Interface** in the **Work Form**.
- Added Mask Phone Numbers permission for specifying whether to mask all phone number occurrences in the **Work Form**.
- Added "Pool Queue" option to the Queue Providers permission for specifying whether the Pool queue is available to users.

Pool queue

Added the Pool queue feature to the **Work Form**. A Pool queue is dynamic in that accounts flow in and out of it as they qualify or disqualify. Accounts in a Pool queue reside on an inventory-type desk, where multiple users have access to them.

Portal redirect

Added ability to display a web site that your organization specified in a new tab in your browser. For more information, see Display a Web Site on a New Browser Tab.

Reference panels

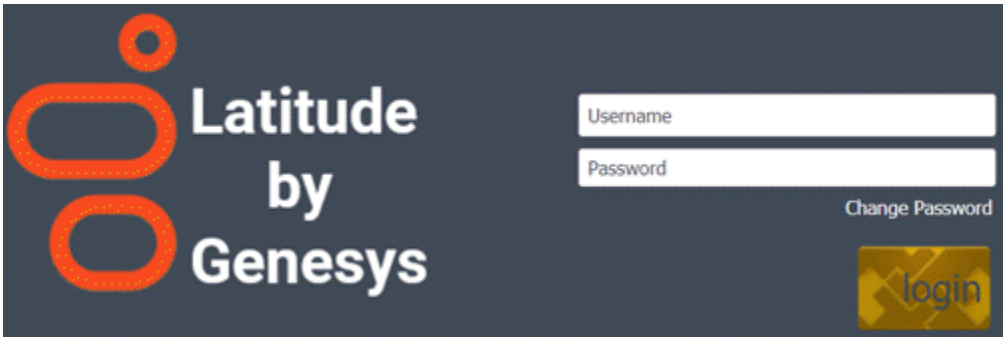
Added a **Communication** panel to display all communications associated to an account, such as inbound and outbound calls; and inbound and outbound letters. If available, you can also play audio recordings associated to calls and view sent letters. For more information, see Communication.

Log On to Latitude by Genesys

Use the **Logon** page to log on to Latitude by Genesys. Your assigned permissions determine which options and features in Latitude are available to you. For more information, see Permissions and Policies.

To log on to Latitude

1. Open Latitude by Genesys in your browser. The **Logon** page appears.



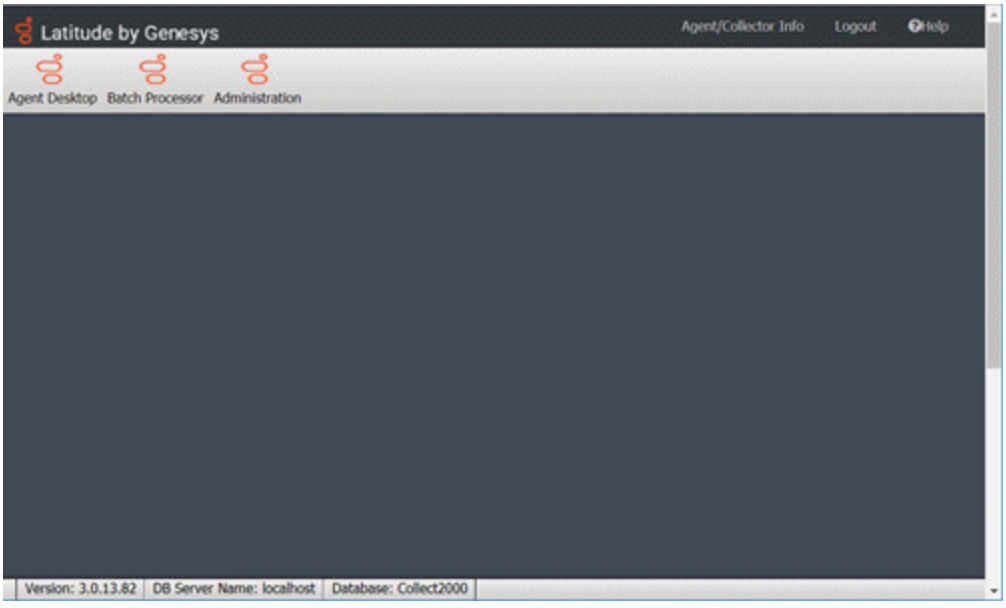
2. Do one of the following:

   - If you have a user ID and password specifically for Latitude by Genesys, type them in the boxes and then click **Log On**.

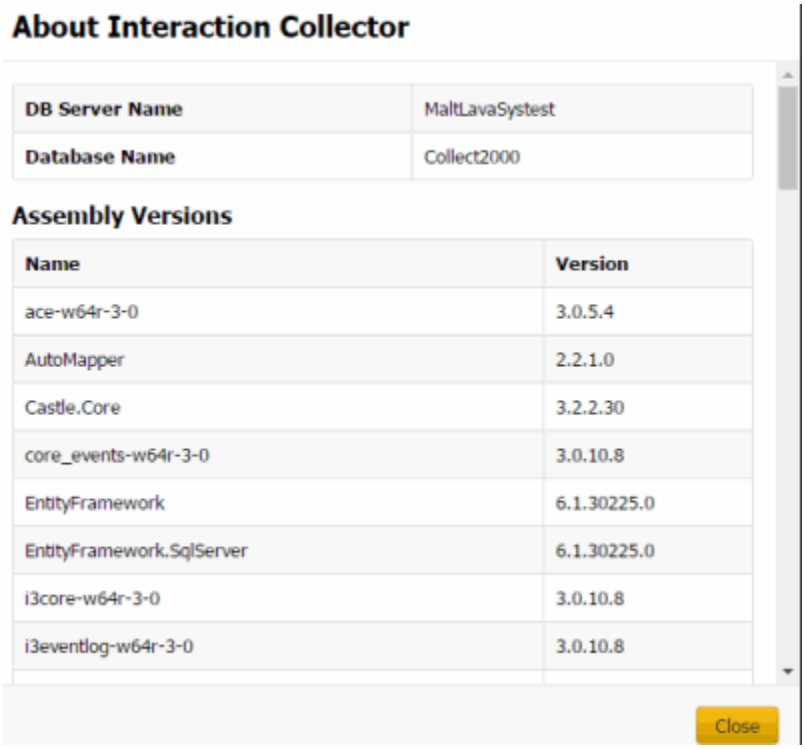
   > **Note:** As you type your password, periods display instead of the typed characters. If your password expires, the system requires you to change it. For more information, see Change Your Password.

   - If your organization configured Latitude by Genesys to allow an external logon (for example, your network credentials), leave the **Username** and **Password** boxes blank and click **External Log On**. If you aren't logged on externally, the system redirects you to your identity provider and prompts you to provide your credentials.

   If your credentials are correct, the **Latitude by Genesys** page appears. Otherwise, an error message appears; provide the correct credentials or contact your system administrator for assistance.



3. To view information about the system (such as assembly versions for each component on the web server), click the version number in the status bar. The **About Latitude by Genesys** dialog box appears. This information is useful for troubleshooting deployments.



4. Do one of the following:
    - To open the **Work Form**, click **Agent Desktop**. A new browser tab opens. If any account interactions remained open when you last logged off, the **Open Interactions** panel appears. Otherwise, the **Search Accounts** panel appears. For more information, see Account Retrieval.
    - If you have the appropriate permissions and you want to process a batch of payment transactions, click **Batch Processor**. For more information, see Process a Payment Batch.
    - If you have the appropriate permissions and you want to configure system codes, settings, permissions, and policies, click **Administration**. For more information, see System Administration.

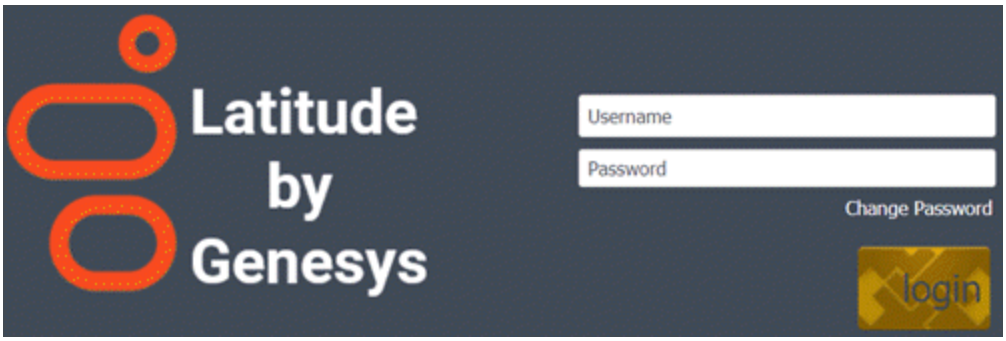
Change Your Password

Use the **Change Password** dialog box to change your Latitude by Genesys password. If your password is close to the expiration date (based on the Password Expiration permission setting), a warning appears under the **Change Password** link.

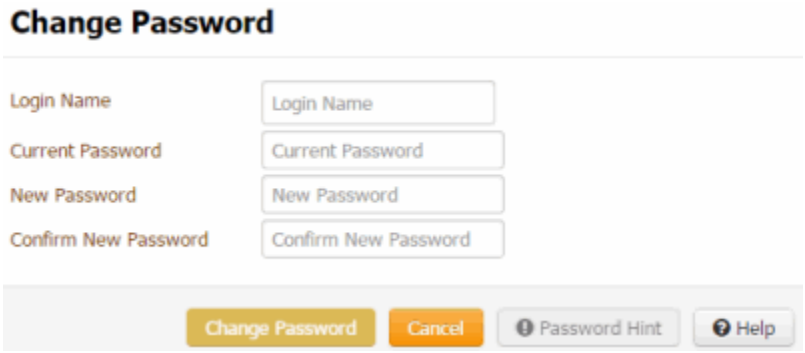
To change your password

1. Do one of the following:
    - On your desktop, click the shortcut to Latitude by Genesys.
    - If you have a bookmark set in your browser for Latitude by Genesys, click the bookmark.
    - In your browser, in the **Address** box, type the address for Latitude by Genesys and press **Enter**.

The **Logon** page appears.



2. Click **Change Password**. The **Change Password** dialog box appears.



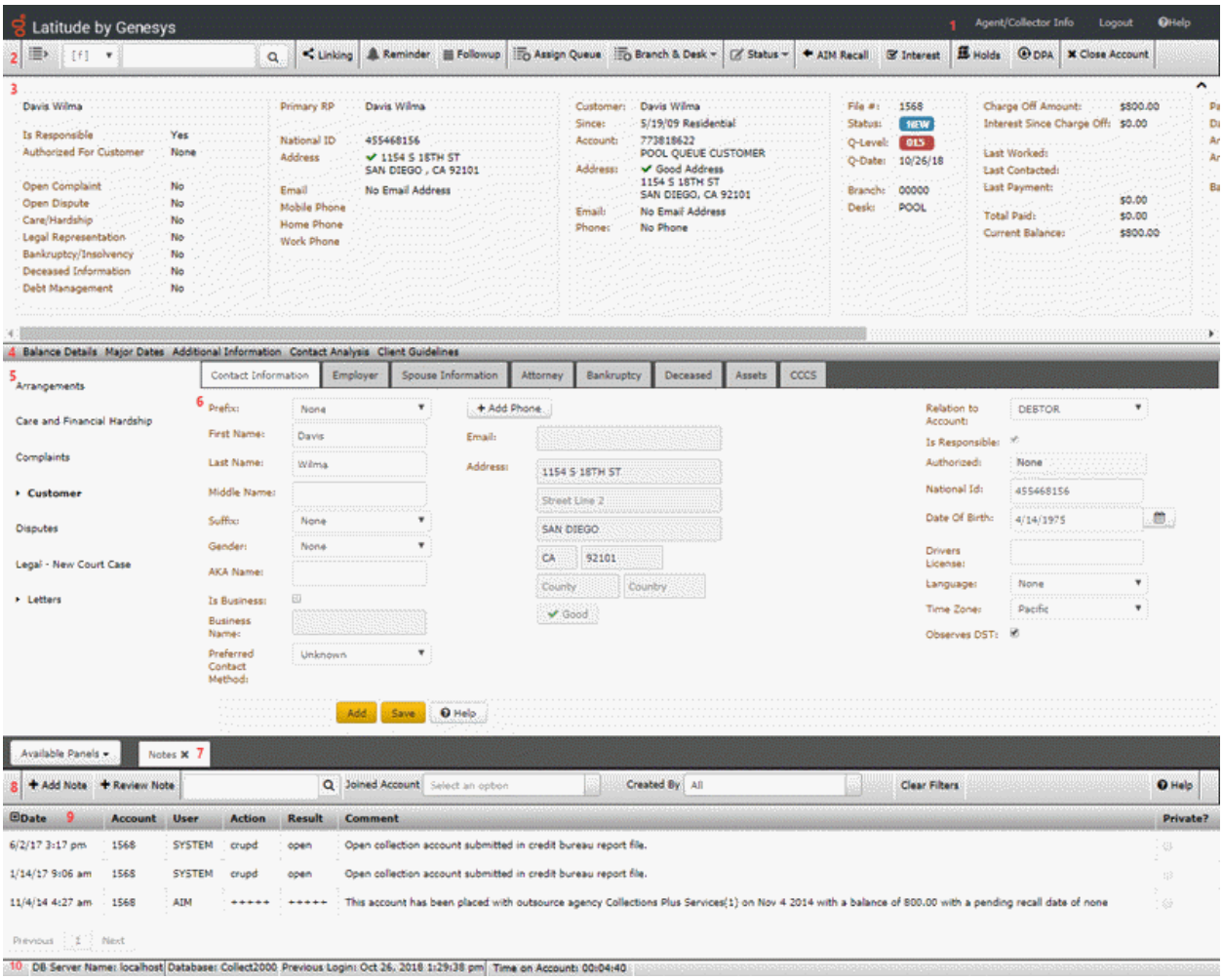
3. In the **Login Name** box, type your user ID.
4. In the **Current Password** box, type your current password.
5. In the **New Password** box, type your new password.

> **Tip:** To view the requirements for creating a password, click **Password Hint**.

6. In the **Confirm Password** box, retype your new password.
7. Click **Change Password**.

Work Form Overview

The **Work Form** is the main page in Latitude, and it consists of several sections. Each section allows you to perform specific actions related to that section.



Note: A red asterisk (*) next to a field indicates a required field.

1. **Application toolbar:** Displays options for viewing the **Welcome** page, logging off Latitude and viewing the documentation. When processing a request, a yellow progress bar appears along the top edge of this toolbar and a circulating progress indicator appears next to the logo.
2. **Account toolbar:** Displays options for displaying and working an account.
3. **Delinquency** or **Recovery anchor:** Displays delinquency or recovery information for the selected account, depending on how your organization configured your system.
4. **Account Detail toolbar:** Displays options for viewing detail and summary information for the selected account.
5. **Task Panel navigation tree:** Displays the available task panels and allows you to open them.
6. **Task panel:** Displays the selected task panel.
7. **Reference Panel navigation bar:** Allows you to open and close reference panels.
8. **Reference Panel toolbar:** Displays options for the selected reference panel.
9. **Reference panel:** Displays the selected reference panel.

10. **Status bar:** Displays the following system and account status information:
    - **DB Server Name:** Name of the Latitude database server.
    - **Database:** Name of the Latitude database.
    - **Previous Login:** Date and time you last logged on to Latitude.
    - **Time on Account:** Length of time that you've spent on this account. If the background color is gray, you haven't reached the threshold set for the **caution** or **warning** zones. If the background color is yellow, you've reached the threshold set for the **caution** zone. If the background color is red, you've reached the threshold set for the **warning** zone. For more information, see the **Time on Account Configuration** permission.
    - **Queue Progress:** Number of accounts in the work queue. This value only appears when you are working accounts in a queue.
    - **Alerts:** Number of issues related to the account. To view details about the alert, click **Alerts**. If you receive this message, "An error has occurred. If this problem persists, please contact Technical Support," you can view the details by clicking **Alerts**.

Icons

An icon allows you to perform a specific action. The following icons are available on the **Work Form:**

Icon	Name	Description
	Search Slide-in	Displays and hides the **Search & Queue Selection** panel, which allows you to search for and display accounts. The Search slide-in is on the **Account** toolbar.
^	Collapse	Collapses a section of the **Work Form** to hide its contents.
v	Expand	Expands a section of the **Work Form** to display its contents.
	Filter	Limits information in a data grid based on criteria you specify.

Form state

When you attempt to save information, the background of the "save" section of the panel you are working changes color to indicate the status of the attempted save.

Color	Description
Gray	Default color that indicates the user hasn't requested a "save" action yet.
Blue	Indicates the "save" action is processing.
Green	Indicates the "save" action completed without errors.
Red	Indicates that there was an error completing the "save" action.

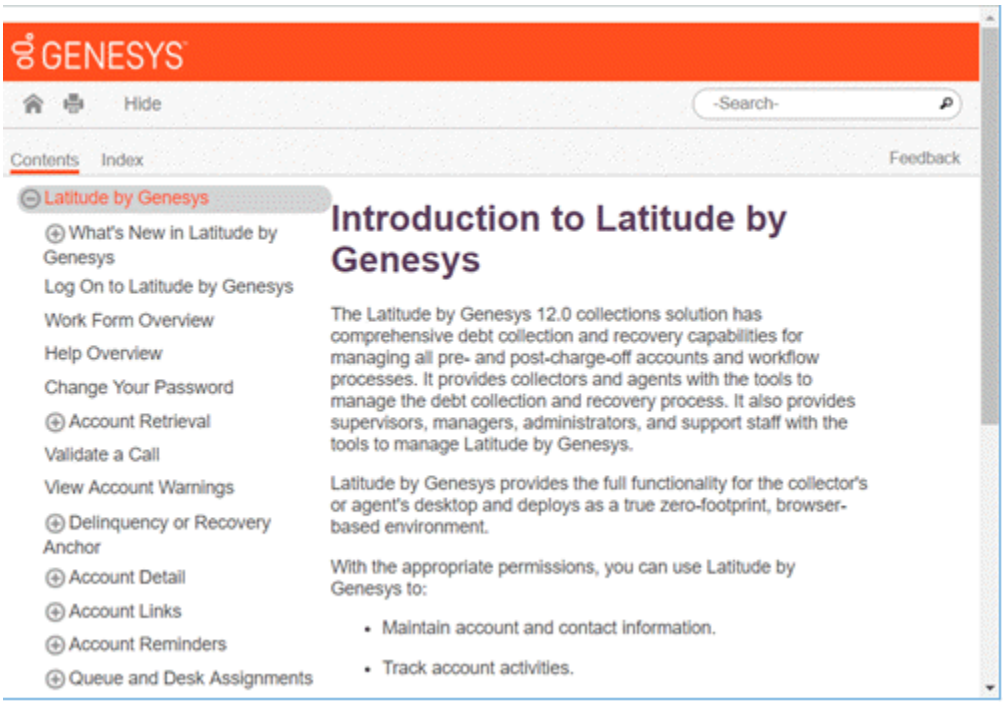
Help Overview

Latitude by Genesys help provides you with information for using Latitude by Genesys. You can locate and view help topics using the table of contents, index, and search features. You can also open help within certain areas of Latitude by Genesys (for example, panels and dialog boxes) to view context-appropriate information.

To open Latitude by Genesys help

- In the **Application** toolbar, click **Help**. The help opens with the introductory topic and table of contents displayed.

> **Note:** To open the help to a context-appropriate topic, in the panel or dialog box you have open currently, click **Help**. The corresponding topic appears in a separate window. To display the table of contents, at the bottom of the help window, click **Show**.



> **Tip**: To adjust the width and height of the window or its panes, click the edge of the window or pane and drag it up or down, left or right.

1. **Toolbar:** Allows you to display the table of contents, index, search feature, or glossary. When you click an option in the toolbar, the corresponding information appears in the **Navigation** pane.
2. **Navigation pane:** Displays the following:

   Contents: Displays the table of contents. To display a topic in the **Content** pane, expand a book and then click the link.

   Index: Displays the index. To display a topic in the **Content** pane, type a keyword or phrase in the box (or scroll through the list) and then click the link in the list.

Search: Displays the search feature. To display a topic in the **Content** pane, type a keyword or phrase in the box and then press **Enter**. In the search results, click the link.

Glossary: Displays a glossary of terms and definitions. To display a definition, click the term.

3. **Breadcrumbs:** Displays your current location within the help system. When you click a breadcrumb, the related topic displays.
4. **Content toolbar:** Displays an option for sending feedback through an email message to Latitude by Genesys Documentation.
5. **Content pane:** Displays the contents of a topic. To display recently visited topics, use your browser's **Back** and **Forward** options. To view the **Content** pane menu, right-click in the **Content** pane.

Search feature

You can use the search feature to locate topics that contain words or phrases that you specify. You formulate a search query following a specific set of rules. You can include wildcard expressions, Boolean operators, and nested expressions in your search query. A list of topics that match your search criteria appear in the search results. When you click a topic title in the search results, the content of that topic appears in the **Content** pane.

Search syntax

The basic rules for formulating search queries are:

- Searches are not case-sensitive, meaning you can type uppercase or lowercase characters.
- You cannot search for a single character or the following reserved words: an, and, as, at, be, but, by, do, for, from, have, he, in, it, not, of, on, or, she, that, the, there, they, this, to, we, which, with, you.
- The search engine ignores punctuation marks and special characters such as @#$%^&()=+[]\.
- Enclose phrases and terms that include a period (such as a file name with an extension) in double quotation marks.

Wildcard expressions

Wildcard expressions allow you to search for one or more characters using a question mark or asterisk. A question mark represents a single character, while an asterisk represents one or more characters.

Search for...	**Example**	**Result**
Topics with text that starts with one or more specified characters and ends in any character or number of characters	log or log*	Returns all topics with text that starts with the specified characters (for example, log, logon, logging).
Topics with text that starts with the specified characters, has a single	32?57	Returns all topics with text that has any character where you placed the question mark (for example, 32?57 returns 32257, 32457, and 32857).

Search for...	Example	Result
character that can be anything, and ends in the specified characters		
Topics that contain all the words specified, in any order or placement within the topic	account status	Returns all topics with both account and status, but not necessarily as a phrase or in the order specified. For example, the search returns topics with "the account status..." or "the status of the account..."
Topics that contain the specified phrase	"account status"	Returns all topics with account status as a phrase. For example, the search returns topics with "the account status..." but not "the status of the account..."

Boolean operators

Boolean operators (AND, OR, NOT, NEAR) allow you to create a relationship between terms. If you don't specify an operator, the system uses AND by default.

Search for...	Example	Result
AND	account AND status	Returns all topics with both account and status, but not necessarily as a phrase or in the order specified. For example, the search returns topics with "the account status..." or "the status of the account..."
OR	account OR status	Returns all topics with either account or status, or both.
NOT	account NOT status	Returns all topics with account but not status.
NEAR	account NEAR status	Returns all topics where account is within eight words of status.

Nested expressions

Nested expressions allow you to perform complex searches. For example, queue AND ((collector OR clerical) not supervisor) finds topics containing queue and collector but not supervisor, or containing queue and clerical but not supervisor. As with mathematical expressions, the system evaluates expressions in parentheses first. If there is no parenthesis, the system evaluates the expression from left to right. For example, queue NOT (clerical OR supervisor) finds topics containing queue but not clerical or supervisor. Queue NOT clerical OR supervisor finds topics containing queue but not clerical, or topics containing supervisor.

Screen captures

Many topics contain a snapshot of the related application page. Use this sample graphic as a frame of reference to match the application page to the help topic. What you see displayed in the application may differ, depending on your system configuration, your permissions, and the options you select.

System Administration

System Administration

Administrators, managers, and supervisors can configure system codes, settings, permissions, and policies to customize the Latitude suite of products according to your organization's preferences.

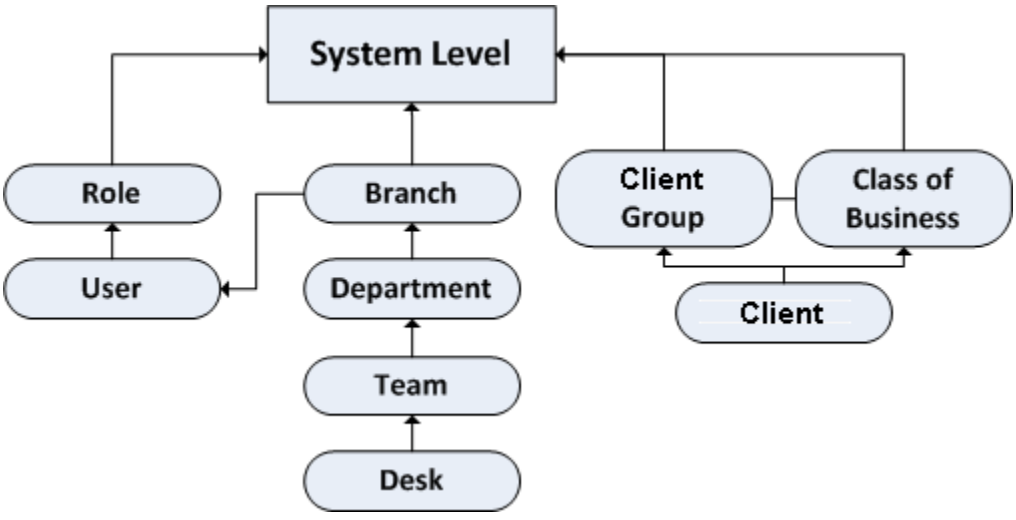
Permissions and Policies

Permissions grant users the authority to use program features and policies define the limitations of permissions. For example, you can set a permission to allow a user to add a post-dated check (PDC) transaction for an Automated Clearing House (ACH) payment. You can then set a policy indicating that the user cannot add transactions that are less than $20.

It's possible for Latitude to apply permissions and policies differently, based on the user or other criteria. Latitude uses a tier (scope) method to create permission and policy layers. So, permissions and policies applied at the base (system) level apply to other scopes, unless an administrator modifies the particular permission and policy. For example, a system-level permission applies to all roles, unless an administrator customizes the permission for the role. Likewise, permissions applied at the role level apply to all users assigned to the role, unless an administrator customizes the permission for an individual user.

Scopes

There are 10 scopes in the permissions and policy structure, split into 4 categories: system, user, desk, and client. These scopes create a hierarchical tree that extends back to the system level. The following diagram shows each scope within its hierarchical structure.



Scopes available for each permission vary. Latitude determines which permissions to use by following hierarchy lines. For example, if a permission doesn't apply at the user scope, Latitude checks the role

scope. If it doesn't apply at the role scope, Latitude checks the system scope. It's also possible to check permissions for both a particular user and a particular client. For example, if the user can add post-dated checks, but the client on the account does not permit post-dated checks, the user cannot add post-dated checks for that particular client.

Latitude checks branch permissions based on the user's assigned branch, along with the branch permissions for the user's assigned desk. Latitude merges these permissions and their settings when all of the following occurs:

- An administrator assigns the user to a desk and a branch not associated to that desk.
- An administrator configures the same permission for the user's branch and the desk's branch.

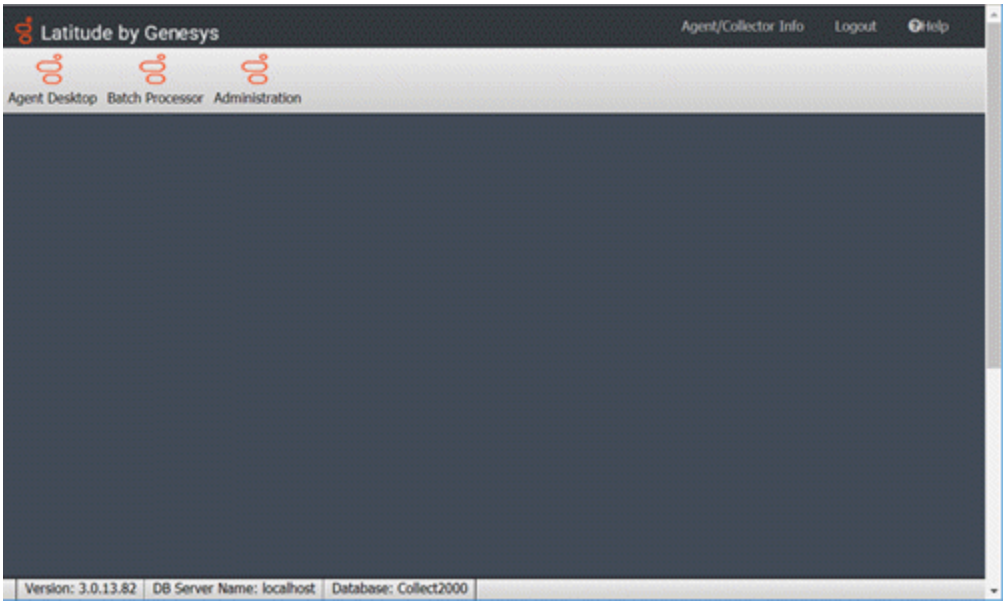
Policies take the permissions one step further. For example, the user-level and client-level permissions allow post-dated checks. At the user level, the permission stipulates that the minimum check amount is $5.00 and the maximum number of days that a user can post-date a check is 30. The permission understands that with the minimum amount a higher number is more restrictive, while with the maximum number of days the lower amount is more restrictive. Latitude considers this logic when creating the intersection for the effective permission. The user can add a post-dated check that is at least $15.00 and within 30 days (unless the administrator doesn't configure the user to observe client rules).

Search for a Permission or System Code

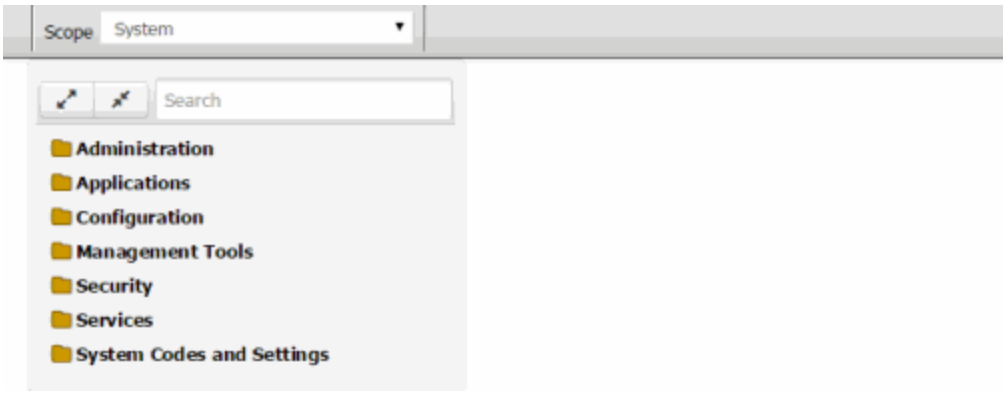
Use the **Administration** page to search for a permission or system code.

To search for a permission or system code

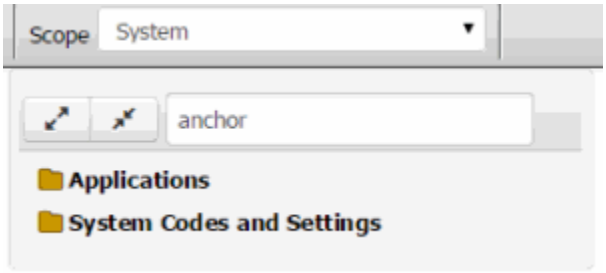
1. Open the **Latitude by Genesys** page.



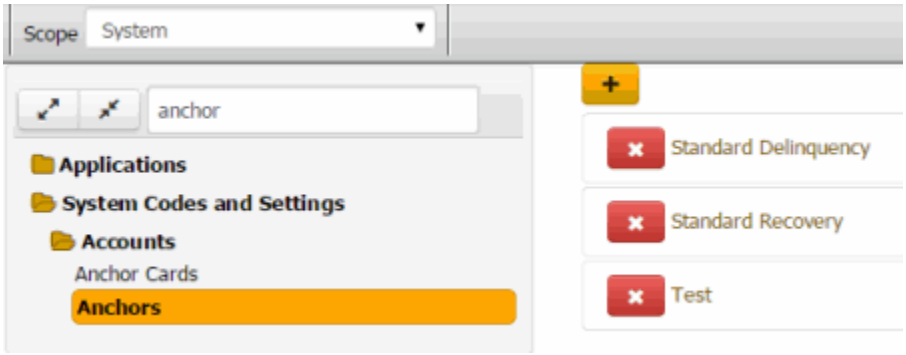
2. In the menu bar, click **Administration**.



3. In the **Search** box, type the full or partial name of the permission or scope and then press **Enter**. The system displays only the folders that contain items that match your search criteria.



4. In the **Navigation** pane, expand a folder and then click an item to view it.



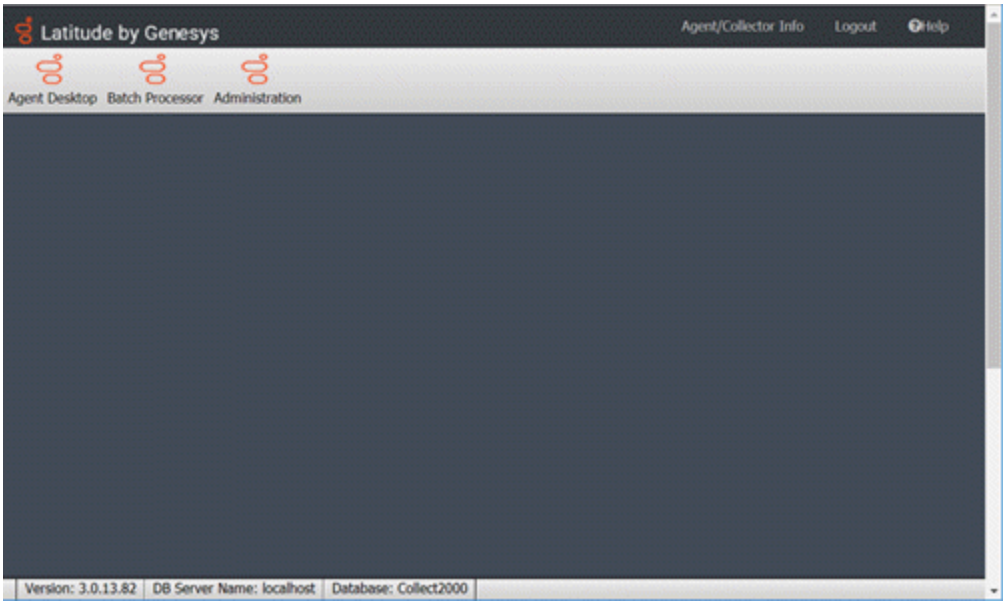
5. To clear the search criteria, delete the content in the **Search** box.

Set a Permission and Policy

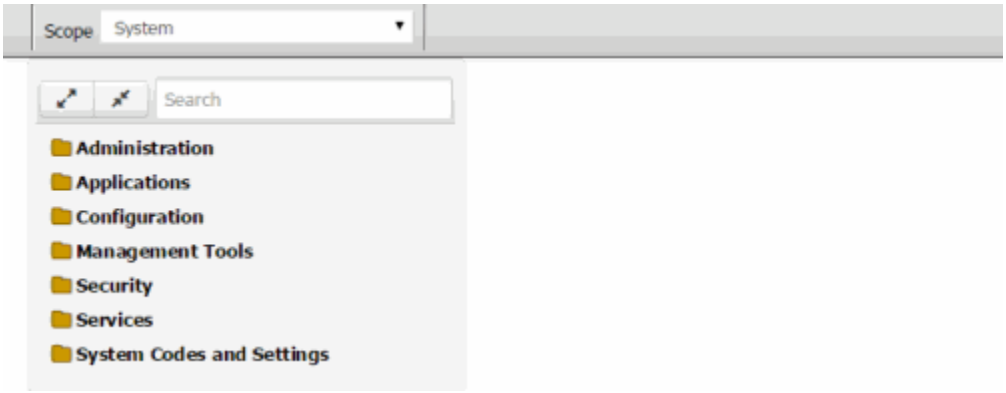
Use the **Administration** page to set permissions and policies for a scope. For more information about scopes and individual permissions and policies, see Permissions and Policies.

To set a permission and policy

1. Open the **Latitude by Genesys** page.



2. In the menu bar, click **Administration**.



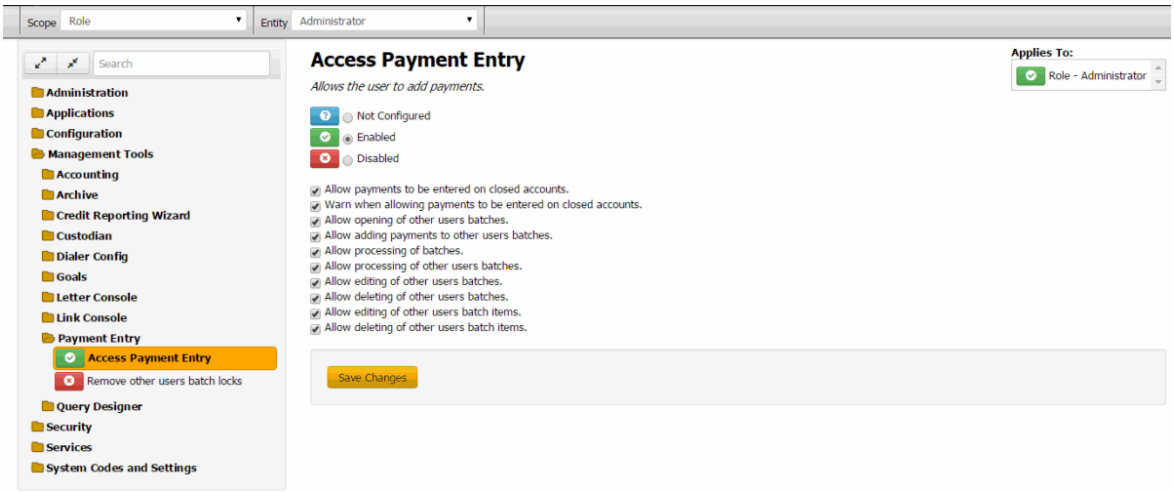
3. In the **Navigation** pane, do one of the following:

a. Expand one or more folders to locate the permission.

> **Tip:** To expand all the folders and sub-folders, click the Expand Tree icon next to the **Search** box. To collapse all the folders and sub-folders, click the Collapse Tree icon next to the **Search** box.

b. Do the steps to Search for a Permission or System Code.

4. In the **Navigation** pane, click a permission. The panel for the selected permission appears. The following example shows the Access Payment Entry permission for the Administrator role.



Scope: Scope level at which to apply the permission (for example, system, role, user, branch). If a permission isn't available for a scope, the system displays a message.

Entity: Entity within the scope to which to apply the permission.

Expand Tree icon: Expands all folders and sub-folders.

Collapse Tree icon: Collapses all folders and sub-folders.

Search: Allows you to search for a permission.

Not Configured: Your organization didn't configure the permission at the selected scope and entity level. The selected scope and entity level can inherit the settings from a higher level.

Enabled: Permission applies at the selected scope and entity level.

Disabled: Permission doesn't apply at the selected scope and entity level, regardless of how it's configured at a higher level.

Policy: Rules to apply to the permission. In the example, the check boxes represent the policy. Not all permissions have policies.

Applies to: Scope and entity to which the permission selected in the **Navigation** tree applies.

5. In the toolbar, specify the scope and entity for the permission.
6. In the permission pane, select a configuration option (Not Configured, Enabled, or Disabled) for the selected scope and entity.
7. If there is a policy associated to the permission, configure the policy.

> **Note**: Policies adhere to the strictest setting when combined. For example, you can set the PDC minimum amount higher for a role scope, and set it lower for a customer scope. Latitude follows the most restrictive setting, which is the lower amount set at the customer level.

8. Click **Save Changes**.

Administration Settings

Administration Settings

Use administration settings to specify permissions and policies for system control, system codes, users, roles, and permissions and policies.

System Configuration Permission

Use the System Configuration permission to specify whether users can maintain Latitude configuration settings, such as your organization's name and contact information.

Location

In the **Navigation** pane, click **Administration** > **System Configuration**.

Scope

This permission is available for all scopes.

Policy

N/A

System Codes and Settings Permission

Use the System Codes and Settings permission to specify whether users can maintain system codes and settings. If you disable the permission for the role or user scope, the role or user cannot access the System Codes and Settings folder or its sub-folders.

Location

In the **Navigation** pane, click **Administration** > **System Codes and Settings**.

Scope

This permission is available for all scopes.

Policy

N/A

Users, Roles, Permissions, and Policies Permission

Use the Users, Roles, Permissions, and Policies permission to specify whether users can maintain users, roles, permissions, and policies. If you disable the permission for the role or user scope, the role or user cannot open the Administration tool. If your organization hasn't configured this permission, only the Administrator **account** (not an Administrator user) can maintain this information.

Location

In the **Navigation** pane, click **Administration** > **Users, Roles, Permissions, and Policies**.

Scope

This permission is available for all scopes.

Policy

N/A

Application Settings

Application Settings

Use application settings to specify permissions and policies for supplemental programs.

AIM Settings

AIM Settings

Use the AIM settings to specify permissions and policies for Agency Interface Module (AIM).

Access Reports Permission

Use the Access Reports permission to specify whether users can display reports in AIM.

Location

In the **Navigation** pane, click **Applications** > **AIM** > **Access Reports**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Access Tools Permission

Use the Access Tools permission to specify whether users can use the tools in AIM.

Location

In the **Navigation** pane, click **Applications** > **AIM** > **Access Tools**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Add/Edit/Delete Account Filters Permission

Use the Add/Edit/Delete Account Filters permission to specify whether users can add, modify, and delete account filters in AIM.

Location

In the **Navigation** pane, click **Applications** > **AIM** > **Add/Edit/Delete Account Filters**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Add/Edit/Delete Agencies Permission

Use the Add/Edit/Delete Agencies permission to specify whether users can add, modify, and delete agencies in AIM.

Location

In the **Navigation** pane, click **Applications** > **AIM** > **Add/Edit/Delete Agencies**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Add/Edit/Delete Business Rules Permission

Use the Add/Edit/Delete Business Rules permission to specify whether users can add, modify, and delete business rules in AIM.

Location

In the **Navigation** pane, click **Applications** > **AIM** > **Add/Edit/Delete Business Rules**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Add/Edit/Delete Distribution Templates Permission

Use the Add/Edit/Delete Distribution Templates permission to specify whether users can add, modify, and delete distribution templates in AIM.

Location

In the **Navigation** pane, click **Applications** > **AIM** > **Add/Edit/Delete Distribution Templates**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Run Actions Permission

Use the Run Actions permission to specify whether users can create placements, final recalls, and pending recalls in AIM. Also allows the user to import and export files.

Location

In the **Navigation** pane, click **Applications** > **AIM** > **Run Actions**.

Scope

This permission is available for the following scopes:

- System
- Role
- User

- Branch

Policy

N/A

Use AIM Permission

Use the Use AIM permission to specify whether users can open AIM.

Location

In the **Navigation** pane, click **Applications** > **AIM** > **Use AIM**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

View Account Filters Permission

Use the View Account Filters permission to specify whether users can view account filters in AIM.

Location

In the **Navigation** pane, click **Applications** > **AIM** > **View Account Filters**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

View Agencies Permission

Use the View Agencies permission to specify whether users can view agencies in AIM.

Location

In the **Navigation** pane, click **Applications** > **AIM** > **View Agencies**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

View Business Rules Permission

Use the View Business Rules permission to specify whether users can view business rules in AIM.

Location

In the **Navigation** pane, click **Applications** > **AIM** > **View Business Rules**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

View Distribution Templates Permission

Use the View Distribution Templates permission to specify whether users can view distribution templates in AIM.

Location

In the **Navigation** pane, click **Applications** > **AIM** > **View Distribution Templates**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Settings for Auxiliary Products Permission

Use the Settings for Auxiliary Products permission to specify settings to allow Exchange, AIM, AIM Receiver, and Job Manager to create payments in Latitude.

Location

In the **Navigation** pane, click **Applications** > **Auxiliary Products** >**Settings for Auxiliary Products**.

Scope

This permission is available for the System scope only.

Policy

The policy allows your organization to specify the URL and API key that allow Exchange, AIM, AIM Receiver, and Job Manager to create payments. Enable the permission for a scope and then specify the settings.

URL for Processing Financial Transactions Through Collector: URL to display the Batch Processor in Latitude.

API Key for Collector: API key for using the Latitude Web Service.

CUBE Server Config Permission

Use the Server Config permission to specify settings for Latitude CUBE, which is an online data warehouse that provides multidimensional views into transaction-level data for improved data mining.

Location

In the **Navigation** pane, click **Applications** > **Cube** > **Server Config Policy**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch
- Department
- Team
- Desk

Policy

The policy allows your organization to specify the settings for the Latitude CUBE. Enable the permission for a scope and then specify the settings.

Server for the location of the InteractionCollector.Cube: Path to the SQL Analysis Services Server (SSAS) where your organization installed the Latitude CUBE. You can use the Windows server name, IP address, local host, or a named instance.

Analysis Services Database name of the InteractionCollector.Cube: Name of the SQL Analysis Services database that contains the Latitude CUBE. The default name is InteractionCollector.Cube.

Dashboard Settings

Dashboard Settings

Use the Dashboard settings to specify permissions and policies for Dashboard.

Manage Dashboards Permission

Use the Manage Dashboards permission to specify whether users can view, create, and modify the dashboards in Dashboard.

Location

In the **Navigation** pane, click **Applications** > **Dashboard** > **Manage Dashboards**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch
- Department
- Team
- Desk

Policy

N/A

View Dashboards Permission

Use the View Dashboards permission to specify which dashboards a user can view and the default dashboard to display when a user logs on to Dashboard.

Location

In the **Navigation** pane, click **Applications** > **Dashboard** > **View Dashboards**.

Scope

This permission is available for the following scopes:

- System

- Role
- User
- Branch
- Department
- Team
- Desk

Policy

The policy allows your organization to specify the default dashboard to display and which dashboards users can view. Enable the permission for a scope and then select the dashboards.

Home Dashboard: Default dashboard to display when the user logs on to Dashboard.

View Dashboards: If you selected a dashboard, it displays when users log on to Dashboard.

Exchange Settings

Exchange Settings

Use the Exchange settings to specify permissions and policies for Exchange Manager.

Modify Client Configuration Permission

Use the Modify Client Configuration permission to specify whether users can modify configuration items in Exchange Manager.

Location

In the **Navigation** pane, click **Applications** > **Exchange** > **Modify Client Configuration**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Use Exchange Permission

Use the Use Exchange permission to specify whether users can open Exchange Manager.

Location

In the **Navigation** pane, click **Applications** > **Exchange** > **Use Exchange**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Use Fusion Permission

Use the Use Fusion permission to specify whether users can open Fusion.

Location

In the **Navigation** pane, click **Applications** > **Fusion** > **Use Fusion**.

Scope

This permission is available for the all scopes.

Policy

N/A

Liquid Latitude Settings

Liquid Latitude Settings

Use the Liquid Latitude settings to specify permissions and policies for Latitude.

Access Accounts Settings

Access Accounts Settings

Use the Access Accounts settings to specify permissions and policies for viewing and working accounts.

Access Account Permission

Use the Access Account permission to specify whether users can view or work accounts. A user who doesn't have this permission can search for an account but cannot view it in the **Work Form**.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Access Accounts** > **Access Account**.

Scope

This permission is available for all scopes.

Policy

N/A

Access Accounts in Another Desk Permission

Use the Access Accounts in Another Desk permission to specify whether users can view or work accounts assigned to another user's desk.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Access Accounts** > **Access Accounts in Another Desk**.

Scope

This permission is available for all scopes.

Policy

N/A

Access AIM Assigned Account Permission

Use the Access AIM Assigned Account permission to specify whether users can view or work an account assigned to an outside collection agency or attorney. A user who doesn't have this permission can search for an AIM account but cannot view it in the **Work Form**.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Access Accounts** > **Access AIM Assigned Account**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Access Archived Account Permission

Use the Access Archived Account permission to specify whether users can view archived accounts. A user who doesn't have this permission can search for an archived account but cannot view it in the **Work Form**. This permission is not related to the user's permissions to archive or restore accounts.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Access Accounts** > **Access Archived Account**.

Scope

This permission is available for all scopes.

Policy

N/A

Access Outside Branch Permission

Use the Access Outside Branch permission to specify whether users can view accounts not assigned to a desk within the user's assigned branch.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Access Accounts** > **Access Outside Branch**.

Scope

This permission is available for all scopes.

Policy

N/A

Access Restricted Access Accounts Permission

Use the Access Restricted Access Accounts permission to specify whether users can view accounts that have restrictions. This permission is unavailable currently.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Access Accounts** > **Access Restricted Access Accounts**.

Scope

This permission is available for all scopes.

Policy

N/A

Access Returned Account Permission

Use the Access Returned Account permission to specify whether users can view accounts flagged as returned to the client (queue level 999).

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Access Accounts** > **Access Returned Account**.

Scope

This permission is available for all scopes.

Policy

N/A

Configure Data Protection Validation Instructions Permission

Use the Configure Data Protection Validation Instructions permission to specify the instructions to display in the **DPA Validation** dialog box for validating a call.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Access Accounts** > **Configure Data Protection Validation Instructions**.

Scope

This permission is available for the following scopes:

- System
- Business Class
- Client Group
- Client

Policy

The policy allows you to specify the instructions for validating a call. Enable the permission for a scope and then specify the criteria.

Data Validation Instructions: Instructions to users on how to verify that they are speaking to the correct customer or authorized third party before discussing an account.

Queues Settings

Queues Settings

Use the Queues settings to specify permissions and policies for work queues.

Change Continue Queuing Setting Permission

Use the Change Continue Queuing Setting permission to specify whether users can flag an account to include in the Collector queue while it's pending work in a Supervisor or Clerical queue.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Access Accounts** > **Queues** > **Change Continue Queuing Setting**.

Scope

This permission is available for all scopes.

Policy

N/A

Custom Queue Options Permission

Use the Custom Queue Options permission to specify the rules to apply to the Custom queue.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Access Accounts** > **Queues** > **Custom Queue Options**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

The policy allows your organization to specify the rules to apply to the Custom queue. Enable the permission for a scope and specify the settings.

Enforce collector queueing rules: If selected, prevents queueing of accounts assigned to a queue level that doesn't queue, should not queue, or a user contacted the accounts on the current date.

Enforce time zone rules: If selected, prevents queueing of accounts that are not in a callable time zone based on the state and postal code associated to the account.

Queue Providers Permission

Use the Queue Providers permission to specify the queues that are available to the user. For more information, see Work Queues.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Access Accounts** > **Queues** > **Queue Providers**.

Scope

This permission is available for all scopes:

- System
- Role
- User
- Branch

Policy

The policy allows your organization to specify the queues that are available to users. Enable the permission for a scope and then specify the queues. If you select a queue, it's available to users.

Select None: Clears all selected items in the list.

Select All: Selects all items in the list.

> **Tip**: To select multiple sequential queues, press and hold the **Shift** key and then click the first and last sequential queue. To select multiple non-sequential queues, press and hold the **Ctrl** key and then click each individual queue.

Require Data Protection Validation Permission

Use the Require Data Protection Validation permission to specify whether to display a dialog box containing information for validating a caller before displaying the account in the **Work Form**.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Access Accounts** > **Require Data Protection Validation**.

Scope

This permission is available for the following scopes:

- System
- Role
- User

Policy

N/A

Search Permission

Use the Search permission to specify settings for searching for accounts.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Access Accounts** > **Search** > **Search**.

Scope

This permission is available for all scopes.

Policy

The policy allows you to specify settings for searching for accounts. Enable the permission for a scope and then specify the criteria.

Default Quick Search Field: Default criteria available to the user when searching for an account using the "quick search" feature.

Search Fields: If you select a field, it displays on the **Simple** tab in the **Search Accounts** panel.

Search Result Fields: If you select a field, it displays on the **Results** tab in the **Search Accounts** panel.

Select None: Clears all selected items in the list.

Select All: Selects all items in the list.

> **Tip**: To select multiple sequential fields, press and hold the **Shift** key and then click the first and last sequential field. To select multiple non-sequential fields, press and hold the **Ctrl** key and then click each individual field.

View Other User Payments Permission

Use the View Other User Payments permission to specify whether users can view payments that other users processed. For more information, see View Applied and Planned Payments.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Access Accounts** > **View Other User Payments**.

Scope

This permission is available for the following scopes:

- System
- Role
- User

Policy

N/A

Account Actions Settings

Account Actions Settings

Use the Account Actions settings to specify permissions and policies for the actions users can take on accounts.

Access Redirect Portal Permission

Use the Access Redirect Portal permission to specify the web site to open in a new browser tab when a user clicks the link on the account toolbar. No data passes from Latitude to this web site. For more information, see Display a Web Site on a New Browser Tab.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Actions** > **Access Redirect Portal**.

Scope

This permission is available for the following scopes:

- System
- Role
- User

Policy

The policy allows you to specify the web site to display on a new tab in your browser. Enable the permission for a scope and then specify the URL.

URL: Address of the web site to display on a new browser tab.

AIM Place/Recall Functionality Permission

Use the AIM Place/Recall Functionality permission to specify whether users can place an account with an outside collection agency or attorney, and recall the placed account. For more information, see Placements and Recalls.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Actions** > **AIM Place/Recall Functionality**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Allow Creation of Holds Permission

Use the Allow Creation of Holds permission to specify whether users can place collection holds at the account and customer levels. For more information, see Collection Holds.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Actions** > **Allow Creation of Holds**.

Scope

This permission is available for the following scopes:

- System
- Role
- User

Policy

N/A

Allow Manual Linking/Unlinking Permission

Use the Allow Manual Linking/Unlinking permission to specify whether users can link and unlink accounts manually. For more information, see Add a Link to an Account and Remove all Links to an Account.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Actions** > **Allow Manual Linking/Unlinking**.

Scope

This permission is available for the following scopes:

- System
- Role
- User

Policy

N/A

Allow Start/Stop Interest Permission

Use the Allow Start/Stop Interest permission to specify whether users can start and stop client interest on accounts. For more information, see Manage Interest.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Actions** > **Allow Start/Stop Interest**.

Scope

This permission is available for the following scopes:

- System
- Role
- User

Policy

N/A

Auto Close Account Permission

Use the Auto Close Account permission to specify whether users can have the system close an interaction automatically under the following conditions:

- User searches for and selects an account using the Search Accounts or Quick Search feature.
- User moves to the next account in the work queue when working accounts in a queue.
- User closes the work queue when working accounts in a queue.
- User selects another account from inventory.
- User selects another account from account history.

For more information, see Open Interactions.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Actions** > **Auto Close Account**.

Scope

This permission is available for all scopes.

Policy

N/A

Change Desk Permission

Use the Change Desk permission to specify whether users can assign an account to another desk. For more information, see Change a Desk Assignment.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Actions** > **Change Desk**.

Scope

This permission is available for all scopes.

Policy

The policy allows your organization to specify which desks users can move accounts from and indicate desks to which they can reassign accounts. Enable the permission for a scope and then specify the settings.

Restrict the desk from which the user may move the account: If selected, your organization restricts the desks a user can move an account from.

Restrict Desks: Indicates whether the user can move accounts assigned to the specified desks. Valid values are:

- **Allow moving accounts from the following desks:** The user can move accounts from the specified desks.
- **Deny moving accounts from the following desks:** The user cannot move accounts from the specified desks.

Desks: If you selected a desk and the **Allow moving accounts from the following desks** option, users can move accounts from that desk. If you selected a desk and the **Deny moving accounts from the following desks** option, users cannot move accounts from that desk.

Restrict the desk to which the user may move the account: If selected, your organization restricts the desks a user can move an account to.

Restrict Desks: Indicates whether the user can move accounts to the specified desks. Valid values are:

- **Allow moving accounts to the following desks:** The user can move accounts to one of the specified desks.
- **Deny moving accounts to the following desks:** The user cannot move accounts to one of the specified desks.

Desks: If you selected a desk and the **Allow moving accounts to the following desks** option, users can move accounts to that desk. If you selected a desk and the **Deny moving accounts to the following desks** option, users cannot move accounts to that desk.

Select None: Clears all selected items in the list.

Select All: Selects all items in the list.

> **Tip**: To select multiple sequential desks, press and hold the **Shift** key and then click the first and last sequential desk. To select multiple non-sequential desks, press and hold the **Ctrl** key and then click each individual desk.

Change Status Permission

Use the Change Status permission to specify whether users can modify the status code assigned to an account. For more information, see Statuses.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Actions** > **Change Status**.

Scope

This permission is available for all scopes.

Policy

The policy allows your organization to specify which account statuses users can and cannot modify. Enable the permission for a scope and then specify the restrictions.

Restrict the status from which the user may change the account: If selected, your organization restricts the statuses a user can change an account from.

Restrict Statuses: Indicates whether the user can change the status for accounts in the specified statuses. Valid values are:

- **Allow changing accounts from the following statuses:** The user can change the status of accounts in one of the specified statuses.
- **Deny changing accounts from the following statuses:** The user cannot change the status of accounts in one of the specified statuses.

Statuses: If you select a status and the **Allow changing accounts from the following statuses** option, users can change the status of accounts in that status. If you select a status and the **Deny changing accounts from the following statuses** option, users cannot change the status of accounts in that status. For example, you can indicate whether the user can or cannot change the status of accounts that have a "pending" status to some other status.

Restrict the status to which the user may change the account: If selected, your organization restricts the statuses a user can change an account to.

Restrict Statuses: Indicates whether the user can change account statuses to the specified statuses. Valid values are:

- **Allow changing accounts to the following statuses:** The user can change the status of accounts to one of the specified statuses.

- **Deny changing accounts to the following statuses:** The user cannot change the status of accounts to one of the specified statuses.

Statuses: If you select a status and the **Allow changing accounts to the following statuses** option, users can change the status of accounts to that status. If you select a status and the **Deny changing accounts to the following statuses** option, users cannot change the status of accounts to that status. For example, you can indicate whether the user can or cannot change accounts to a "pending" status.

Select None: Clears all selected items in the list.

Select All: Selects all items in the list.

> **Tip**: To select multiple sequential statuses, press and hold the **Shift** key and then click the first and last sequential status. To select multiple non-sequential statuses, press and hold the **Ctrl** key and then click each individual status.

Require Note on Account Permission

Use the Require Note on Account permission to specify whether your organization requires the user to add a note to accounts before moving to another account in the Collector queue.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Actions** > **Require Note on Account**.

Scope

This permission is available for all scopes.

Policy

The policy allows you to specify whether users must add notes containing action or result codes that meet specific criteria before moving to the next account in the Collector queue. Enable the permission for a scope and then specify the settings.

Require a note with an action or result code that is considered as worked: If selected, the user cannot continue in the queue until adding a note with an action or result code signifying a worked account.

Require a note with an action code that is considered as attempted: If selected, the user cannot continue in the queue until adding a note with an action code signifying an attempted contact.

Set Follow-up Date Permission

Use the Set Follow-up Date permission to specify whether users can set follow-up dates on accounts. For more information, see Set an Account Follow-up Date.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Actions** > **Set Follow-up Date**.

Scope

This permission is available for the following scopes:

- System
- Role

- User
- Branch

Policy

N/A

Set Reminders for Others Permission

Use the Set Reminders for Others permission to specify whether users can set a reminder for accounts assigned to another desk. For more information, see Set a Timed Reminder.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Actions** > **Set Reminders**.

Scope

This permission is available for all scopes.

Policy

N/A

Account Data Settings

Account Data Settings

Use the Account Data settings to specify permissions and policies for account data.

Care and Financial Hardship Panel Permission

Use the Care and Financial Hardship Panel permission to configure the **Care and Financial Hardship** panel. For more information, see Care and Financial Hardship.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Care and Financial Hardship** > **Care and Financial Hardship Panel Config**.

Scope

This permission is available for the following scopes:

- System
- Role
- User

Policy

The policy allows your organization to configure the **Care and Financial Hardship** panel. Enable the permission for a scope and then specify the settings.

View Care Types: If selected, users can view care types.

Edit Care: If selected, users can modify care information.

Approve Hold Days: If selected, users can approve the number of days to place the account on hold to suspend collection activity.

Override Hold Days: If selected, users can override the default number of days to place the account on hold to suspend collection activity.

Edit the Care and Financial Hardship Comment: If selected, users can add or modify comments regarding a care or financial hardship case.

Complaints Panel Permission

Use the Complaints Panel permission to configure the **Complaints** panel. For more information, see Complaints.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Complaints** > **Complaints Panel Config**.

Scope

This permission is available for the following scopes:

- System
- Role
- User

Policy

The policy allows your organization to configure the **Complaints** panel. Enable the permission for a scope and then specify the settings.

Close Complaint: If selected, users can close complaints.

Reopen Complaint: If selected, users can reopen complaints.

Edit Compensation Amount: If selected, users can specify the compensation amount.

View Compensation Amount: If selected, users can view the compensation amount.

View Complaint Outcome: If selected, users can view the outcome of a complaint.

View Complaint Details: If selected, users can view details about a complaint.

Assign Complaint Owner: If selected, users can assign an owner to the complaint.

Assign and Edit Department: If selected, users can assign a department to the complaint.

Assign and Edit Complaint Category: If selected, users can assign a category to the complaint.

Edit Complaint Against: If selected, users can specify who the complaint is against.

Edit Referred by: If selected, users can specify who referred the customer.

Edit Investigation to Date: If selected, users can modify the details of the investigation.

Edit Conclusion: If selected, users can modify the complaint conclusion.

Edit Complaint Justified: If selected, users can specify whether the complaint is justified.

Edit Complaint Outcome: If selected, users can specify the outcome of the complaint.

Enable Existing Complaint Button: If selected, users can remove a duplicate complaint.

Edit Complaint Status: If selected, users can specify the status of the complaint.

Edit Root Cause: If selected, users can modify the root cause of the complaint.

Credit Reporting Settings

Credit Reporting Settings

Use the Credit Reporting settings to specify permissions and policies for reporting accounts to credit bureaus.

Allow Delete Options Permission

Use the Allow Delete Options permission to specify whether users can delete accounts from credit reporting for reasons such as reported in error, fraud, or account paid by insurance. For more information, see the following topics:

- Send Delete Request for Account Reported in Error
- Send Delete Request for Account Reported Based on Fraud
- Send Delete Request for Medical Account

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Credit Reporting** > **Allow Delete Options.**

Scope

This permission is available for all scopes.

Policy

N/A

Allow Manual Evaluation Permission

Use the Allow Manual Evaluation permission to specify whether users can run a manual evaluation of an account for credit reporting purposes. For more information, see Evaluate an Account for Credit Reporting.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Credit Reporting** > **Allow Manual Evaluation**.

Scope

This permission is available for all scopes.

Policy

N/A

Allow Prevent Flag and Undo Delete Permission

Use the Allow Prevent Flag and Undo Delete permission to specify whether users can undo credit reporting delete requests for the following:

- Accounts reported in error.
- Accounts with a customer who is a victim of fraud.
- Accounts that insurance is paying or paid in full.

For more information, see Undo a Credit Reporting Delete Request.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Credit Reporting** > **Allow Prevent Flag and Undo Delete**.

Scope

This permission is available for all scopes.

Policy

N/A

Alter Credit Reporting Settings Permission

Use the Alter Credit Reporting Settings permission to specify whether users can modify credit reporting settings. For more information, see Credit Bureau Reporting.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Credit Reporting** > **Alter Credit Reporting Settings**.

Scope

This permission is available for all scopes.

Policy

N/A

Utility Tab Permission

Use the Utility Tab permission to specify whether to display or hide the **Utility** tab on the **CB Reporting** panel. For more information, see Manage Miscellaneous CBR Settings.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Credit Reporting** > **Utility Tab**.

Scope

This permission is available for the following scopes:

- System
- Role

- User

Policy

N/A

Disputes Panel Permission

Use the Disputes Panel permission to configure the **Disputes** panel. For more information, see Disputes.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Disputes** > **Disputes Panel Config**.

Scope

This permission is available for the following scopes:

- System
- Role
- User

Policy

The policy allows your organization to configure the **Disputes** panel. Enable the permission for a scope and then specify the settings.

Edit Dispute Type: If selected, users can specify the dispute type.

Edit Received Date: If selected, users can specify the dispute received date.

Edit Referred by: If selected, users can specify who referred the customer.

Edit Dispute Details: If selected, users can specify the details of the dispute.

Edit Dispute Category: If selected, users can specify the dispute category.

Edit Dispute Against: If selected, users can specify who the dispute is against.

Edit Dispute Justified: If selected, users can specify whether the dispute is justified.

Edit Dispute Outcome: If selected, users can specify the outcome of the dispute.

Documentation Settings

Documentation Settings

Use the Documentation settings to specify permissions and policies for account documentation.

Attach Documentation Permission

Use the Attach Documentation permission to specify whether users can attach documentation to accounts. For more information, see Attach a Document to an Account.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Documentation** > **Attach Documentation**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch
- Business Class
- Client Group
- Client

Policy

The policy allows your organization to specify which document categories are available to users when attaching documents to accounts. Enable the permission for a scope and then specify the codes.

Permitted Categories: If you select a documentation category, it's available when users attach documents to accounts. For information about creating documentation categories, see Documentation Categories.

Select None: Clears all selected items in the list.

Select All: Selects all items in the list.

> **Tip**: To select multiple sequential categories, press and hold the **Shift** key and then click the first and last sequential category. To select multiple non-sequential categories, press and hold the **Ctrl** key and then click each individual category.

Delete Documentation Permission

Use the Delete Documentation permission to specify whether users can delete documentation attached to accounts. For more information, see Delete a Document From an Account.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Documentation** > **Delete Documentation**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch
- Business Class
- Client Group

- Client

Policy

N/A

View Attached Documents Permission

Use the View Attached Documents permission to specify whether users can view documents that are attached to accounts. For more information, see View Documents Attached to an Account.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Documentation** > **View Attached Documents**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch
- Business Class
- Client Group
- Client

Policy

The policy allows your organization to specify which documentation categories are available to users when viewing documents that are attached to accounts. Enable the permission for a scope and then specify the codes.

Permitted Categories: If you select a documentation category, it's available when users view documents attached to accounts. For information about creating documentation categories, see Documentation Categories.

Select None: Clears all selected items in the list.

Select All: Selects all items in the list.

> **Tip**: To select multiple sequential categories, press and hold the **Shift** key and then click the first and last sequential category. To select multiple non-sequential categories, press and hold the **Ctrl** key and then click each individual category.

Extra Data Settings

Extra Data Settings

Use the Extra Data settings to specify permissions and policies for custom data.

Create Extra Data Permission

Use the Create Extra Data permission to specify whether users can add custom data. For more information, see Add Extra Data.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Extra Data** > **Create Extra Data**.

Scope

This permission is available for all scopes.

Policy

N/A

Update Extra Data Permission

Use the Update Extra Data permission to specify whether users can modify custom data. For more information, see Modify Extra Data.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Extra Data** > **Update Extra Data**.

Scope

This permission is available for all scopes.

Policy

N/A

Fusion Services - Verify Responses Permission

Use the Fusion Services - Verify Responses permission to specify whether users can flag the responses received from outside vendors as verified. For more information, see Verify a Response From an Outside Service Provider.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Fusion Services** > **Verify Responses**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Income and Expenditure Settings

Income and Expenditure Settings

Use the Income and Expenditure settings to specify permissions and policies for income and expenditures.

Maintain Income and Expense Items Permission

Use the Maintain Income and Expense Items permission to specify whether users can add and modify income, expenditure, and arrears information in the **Income and Expenditure** panel. For more information, see Income and Expenditures.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Income & Expenditure** > **Maintain Income & Expense Items**.

Scope

This permission is available for the following scopes:

- System
- Role
- User

Policy

N/A

Trigger Values Permission

Use the Trigger Values permission to specify the Common Financial Statement trigger values for expenditures. For more information, see Add Expenses.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Income & Expenditure** > **Trigger Values**.

Scope

This permission is available for the System scope only.

Policy

The policy allows your organization to configure trigger values for income and expenditures. Enable the permission for a scope and then specify the settings.

Specify the trigger values for each category of person: first adult, other adults, children under 14, and children aged 14-18.

Phone: Maximum amount that your organization considers normal for telephone expenses.

Travel: Maximum amount that your organization considers normal for travel expenses. Travel expenses include car tax, insurance, fuel, and other travel expenses such as public transport.

Housekeeping: Maximum amount that your organization considers normal for housekeeping expenses.

Other: Maximum amount that your organization considers normal for other expenses.

Labels - User Policy Permission

Use the User Policy permission to specify whether users can create, assign, view, or delete account labels. You can use account labels to flag accounts for your own purpose. For example, you can use account labels as tags, conditions, or properties. For more information, see Account Labels Card.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Labels** > **User Policy**.

Scope

This permission is available for all scopes.

Policy

The policy allows your organization to specify whether users can view, add, associate, and delete account labels. Enable the permission for a scope and then specify the settings.

User can Add an Existing Label to an Account: Allows the user to select an existing label and associate it to an account.

User can Create and Add a Newly Defined Label to an Account: Allows the user to create account labels and add them to accounts.

User can Delete a label from an Account: Allows the user to delete labels from accounts.

Legal Settings

Legal Settings

Use the Legal settings to specify permissions and policies for legal judgments against accounts.

Award/Reverse Judgment Permission

Use the Award/Reverse Judgment permission to specify whether users can award and reverse judgments on accounts. For more information, see Award a Judgment.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Legal** > **Award/Reverse Judgment**.

Scope

This permission is available for the following scopes:

- System
- Role
- User

Policy

N/A

Delete Legal Case Permission

Use the Delete Legal Case permission to specify whether users can delete legal cases. For more information, see Delete a Legal Case.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Legal** > **Delete Legal Case**.

Scope

This permission is available for the following scopes:

- System
- Role
- User

Policy

N/A

Judgment Award Bucket Mappings Permission

Use the Judgment Award Bucket Mappings permission to map judgment awards to the money buckets to which to apply the award. For more information, see Award a Judgment.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Legal** > **Judgment Award Bucket Mappings**.

Scope

This permission is available for the System scope only.

Policy

The policy allows your organization to specify the money buckets to which to apply judgment awards. Enable the permission for a scope and then specify the settings.

> **Note:** The values in the list boxes are based on money titles that your organization specified in system configuration. For more information, see Maintain Money Titles.

Principal Award: Money bucket in which to store the judgment amount awarded for principal.

Interest Award: Money bucket in which to store the judgment amount awarded for interest.

Court Cost Award: Money bucket in which to store the judgment amount awarded for court costs.

Attorney Cost Award: Money bucket in which to store the judgment amount awarded for attorney costs.

OtherCost1 Award through **OtherCost5 Award:** Money buckets in which to store the judgment amount awarded for other costs.

Miscellaneous Cost Award: Money bucket in which to store the judgment amount awarded for miscellaneous costs.

Update Interest Permission

Use the Update Interest permission to specify whether users can update interest for the linked accounts in a judgment. For more information, see Update Interest on Linked Accounts in a Judgment.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Legal** > **Update Interest**.

Scope

This permission is available for the following scopes:

- System
- Role
- User

Policy

N/A

Letters Settings

Letters Settings

Use the Letters settings to specify permissions and policies for letter requests.

Delete Request Permission

Use the Delete Request permission to specify whether users can delete pending letter requests and system-generated letter requests. If you enable the permission, users can delete pending letter requests that the user created. For more information, see Delete a Pending Letter Request.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Letters** > **Delete Request**.

Scope

This permission is available for all scopes.

Policy

The policy allows your organization to specify whether users can delete system-generated letter requests. Enable the permission for a scope and then specify the settings.

Can delete system generated letters: If selected, the user can delete system-generated letter requests.

OnHold Request Permission

Use the OnHold Request permission to specify whether users can place pending letter requests on hold for an account. For more information, see Suspend a Pending Letter Request.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Letters** > **OnHold Request**.

Scope

This permission is available for all scopes.

Policy

N/A

Linked Letters Permission

Use the Linked Letters permission to specify whether users can specify the linked accounts to include when requesting a letter that can include linked accounts. For more information, see Request a Letter.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Letters** > **Linked Letters**.

Scope

This permission is available for all scopes.

Policy

N/A

Request Permission

Use the Request permission to specify whether users can request a letter for an account. For more information, see Request a Letter.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Letters** > **Request**.

Scope

This permission is available for all scopes.

Policy

N/A

Misc Extra Data Settings

Misc Extra Data Settings

Use the Misc Extra Data settings to specify permissions and policies for miscellaneous extra data. Miscellaneous extra data is any type of information related to an account that users cannot record elsewhere within Latitude.

Create Misc Extra Data Permission

Use the Create Misc Extra Data permission to specify whether users can add miscellaneous extra data. For more information, see Add Miscellaneous Extra Data.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Misc Extra Data** > **Create Misc Extra Data**.

Scope

This permission is available for all scopes.

Policy

N/A

Update Misc Extra Data Permission

Use the Update Misc Extra Data permission to specify whether users can modify miscellaneous extra data. For more information, see Modify Miscellaneous Extra Data.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Misc Extra Data** > **Update Misc Extra Data**.

Scope

This permission is available for all scopes.

Policy

N/A

Name Template Config Permission

Use the Name Template Config permission to specify the format to use to display names in Latitude.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Name Template Config**.

Scope

This permission is available for the system scope only.

Policy

The policy allows your organization to specify the format for displaying names. Enable the permission for a scope and then specify the settings.

Template: Template to apply to names when displaying them in Latitude. The order in which you place the tokes is the order the system displays them in Latitude. Place formatting outside the curly brackets. For example, to display names in the system as "Doe, John E", type the following:

{{last}}, {{first}} {{middle}}

Notes Settings

Notes Settings

Use the Notes settings to specify permissions and policies for account notes.

Allow Redaction Permission

Use the Allow Redaction permission to specify whether users can redact (obscure) all or a portion of a note comment. For more information, see Redact an Account Note Comment.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Notes** > **Allow Redaction**.

Scope

This permission is available for all scopes.

Policy

N/A

Create Notes Permission

Use the Create Notes permission to specify whether users can add notes to accounts. For more information, see Add an Account Note.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Notes** > **Create Notes**.

Scope

This permission is available for all scopes.

Policy

The policy allows your organization to specify which action and result codes are available to users when adding notes to an account. Enable the permission for a scope and then specify the codes.

Restrict the available action codes to the following: If selected, the action codes available to users only includes the ones specified.

Action Codes: If you select an action code, it's available when users add notes to accounts.

Restrict the available result codes to the following: If selected, the result codes available to users only include the ones specified.

Result Codes: If you select a result code, it's available when users add notes to accounts.

Select None: Clears all selected items in the list.

Select All: Selects all items in the list.

> **Tip**: To select multiple sequential codes, press and hold the **Shift** key and then click the first and last sequential code. To select multiple non-sequential codes, press and hold the **Ctrl** key and then click each individual code.

Create Private Notes Permission

Use the Create Private Notes permission to specify whether users can add private notes to accounts. Only users who have the **View Private Notes** permission can see private notes. For more information, see Add an Account Note.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Notes** > **Create Private Notes**.

Scope

This permission is available for all scopes.

Policy

N/A

View Private Notes Permission

Use the View Private Notes permission to specify whether users can view private notes on accounts. For more information, see View Account Notes.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Notes** > **View Private Notes**.

Scope

This permission is available for all scopes.

Policy

N/A

Parties Settings

Parties Settings

Use the Parties settings to specify permissions and policies for the parties on accounts.

Update Address Permission

Use the Update Address permission to specify whether users can modify the addresses on accounts. For more information, see Modify an Address.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Parties** > **Update Address**.

Scope

This permission is available for all scopes.

Policy

N/A

Update Name Permission

Use the Update Name permission to specify whether users can modify the names on accounts. For more information, see Maintain Contact Information.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Parties** > **Update Name**.

Scope

This permission is available for all scopes.

Policy

N/A

Update Name Alias Permission

Use the Update Name Alias permission to specify whether users can modify the alias names on accounts. For more information, see Maintain Contact Information.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Parties** > **Update Name Alias**.

Scope

This permission is available for all scopes.

Policy

N/A

Update Responsibility - Add Permission

Use the Update Responsibility - Add permission to specify whether users can designate the party responsible for an account. For more information, see Maintain Contact Information.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Parties** > **Update Responsibility - Add**.

Scope

This permission is available for all scopes.

Policy

N/A

Update Responsibility - Remove Permission

Use the Update Responsibility - Remove permission to specify whether users can indicate that a party on an account is not responsible for the account. For more information, see Maintain Contact Information.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Parties** > **Update Responsibility - Remove**.

Scope

This permission is available for all scopes.

Policy

N/A

Update SSN Permission

Use the Update SSN permission to specify whether users can modify an SSN on an account. This permission is not in use currently.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Parties** > **Update SSN**.

Scope

This permission is available for all scopes.

Policy

N/A

View SSN Permission

Use the View SSN permission to specify whether users can view SSNs on accounts. This permission is not in use currently.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Parties** > **View SSN**.

Scope

This permission is available for all scopes.

Policy

N/A

Phones Settings

Phones Settings

Use the Phones settings to specify permissions and policies for phone numbers associated to accounts.

Change Phone Consent Permission

Use the Change Phone Consent permission to specify whether users can modify the permission to call, auto-dial, text, or fax a phone number. For more information, see Add a Phone Number to an Account and Modify an Account Phone Number.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Phones** > **Change Phone Consent**.

Scope

This permission is available for all scopes.

Policy

N/A

Create Phone Numbers Permission

Use the Create Phone Numbers permission to specify whether users can add phone numbers to accounts. For more information, see Add a Phone Number to an Account.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Phones** > **Create Phone Numbers**.

Scope

This permission is available for all scopes.

Policy

N/A

Mask Phone Numbers Permission

Use the Mask Phone Numbers permission to specify whether to mask all phone number occurrences in the **Work Form**.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Phones** > **Mask Phone Numbers**.

Scope

This permission is available for the System scope only.

Policy

The policy allows your organization to specify the settings for masking phone numbers in the **Work Form**. Enable the permission for a scope and then specify the settings.

Trailing Digits to Display: Number of trailing digits in the phone number to display in Latitude instead of asterisks (*). For example, if you type "2", the last two digits of the phone number display in Latitude and the remaining digits appear as asterisks.

Update Phone Numbers Permission

Use the Update Phone Numbers permission to specify whether users can modify phone numbers on accounts. For more information, see Modify a Phone Number on an Account.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Phones** > **Update Phone Numbers**.

Scope

This permission is available for all scopes.

Policy

N/A

Update Phone Status Permission

Use the Update Phone Status permission to specify whether users can modify the status of phone numbers on accounts. For more information, see Change the Status of an Account Phone Number or Modify a Phone Number on an Account.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Phones** > **Update Phone Status**.

Scope

This permission is available for all scopes.

Policy

N/A

Update Phone Type Permission

Use the Update Phone Type permission to specify whether users can modify the phone types on accounts. For more information, see Modify a Phone Number on an Account.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Phones** > **Update Phone Type**.

Scope

This permission is available for all scopes.

Policy

N/A

Scheduled Payments Settings

Scheduled Payments Settings

Use the Scheduled Payments settings to specify permissions and policies for scheduled payments.

Allow Overpayments Permission

Use the Allow Overpayments permission to specify whether to allow payment arrangements that exceed the account balance and if so, the maximum overpayment percentage allowed. For more information, see Propose a Payment Arrangement.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Scheduled Payments** > **Allow Overpayments**.

Scope

This permission is available for the following scopes:

- System
- Business Class
- Client
- Client Group

Policy

The policy allows your organization to specify the settings for overpayments. Enable the permission for a scope and then specify the setting.

Maximum Over Payment Percent (0 = No Limit): Maximum percentage of the account balance that users are allowed to increase the payment by when scheduling overpayments. For example, if the account balance is $100 and the maximum overpayment percentage allowed is 10%, users cannot create an overpayment arrangement for more than $110. If you specify zero (0), no limitation applies.

Create Scheduled Payments Permission

Use the Create Scheduled Payments permission to specify the settings for scheduling payments on an account. For more information, see Arrangements.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Scheduled Payments** > **Create Scheduled Payments**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

The policy allows your organization to specify the settings for scheduling payments on an account. Enable the permission for a scope and then specify the settings.

Minimum Payment Amount: Minimum amount required for a payment where no future scheduled payments exist, or the first payment in the arrangement.

Maximum Days to Payment: Maximum number of days into the future that you can post-date the payment or first payment in the arrangement.

Minimum Balance to Create an Arrangement: Minimum account balance required to create a payment arrangement.

Basis for Minimum Balance: Amount that represents the minimum balance.

Allow Mixing of Payment Types for an Arrangement: If selected, the user can include more than one payment type in a payment arrangement.

Allow Overpayments for Ad Hoc Payments: If selected, the user can schedule a payment when the payment is more than the current balance less the sum of the existing scheduled payments.

Accrue Interest: If selected, arrangements accrue interest.

Settlements Not Allowed: If selected, users cannot create SIF arrangements.

Maximum Total Number of Scheduled Payments (0 = unlimited): Maximum number of payments that the payment arrangement can include. If you specify zero (0), no limitation applies.

Minimum Subsequent Payment Amount: Minimum amount required for all payments that follow the first payment in the arrangement.

Minimum Days Between Payments (0 = disable): Minimum number of days required between payments in the payment arrangement. If you specify zero (0), no limitation applies.

Maximum Days Between Payments (0 = disable): Maximum number of days required between payments in the payment arrangement. If you specify zero (0), no limitation applies.

Maximum Days to Last Payment (0 = disable): Maximum number of days into the future from the current date that the user can create the last payment in the payment arrangement.

Maximum Balance Not to Exceed: Maximum amount the account balance cannot exceed.

Accepted Payment Types: If you select a payment type, it's available when users create or reschedule scheduled payments.

Accepted Credit Cards: If you select a credit card type, it's available when users create or reschedule scheduled payments.

Filter Payment Frequencies: If selected, only the frequencies selected in the **Acceptable Payment Frequencies** list box are available when users create or reschedule scheduled payments. If cleared, all payment frequencies are available when users create or reschedule scheduled payments, regardless of what you have selected in the **Acceptable Payment Frequencies** list box.

Acceptable Payment Frequencies: If you select a payment frequency and select the **Filter Payment Frequencies** check box, the payment frequency is available when users create or reschedule scheduled payments. If you select a payment frequency and clear the **Filter Payment Frequencies** check box, all payment frequencies are available when users create or reschedule scheduled payments.

Select None: Clears all selected items in the list.

Select All: Selects all items in the list.

> **Tip**: To select multiple sequential payment or credit card types, press and hold the **Shift** key and then click the first and last sequential payment or credit card type. To select multiple non-sequential payment or credit card types, press and hold the **Ctrl** key and then click each individual payment or credit card type.

Credit Cards Permission

Use the Credit Cards permission to specify the settings for credit cards. For more information, see Add a Credit Card.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Scheduled Payments** > **Credit Cards**.

Scope

This permission is available for the System scope only.

Policy

The policy allows your organization to specify whether the user can include the credit card security code and whether your organization requires the security code. Enable the permission for a scope and then specify the settings.

Allow entry of credit card security code: If selected, the user can include the credit card security code when adding a credit card payment to an account.

Require credit card security code: If selected, your organization requires the user to provide the credit card security code when adding a credit card payment to an account.

Allow entry of credit card postal code: If selected, the user can include the credit card postal code when adding a credit card payment to an account.

Require credit card postal code: If selected, your organization requires the user to provide the credit card postal code when adding a credit card payment to an account.

Allow entry of credit card street 1: If selected, the user can include the credit card street address line 1 when adding a credit card payment to an account.

Require credit card street 1: If selected, your organization requires the user to provide the credit card street address line 1 when adding a credit card payment to an account.

Mask data when typing credit card account number: If selected, when the user types the credit card account number, the system replaces the typed characters with periods.

Require dual entry of credit card account number for validation: If selected, the user must type the credit card account number twice for validation purposes. If the numbers don't match, an error message displays.

Direct Debit Permission

Use the Direct Debit permission to specify the settings for Direct Debits. For more information, see Add a Direct Debit Account.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Scheduled Payments** > **Direct Debit**.

Scope

This permission is available for the System scope only.

Policy

The policy allows your organization to specify the threshold for scheduling first and subsequent Direct Debit payments. Enable the permission for a scope and then specify the settings.

Lead-time Days threshold for first payment: Minimum number of days from the current date that a user can schedule the first Direct Debit payment. For example, if the current date is "April 28, 2016" and the threshold is "7," the user cannot schedule the first payment until May 5, 2016 or later.

Direct Debit Client Representment Rules Permission

Use the Direct Debit Client Representment Rules permission to specify the rules for representing returned Direct Debit payments.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Scheduled Payments** > **Direct Debit Client Representment Rules**.

Scope

This permission is available for the following scopes:

- Client
- Client Group
- Business Class

Policy

The policy allows your organization to specify the rules for representing returned payments. Enable the permission for a scope and then specify the settings.

Allow payments to be represented: If selected, users can represent returned payments.

Represent in Care: If selected, users can represent returned payments for accounts that are in care.

Minimum amount to represent: Minimum payment amount required to represent.

Days in future to represent on processing a return: Number of days after processing the error file to schedule the payment for representment.

Maximum days from return to represent: Maximum number of days after which a user can no longer represent the payment. The calculation starts from the returned payment receipt date.

Direct Debit Guarantee Entity Name Permission

Use the Direct Debit Guarantee Entity Name permission to specify the entity who is guaranteeing Direct Debits.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Scheduled Payments** > **Direct Debit Guarantee Entity Name**.

Scope

This permission is available for the System scope only.

Policy

The policy allows your organization to specify the entity who is guaranteeing Direct Debits. Enable the permission for a scope and then specify the entity.

Entity used in Direct Debit Guarantee: Name of the entity who is guaranteeing Direct Debits..

Scheduled Payments - User Policy Permission

Use the User Policy permission to specify the actions a user can take when scheduling or modifying a payment on an account. For more information, Arrangements.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Scheduled Payments** > **User Policy**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

The policy allows your organization to specify the actions a user can take when creating or modifying scheduled payments. Enable the permission for a scope and then specify the settings.

Allow user to bypass business rules when scheduling or editing payments: If selected, the user can bypass the payment business rules.

Allow user to suppress surcharge assessment on new arrangements: If selected, the user can remove the surcharge on a new arrangement.

Allow Updating of Scheduled Payments entered by Other Users: If selected, allows the user to modify scheduled payments that other users created.

Allow User to Update Their Own Scheduled Payments: If selected, allows the user to modify scheduled payments that the user created.

Allow Updating of Scheduled Payments Hold Flag: If selected, allows the user to place a scheduled payment on hold and release the hold.

Maximum Total Number of Scheduled Payments (0 = unlimited): Maximum number of scheduled payments allowed. If blank or zero, there is no maximum limit.

Allow saving Payment Instrument to Wallet: If selected, allows the user to save a payment instrument to a customer's wallet.

Allow deleting Payment Instrument from Wallet: If selected, allows the user to delete a payment instrument from a customer's wallet.

Allow lookup of previously used Payment Instruments not saved in Wallet: If selected, allows the user to look up payment instruments previously used on an account and not saved to a customer's wallet.

% Allowed Below Minimum: Percent below the minimum settlement amount allowed before requiring supervisor approval.

Update User Date 1 Permission

Use the Update User Date 1 permission to specify whether users can modify dates for the user-defined date 1 box. For more information, see View or Modify Account Dates.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Update User Date 1**.

Scope

This permission is available for all scopes.

Policy

N/A

Update User Date 2 Permission

Use the Update User Date 2 permission to specify whether users can modify dates for the user-defined date 2 box. For more information, see View or Modify Account Dates.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Update User Date 2**.

Scope

This permission is available for all scopes.

Policy

N/A

Update User Date 3 Permission

Use the Update User Date 3 permission to specify whether users can modify dates for the user-defined date 3 box. For more information, see View or Modify Account Dates.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Update User Date 3**.

Scope

This permission is available for all scopes.

Policy

N/A

Warnings Settings

Warnings Settings

Use the Warnings settings to specify permissions and policies for displaying state and time zone warnings.

Display State Warnings Permission

Use the Display State Warnings permission to specify whether state warnings display when viewing an account for a state with restrictions. For more information, see View Account Warnings.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Warnings** > **Display State Warnings**.

Scope

This permission is available for all scopes.

Policy

N/A

Display Time Zone Warnings Permission

Use the Display Time Zone Warnings permission to specify whether a warning displays when viewing an account during a restricted time period. Latitude calculates the time based on the postal code associated to the account. For more information, see View Account Warnings.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Warnings** > **Display Time Zone Warnings**.

Scope

This permission is available for all scopes.

Policy

N/A

Warning Dialog Permission

Use the Warning Dialog permission to specify whether warnings appear automatically for accounts displayed in the **Work Form**. For more information, see View Account Warnings.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Account Data** > **Warnings** > **Warning Dialog Policy**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

The policy allows your organization to specify under what conditions warning messages display. Enable the permission for a scope and then specify the condition.

Display Behavior: Condition under which warnings display automatically. Valid values are:

- **Always display warning dialog:** Displays warning messages when an account displays in the **Work Form** even when no warnings exist for the account.
- **Only display warning dialog if warnings exist:** Displays warning messages when an account displays in the **Work Form** only when warnings exist for the account.

> **Note:** If your organization disabled the permission or didn't configure it, Latitude doesn't display warning messages automatically when an account displays in the **Work Form**. However, if warnings exist for an account, users can click an option in the menu bar to display the warning messages.

Applicable Processes and Stages Permission

Use the Applicable Processes and Stages permission to select the processes and stages available to users in the **Work Form**. For more information, see Process Stages.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Process Orchestration** > **Applicable Processes and Stages**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Business Class
- Client Group
- Client

Policy

The policy allows your organization to specify which processes are available to users and which stages within that process that users can move accounts through. Enable the permission for a scope and then select the allowed processes and stages. If you select a process and stage, it's available to users.

Conditions: If you select a condition (process and stage), it's available to users in the **Work Form**.

> **Tip**: To select multiple sequential conditions, press and hold the **Shift** key and then click the first and last sequential condition. To select multiple non-sequential conditions, press and hold the **Ctrl** key and then click each individual condition.

Dialer Functionality Settings

Dialer Functionality Settings

Use the Dialer Functionality settings to specify permissions and policies for the Dialer Agent Interface.

Dialer Permission

Use the Dialer permission to specify whether to display the **Dialer Agent Interface** in the **Work Form**.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Dialer Functionality** > **Dialer**.

Scope

This permission is available for the following scopes:

- System
- Role

- User

Policy

The policy allows your organization to specify the settings for displaying the **Dialer Agent Interface** in the **Work Form**. Enable the permission for a scope and then specify the settings.

Type of Dialer: Type of dialer to display in the **Work Form**.

Server Name: Name of your dialer server.

Dialer Client URL: Web address >>>> ORIGINAL //liquid/lava_su12/int/src/Products/Documentation/Source/Interaction_Collector_Help/Dialer_Permission.htm#6 for the Interaction Dialer client.

Dialer API: Not available.

Token: Not available.

Default Result Code: Result code to use when the agent selects a disposition code that doesn't map to a Latitude result code.

Disposition Code Mappings: Allows you to map disposition codes from your dialer server to result codes in Latitude. For more information about mapping codes, see Map a Disposition Code to a Result Code.

Disposition Code: Dialer server disposition code to map to the Latitude result code.

Result Code: Latitude result code to map to the dialer disposition code.

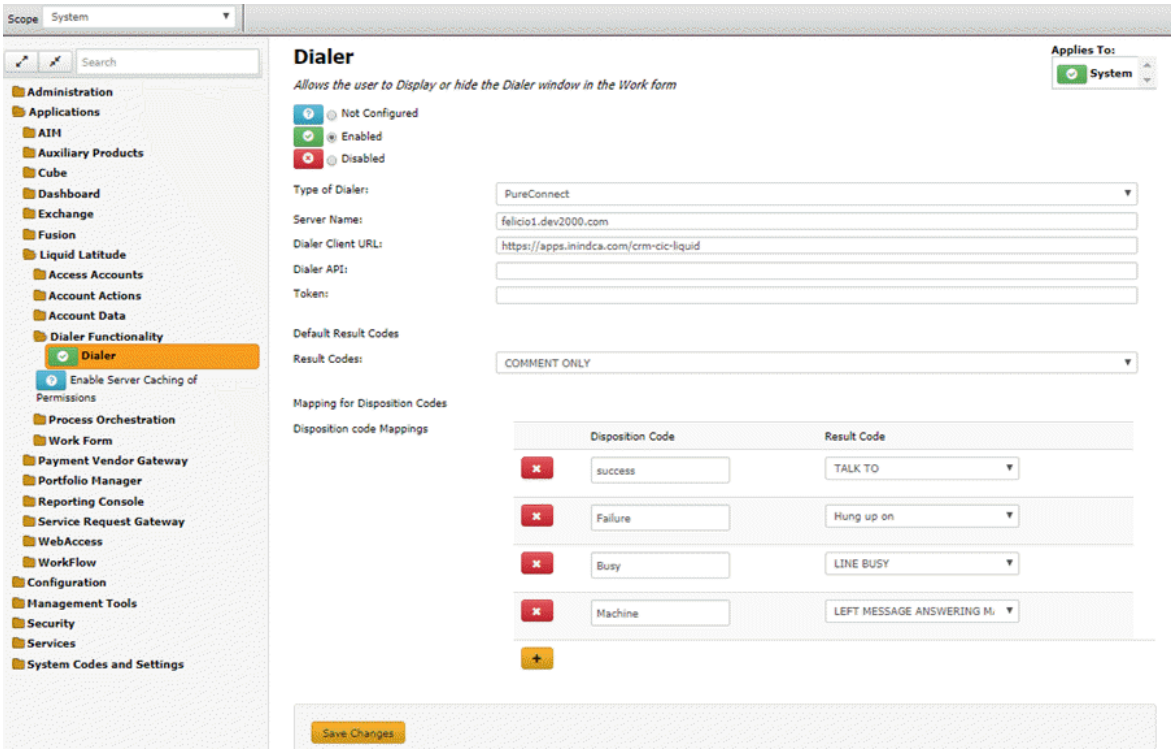
Related Topics

Map a Disposition Code to a Result Code

Use the **Dialer** panel to map disposition codes from your Dialer server to result codes in Latitude.

To map a disposition code to a result code

1. In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Dialer Functionality** > **Dialer**.



Disposition Code: Dialer server disposition code to map to the Latitude result code.

Result Code: Latitude result code to map to the Dialer server disposition code.

> **Note:** This code must match exactly to an existing disposition that you mapped in the Script in Interaction Administrator.

2. Click the plus sign (+). A blank row appears in the data grid.
3. Complete the information and then click **Save Changes**.

> **Note:** To modify a mapping, type or select a new value and then save it. To delete a mapping, click the Delete icon.

Enable Server Caching of Permissions

Use the Enable Server Caching of Permissions permission to turn on or off the caching of permissions. When you turn on caching, the system attempts to retrieve permission settings from the cache. If the permission setting isn't in the cache, the system retrieves the permission setting from the database and stores it in the cache for future retrieval. When a user modifies a permission, the system clears the cache. When you turn off caching, the system retrieves permission settings from the database.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Enable Server Caching of Permissions**.

Scope

This permission is available for all scopes.

Policy

N/A

Work Form Settings

Work Form Settings

Use the Work Form settings to specify which components appear in the **Work Form**.

Anchor Permission

Use the Anchor permission to specify the account anchor to display in the **Work Form**. For more information, see Delinquency or Recovery Anchor.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Work Form** > **Anchor**.

Scope

This permission is available for the System scope only.

Policy

The policy allows your organization to specify the default anchor to display in the **Work Form** (for example, delinquency or recovery)**.** Enable the permission for a scope and then specify the default anchor to display.

Anchor Follow-up Data Permission

Use the Anchor Follow-up Data permission to specify the follow-up data to display when an account is open in the **Work Form**.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Work Form** > **Anchor Followup Data**.

Scope

This permission is available for the following scopes:

- System
- Business Class
- Customer Group
- Customer

Policy

The policy allows your organization to specify the follow-up data to display when an account is open in the **Work Form.** Enable the permission for a scope and then specify the follow-up data to display.

Reference Panels Permission

Use the Reference Panels permission to specify the reference panels to display, and to specify which panel is the default panel. All users can display the **Notes** and **Interactions** panels. For more information, see Reference Panels.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Work Form** > **Reference Panels**.

Scope

This permission is available for all scopes.

Policy

The policy allows your organization to specify the reference panels that are available in the lower section of the **Work Form**. Enable the permission for a scope and then specify the panels to display.

Default Panel: Default panel to display when an account is open in the **Work Form**.

Available Panels: If you select a reference panel, users can view it in the **Work Form**.

Select None: Clears all selected items in the list.

Select All: Selects all items in the list.

> **Tip**: To select multiple sequential panels, press and hold the **Shift** key and then click the first and last sequential panel. To select multiple non-sequential panels, press and hold the **Ctrl** key and then click each individual panel.

Task Panels Permission

Use the Task Panels permission to specify which task panels that user can view in the **Work Form**, and which task panel is the default panel to display. For more information, see Task Panels.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Work Form** > **Task Panels**.

Scope

This permission is available for all scopes.

Policy

The policy allows your organization to specify the task panels that are visible in the **Work Form**. Enable the permission for a scope and then specify the task panels to display.

Default Task Panel: Default task panel to display when an account is open in the **Work Form**.

Available Task Panels: If you select a task panel, users can display it in the **Work Form**.

Select None: Clears all selected items in the list.

Select All: Selects all items in the list.

> **Tip**: To select multiple sequential panels, press and hold the **Shift** key and then click the first and last sequential panel. To select multiple non-sequential panels, press and hold the **Ctrl** key and then click each individual panel.

Time on Account Configuration Permission

Use the Time on Account Configuration permission to specify the caution and warning thresholds for time spent on an account, and the duration of an open interaction. When the time reaches the specified

thresholds, the background color of the **Time on Account** indicator in the status bar and on the **Since** column in the **Open Interactions** panel changes color accordingly. For more information, see Work Form Overview and View Open Interactions.

Location

In the **Navigation** pane, click **Applications** > **Liquid Latitude** > **Work Form** > **Time on Account Configuration**.

Scope

This permission is available for all scopes.

Policy

These policies allow your organization to specify the thresholds for caution and warning zones. Enable the permission for a scope and then specify the thresholds for each zone.

Caution Color Boundary: Threshold (in hours, minutes, and seconds) for displaying a yellow background on the **Time on Account** indicator in the status bar and on the **Since** column in the **Open Interactions** panel.

Warning Color Boundary: Threshold (in hours, minutes, and seconds) for displaying a red background on the **Time on Account** indicator in the status bar and on the **Since** column in the **Open Interactions** panel.

Payment Vendor Gateway Settings

Payment Vendor Gateway Settings

Use the Payment Vendor Gateway settings to specify permissions and policies for Payment Vendor Gateway (PVG). PVG allows users to request payment transaction processing from vendors over a secure connection.

Access Batch Wizard Permission

Use the Access Batch Wizard permission to specify whether users can use the Batch Processor. For more information, see Process a Payment Batch.

Location

In the **Navigation** pane, click **Applications** > **Payment Vendor Gateway** > **Access Batch Wizard**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

ACH Vendor Information Permission

Use the ACH Vendor Information permission to specify a vendor's settings for processing ACH payment transactions using Payment Vendor Gateway (PVG).

Location

In the **Navigation** pane, click **Applications** > **Payment Vendor Gateway** > **ACH Vendor Information**.

Scope

This permission is available for the following scopes:

- System
- Business Class
- Client Group
- Client

Policy

The policy allows your organization to specify settings for ACH payment processing through a payment vendor using PVG. Enable the permission for a scope and then specify the settings.

Vendor Info Parameter 1: Credentials that the payment vendor provided to allow you to process ACH payment transactions. The format is:

securityToken=<principalCredential>|securityTokenSurcharge=<surchargeCredential>|mode=principal

Vendor Info Parameter 2: PINs that the payment vendor provided to allow you to process ACH payment transactions. The format is:

pin=<principalCredentialPIN>|pinSurcharge=<surchargeCredentialPIN>

> **Note:** Replace the text within the less than and greater than signs (<>) with the appropriate values. If you are sending surcharges with the principal as a single transaction, specify the "surchargeCredential" and "surchargeCredentialPIN."

Send the surcharge as a separate transaction?: If selected, Latitude sends surcharges as separate transactions and records two transactions on the account.

> **Note:** If you are sending surcharges as separate transactions, specify the **Vendor Surcharge Info Parameter 1** and **Vendor Surcharge Info Parameter 1** values. Replace the text within the less than and greater than signs (<>) with the appropriate values.

Vendor Surcharge Info Parameter 1: Credential that the payment vendor provided to allow you to process ACH surcharge transactions separately from the principal. The format is:

securityTokenSurcharge=<surchargeCredential>|mode=surcharge

Vendor Surcharge Info Parameter 2: PIN that the payment vendor provided to allow you to process ACH surcharge transactions separately from the principal. The format is:

pinSurcharge=<surchargeCredentialPIN>

Batch Processor System Permission

Use the Batch Processor System permission to specify system settings for the Batch Processor that creates batches of payments for each payment type. The Batch Processor posts transactions to the affected accounts.

Location

In the **Navigation** pane, click **Applications** > **Payment Vendor Gateway** > **Batch Processor System**.

Scope

This permission is available for the System scope only.

Policy

The policy allows your organization to specify the URL for the Batch Processor. Enable the permission for a scope and then specify the settings.

URL for Batch Job Processor System: URL to display the Batch Processor in Latitude.

Credit Card Vendor Information Permission

Use the Credit Card Vendor Information permission to specify a vendor's settings for processing credit card payment transactions using Payment Vendor Gateway (PVG).

Location

In the **Navigation** pane, click **Applications** > **Payment Vendor Gateway** > **Credit Card Vendor Information**.

Scope

This permission is available for the following scopes:

- System
- Business Class
- Client Group
- Client

Policy

The policy allows your organization to specify settings for credit card payment processing through a payment vendor using PVG. Enable the permission for a scope and then specify the settings.

Vendor Info Parameter 1: Credentials that the payment vendor provided to allow you to process credit card payment transactions. The format is:

> securityToken=<principalCredential>|securityTokenSurcharge=<surchargeCredential>|mode=principal

Vendor Info Parameter 2: PINs that the payment vendor provided to allow you to process credit card payment transactions. The format is:

> pin=<principalCredentialPIN>|pinSurcharge=<surchargeCredentialPIN>

> **Note:** Replace the text within the less than and greater than signs (<>) with the appropriate values. If you are sending surcharges with the principal as a single transaction, specify the "surchargeCredential" and "surchargeCredentialPIN."

Send the surcharge as a separate transaction?: If selected, Latitude sends surcharges as separate transactions and records two transactions on the account.

> **Note:** If you are sending surcharges as separate transactions, specify the **Vendor Surcharge Info Parameter 1** and **Vendor Surcharge Info Parameter 1** values. Replace the text within the less than and greater than signs (<>) with the appropriate values.

Vendor Surcharge Info Parameter 1: Credential that the payment vendor provided to allow you to process credit card surcharge transactions separately from the principal. The format is:

securityTokenSurcharge=<surchargeCredential>|mode=surcharge

Vendor Surcharge Info Parameter 2: PIN that the payment vendor provided to allow you to process credit card surcharge transactions separately from the principal. The format is:

pinSurcharge=<surchargeCredentialPIN>

Customer Information Profiles Permission

Use the Customer Information Profiles permission to specify the profiles to use to send information to Payment Vendor Gateway (PVG) for the payment processing vendor's use.

Location

In the **Navigation** pane, click **Applications** > **Payment Vendor Gateway** > **Customer Information Profiles**.

Scope

This permission is available for the System scope only.

Policy

The policy allows your organization to specify profiles to use to send information to PVG for the payment processing vendor's use. Enable the permission for a scope and then specify the settings.

Select the Customer Information Profile for Real Time Batch Credit Card Processing: Profile to use when processing batches of credit card payments.

Select the Customer Information Profile for Batch ACH Processing: Profile to use when processing batches of ACH payments.

Select the Customer Information Profile for Batch Paper Draft Processing: Profile to use when processing batches of paper draft payments.

Enable Payment Vendor Gateway Permission

Use the Enable Payment Vendor Gateway permission to allow your organization to use Payment Vendor Gateway (PVG) for sending transactions to payment processing vendors. The default value points to an IIS server that Latitude uses (primarily for hosted clients). If you are not using Latitude in a hosted environment, set up an IIS server to host the service.

Location

In the **Navigation** pane, click **Applications** > **Payment Vendor Gateway** > **Enable Latitude Payment Vendor Gateway**.

Scope

This permission is available for the System scope only.

Policy

The policy allows your organization to specify Payment Vendor Gateway settings. Enable the permission for a scope and then specify the settings.

URL for Payment Vendor Gateway: URL address for PVG. The default value points to an IIS server that Latitude uses (primarily for hosted clients). If you are not using Latitude in a hosted environment, set up an IIS server to host the service.

Select the Vendor for Real Time and Batch Credit Card Processing: Default vendor your company uses for credit card processing. Configure the Credit Card Vendor Information permission also.

Use vendor interface to capture credit card information: If selected, Latitude presents the vendor's interface to the user to collect credit card information.

Use alternative method for surcharge transaction: If selected, Latitude uses another method for surcharge transactions.

Vendor manages payment arrangements: If selected, the vendor manages payment arrangements.

Select the Vendor for Batch ACH Processing: Default vendor your company uses for ACH processing. Configure the ACH Vendor Information permission also.

Use vendor interface to capture bank account information: If selected, Latitude presents the vendor's interface to the user to collect bank account information.

Use alternative method for surcharge transaction: If selected, Latitude uses another method for surcharge transactions.

Vendor manages payment arrangements: If selected, the vendor manages payment arrangements.

Select the Vendor for Batch Paper Draft Processing: Default vendor your company uses for paper draft processing. Configure the Paper Draft Vendor Information permission also.

Paper Draft Vendor Information Permission

Use the Paper Draft Vendor Information permission to specify a vendor's settings for processing paper draft payment transactions using Payment Vendor Gateway (PVG).

Location

In the **Navigation** pane, click **Applications** > **Payment Vendor Gateway** > **Paper Draft Vendor Information**.

Scope

This permission is available for the following scopes:

- System

- Business Class
- Client Group
- Client

Policy

The policy allows your organization to specify settings for paper draft payment processing through a payment vendor using PVG. Enable the permission for a scope and then specify the settings.

Vendor Info Parameter 1: Credentials that the payment vendor provided to allow you to process paper draft payment transactions. The format is:

securityToken=<principalCredential>|securityTokenSurcharge=<surchargeCredential>|mode=principal

Vendor Info Parameter 2: PINs that the payment vendor provided to allow you to process paper draft payment transactions. The format is:

pin=<principalCredentialPIN>|pinSurcharge=<surchargeCredentialPIN>

> **Note:** Replace the text within the less than and greater than signs (<>) with the appropriate values. If you are sending surcharges with the principal as a single transaction, specify the "surchargeCredential" and "surchargeCredentialPIN."

Send the surcharge as a separate transaction?: If selected, Latitude sends surcharges as separate transactions and records two transactions on the account.

> **Note:** If you are sending surcharges as separate transactions, specify the **Vendor Surcharge Info Parameter 1** and **Vendor Surcharge Info Parameter 1** values. Replace the text within the less than and greater than signs (<>) with the appropriate values.

Vendor Surcharge Info Parameter 1: Credential that the payment vendor provided to allow you to process paper draft surcharge transactions separately from the principal. The format is:

securityTokenSurcharge=<surchargeCredential>|mode=surcharge

Vendor Surcharge Info Parameter 2: PIN that the payment vendor provided to allow you to process paper draft surcharge transactions separately from the principal. The format is:

pinSurcharge=<surchargeCredentialPIN>

Portfolio Manager Settings

Portfolio Manager Settings

Use the Portfolio Manager settings to specify permissions and policies for Portfolio Manager.

Access Portfolio Manager Permission

Use the Access Portfolio Manager permission to specify whether users can open Portfolio Manager.

Location

In the **Navigation** pane, click **Applications** > **Portfolio Manager** > **Access Portfolio Manager**.

Scope

This permission is available for all scopes.

Policy

N/A

Access Reports Permission

Use the Access Reports permission to specify whether users can display reports in Portfolio Manager.

Location

In the **Navigation** pane, click **Applications** > **Portfolio Manager** > **Access Reports**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Access Tools Permission

Use the Access Tools permission to specify whether users can use the tools in Portfolio Manager.

Location

In the **Navigation** pane, click **Applications** > **Portfolio Manager** > **Access Tools**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Add/Edit/Delete Buyers Permission

Use the Add/Edit/Delete Buyers permission to specify whether users can add, modify, and delete buyers in Portfolio Manager.

Location

In the **Navigation** pane, click **Applications** > **Portfolio Manager** > **Add/Edit/Delete Buyers**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Add/Edit/Delete Investors Permission

Use the Add/Edit/Delete Investors permission to specify whether users can add, modify, and delete investors in Portfolio Manager.

Location

In the **Navigation** pane, click **Applications** > **Portfolio Manager** > **Add/Edit/Delete Investors**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Add/Edit/Delete Purchases Permission

Use the Add/Edit/Delete Purchases permission to specify whether users can add, modify, and delete purchases in Portfolio Manager.

Location

In the **Navigation** pane, click **Applications** > **Portfolio Manager** > **Add/Edit/Delete Purchases**.

Scope

This permission is available for the following scopes:

- System
- Role

- User
- Branch

Policy

N/A

Add/Edit/Delete Sales Permission

Use the Add/Edit/Delete Sales permission to specify whether users can add, modify, and delete sales in Portfolio Manager.

Location

In the **Navigation** pane, click **Applications** > **Portfolio Manager** > **Add/Edit/Delete Sales**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Add/Edit/Delete Samples Permission

Use the Add/Edit/Delete Samples permission to specify whether users can add, modify, and delete samples in Portfolio Manager.

Location

In the **Navigation** pane, click **Applications** > **Portfolio Manager** > **Add/Edit/Delete Samples**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Add/Edit/Delete Sellers Permission

Use the Add/Edit/Delete Sellers permission to specify whether users can add, modify, and delete sellers in Portfolio Manager.

Location

In the **Navigation** pane, click **Applications** > **Portfolio Manager** > **Add/Edit/Delete Sellers**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

View Buyers Permission

Use the View Buyers permission to specify whether users can view buyers in Portfolio Manager.

Location

In the **Navigation** pane, click **Applications** > **Portfolio Manager** > **View Buyers**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

View Investors Permission

Use the View Investors permission to specify whether users can view investors in Portfolio Manager.

Location

In the **Navigation** pane, click **Applications** > **Portfolio Manager** > **View Investors**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

View Purchases Permission

Use the View Purchases permission to specify whether users can view purchases in Portfolio Manager.

Location

In the **Navigation** pane, click **Applications** > **Portfolio Manager** > **View Purchases**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

View Sales Permission

Use the View Sales permission to specify whether users can view sales in Portfolio Manager.

Location

In the **Navigation** pane, click **Applications** > **Portfolio Manager** > **View Sales**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

View Samples Permission

Use the View Samples permission to specify whether users can view samples in Portfolio Manager.

Location

In the **Navigation** pane, click **Applications** > **Portfolio Manager** > **View Samples**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

View Sellers Permission

Use the View Sellers permission to specify whether users can view sellers in Portfolio Manager.

Location

In the **Navigation** pane, click **Applications** > **Portfolio Manager** > **View Sellers**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Reporting Console Settings

Reporting Console Settings

Use the Reporting Console permissions and policies to specify settings for Reporting Console.

Access Reporting Console Permission

Use the Access Reporting Console permission to specify whether users can open Reporting Console.

Location

In the **Navigation** pane, click **Applications** > **Reporting Console** > **Access Reporting Console**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Manage Reporting Console Permission

Use the Manage Reporting Console permission to specify whether users can manage reports in Reporting Console. The actions include: exporting, importing, deleting, organizing, and renaming reports.

Location

In the **Navigation** pane, click **Applications** > **Reporting Console** > **Manage Reporting Console**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

View Reports Permission

Use the View Reports permission to specify whether users can view reports in Reporting Console.

Location

In the **Navigation** pane, click **Applications** > **Reporting Console** > **View Reports**.

Scope

This permission is available for the following scopes:

- System
- Role
- User

- Branch

Policy

The policy allows your organization to specify what users can do in Reporting Console. Enable the permission for a scope and then select the Reporting Console permissions.

Permit the user to create snapshots of reports they have run: If selected, the user can create snapshots of reports the user runs.

Permit the user to view snapshots of reports created by other users: If selected, the user can view snapshots of reports other users created.

Restrict user to only execute the following reports: If selected, the user can run the specified reports only.

Reports: If you select a report, users can run it.

Select None: Clears all selected items in the list.

Select All: Selects all items in the list.

> **Tip**: To select multiple sequential reports, press and hold the **Shift** key and then click the first and last sequential report. To select multiple non-sequential reports, press and hold the **Ctrl** key and then click each individual report.

Service Request Gateway Settings

Service Request Gateway Settings

Use the Service Request Gateway settings to specify permissions and policies for Service Request Gateway (SRG). SRG allows users to request services from a service vendor, such as a credit reporting vendor, over a secure connection.

Access Quota Management Application Permission

Use the Access Quota Management Application permission to specify whether users can open the Quota Management program to define user and customer quotas.

Location

In the **Navigation** pane, click **Applications** > **Quota Management** > **Access Quota Management Application**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

The policy allows your organization to specify whether users can open the Quota Management program. Enable the permission for a scope and then specify the overrides.

Allow the user to temporarily add to or remove from a user's quota allotment for any product. Only valid for current period: If selected, allows the user to modify a user's quota allotment for the current period only.

Allow the user to temporarily add to or remove from a customer's quota allotment for any product. Only valid for current period: If selected, allows the user to modify a customer's quota allotment for the current period only.

Allow the user to view the audit of changes to quota allotments: If selected, allows the user to view the audit trail that shows changes to quota allotments.

Access SRG Module Installer Permission

Use the Access SRG Module Installer permission to specify whether users can use the SRG Module Installer to configure Service Request Gateway (SRG).

Location

In the **Navigation** pane, click **Applications** > **Service Request Gateway** > **Access SRG Module Installer**.

Scope

This permission is available for the following scopes:

- System
- Role
- User

Policy

N/A

Credit Report Requests Settings

Credit Report Requests Settings

Use the Credit Report Requests settings to specify permissions and policies for credit report requests.

Access the Credit Report Request Wizard Permission

Use the Access the Credit Report Request Wizard permission to specify whether users can use the Credit Report Request Wizard**.**

Location

In the **Navigation** pane, click **Applications** > **Service Request Gateway** > **Credit Report Requests** > **Access the Credit Report Request Wizard**.

Scope

This permission is available for the following scopes:

- System

- Role
- User
- Branch

Policy

N/A

Allow Viewing of Credit Reports Permission

Use the Allow Viewing of Credit Reports permission to specify whether users can view credit reports.

Location

In the **Navigation** pane, click **Applications** > **Service Request Gateway** > **Credit Report Requests** > **Allow Viewing of Credit Reports**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch
- Business Class
- Client Group
- Client

Policy

N/A

Credit Report Requests Settings Permission

Use the Credit Report Requests Settings permission to configure general settings for credit report requests.

Location

In the **Navigation** pane, click **Applications** > **Service Request Gateway** > **Credit Report Requests** > **Credit Report Requests Settings**.

Scope

This permission is available for the System scope only.

Policy

The policy allows your organization to specify general settings for credit report requests. Enable the permission for a scope and then specify the settings.

"One Off" time out period in seconds before user is prompted to wait or continue working: Number of seconds to wait after requesting a report before prompting the user to continue waiting or continue working.

Minimum number of days that must pass before next credit report request on an account: Minimum number of days after requesting a credit report for the user to wait before requesting another report.

Apply "minimum number of days" policy only to credit reports from same vendor: If selected, the "minimum number of days" policy applies to credit reports from the same vendor only.

Minimum balance on account to request credit report: Minimum account balance required for the user to request a credit report.

Maximum number of credit report requests per account: Maximum number of credit report requests allowed for each account.

Enable "One Off" Credit Report Requests Permission

Use the Enable "One Off" Credit Report Requests permission to specify whether users can request a single credit report.

Location

In the **Navigation** pane, click **Applications** > **Service Request Gateway** > **Credit Report Requests** > **Enable "One Off" Credit Report Requests**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch
- Business Class
- Client Group
- Client

Policy

N/A

Enable Overrides to Credit Report Request Settings Permission

Use the Enable Overrides to Credit Report Request Settings permission to specify whether users can override general settings for credit report requests.

Location

In the **Navigation** pane, click **Applications** > **Service Request Gateway** > **Credit Report Requests** > **Enable Overrides to Credit Report Request Settings**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

The policy allows your organization to override the general settings for credit report requests. Enable the permission for a scope and then specify the overrides.

Override minimum number of days that must pass before next credit report request on an account: If selected, allows the user to override the minimum number of days after requesting a credit report for the user to wait before requesting another report.

Override minimum balance on account to request credit report: If selected, allows the user to override the minimum account balance required for the user to request a credit report.

Override maximum number of credit report requests per account: If selected, allows the user to override the maximum number of credit report requests allowed for each account.

Enable Service Request Gateway Permission

Use the Enable Service Request Gateway permission to specify whether your company can use Service Request Gateway (SRG) to request services from vendors. The default value points to an IIS server that Latitude uses (primarily for hosted clients). If you are not using Latitude in a hosted environment, set up an IIS server to host the service.

Location

In the **Navigation** pane, click **Applications** > **Service Request Gateway** > **Enable Latitude Service Request Gateway**.

Scope

This permission is available for the System scope only.

Policy

The SRG Module Installer populates these boxes for the Latitude server where your organization installed SRG. Enable the permission for a scope and then provide these values for each workstation where your organization installed SRG.

URL of the Service Request Gateway (SRG): Address of the SRG server.

Client Identifier authenticating with the SRG: Client ID for authenticating to the SRG server.

Password for authenticating with the SRG: Password for authenticating to the SRG server.

Password for configuring the SRG: Password for configuring SRG.

SRG Server Identifier: Tokenizer identity thumbprint.

Web Access Settings

Web Access Settings

Use the Web Access settings to specify permissions and policies for Web Access.

Account View Client Code Override Policy Permission

Use the Account View Client Code Override Policy permission to specify the report to display when viewing an account in Web Access. If your organization specified a default report in the Website User Policy Permission for a user or role, the report specified in this permission displays instead.

Location

In the **Navigation** pane, click **Applications** > **Web Access** > **Account View Client Code Override Policy**.

Scope

This permission is available for the following scopes:

- System
- Business Class
- Client Group
- Client

Policy

The policy allows your organization to specify the default report to display when viewing an account. Enable the permission for a scope and then specify the report.

Website System Policy Permission

Use the Website System Policy permission to specify the Web Access system administrator's email address. All system, client, and customer emails sent from Web Access go to this email address.

Location

In the **Navigation** pane, click **Applications** > **Web Access** > **Website System Policy**.

Scope

This permission is available for the System scope only.

Policy

The policy allows your organization to specify the administrator's email address. Enable the permission for a scope and then type the administrator's email address.

Website User Client Access Policy Permission

Use the Website User Client Access Policy permission to specify the client and client groups available to Web Access users.

Location

In the **Navigation** pane, click **Applications** > **Web Access** > **Website User Client Access Policy**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

The policy allows your organization to specify the client and client groups available to Web Access users. Enable the permission for a scope and then select the client groups and clients.

Client Groups: If you select a client group, it's available to Web Access users.

Clients: If you select a client, it's available to Web Access users.

Select None: Clears all selected items in the list.

Select All: Selects all items in the list.

> **Tip**: To select multiple sequential client groups or clients, press and hold the **Shift** key and then click the first and last sequential client group or client. To select multiple non-sequential client groups or clients, press and hold the **Ctrl** key and then click each individual client group or client.

Website User Policy Permission

Use the Website User Policy permission to specify the Web Access features available to a user or role.

Location

In the **Navigation** pane, click **Applications** > **Web Access** > **Website User Policy**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

The policy allows your organization to specify the Web Access features that are available to a user or role. Enable the permission for a scope and then specify the settings.

User Can Search for Customers: If selected, the user can search for accounts.

User Can View the Audit Logs: If selected, the user can view the audit trail for all user activities. We don't recommend that you set this policy for clients or customers because the logs contain user IP addresses.

User Can Add Notes to Customer Accounts: If selected, the user can add notes to accounts.

User Can Send a Message to Admin regarding Customer Accounts: If selected, the user can send an email message to the administrator regarding an account. The account number appears in the email subject line and the email goes to the email address specified in the Website System permission.

User Can Send a Message to the Administrator: If selected, the user can send an email message to the administrator. The email goes to the email address specified in the Website System permission.

User Can Add a Report: If selected, the user can add a report.

Send Admin an email when user logs into the website: If selected, Web Access sends an email message to the administrator when the user logs on to the website. The email goes to the email address specified in the Website System permission.

Echo email sent to user when they Add a Note or Send any Message: If selected, Web Access sends an email message to the user when the user adds a note to an account or sends an email message to the administrator.

User Can Upload and Download files to the Web Server: If selected, the user can upload files to and download files from the web server.

Choose the report used for the Account View: Default report to display when viewing an account. If your organization enabled the Account View Customer Code Override Policy permission, the default report specified for that permission displays instead of the report specified here.

Choose the report used to return Search Results: Default report to display when viewing search results.

Reports: If you select a report, it's available to Web Access users.

Select None: Clears all selected items in the list.

Select All: Selects all items in the list.

> **Tip**: To select multiple sequential reports, press and hold the **Shift** key and then click the first and last sequential report. To select multiple non-sequential reports, press and hold the **Ctrl** key and then click each individual report.

WorkFlow Settings

WorkFlow Settings

Use the WorkFlow settings to specify permissions and policies for WorkFlow.

Manually Pause WorkFlow Permission

Use the Manually Pause WorkFlow permission to specify whether users can pause a workflow that is running on an account in WorkFlow.

Location

In the **Navigation** pane, click **Applications** > **WorkFlow** > **Manually Pause WorkFlow**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch
- Business Class
- Client Group
- Client

Policy

N/A

Manually Raise Event Permission

Use the Manually Raise Event permission to specify whether users can raise an event on an account in WorkFlow.

Location

In the **Navigation** pane, click **Applications** > **WorkFlow** > **Manually Raise Event**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch
- Business Class
- Client Group
- Client

Policy

N/A

Manually Release WorkFlow Permission

Use the Manually Release WorkFlow permission to specify whether users can release a parent workflow in WorkFlow that is waiting on a child workflow to complete, which allows the parent workflow to continue.

Location

In the **Navigation** pane, click **Applications** > **WorkFlow** > **Manually Release WorkFlow**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch
- Business Class
- Client Group
- Client

Policy

N/A

Manually Resume WorkFlow Permission

Use the Manually Resume WorkFlow permission to specify whether users can resume a paused workflow for an account in WorkFlow.

Location

In the **Navigation** pane, click **Applications** > **WorkFlow** > **Manually Resume WorkFlow**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch
- Business Class
- Client Group
- Client

Policy

N/A

Manually Start WorkFlow Permission

Use the Manually Start WorkFlow permission to specify whether users can start a workflow on an account in WorkFlow.

Location

In the **Navigation** pane, click **Applications** > **WorkFlow** > **Manually Start WorkFlow**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch
- Business Class
- Client Group
- Client

Policy

N/A

Manually Stop WorkFlow Permission

Use the Manually Stop WorkFlow permission to specify whether users can stop a workflow that is running on an account in WorkFlow.

Location

In the **Navigation** pane, click **Applications** > **WorkFlow** > **Manually Stop WorkFlow**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch
- Business Class
- Client Group
- Client

Policy

N/A

WorkFlow Engine Settings Permission

Use the WorkFlow Engine Settings permission to specify settings for WorkFlow Engine.

Location

In the **Navigation** pane, click **Applications** > **WorkFlow** > **Latitude WorkFlow Engine Settings**.

Scope

This permission is available for the System scope only.

Policy

The policy allows your organization to specify settings for WorkFlow Engine. Enable the permission for a scope and then specify the settings.

Execution Duration [min]: Maximum number of minutes WorkFlow Engine continues to run in a single session. WorkFlow Engine processes events and activities until the event queue is empty or it reaches the time limit set here.

Action Activities: Maximum number of accounts WorkFlow Engine can process when running action activities. This setting represents "batches" of account activity by type and prevents server process overload.

Condition Activities: Maximum number of accounts WorkFlow Engine can process when running condition activities.

Query Activities: Maximum number of accounts WorkFlow Engine can process when running query activities.

Switch Activities: Maximum number of accounts WorkFlow Engine can process when running switch activities.

Email Address: Email address of the person who is monitoring WorkFlow Engine activity.

Configuration Settings

Configuration Settings

Use the Configuration settings to specify configuration permissions and policies for Latitude.

Delinquency Aging Bucket Labels Permission

Use the Delinquency Aging Bucket Labels permission to specify the labels to display for the delinquency aging buckets. For more information, see Delinquency Card.

Location

In the **Navigation** pane, click **Configuration** > **Delinquency Aging Bucket Labels**.

Scope

This permission is available for the System scope only.

Policy

The policy allows your organization to specify the labels to display for the delinquency aging buckets. Enable the permission for a scope and then specify the label names and their values.

Payment Processing Settings

Payment Processing Settings

Use the Payment Processing settings to specify permissions and policies for payment methods and payment spreads.

Configuration for Handling Broken Promises Permission

Use the Configuration for Handling Broken Promises permission to specify the status and queue level to assign to accounts when customers break a promise.

Location

In the **Navigation** pane, click **Configuration** > **Payment Processing** > **Configuration for Handling Broken Promises**.

Scope

This permission is available for the System scope only.

Policy

The policy allows your organization to specify the status and queue level to assign to accounts when customers break a promise. Enable the permission for a scope and then specify the settings.

Change Status and Qlevel: If selected, the system changes the account status and queue level when customers break promises.

Change Status to: Status to assign to accounts when processing broken promises.

Change Qlevel to: Queue level to assign to accounts when processing broken promises.

Configuration for Handling NSFs/Reversals Permission

Use the Configuration for Handling NSFs/Reversals permission to specify the status and queue level to assign to accounts when importing NSF or payment reversals using Exchange. This permission has no effect on manual payment entries.

Location

In the **Navigation** pane, click **Configuration** > **Payment Processing** > **Configuration for Handling NSFs/Reversals**.

Scope

This permission is available for the System scope only.

Policy

The policy allows your organization to specify the status and queue level to assign to accounts when importing NSF or payment reversals using Exchange. Enable the permission for a scope and then specify the settings.

Change Status and Qlevel: If selected, the system changes the account status and queue level when importing accounts with NSF or payment reversals.

Change Status to: Status to assign to accounts when processing NSF or payment reversals.

Change Qlevel to: Queue level to assign to accounts when processing NSF or payment reversals.

Notes:

- The system does not change the queue level for accounts assigned to queue level "875."
- If you reopen a closed account that is linked and is not the link driver, the system changes the queue level from "998" to "875."

Change the status of future arrangements: If selected, the system assigns the specified status to future payment arrangements for accounts with NSF or payment reversals imported using Exchange.

Status for future arrangements: Status to assign to future payment arrangements for accounts with NSF or payment reversals imported using Exchange.

Deactivate Automatic Status and Queue Level Permission

Use the Deactivate Automatic Status and Queue Level permission to specify whether to prevent Latitude from changing the account status and queue levels automatically for arrangements. If you enable the permission, Collector doesn't change the account status and queue levels automatically. Instead, the account status and queue levels remain unchanged.

If you don't configure or enable the permission, Collector changes account status and queue levels automatically. If your organization configured the Configuration for Handling Broken Promises permission or the Configuration for Handling NSFs/Reversals permission, Collector changes account status and queue levels according to those configurations. Otherwise, Collector changes account status and queue levels according to the following table:

Account has...	Account Status	Queue Level	Status of Non-driver Linked Accounts	Queue Level of Non-driver Linked Accounts
Promises	PPA	820	PPA	875
Broken promise	ACT	010	ACT	875
No promises remaining	ACT	013	ACT	875
Post-dated check	PDC	820	PDC	875
No post-dated checks remaining	ACT	011	ACT	875
Bounced check with post-dated checks remaining	NSF	012	ACT	875
Bounced check with no post-dated checks remaining	NSF	019	ACT	875
Post-dated credit card	PCC	820	PCC	875

Account has...	Account Status	Queue Level	Status of Non-driver Linked Accounts	Queue Level of Non-driver Linked Accounts
No post-dated credit cards remaining	ACT	010	ACT	875
Declined credit card	ACT	012	ACT	875
Declined credit with post-dated credit cards remaining	PCC	019	ACT	875

Location

In the **Navigation** pane, click **Configuration** > **Payment Processing** > **Deactivate Automatic Status and Queue Level**.

Scope

This permission is available for the System scope only.

Policy

N/A

Override Payment Spread Permission

Use the Override Payment Spread permission to specify whether users can override the configured payment spread for linked account arrangements and specify the order in which to apply payments. For more information about the configured payment spread, see Payment Spread Permission. For more information about overriding the configured payment spread, see Override a Payment Spread.

Location

In the **Navigation** pane, click **Configuration** > **Payment Processing** > **Override Payment Spread**.

Scope

This permission is available for the following scopes:

- System
- Business Class
- Client Group
- Client

Policy

N/A

Payment Method Fee Schedule Permission

Use the Payment Method Fee Schedule permission to associate payment methods with fee schedules. For more information, see Map a Payment Method to a Fee Schedule.

Location

In the **Navigation** pane, click **Configuration** > **Payment Processing** > **Payment Method Fee Schedule**.

Scope

This permission is available for the following scopes:

- System
- Business Class
- Client Group
- Client

Policy

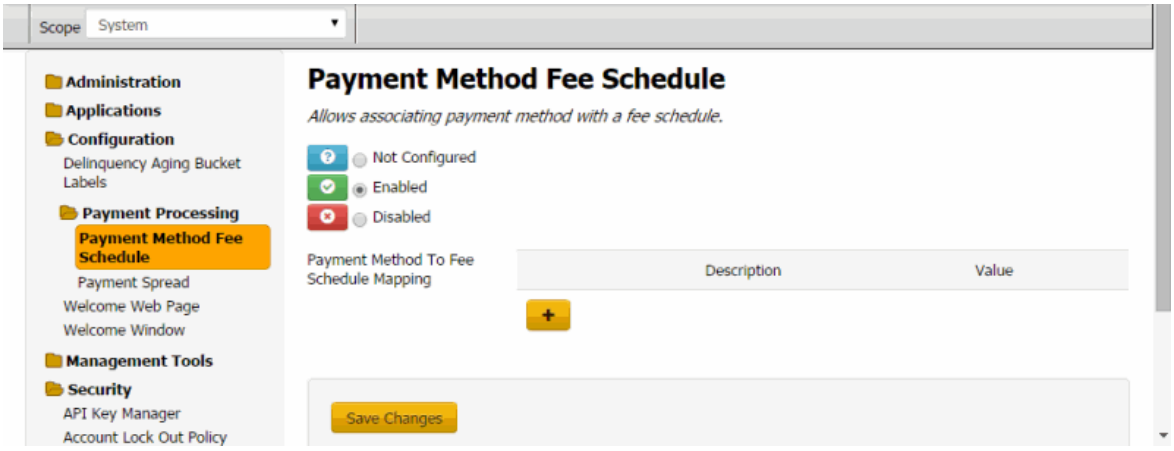
The policy allows your organization to associate payment methods to fee schedules. Enable the permission for a scope and then specify the mappings.

Map a Payment Method to a Fee Schedule

Use the **Payment Fee Schedule** panel to map a payment method to a fee schedule. You must have the appropriate permissions to map payment methods. For more information, see Payment Method Fee Schedule Permission.

To map a payment method to a fee schedule

1. In the **Navigation** pane, click **Configuration** > **Payment Processing** > **Payment Method Fee Schedule**.



Description: Unique code that identifies the fee schedule.

Value: Payment method (for example, credit card, check, money order) to associate to the fee schedule.

> **Note:** The text you type in the **Value** box must match exactly to an existing payment method that your organization set up in the Payment Methods system code.

2. Click the plus sign (+). A blank row appears in the data grid.
3. Complete the information and then click **Save Changes**.

> **Note:** To modify a mapping, type a new value in the appropriate box. To delete a mapping, click the Delete icon.

Payment Spread Permission

Use the Payment Spread permission to specify settings for how to spread payments across linked accounts.

Location

In the **Navigation** pane, click **Configuration** > **Payment Processing** > **Payment Spread**.

Scope

This permission is available for the following scopes:

- System
- Business Class
- Client Group
- Client

Policy

The policy allows your organization to specify how the system spreads payments across linked accounts. Enable the permission for a scope and then specify the settings.

Payment Spread Method: Method for spreading payments across linked accounts. Valid values are:

- **Spread payments in order of the customer priority:** The system applies payments to the linked accounts based on how you prioritized the payments for each customer, starting with the highest priority. If you assigned the same priority to accounts, the system applies the payments proportionally.
- **Spread payments evenly over each account:** The system divides the payments and applies an equal amount to each linked account.
- **Spread payments according to their fees:** The system applies payments to the highest yielding linked account first, based on the balance and fee schedule.
- **Spread payments over each account in the specified order:** The system sorts the linked accounts according to the order you specify in the **Sort Field 1** through **Sort Field 4** and **Sort Field 1 Order** through **Sort Field 4 Order** policies in this permission and then applies the payments in that order.
- **Spread payments over each account proportionally by current balance:** The system applies payments to each linked account based on the amount owed in relation to the total balance of all the linked accounts listed. The system divides the amount owed for an account by the total

balance for the combined accounts to get a percent. The system multiplies the payment by that percent and applies the result to that account.

For example, the total balance for the three accounts shown in the example is 3,217.47.

- **First Account:** Divide 250 (the balance for the first account) by 3,217.47 to get .08. If the payment amount is $200, multiply 0.08 by 200 to get 16. The system applies $16 of the $200 payment to the first account.
- **Second Account:** Divide 967.47 (the balance for the second account) by 3,217.47 to get 0.30. Multiply 0.30 by 200 to get 60. The system applies $60 of the $200 payment to the second account.
- **Third Account:** Divide 2,000 (the balance for the third account) by 3,217.47 to get 0.62. Multiply 0.62 by 200 to get 124. The system applies $124 of the $200 payment to the third account. 16 + 60 + 124 = 200.
- **Spread payments in order of the Fee Schedule Bucket priority and then in the specified order:** The system applies payments to the linked accounts according to the money bucket priory set for the fee schedule and the order you specify in the **Sort Field 1** through **Sort Field 4** and **Sort Field 1 Order** through **Sort Field 4 Order** policies in this permission. The system sorts the accounts according to the sort policies specified. The system applies the payment to the priority 1 bucket of the first account in the sorted list, until the balance in that bucket is zero or no funds remain to apply. If funds remain, the system applies the payment to the priority 1 bucket of the next account in the sorted list until the balance in that bucket is zero or no funds remain to apply. If funds remain after applying the payment to the priority 1 buckets for all the linked accounts, the system begins applying the remaining funds to the priority 2 buckets in the same manner. The system continues applying the payment until no funds remain to apply or all linked account balances are zero.

Sort Field 1: First field by which to sort accounts when applying payments.

Sort Field 1 Order: Order in which to sort the data in the field specified in **Sort Field 1**.

Sort Field 2: Second field by which to sort accounts when applying payments.

Sort Field 2 Order: Order in which to sort the data in the field specified in **Sort Field 2**.

Sort Field 3: Third field by which to sort accounts when applying payments.

Sort Field 3 Order: Order in which to sort the data in the field specified in **Sort Field 3**.

Sort Field 4: Fourth field by which to sort accounts when applying payments.

Sort Field 4 Order: Order in which to sort the data in the field specified in **Sort Field 4**.

Note: If you specify more than one sort field, the system sorts the accounts by the first field specified. Within that sort order, the system then sorts the accounts by the second field specified. The system continues sorting in this manner for any subsequent sort fields specified. After sorting the accounts, the system applies payments to the accounts beginning with the first account in the sorted list.

Prevent Multiple Account Access Permission

Use the Prevent Multiple Account Access permission to prevent users from accessing the same account simultaneously.

Location

In the **Navigation** pane, click **Configuration** > **Prevent Multiple Account Access**.

Scope

This permission is available for the System scope only.

Policy

N/A

SMTP Permission

Use the SMTP permission to specify Simple Mail Transfer Protocol (SMTP) settings for email messages.

Location

In the **Navigation** click **Configuration** > **SMTP**.

Scope

This permission is available for the System scope only.

Policy

The policy allows your organization to specify the configuration used to send email messages through Simple Mail Transfer Protocol (SMTP). Enable the permission for a scope and then specify the email message settings at the system level.

SMTP Server: mailserver.domain_name

Port (0=default): If 0, use the default SMTP port of 25. Otherwise, specify the port number to use.

Connect Using Secure Sockets Layer: If selected, connects to the SMTP server using Secure Sockets Layer (SSL).

Authentication: The options are:

- **Anonymous** (default) = no authentication
- **Basic** = Provide a user name and password and select SSL
- **Integrated** = Use Windows authentication

Username and Password: If you selected **Basic Authentication**, specify the user name and password to use.

Sender Domain: Domain address used for email messages (for example, inin.com).

Timeout[sec]: Number of seconds to wait when sending an email message before displaying a time-out message.

Welcome Web Page Permission

Use the Welcome Web Page permission to specify settings for the webpage to display when logging on to Latitude. The address can point to a local HTML file or a hosted webpage. If using a hosted webpage, Latitude passes the database information and current user ID to the web server to permit displaying user-specific information.

Location

In the **Navigation** pane, click **Configuration** > **Welcome Web Page**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

The policy allows your organization to specify the address for the webpage to display as the background on the Latitude welcome page. Enable the permission for a scope and then specify the settings.

URL: Address of the HTML resource to display as the background on the Latitude welcome page. You can specify a different path for each scope.

Pass user credentials to web server: If selected, Latitude passes credentials to the web server when displaying the webpage.

Welcome Window Permission

Use the Welcome Window permission to specify settings for the Welcome window to display when logging on to Latitude.

Location

In the **Navigation** pane, click **Configuration** > **Welcome Window**.

Scope

This permission is available for all scopes.

Policy

The policy allows your organization to specify a window to display on the Latitude welcome page. Enable the permission for a scope and then specify the window information.

Assembly DLL Path: Assembly DLL path to the welcome window.

WCF Host Name: WCF host name.

WCF Host Port (495 = default): WCF host port.

Connect using Secure Sockets layer (SSL): If selected, connects to the welcome page using SSL.

Management Tool Settings

Management Tool Settings

Use the Management Tools settings to specify permissions and policies for management tools.

Accounting Settings

Accounting Settings

Use the Accounting settings to specify permissions and policies for the Invoices and Overpayment Manager programs.

Access Invoices Program Permission

Use the Access Invoices Program permission to specify whether users can open the Invoices program.

Location

In the **Navigation** pane, click **Management Tools** > **Accounting** > **Access Invoices Program**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Access Overpayment Manager Permission

Use the Access Overpayment Manager Program permission to specify whether users can open Overpayment Manager.

Location

In the **Navigation** pane, click **Management Tools** > **Accounting** > **Access Overpayment Manager Program**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

- Business Class
- Client Group
- Client

Policy

The policy allows users to add refunds and transfers using Overpayment Manager. Enable the permission for a scope and then specify the settings.

Allow the user to edit this selection criteria (for viewing only): If selected, the user can select or clear the **Maximum Amount** and **Invoiced Only** check boxes in Overpayment Manager to display or hide overpaid transactions.

Allow refund/transfer of overpayments on uninvoiced payments: If selected, the user can refund or transfer overpayment amounts not invoiced yet.

Maximum amount of overpayment allowed for refund/transfer: Maximum amount users can refund or transfer.

Allow refund of PU overpayments to the customer: If selected, the user can create refund checks on overpayment amounts for PU (paid us) transaction types.

Allow refund of PA overpayments to the customer: If selected, the user can create refund checks on overpayment amounts for PA (paid agency) transaction types.

Allow refund of PC overpayments to the customer: If selected, the user can create refund checks on overpayment amounts for PC (paid client) transaction types.

How many days must pass before allowing a refund of overpayment to the customer: Time to wait before granting a refund. Latitude uses this value with the value in the **How many days must pass before allowing a transfer of overpayment to another account** box.

Minimum amount of overpayment refund to the customer: Minimum amount users can refund.

Allow transfer of PU overpayments to another account: If selected, the user can transfer funds on overpayment amounts for PU (paid us) transaction types.

Allow transfer of PA overpayments to another account: If selected, the user can transfer funds on overpayment amounts for PA (paid agency) transaction types.

Allow transfer of PC overpayments to another account: If selected, the user can transfer funds on overpayment amounts for PC (paid client) transaction types.

How many days must pass before allowing a transfer of overpayment to another account: Time to wait before granting a fund transfer. Latitude uses this value with the value in the **How many days must pass before allowing a refund of overpayment to the debtor** box.

Minimum amount of an overpayment transfer to another account: Minimum amount users can transfer.

Have the Overpayment Manager application create a check when the batch is created: If selected, Latitude creates a check record for the refund. Process the batch or delete the check. You can print the check from the **Check Register** in the Invoices program.

Enter AR Payments Permission

Use the Enter AR Payments permission to specify whether users can add accounts receivable payment information to apply toward client invoices in the Invoices program.

Location

In the **Navigation** pane, click **Management Tools** > **Accounting** > **Enter AR Payments**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch
- Business Class
- Client Group
- Client

Policy

N/A

Enter Bank Transactions Permission

Use the Enter Bank Transactions permission to specify whether users can add bank transaction information for trust accounts using the Invoices program.

Location

In the **Navigation** pane, click **Management Tools** > **Accounting** > **Enter Bank Transactions**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch
- Business Class
- Client Group
- Client

Policy

N/A

Generate Invoices Permission

Use the Generate Invoices permission to specify whether users can create client invoices using the Invoices program.

Location

In the **Navigation** pane, click **Management Tools** > **Accounting** > **Generate Invoices**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch
- Business Class
- Client Group
- Client

Policy

N/A

Generate Statements Permission

Use the Generate Statements permission to specify whether users can create account statements using the Invoices program.

Location

In the **Navigation** pane, click **Management Tools** > **Accounting** > **Generate Statements**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch
- Business Class
- Client Group
- Client

Policy

N/A

Print Checks Permission

Use the Print Checks permission to specify whether users can print checks using the Invoices program.

Location

In the **Navigation** pane, click **Management Tools** > **Accounting** > **Print Checks**.

Scope

This permission is available for all scopes.

Policy

N/A

Access Credit Reporting Wizard Permission

Use the Access Credit Reporting Wizard permission to specify whether users can open the Credit Bureau Reporting Wizard to create a file to send to a credit bureau.

Location

In the **Navigation** pane, click **Management Tools** > **Credit Reporting Wizard** > **Access Credit Reporting Wizard**.

Scope

This permission is available for all scopes.

Policy

N/A

Access Custodian Editor Permission

Use the Access Custodian Editor permission to specify whether users can configure end-of-day processing tasks in Custodian.

Location

In the **Navigation** pane, click **Management Tools** > **Custodian** > **Access Custodian Editor**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Access Dialer Config Permission

Use the Access Dialer Config permission to specify whether users can open Dialer Configuration to create and modify dialer campaigns.

Location

In the **Navigation** pane, click **Management Tools** > **Dialer Config** > **Access Dialer Config**.

Scope

This permission is available for the following scopes:

- System
- Role
- User

Policy

N/A

Access Goal Manager Permission

Use the Access Goal Manager permission to specify whether users can open Goals Manager to view statistics for collectors, supervisors, managers, and owners.

Location

In the **Navigation** pane, click **Management Tools** > **Goals** > **Access Goals Manager**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Archive Settings

Archive Settings

Use the Archive settings to specify permissions and policies for archiving and restoring account data.

Access Archive/Restore Functionality Permission

Use the Access Archive/Restore Functionality permission to specify whether users can archive accounts and restore archived accounts.

Location

In the **Navigation** pane, click **Management Tools** > **Archive** > **Access Archive/Restore Functionality**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

The policy allows your organization to specify which archive functionality is available. Enable the permission for a scope and then select the archive permissions.

Allow user to run Archive Configuration application: If selected, allows the user to run the Archive Configuration program.

Allow user to run Archive/Restore application: If selected, allows the user to run the Archive/Restore program.

Allow user to edit archive relationship: If selected, allows the user to modify the archive relationship.

Allow user to archive account data: If selected, allows the user to archive account data.

Allow user to restore archived data: If selected, allows the user to restore archived data.

Enable Archive of Account Data Permission

Use the Enable Archive of Account Data permission to specify whether Latitude can archive account data.

Location

In the **Navigation** pane, click **Management Tools** > **Archive** > **Enable Archive of Account Data**.

Scope

This permission is available for the System scope only.

Policy

The policy allows your organization to specify which archive processes are available. Enable the permission for a scope and then select the archive process permissions.

Minimum number of months after an account is returned before allowing archive: Minimum number of months after returning an account that must pass before the user can archive the account.

Add note to account after it has been archived: If selected, Latitude adds a note to the account after archiving it.

Log archive operations to ArchiveHistory table: If selected, Latitude logs archive operations to the Archive History table.

Synchronize archive table schema before every archive/restore operation: If selected, Latitude synchronizes table schema before every archive or restore operation. If cleared, users synchronize the schema using the Archive Configuration tool.

Letter Console Settings

Letter Console Settings

Use the Letter Console settings to specify permissions and policies for Letter Console.

Access Letter Console Permission

Use the Access Letter Console permission to specify whether users can open Letter Console to print and modify letters.

Location

In the **Navigation** pane, click **Management Tools** > **Letter Console** > **Access Letter Console**.

Scope

This permission is available for all scopes.

Policy

N/A

Change Settings Permission

Use the Change Settings permission to specify whether users can modify letter settings in Letter Console.

Location

In the **Navigation** pane, click **Management Tools** > **Letter Console** > **Change Settings**.

Scope

This permission is available for all scopes.

Policy

N/A

Create/Delete Permission

Use the Create/Delete permission to specify whether users can create and delete letters in Letter Console.

Location

In the **Navigation** pane, click **Management Tools** > **Letter Console** > **Create/Delete**.

Scope

This permission is available for all scopes.

Policy

N/A

Merge Using Microsoft Word Permission

Use the Merge Using Microsoft Word permission to specify whether users can use Microsoft Word to modify letter templates in Letter Console without having to download, edit, and then upload them. You must have Microsoft Word installed to use this feature. For more information about modifying letter templates using Word, see "Modify a Letter Template Using Microsoft Word" in the Letter Console documentation.

> **Note:** If you disable this permission or don't configure it, you must download the letter template, modify it, and then upload it back to Letter Console. For more information, see "Modify a Letter Template" in the Letter Console documentation.

Location

In the **Navigation** pane, click **Management Tools** > **Letter Console** > **Merge Using Microsoft Word**.

Scope

This permission is available for the following scopes:

- System
- Role
- User

Policy

N/A

Link Console Settings

Link Console Settings

Use the Link Console settings to specify permissions and policies for Link Console.

Access Link Console Permission

Use the Access Link Console permission to specify whether users can open Link Console to modify automatic account linking settings.

Location

In the **Navigation** pane, click **Management Tools** > **Link Console** > **Access Link Console**.

Scope

This permission is available for all scopes.

Policy

N/A

Link Accounts Permission

Use the Link Accounts permission to specify whether users can use Link Console to link accounts manually that belong to the same party.

Location

In the **Navigation** pane, click **Management Tools** > **Link Console** > **Link Accounts**.

Scope

This permission is available for all scopes.

Policy

N/A

Payment Entry Settings

Payment Entry Settings

Use the Payment Entry settings to specify permissions and policies for viewing and managing payments in Latitude Console. For more information, see the *Latitude Console* documentation.

Access Payment Entry Permission

Use the Access Payment Entry permission to specify whether users can open the **Payment Entry** window in Latitude Console.

Location

In the **Navigation** pane, click **Management Tools** > **Payment Entry** > **Access Payment Entry**.

Scope

This permission is available for all scopes.

Policy

The policy allows users to specify the settings for adding payments. Enable the permission for a scope and then specify the settings.

Allow payments to be entered on closed accounts: If selected, allows the user to add payments to closed accounts.

Warn when allowing payments to be entered on closed accounts: If selected, displays a warning when the user adds a payment to closed accounts.

Allow opening of other users batches: If selected, allows the user to open payment batches that other users created.

Allow adding payments to other users batches: If selected, allows the user to add payments to payment batches that other users created.

Allow processing of batches: If selected, allows the user to process payment batches.

Allow processing of other users batches: If selected, allows the user to process payment batches that other users created.

Allow editing of other users batches: If selected, allows the user to modify payment batches that other users created.

Allow deleting of other users batches: If selected, allows the user to delete payment batches that other users created.

Allow editing of other users batch items: If selected, allows the user to modify payment batch items that other users created.

Allow deleting of other users batch items: If selected, allows the user to delete payment batch items that other users created.

Remove Other Users Batch Locks Permission

Use the Remove Other Users Batch Locks permission to specify whether users can unlock payment batches that other users locked in Latitude Console.

Location

In the **Navigation** pane, click **Management Tools** > **Payment Entry** > **Remove Other Users Batch Locks**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Query Designer Settings

Query Designer Settings

Use the Query Designer settings to specify settings for using Query Designer.

User Restrictions by Conditions Permission (Account Analysis)

Use the User Restrictions by Conditions permission to restrict the accounts that the user can modify using Account Analysis.

Location

In the **Navigation** pane, click **Management Tools** > **Query Designer** > **Account Analysis** > **User Restrictions by Conditions**.

Scope

This permission is available for the following scopes:

- System

- Role
- User
- Branch

Policy

N/A

Access Condition Builder Permission

Use the Access Condition Builder permission to specify whether users can open Condition Builder to maintain conditions for Query Designer. This permission is available for all scopes.

Location

In the **Navigation** pane, click **Management Tools** > **Query Designer** > **Condition Builder** > **Access Condition Builder**.

Scope

This permission is available for all scopes.

Policy

N/A

Access Custom Queue Manager Permission

Use the Access Custom Queue Manager permission to specify whether users can open Custom Queue Manager to maintain custom queues.

Location

In the **Navigation** pane, click **Management Tools** > **Query Designer** > **Custom Queue Manager** > **Access Custom Queue Manager**.

Scope

This permission is available for all scopes.

Policy

N/A

Access List Builder Permission

Use the Access List Builder permission to specify whether users can open List Builder to create dialer call lists from List Builder query results.

Location

In the **Navigation** pane, click **Management Tools** > **Query Designer** > **List Builder** > **Access List Builder**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Access Management Suite Extension Wizard Permission

Use the Access Management Suite Extension Wizard permission to specify whether users can open the Management Suite Extension Wizard to create a query for accomplishing a specific task.

Location

In the **Navigation** pane, click **Management Tools** > **Query Designer** > **Extension Wizard** > **Access Latitude Management Suite Extension Wizard**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

CBR Requester Settings

CBR Requester Settings

Use the CBR Requester settings to specify permissions and policies for Credit Report Requester.

Access CBR Requester Permission

Use the Access CBR Requester permission to specify whether users can open Credit Report Requester to request credit bureau reports.

Location

In the **Navigation** pane, click **Management Tools** > **Query Designer** > **CBR Requester** > **Access CBR Requester**.

Scope

This permission is available for all scopes.

Policy

N/A

Services Settings

Services Settings

Use the Services settings to specify permissions for requesting credit bureau reports using Credit Report Requester.

Equifax DTEC Permission

Use the Equifax DTEC permission to specify whether users can request an Equifax DTEC (SSN) report using Credit Report Requester.

Location

In the **Navigation** pane, click **Management Tools** > **Query Designer** > **CBR Requester** > **Services** > **Equifax DTEC**.

Scope

This permission is available for all scopes.

Policy

N/A

Equifax Finders Permission

Use the Equifax Finders permission to specify whether users can request an Equifax Finders report using Credit Report Requester.

Location

In the **Navigation** pane, click **Management Tools** > **Query Designer** > **CBR Requester** > **Services** > **Equifax Finders**.

Scope

This permission is available for all scopes.

Policy

N/A

Equifax Full Permission

Use the Equifax Full permission to specify whether users can request an Equifax full credit report using Credit Report Requester.

Location

In the **Navigation** pane, click **Management Tools** > **Query Designer** > **CBR Requester** > **Services** > **Equifax Full**.

Scope

This permission is available for all scopes.

Policy

N/A

Experian Collect Permission

Use the Experian Collect permission to specify whether users can request an Experian collection report using Credit Report Requester.

Location

In the **Navigation** pane, click **Management Tools** > **Query Designer** > **CBR Requester** > **Services** > **Experian Collect**.

Scope

This permission is available for all scopes.

Policy

N/A

Experian Full Permission

Use the Experian Full permission to specify whether users can request an Equifax full credit report using Credit Report Requester.

Location

In the **Navigation** pane, click **Management Tools** > **Query Designer** > **CBR Requester** > **Services** > **Experian Full**.

Scope

This permission is available for all scopes.

Policy

N/A

Experian SSN Search Permission

Use the Experian SSN Search permission to specify whether users can request an Experian SSN search report using Credit Report Requester.

Location

In the **Navigation** pane, click **Management Tools** > **Query Designer** > **CBR Requester** > **Services** > **Experian SSN Search**.

Scope

This permission is available for all scopes.

Policy

N/A

TransUnion DTEC Permission

Use the TransUnion DTEC permission to specify whether users can request an TransUnion DTEC (SSN) report using Credit Report Requester.

Location

In the **Navigation** pane, click **Management Tools** > **Query Designer** > **CBR Requester** > **Services** > **TransUnion DTEC**.

Scope

This permission is available for all scopes.

Policy

N/A

TransUnion Fact Permission

Use the TransUnion Fact permission to specify whether users can request an TransUnion fact report using Credit Report Requester.

Location

In the **Navigation** pane, click **Management Tools** > **Query Designer** > **CBR Requester** > **Services** > **TransUnion Fact**.

Scope

This permission is available for all scopes.

Policy

N/A

TransUnion Full Permission

Use the TransUnion Full permission to specify whether users can request an TransUnion full credit report using Credit Report Requester.

Location

In the **Navigation** pane, click **Management Tools** > **Query Designer** > **CBR Requester** > **Services** > **TransUnion Full**.

Scope

This permission is available for all scopes.

Policy

N/A

User Restrictions by Conditions Permission (CBR Requester)

Use the User Restrictions by Conditions permission to restrict the accounts for which the user can request a credit bureau report using Credit Report Requester.

Location

In the **Navigation** pane, click **Management Tools** > **Query Designer** > **CBR Requester** > **User Restrictions by Conditions**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Desk Mover Settings

Desk Mover Settings

Use the Desk Mover settings to specify permissions and policies for Desk Mover.

Access Desk Mover Permission

Use the Access Desk Mover permission to specify whether users can open Desk Mover to change desk assignments.

Location

In the **Navigation** pane, click **Management Tools** > **Query Designer** > **Desk Mover** > **Access Desk Mover**.

Scope

This permission is available for all scopes.

Policy

N/A

User Restrictions by Conditions Permission (Desk Mover)

Use the User Restrictions by Conditions permission to restrict the accounts that the user can move to another desk using Desk Mover.

Location

In the **Navigation** pane, click **Management Tools** > **Query Designer** > **Desk Mover** > **User Restrictions by Conditions**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Letter Requester Settings

Letter Requester Settings

Use the Letter Requester settings to specify permissions and policies for Letter Requester.

Access Letter Requester Permission

Use the Access Letter Requester permission to specify whether users can open Letter Requester to request letters.

Location

In the **Navigation** pane, click **Management Tools** > **Query Designer** > **Letter Requester** > **Access Letter Requester**.

Scope

This permission is available for all scopes.

Policy

N/A

SIF Letters Permission

Use the SIF Letters permission to specify whether users can create Settled in Full (SIF) letter requests using Letter Requester.

Location

In the **Navigation** pane, click **Management Tools** > **Query Designer** > **Letter Requester** > **SIF Letters**.

Scope

This permission is available for all scopes.

Policy

N/A

User Restrictions by Conditions Permission (Letter Requester)

Use the User Restrictions by Conditions permission to restrict the accounts for which the user can request a letter using Letter Requester.

Location

In the **Navigation** pane, click **Management Tools** > **Query Designer** > **Letter Requester** > **User Restrictions by Conditions**.

Scope

This permission is available for the following scopes:

- System

- Role
- User
- Branch

Policy

N/A

Restrict Conditions Permission

Use the Restrict Conditions permission to specify the conditions available to the user in Query Designer.

Location

In the **Navigation** pane, click **Management Tools** > **Query Designer** > **Restrict Conditions**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

The policy allows your organization to limit the number of conditions that are available to users. Enable the permission for a scope and then specify the conditions to allow. Conditions appear alphabetically within their folders.

Restrict user to only allow the following conditions: If selected, users can select the specified conditions only when using Query Designer.

Conditions: If selected, the condition is available to users.

Select None: Clears all selected items in the list.

Select All: Selects all items in the list.

> **Tip**: To select multiple sequential conditions, press and hold the **Shift** key and then click the first and last sequential condition. To select multiple non-sequential conditions, press and hold the **Ctrl** key and then click each individual condition.

Status Changer Settings

Status Changer Settings

Use the Status Changer settings to specify permissions and policies for Status Changer.

Access Status Changer Permission

Use the Access Status Changer permission to specify whether users can open Status Changer to change the status of a group of accounts.

Location

In the **Navigation** pane, click **Management Tools** > **Query Designer** > **Status Changer** > **Access Status Changer**.

Scope

This permission is available for all scopes.

Policy

N/A

User Restrictions by Conditions Permission (Status Changer)

Use the User Restrictions by Conditions permission to restrict the accounts for which users can change the status using Status Changer.

Location

In the **Navigation** pane, click **Management Tools** > **Query Designer** > **Status Changer** > **User Restrictions by Conditions**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

N/A

Use Literal Conditions Permission

Use the Use Literal Conditions permission to specify whether users can create a condition in Query Designer called "Literal Condition" and specify a block of SQL to use instead of the predefined conditions.

Location

In the **Navigation** pane, click **Management Tools** > **Query Designer** > **Use Literal Conditions**.

Scope

This permission is available for all scopes.

Policy

N/A

Security Settings

Security Settings

Security Settings

Use the Security settings to specify permissions and policies for locking user accounts and managing user passwords.

Account Lockout Permission

Use the Account Lockout permission to specify the settings for locking a user's account when the user's attempt to log on to Latitude is unsuccessful.

Location

In the **Navigation** pane, click **Security** > **Account Lock Out Policy**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

The policy allows your organization to specify settings for unsuccessful logon attempts. Enable the permission for a scope and then specify the settings.

Maximum unsuccessful attempts: Maximum number of unsuccessful logon attempts allowed before Latitude locks the user account.

Duration of account lockout (min): Length of time in minutes that the account remains locked after an unsuccessful logon attempt.

API Key Manager

API Key Manager

You can generate and assign API keys to users to allow them to use the Latitude Web Service without requiring a user name and password in a configuration file. When a user sends a request to the Web Service using a valid API key, the system logs all activity to the user associated to that key. For example, external developers can send requests from their web application to query the Latitude Web Service for account information. Examples of external applications include web services, Windows services, desktop applications, and anything else that can send an HTTP request to access the Latitude Web Service.

Location

In the **Navigation** pane, click **Security** > **API Key Manager**.

Scope

This permission is available for the system scope only.

Policy

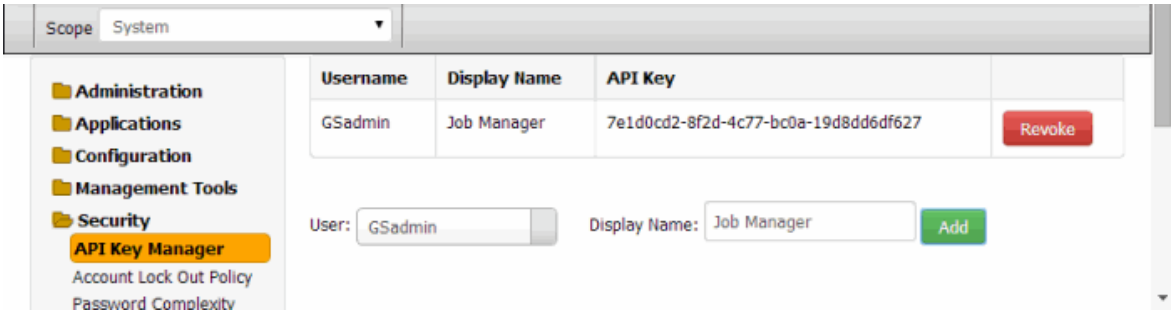
N/A

Add an API Key

Use the **API Key Manager** panel to generate and assign an API key to a user.

To add an API key

1. In the **Navigation** pane, click **Security** > **API Key Manager**.



User: Latitude User ID to assign to the API key.

Display Name: Name that identifies the API key assignment for internal reference. For example, you can use the display name to identify where to use the key.

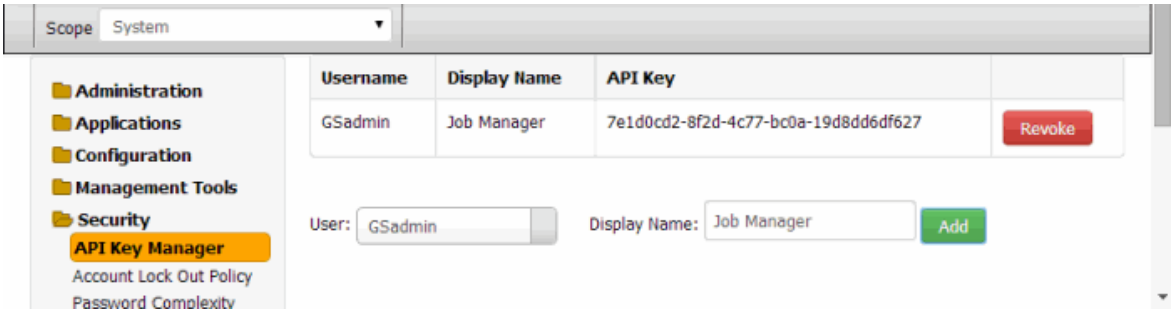
2. Complete the information and then click **Add**. The system assigns a unique API key to the user and adds it to the data grid.

Revoke an API Key

Use the **API Key Manager** panel to revoke an API key assigned to a user. Once revoked, the system denies requests to the Latitude Web Service using that API key.

To revoke an API key

1. In the **Navigation** pane, click **Security** > **API Key Manager**.



2. In the data grid, click **Revoke**. The system revokes the API key and removes it from the data grid.

Password Complexity Permission

Use the Password Complexity permission to specify the requirements for creating a user password for Latitude.

Location

In the **Navigation** pane, click **Security** > **Password Complexity**.

Scope

This permission is available for the following scopes:

- System
- Role
- User
- Branch

Policy

The policy allows your organization to specify requirements for creating passwords. Enable the permission for a scope and then specify the requirements.

Minimum characters: Minimum number of characters required when creating a password.

Minimum character classes: Minimum number of different types of characters required when creating a password. Character classes include:

- Uppercase letters (A-Z)
- Lowercase letters (a-z)
- Numbers (0-9)
- Special characters (for example, ~!@#$%)
- Control characters (for example, LF, TAB)

Password Expiration Permission

Use the Password Expiration permission to specify the settings for the expiration of user passwords in Latitude.

Location

In the **Navigation** pane, click **Security** > **Password Expiration**.

Scope

This permission is available for the following scopes:

- System
- Role
- User

- Branch

Policy

The policy allows your organization to specify settings for the expiration of passwords. Enable the permission for a scope and then specify the settings.

Maximum password age (days): Maximum number of days that users can use a password before it expires. If you set this value to zero, passwords never expire.

Minimum password age (days): Minimum number of days required to use a password before a user can change it. If you set this value to zero, users can change their password any time.

Enforce password history: Number of unique new passwords required before a user can reuse an old password.

Access Services Permission

Use the Access Services permission to specify whether users can view the Services menu in Fusion.

Location

In the **Navigation** pane, click **Services** > **Access Services**.

Scope

This permission is available for the all scopes.

Policy

N/A

System Codes and Settings

System Codes and Settings

Users with the System Codes and Settings Permission can customize codes and settings in the Latitude suite of products. For example, you can set up money buckets for storing money amounts related to an account. You can also set up letter types, claim types, status codes, payment methods, and various other codes.

For information about sorting and filtering data, see Data Grids.

Account Codes

Account Codes

You can set up and configure system account-related codes.

Anchor Cards

Anchor Cards

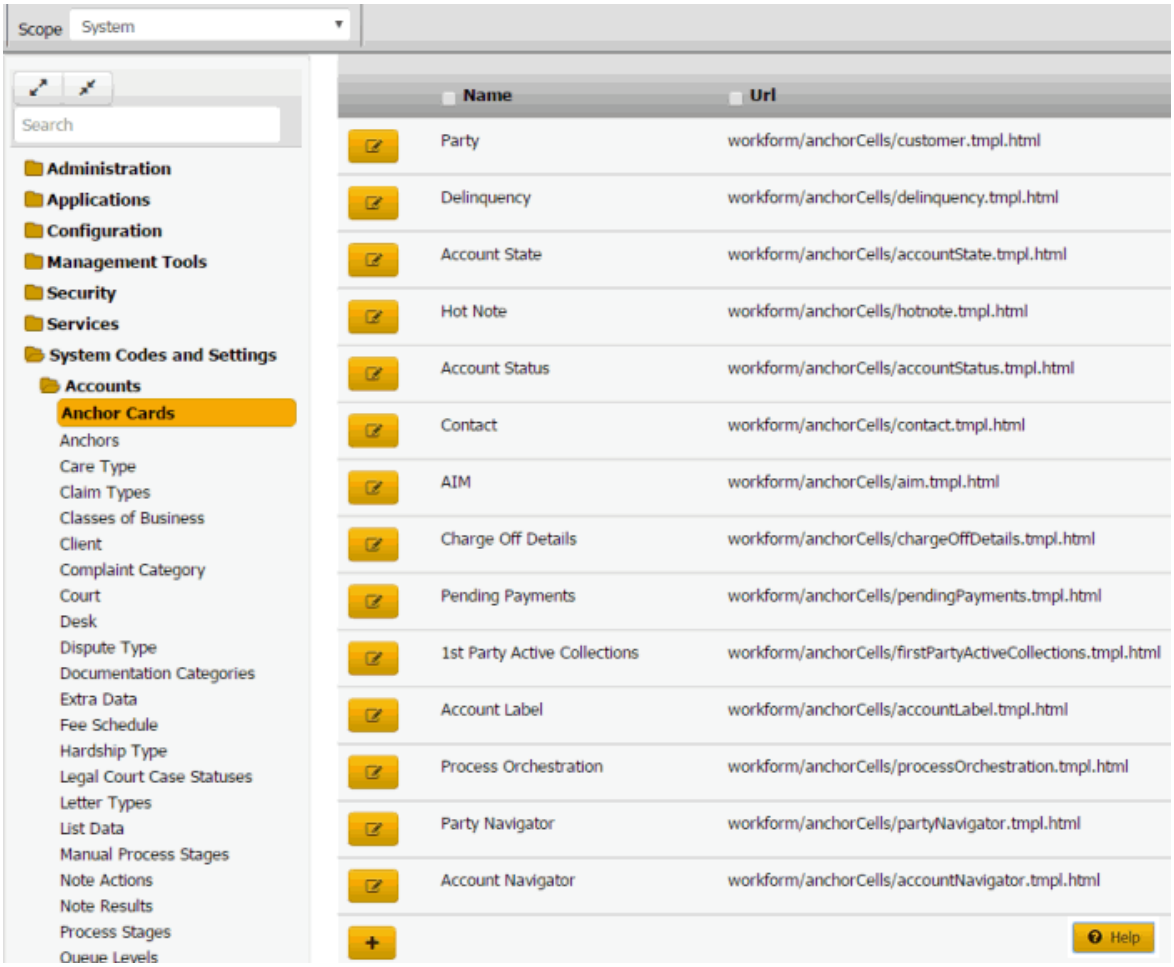
You can search for, add, and modify anchor cards to display in anchors. Anchors allow you to group anchor cards and display them in the **Work Form**. For more information, see Delinquency or Recovery Anchor.

Add an Anchor Card

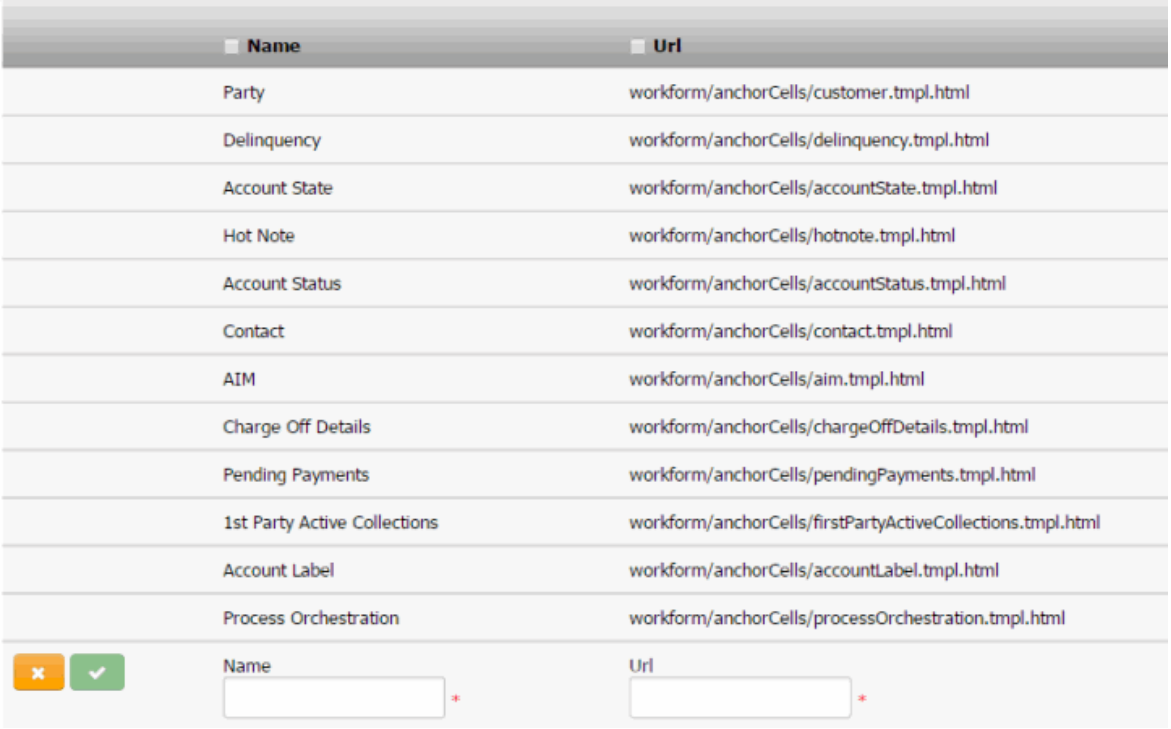
Use the **Anchor Cards** panel to add an anchor card.

To add an anchor card

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Anchor Cards**.



2. Click the plus sign (+). A blank row appears in the data grid.



Name	Url
Party	workform/anchorCells/customer.tmpl.html
Delinquency	workform/anchorCells/delinquency.tmpl.html
Account State	workform/anchorCells/accountState.tmpl.html
Hot Note	workform/anchorCells/hotnote.tmpl.html
Account Status	workform/anchorCells/accountStatus.tmpl.html
Contact	workform/anchorCells/contact.tmpl.html
AIM	workform/anchorCells/aim.tmpl.html
Charge Off Details	workform/anchorCells/chargeOffDetails.tmpl.html
Pending Payments	workform/anchorCells/pendingPayments.tmpl.html
1st Party Active Collections	workform/anchorCells/firstPartyActiveCollections.tmpl.html
Account Label	workform/anchorCells/accountLabel.tmpl.html
Process Orchestration	workform/anchorCells/processOrchestration.tmpl.html
Name *	Url *

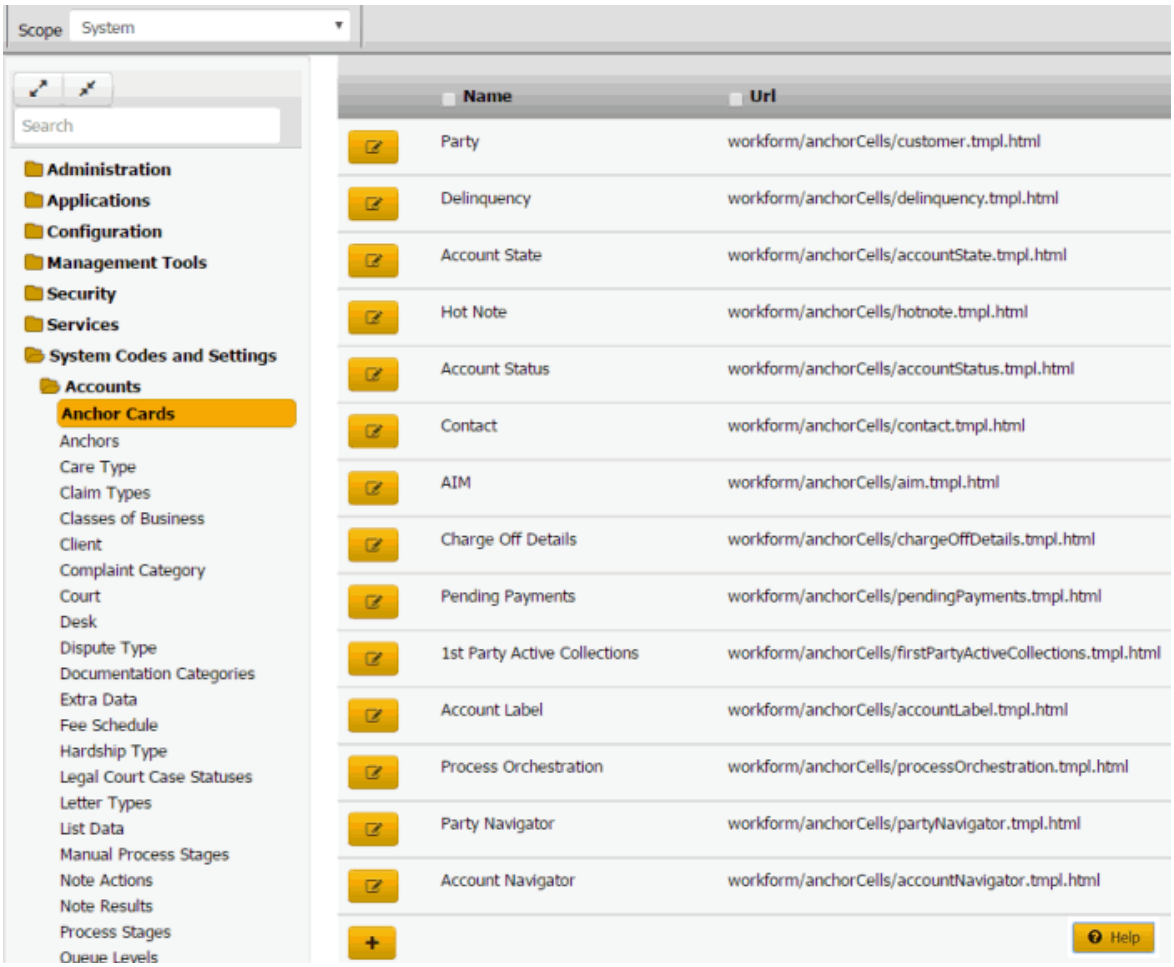
3. In the **Name** box, type the name of the anchor card.
4. In the **URL** box, type the path to the anchor card application page. For example, "workform/anchorCells/customer.tmpl.html."
5. Click the check mark.

Modify an Anchor Card

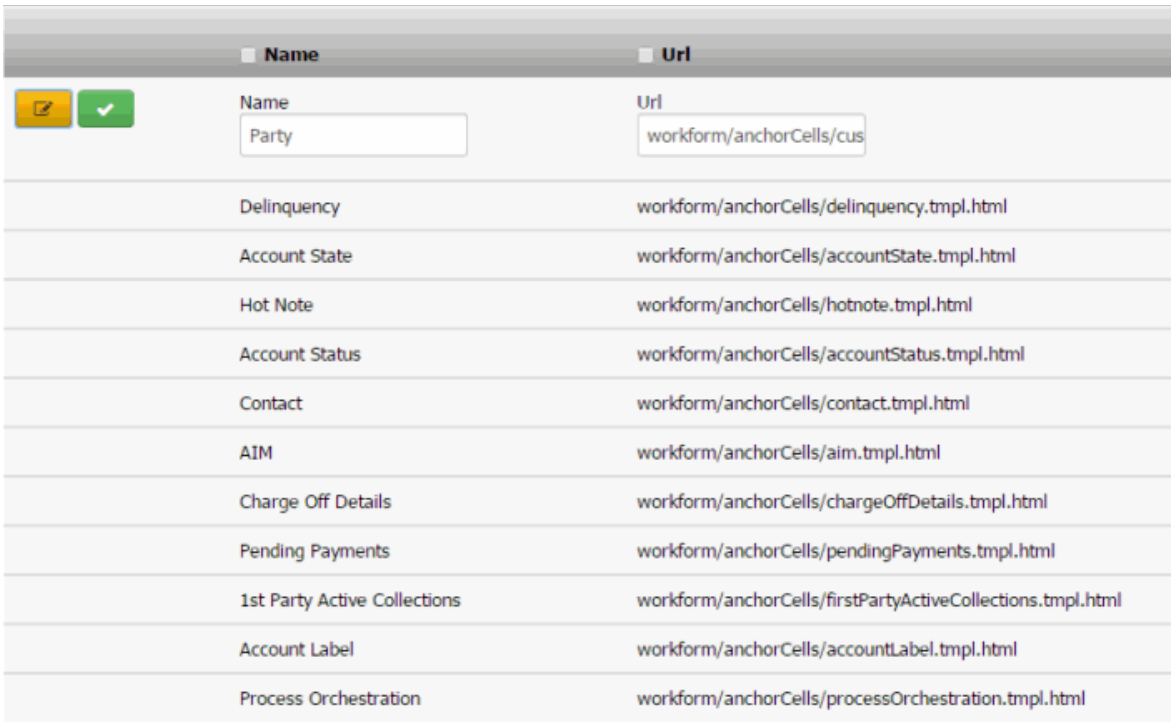
Use the **Anchor Cards** panel to modify an anchor card.

To modify an anchor card

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Anchor Cards**.



2. Click the Edit icon. The anchor card appears in edit mode.



Name	Url
Name: Party	Url: workform/anchorCells/cus
Delinquency	workform/anchorCells/delinquency.tmpl.html
Account State	workform/anchorCells/accountState.tmpl.html
Hot Note	workform/anchorCells/hotnote.tmpl.html
Account Status	workform/anchorCells/accountStatus.tmpl.html
Contact	workform/anchorCells/contact.tmpl.html
AIM	workform/anchorCells/aim.tmpl.html
Charge Off Details	workform/anchorCells/chargeOffDetails.tmpl.html
Pending Payments	workform/anchorCells/pendingPayments.tmpl.html
1st Party Active Collections	workform/anchorCells/firstPartyActiveCollections.tmpl.html
Account Label	workform/anchorCells/accountLabel.tmpl.html
Process Orchestration	workform/anchorCells/processOrchestration.tmpl.html

3. Modify the information and then click the check mark.

Anchors

Anchors

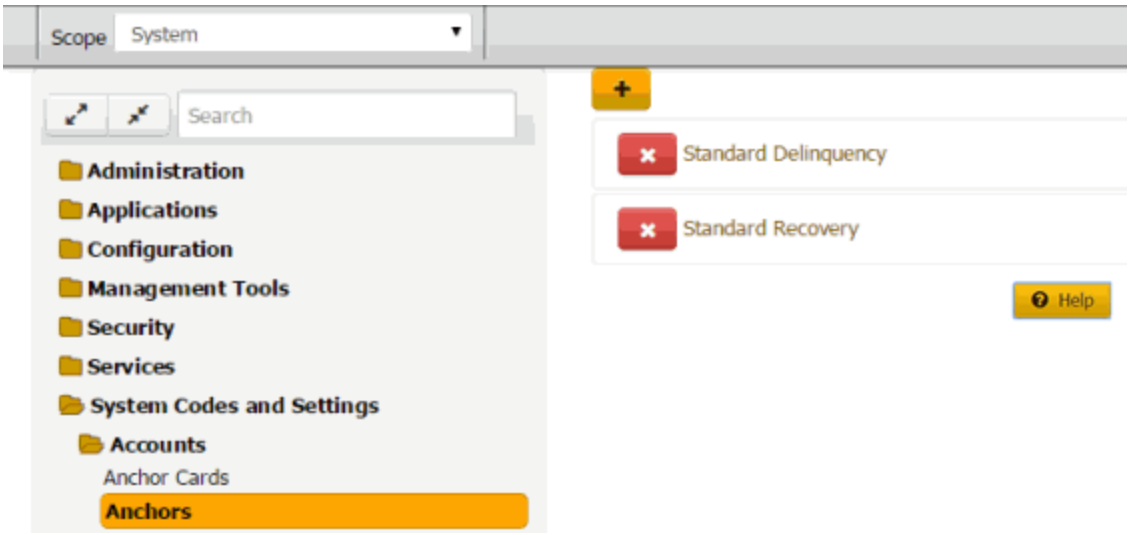
You can add anchors, delete anchors, add anchor cards to an anchor, and remove anchor cards from an anchor. Anchors allow you to group anchor cards and display them in the **Work Form**. For more information, see Delinquency or Recovery Anchor.

Add an Anchor

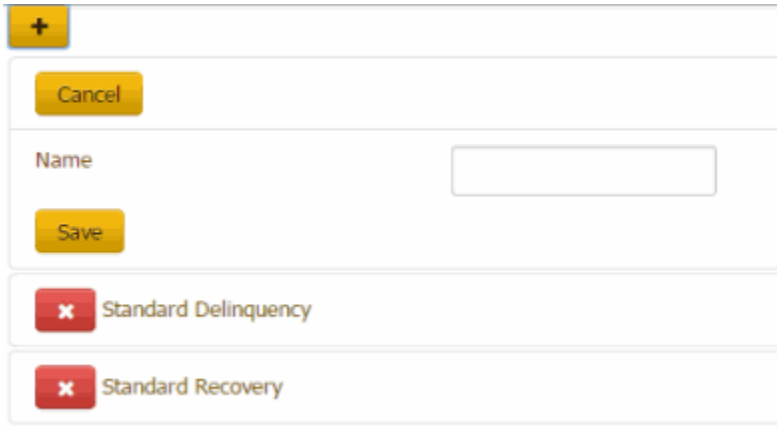
Use the **Anchors** panel to add an anchor.

To add an anchor

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Anchors**.



2. Click the plus sign (+). The panel appears in add mode.



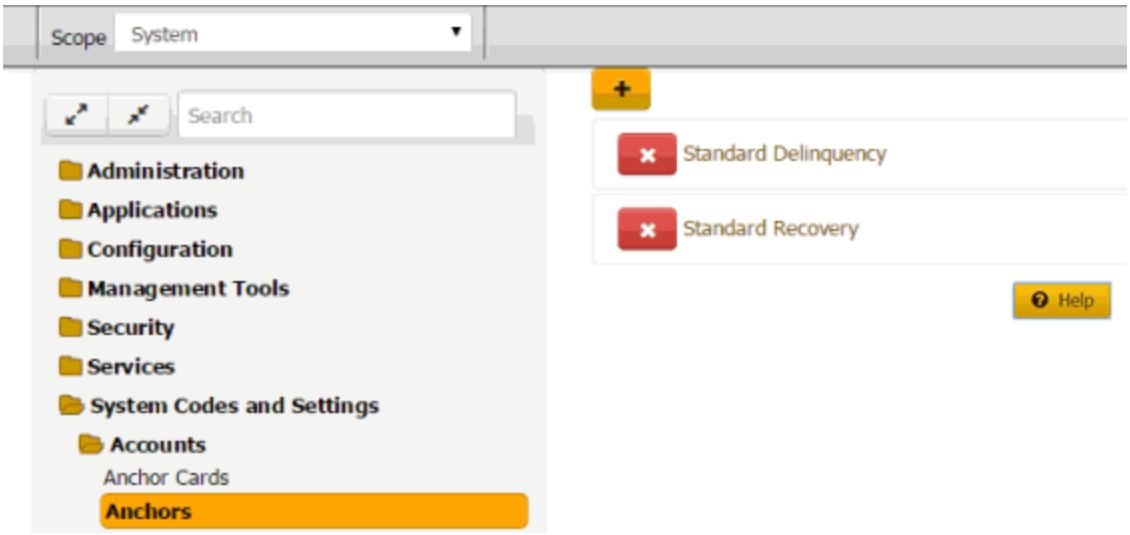
3. In the **Name** box, type the name of the anchor and then click **Save**.

Delete an Anchor

Use the **Anchors** panel to delete an anchor.

To delete an anchor

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Anchors**.



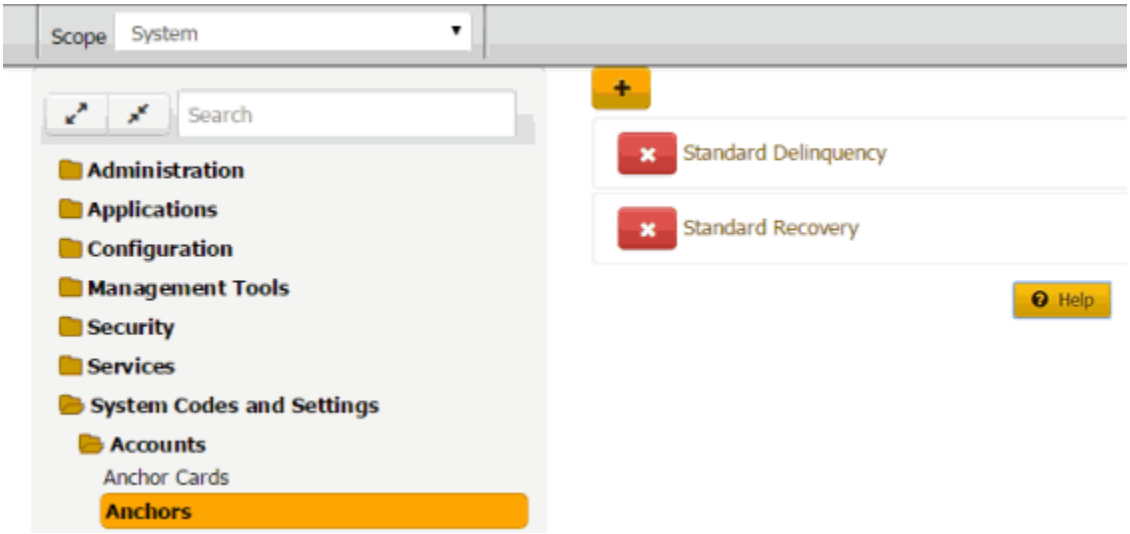
2. Click the Delete icon and then click **Yes**.

Add an Anchor Card to an Anchor

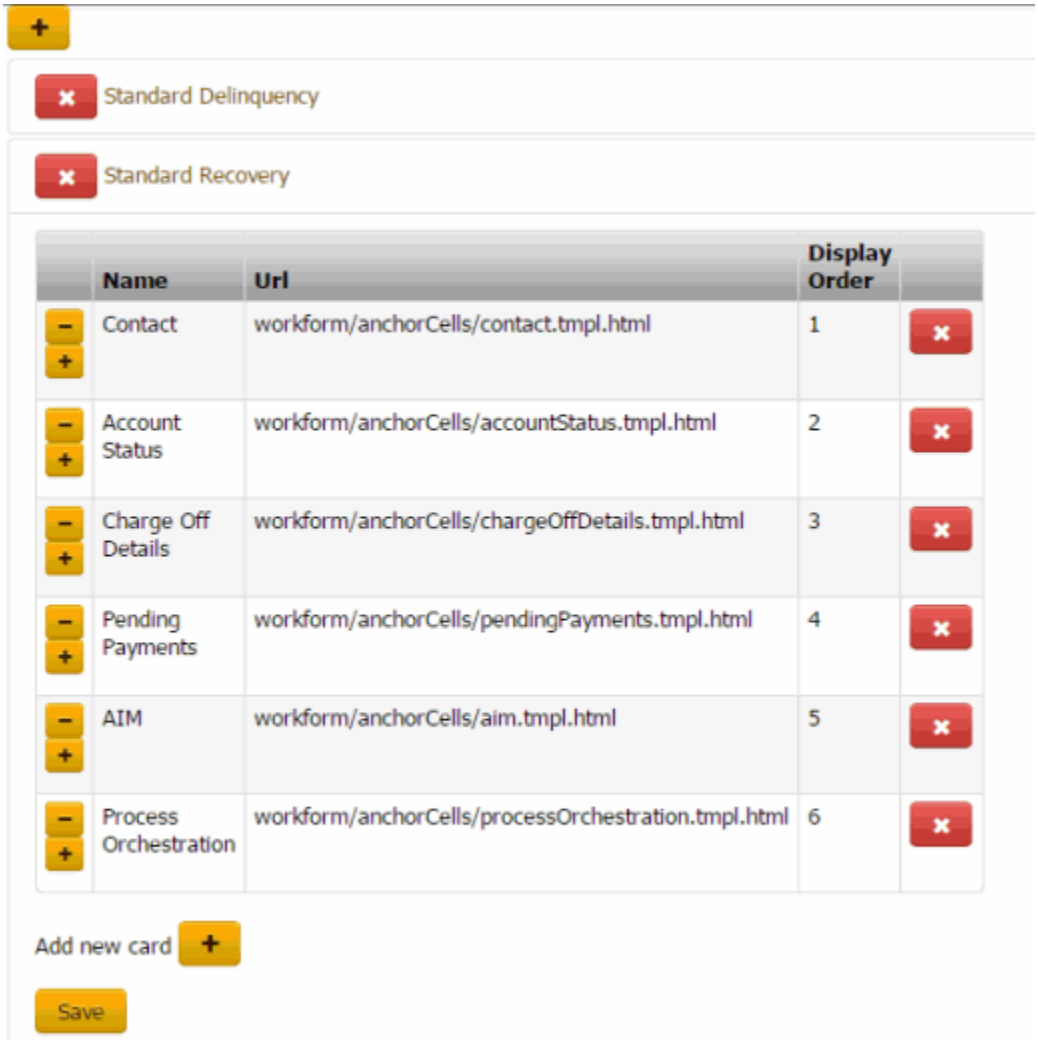
Use the **Add Anchor Cell** dialog box to add an anchor card to an anchor.

To add an anchor card to an anchor

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Anchors**.



2. Click the anchor to which to add an anchor card. The anchor expands.



3. Under the data grid, click the plus sign (+). The **Add Anchor Cell** dialog box appears.

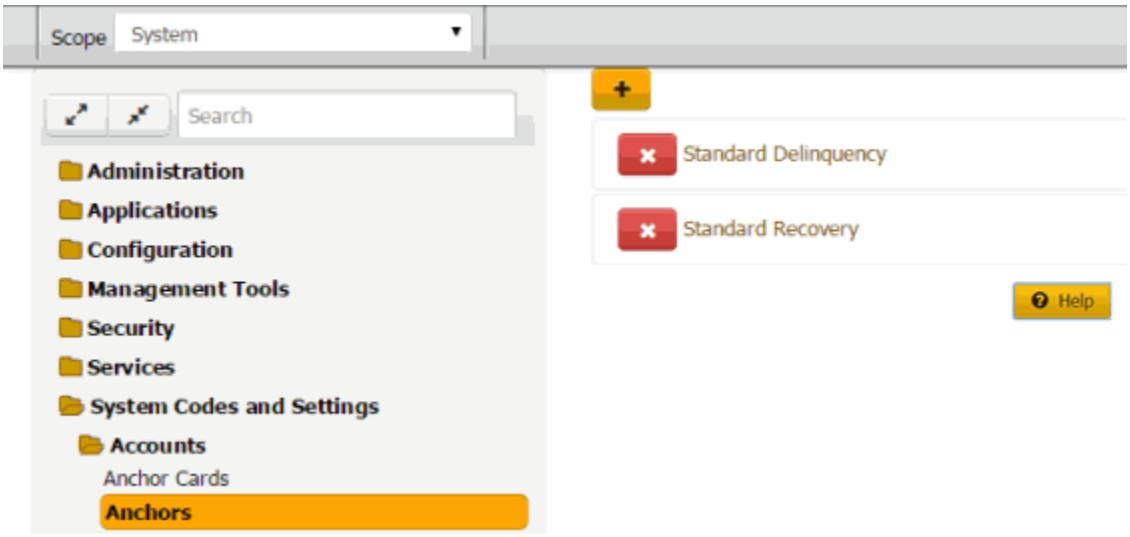
4. In the list box, click the anchor card to add to the anchor and then click **Save**. The system adds the anchor card to the data grid.
5. To change the card's display order, click the minus sign (-) to move up the card in the list. Click the plus sign (+) to move down the card in the list.
6. Click **Save**.

Delete an Anchor Card From an Anchor

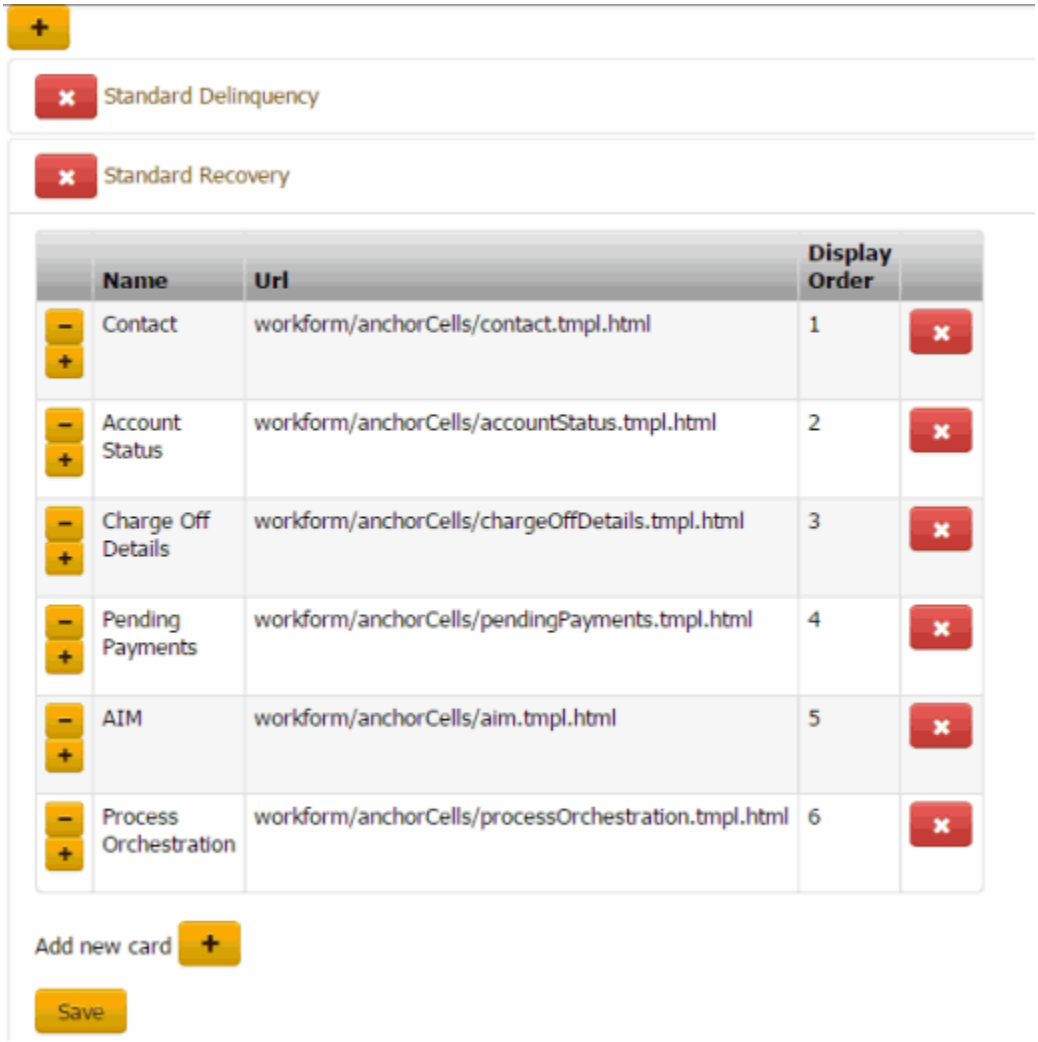
Use the **Anchor Card** panel to delete an anchor card from an anchor.

To delete an anchor card from an anchor

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Anchors**.



2. Click the anchor to modify. The anchor expands.



3. In the data grid, click the Delete icon and then click **OK**.

Care Types

Care Types

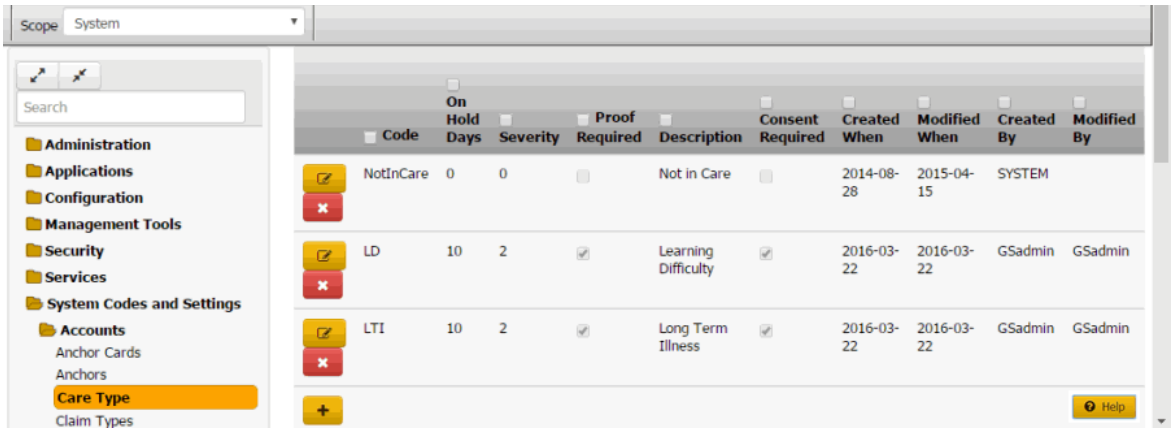
You can add, modify, and delete customer care types, such as armed forces, prison, and family bereavement. Users specify a care type when creating care cases. For more information, see Add a Care or Financial Hardship Case.

Add a Care Type

Use the **Care Type** panel to add a care type.

To add a care type

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Care Type**.



Code: Code that identifies the type of care, such as long-term illness or literacy issues.

On Hold Days: Default number of days to place the account on hold to suspend collection activity.

Severity: Level of severity (1-10) for the care type.

Proof Required: If selected, your organization requires proof of the need for care.

Description: Description of the care type.

Consent: If selected, you have consent from the customer to discuss care and financial hardship information.

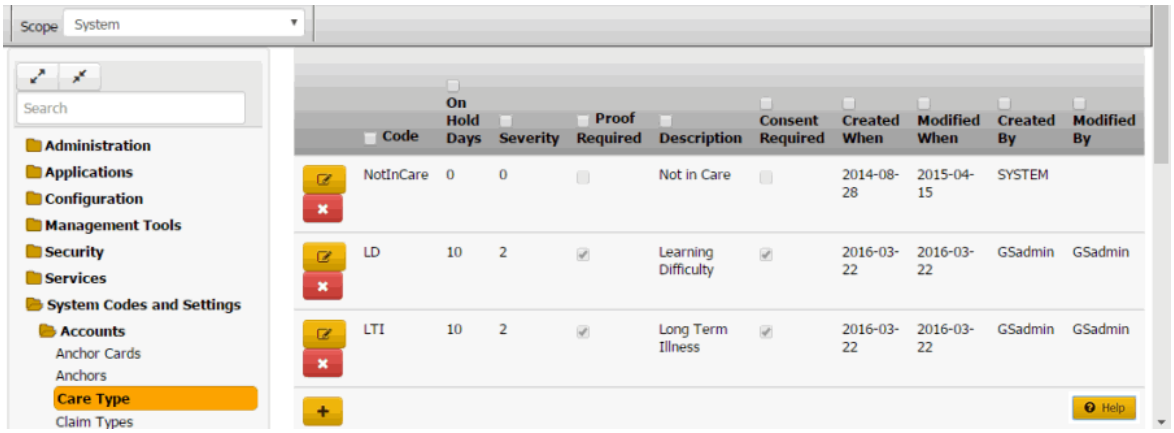
2. Click the plus sign (+). A blank row appears in the data grid.
3. Complete the information and then click the check mark.

Modify a Care Type

Use the **Care Type** panel to modify a care type.

To modify a care type

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Care Type**.



Code: Code that identifies the type of care, such as long-term illness or literacy issues.

On Hold Days: Default number of days to place the account on hold to suspend collection activity.

Severity: Level of severity (1-10) for the care type.

Proof Required: If selected, your organization requires proof of the need for care.

Description: Description of the care type.

Consent: If selected, you have consent from the customer to discuss care and financial hardship information.

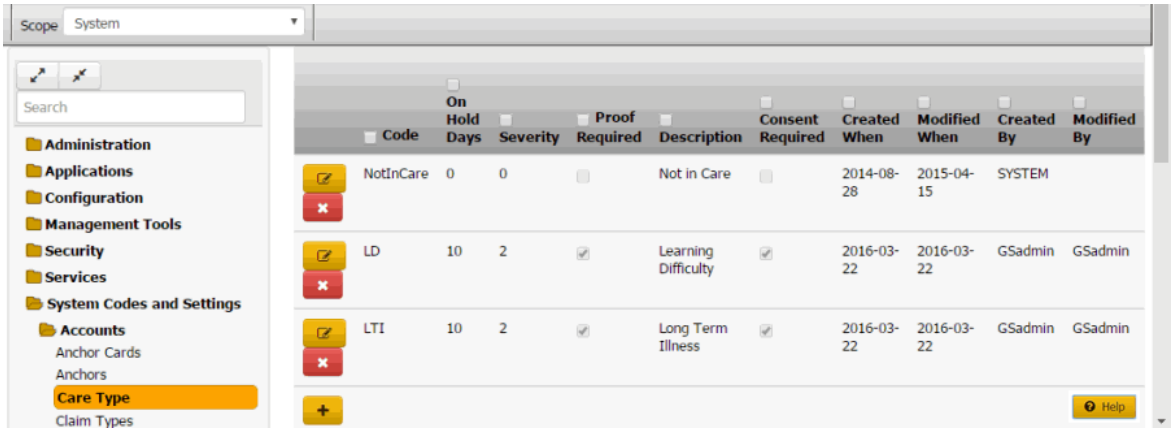
2. Click the Edit icon. The care type appears in edit mode.
3. Modify the information and then click the check mark.

Delete a Care Type

Use the **Care Type** panel to delete a care type.

To delete a care type

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Care Type**.



2. Click the Delete icon and then click **Yes**.

Claim Types

Claim Types

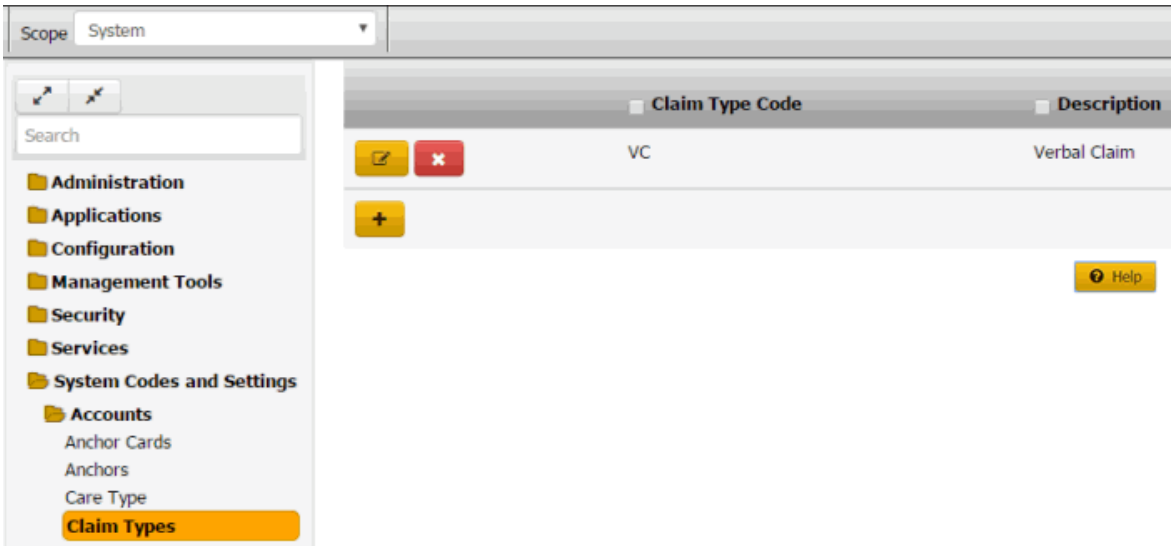
You can search for, add, modify, and delete claim types. The system uses claim types to determine the statute of limitations.

Add a Claim Type

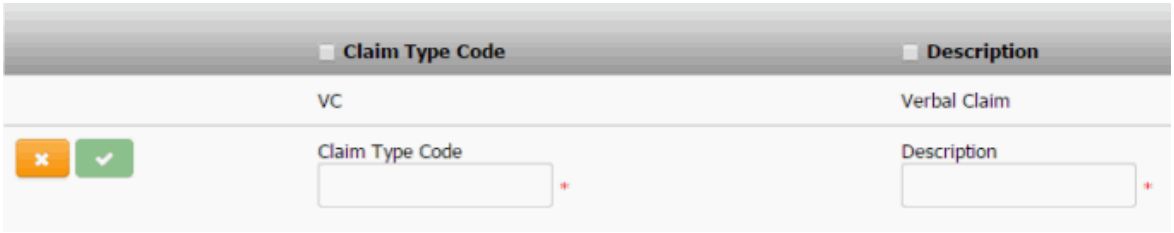
Use the **Claim Types** panel to add a claim type.

To add a claim type

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Claim Types**.



2. Click the plus sign (+). A blank row appears in the data grid.



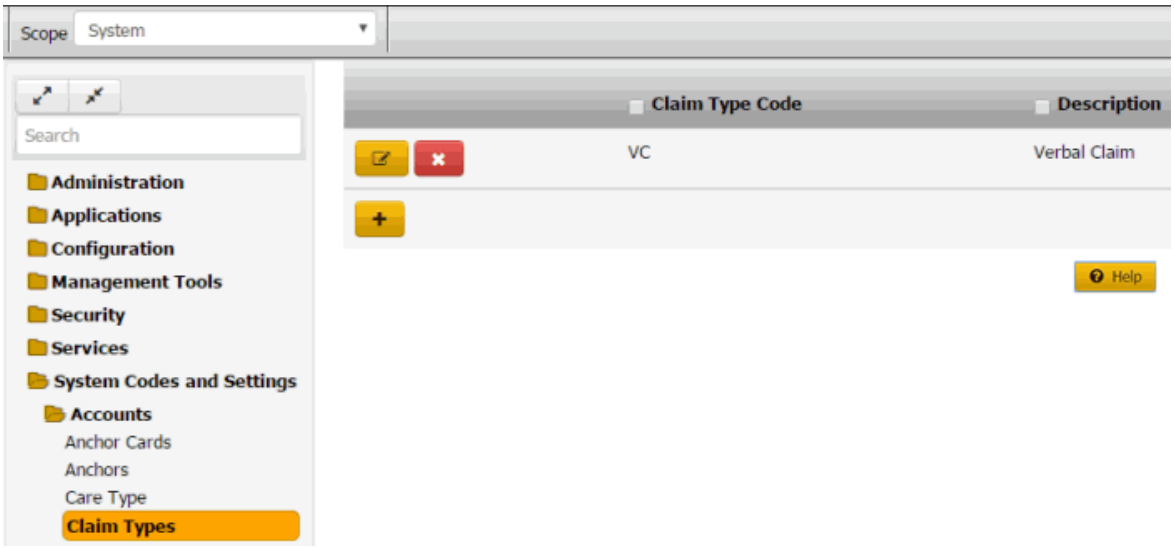
3. In the **Claim Type Code** box, type a unique code for the claim type.
4. In the **Description** box, type a description of the claim type.
5. Click the check mark.

Modify a Claim Type

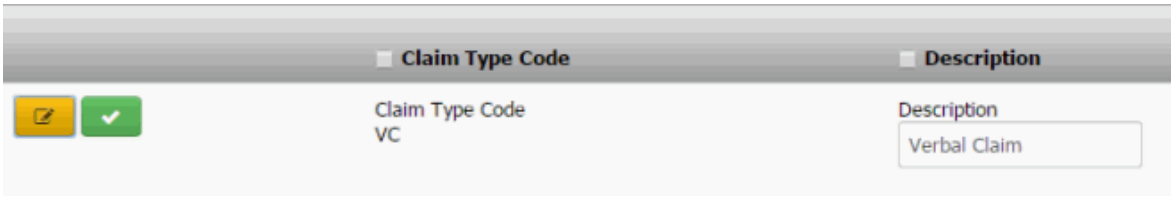
Use the **Claim Types** panel to modify a claim type.

To modify a claim type

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Claim Types**.



2. Click the Edit icon. The claim type appears in edit mode.



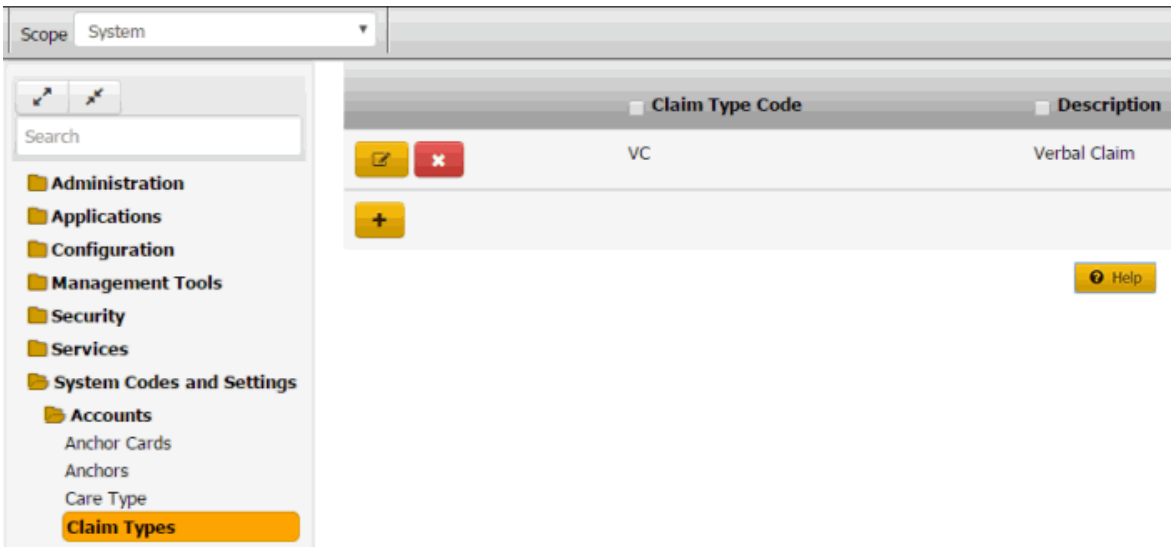
3. Modify the information and then click the check mark.

Delete a Claim Type

Use the **Claim Types** panel to delete a claim type.

To delete a claim type

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Claim Types**.



2. Click the Delete icon and then click **Yes**.

Classes of Business

Classes of Business

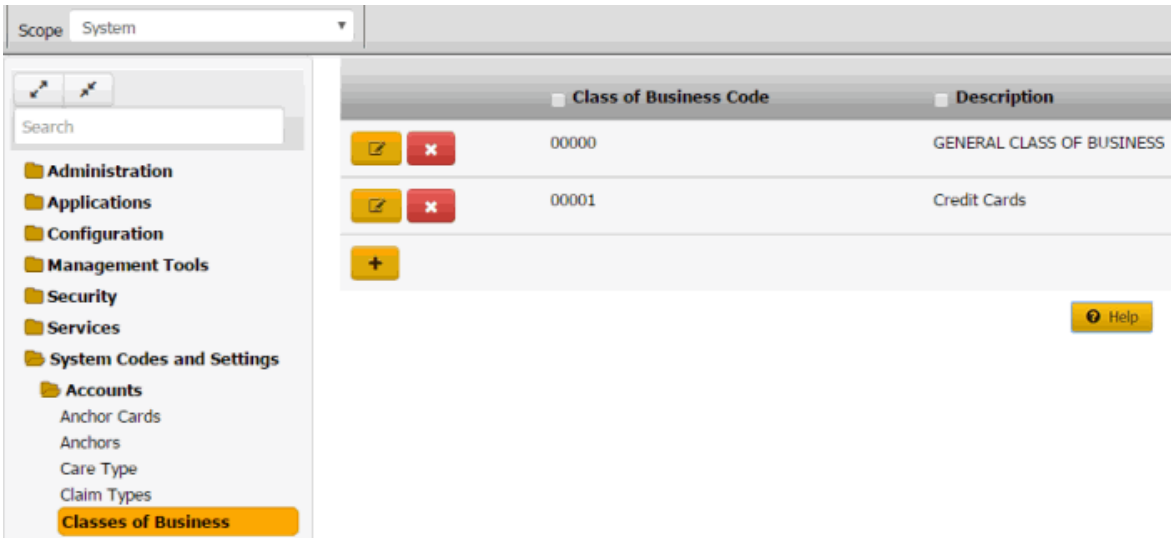
You can search for, add, modify, and delete classes of business. You assign classes of business to clients to group them according to the type of company each of your clients represents. For more information, see Maintain Client Account Information. For imported accounts, Latitude assigns the class of business.

Add a Class of Business

Use the **Classes of Business** panel to add a class of business.

To add a class of business

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Classes of Business**.



2. Click the plus sign (+). A blank row appears in the data grid.

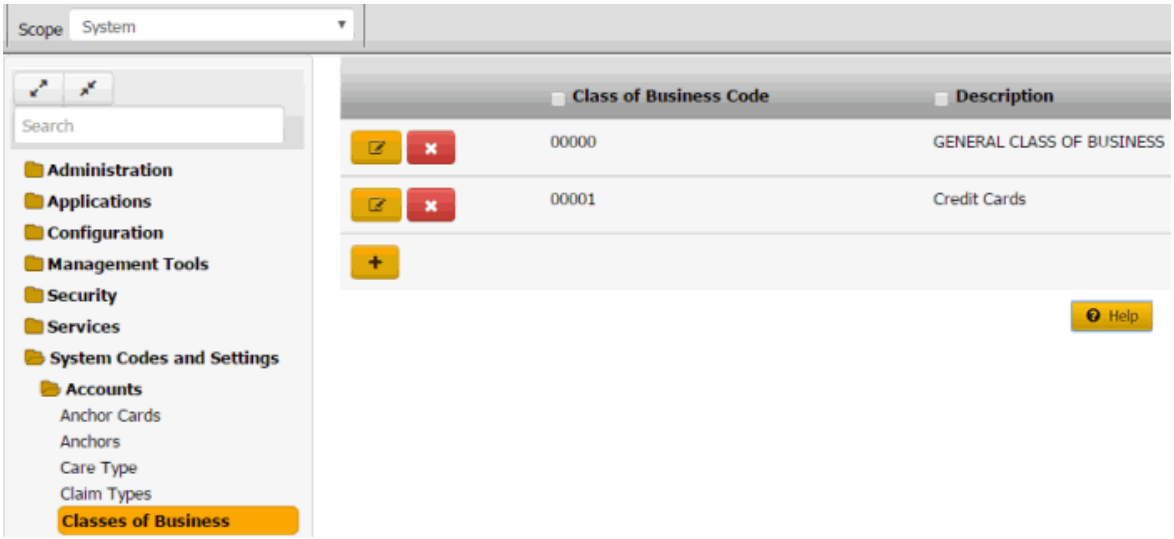
3. In the **Class of Business Code** box, type a unique code for the class of business.
4. In the **Description** box, type a description of the class of business.
5. Click the check mark.

Modify a Class of Business

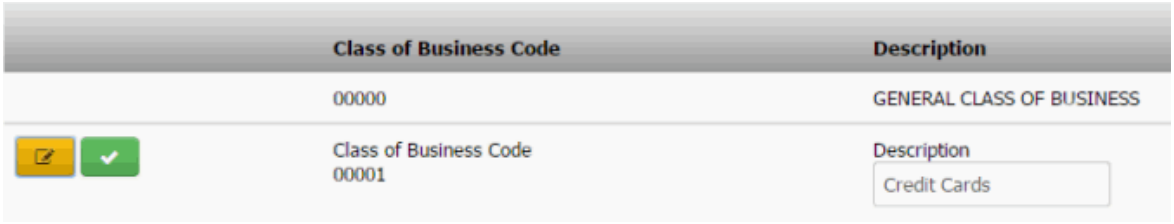
Use the **Classes of Business** panel to modify a class of business.

To modify a class of business

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Classes of Business**.



2. Click the Edit icon. The class of business appears in edit mode.



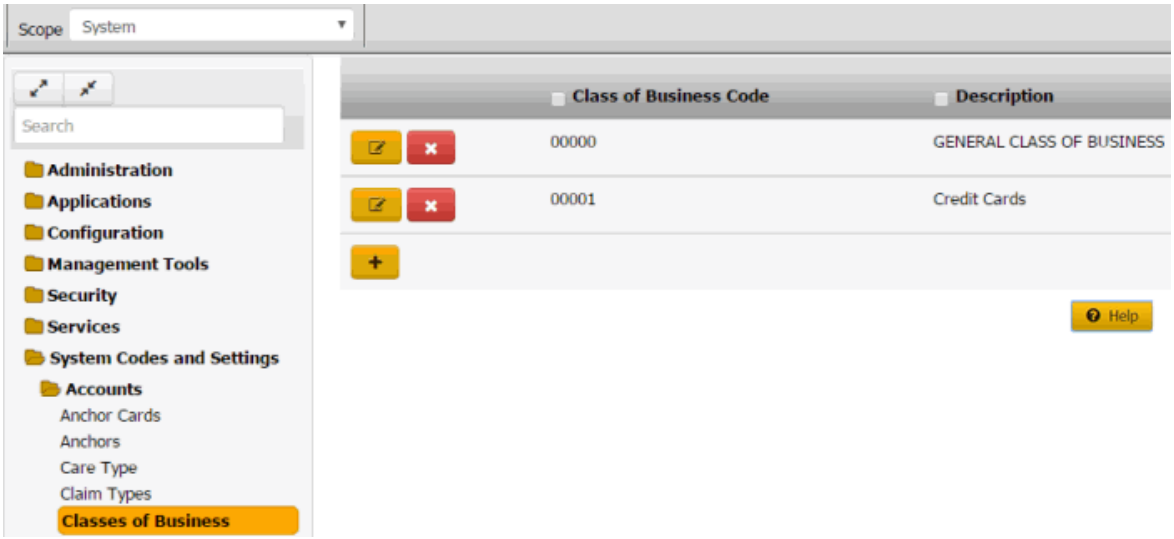
3. Modify the description and then click the check mark.

Delete a Class of Business

Use the **Classes of Business** panel to delete a class of business.

To delete a class of business

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Classes of Business**.



2. Click the Delete icon and then click **Yes**.

Clients

Clients

You can add and modify clients, but you cannot delete them.

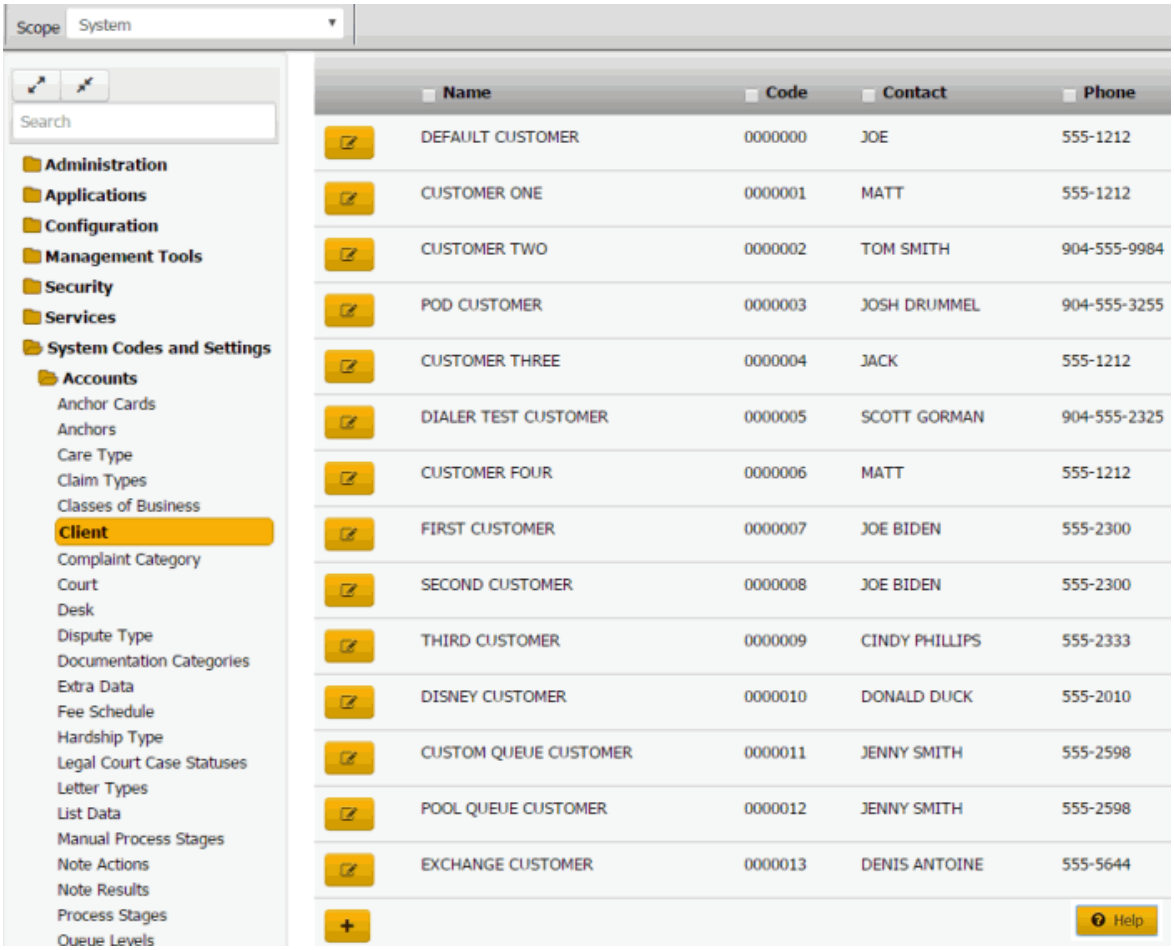
> **Note:** To add a client to a client group, use Latitude Console. For more information, see *Customer Groups* in the Latitude Console documentation. Clients are still referred to as "customers" in Latitude Console.

Add a Client

Use the **General** tab in the **Client** dialog box to maintain general information for a client.

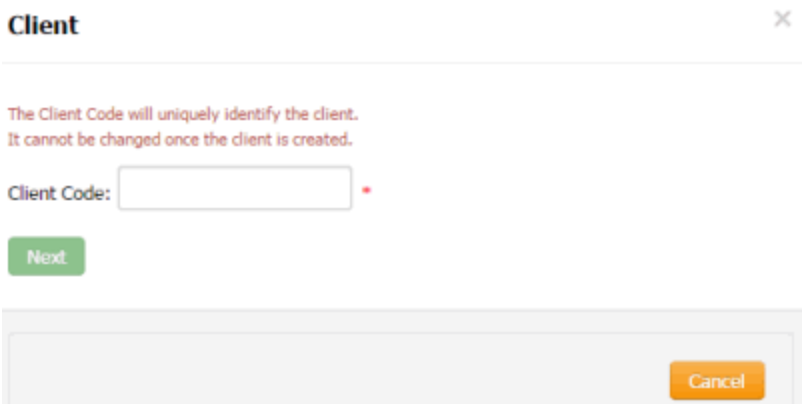
To maintain general client information

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Client**.

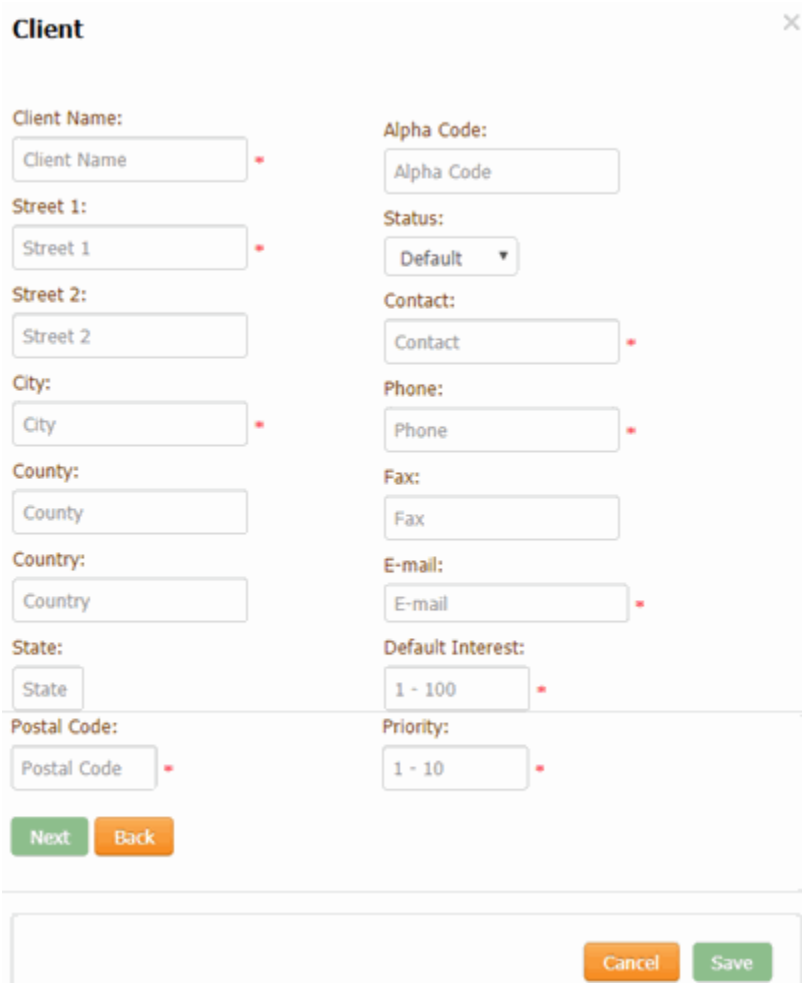


> **Tip:** To limit the clients that display in the data grid, click one or more check boxes next to a column heading. In the **Filter** box, type one or more characters and then press **Enter**. To clear a filter, clear the check boxes and then click the Refresh icon.

2. Click the plus sign (+).



3. In the **Client Code** box, type a unique code to identify the client and then click **Next**.



Client Name: Full name of the client.

Street 1: First line of the client's street address.

Street 2: Second line of the client's street address.

City: Client's city.

County: Client's county.

Country: Client's country.

State: Client's state.

Postal Code: Client's postal code.

Alpha Code: Generic code used for conversions from other systems. Allows your organization to reference any code associated to the client previously.

Status: Status of the account.

Contact: Full name of the contact person.

Phone: Contact person's phone number.

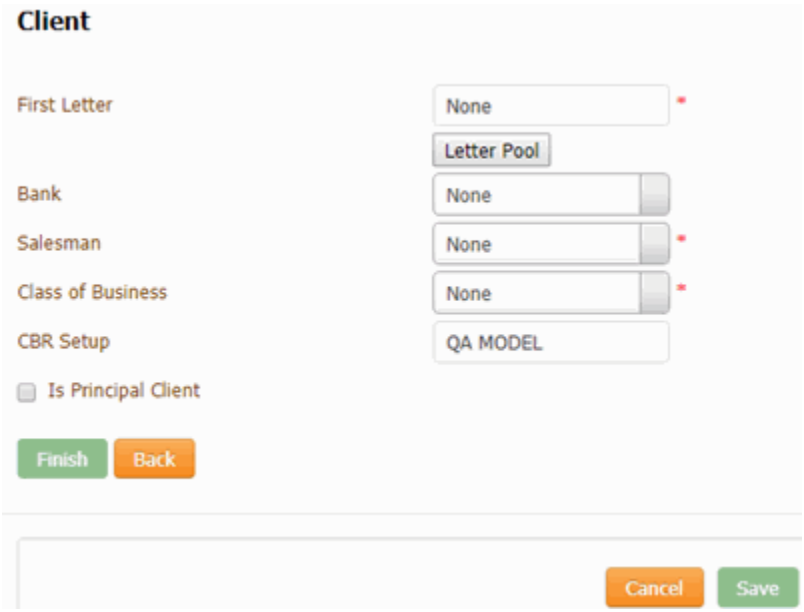
Fax: Contact person's fax number.

Email: Contact person's email address.

Default Interest: Interest rate to assign to new accounts imported for this client. You can override the rate using Exchange or manually. For more information, see Maintain General Client Information.

Priority: Sets the priority when spreading payments across linked accounts. Generally, the values are 1-10 (with 10 being the highest priority). You can assign the same priority to clients. Maximum settings allow up to 255 priorities.

4. Complete the information and then click **Next**.



First Letter: First letter to generate for new accounts. For information about managing letters, see the *Letter Console* documentation.

Bank: If your organization prints checks for the client, this value is the trust account your organization uses for this client. For information about setting up trust accounts and printing checks, see the *Invoices* documentation.

Salesman: Salesman handling this client account. For more information, see Salesman.

Class of Business: Class of business to assign to this client account. For more information, see Classes of Business.

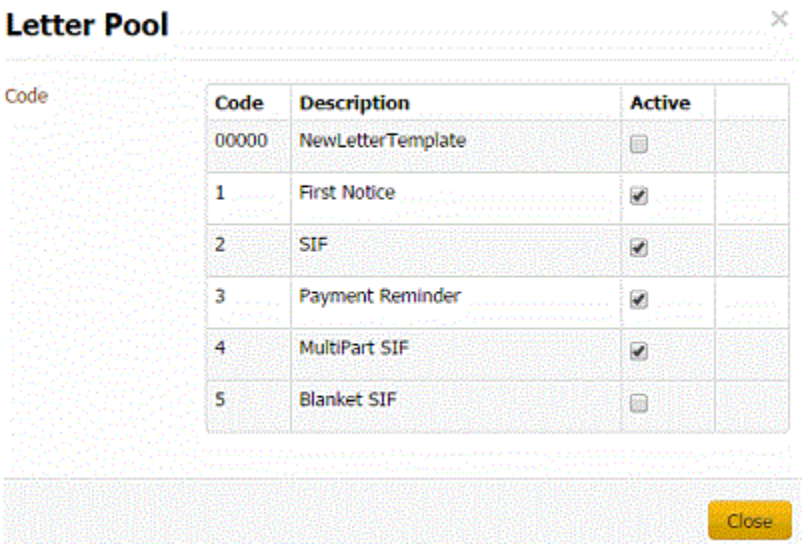
CBR Setup: Credit Bureau Reporting method.

Is Principle Client: If selected, your organization owns the accounts that this client holds. If cleared, your organization holds this client's accounts for collection purposes only.

5. To specify one or more letters to populate the **First Letter** list box, do the following:

a. Click **Letter Pool**.

> **Note:** Only the letters with a time restriction set in Letter Console to either "Allow Always" or "Only Allow in First 30 Days" appear in this dialog box.



b. Select the check box for each letter you want to display in the **First Letter** list box.

c. Clear the check box for each letter you don't want to display in the **First Letter** list box.

d. Click **Close**.

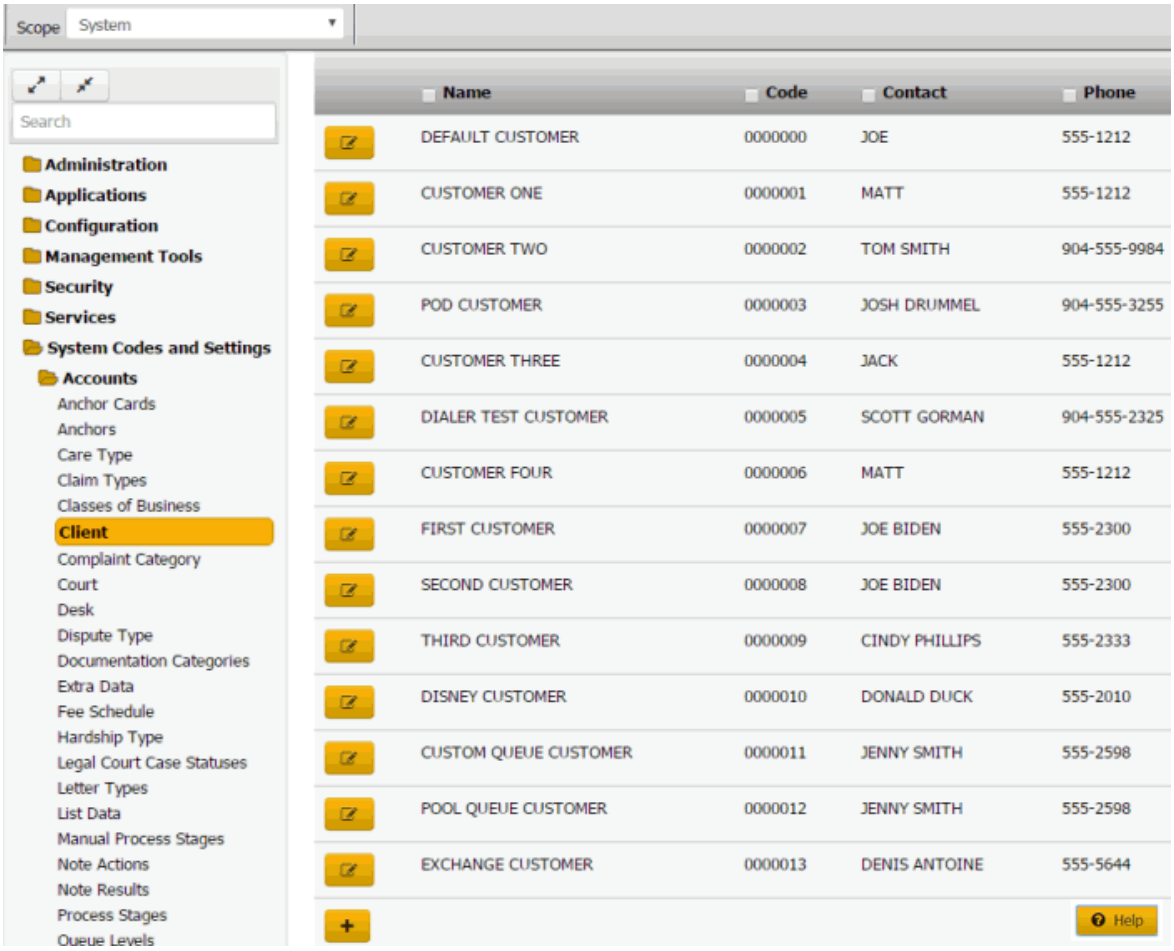
6. In the **First Letter** list box, click the first letter to send to customers.
7. Complete the remaining information and then click **Finish**.

Maintain General Client Information

Use the **General** tab in the **Client** dialog box to maintain general information for a client.

To maintain general client information

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Client**.



> **Tip:** To limit the clients that display in the data grid, click one or more check boxes next to a column heading. In the **Filter** box, type one or more characters and then press **Enter**. To clear a filter, clear the check boxes and then click the Refresh icon.

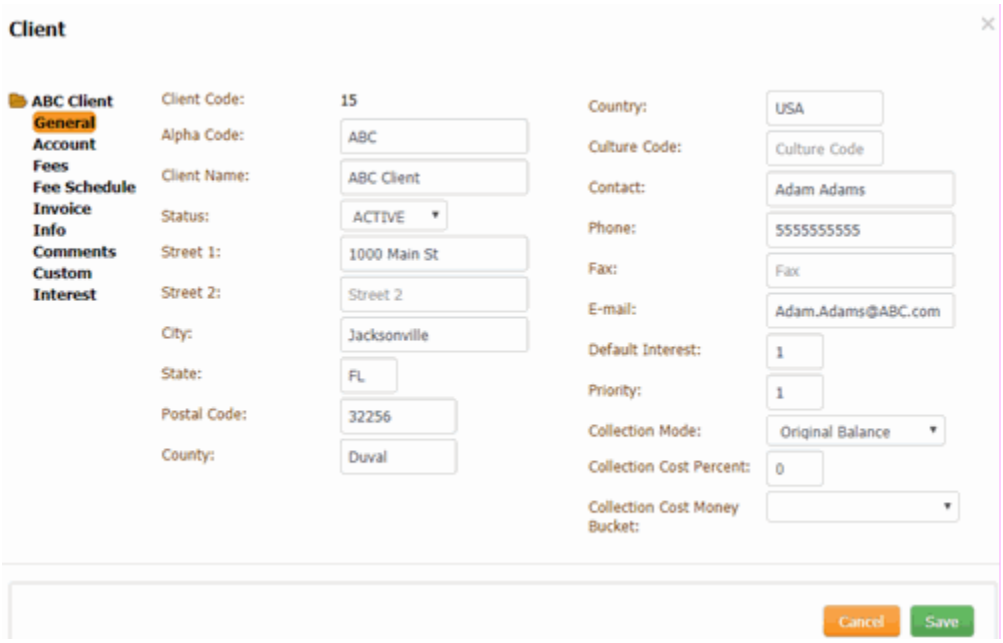
2. To search for a client, do the following:

a. Click one or more check boxes next to a column heading.

b. In the **Filter** box for each check box selected, type the criteria for which to search.

c. Click the Refresh icon. The system displays clients that match the specified criteria only.

3. In the data grid, click the Edit icon and then click **General**.



Client Code: Unique code that your organization assigned to identify the client.

Alpha Code: Generic code used for conversions from other systems. Allows your organization to reference any code associated to the client previously.

Client Name: Full name of the client.

Status: Status of the account.

Street 1: First line of the client's street address.

Street 2: Second line of the client's street address.

City: Client's city.

State: Client's state.

Postal Code: Client's postal code.

County: Client's county.

Country: Client's country.

Culture Code: Code that indicates the region where the client is located. For example, "en-US" indicates the client is in an English-speaking country, and the country is the United States of America. Latitude uses this information for things such as determining which currency symbol to use.

Contact: Full name of the contact person.

Phone: Contact person's phone number.

Fax: Contact person's fax number.

E-mail: Contact person's email address.

Default Interest: Interest rate to assign to new accounts imported for this client. You can override the rate using Exchange or manually.

Priority: Sets the priority when spreading payments across linked accounts. Generally, the values are 1-10 (with 10 being the highest priority). You can assign the same priority to clients. Maximum settings allow up to 255 priorities.

Collection Mode: Method to use to calculate the portion of a payment to apply toward collection costs. Latitude allocates a portion of the payment toward the Collection Cost money bucket before applying the remaining payment amount to the other money buckets.

Original Balance: Calculates the collection cost on the original account balance. The formula is: Original account balance x Collection Cost Percent.

Current Gross: Calculates the collection cost on the current gross account balance. The formula is: ((1/(1-(Collection Cost Percent)))-1) x (Principal + Interest + Other fees).

Collection Cost Percent: Percent to use to calculate collection costs.

Collection Cost Money Bucket: Money bucket for storing collection costs. Latitude calculates the collection cost and adds it to this bucket when users add accounts manually for this client.

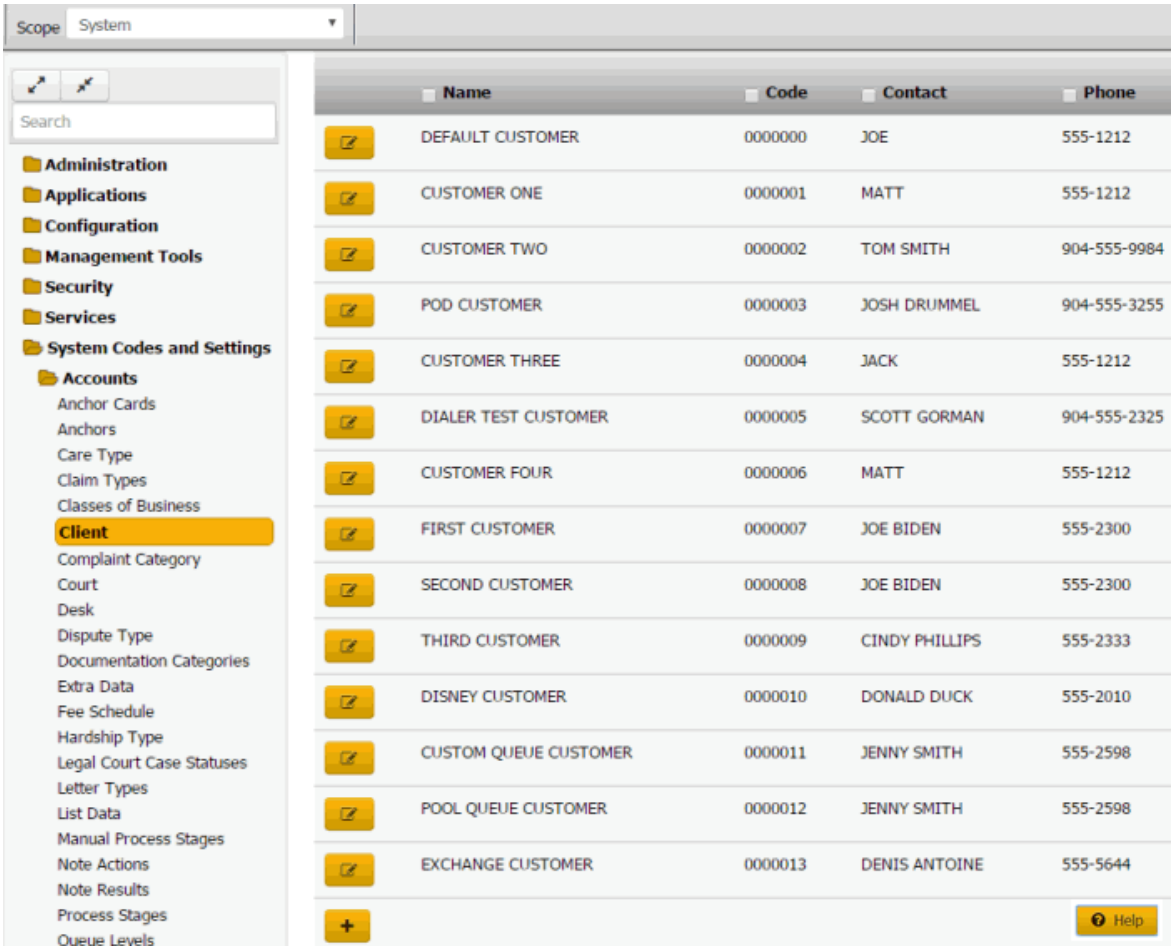
4. Complete the information and then click **Save**.

Maintain Client Account Information

Use the **Account** tab in the **Client** dialog box to maintain account information for a client.

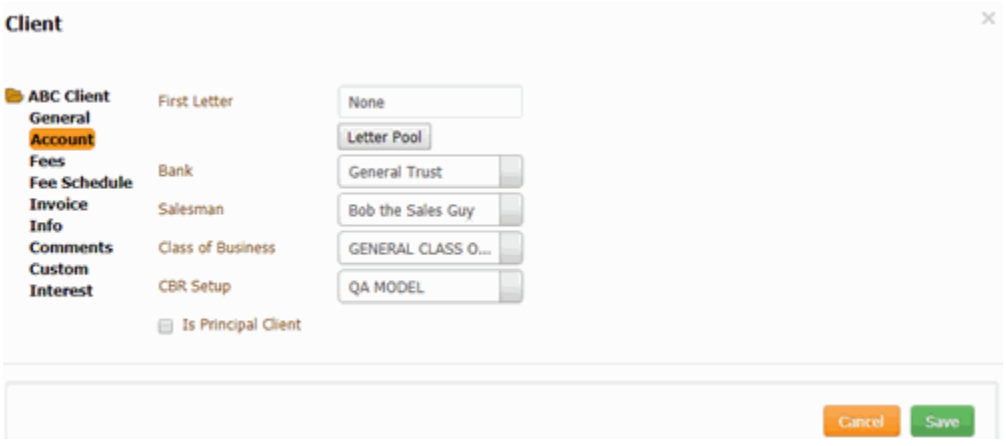
To maintain client account information

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Client**.



Tip: To limit the clients that display in the data grid, click one or more check boxes next to a column heading. In the **Filter** box, type one or more characters and then press **Enter**. To clear a filter, clear the check boxes and then click the Refresh icon.

2. In the data grid, click the Edit icon and then click **Account**.



First Letter: First letter to generate for new accounts. For information about managing letters, see the *Letter Console* documentation.

Bank: If your organization prints checks for the client, this value is the trust account your organization uses for this client. For information about setting up trust accounts and printing checks, see the *Invoices* documentation.

Salesman: Salesman handling this client account. For more information, see Salesman.

Class of Business: Class of business to assign to this client account. For more information, see Classes of Business.

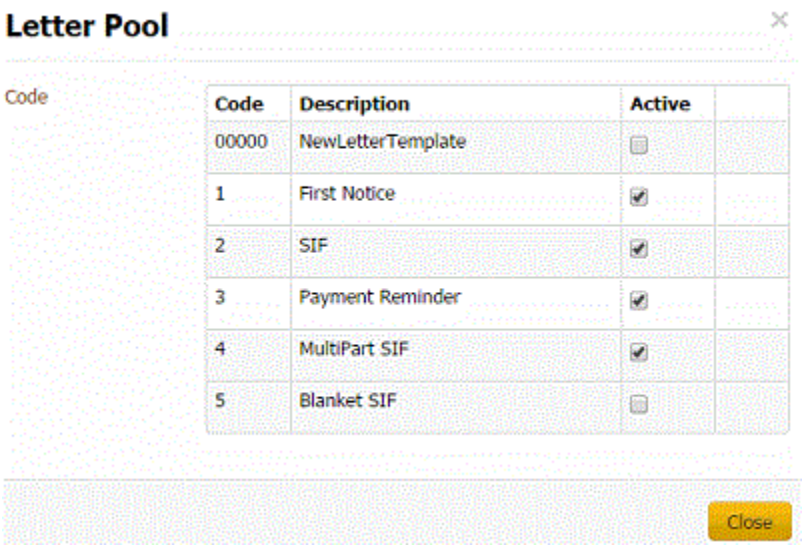
CBR Setup: Credit Bureau Reporting method.

Is Principle Client: If selected, your organization owns the accounts that this client holds. If cleared, your organization holds this client's accounts for collection purposes only.

3. To specify one or more letters to populate the **First Letter** list box, do the following:

a. Click **Letter Pool**.

> **Note:** Only the letters with a time restriction set in Letter Console to either "Allow Always" or "Only Allow in First 30 Days" appear in this dialog box.



b. Select the check box for each letter you want to display in the **First Letter** list box.

c. Clear the check box for each letter you don't want to display in the **First Letter** list box.

d. Click **Close**.

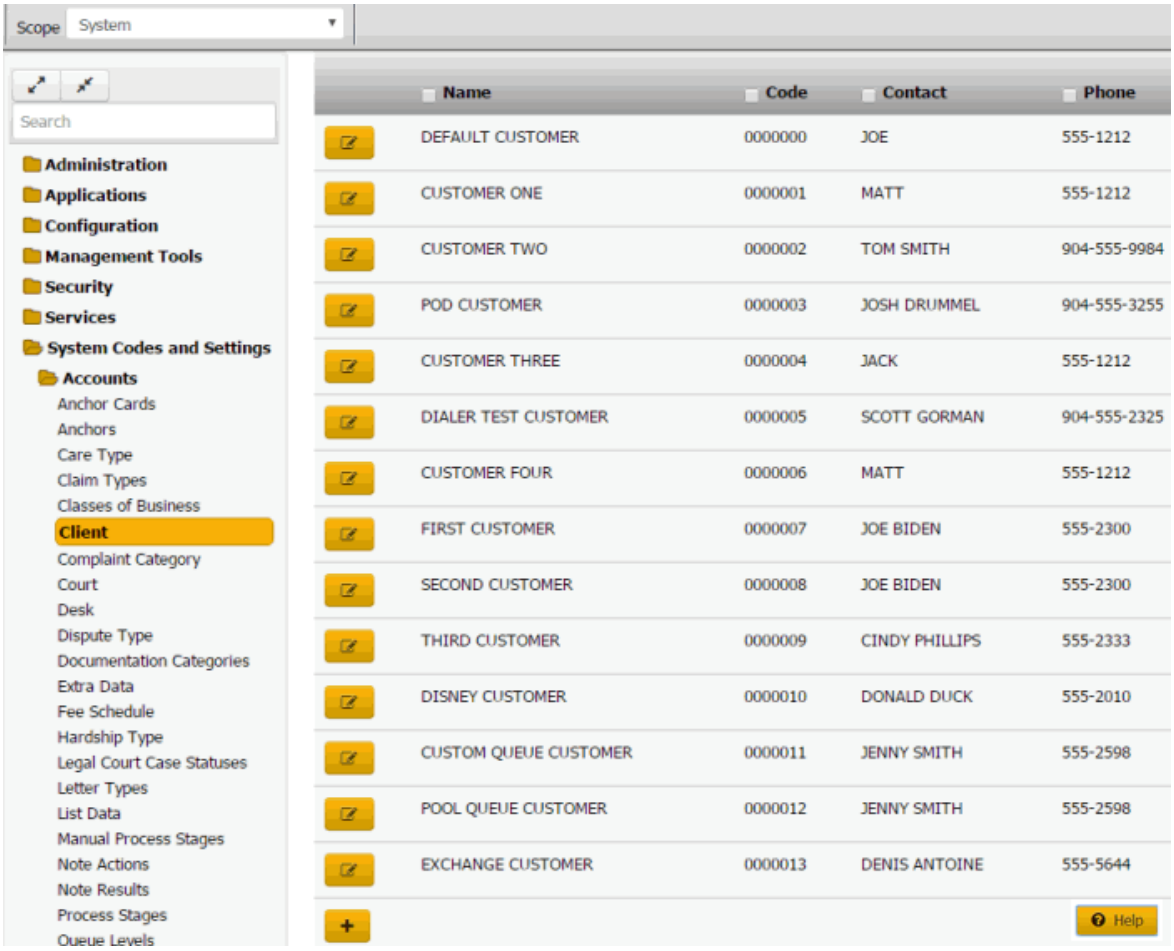
4. In the **First Letter** list box, click the first letter to send to customers.
5. Complete the remaining information and then click **Save**.

Maintain Client Fees

Use the **Fees** tab in the **Client** dialog box to maintain fees for a client.

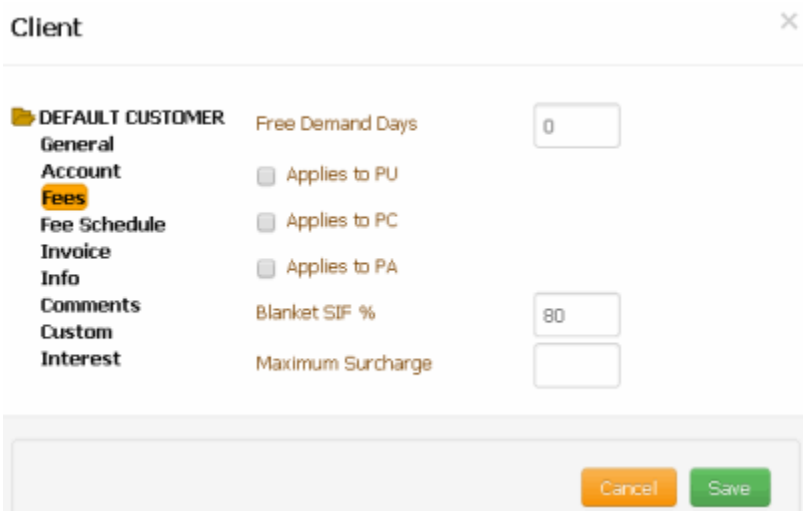
To maintain client fees

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Client**.



Tip: To limit the clients that display in the data grid, click one or more check boxes next to a column heading. In the **Filter** box, type one or more characters and then press **Enter**. To clear a filter, clear the check boxes and then click the Refresh icon.

2. In the data grid, click the Edit icon and then click **Fees**.



Free Demand Days: Number of "grace" days to grant to a client when receiving new business.

Applies to PU: If selected, Latitude doesn't apply fees to the "Paid Us" payment type for the number days indicated in the **Free Demand Days** box.

Applies to PC: If selected, Latitude doesn't apply fees to the "Paid Client" payment type for the number days indicated in the **Free Demand Days** box.

Applies to PA: If selected, Latitude doesn't apply fees to the "Paid Agency" payment type for the number days indicated in the **Free Demand Days** box.

Blanket SIF %: Percentage of the account balance that the client requires as a minimum to consider an account settled in full.

Maximum Surcharge: Maximum surcharge amount on payments received. For more information, see Surcharge Rules.

3. Complete the information and then click **Save**.

Client Fee Schedule

Client Fee Schedule

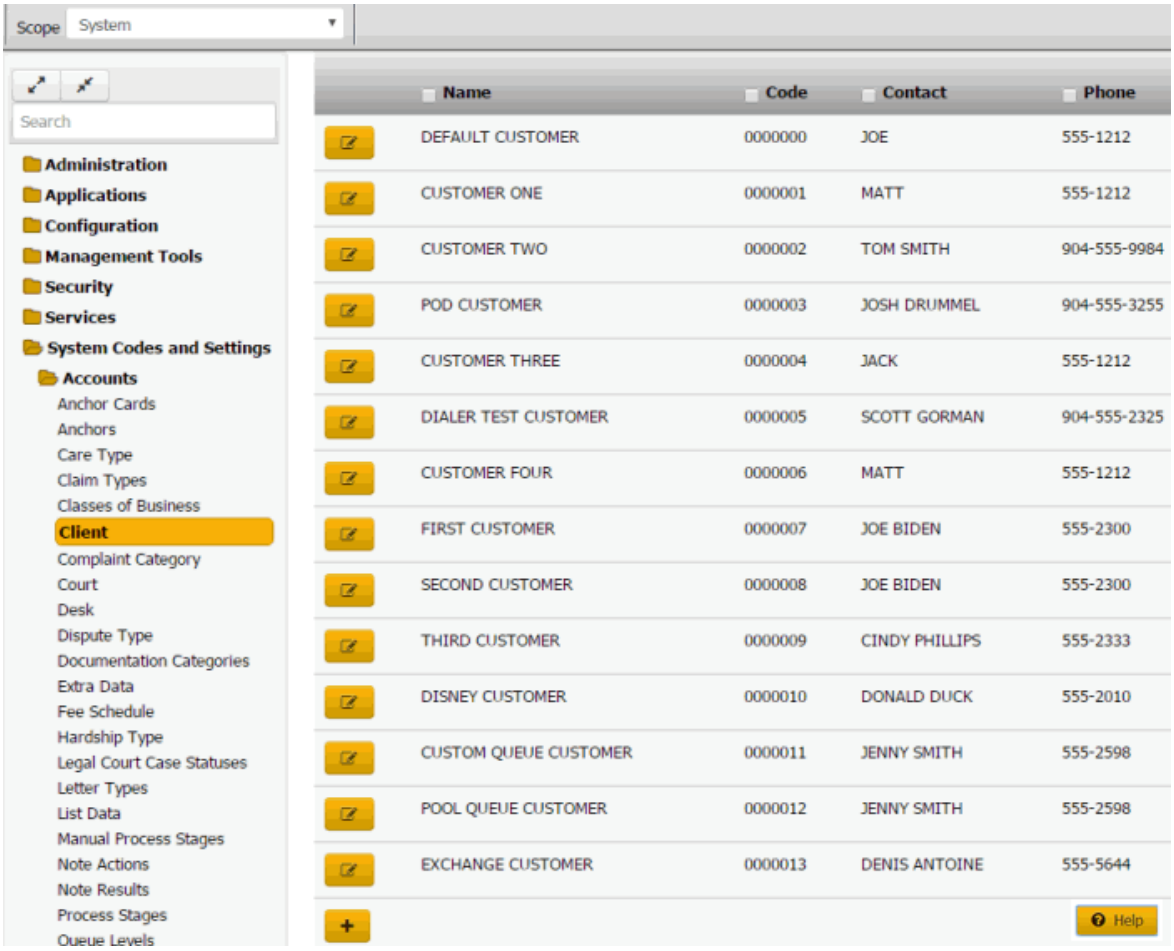
You can add, modify, and delete fee schedules for a client. For more information, see Fee Schedules.

Add a Client Fee Schedule

Use the **Fee Schedule Detail** dialog box to add a fee schedule for a client. The fee schedule takes effect on the date you specify and remains in effect until you add a fee schedule with a later effective date.

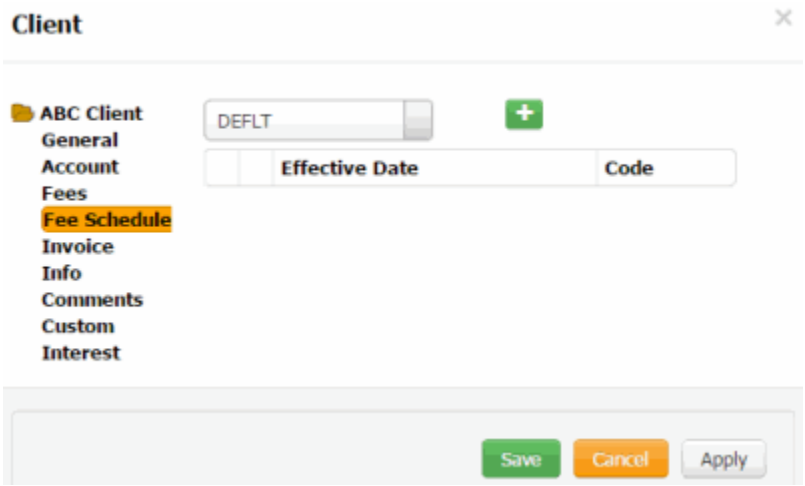
To add a client fee schedule

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Client**.

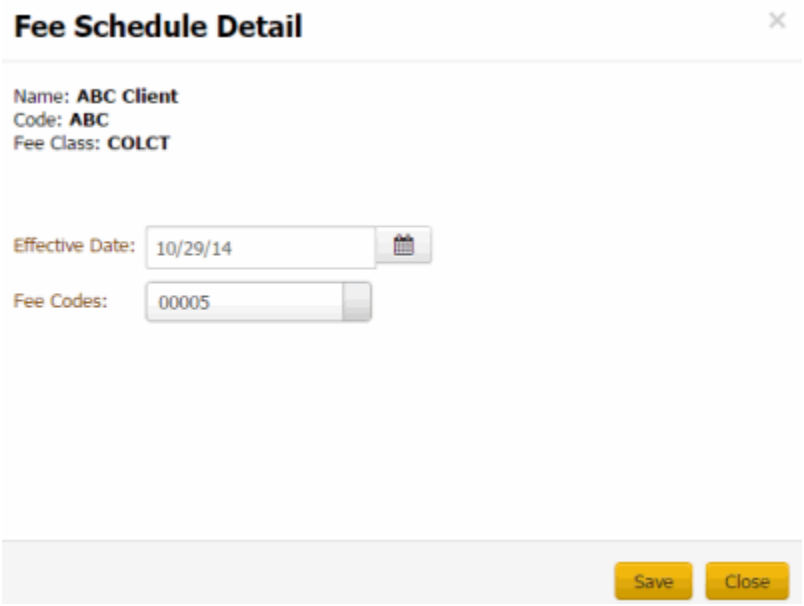


Tip: To limit the clients that display in the data grid, click one or more check boxes next to a column heading. In the **Filter** box, type one or more characters and then press **Enter**. To clear a filter, clear the check boxes and then click the Refresh icon.

2. In the data grid, click the Edit icon and then click **Fee Schedule**.



3. In the list box, click the fee class and then click the plus sign (+).



Name: Client's name.

Code: Unique code that identifies the client.

Fee Class: Category of fee schedule.

Effective Date: Date the fee schedule takes effect.

Fee Code: Unique number that identifies the fee schedule to use.

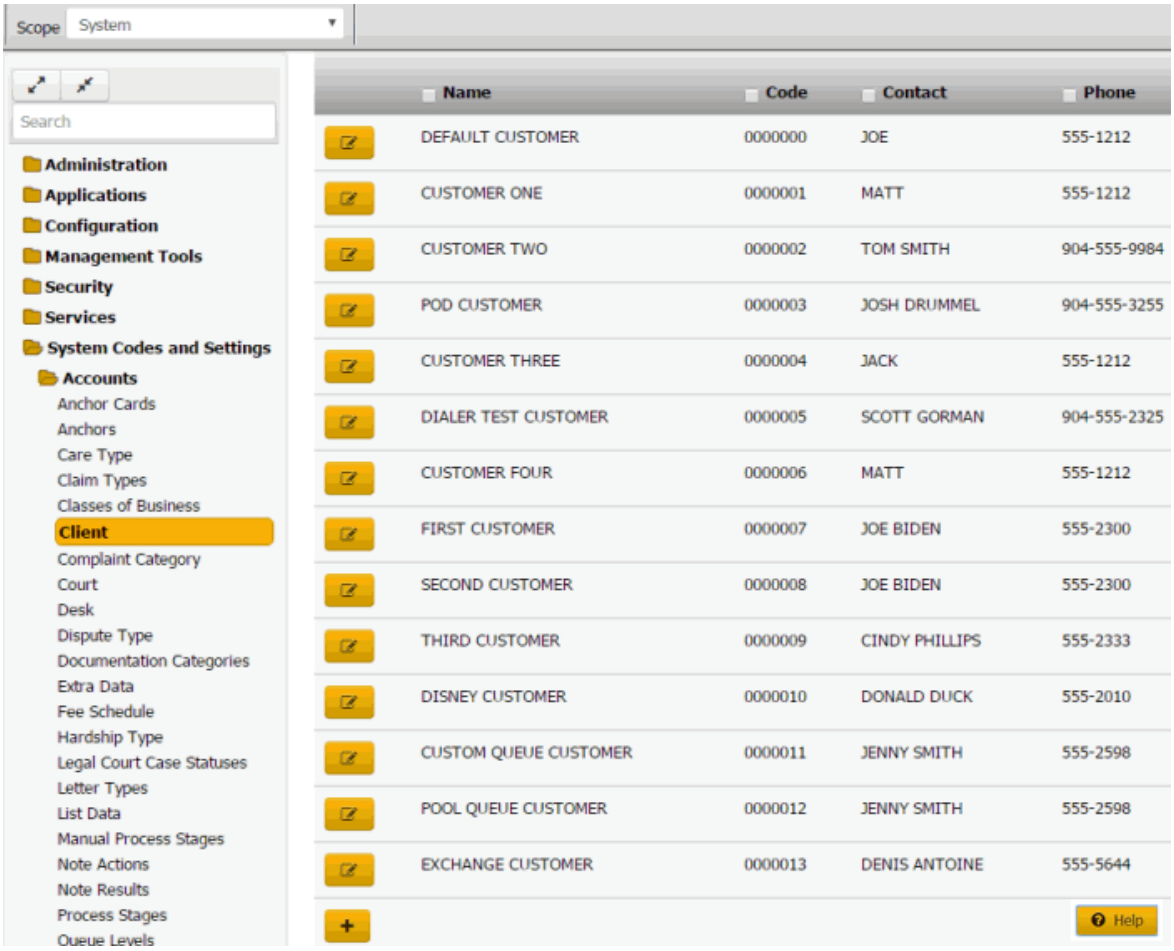
4. Complete the information and then click **Save**.

Modify a Client Fee Schedule

Use the **Fee Schedule Detail** dialog box to modify a fee schedule for a client. You cannot modify a fee schedule that has an effective date that is earlier than the current date.

To modify a client fee schedule

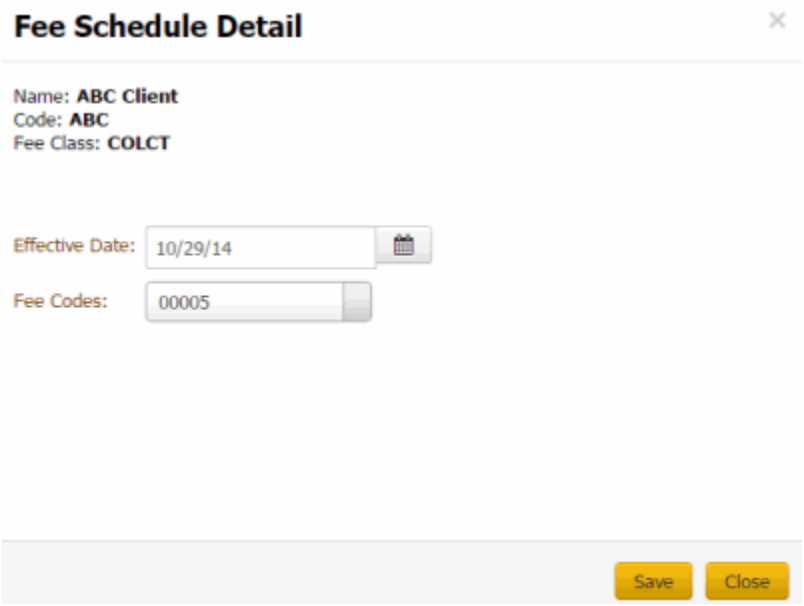
1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Client**.



> **Tip:** To limit the clients that display in the data grid, click one or more check boxes next to a column heading. In the **Filter** box, type one or more characters and then press **Enter**. To clear a filter, clear the check boxes and then click the Refresh icon.

2. In the data grid, click the Edit icon and then click **Fee Schedule**.

3. In the list box, click the fee class and then, in the data grid, click the Edit icon.



Name: Client's name.

Code: Unique code that identifies the client.

Fee Class: Category of fee schedule. Valid values are:

COLCT = Collector Fee Schedule.

DEFLT: = Client Fee Schedule.

Effective Date: Date the fee schedule takes effect.

Fee Code: Unique number that identifies the fee schedule to use.

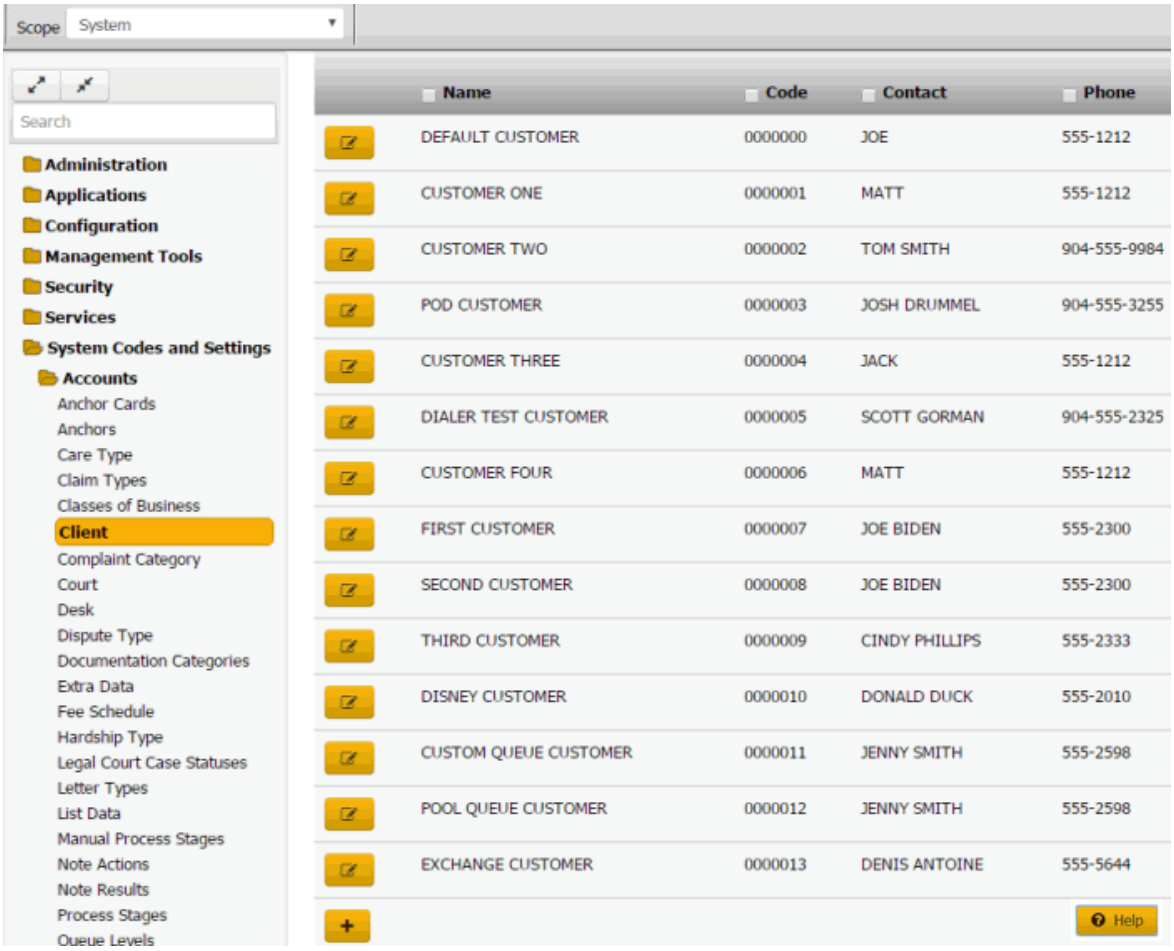
4. Modify the information and then click **Save**.

Delete a Client Fee Schedule

Use the **Fee Schedule** tab in the **Client** dialog box to delete a fee schedule for a client.

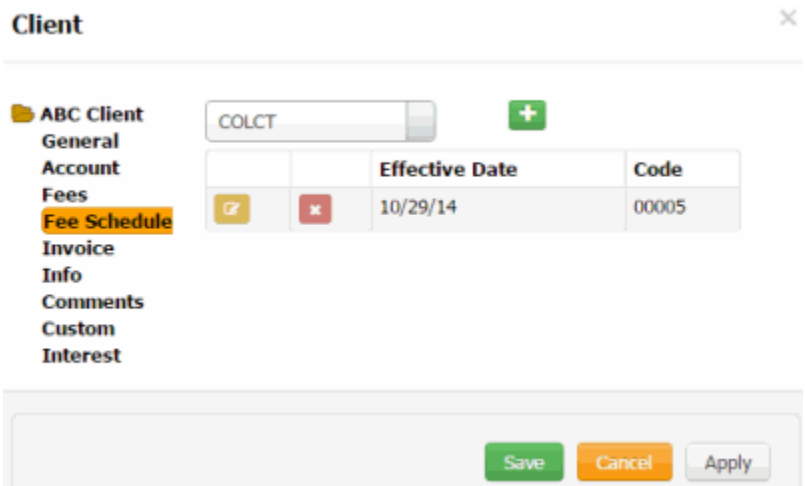
To delete a client fee schedule

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Client**.



Tip: To limit the clients that display in the data grid, click one or more check boxes next to a column heading. In the **Filter** box, type one or more characters and then press **Enter**. To clear a filter, clear the check boxes and then click the Refresh icon.

2. In the data grid, click the Edit icon and then click **Fee Schedule**.



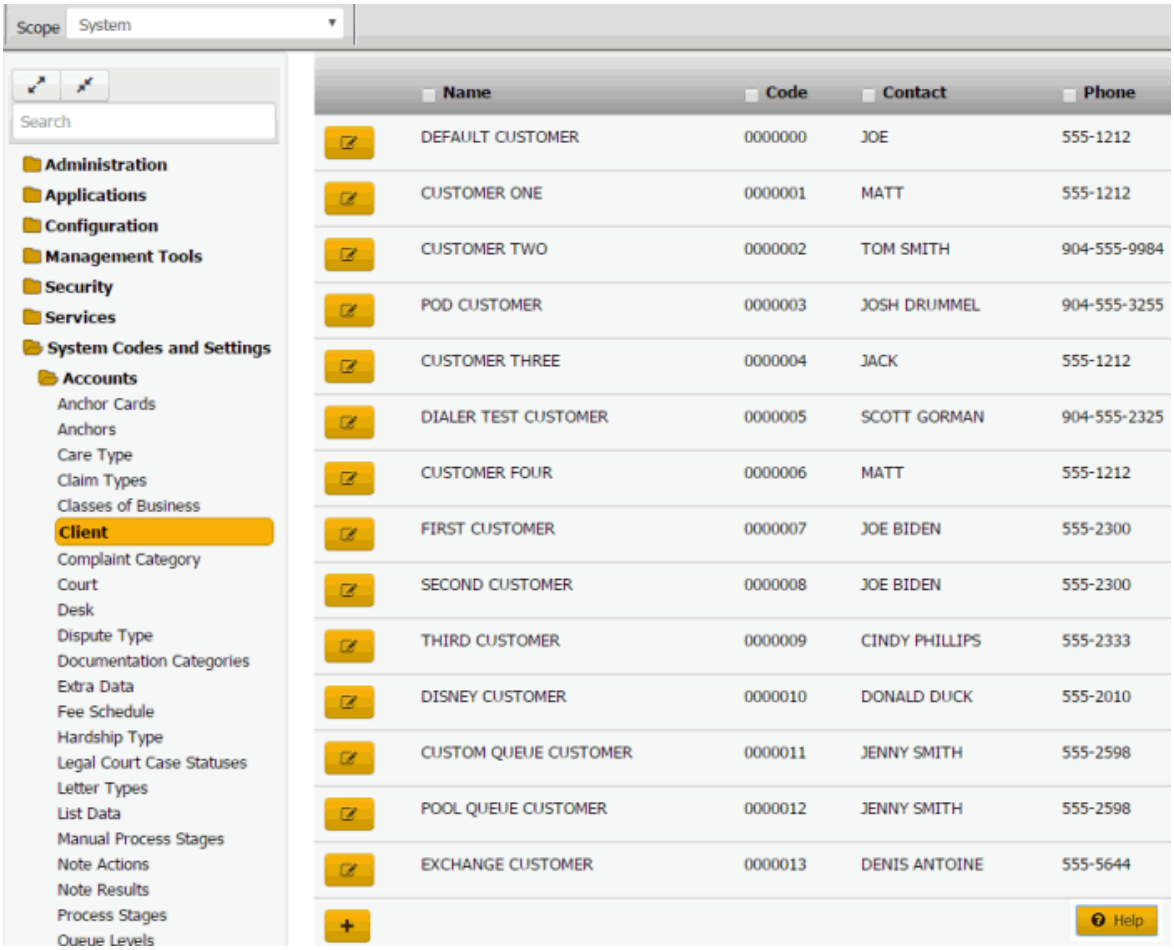
3. In the data grid, click the Delete icon and then click **Yes**.

Maintain Client Invoice Settings

Use the **Invoice** tab in the **Client** dialog box to maintain invoice settings for a client. These settings apply when invoicing clients using the Invoices program.

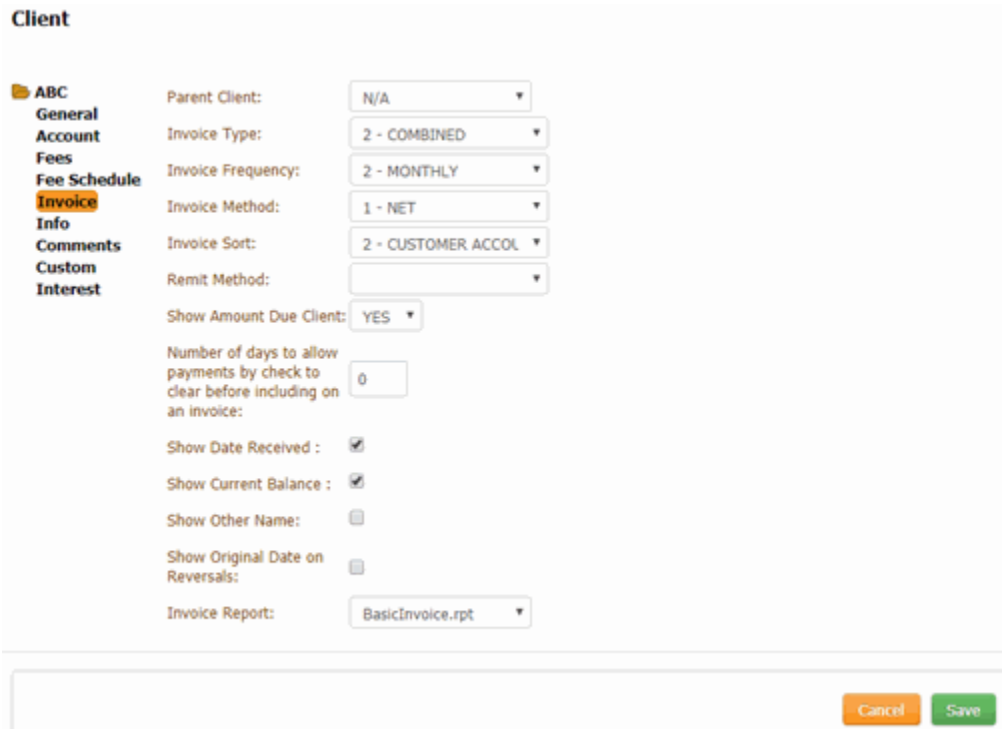
To maintain client invoice settings

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Client**.



> **Tip:** To limit the clients that display in the data grid, click one or more check boxes next to a column heading. In the **Filter** box, type one or more characters and then press **Enter**. To clear a filter, clear the check boxes and then click the Refresh icon.

2. In the data grid, click the Edit icon and then click **Invoice**.



Parent Client: Parent client associated to this client for invoicing purposes.

Invoice Type: Type of invoices to create. Valid values are:

> **Combined:** Creates one invoice for all payment types (PA, PC, PU, PAR, PCR, and PUR).
>
> **Separate:** Creates one invoice for PC and PCR, one invoice for PA and PU, and one invoice for PAR and PUR payment types.
>
> **Separate Direct:** Creates one invoice for PC and PCR payment types and a separate invoice for PA, PAR, PU, and PUR payment types.

Invoice Frequency: Indicates how often to invoice the client.

Invoice Method: Method for invoicing the client.

> **Net:** Doesn't include your organization's fee on client invoices.
>
> **Gross:** Includes your organization's fee on client invoices.

Invoice Sort: Order to sort the invoices.

> **Remit Method:** Determines the method for remitting invoices.
>
> **Manual:** Your organization writes checks for the client manually.
>
> **Check**: Your organization uses the Invoices program to print checks for the client.
>
> **ACH Transfer:** Your organization uses the Invoices program to create ACH wire transfers for the client.

Show Amount Due Client: Indicates whether to include the amount due to the client on the invoice.

Number of days to allow payments by check to clear before including on invoice: Number of days to wait before including payments on a client invoice. If the customer's check does not clear, use this option to avoid sending payment information to a client.

Show Date Received, **Current Balance**, **Amount Due Client**, **Other Name**, **Original Date on Reversals:** If selected, the information prints on the client's invoices.

Invoice Report: File to use when creating invoices for the client. This option allows you to use custom invoices for each customer. The default file is **BasicInvoice.rpt**. Import the reports into Latitude to make them available for selection from the list box.

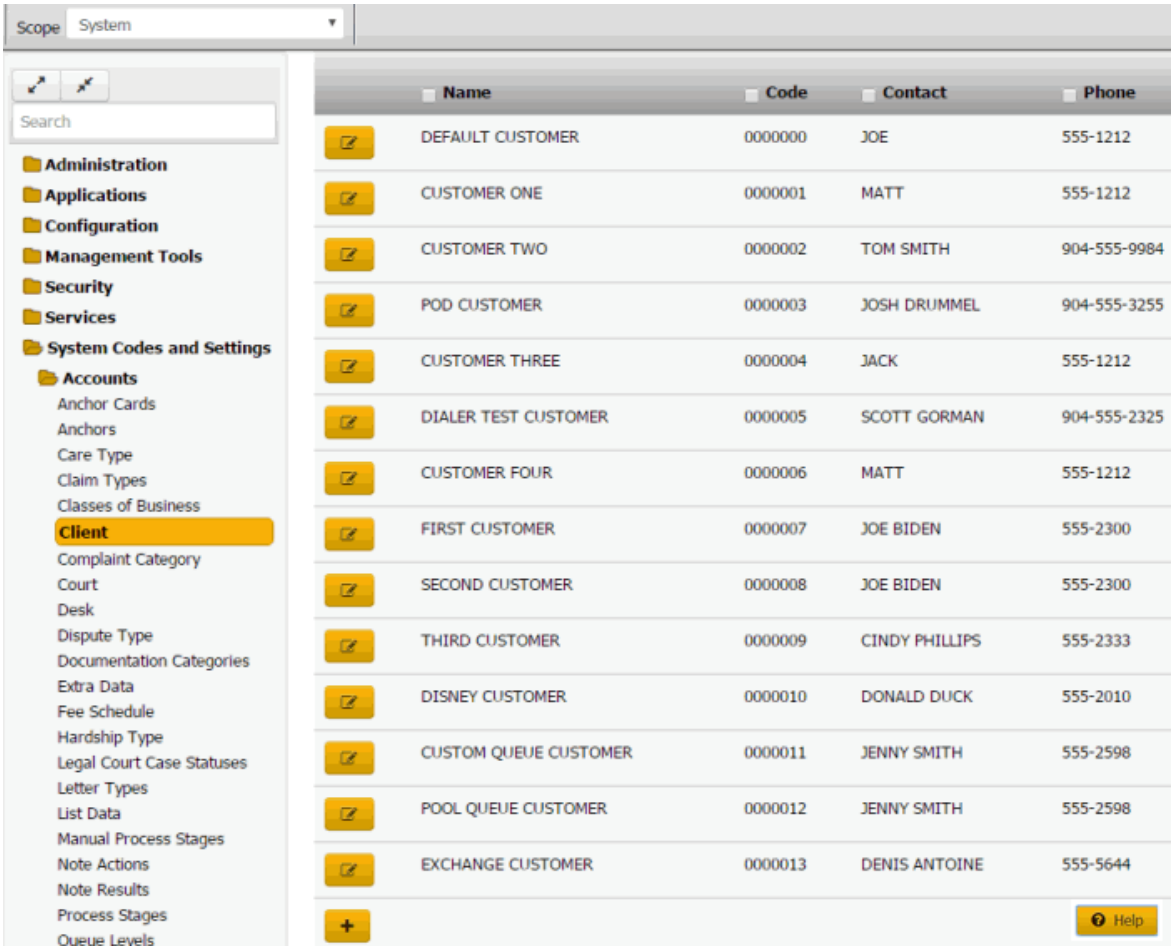
3. Complete the information and then click **Save**.

Maintain Client Guidelines

Use the **Info** tab in the **Client** dialog box to maintain the work plan, settlement guidelines, and miscellaneous information to display to users working a client's accounts. For more information, see View Client Guidelines.

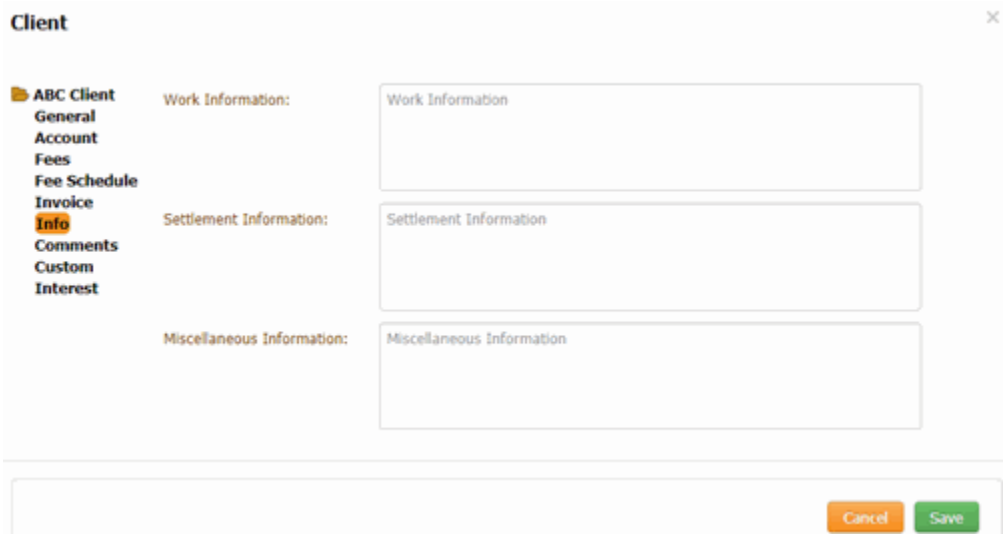
To maintain client guidelines

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Client**.



> **Tip:** To limit the clients that display in the data grid, click one or more check boxes next to a column heading. In the **Filter** box, type one or more characters and then press **Enter**. To clear a filter, clear the check boxes and then click the Refresh icon.

2. In the data grid, click the Edit icon and then click **Info**.



Work Information: Information for working this client's accounts.

Settlement Information: Information on what constitutes a settlement on this client's accounts.

Miscellaneous Information: Miscellaneous information such as special client requirements.

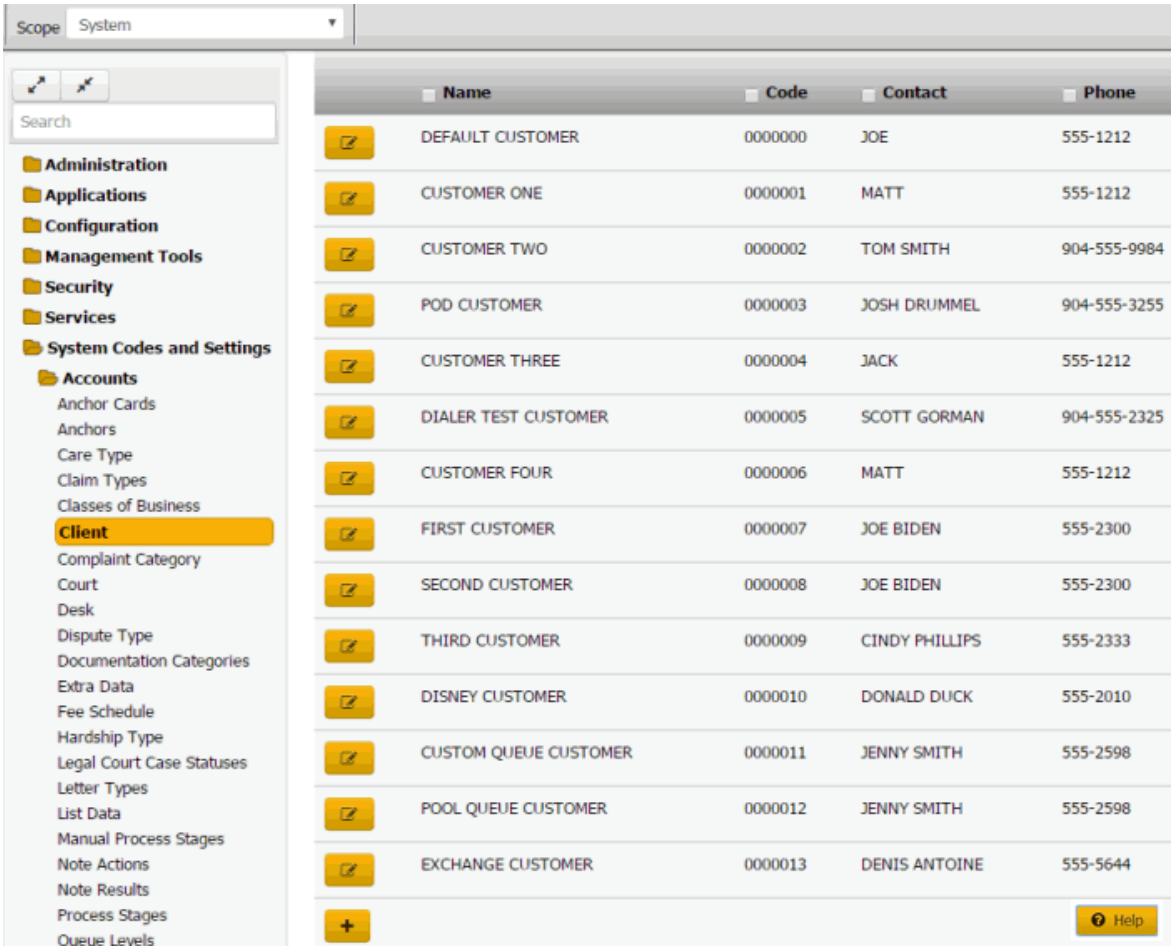
3. Complete the information and then click **Save**.

Add a Client Comment

Use the **Comments** tab in the **Client** dialog box to add a client comment. Latitude creates comments for changes to client information and flags the comments as "Created by AUDIT." You cannot modify or delete client comments.

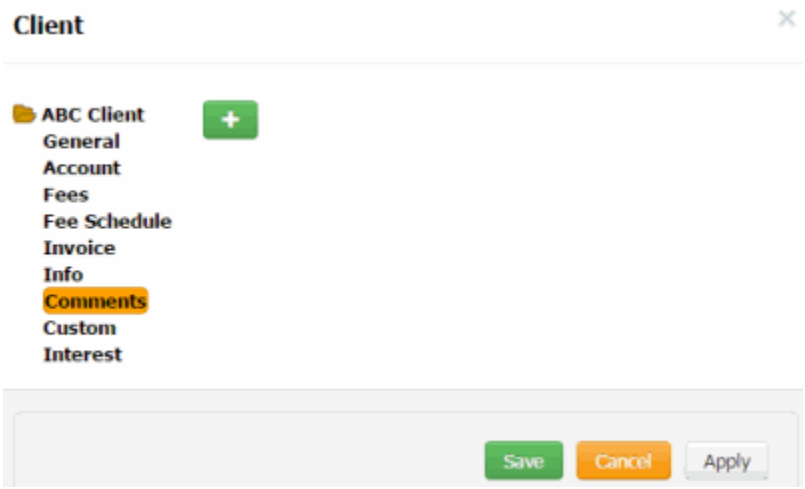
To add a client comment

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Client**.

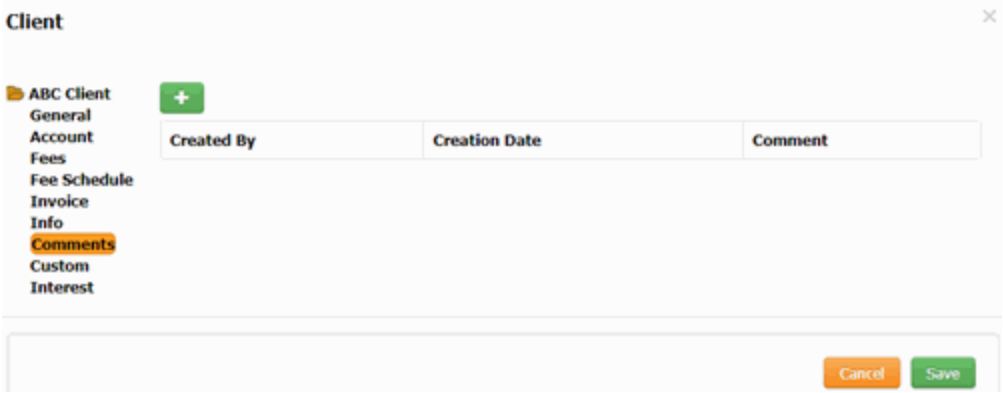


Tip: To limit the clients that display in the data grid, click one or more check boxes next to a column heading. In the **Filter** box, type one or more characters and then press **Enter**. To clear a filter, clear the check boxes and then click the Refresh icon.

2. In the data grid, click the Edit icon and then, in the **Client** dialog box, click **Comments**.



3. Click the plus sign (+).



4. Type a comment and then click the **Save** under the **Comment** box.
5. Click **Save**.

Custom Data

Custom Data

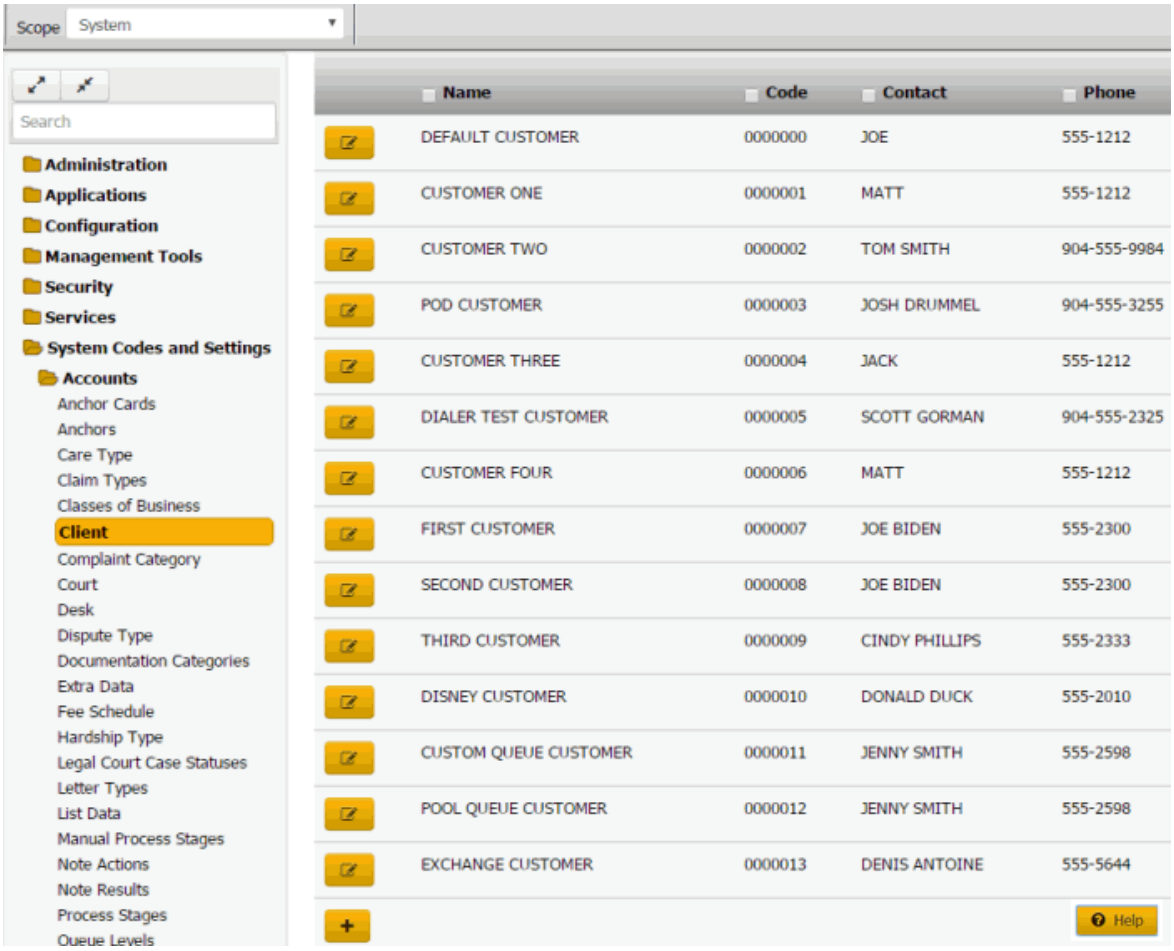
You can add or modify custom data for a client. This feature allows your organization to capture information for the client that you cannot include elsewhere in Latitude. Custom data includes dates, check box options, numeric values, and text. If your organization configured custom labels, you can add or modify custom data. For more information, see Client Titles.

Maintain Custom Dates

Use the **Dates** tab in the **Client** dialog box to maintain custom dates for a client. For more information, see Maintain Client Date Titles.

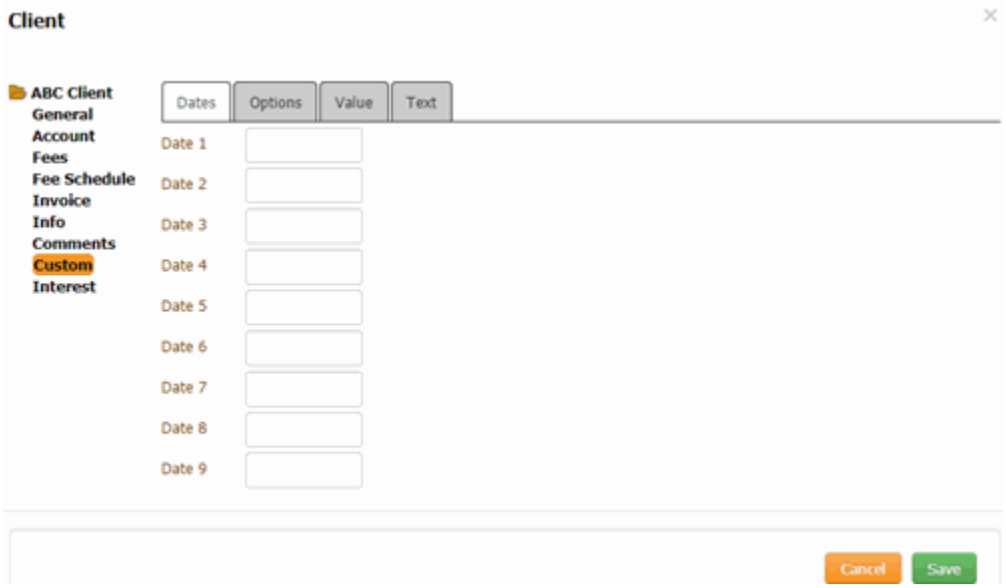
To maintain custom dates

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Client**.



> **Tip:** To limit the clients that display in the data grid, click one or more check boxes next to a column heading. In the **Filter** box, type one or more characters and then press **Enter**. To clear a filter, clear the check boxes and then click the Refresh icon.

2. In the data grid, click the Edit icon and then click **Custom**.
3. Click the **Dates** tab.



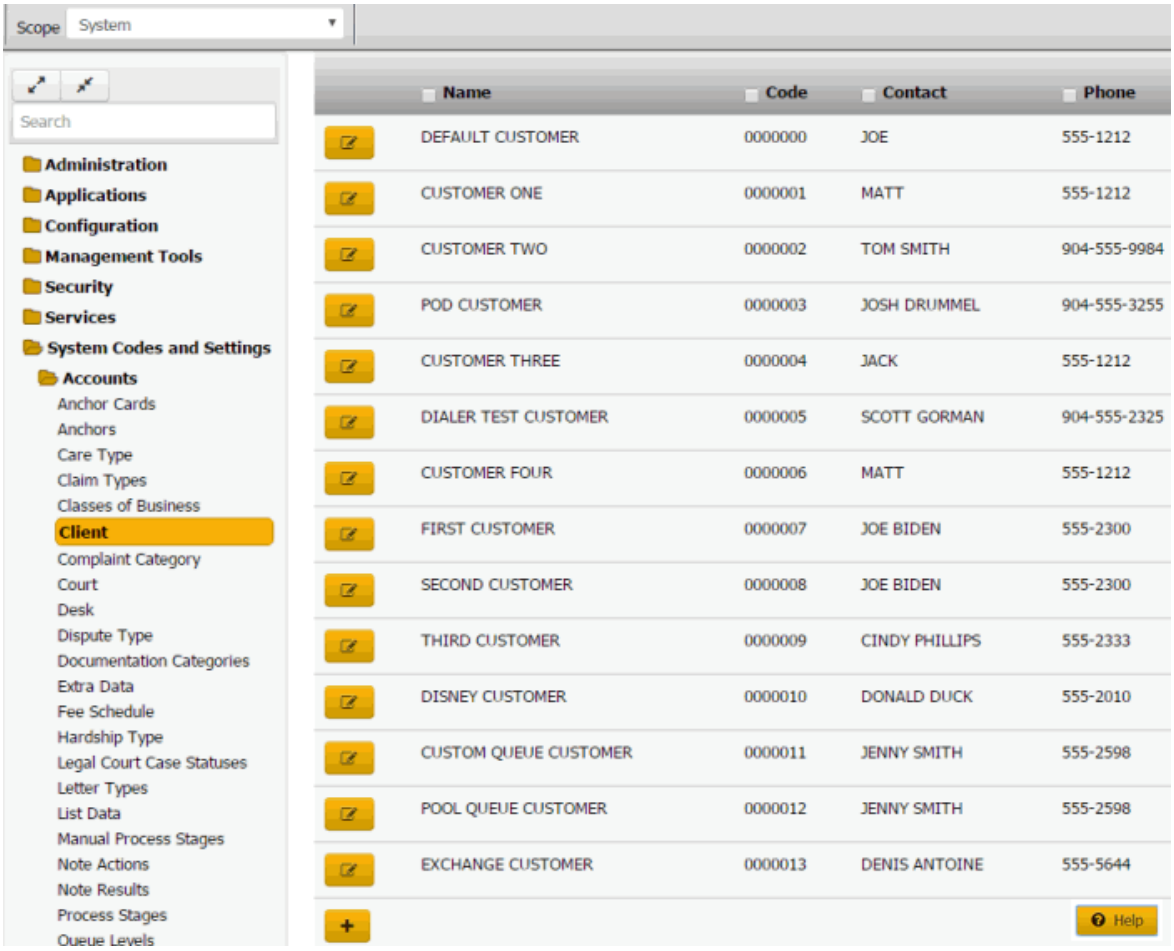
4. For each box with a custom label to the right, type a date and then click **Save**.

Maintain Custom Options

Use the **Options** tab in the **Client** dialog box to maintain custom options for a client. For more information, see Maintain Client Option Titles.

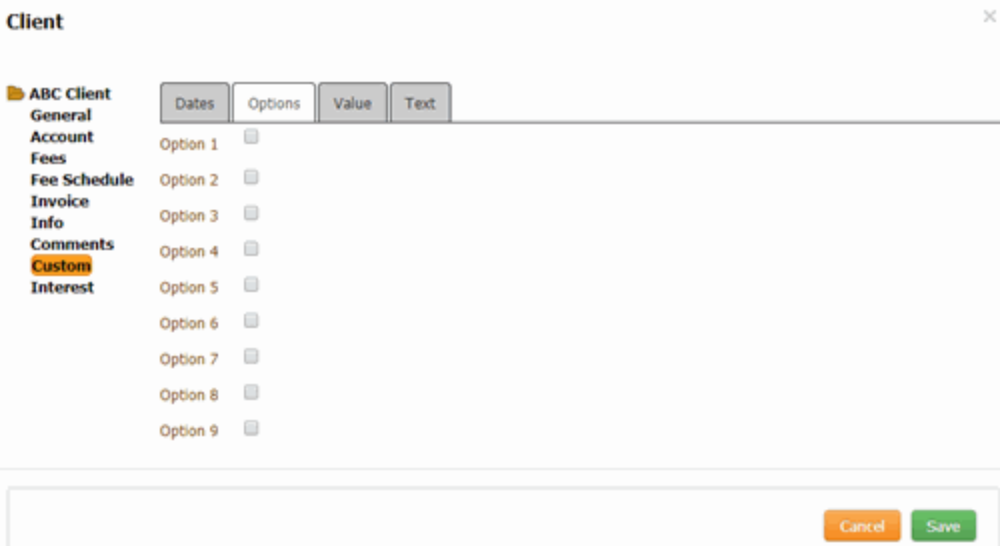
To maintain custom options

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Client**.



> **Tip:** To limit the clients that display in the data grid, click one or more check boxes next to a column heading. In the **Filter** box, type one or more characters and then press **Enter**. To clear a filter, clear the check boxes and then click the Refresh icon.

2. In the data grid, click the Edit icon and then click **Custom**.
3. Click the **Options** tab.



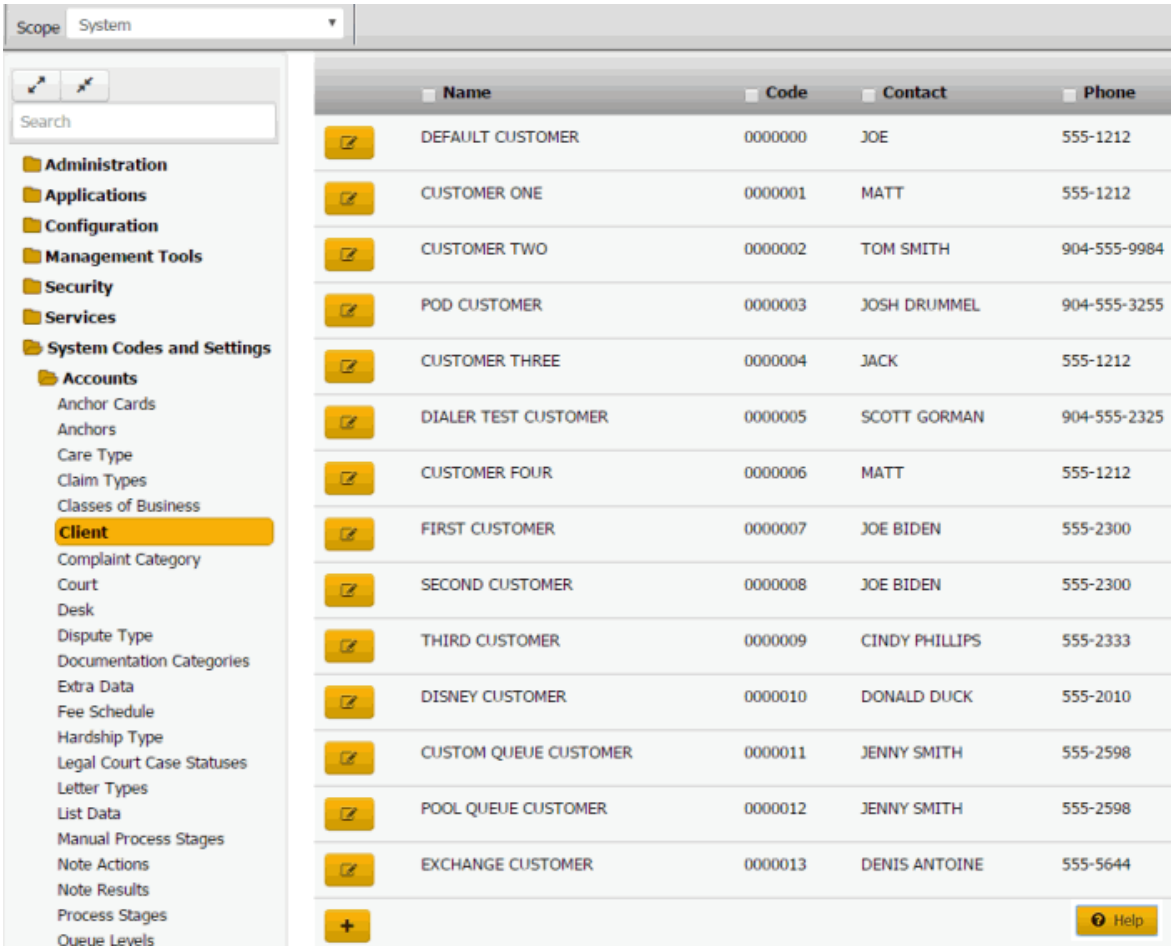
4. For each check box with a custom label to the right, do one of the following:
    - To indicate a true statement, select the check box.
    - To indicate a false statement, clear the check box.
5. Click **Save**.

Maintain Custom Text

Use the **Text** tab in the **Client** dialog box to maintain custom alphanumeric values for a client. For more information, see Maintain Client Text Titles.

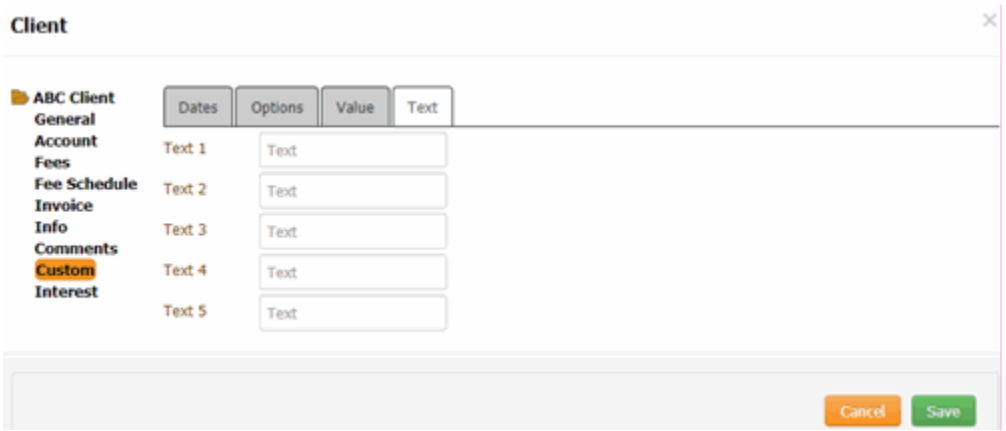
To maintain custom text

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Client**.



> **Tip:** To limit the clients that display in the data grid, click one or more check boxes next to a column heading. In the **Filter** box, type one or more characters and then press **Enter**. To clear a filter, clear the check boxes and then click the Refresh icon.

2. In the data grid, click the Edit icon and then click **Custom**.
3. Click the **Text** tab.



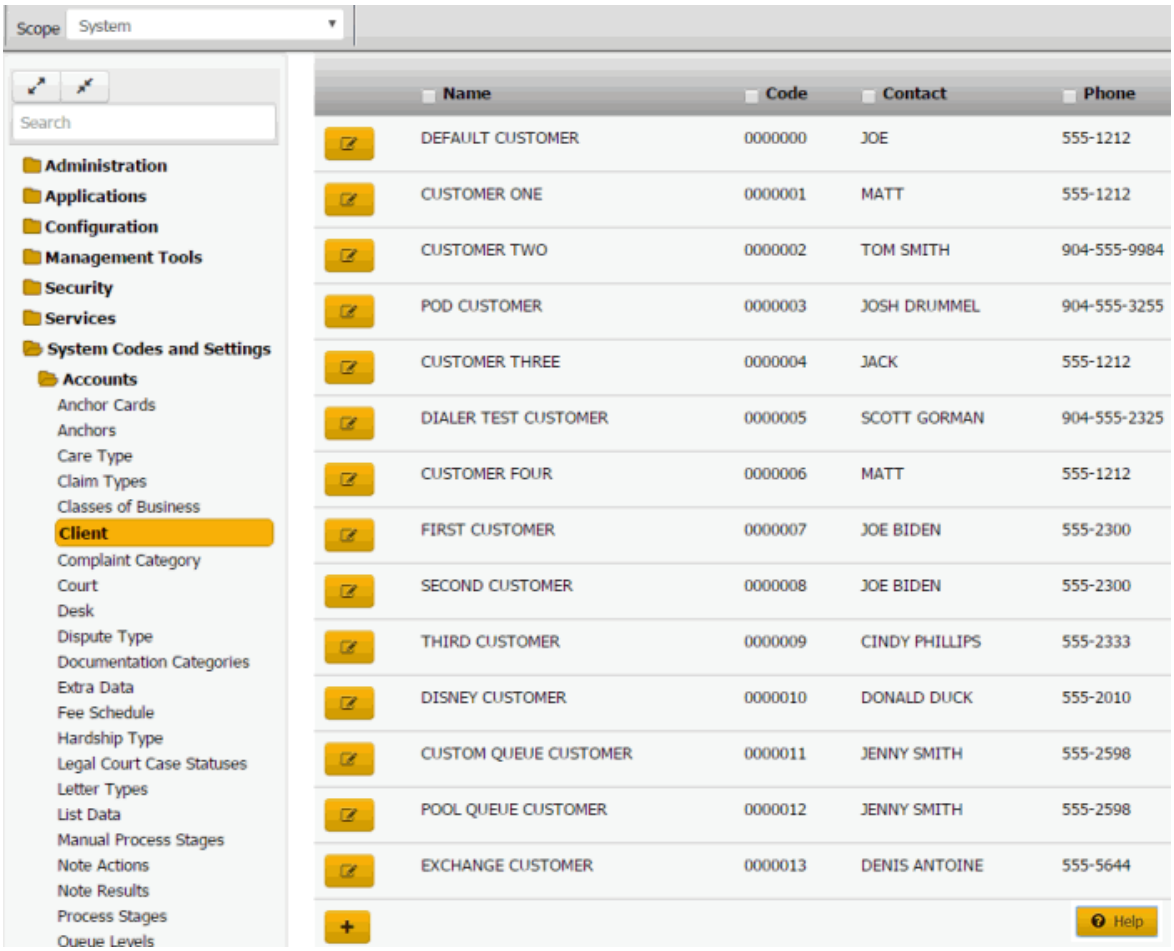
4. For each box with a custom label to the right, type information and then click **Save**.

Maintain Custom Values

Use the **Values** tab in the **Client** dialog box to maintain custom numeric values for a client. For more information, see Maintain Client Value Titles.

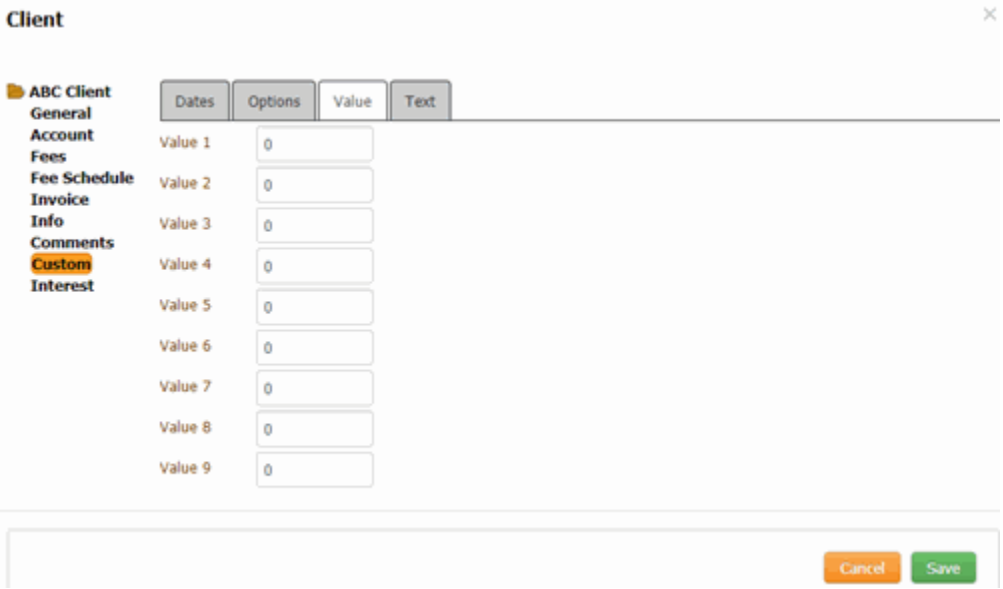
To maintain custom values

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Client**.



> **Tip:** To limit the clients that display in the data grid, click one or more check boxes next to a column heading. In the **Filter** box, type one or more characters and then press **Enter**. To clear a filter, clear the check boxes and then click the Refresh icon.

2. In the data grid, click the Edit icon and then click **Custom**.
3. Click the **Values** tab.



4. For each box with a custom label to the right, type a numeric value and then click **Save**.

Client Interest

Client Interest

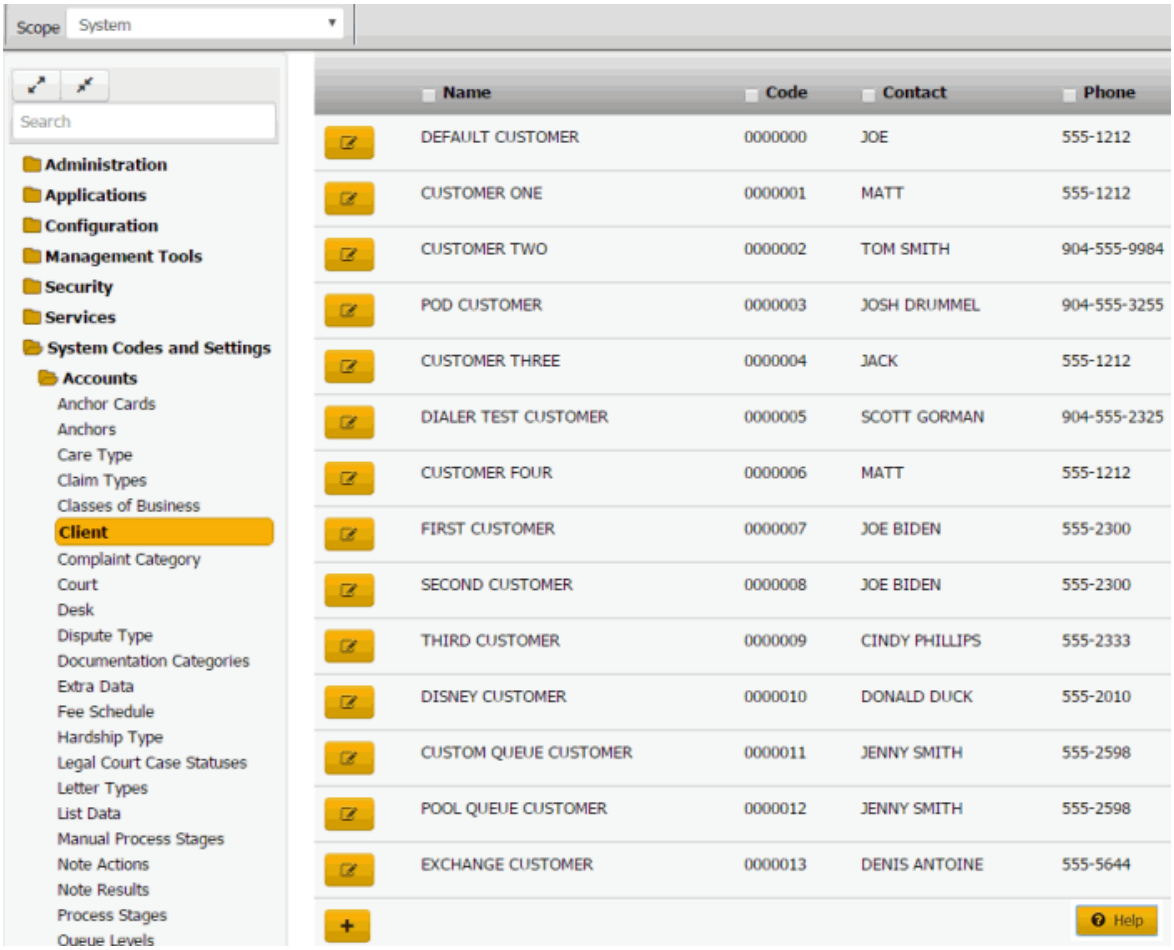
You can add, modify, and delete interest for a client. For more information, see Manage Interest.

Add Client Interest

Use the **Interest Detail** dialog box to add an interest rate used to calculate interest for a client.

To add client interest

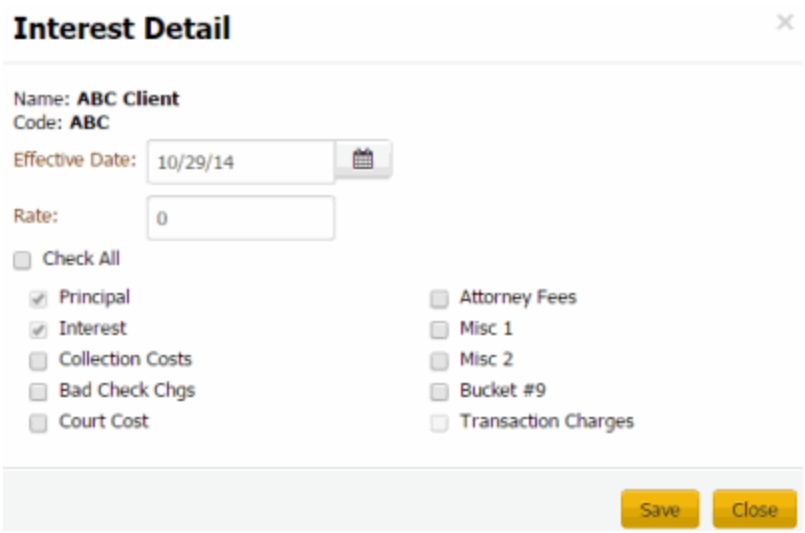
1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Client**.



Tip: To limit the clients that display in the data grid, click one or more check boxes next to a column heading. In the **Filter** box, type one or more characters and then press **Enter**. To clear a filter, clear the check boxes and then click the Refresh icon.

2. In the data grid, click the Edit icon and then click **Interest**.

3. Click the plus sign (+).



Name: Client's name.

Code: Unique code that identifies the client.

Effective Date: Date the interest rate takes effect.

Rate: Interest rate as a whole number. For example, if the interest rate is 7 percent, type "7" in the box.

Check All: If selected, Latitude selects all the money bucket check boxes.

Principal: If selected, Latitude includes principal when calculating interest.

Collection Costs: If selected, Latitude includes collection costs when calculating interest.

Bad Check Charges: If selected, Latitude includes bad check charges when calculating interest.

Court Costs: If selected, Latitude includes court costs when calculating interest.

Attorney Fees: If selected, Latitude includes attorney fees when calculating interest.

Misc 1 and **Misc 2:** If selected, Latitude includes miscellaneous costs when calculating interest.

Bucket #9: If selected, Latitude includes the amount in this money bucket when calculating interest.

Transaction Charges: If selected, Latitude includes transaction charges when calculating interest.

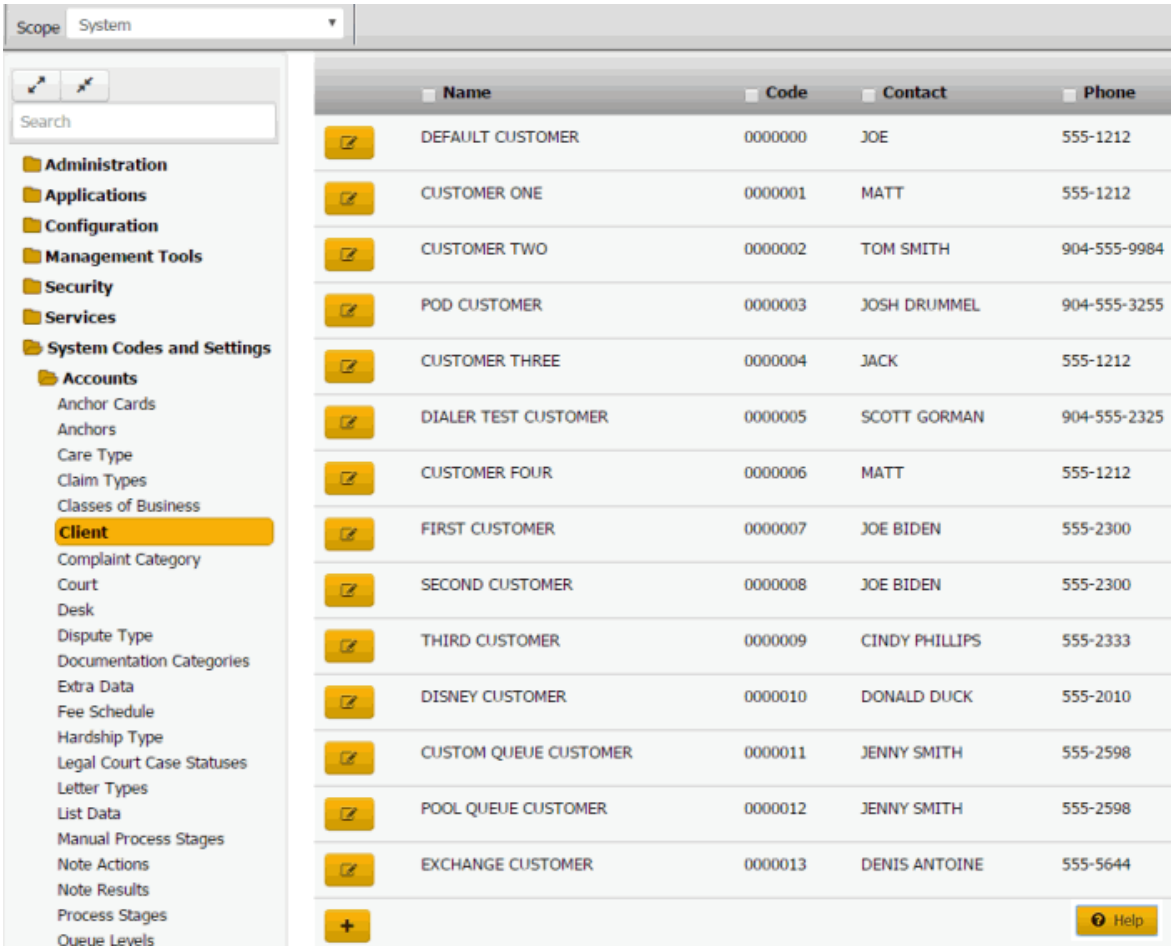
4. Complete the information and then click **Save**.

Modify Client Interest

Use the **Interest Detail** dialog box to modify an interest rate for a client. You can modify the effective date, interest rate, and money buckets to include in interest calculations.

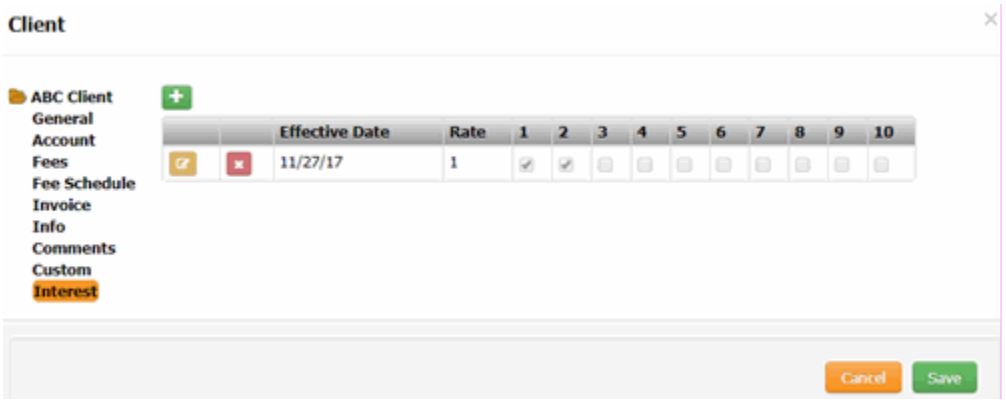
To modify client interest

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Client**.

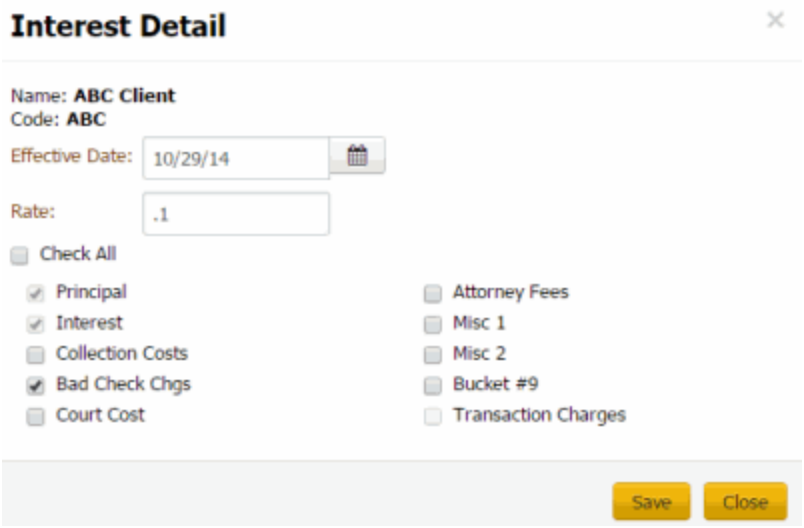


Tip: To limit the clients that display in the data grid, click one or more check boxes next to a column heading. In the **Filter** box, type one or more characters and then press **Enter**. To clear a filter, clear the check boxes and then click the Refresh icon.

2. In the data grid, click the Edit icon and then click **Interest**.



3. In the data grid, click the Edit icon.



Name: Client's name.

Code: Unique code that identifies the client.

Effective Date: Date the interest rate takes effect.

Rate: Interest rate as a whole number. For example, if the interest rate is 7 percent, type "7" in the box.

Check All: If selected, Latitude selects all the money bucket check boxes.

Principal: If selected, Latitude includes principal when calculating interest.

Collection Costs: If selected, Latitude includes collection costs when calculating interest.

Bad Check Charges: If selected, Latitude includes bad check charges when calculating interest.

Court Costs: If selected, Latitude includes court costs when calculating interest.

Attorney Fees: If selected, Latitude includes attorney fees when calculating interest.

Misc 1 and **Misc 2:** If selected, Latitude includes miscellaneous costs when calculating interest.

Bucket #9: If selected, Latitude includes the amount in this money bucket when calculating interest.

Transaction Charges: If selected, Latitude includes transaction charges when calculating interest.

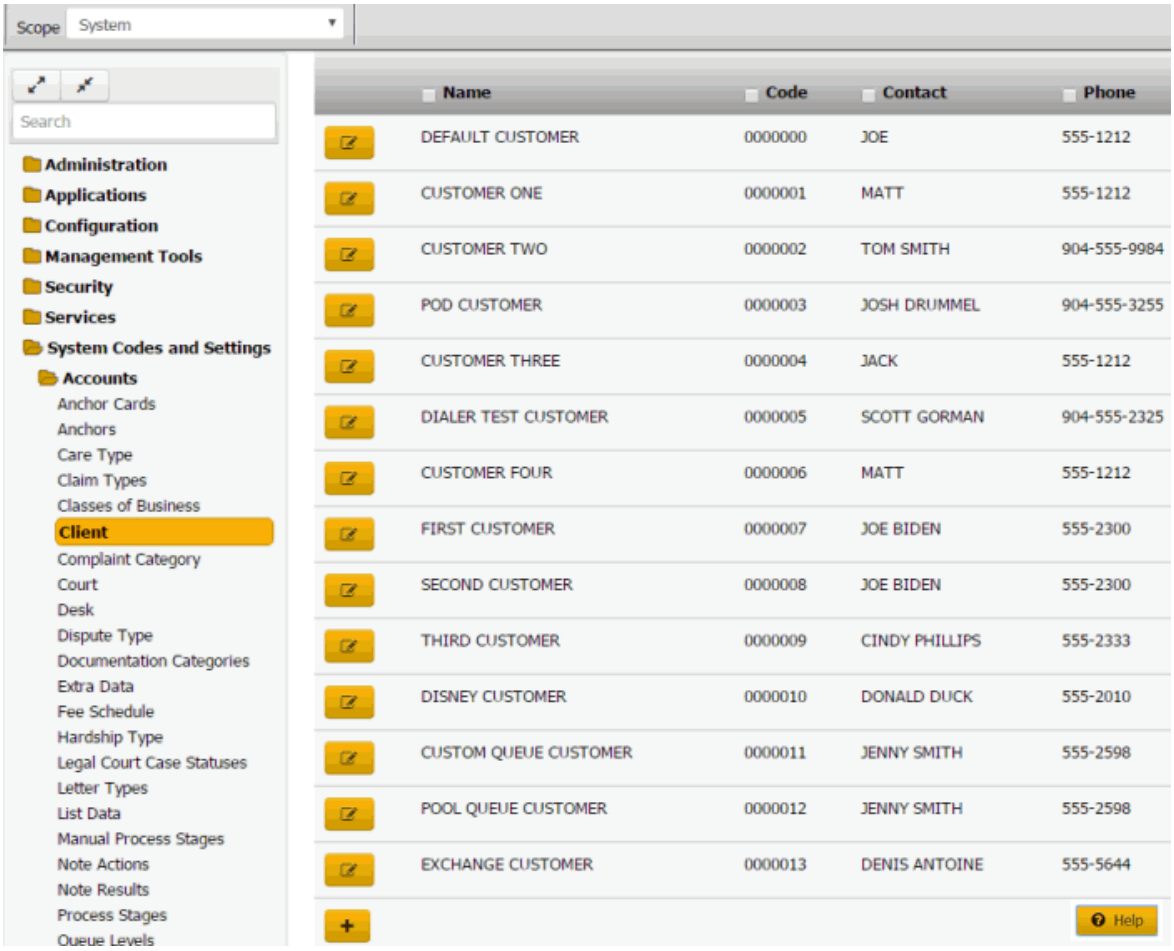
4. Modify the information and then click **Save**.

Delete Client Interest

Use the **Interest** tab in the **Client** dialog box to delete an interest rate for a client.

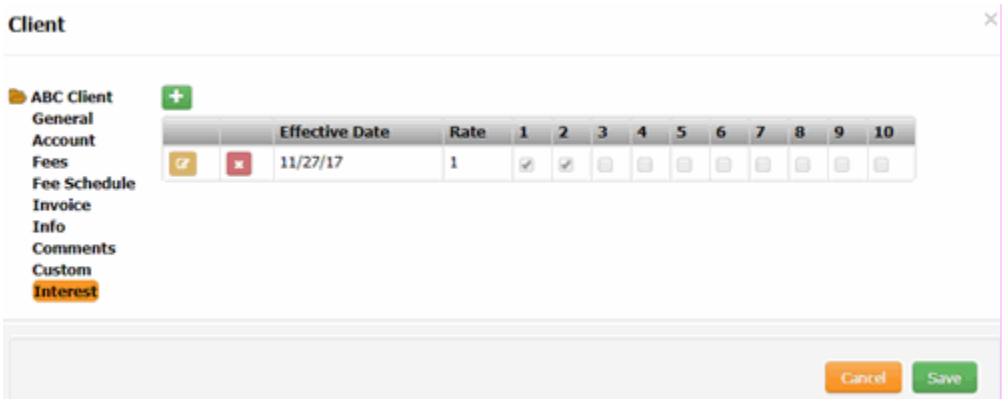
To modify client interest

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Client**.



Tip: To limit the clients that display in the data grid, click one or more check boxes next to a column heading. In the **Filter** box, type one or more characters and then press **Enter**. To clear a filter, clear the check boxes and then click the Refresh icon.

2. In the data grid, click the Edit icon and then click **Interest**.



3. In the data grid, click the Delete icon and then click **Yes**.

Complaint Categories

Complaint Categories

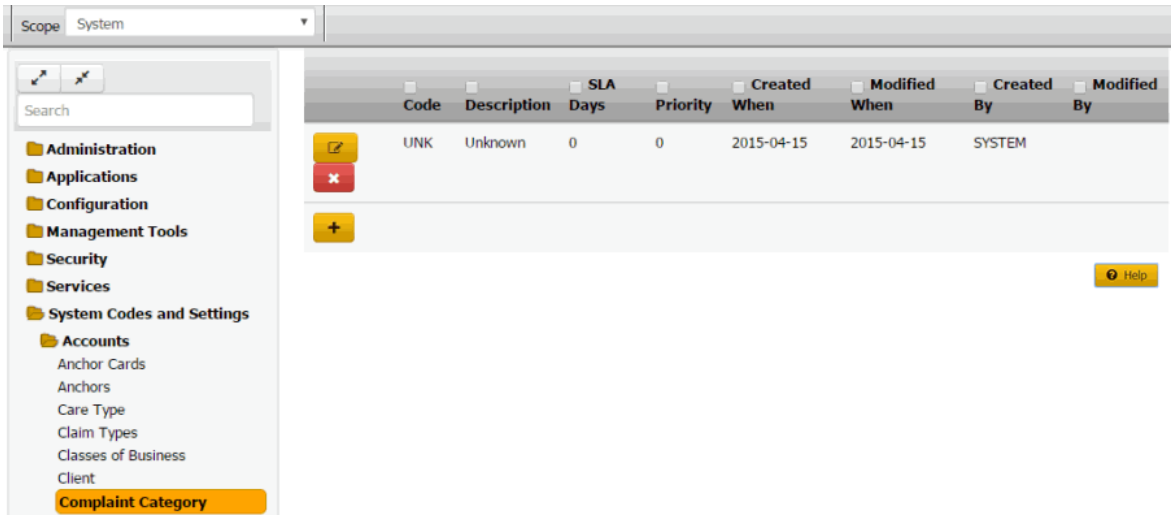
You can add, modify, and delete complaint categories, such as contact strategy, regulatory, and service. Users specify a complaint category when adding complaints. For more information, see Add a Complaint.

Add a Complaint Category

Use the **Complaint Category** panel to add a complaint category.

To add a complaint category

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Complaint Category**.



Code: Code that identifies the complaint category.

Description: Description of the complaint category.

SLA Days: Number of days after receiving the complaint that you have to resolve it before breaching the Service Level Agreement (SLA).

Priority: Priority level that determines when the Complaint Department works the complaint.

Created When: Date and time a user created this complaint category.

Modified When: Date and time a user last modified this complaint category.

Created By: User who created this complaint category.

Modified By: User who last modified this complaint category.

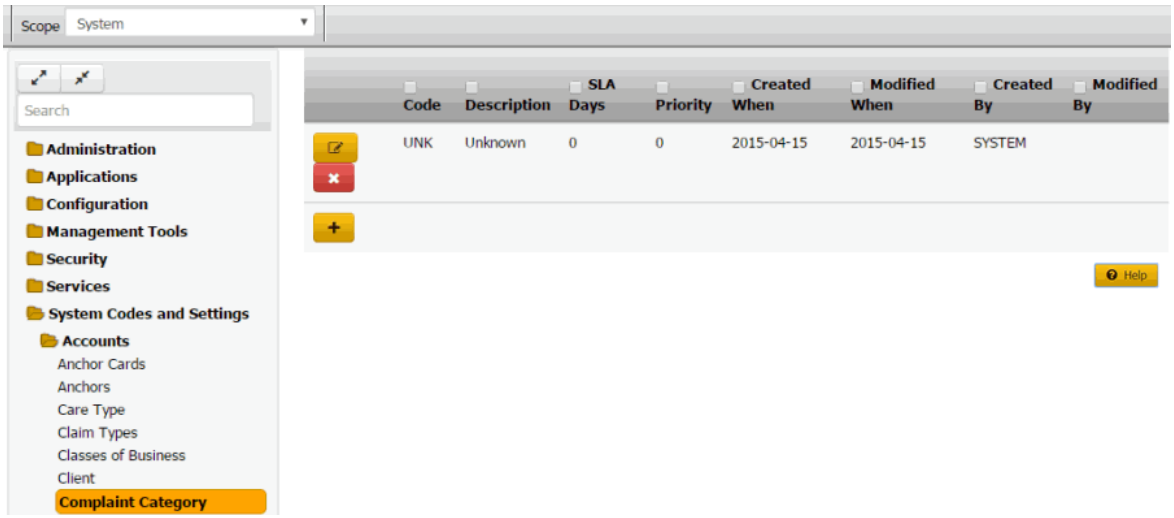
2. Click the plus sign (+). A blank row appears in the data grid.
3. Complete the information and then click the check mark.

Modify a Complaint Category

Use the **Complaint Category** panel to modify a complaint category.

To modify a complaint category

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Complaint Category**.



Code: Code that identifies the complaint category.

Description: Description of the complaint category.

SLA Days: Number of days after receiving the complaint that you have to resolve it before breaching the Service Level Agreement (SLA).

Priority: Priority level that determines when the Complaint Department works the complaint.

Created When: Date and time a user created this complaint category.

Modified When: Date and time a user last modified this complaint category.

Created By: User who created this complaint category.

Modified By: User who last modified this complaint category.

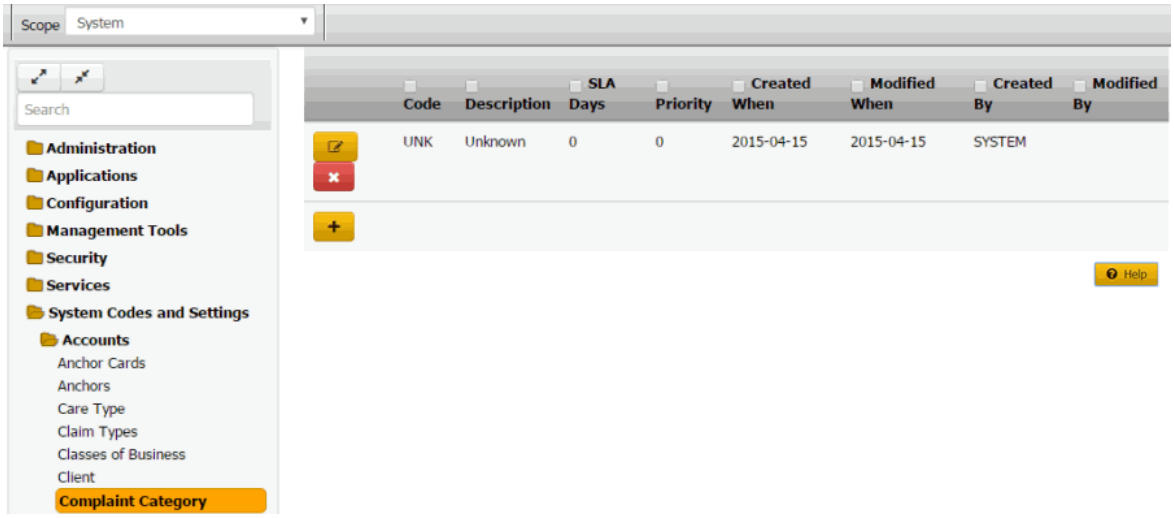
2. Click the Edit icon. The complaint category appears in edit mode.
3. Modify the information and then click the check mark.

Delete a Complaint Category

Use the **Complaint Category** panel to delete a complaint category.

To delete a complaint category

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Complaint Category**.



2. Click the Delete icon and then click **Yes**.

Courts

Courts

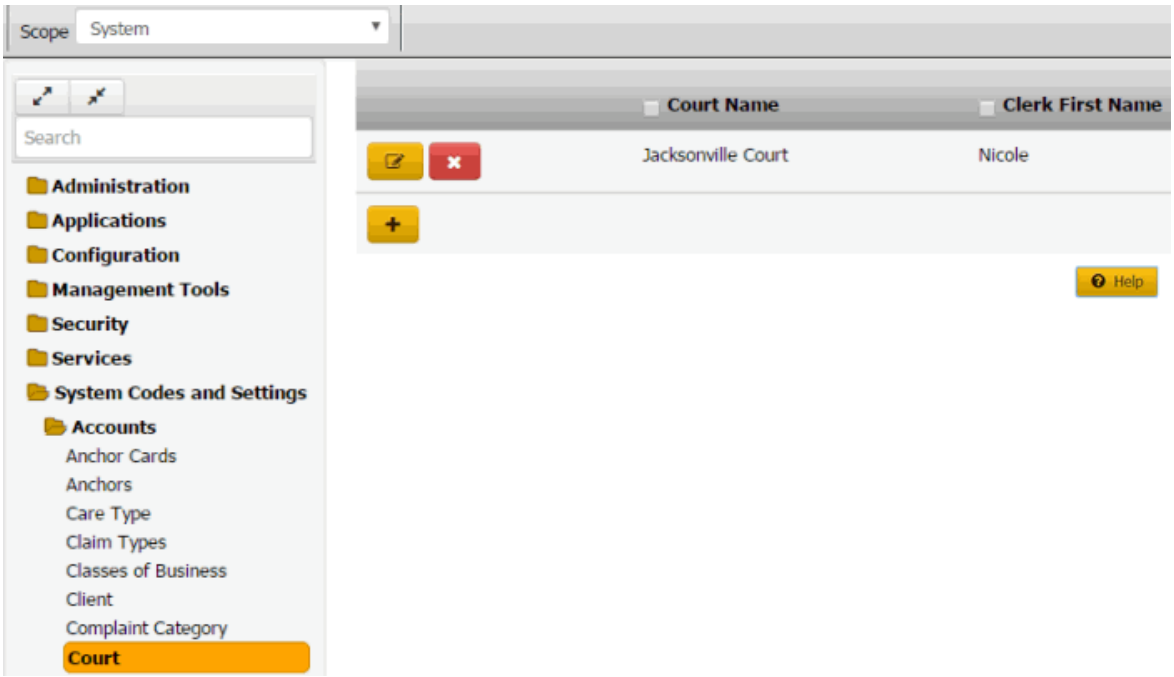
You can search for, add, modify, and delete courts of law. Users specify a court when assigning a court to a legal case. For more information, see Assign a Court.

Add a Court of Law

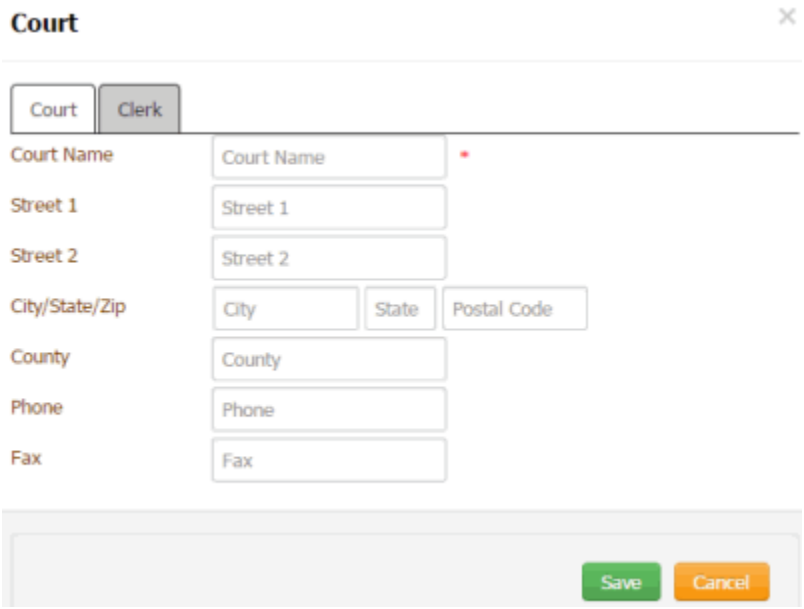
Use the **Court** dialog box to add a court of law.

To add a court of law

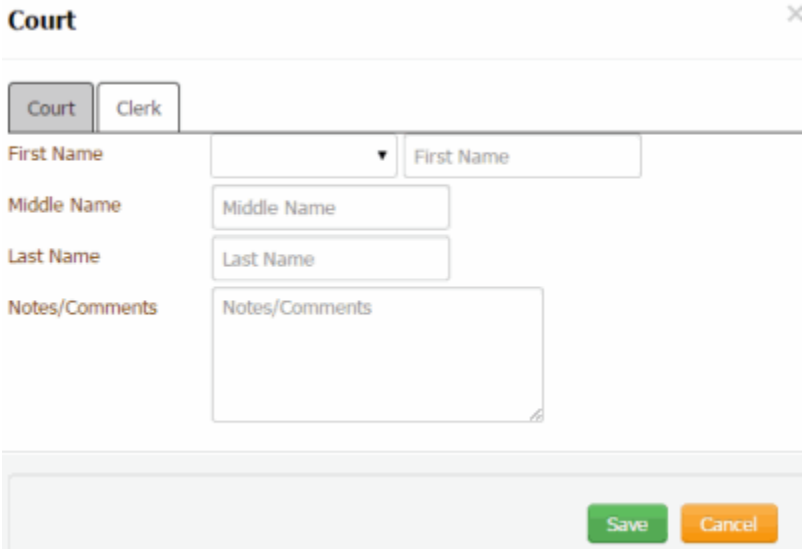
1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Court**.



2. Click the plus sign (+). The **Court** dialog box appears.



3. Complete the information and then click the **Clerk** tab.



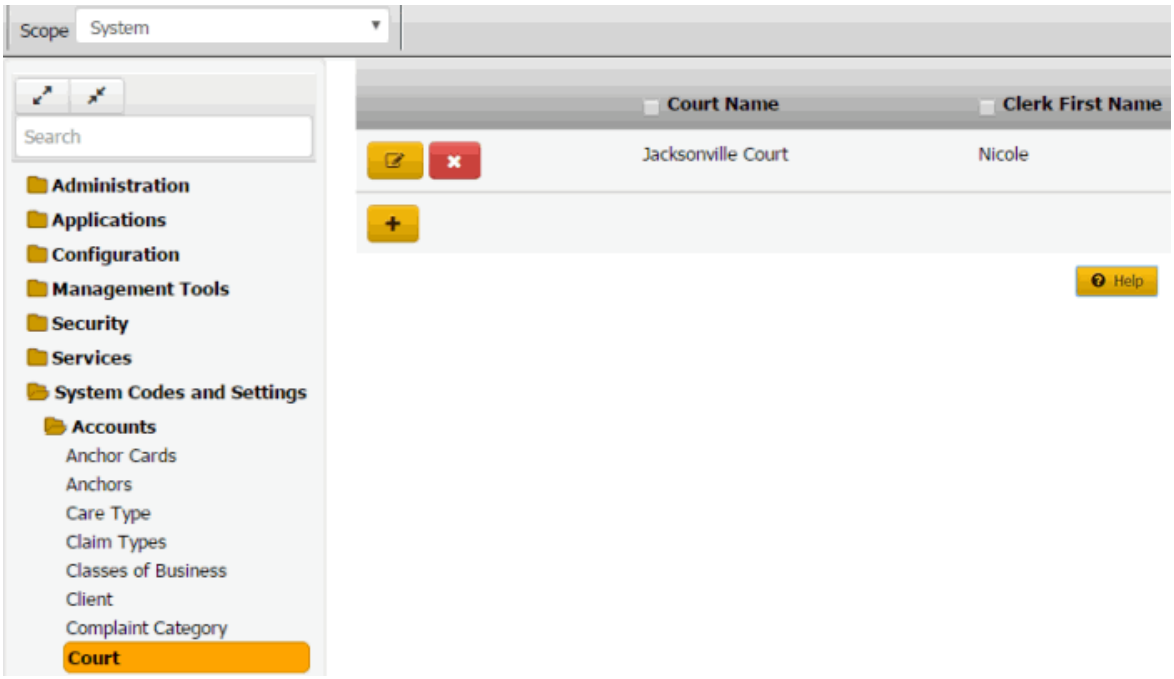
4. Complete the information and then click **Save**.

Modify a Court of Law

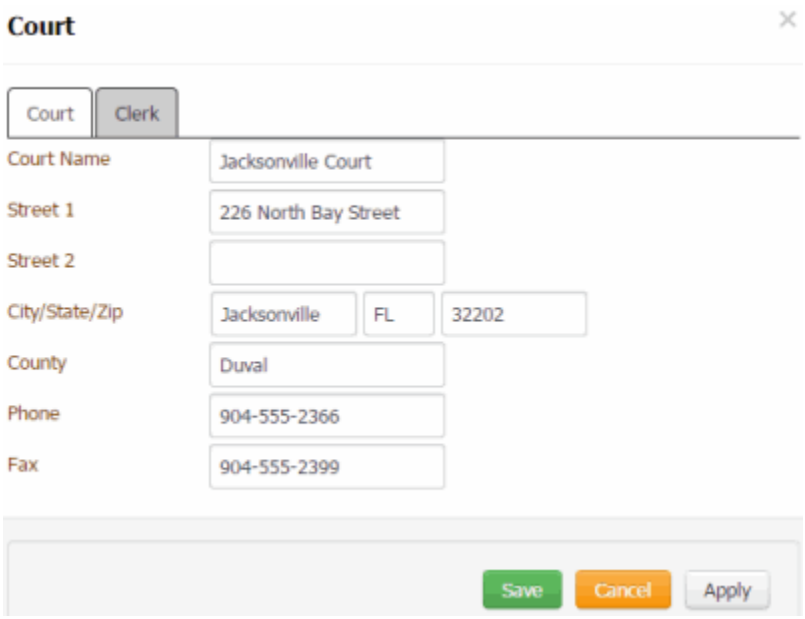
Use the **Court** dialog box to modify a court of law.

To modify a court of law

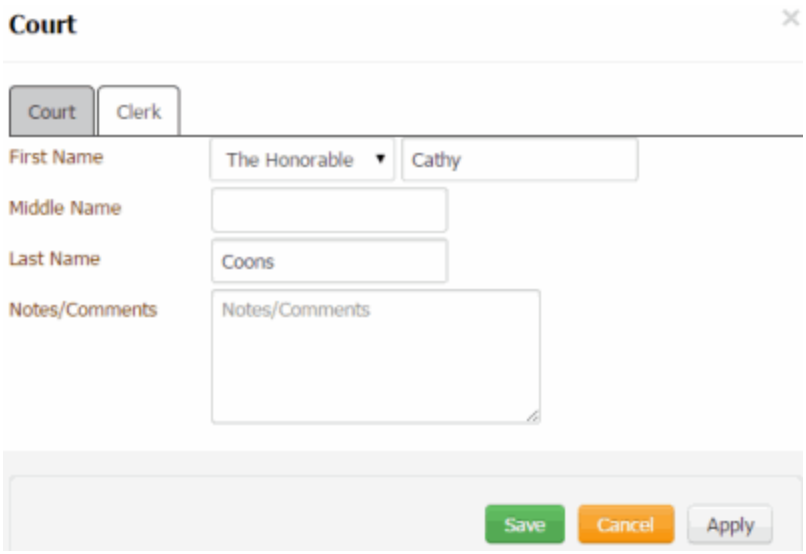
1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Court**.



2. Click the Edit icon . The **Court** dialog box appears.



3. Modify the information and then click the **Clerk** tab.



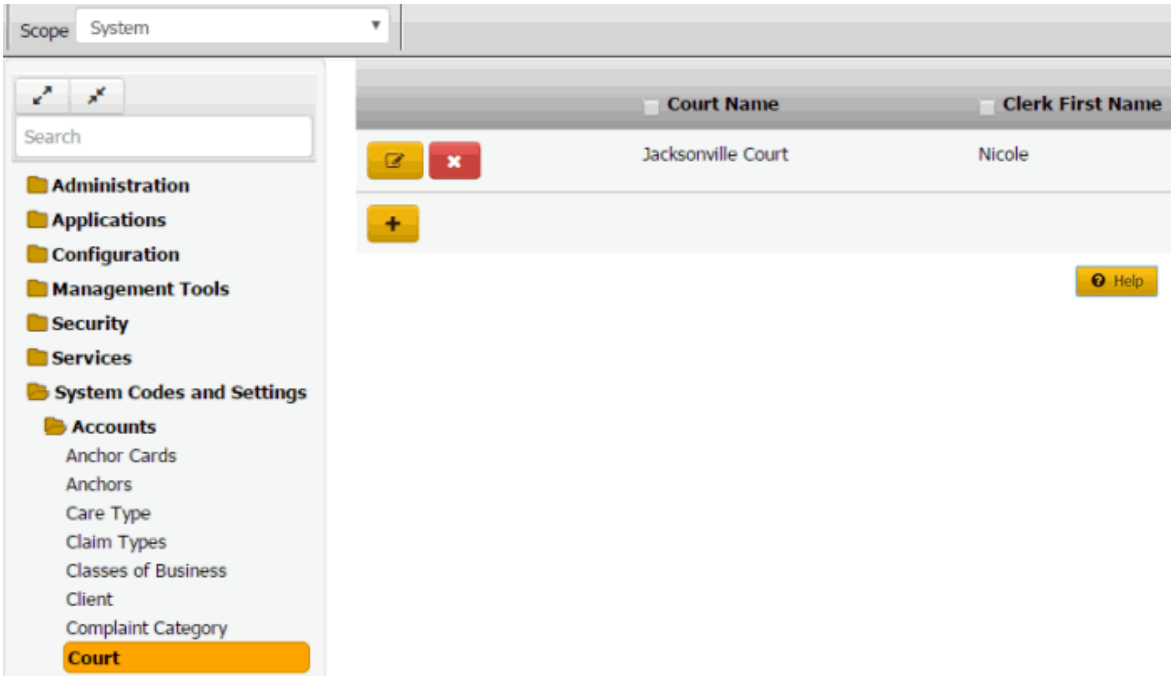
4. Modify the information and then click **Save**.

Delete a Court of Law

Use the **Court** panel to delete a court of law.

To delete a court of law

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Court**.



2. Click the Delete icon and then click **Yes**.

Custom Panel Mapping

Custom Panel Mapping

You can search for, add, modify, and delete custom anchor cards and reference panels that display in the **Work Form**. You map a custom anchor card or reference panel to a query that specifies the data to display in the card or panel. You can map a single query to one anchor card and one reference panel only.

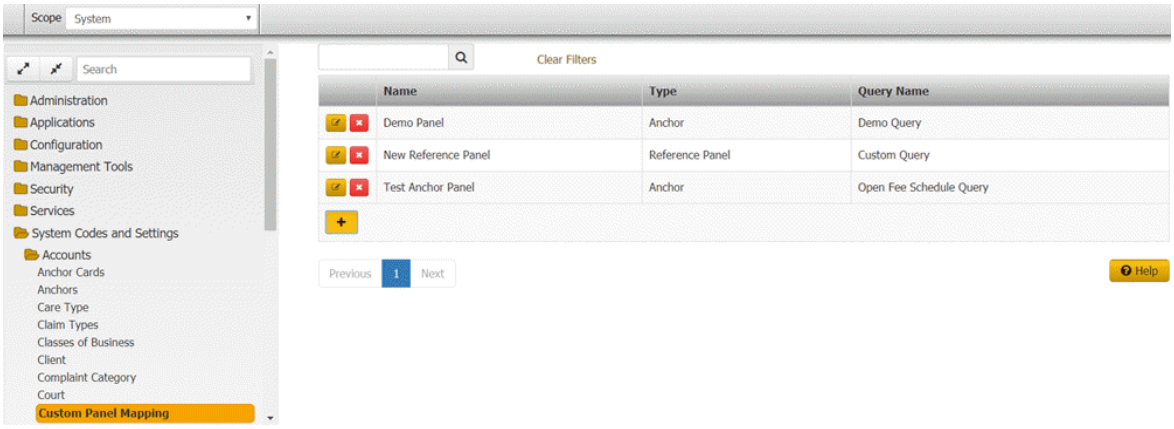
For more information about creating queries for custom anchor cards or reference panels, see "Custom Panel Query Creator" in the Latitude Console documentation.

Search for a Custom Anchor Card or Reference Panel

Use the **Custom Panel Mapping** panel to search for a custom anchor card or reference panel.

To search for a custom anchor card or reference panel

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Custom Panel Mapping**.



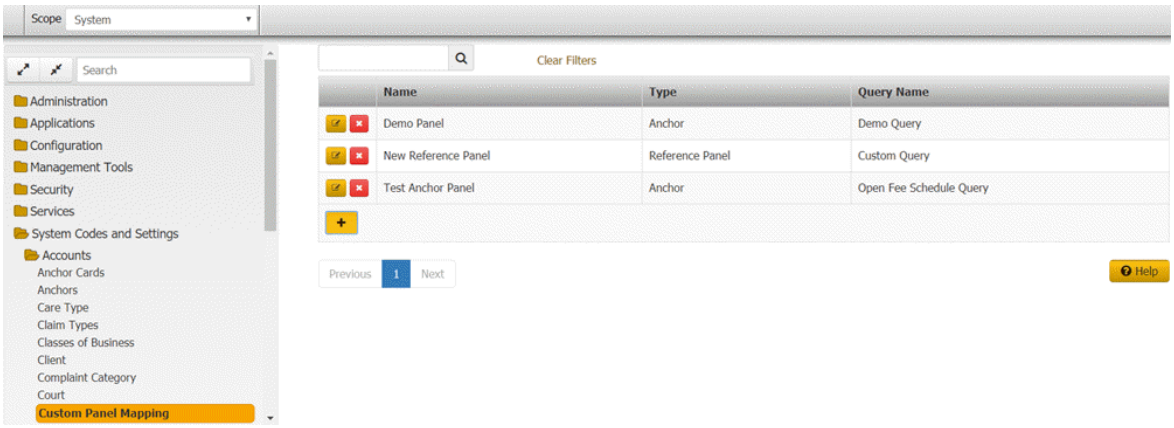
2. In the **Search** box in the **Custom Panel Mapping** panel, type one or more characters to search and then press **Enter** or click the Search icon. The system searches the custom anchor card or reference panel name, type, and query name for a match. It displays only the custom anchor cards and reference panels that match your search criteria.
3. To clear the search criteria, click **Clear Filters**. The system displays all custom panel mappings.

Add a Custom Anchor Card or Reference Panel

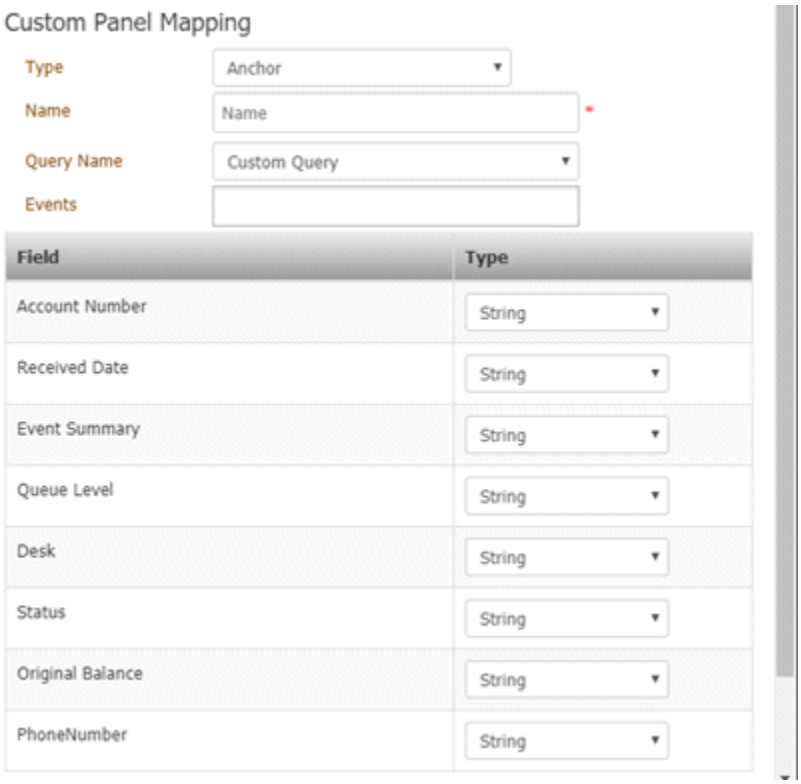
Use the **Custom Panel Mapping** panel to add a custom anchor card or reference panel.

To add a custom anchor card or reference panel

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Custom Panel Mapping**.



2. Click the plus sign (+). The **Custom Panel Mapping** dialog box appears.



Type: Indicates whether the mapping is for a custom anchor card or reference panel.

Name: Name to assign to the custom anchor card or reference panel.

Query Name: Name of the query to map to the custom anchor card or reference panel.

> **Note:** You can map a single query to one anchor card and one reference panel only.

Events: Events that, when triggered, refresh the custom anchor card or reference panel in the **Work Form**.

Field: Field specified in the query to display in the custom anchor card or reference panel.

Type: Data type to assign to the field.

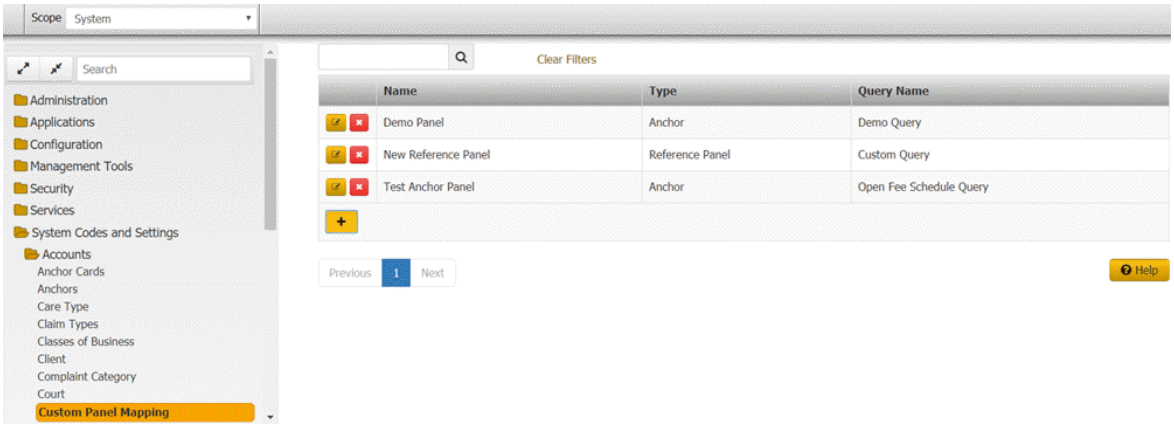
3. Complete the information and then click **Save**. One of the following occurs:
    - If you mapped a custom anchor card, the system adds the custom anchor card to the list of available anchor cards that you can associate to an anchor. For more information about anchor cards, see Anchor Cards.
    - If you mapped a custom reference panel, the system adds the custom reference panel to the list of available reference panels in the Reference Panels permission. For more information about the permission, see Reference Panels Permission.
4. Do one of the following:
    - If you mapped a custom anchor card, add the anchor card to an anchor to allow users to view the card in the **Work Form**. For more information, see Add an Anchor Card to an Anchor.
    - If you mapped a custom reference panel, select the reference panel in the Reference Panels permission to allow users to view the panel in the **Work Form**. For more information, see Reference Panels Permission.

Modify a Custom Anchor Card or Reference Panel

Use the **Custom Panel Mapping** panel to modify a custom anchor or reference panel.

To modify a custom anchor card or reference panel

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Custom Panel Mapping**.

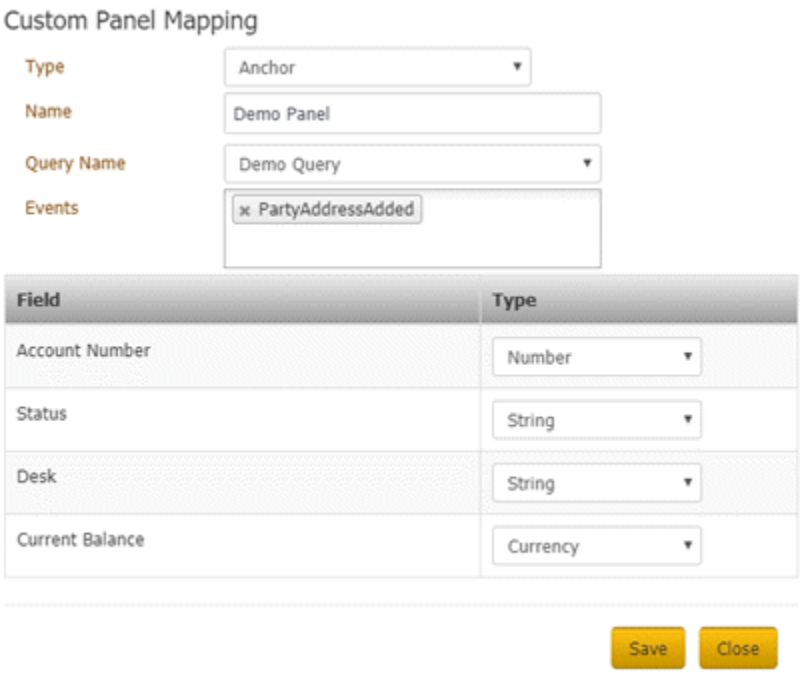


Name: Name of the custom anchor card or reference panel.

Type: Indicates whether the mapping is for an anchor card or reference panel.

Query Name: Name of the query to map to the custom anchor card or reference panel.

2. Click the Edit icon. The **Custom Panel Mapping** dialog box appears.



Type: Indicates whether the mapping is for a custom anchor card or reference panel.

Name: Name of the custom anchor card or reference panel.

Query Name: Name of the query mapped to the custom anchor card or reference panel.

> **Note:** You can map a single query to one anchor card and one reference panel only.

Events: Events that, when triggered, refresh the custom anchor card or reference panel in the **Work Form**.

Field: Field specified in the query to display in the custom anchor card or reference panel.

Type: The field's data type.

3. Modify the information and then click **Save**. One of the following occurs:
    - If you changed the mapping from a custom reference panel to a custom anchor card, the system adds the card to the list of available anchor cards. The system removes the custom reference panel from the list of available reference panels in the Reference Panels permission.
    - If you changed the mapping from a custom anchor card to a custom reference panel, the system adds the panel to the list of available reference panels in the Reference Panels permission. The system removes the custom anchor card from the list of available anchor cards and removes it from the associated anchor.
4. Do one of the following:
    - If you changed the mapping from a custom reference panel to a custom anchor card, add the anchor card to an anchor to allow users to view the card in the **Work Form**. For more information, see Add an Anchor Card to an Anchor.

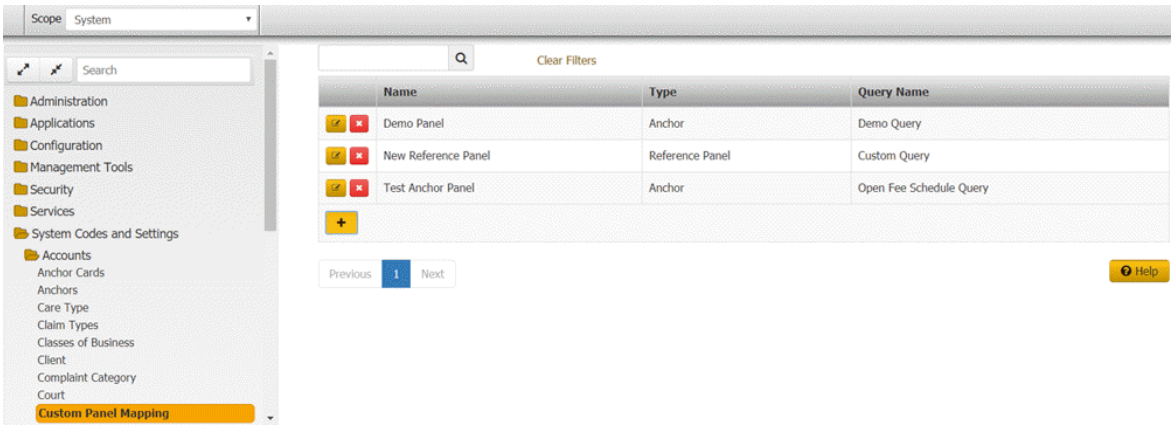
- If you changed the mapping from a custom anchor card to a custom reference panel, select the reference panel in the Reference Panels permission to allow users to view the panel in the **Work Form**. For more information, see Reference Panels Permission.

Delete a Custom Anchor Card or Reference Panel

Use the **Custom Panel Mapping** panel to delete a custom anchor card or reference panel.

To delete a custom anchor card or reference panel

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Custom Panel Mapping**.



2. Click the Delete icon and then click **Yes**.

Desks

Desks

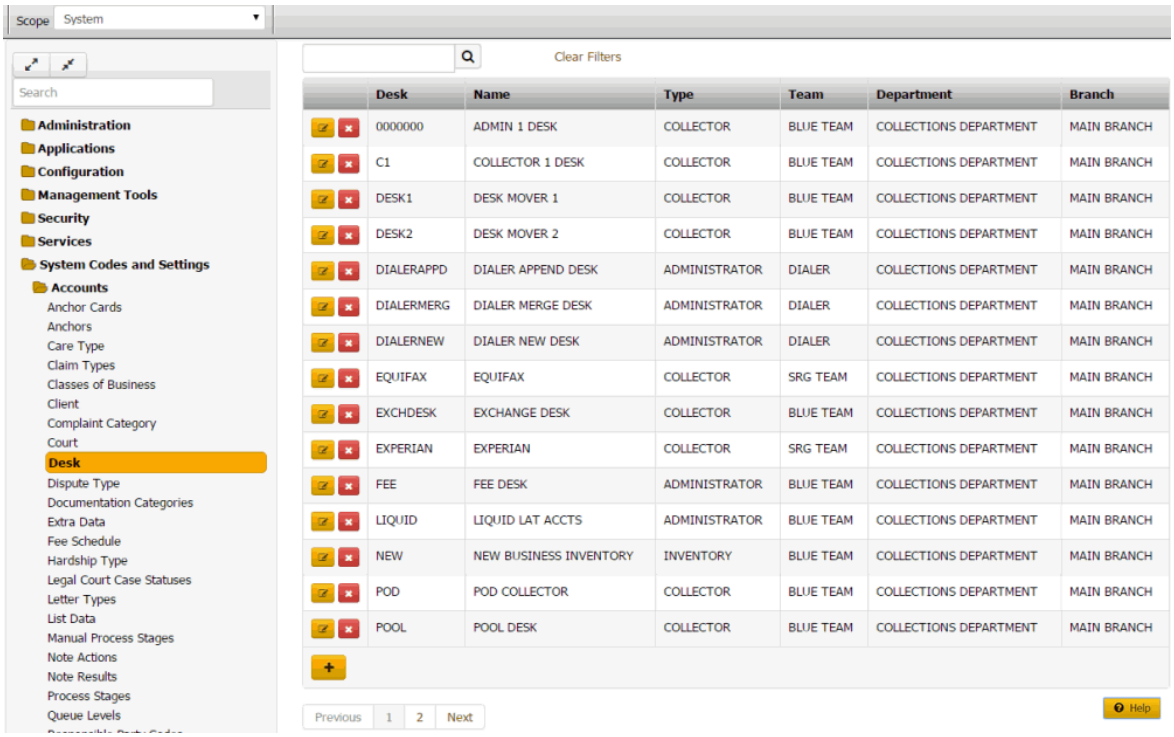
You can search for, add, modify, copy, and delete desks. You can also set limits for desks. You assign users to desks and then assign accounts to desks. Users work the accounts assigned to their desk.

Search for a Desk

Use the **Desk** panel to search for a desk.

To search for a desk

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Desk**.



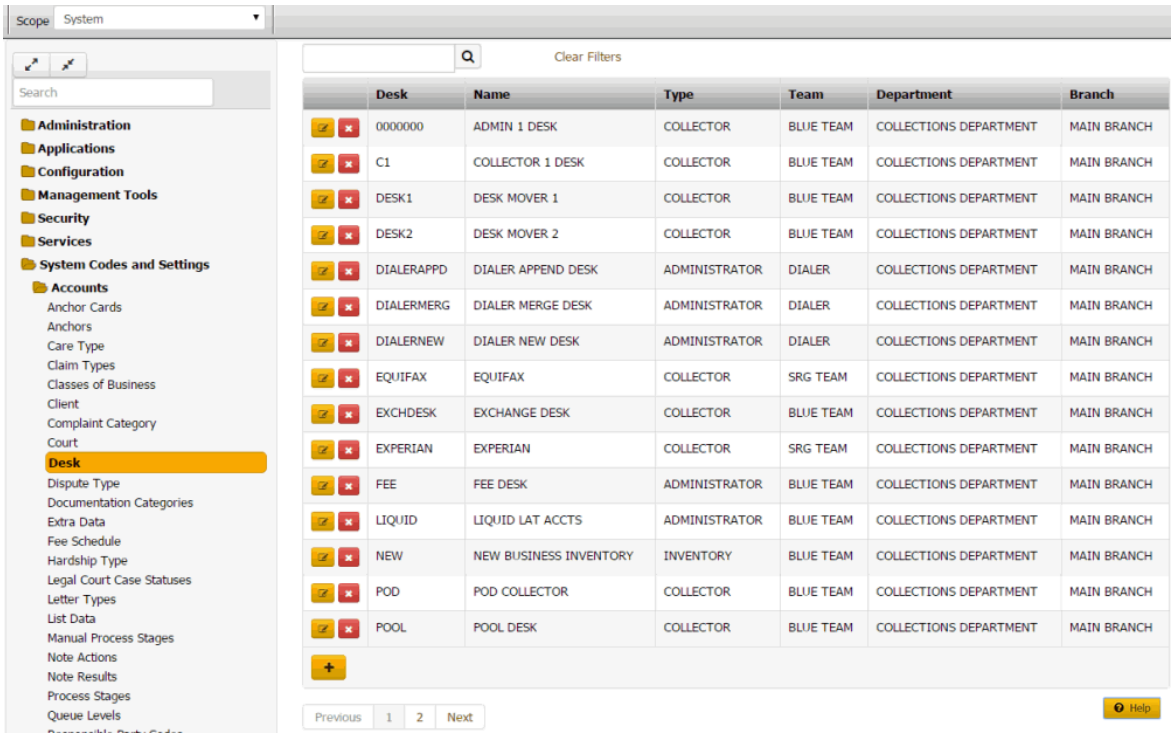
2. In the **Search** box in the **Desk** panel, type one or more characters to search and then press **Enter** or click the Search icon. The system searches the desk code, desk name, desk type, team, department, and branch for a match. It displays only the desks that match your search criteria.
3. To clear the search criteria, click **Clear Filters**. The system displays all desks.

Add a Desk

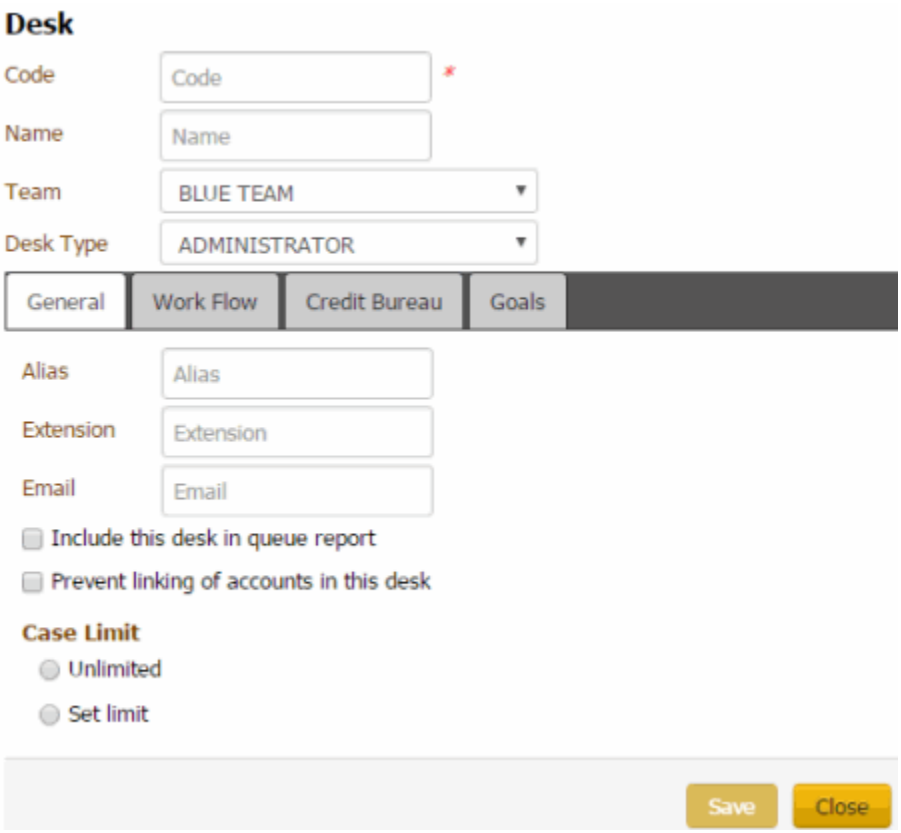
Use the **Desk** dialog box to add a desk code.

To add a desk code

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Desk**.



2. Click the plus sign (+). The **Desk** dialog box appears with the **General** tab selected.



Code: Unique code that identifies the desk.

Name: Name of the desk.

Team: Used to determine the department and branch assigned to the desk.

Desk Type: The type of desk assigned is for information purposes only, except for the inventory desk. Latitude uses Inventory desks to receive new business for your organization. Valid values are:

Administrator: Not used

Clerical: Not used

Supervisor: Not used

AIM: Used only for holding accounts forwarded to outside agencies using the Agency Interface Module (AIM) program.

Collector: Holds accounts for a particular user.

Inventory: Repository for new accounts, used when importing new business. You can distribute accounts in the inventory desk using the Desk Mover program.

Alias: Collector's name inserted in letters in place of the **Alias** merge field.

Extension: Collector's phone extension inserted in letters in place of the **Extension** merge field.

Email: Collector's email address inserted in letters in place of the **Email** merge field.

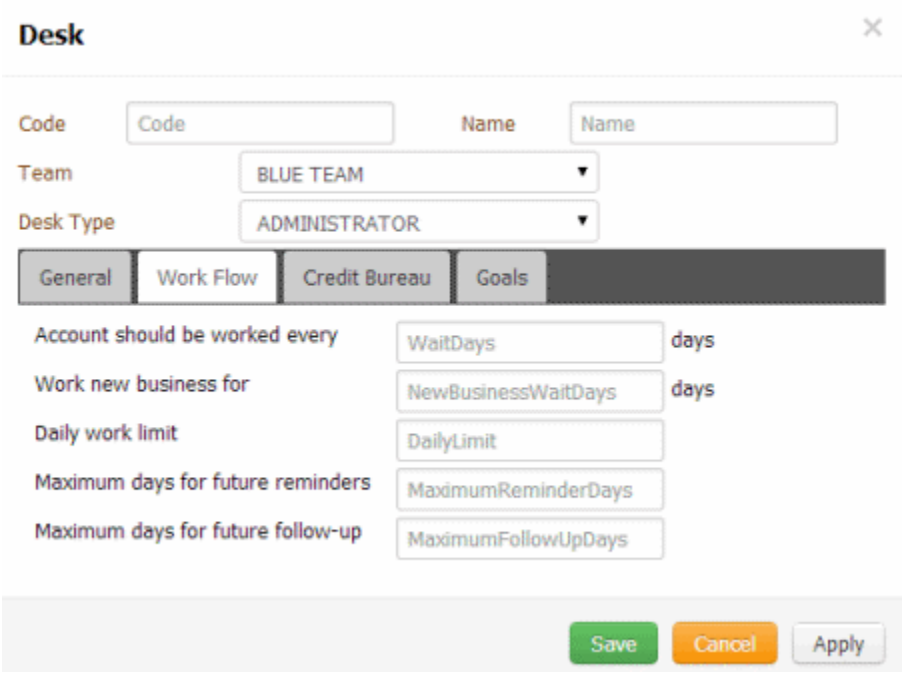
Include this desk in queue report: If selected, the Collector Queue and Monthly Collections reports include account information for this desk.

Prevent linking of accounts in this desk: If selected, you cannot link accounts in this desk to other accounts. This option only applies when linking accounts automatically using Link Console. Manual linking does not respect this rule.

Unlimited: If selected, the desk can have an unlimited number of accounts assigned to it.

Set Limit: If selected, type the maximum number of accounts that users can assign to a desk.

3. Complete the information and then click the **Work Flow** tab.



Accounts should be worked every __ days: Maximum number of days between working an account assigned to this desk that Latitude waits before setting an account follow-up for the next day.

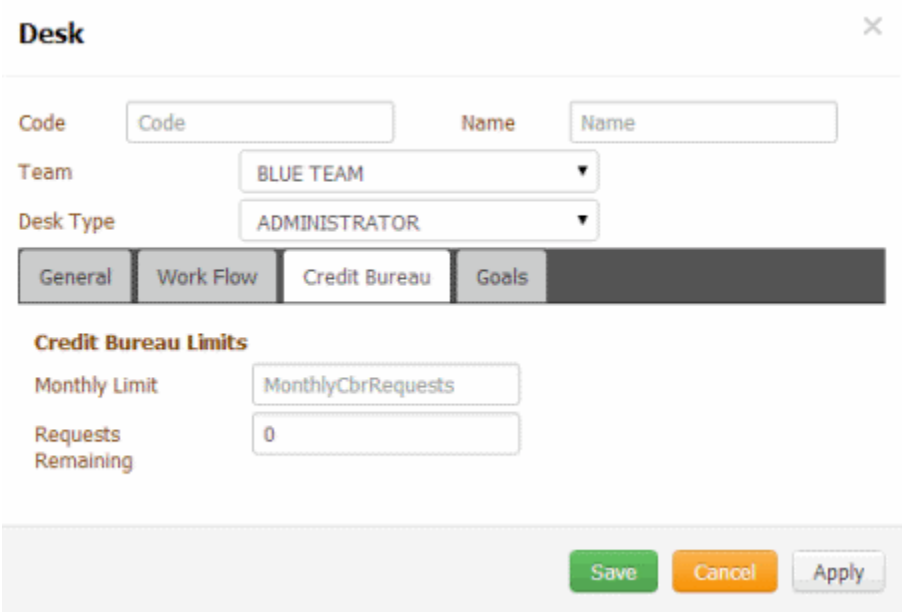
Work new business for __ days: Maximum number of days that the user can work an account assigned to this desk as queue level 016 (new business follow-up) before the account moves to another queue level.

Daily Work Limit: Maximum number of accounts that this desk can have set for follow-up work for any 24 hour period.

Maximum days for future reminders: Maximum number of days ahead a user can set a reminder for an account assigned to this desk.

Maximum days for future follow-up: Maximum number of days ahead a user can set a follow-up date for an account assigned to this desk.

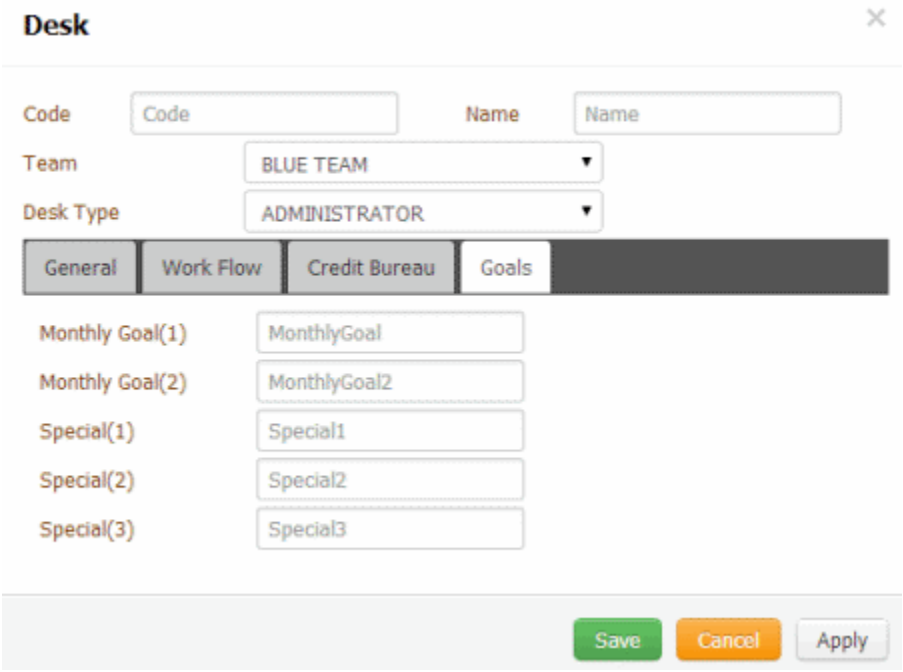
4. Complete the information and then click the **Credit Bureau** tab.



Monthly Limit: Maximum number of credit bureau reports the desk can request each month. You cannot set this number higher than 32,000.

Requests Remaining: If setting up a new desk, the number of requests allowed for the desk for the rest of the current month. For example, if the monthly limit is "50" and the desk has already requested "20" reports this month, type "30" in this box. Latitude starts tracking this number after you save the desk.

5. Complete the information and then click the **Goals** tab.



Monthly Goal (1): Number of credit bureau reports the desk strives to attain each month.

Monthly Goal (2): Number of credit bureau reports the desk strives to attain each alternative month.

Special (1): Number of special request goals for the desk.

Special (2): Number of special request goals for the desk.

Special (3): Number of special request goals for the desk.

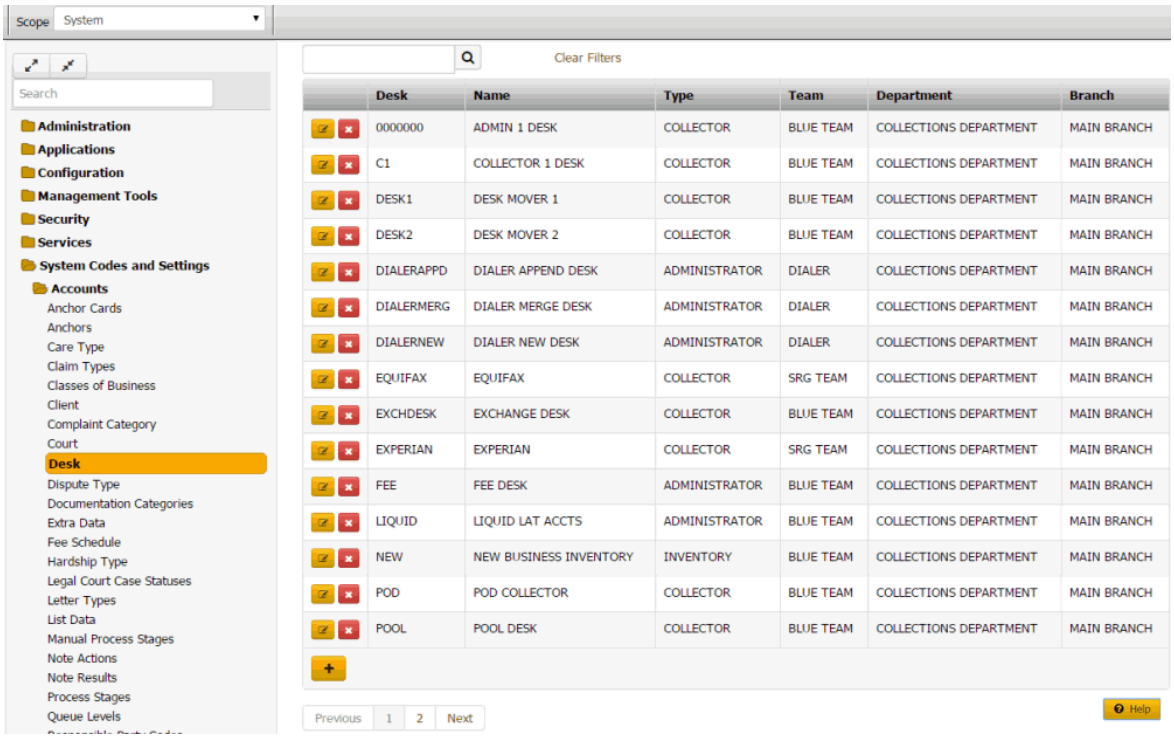
6. Complete the information and then click **Save**.

Modify a Desk

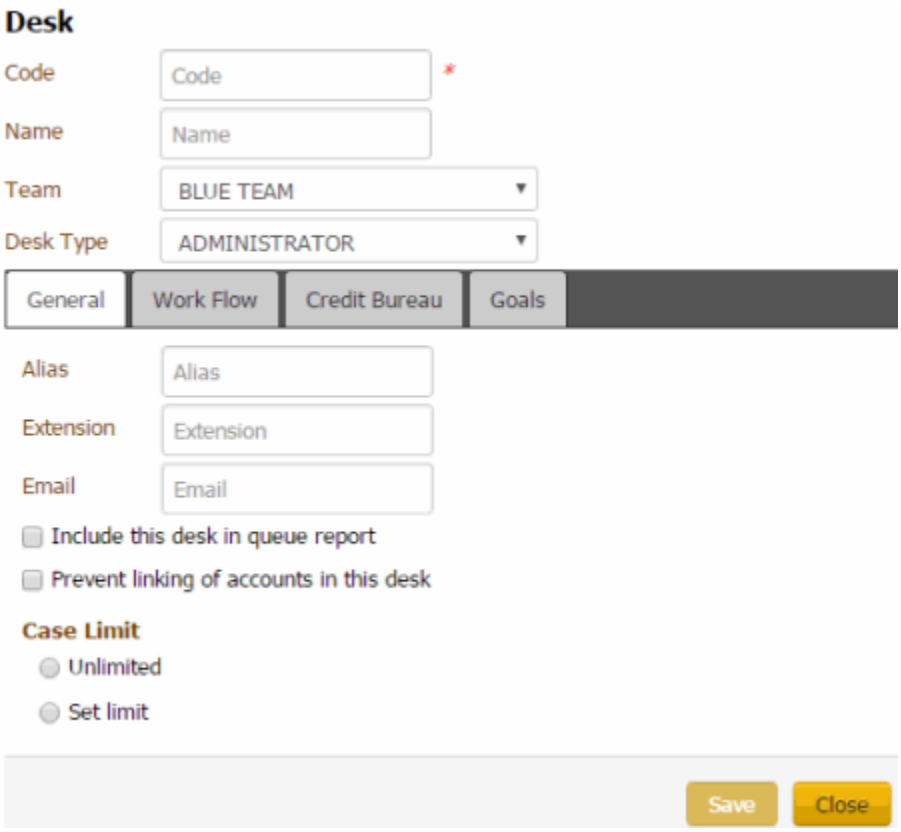
Use the **Desk** dialog box to modify a desk code.

To modify a desk code

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Desk**.



2. Click the Edit icon. The **Desk** dialog box appears with the **General** tab selected.



Code: Unique code that identifies the desk.

Name: Name of the desk.

Team: Used to determine the department and branch assigned to the desk.

Desk Type: The type of desk assigned is for information purposes only, except for the inventory desk. Latitude uses Inventory desks to receive new business for your organization. Valid values are:

> **Administrator**: Not used
>
> **Clerical**: Not used
>
> **Supervisor**: Not used
>
> **AIM**: Used only for holding accounts forwarded to outside agencies using the Agency Interface Module (AIM) program.
>
> **Collector**: Holds accounts for a particular user.
>
> **Inventory**: Repository for new accounts, used when importing new business. You can distribute accounts in the inventory desk using the Desk Mover program.

Alias: Collector's name inserted in letters in place of the **Alias** merge field.

Extension: Collector's phone extension inserted in letters in place of the **Extension** merge field.

Email: Collector's email address inserted in letters in place of the **Email** merge field.

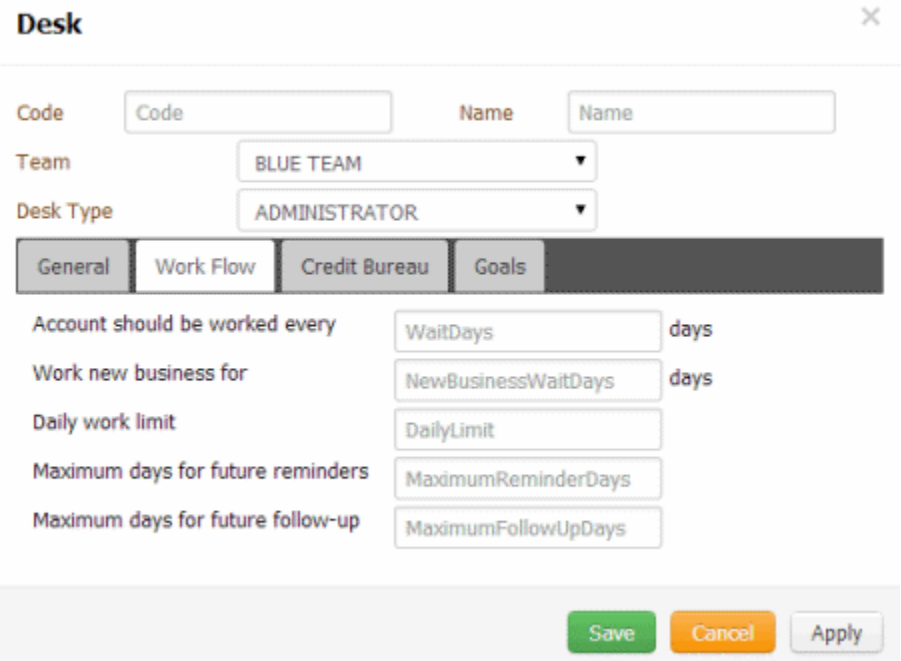
Include this desk in queue report: If selected, the Collector Queue and Monthly Collections reports include account information for this desk.

Prevent linking of accounts in this desk: If selected, you cannot link accounts in this desk to other accounts. This option only applies when linking accounts automatically using Link Console. Manual linking does not respect this rule.

Unlimited: If selected, the desk can have an unlimited number of accounts assigned to it.

Set Limit: If selected, type the maximum number of accounts that users can assign to a desk.

3. Modify the information and then click the **Work Flow** tab.



Accounts should be worked every __ days: Number of days an account is idle while assigned to the desk that Latitude waits before prompting the user to work it. Once this number of days passes, Latitude sets the follow-up date to the next day.

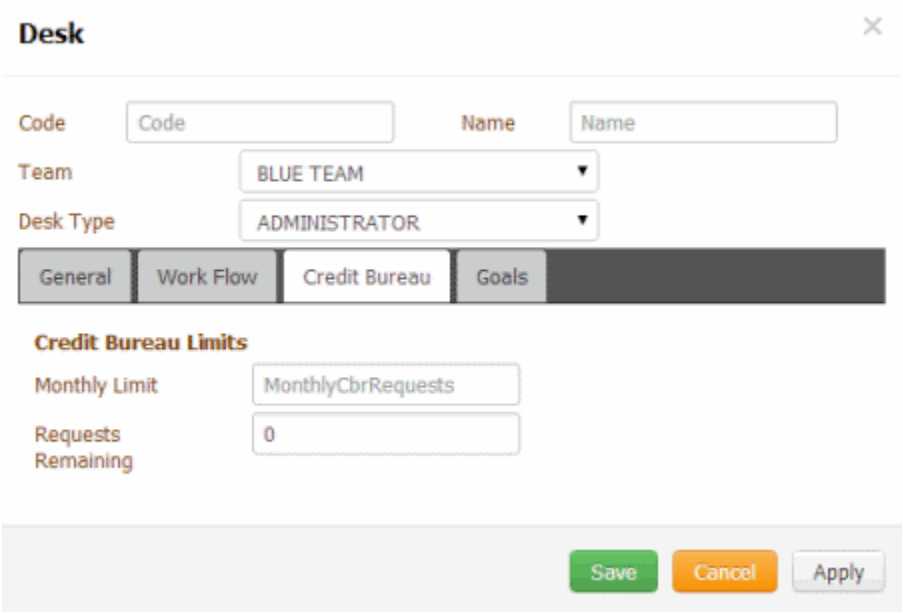
Work new business for __ days: Number of days that the user works new business while it's assigned to the desk. Once the user works the new business for the specified number of days, Latitude moves the account to the 0-30 day queue (020).

Daily Work Limit: Number of accounts that the desk can set for follow-up work for any 24 hour period.

Maximum days for future reminders: Maximum number of days ahead a user can set a reminder for an account assigned to this desk.

Maximum days for future follow-up: Maximum number of days ahead a user can set a follow-up date for an account assigned to this desk.

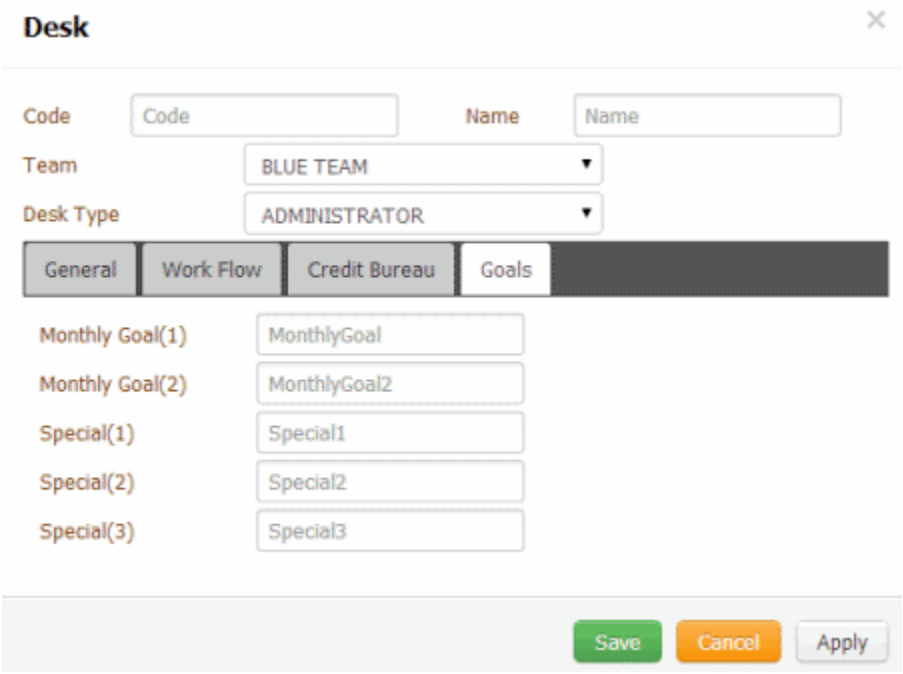
4. Modify the information as necessary and then click the **Credit Bureau** tab.



Monthly Limit: Maximum number of credit bureau reports the desk can request each month. You cannot set this number higher than 32,000.

Requests Remaining: If setting up a new desk, the number of requests allowed for the desk for the rest of the current month. For example, if the monthly limit is "50" and the desk has already requested "20" reports this month, type "30" in this box. Latitude starts tracking this number after you save the desk.

5. Modify the information as necessary and then click the **Goals** tab.



Monthly Goal (1): Number of credit bureau reports the desk strives to attain each month.

Monthly Goal (2): Number of credit bureau reports the desk strives to attain each alternative month.

Special (1): Number of special request goals for the desk.

Special (2): Number of special request goals for the desk.

Special (3): Number of special request goals for the desk.

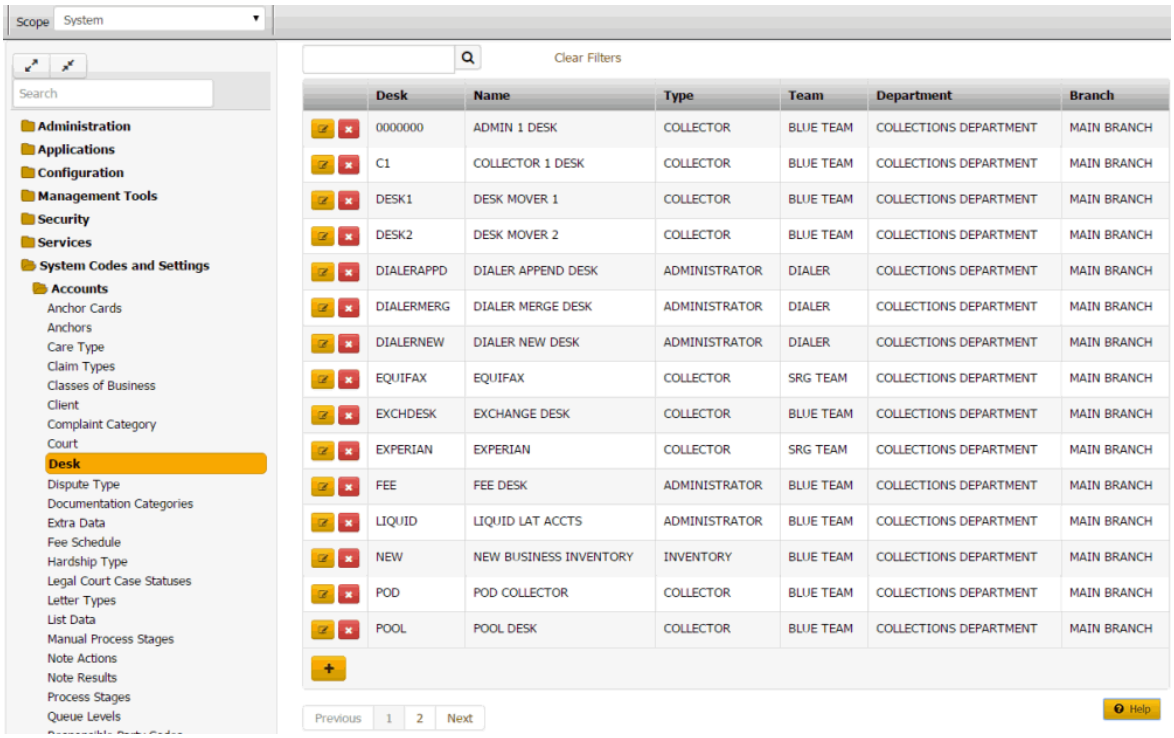
6. Modify the information as necessary and then click **Save**.

Delete a Desk

Use the **Desk** panel to delete a desk code. Only Administrators can delete desk codes.

To delete a desk code

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Desk**.



2. Click the Delete icon and then click **Yes**.

Dispute Types

Dispute Types

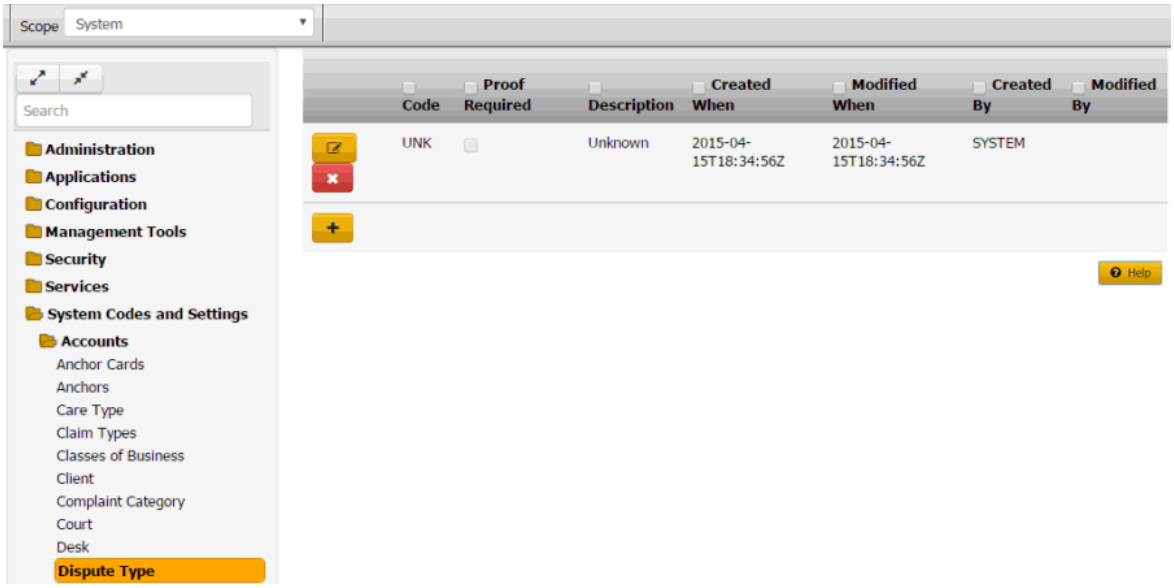
You can add, modify, and delete debt dispute types, such as partial balance, full balance, and account ownership. Users specify a dispute type when adding disputes. For more information, see Add a Dispute.

Add a Dispute Type

Use the **Dispute Type** panel to add a dispute type.

To add a dispute type

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Dispute Type**.



Code: Code that identifies the dispute type.

Proof Required: If selected, your organization requires proof of the dispute.

Description: Description of the dispute type.

Created When: Date and time a user created this dispute type.

Modified When: Date and time a user last modified this dispute type.

Created By: User who created this dispute type.

Modified By: User who last modified this dispute type.

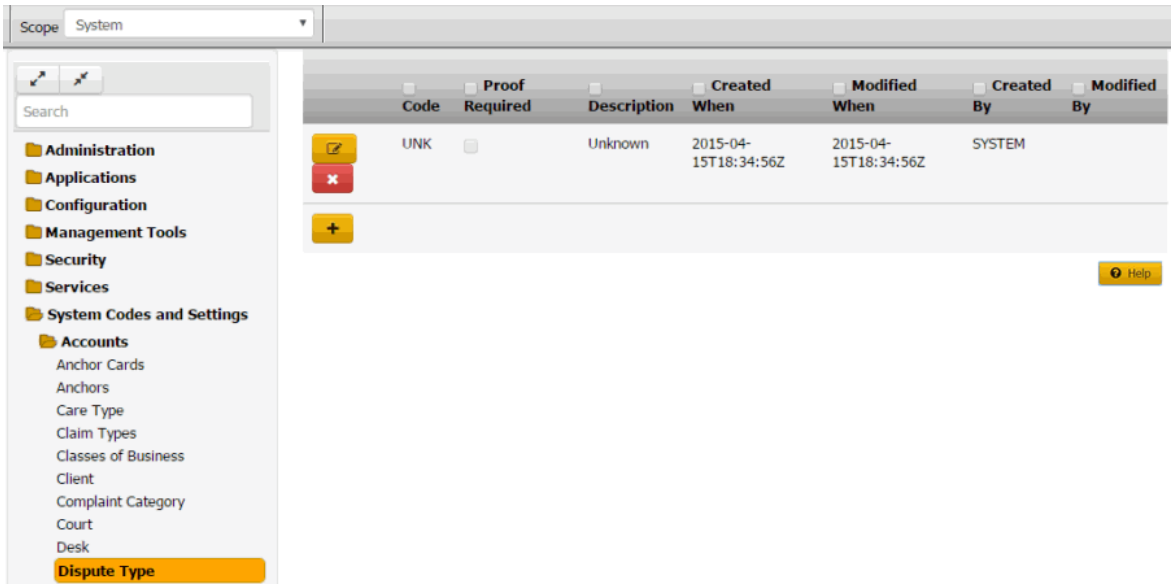
2. Click the plus sign (+). A blank row appears in the data grid.
3. Complete the information and then click the check mark.

Modify a Dispute Type

Use the **Dispute Type** panel to modify a dispute type.

To modify a dispute type

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Dispute Type**.



Code: Code that identifies the dispute type.

Proof Required: If selected, your organization requires proof of the dispute.

Description: Description of the dispute type.

Created When: Date and time a user created this dispute type.

Modified When: Date and time a user last modified this dispute type.

Created By: User who created this dispute type.

Modified By: User who last modified this dispute type.

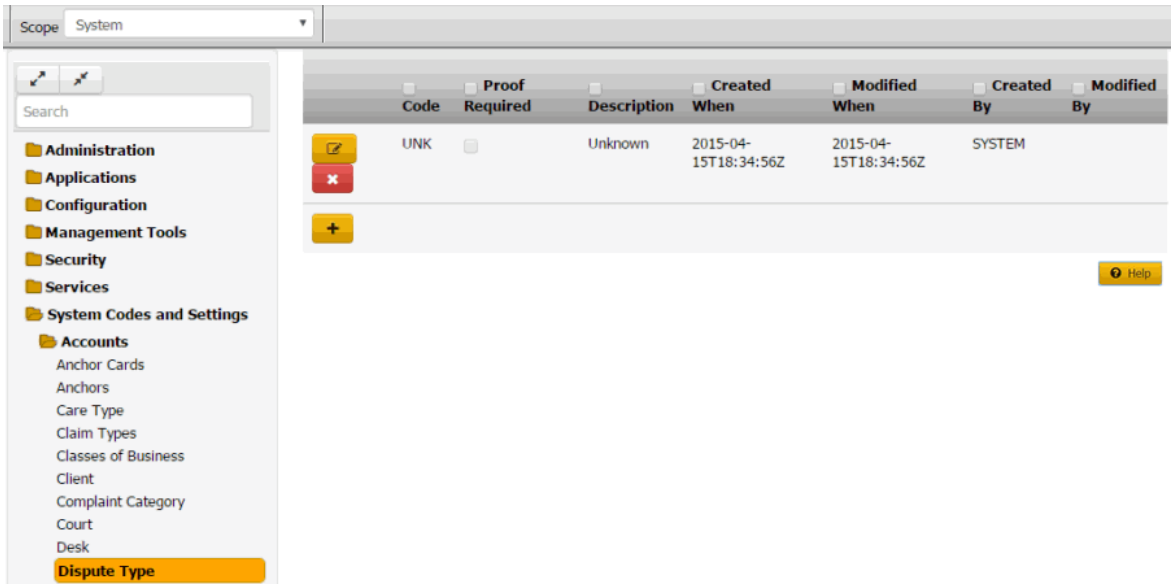
2. Click the Edit icon. The dispute type appears in edit mode.
3. Modify the information and then click the check mark.

Delete a Dispute Type

Use the **Dispute Type** panel to delete a dispute type.

To delete a dispute type

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Dispute Type**.



2. Click the Delete icon and then click **Yes**.

Documentation Categories

Documentation Categories

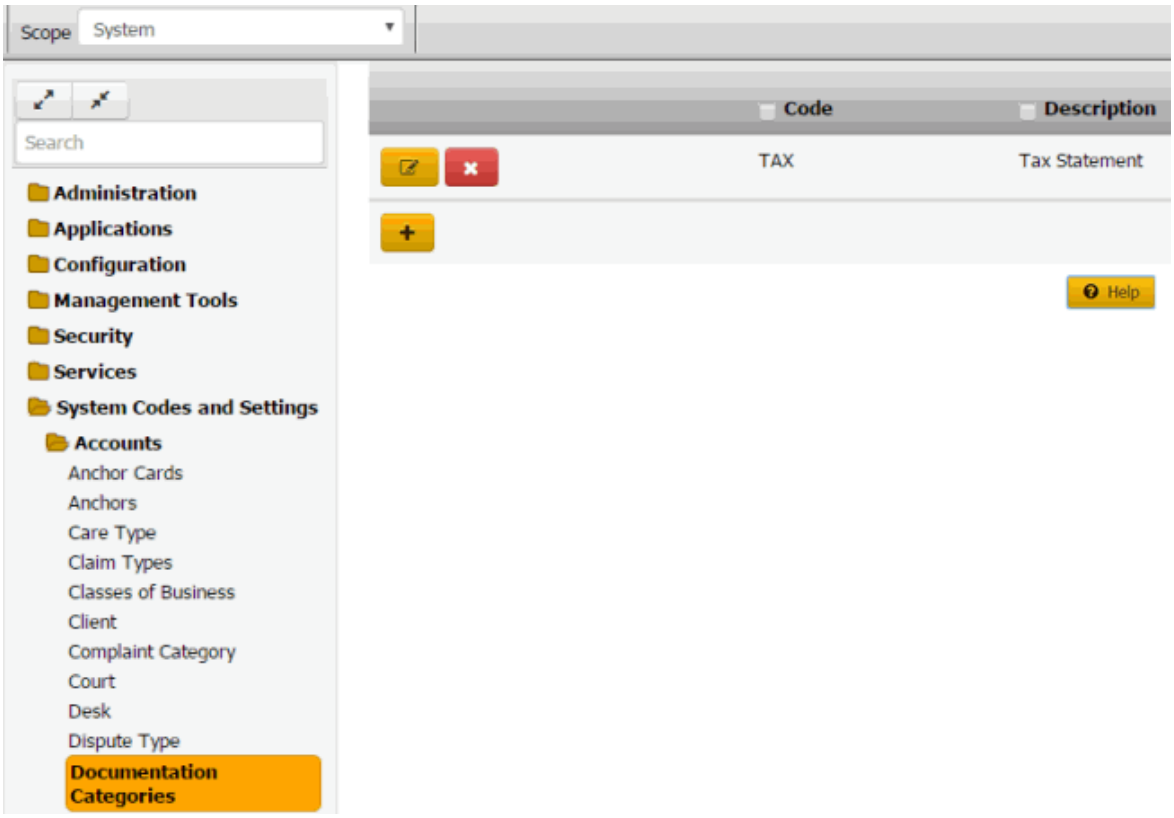
You can search for, add, modify, and delete documentation categories. Users specify a documentation category when attaching a document to an account. For more information, see Attach a Document to an Account.

Add a Documentation Category

Use the **Documentation Categories** panel to add a documentation category.

To add a documentation category

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Documentation Categories**.



2. Click the plus sign (+). A blank row appears in the data grid.

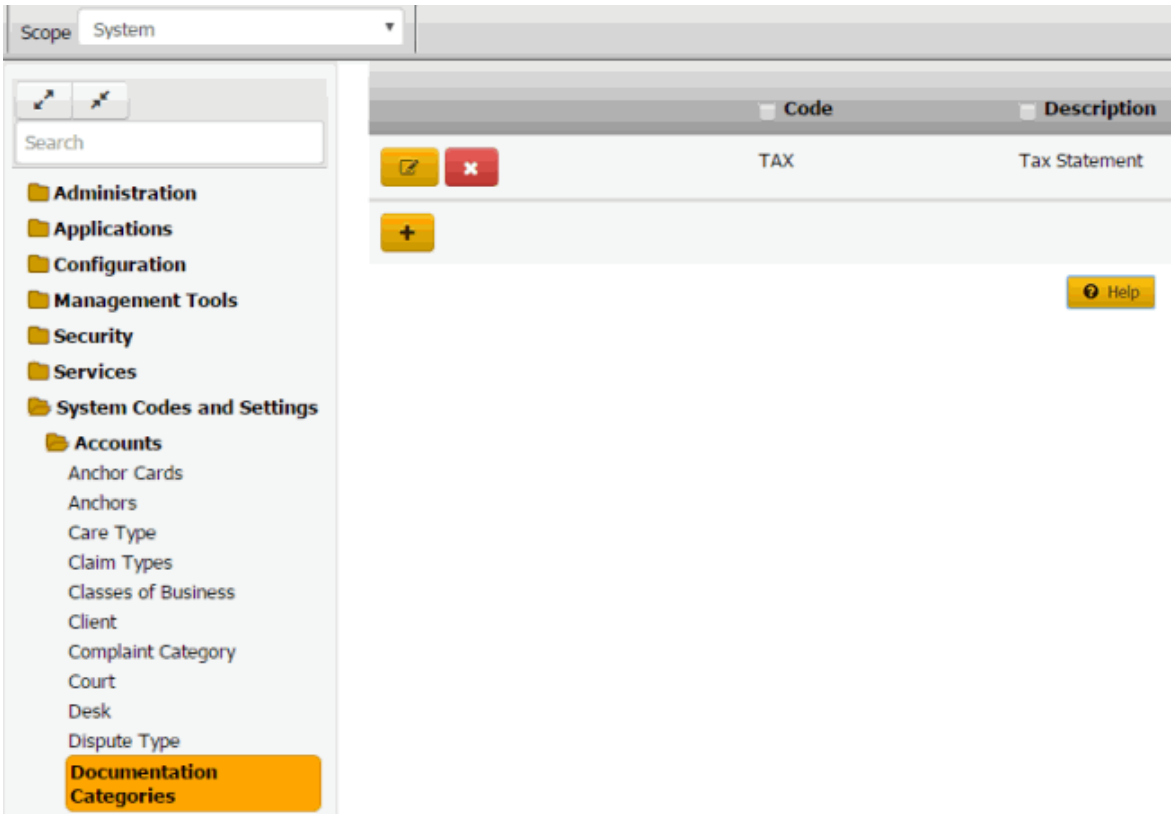
3. In the **Code** box, type a unique code for the documentation category.
4. In the **Description** box, type a description of the documentation category.
5. Click the check mark.

Modify a Documentation Category

Use the **Documentation Categories** panel to modify a documentation category.

To modify a documentation category

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Documentation Categories**.



2. Click the Edit icon. The documentation category appears in edit mode.

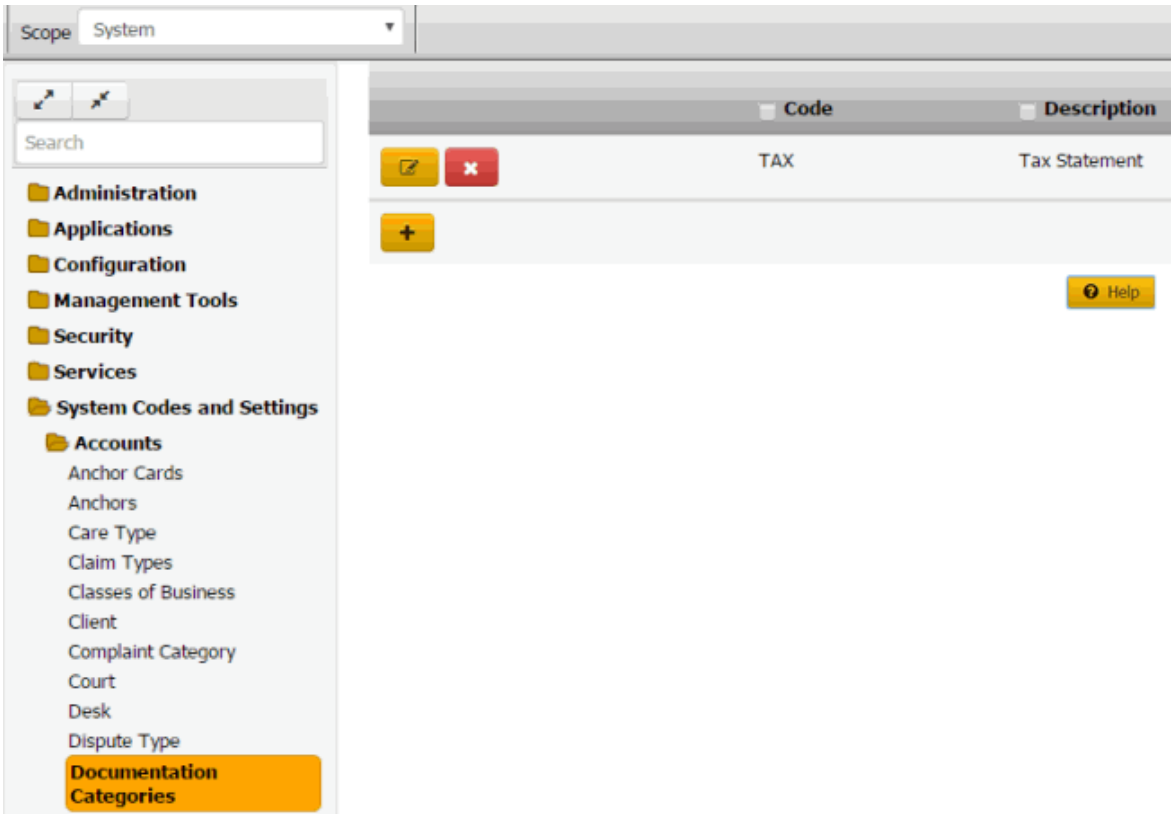
3. Modify the information and then click the check mark.

Delete a Documentation Category

Use the **Documentation Categories** panel to delete a documentation category.

To delete a documentation category

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Documentation Categories**.



2. Click the Delete icon and then click **Yes**.

Extra Data Codes

Extra Data Codes

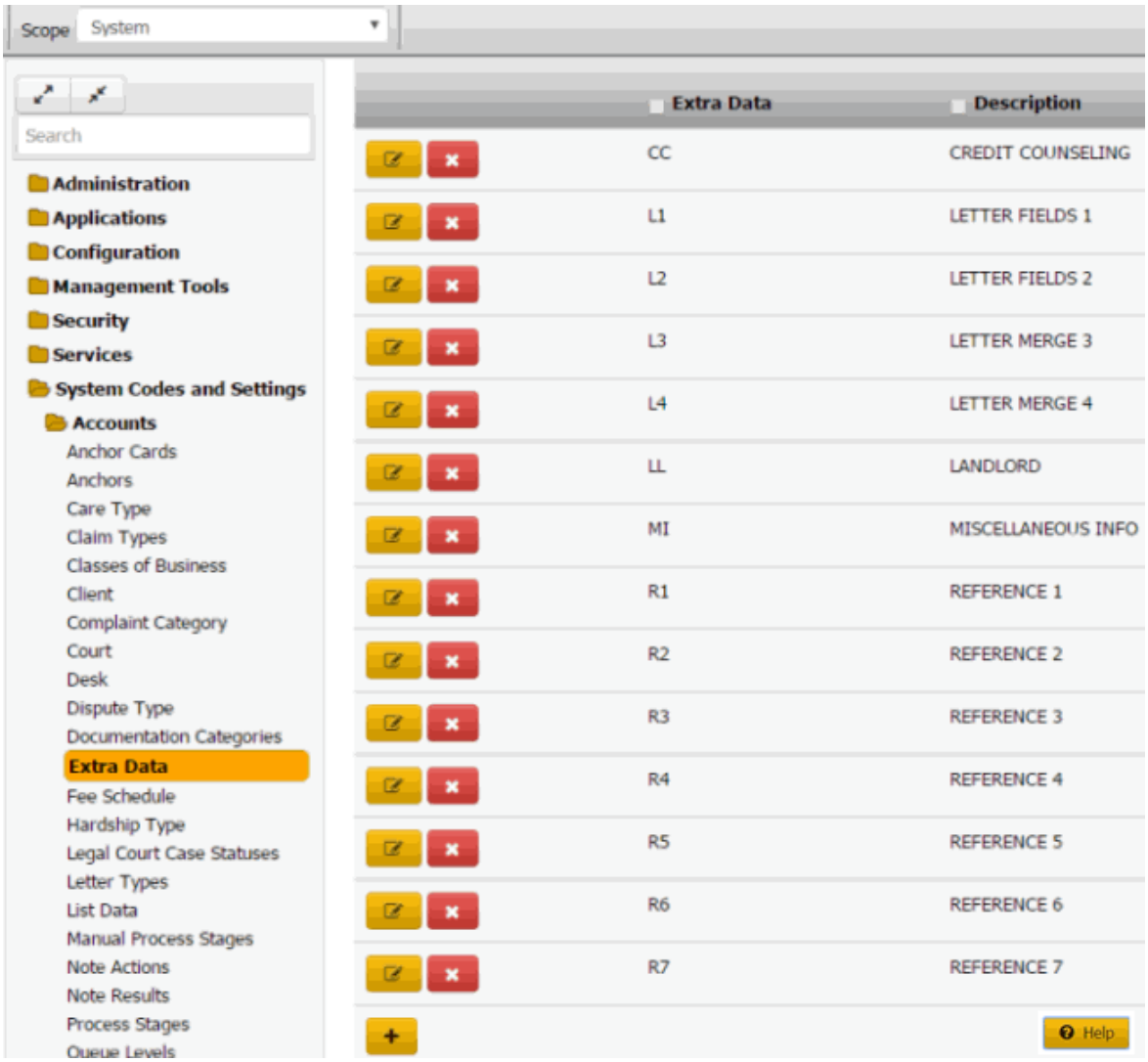
You can search for, add, modify, and delete extra data codes. Extra data codes allow your organization to create categories to assign to custom data that users create. Users specify an extra data code when adding extra data. For more information, see Extra Data.

Add an Extra Data Code

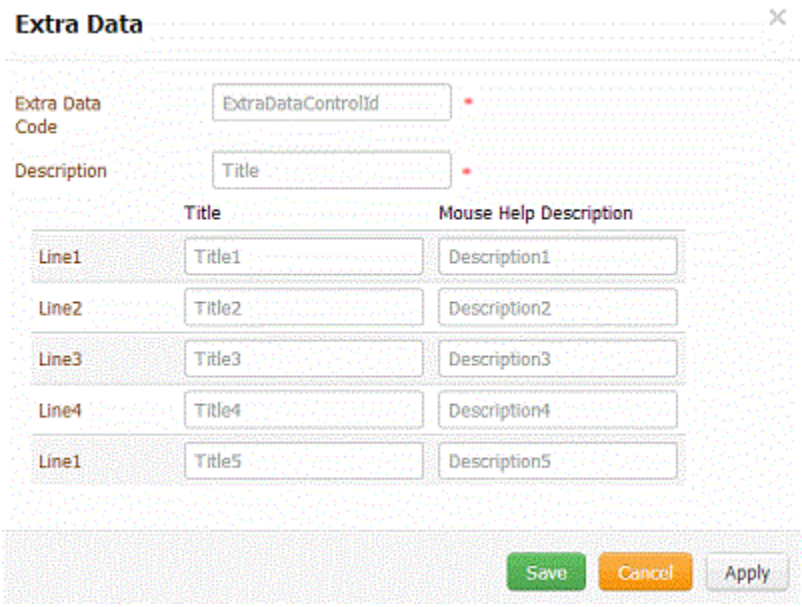
Use the **Extra Data** dialog box to add an extra data code.

To add an extra data code

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Extra Data**.



2. Click the plus sign (+). The **Extra Data** dialog box appears.



Extra Data Code: Unique two-character code that identifies the extra data.

Description: Description that appears next to the extra data code when a user is adding extra data to an account.

Title: Title for the information.

Mouse Help Description: Text to display when a user rests the mouse on the title.

Note: You can assign up to five lines of information to the code.

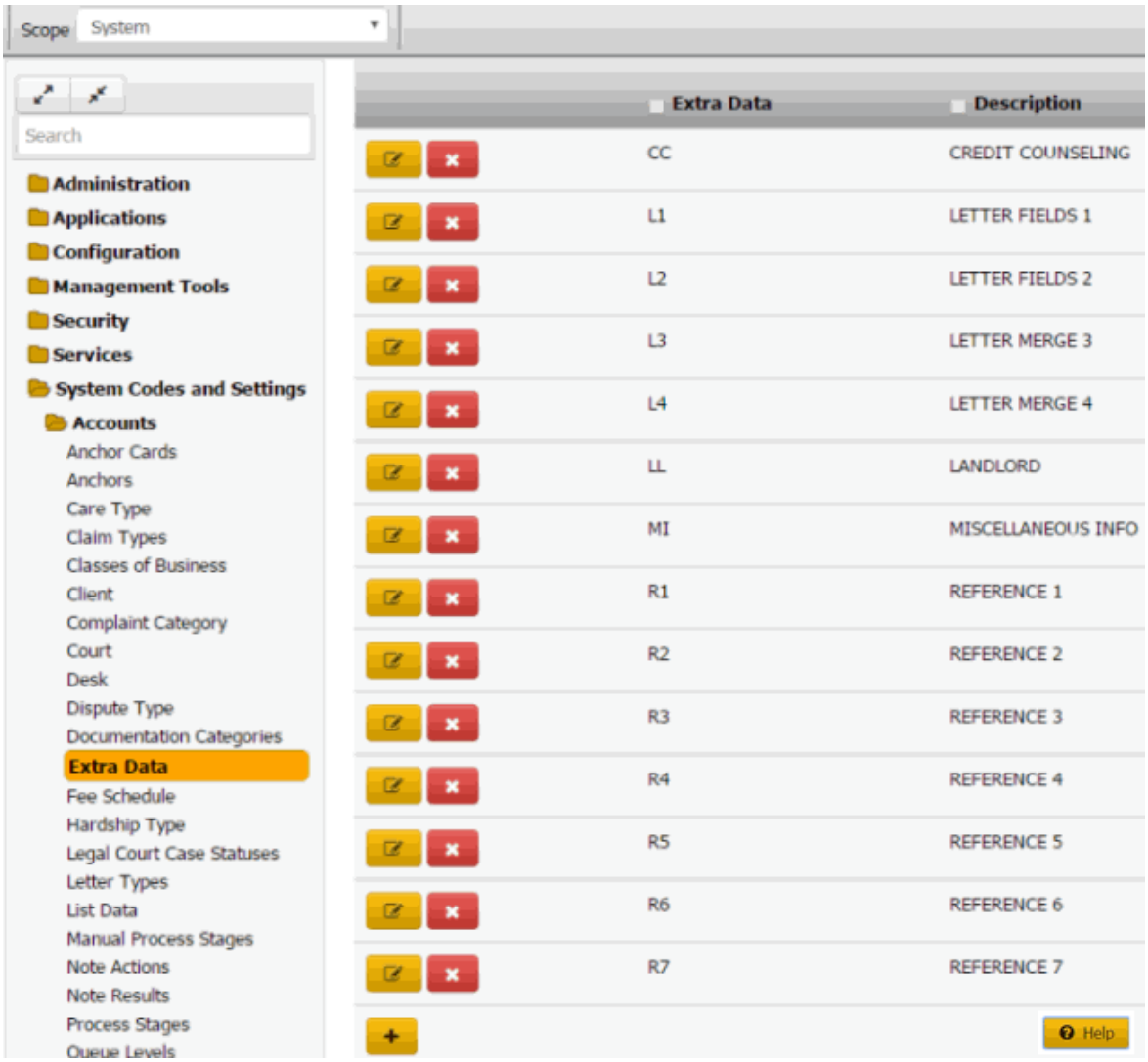
3. Complete the information and then click **Save**.

Modify an Extra Data Code

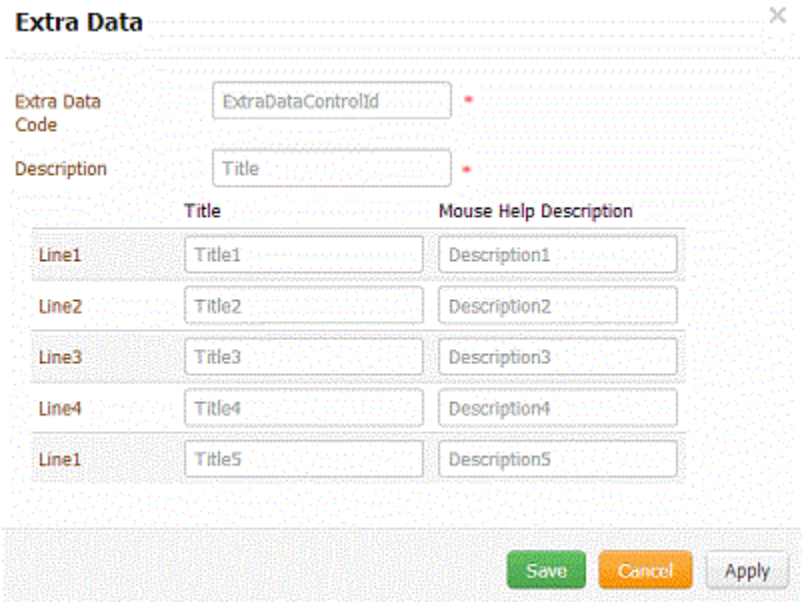
Use the **Extra Data** dialog box to modify an extra data code.

To modify an extra data code

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Extra Data**.



2. Click the plus sign (+). The **Extra Data** dialog box appears.



Extra Data Code: Unique two-character code that identifies the extra data.

Description: Description that appears next to the extra data code when a user is adding extra data to an account.

Title: Title for the information.

Mouse Help Description: Text to display when a user rests the mouse on the title.

Note: You can assign up to five lines of information to the code.

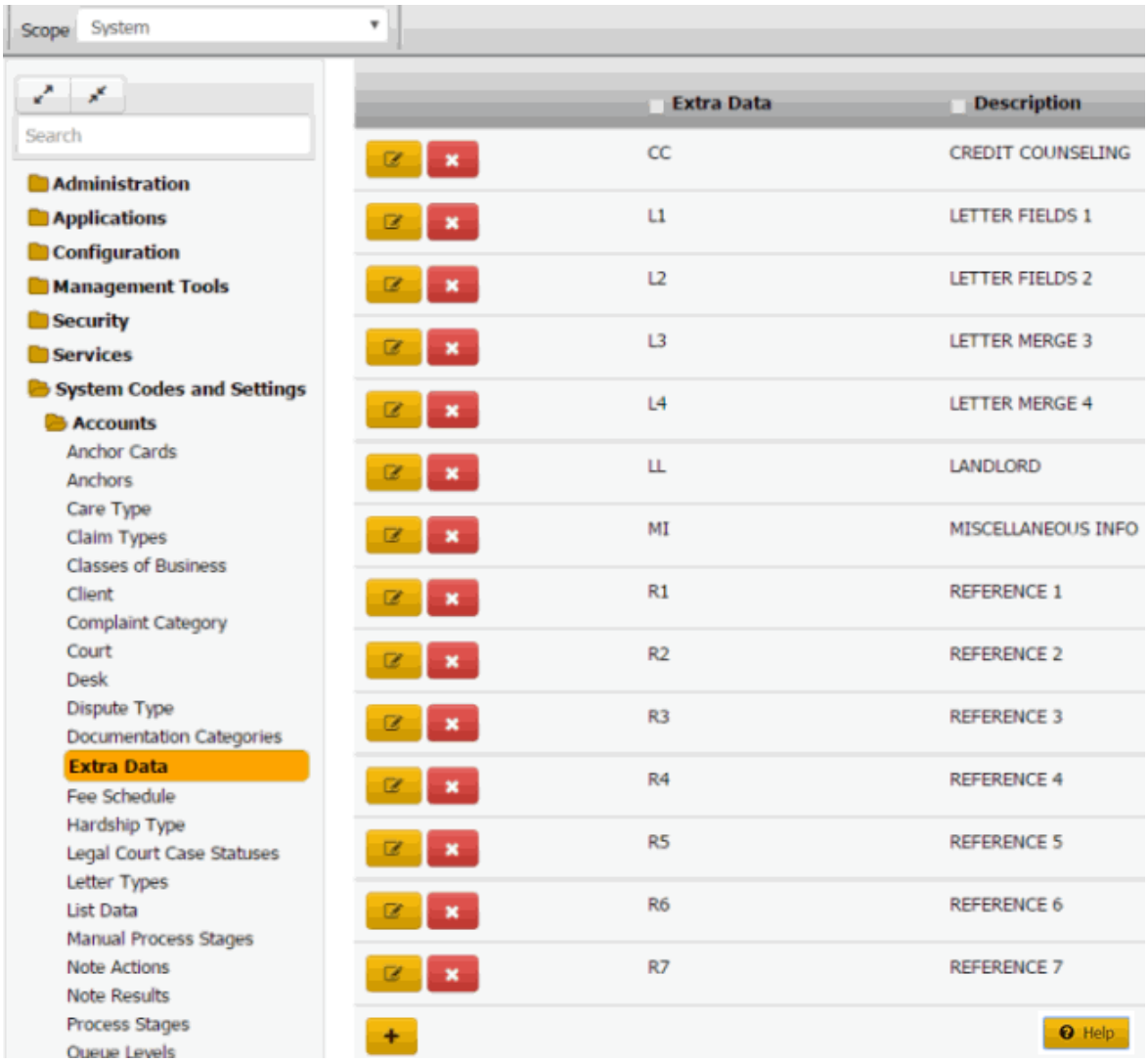
3. Modify the information and then click **Save**.

Delete an Extra Data Code

Use the **Extra Data** panel to delete an extra data code.

To delete an extra data code

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Extra Data**.



2. Click the Delete icon and then click **Yes**.

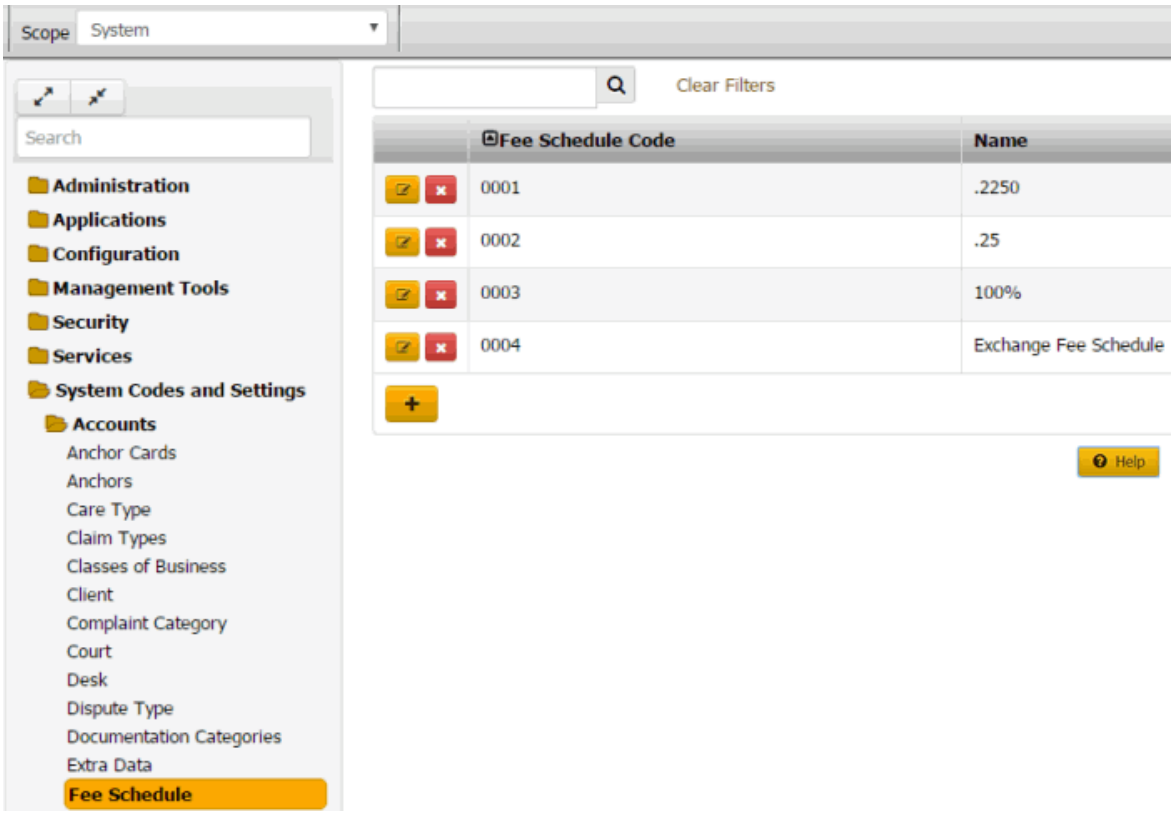
Fee Schedules

Search for a Fee Schedule

Use the **Fee Schedule** panel to search for a fee schedule.

To search for a fee schedule

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Fee Schedule**.



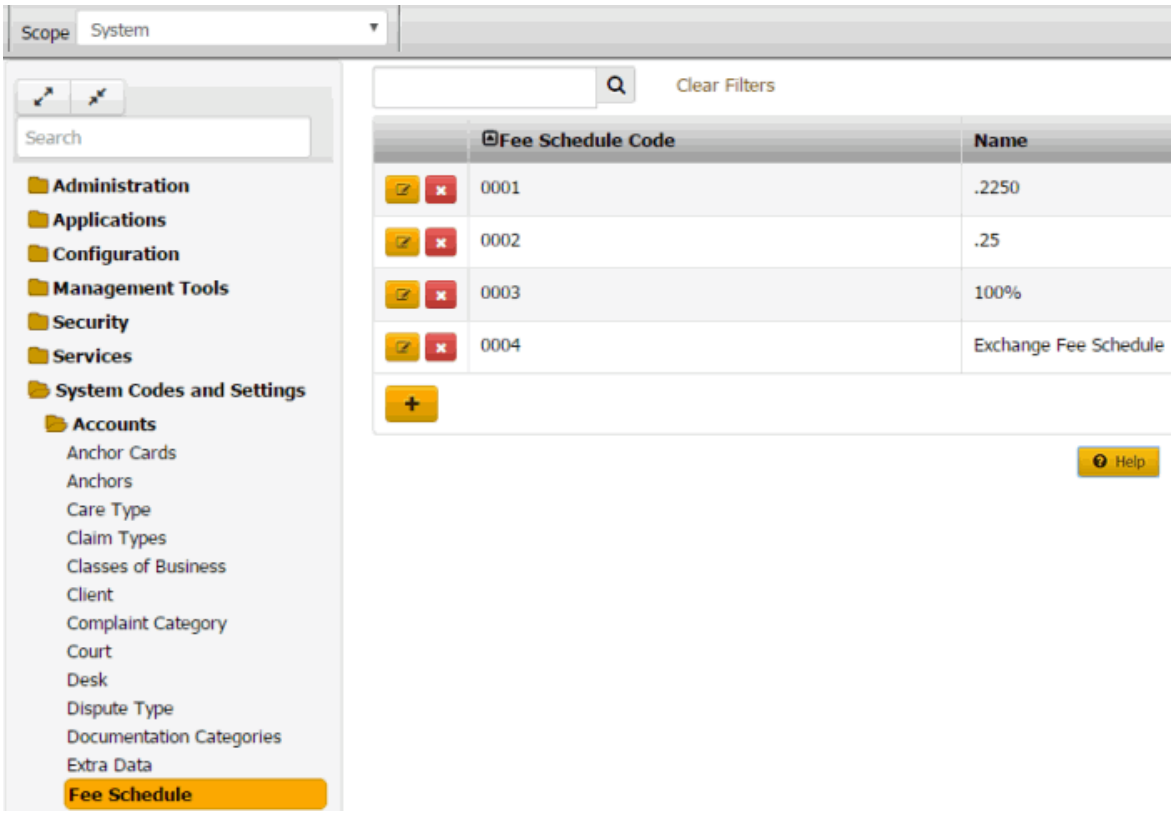
2. In the **Search** box in the **Fee Schedule** panel, type one or more characters to search and then press **Enter** or click the Search icon. The system searches the fee schedule code and name for a match. It displays only the fee schedules that match your search criteria.
3. To clear the search criteria, click **Clear Filters**. The system displays all fee schedules.

Add a Fee Schedule

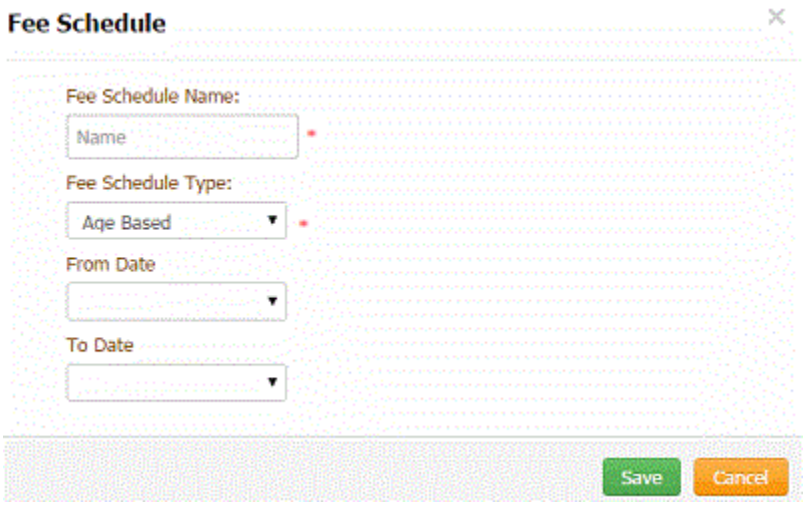
Use the **Fee Schedule** dialog box to add a fee schedule.

To add a fee schedule

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Fee Schedule**.



2. Click the plus sign (+). The **Fee Schedule** dialog box appears.



Fee Schedule Name: Description of the fee schedule.

Fee Schedule Type: Method for calculating fees.

From Date (available for age-based fee schedules only)

Received Date: Calculate fees starting on the account placement date.

Client DLP: Calculate fees starting on the date of the last payment to the client.

Client DLC: Calculate fees starting on the date of the last charge to the account.

Our DLP: Calculate fees starting on the date of the last payment to your organization.

[Blank]: Calculate fees starting from a user-defined date. These options represent the user-defined dates from your organization's control file.

To Date (available for age-based fee schedules only)

Entered Date: Calculate fees up to the payment entry date.

Received Date: Calculate fees up to the account placement date.

Client DLP: Calculate fees up to the date of the last payment to the client.

Client DLC: Calculate fees up to the date of the last charge to the account.

Our DLP: Calculate fees up to the date of the last payment to your organization.

[Blank]: Calculate fees up to the user-defined date. These options represent the user-defined dates from your organization's control file.

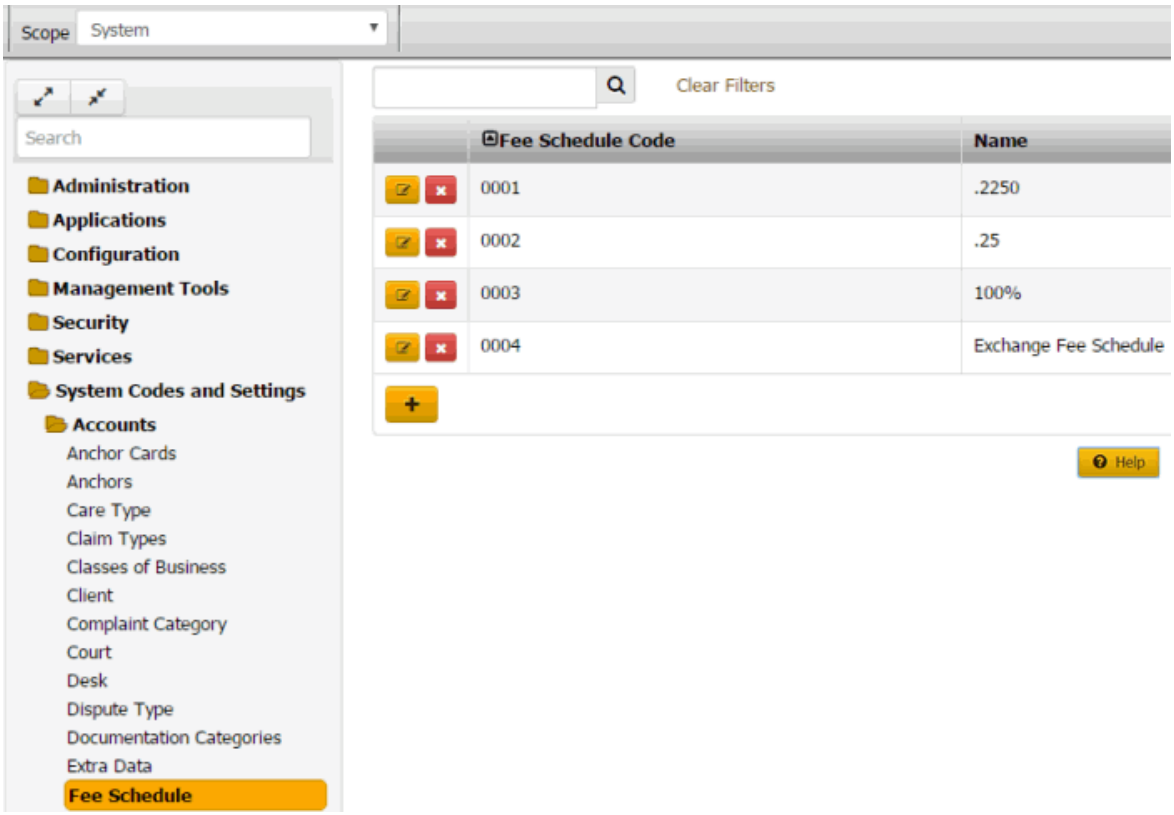
3. Complete the information and then click **Save**.

Modify an Age-Based Fee Schedule

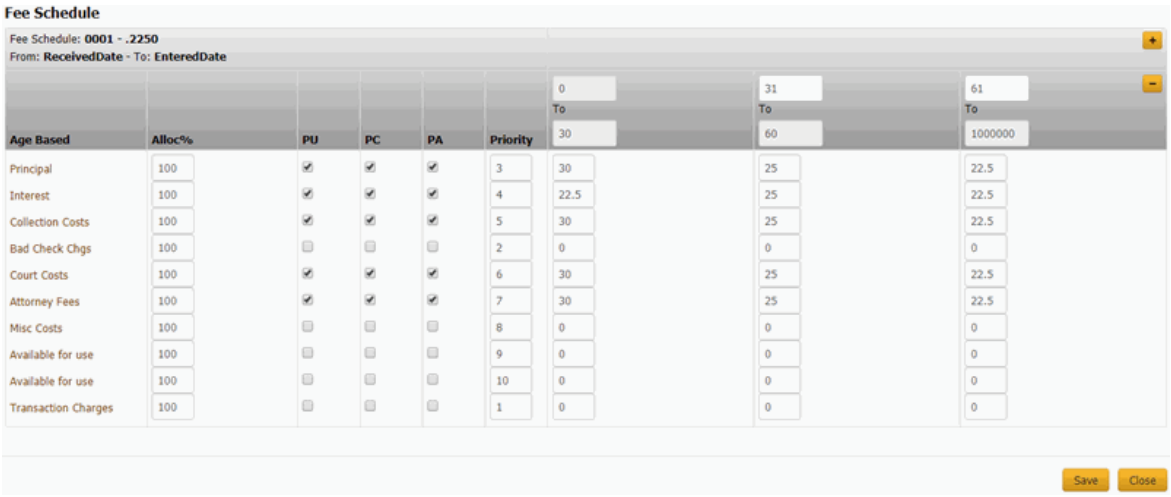
Use the **Fee Schedule** dialog box to modify an age-based fee schedule.

To modify an age-based fee schedule

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Fee Schedule**.



2. Click the Edit icon. The **Fee Schedule** dialog box appears.



Fee Schedule: Number and name that identifies the fee schedule.

From Date

Received Date: Calculate fees starting on the account placement date.

Client DLP: Calculate fees starting on the date of the last payment to the client.

Client DLC: Calculate fees starting on the date of the last charge to the account.

Our DLP: Calculate fees starting on the date of the last payment to your organization.

[Blank]: Calculate fees starting from a user-defined date. These options represent the user-defined dates from your organization's control file.

To Date

Entered Date: Calculate fees up to the payment entry date.

Received Date: Calculate fees up to the account placement date.

Client DLP: Calculate fees up to the date of the last payment to the client.

Client DLC: Calculate fees up to the date of the last charge to the account.

Our DLP: Calculate fees up to the date of the last payment to your organization.

[Blank]: Calculate fees up to the user-defined date. These options represent the user-defined dates from your organization's control file.

[Money Buckets]: Repositories for amounts you want to record in Latitude.

Alloc %: (Allocation percent) Percentage of the payment amount to allocate to the money bucket. The amount available to allocate toward a money bucket is the remaining payment amount to allocate times the money bucket's allocation rate. When Latitude allocates all the money buckets and an amount to pay remains, Latitude allocates the remaining amount based on priority. If the balance in a money bucket is less than the allocation amount, the remaining allocation amount becomes available to allocate to other money buckets with a lower priority.

PU: (Paid Us) If selected, client invoices include the amounts shown or paid into the money bucket for this payment type.

PC: (Paid Client) If selected, client invoices include the amounts shown or paid into the money bucket for this payment type.

PA: (Paid Agency) If selected, client invoices include the amounts shown or paid into the money bucket for this payment type.

Priority: Order in which to apply payments to the corresponding money bucket. Latitude applies payments to the money bucket with a priority of "1" first. If there are funds remaining, the system applies the payment to the bucket set as priority 2. The system continues applying the payment until no funds remain or the account balance is zero. If the account has a balance after applying the full payment amount received, the system applies the next payment you receive to the highest priority bucket that has a balance remaining. Generally, you order the priority from 1 to 10, from top to bottom.

To: Account balance range in which to apply fees. The first **To** column is always active, and indicates the first (or only) account balance range to use for the specified fee. For example, if you set the fee code to apply for balances from $0 to $999.99, this fee is the only one applied to the account. You may want to accept the default, which is $0 to $100000000 (so as not to activate any other fee schedule columns).

[Percent]: Percentage to set as the fee for each money bucket for the specified account balance range. For example, if you type an amount of "25," all payments applied toward the Principal bucket generate a fee of 25 percent of the money collected.

3. In the **Alloc %** column, specify the percentage of the payment amount to allocate to each money bucket.
4. In the **PU**, **PC**, and **PA** column, select or clear the check boxes to indicate whether to include these payment types on client invoices.

> **Note:** If you don't select at least one of these check boxes, the system displays a warning message. To continue without selecting a check box, click **OK**.

5. In the **Priority** column, specify the order in which to apply payments.
6. In the **To** column, do the following:

a. Specify the beginning and ending account balance range in which to apply fees.

b. Specify the percent to calculate as the fee for each money bucket.

7. To set up subsequent account balance ranges, do the following:

. Click the plus sign (**+**). The system inserts a column.

a. Type the next account balance range to use for applying fees.

b. Specify the percent to calculate as the fee for each money bucket.

> **Tip:** To delete a "To" column, click the minus sign (**-**).

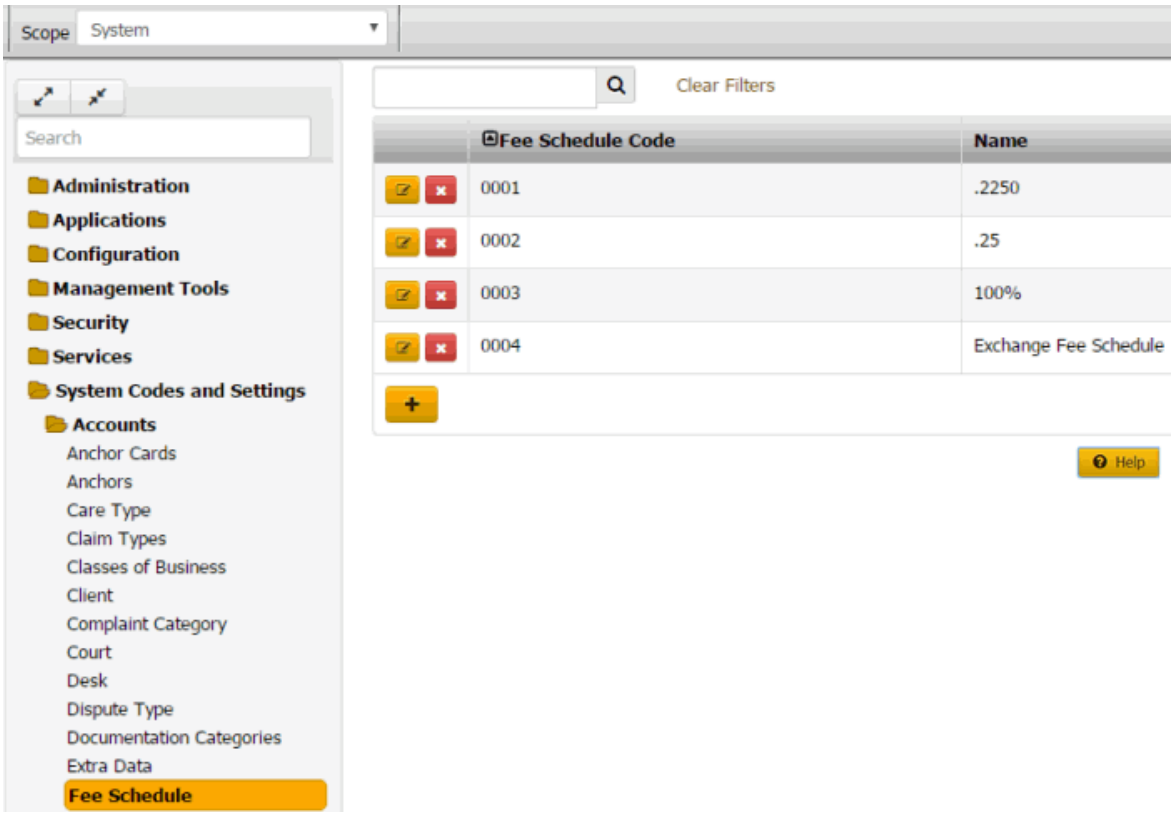
8. Click **Save**.

Modify a Balance-Based Fee Schedule

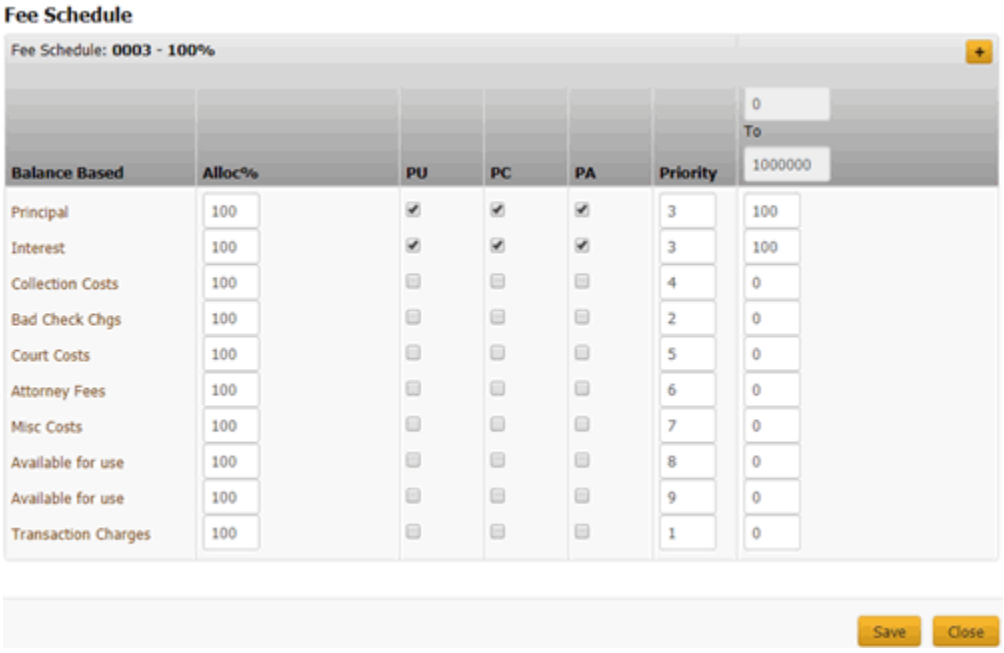
Use the **Fee Schedule** dialog box to modify a balance-based fee schedule.

To modify a balance-based fee schedule

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Fee Schedule**.



2. Click the Edit icon. The **Fee Schedule** dialog box appears.



Fee Schedule Code/Name: Number and name that identifies the fee schedule.

[Money Buckets]: Repositories for amounts you want to record in Latitude.

Alloc %: (Allocation percent) Percentage of the payment amount to allocate to the money bucket. The amount available to allocate toward a money bucket is the remaining payment amount to allocate times the money bucket's allocation rate. When Latitude allocates all the money buckets and an amount to pay remains, Latitude allocates the remaining amount based on priority. If the balance in a money bucket is less than the allocation amount, the remaining allocation amount becomes available to allocate to other money buckets with a lower priority.

PU: (Paid Us) If selected, client invoices include the amounts shown or paid into the money bucket for this payment type.

PC: (Paid Client) If selected, client invoices include the amounts shown or paid into the money bucket for this payment type.

PA: (Paid Agency) If selected, client invoices include the amounts shown or paid into the money bucket for this payment type.

Priority: Order in which to apply payments to the corresponding money bucket. Latitude applies payments to the money bucket with a priority of "1" first. If there are funds remaining, the system applies the payment to the bucket set as priority 2. The system continues applying the payment until no funds remain or the account balance is zero. If the account has a balance after applying the full payment amount received, the system applies the next payment you receive to the highest priority bucket that has a balance remaining. Generally, you order the priority from 1 to 10, from top to bottom.

To: Account balance range in which to apply fees. The first **To** column is always active, and indicates the first (or only) account balance range to use for the specified fee. For example, if you set the fee code to apply for balances from $0 to $999.99, this fee is the only one applied to the account. You may want to accept the default, which is $0 to $100000000 (so as not to activate any other fee schedule columns).

[Percent]: Percentage to set as the fee for each money bucket for the specified account balance range. For example, if you type an amount of "25," all payments applied toward the Principal bucket generate a fee of 25 percent of the money collected.

3. In the **Alloc %** column, specify the percentage of the payment amount to allocate to each money bucket.
4. In the **PU**, **PC**, and **PA** column, select or clear the check boxes to indicate whether to include these payment types on client invoices.

> **Note:** If you don't select at least one of these check boxes, the system displays a warning message. To continue without selecting a check box, click **OK**.

5. In the **Priority** column, specify the order in which to apply payments.
6. In the **To** column, do the following:

a. Specify the beginning and ending account balance range in which to apply fees.

b. Specify the percent to calculate as the fee for each money bucket.

7. To set up subsequent account balance ranges, do the following:

. Click the plus sign (**+**). The system inserts a column.

a. Type the next account balance range to use for applying fees.

b. Specify the percent to calculate as the fee for each money bucket.

> **Tip:** To delete a "To" column, click the minus sign (-).

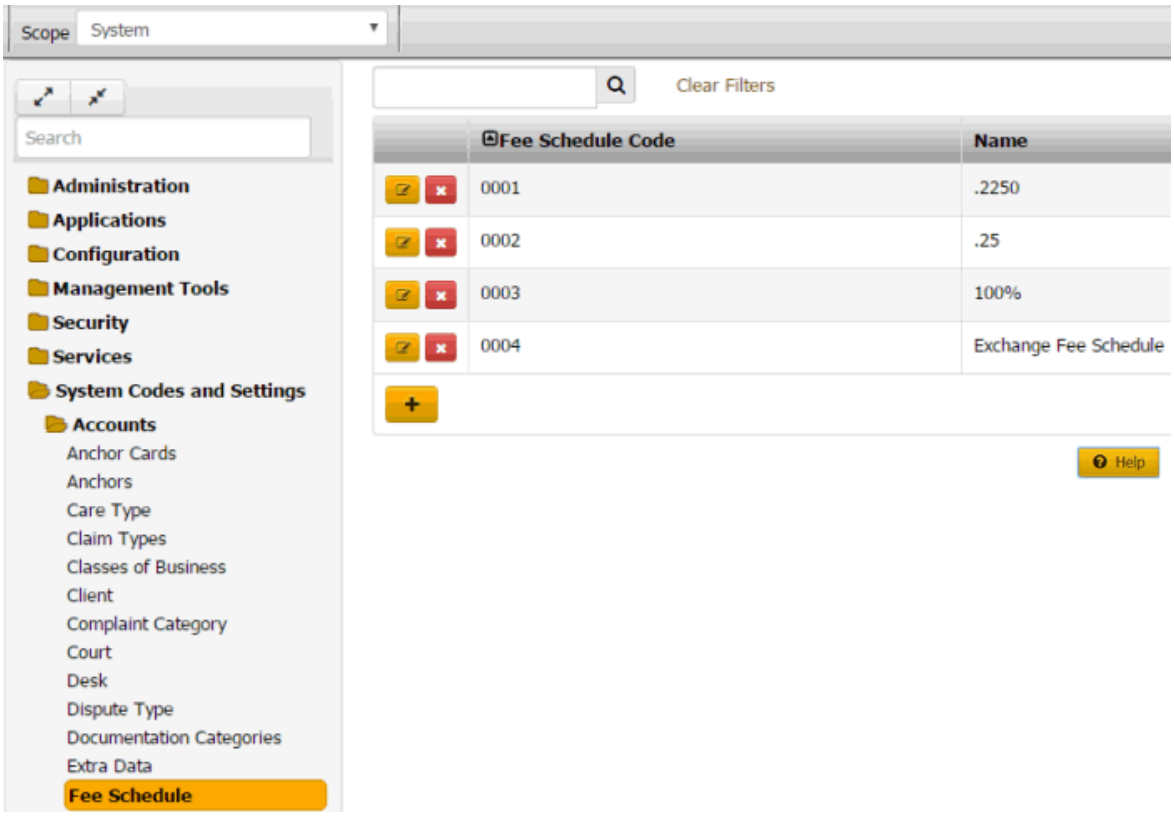
8. Click **Save**.

Delete a Fee Schedule

Use the **Fee Schedule** tab to delete a fee schedule.

To delete a fee schedule

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Fee Schedule**.



2. Click the Delete icon and then click **Yes**.

Hardship Types

Hardship Types

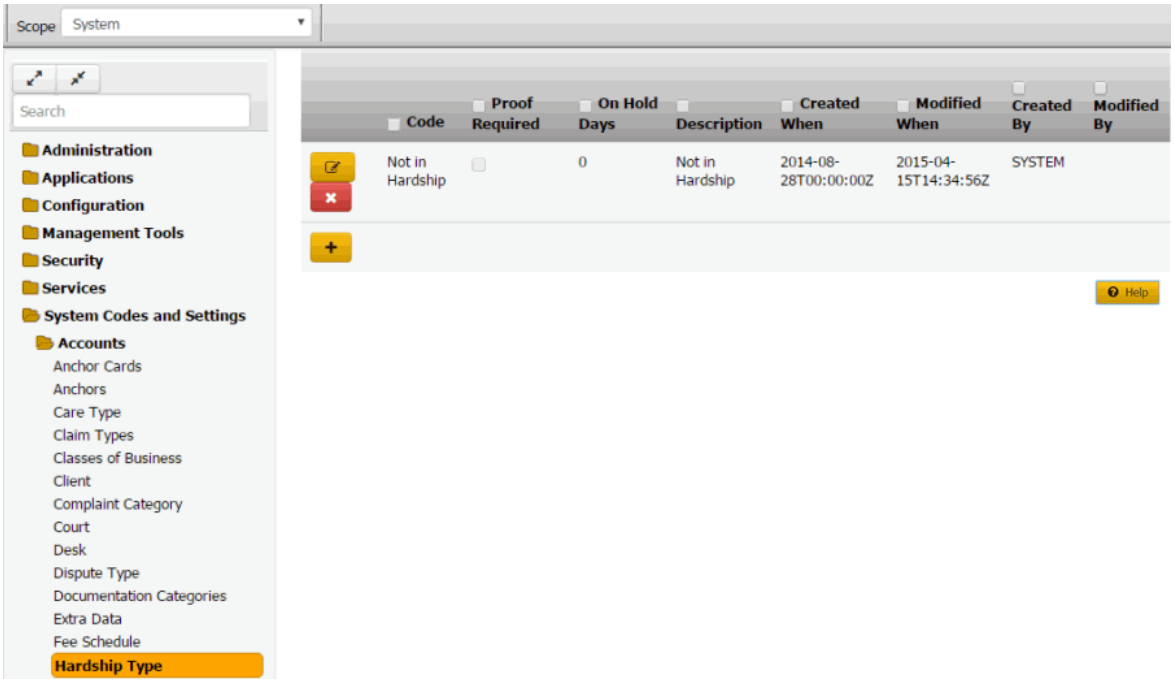
You can add, modify, and delete financial hardship types, such as unemployment, short-term illness, and reduced income. Users specify a hardship type when creating financial hardship cases. For more information, see Add a Care or Financial Hardship Case.

Add a Hardship Type

Use the **Hardship Type** panel to add a financial hardship type.

To add a hardship type

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Hardship Type**.



   Code: Code that identifies the type of financial hardship.

   Proof Required: If selected, your organization requires proof of the financial hardship.

   On Hold Days: Default number of days to place the account on hold to suspend collection activity.

   Description: Description of the hardship type.

   Created When: Date and time a user created this hardship type.

   Modified When: Date and time a user last modified this hardship type.

   Created By: User who created this hardship type.

   Modified By: User who last modified this hardship type.

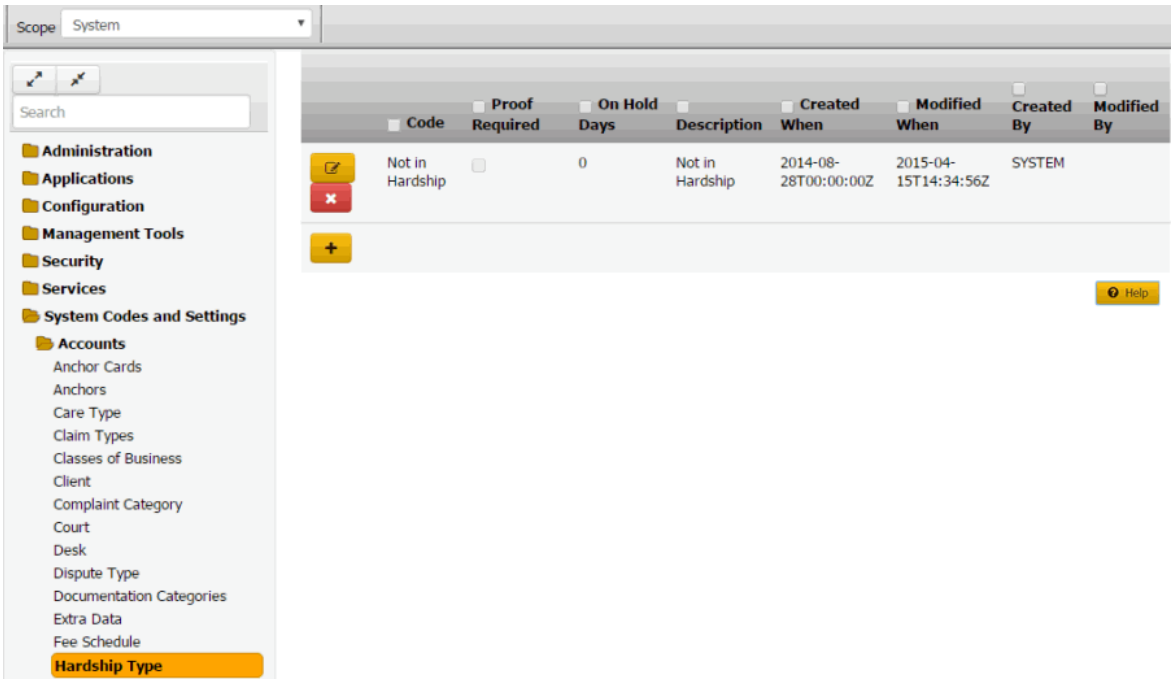
2. Click the plus sign (+). A blank row appears in the data grid.
3. Complete the information and then click the check mark.

Modify a Hardship Type

Use the **Hardship Type** panel to modify a financial hardship type.

To modify a hardship type

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Hardship Type**.



Code: Code that identifies the type of financial hardship.

Proof Required: If selected, your organization requires proof of the financial hardship.

On Hold Days: Default number of days to place the account on hold to suspend collection activity.

Description: Description of the hardship type.

Created When: Date and time a user created this hardship type.

Modified When: Date and time a user last modified this hardship type.

Created By: User who created this hardship type.

Modified By: User who last modified this hardship type.

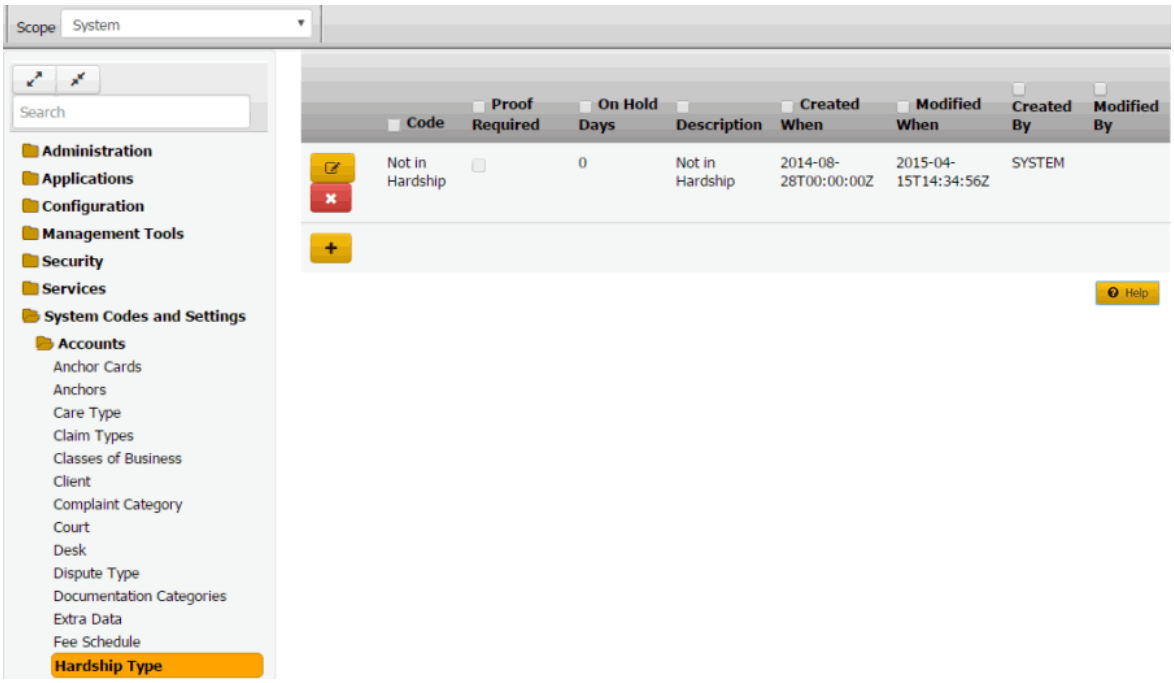
2. Click the Edit icon. The hardship type appears in edit mode.
3. Modify the information and then click the check mark.

Delete a Hardship Type

Use the **Hardship Type** panel to delete a financial hardship type.

To delete a hardship type

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Hardship Type**.



2. Click the Delete icon and then click **Yes**.

Legal Court Case Statuses

Legal Court Case Statuses

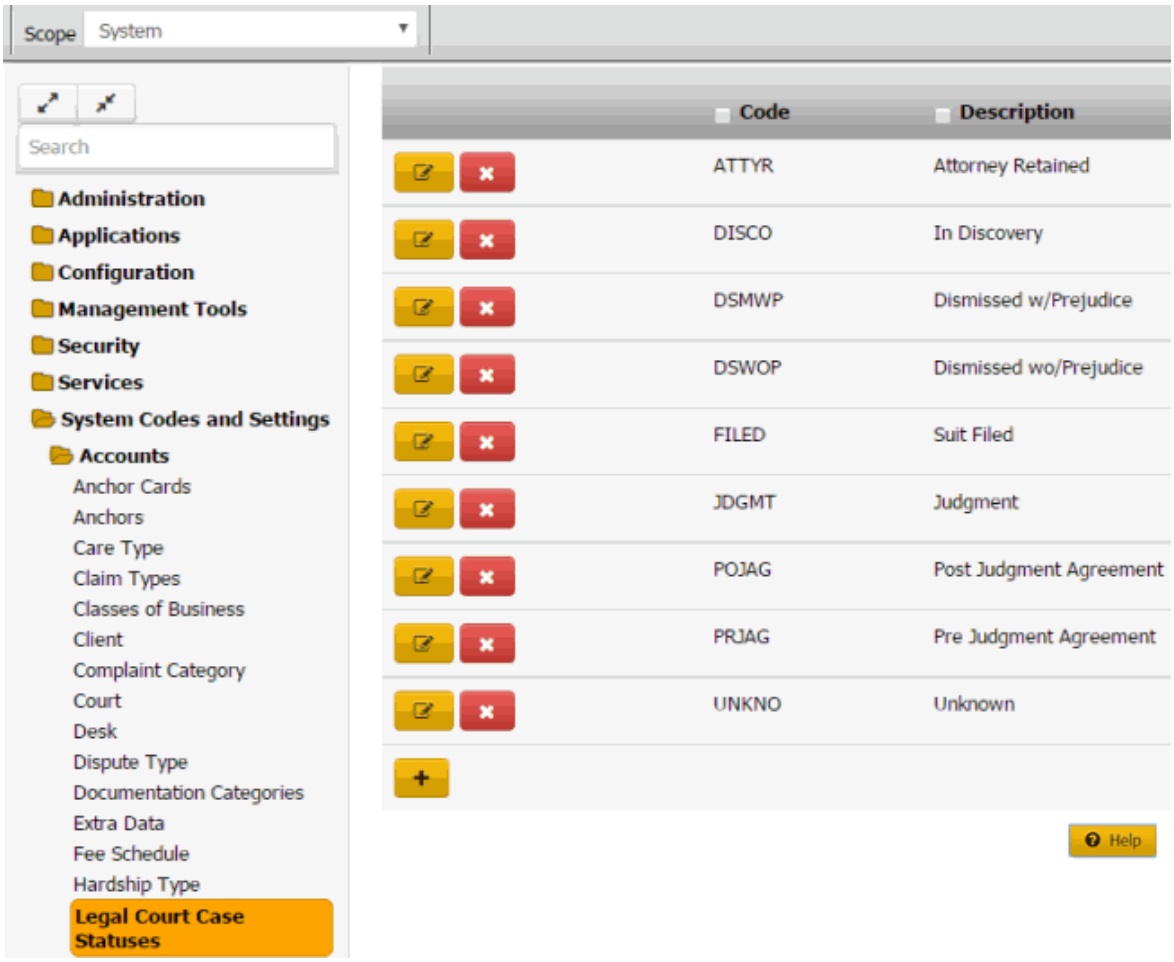
You can search for, add, modify, and delete court case statuses. Users specify a court case status when creating or maintaining legal cases. For more information, see Maintain General Legal Information.

Add a Court Case Status

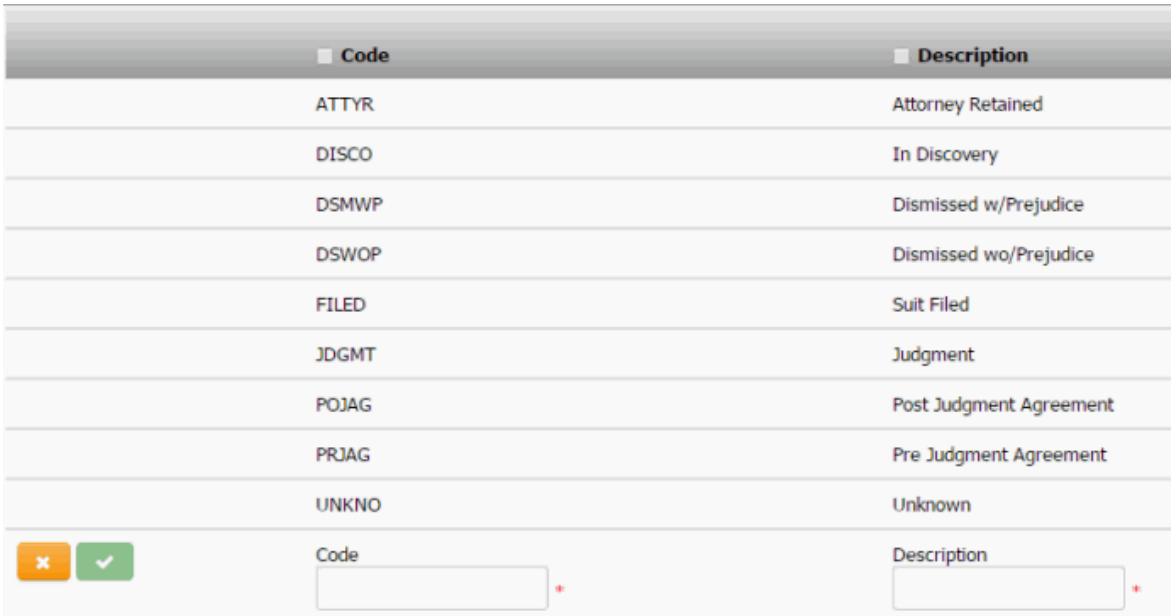
Use the **Legal Court Case Statuses** panel to add a court case status.

To add a court case status

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Legal Court Case Statuses**.



2. Click the plus sign (+). A blank row appears in the data grid.



3. In the **Code** box, type a unique code for the court case status.

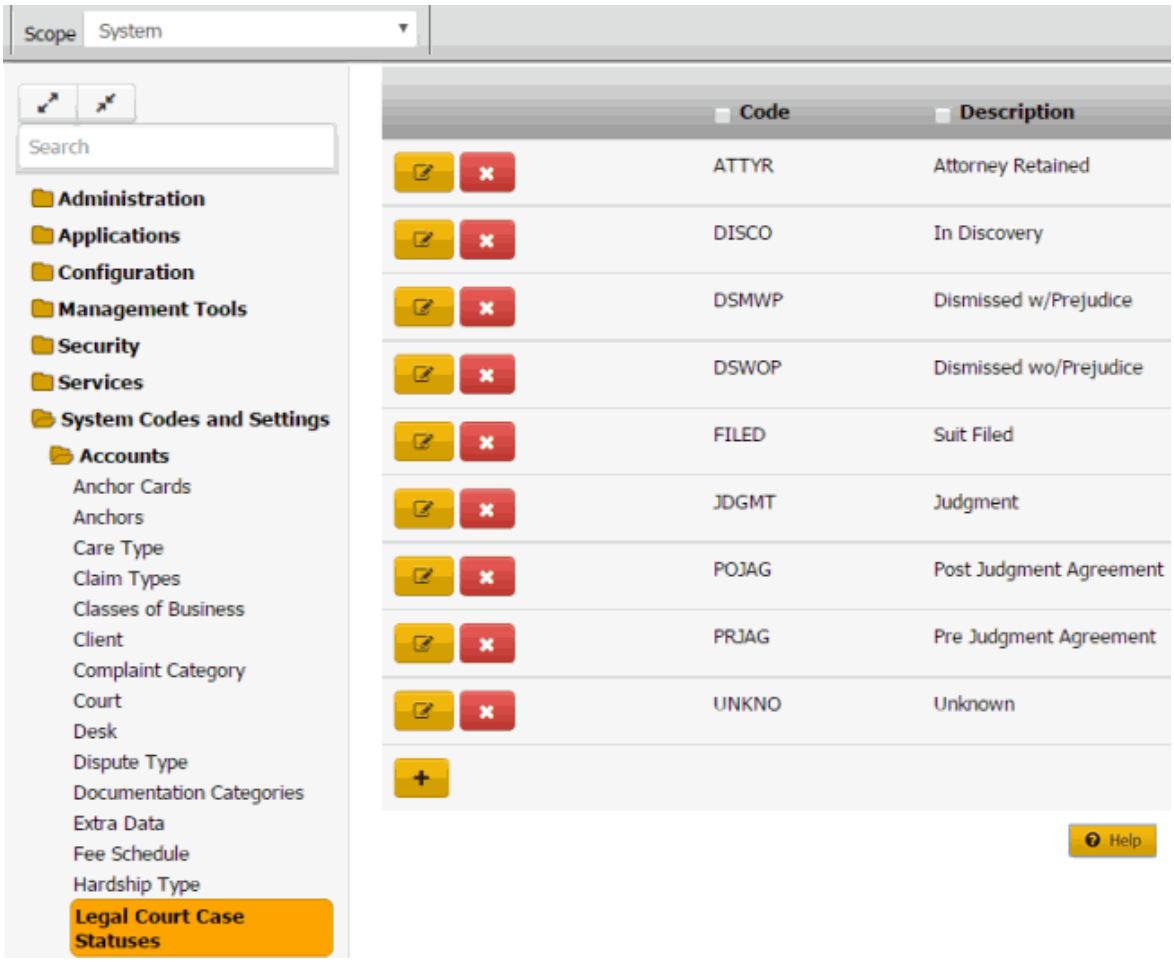
4. In the **Description** box, type a description of the court case status.
5. Click the check mark.

Modify a Court Case Status

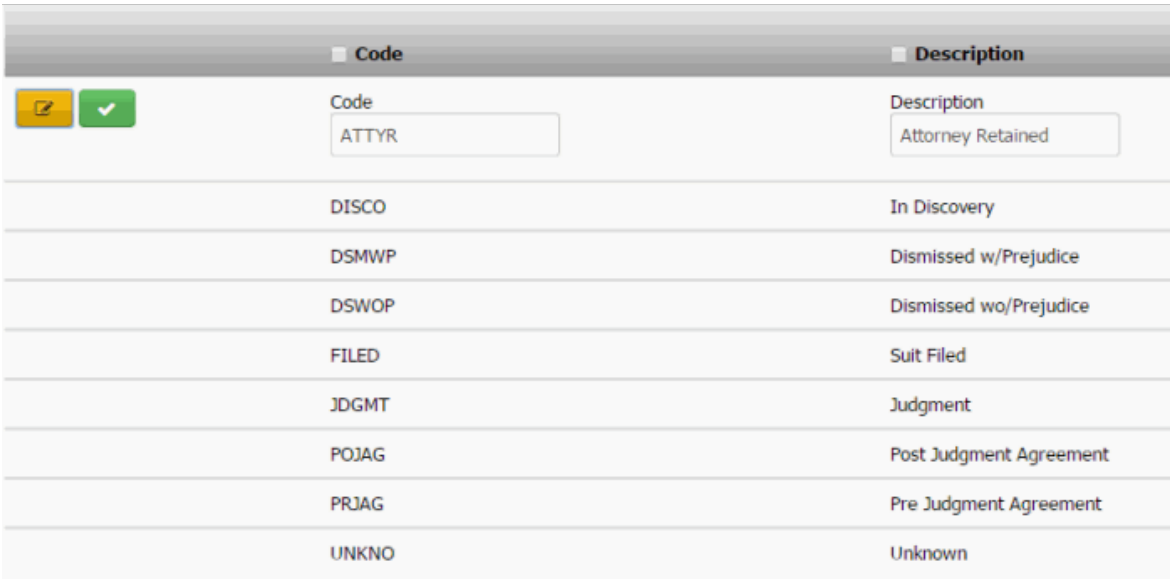
Use the **Legal Court Case Statuses** panel to modify a court case status.

To modify a court case status

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Legal Court Case Statuses**.



2. Click the Edit icon. The court case status appears in edit mode.



	Code	Description
	Code ATTYR	Description Attorney Retained
	DISCO	In Discovery
	DSMWP	Dismissed w/Prejudice
	DSWOP	Dismissed wo/Prejudice
	FILED	Suit Filed
	JDGMT	Judgment
	POJAG	Post Judgment Agreement
	PRJAG	Pre Judgment Agreement
	UNKNO	Unknown

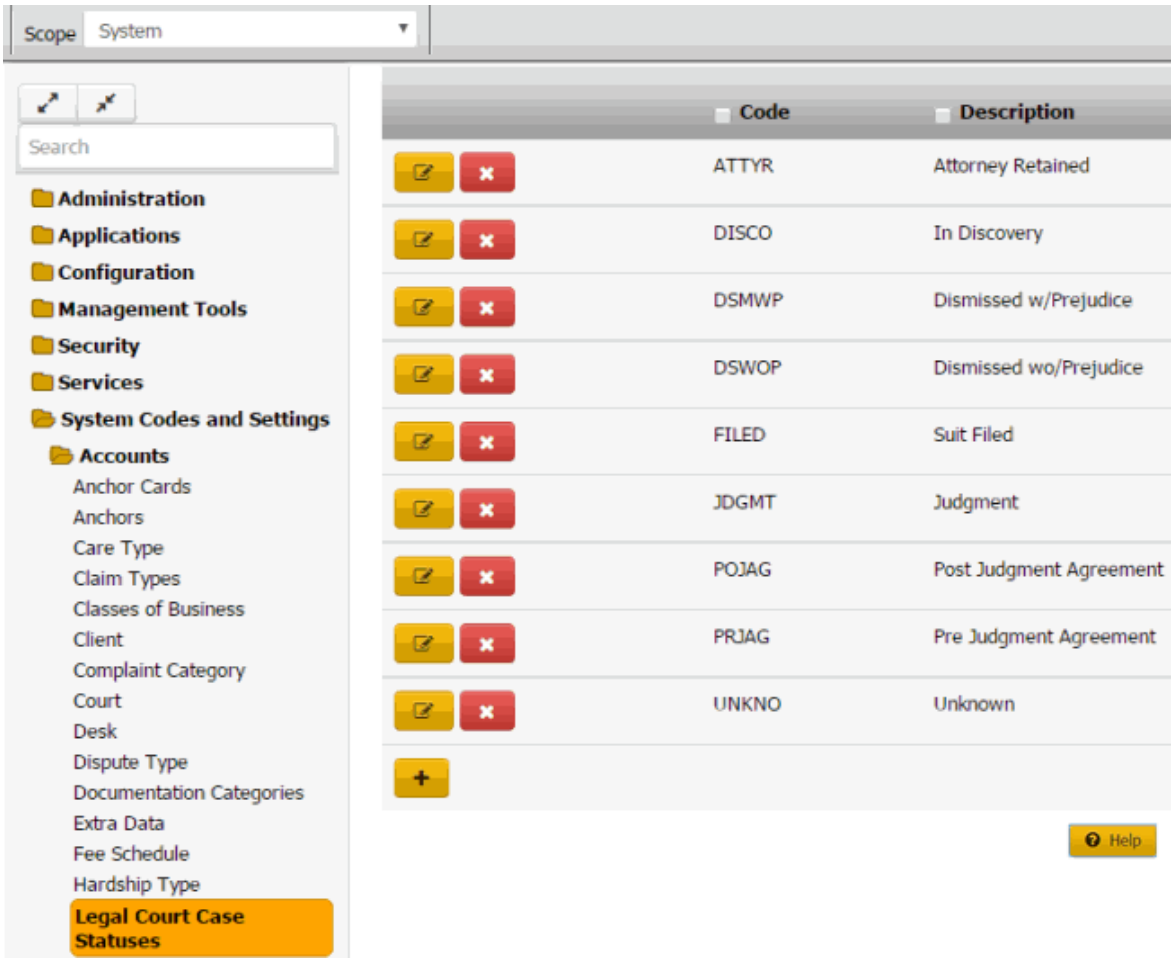
3. Modify the information and then click the check mark.

Delete a Court Case Status

Use the **Legal Court Case Statuses** panel to delete a court case status.

To delete a court case status

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Legal Court Case Statuses**.



2. Click the Delete icon and then click **Yes**.

Letter Types

Letter Types

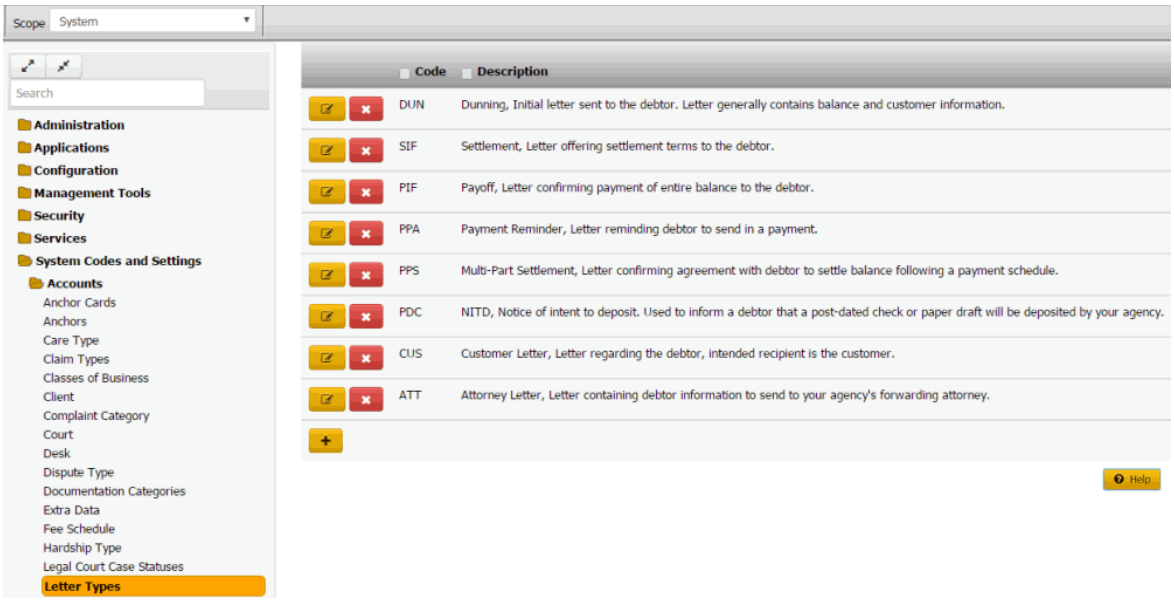
You can search for, add, modify, and delete letter types. User-defined letters have no functionality associated to them and Latitude cannot determine what type of letter it is. If you need specific functionality associated to a letter, use a system-defined letter. For example, if you want to send a settlement letter, use the system-defined settlement letter.

Add a Letter Type

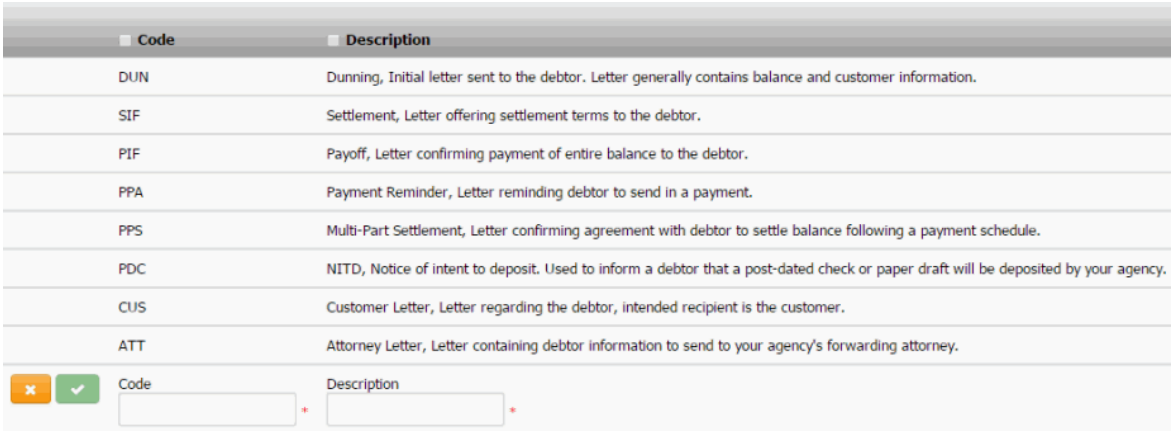
Use the **Letter Types** panel to add a letter type.

To add a letter type

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Letter Types**.



2. Click the plus sign (+). A blank row appears in the data grid.



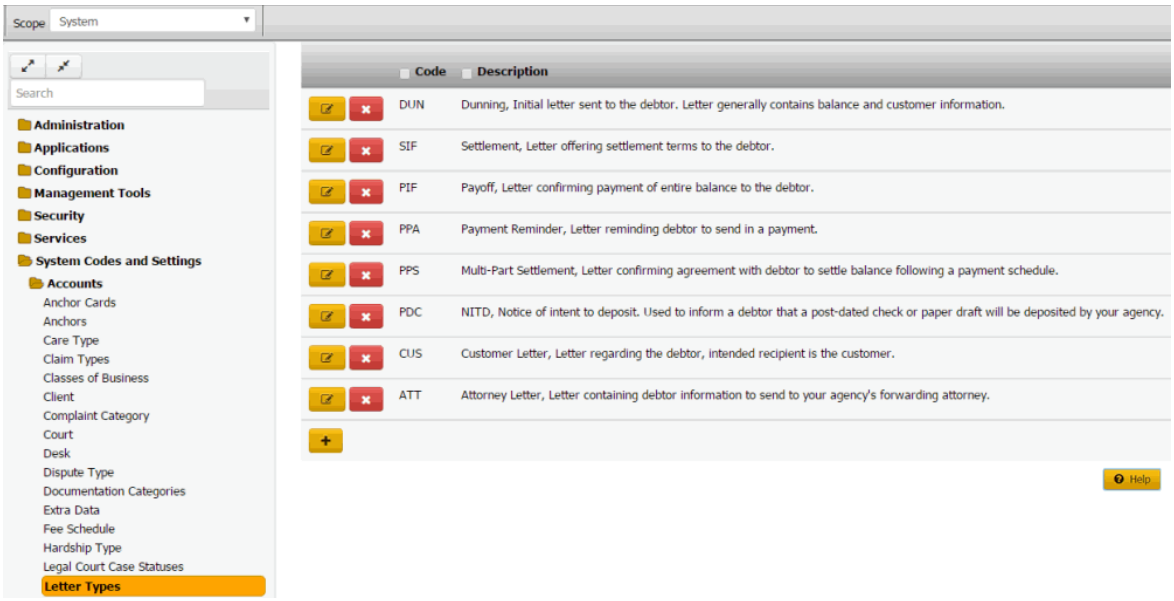
3. Complete the information and then click the check mark.

Modify a Letter Type

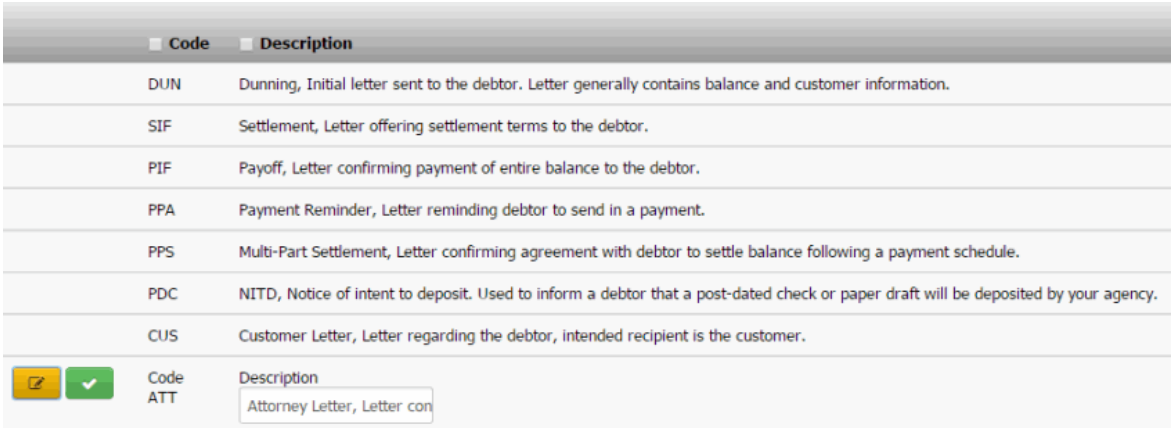
Use the **Letter Types** panel to modify a letter type.

To modify a letter type

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Letter Types**.



2. Click the Edit icon. The letter type appears in edit mode.



3. Modify the information and then click the check mark.

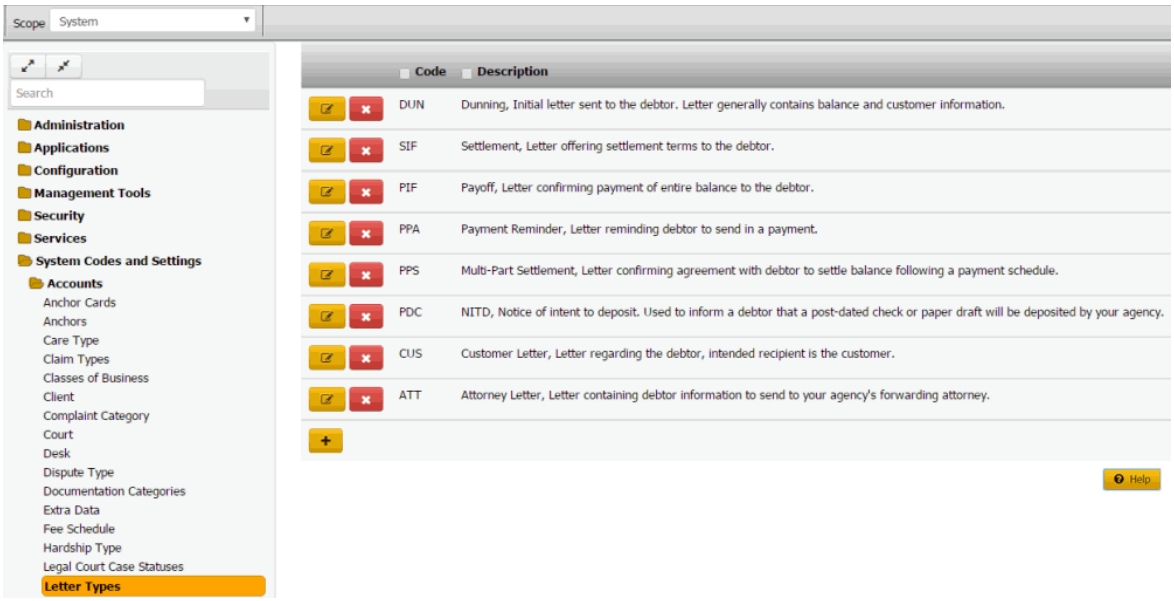
Note: For system-level letter types, you cannot modify the code.

Delete a Letter Type

Use the **Letter Types** panel to delete a letter type. You cannot delete system-defined letter types.

To delete a letter type

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Letter Types**.



2. Click the Delete icon and then click **Yes**.

List Codes

List Codes

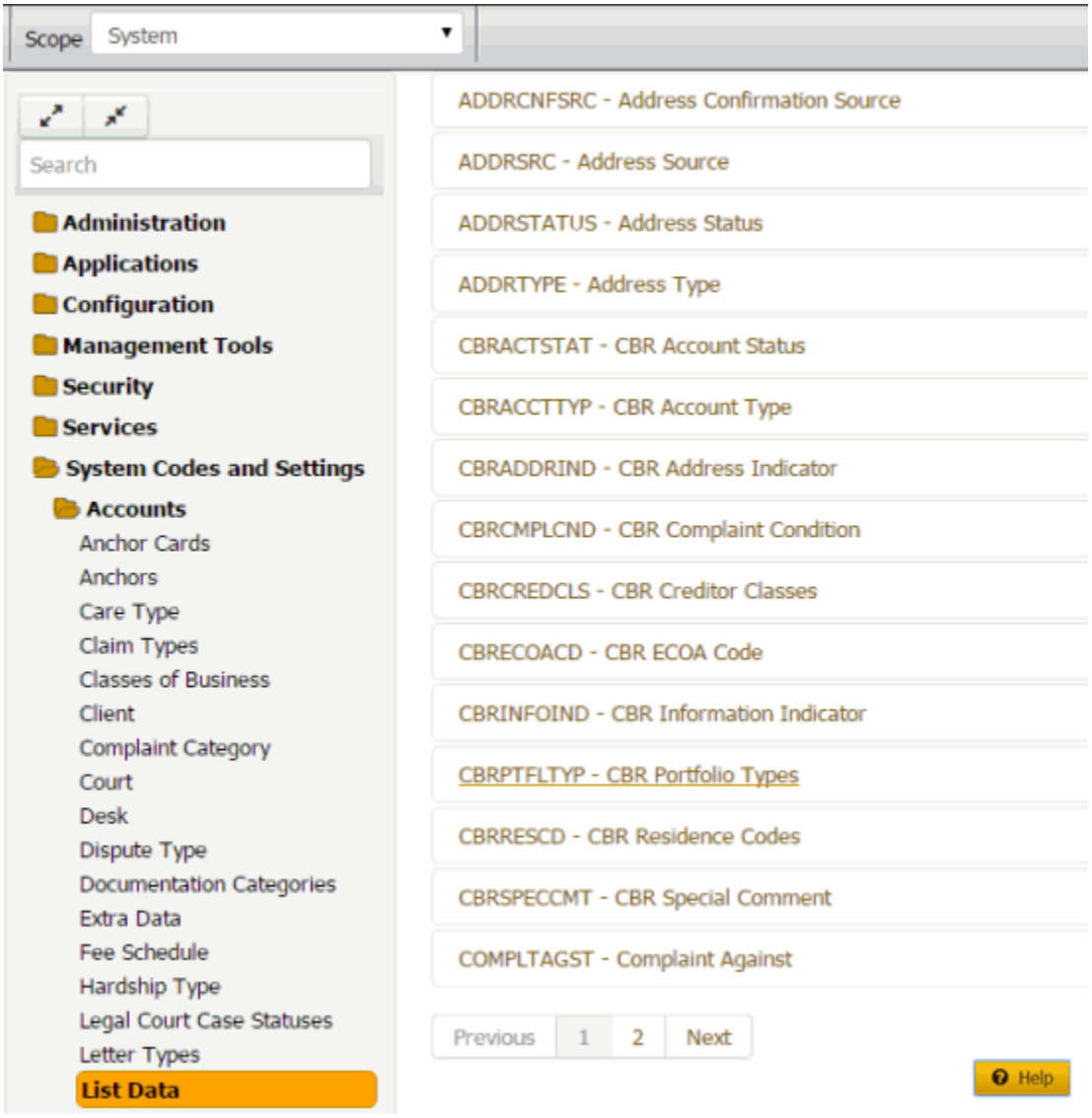
You can modify user-defined list codes and associate data to the list codes. You cannot add list codes or modify system-defined list codes. List codes allow your organization to specify data to use in related panels in Latitude.

Modify a List Code

Use the **List Data** panel to modify a custom list code. You cannot modify system-defined list codes.

To modify a list code

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **List Data**.



2. Click the list code to modify. The list code expands.

List Code: Unique code that identifies the custom list.

Namespace: Alternate name for the custom list.

Display Name: Name of the custom list. This name appears when displaying the list in a custom panel.

Description: A description of the custom list.

Code is Numeric: If selected, the list data identifier is numeric. If cleared, the list data identifier is alphanumeric.

Code Length Max: Maximum number of characters allowed for the list data identifier.

Description Length Max: Maximum number of characters allowed for the list data description.

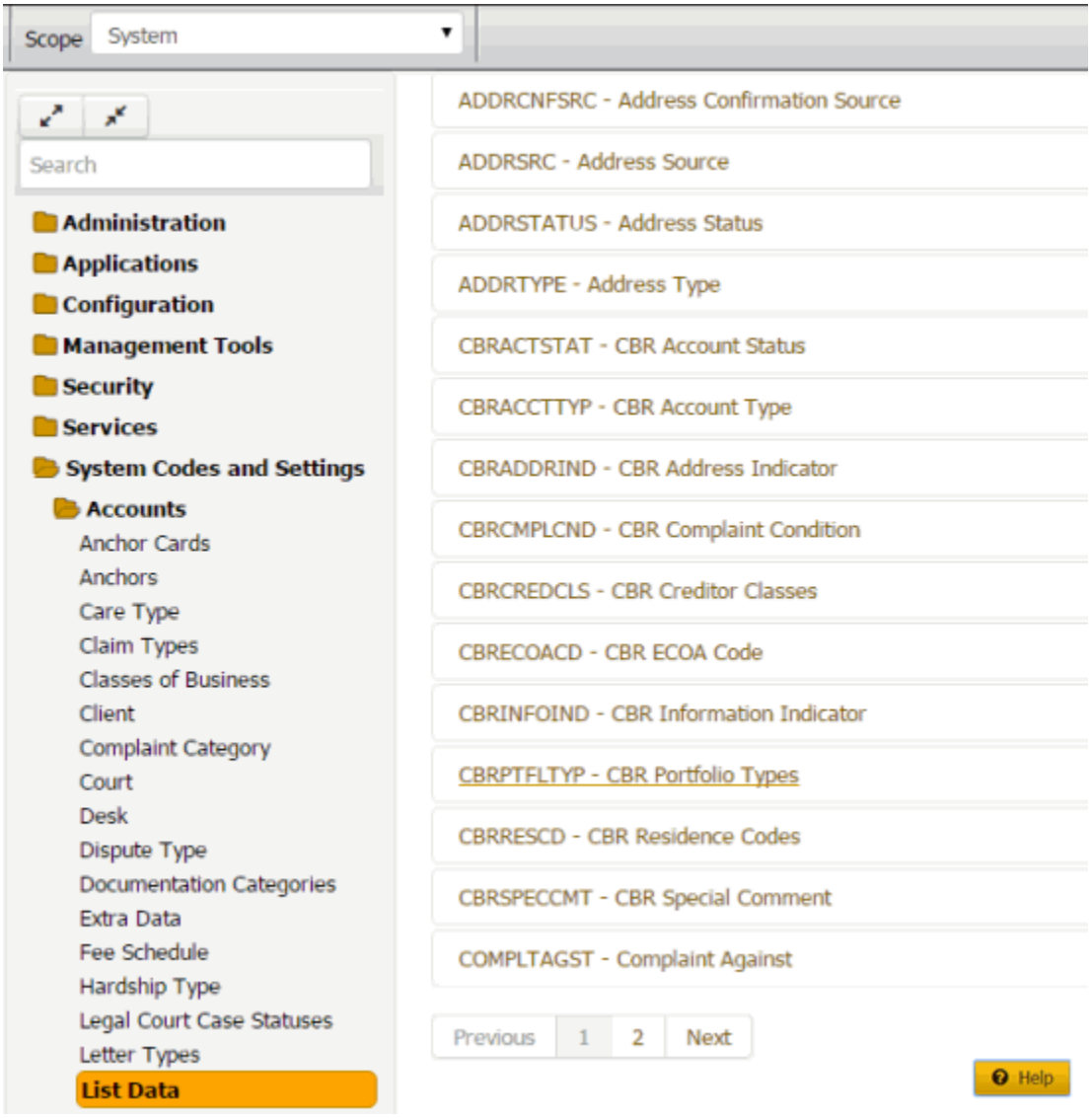
3. Modify the information and then click **Save**.

Add List Data

Use the **List Data** panel to add data to a custom list.

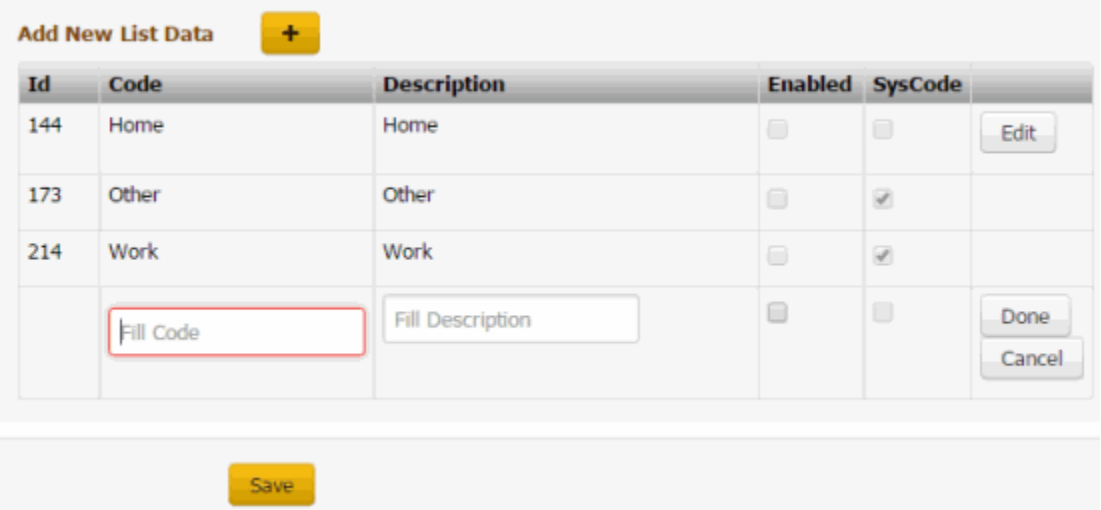
To add list data

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **List Data**.



2. Click the list code to which to add list data. The list code expands.

3. Next to **Add New List Data**, click the plus sign (+). A blank row appears in the data grid.



ID: Code that the system assigns to identify the custom list data.

Code: Code that you assign to identify the custom list data. The system limits the maximum number of characters allowed to what is set as the **Code Length Max** in the List Code section.

Description: Description of the custom list data. The system limits the maximum number of characters allowed to what is set as the **Description Length Max** in the List Code section.

Enabled: If selected, you want the custom list data to appear on a custom panel. You cannot delete list data; however, you can clear this check box so that the data doesn't appear on a custom panel.

SysCode: If selected, all list data that you add to this custom list is system-defined. If cleared, the list data is user-defined. Users cannot select or clear this check box.

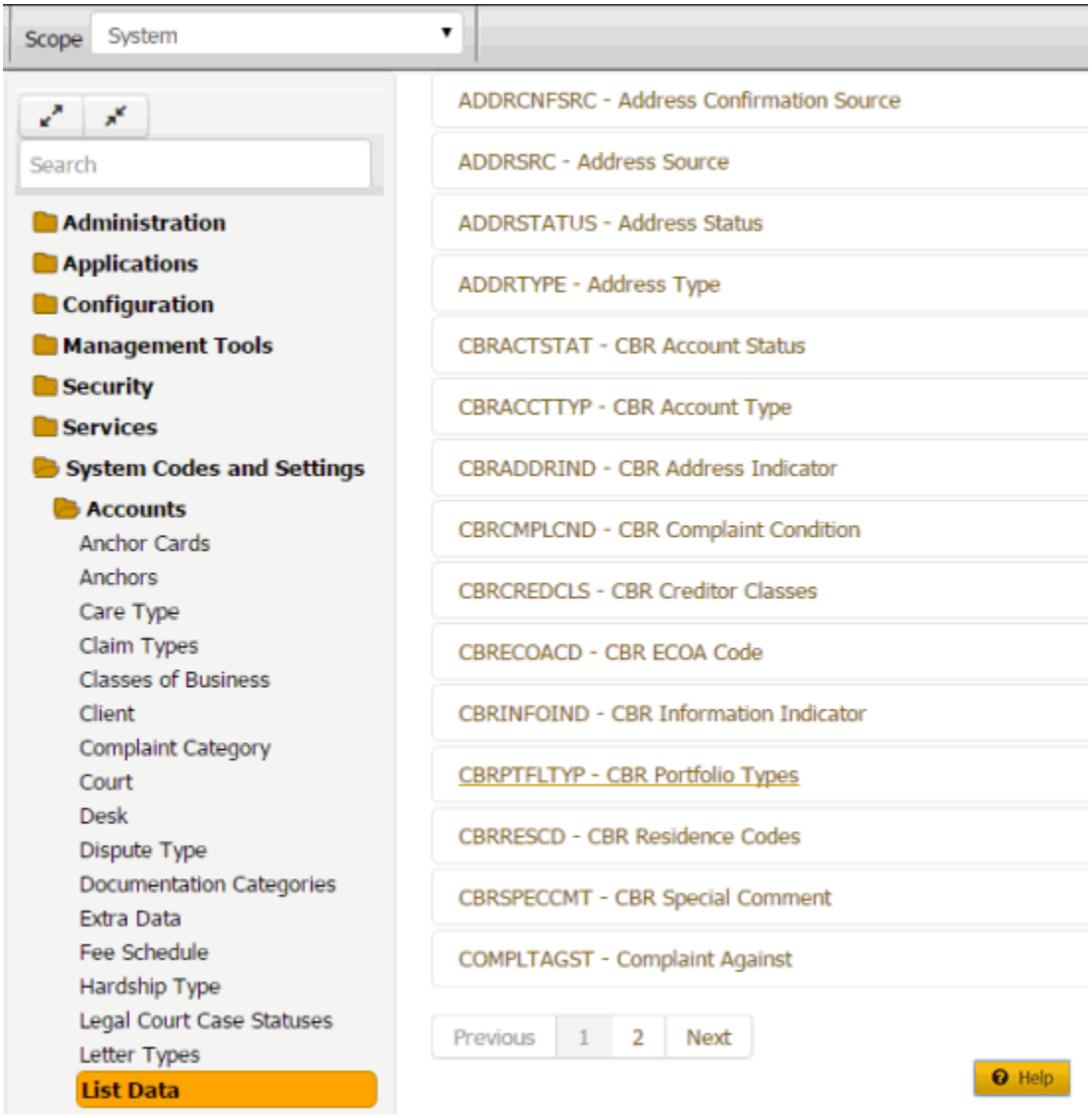
4. Complete the information and then click **Done**.
5. Click **Save**. The system assigns an ID to the list data item.

Modify List Data

Use the **List Data** panel to modify data in a custom list. You cannot modify system-defined list data.

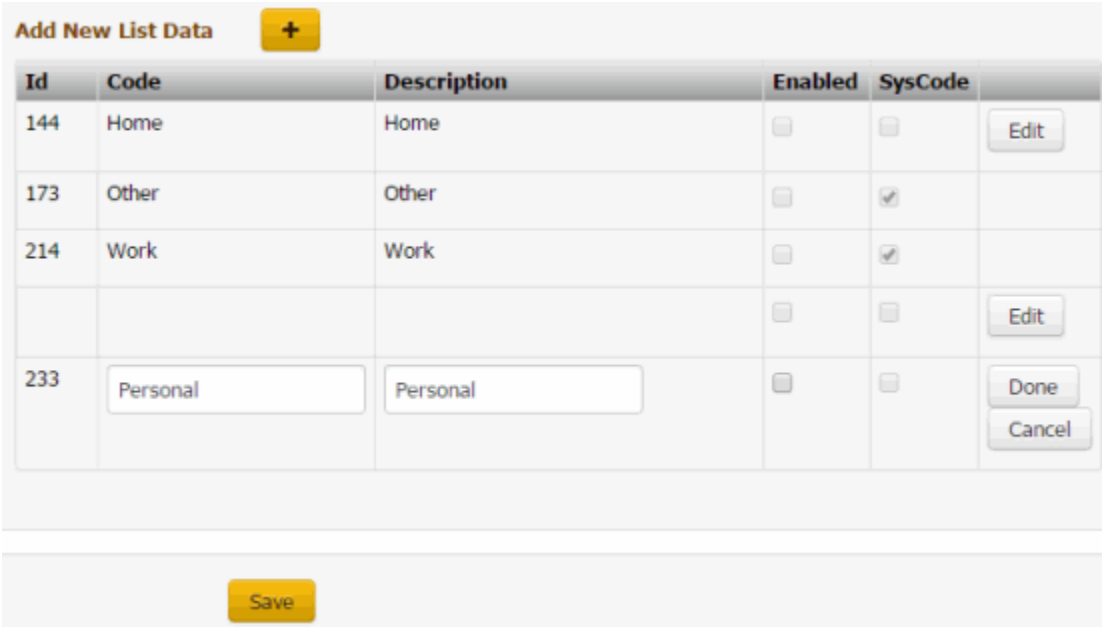
To modify list data4

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **List Data**.



2. Click the list code to modify. The list code expands.

3. In the data grid, click **Edit**. The data grid appears in edit mode.



ID: Code that the system assigns to identify the custom list data.

Code: Code that you assign to identify the custom list data. The system limits the maximum number of characters allowed to what is set as the **Code Length Max** in the List Code section.

Description: Description of the custom list data. The system limits the maximum number of characters allowed to what is set as the **Description Length Max** in the List Code section.

Enabled: If selected, you want the custom list data to appear on a custom panel. You cannot delete list data; however, you can clear this check box so that the data doesn't appear on a custom panel.

SysCode: If selected, all list data that you add to this custom list is system-defined. If cleared, the list data is user-defined. Users cannot select or clear this check box.

4. Modify the information and then click **Done**.
5. Click **Save**.

Manual Process Stages

Manual Process Stages

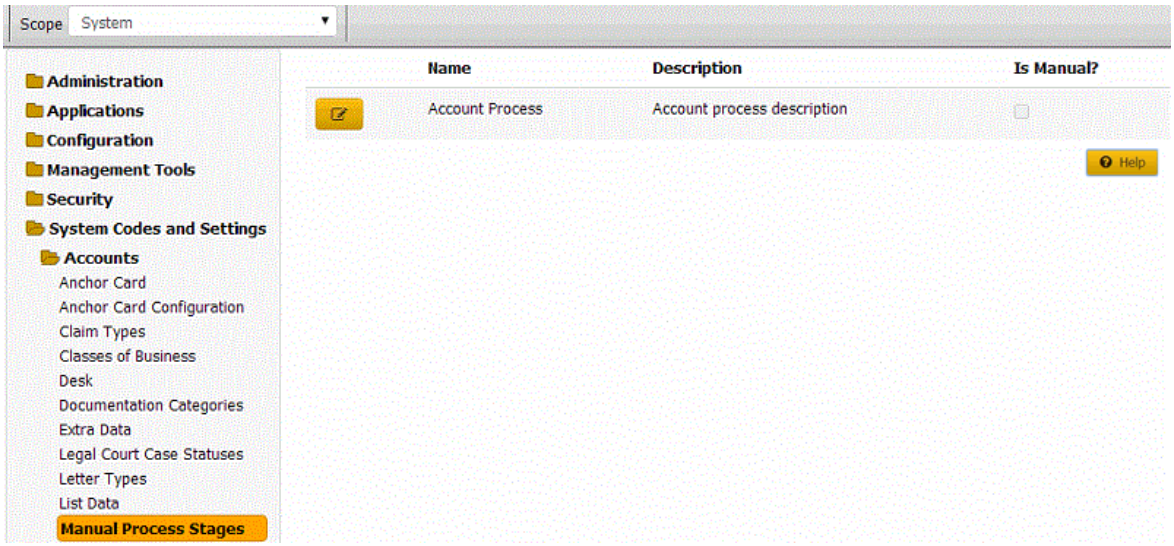
You can flag processes as either manual or automated. For more information, see Processes and Stages.

Flag a Process as Manual or Automated

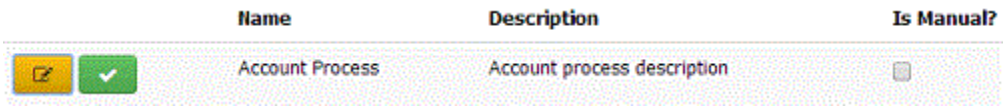
Use the **Manual Process Stages** panel to flag a process as manual or automated.

To flag a process as manual or automated

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Manual Process Stages**.



2. Click the Edit icon. The process appears in edit mode.



Is Manual: If selected, the process is manual. Users move the process to subsequent stages manually. If cleared, the process is automated. The system moves the process to subsequent stages automatically, based on the stage order set for the process.

3. Select or clear the check box and then click the check mark.

Note Action Codes

Note Action Codes

You can search for, add, modify, and delete action codes. Action codes represent the actions a user took on an account. When working an account, a user selects the action code that represents the action the user took on the account and Latitude records the action in the account notes. These codes are available on certain reports. Latitude releases with several standard action codes.

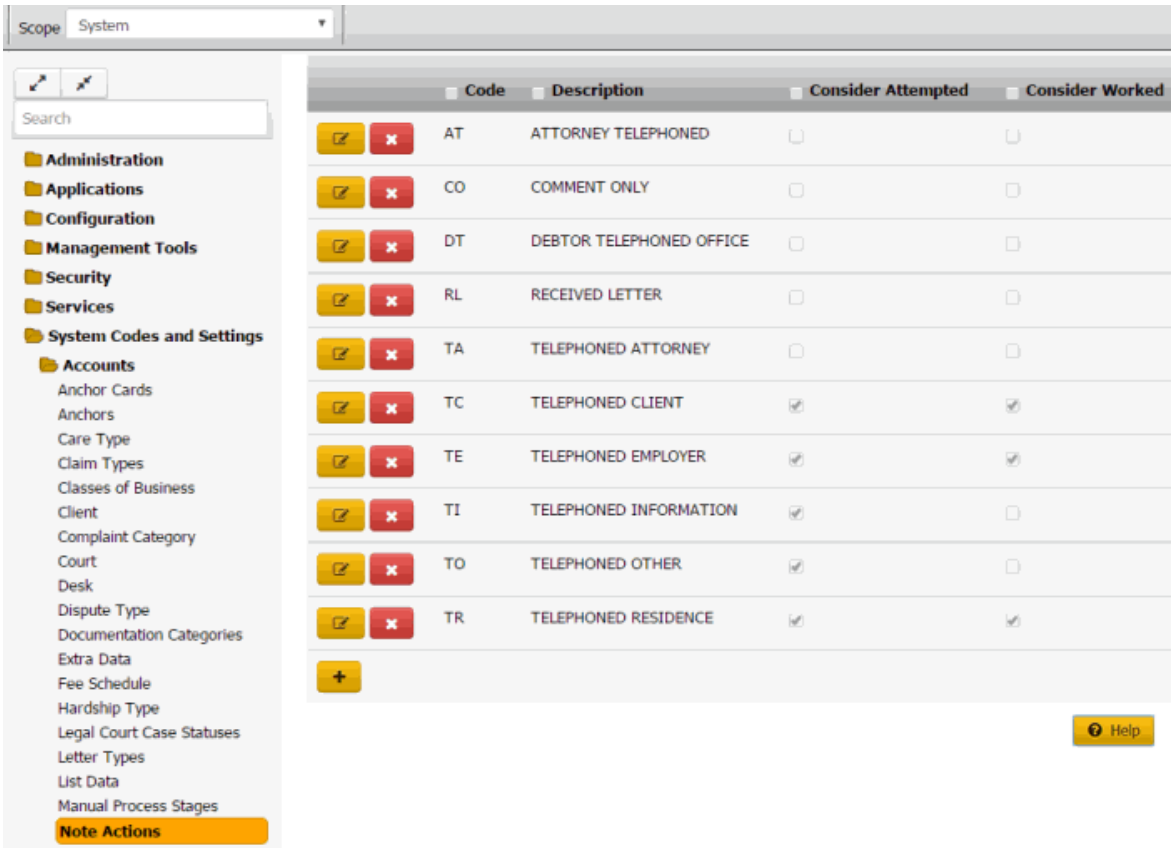
> **Note**: Some Latitude system processes require specific codes. For more information, see Action and Result Codes.

Add a Note Action Code

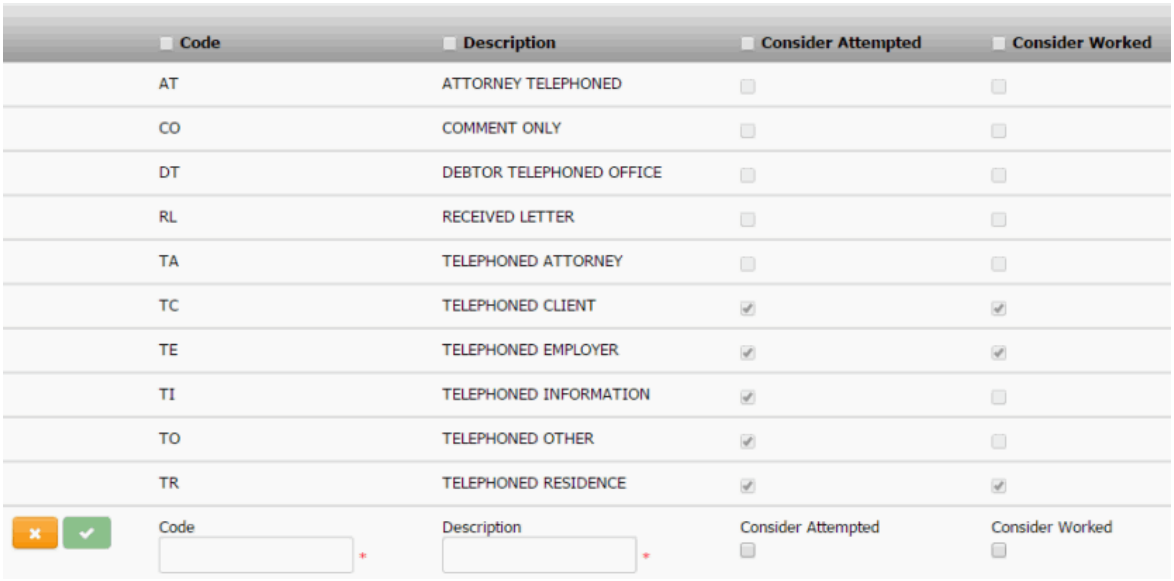
Use the **Note Actions** panel to add an action code for notes.

To add an action code

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Note Actions**.



2. Click the plus sign (+). A blank row appears in the data grid.



Code: Unique code that identifies the action.

Description: Description of the action.

Consider as attempted: If selected, the action code signifies an attempt at working the account.

Consider as worked: If selected, the action code signifies a worked account.

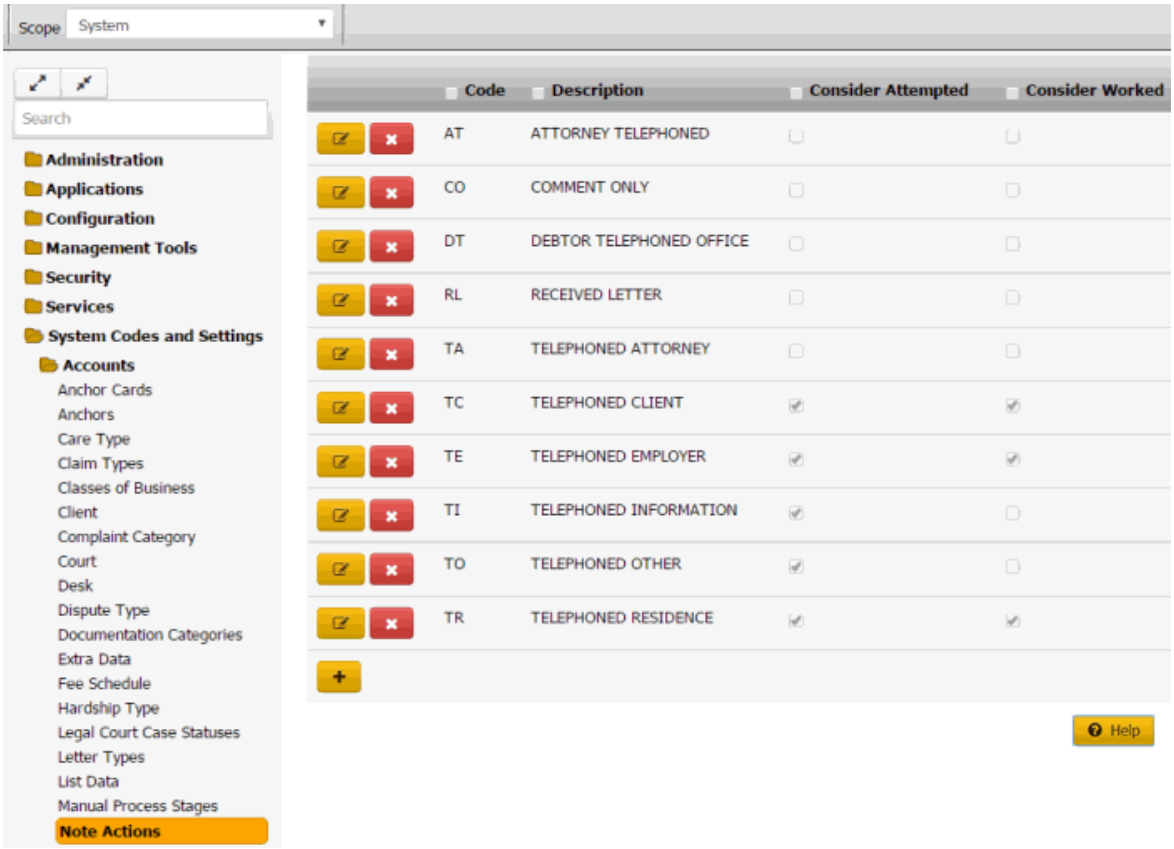
3. Complete the information and then click the check mark.

Modify a Note Action Code

Use the **Note Actions** panel to modify an action code.

To modify an action code

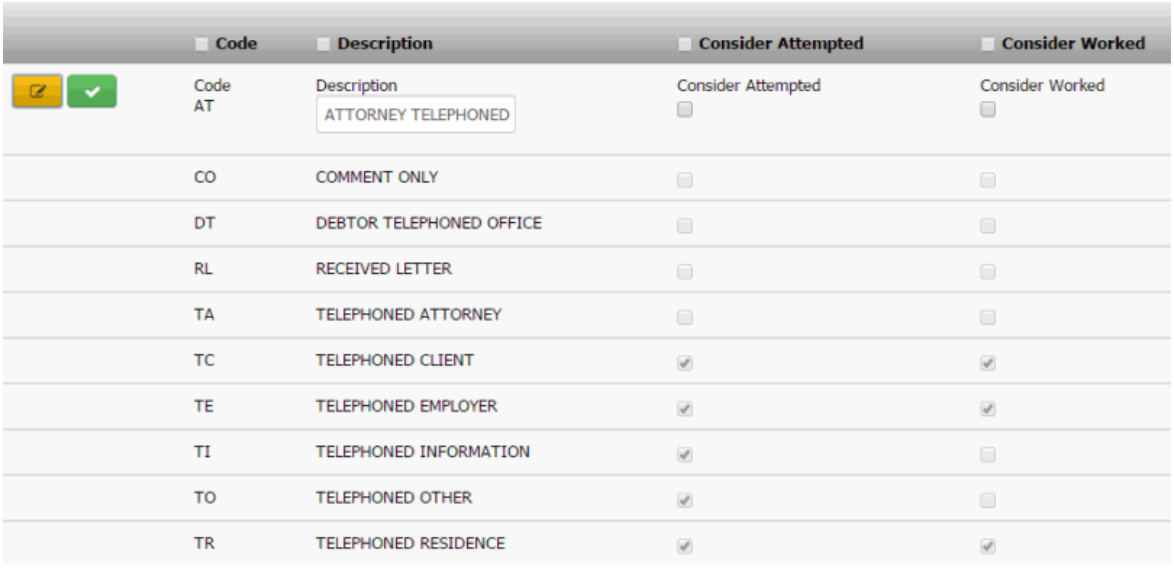
1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Note Actions**.



Consider as attempted: If selected, indicates that the action code signifies an attempt at working the account.

Consider as worked: If selected, indicates that the action code signifies a worked account.

2. Click the Edit icon. The action code appears in edit mode.



Code	Description	Consider Attempted	Consider Worked
Code AT	Description ATTORNEY TELEPHONED	Consider Attempted	Consider Worked
CO	COMMENT ONLY		
DT	DEBTOR TELEPHONED OFFICE		
RL	RECEIVED LETTER		
TA	TELEPHONED ATTORNEY		
TC	TELEPHONED CLIENT	✓	✓
TE	TELEPHONED EMPLOYER	✓	✓
TI	TELEPHONED INFORMATION	✓	
TO	TELEPHONED OTHER	✓	
TR	TELEPHONED RESIDENCE	✓	✓

Code: Unique code that identifies the action.

Description: Description of the action.

Consider as attempted: If selected, the action code signifies an attempt at working the account.

Consider as worked: If selected, the action code signifies a worked account.

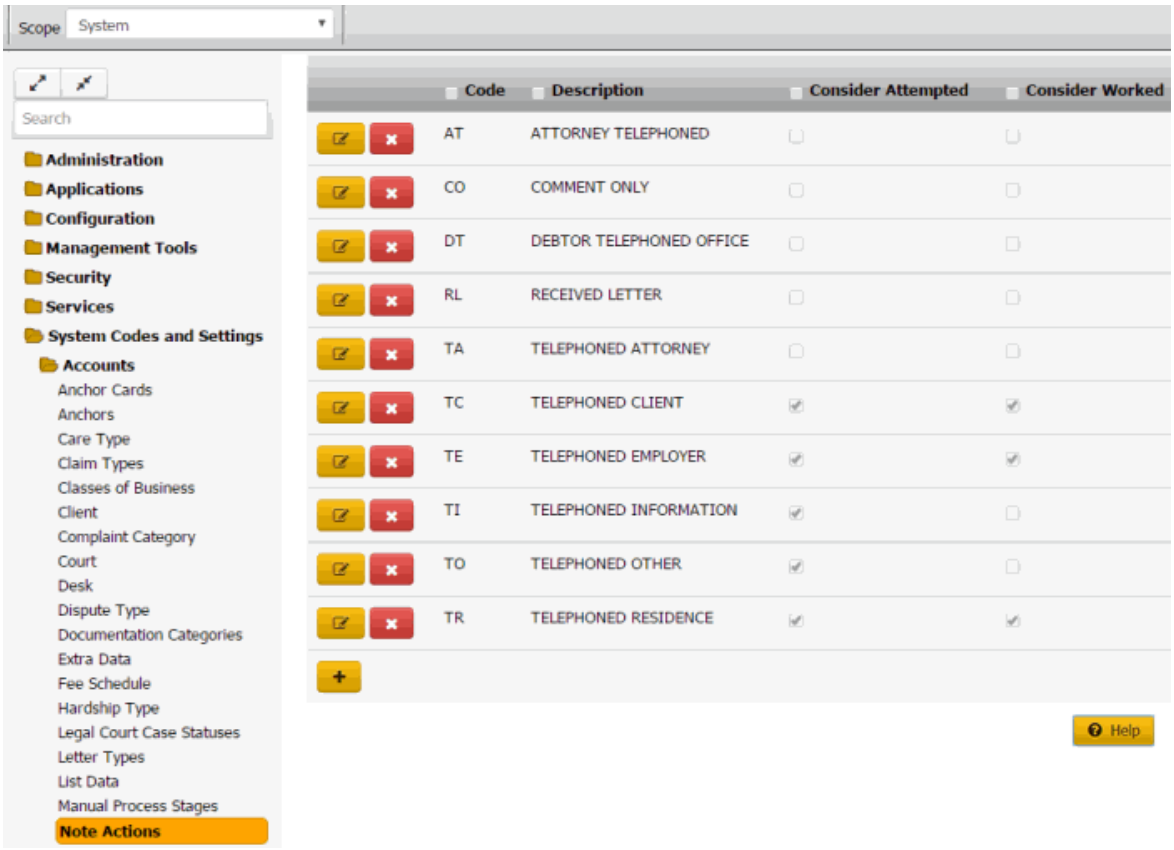
3. Modify the information and then click the check mark.

Delete a Note Action Code

Use the **Note Actions** panel to delete an action code.

To delete an action code

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Note Actions**.



2. Click the Delete icon and then click **Yes**.

Note Result Codes

Note Result Codes

You can search for, add, modify, and delete result codes. Result codes represent the results of an action a user took on an account. When working an account, a user selects the result code that represents the result of an action the user took on the account. Latitude records the result in the account notes. Latitude uses result codes to count the number of accounts that each user worked and contacted.

Latitude releases with several standard result codes.

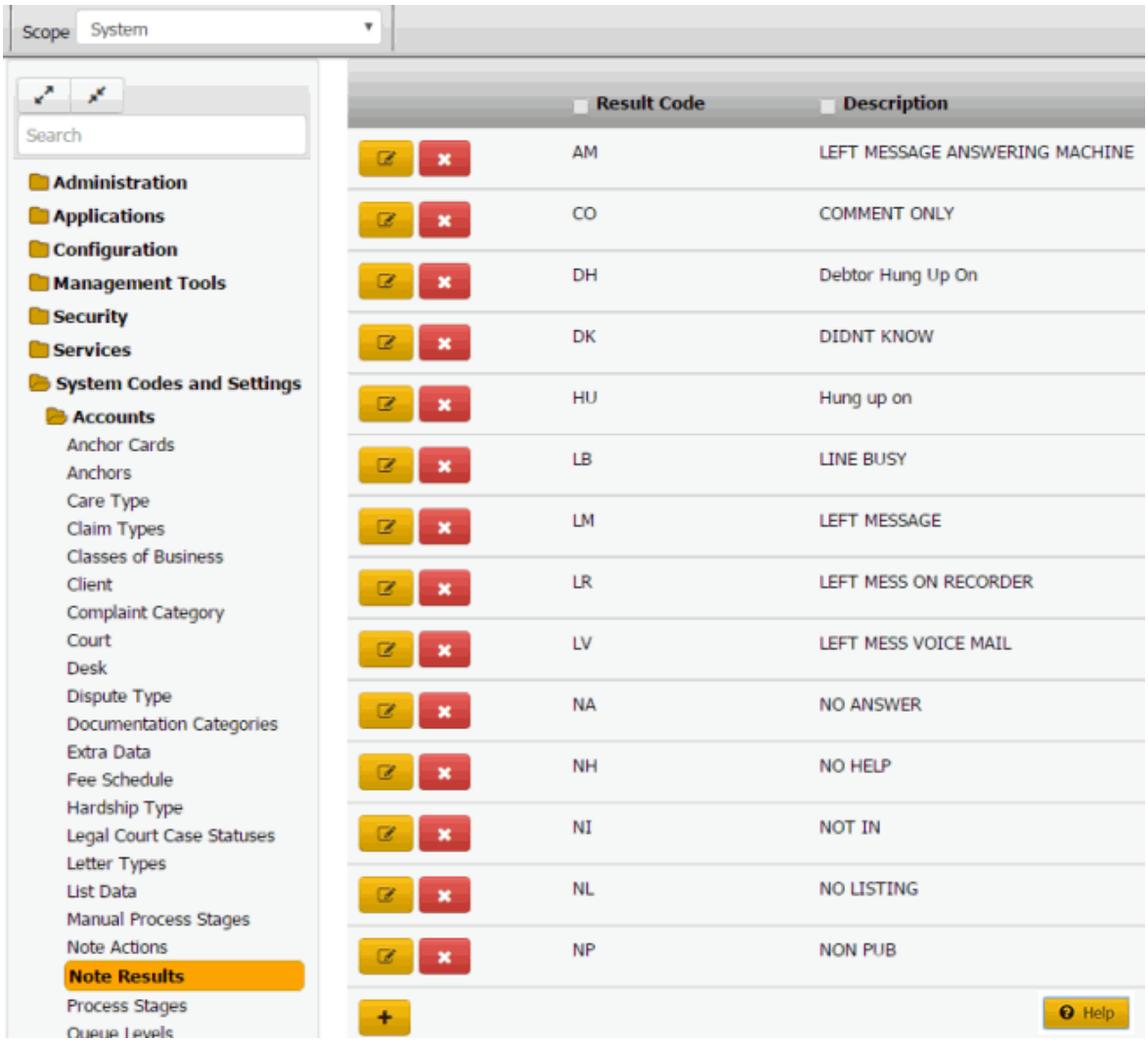
> **Note**: Some Latitude system processes require specific result codes. For more information about system-utilized codes, see Action and Result Codes.

Add a Note Result Code

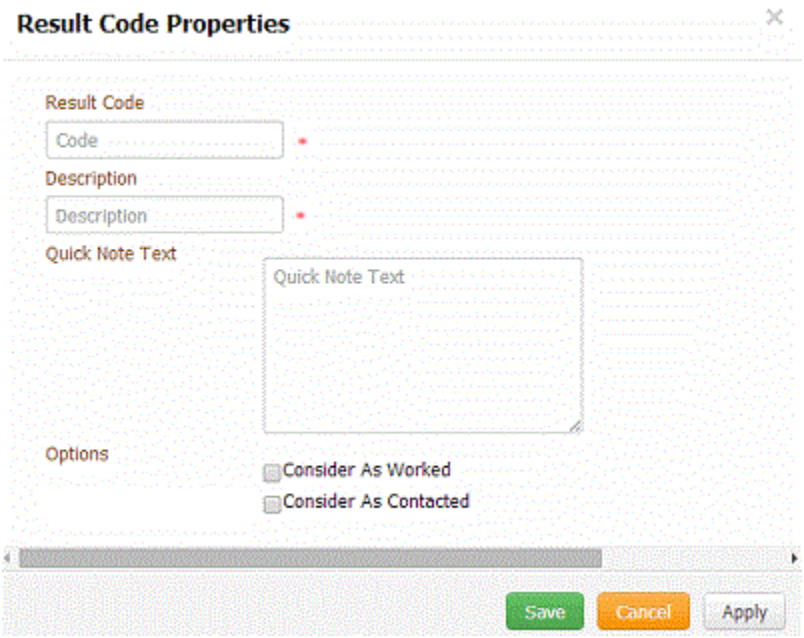
Use the **Result Code Properties** dialog box to add a result code.

To add a result code

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Note Results**.



2. Click the plus sign (+). The **Result Code Properties** dialog box appears.



Result Code: Unique (up to) five-character code that identifies an event.

Description: Description of the result code.

Quick Note Text: Default information to appear in the note. When users create a note using this result code, they can modify the quick note text.

Consider As Worked: If selected, the result code signifies a worked account.

Consider As Contacted: If selected, the result code signifies a contacted account.

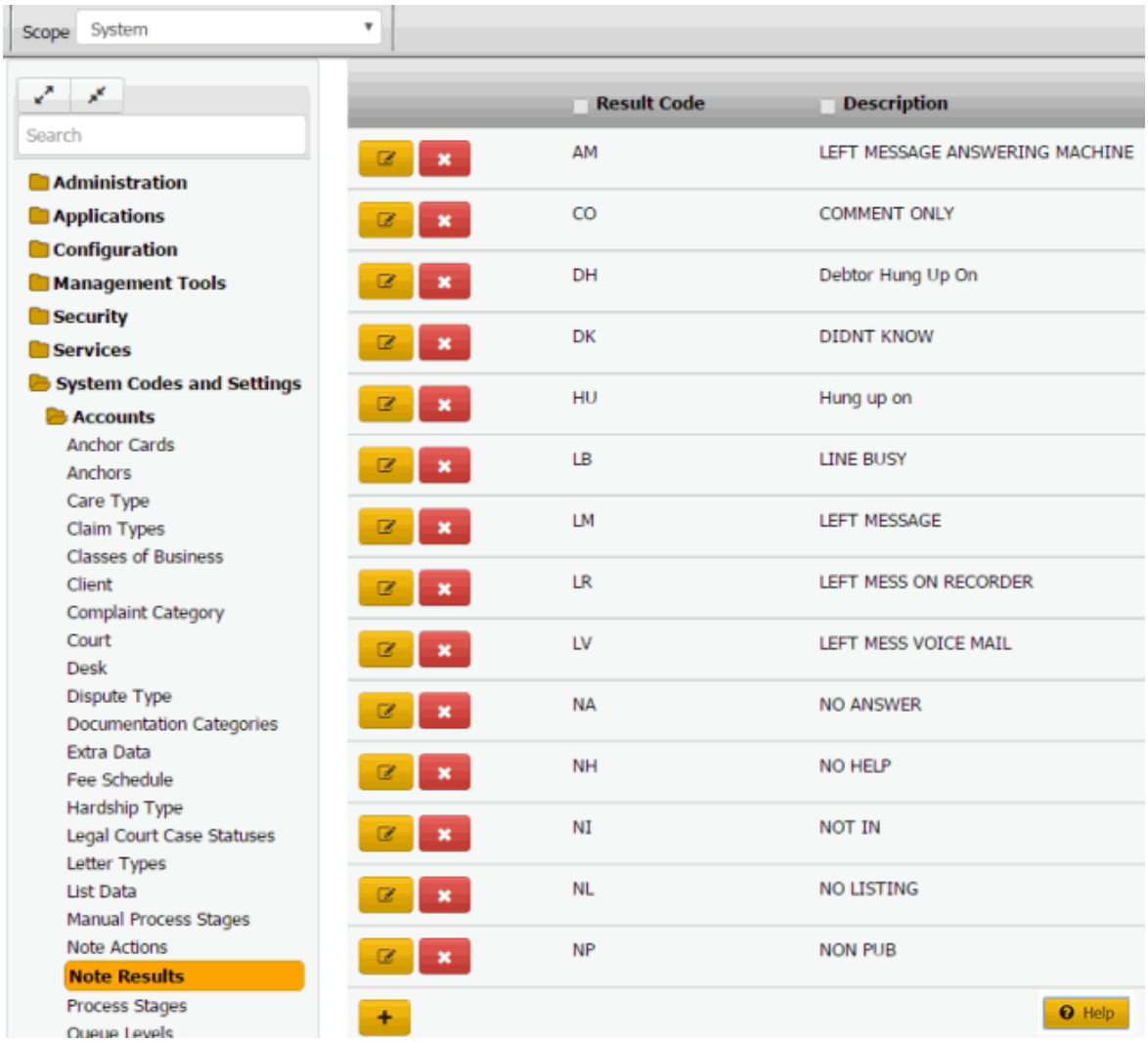
3. Complete the information and then click **Save**.

Modify a Note Result Code

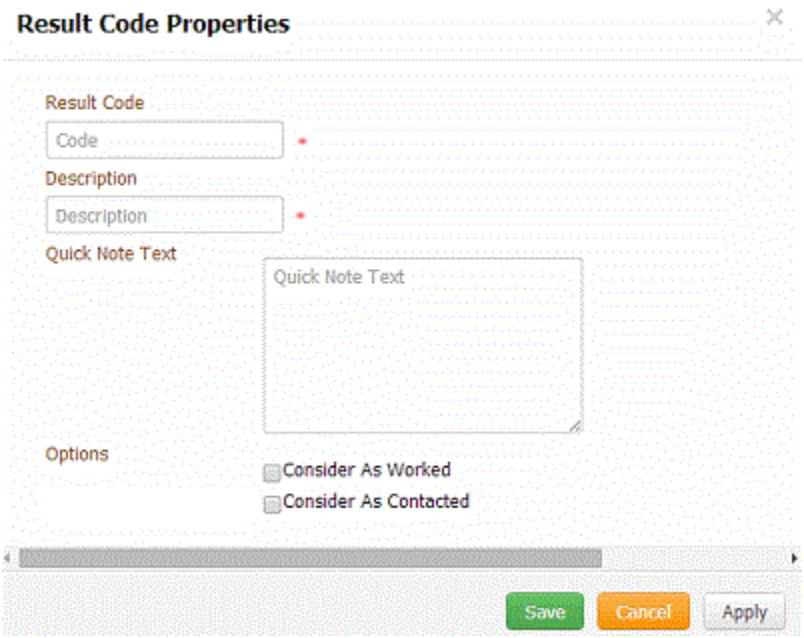
Use the **Result Code Properties** dialog box to modify a result code.

To modify a result code

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Note Results**.



2. Click the Edit icon. The **Result Code Properties** dialog box appears.



Result Code: Unique (up to) five-character code that identifies an event.

Description: Description of the result code.

Quick Note Text: Default information to appear in the note. When users create a note using this result code, they can modify the quick note text.

Consider As Worked: If selected, the result code signifies a worked account.

Consider As Contacted: If selected, the result code signifies a contacted account.

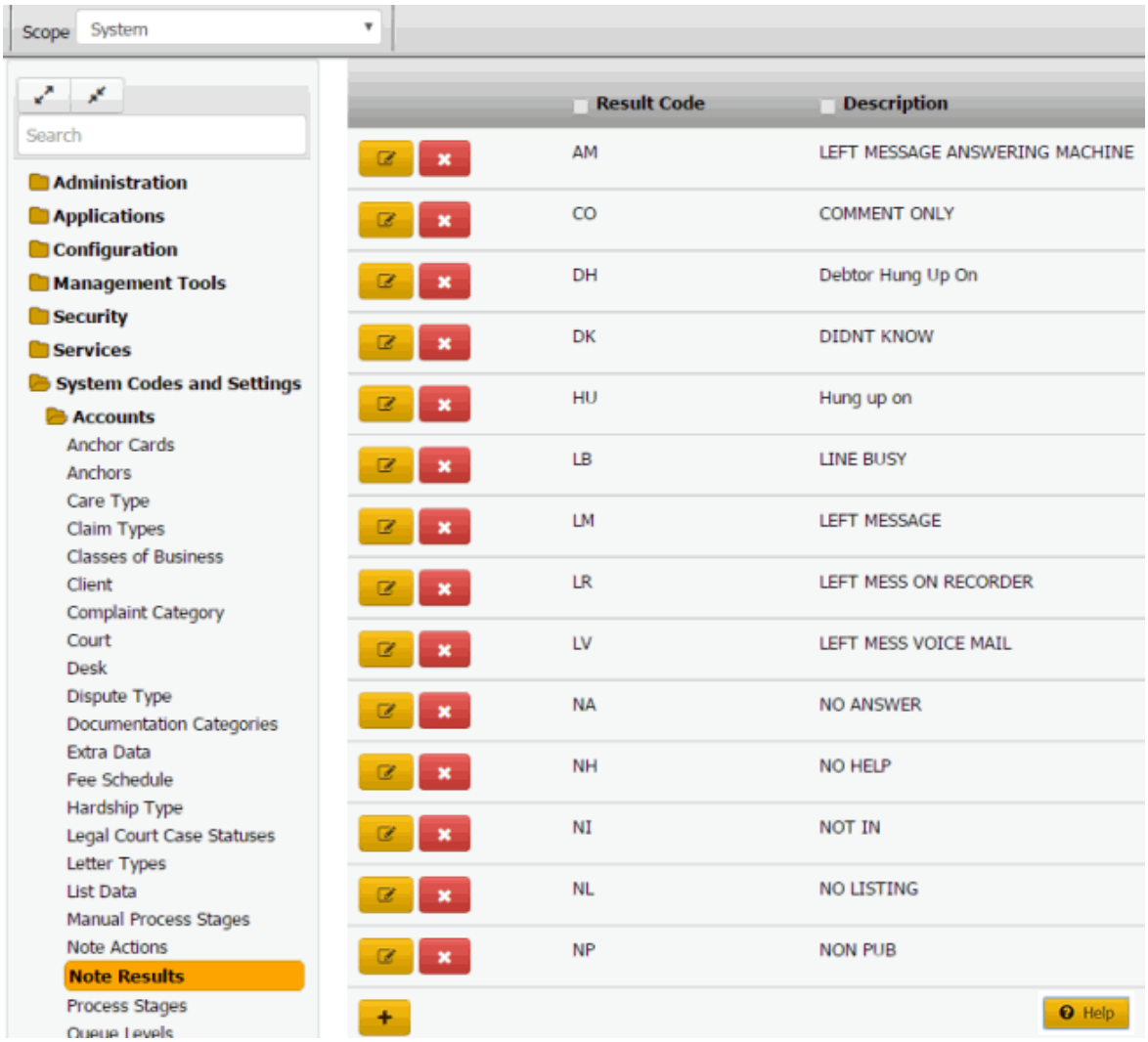
3. Modify the information and then click **Save**.

Delete a Note Result Code

Use the **Note Results** panel to delete a result code.

To delete a result code

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Note Results**.



2. Click the Delete icon and then click **Yes**.

Process Stages

Process Stages

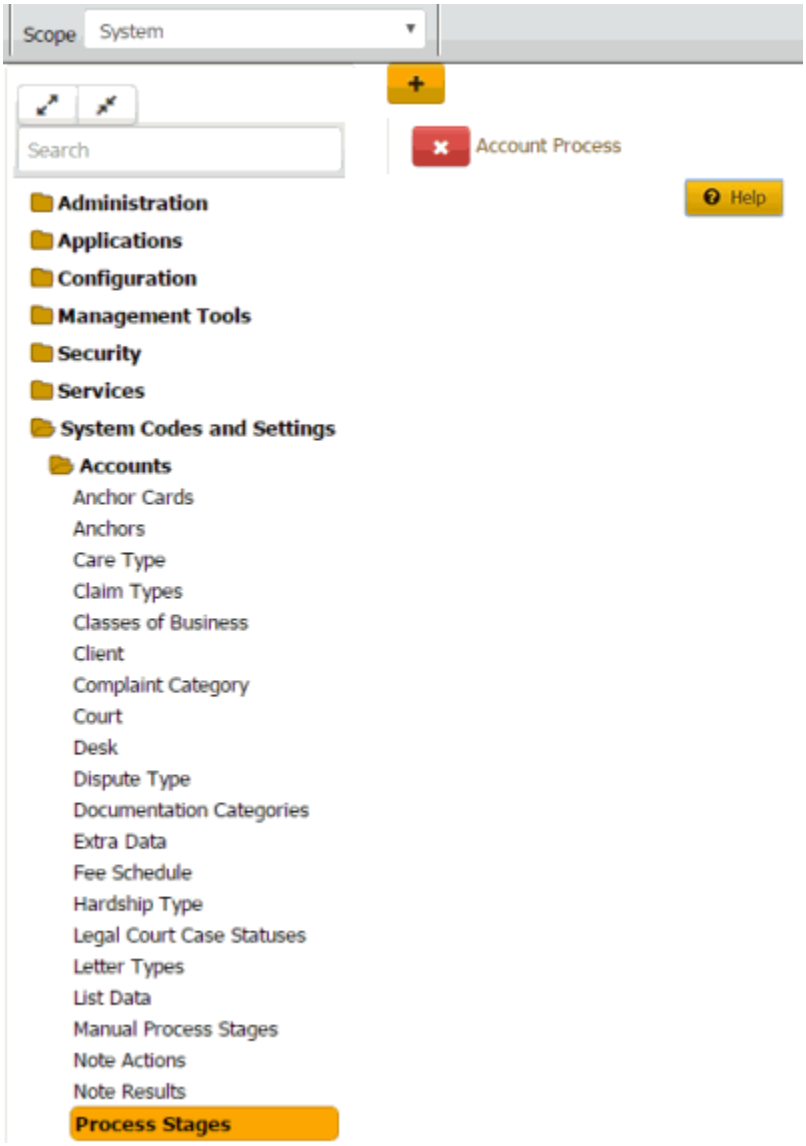
You can add, modify, and delete processes and their stages. For more information, see Processes and Stages.

Add a Process

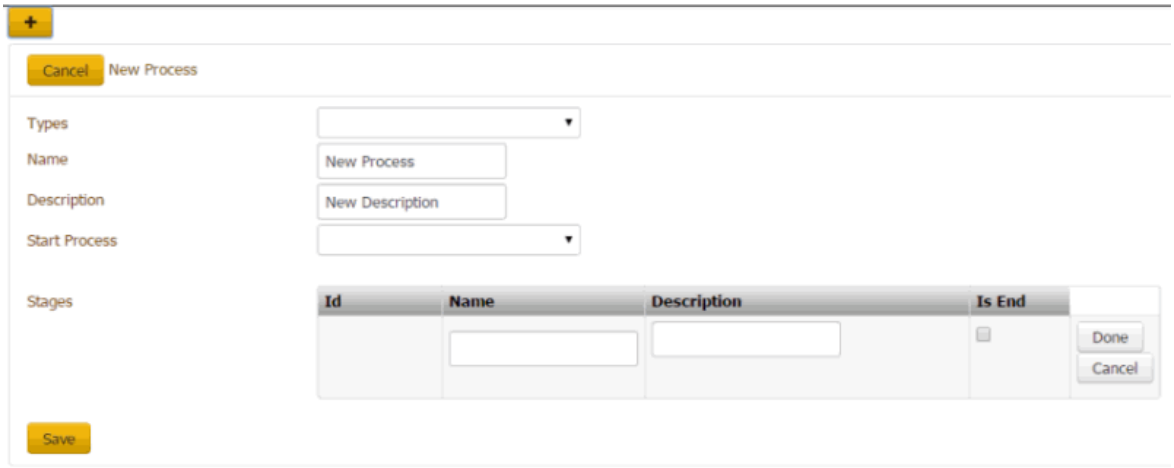
Use the **Process Stages** panel to add a process.

To add a process

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Process Stages**.



2. Click the plus sign (+). The panel appears in add mode.



Types: Type of process.

Name: Name of process.

Description: Description of process.

Start Process: Stage at which to start the process.

Stages

ID: Code that the system assigns to identify the stage.

Name: Name of the stage.

Description: Description of the stage.

Is End: If selected, this stage is the last stage in the process.

3. Complete the information and then click **Save**.

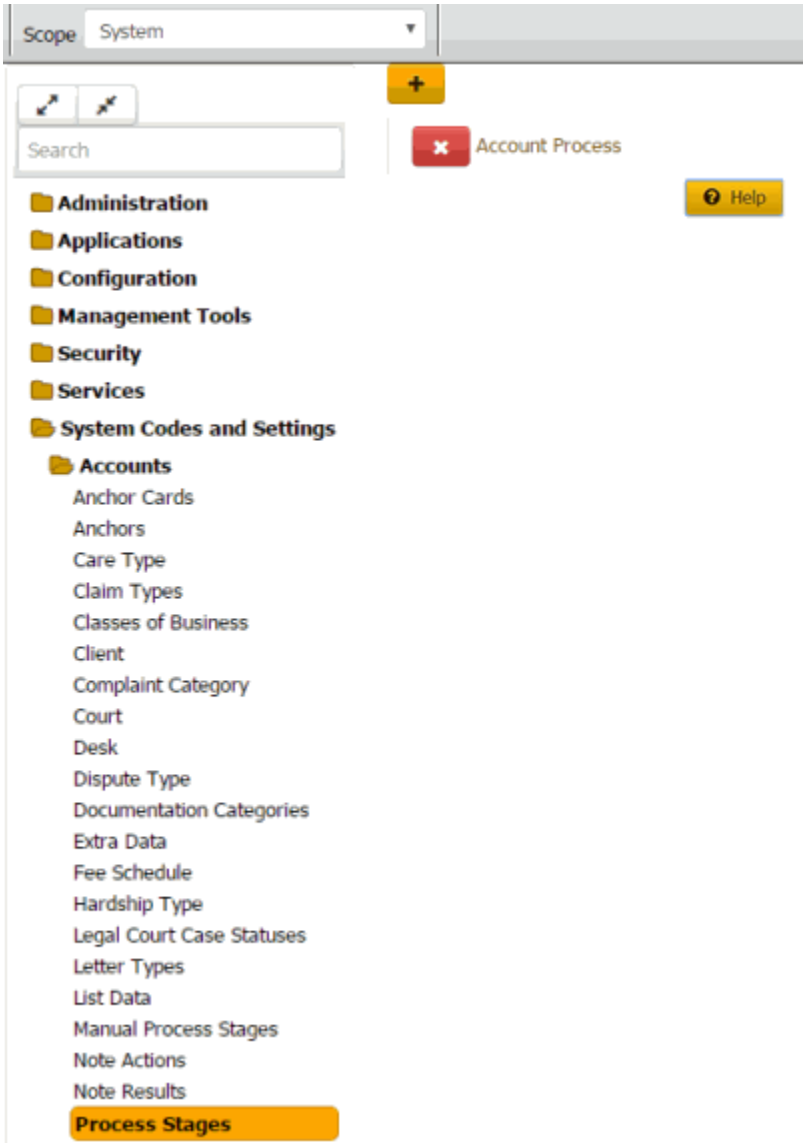
Note: For information about adding a stage to the process, see Add a Stage to a Process.

Modify a Process

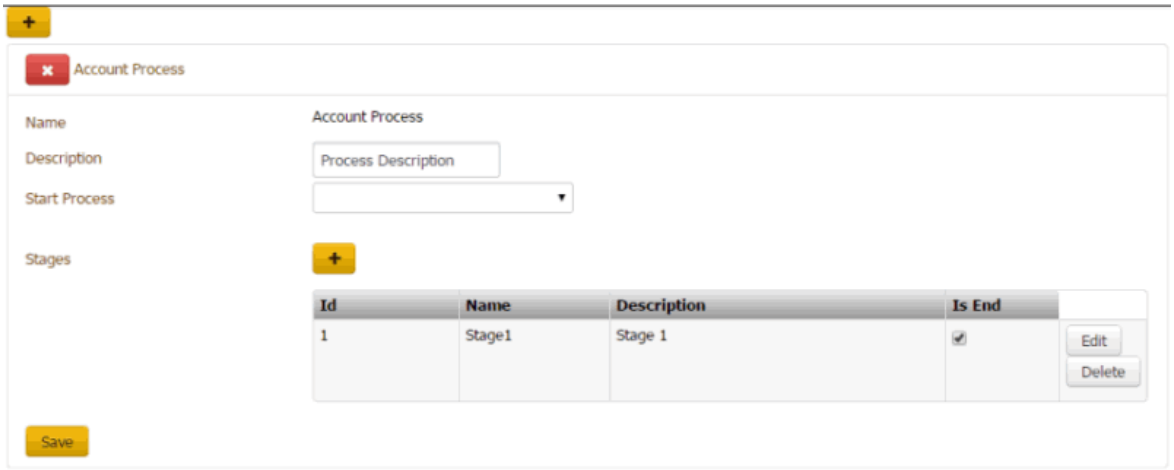
Use the **Process Stages** panel to modify a process.

To modify a process

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Process Stages**.



2. Click the process to modify. The process expands.



Name: Name of process.

Description: Description of process.

Start Process: Stage at which to start the process.

Stages

ID: Code that the system assigns to identify the stage.

Name: Name of the stage.

Description: Description of the stage.

Is End: If selected, this stage is the last stage in the process.

3. Modify the information and then click **Save**.

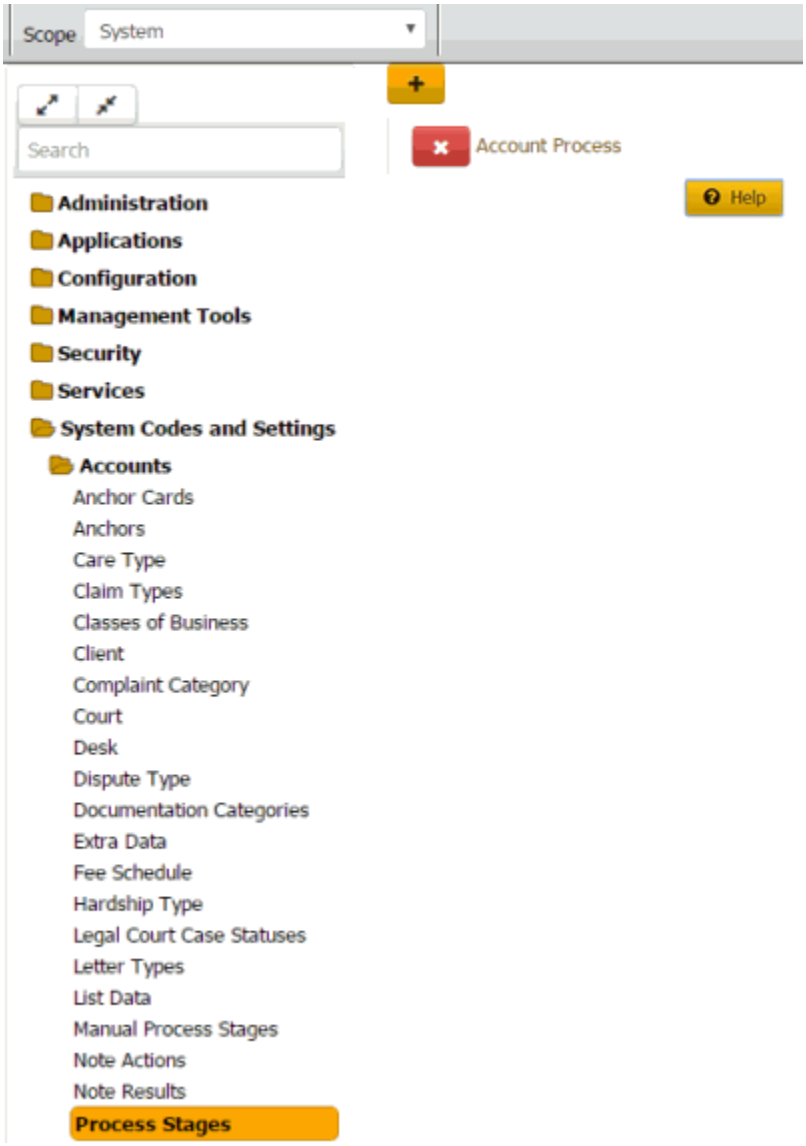
Note: For information about adding or modifying a stage, see Add a Stage to a Process.

Delete a Process

Use the **Process Stages** panel to delete a process.

To delete a process

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Process Stages**.



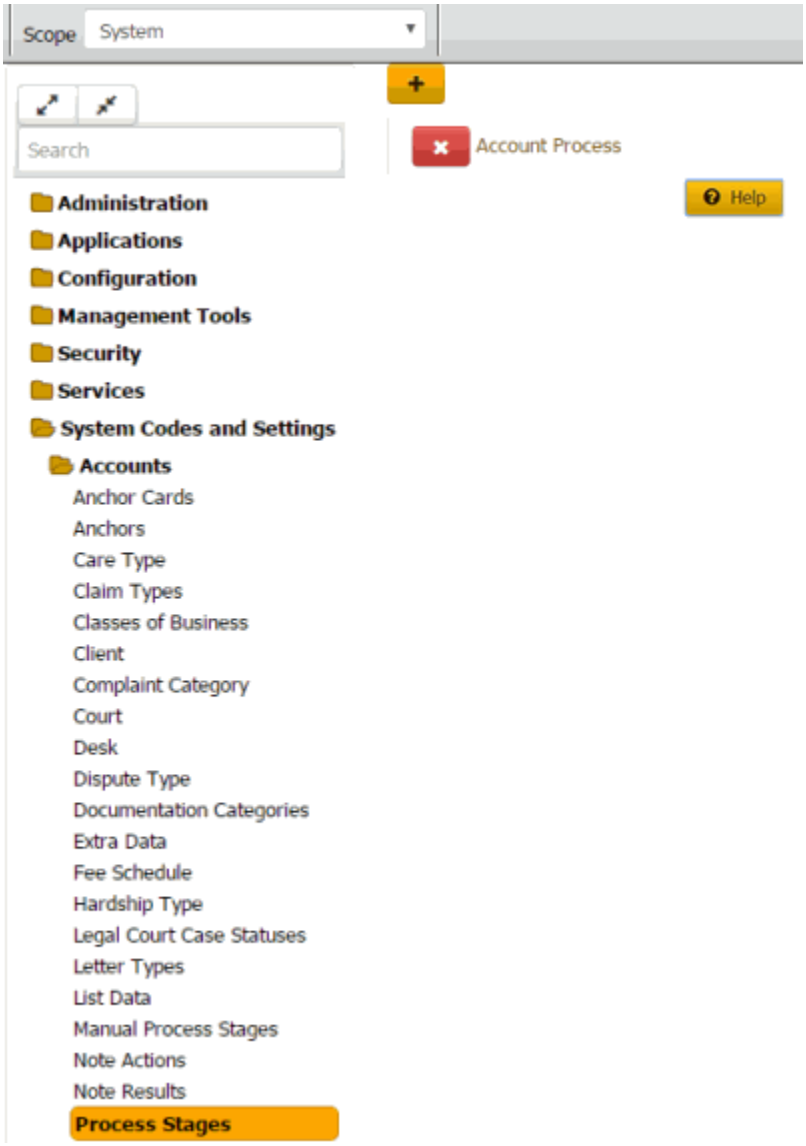
2. Click the Delete icon and then click **Yes**.

Add a Stage to a Process

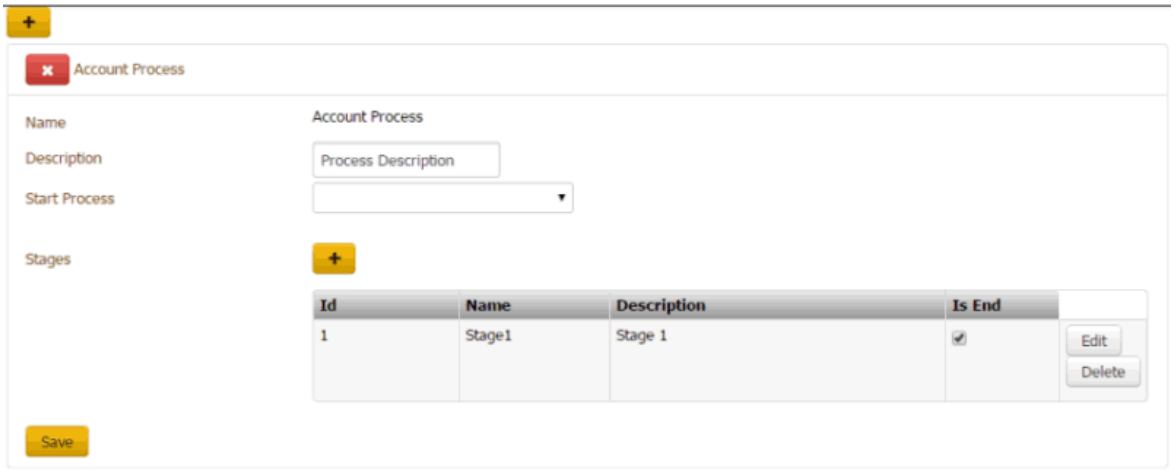
Use the **Process Stages** panel to add a stage to a process.

To add a stage to a process

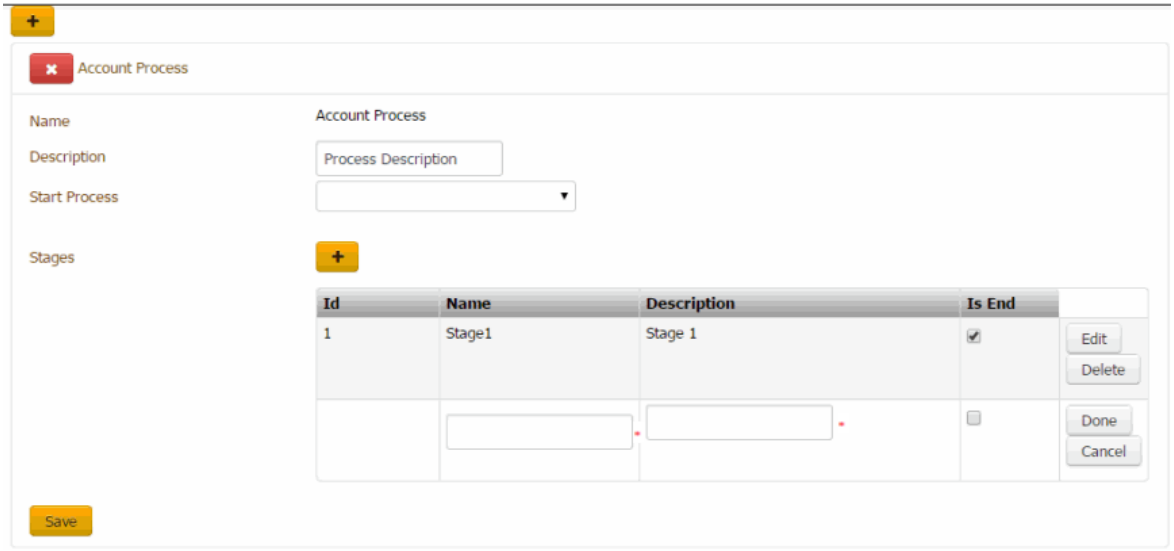
1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Process Stages**.



2. Click the process to which to add a stage. The process expands.



3. Next to **Stages**, click the plus sign (+). A blank row appears in the data grid.



ID: Code that the system assigns to identify the stage.

Name: Name of the stage.

Description: Description of the stage.

Is End: If selected, this stage is the last stage in the process.

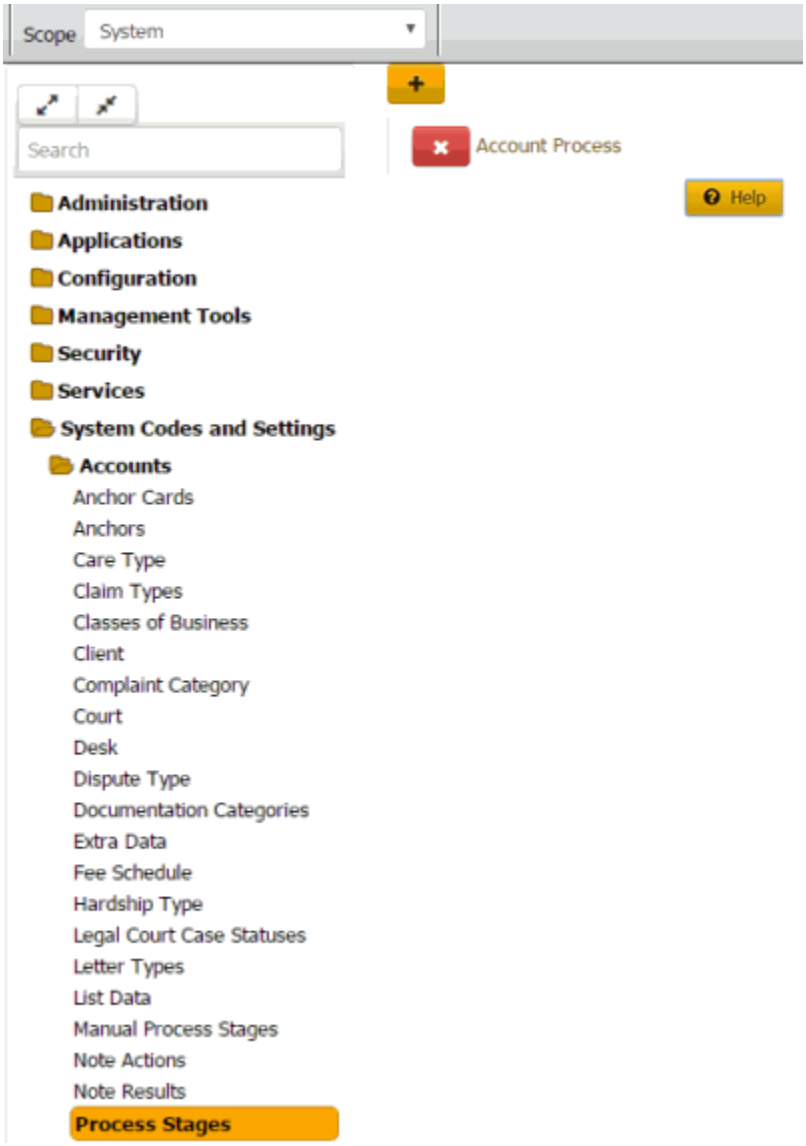
4. Complete the information and then click **Done**.
5. To modify a stage, click **Edit**, complete the information, and then click **Done**.
6. Click **Save**.

Modify a Process Stage

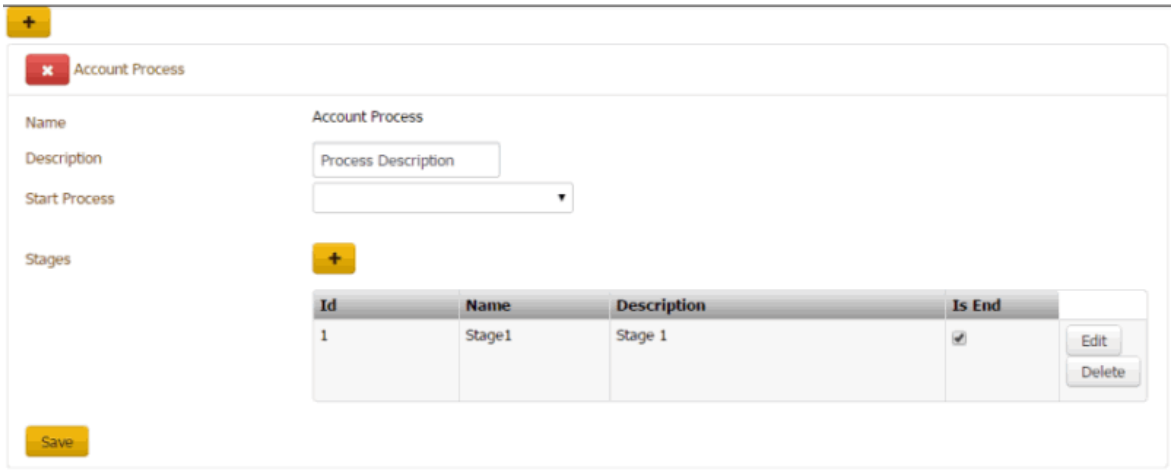
Use the **Process Stages** panel to modify a process stage.

To modify a process stage

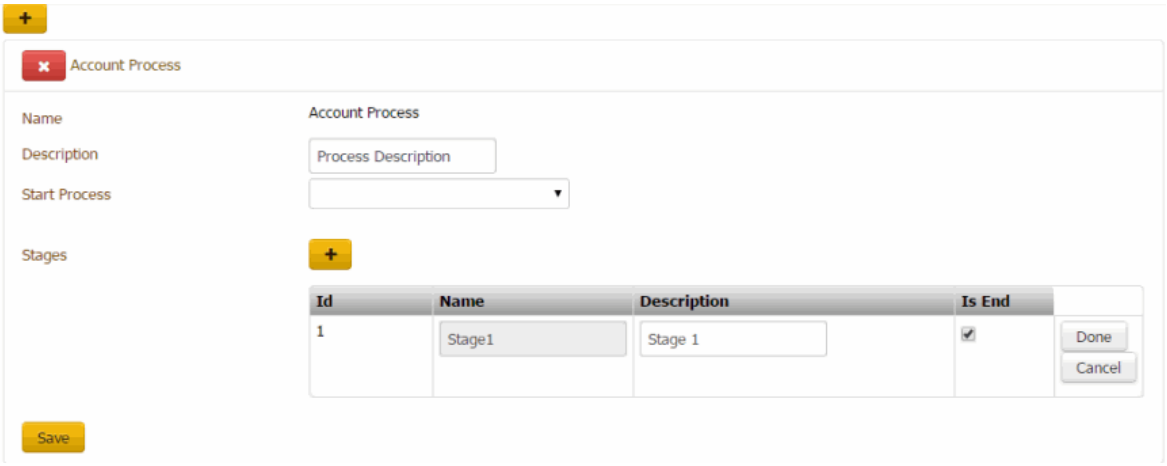
1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Process Stages**.



2. Click the process for which to modify a stage. The process expands.



3. In the data grid, click **Edit**. The data grid appears in edit mode.



ID: Code that the system assigns to identify the stage.

Name: Name of the stage.

Description: Description of the stage.

Is End: If selected, this stage is the last stage in the process.

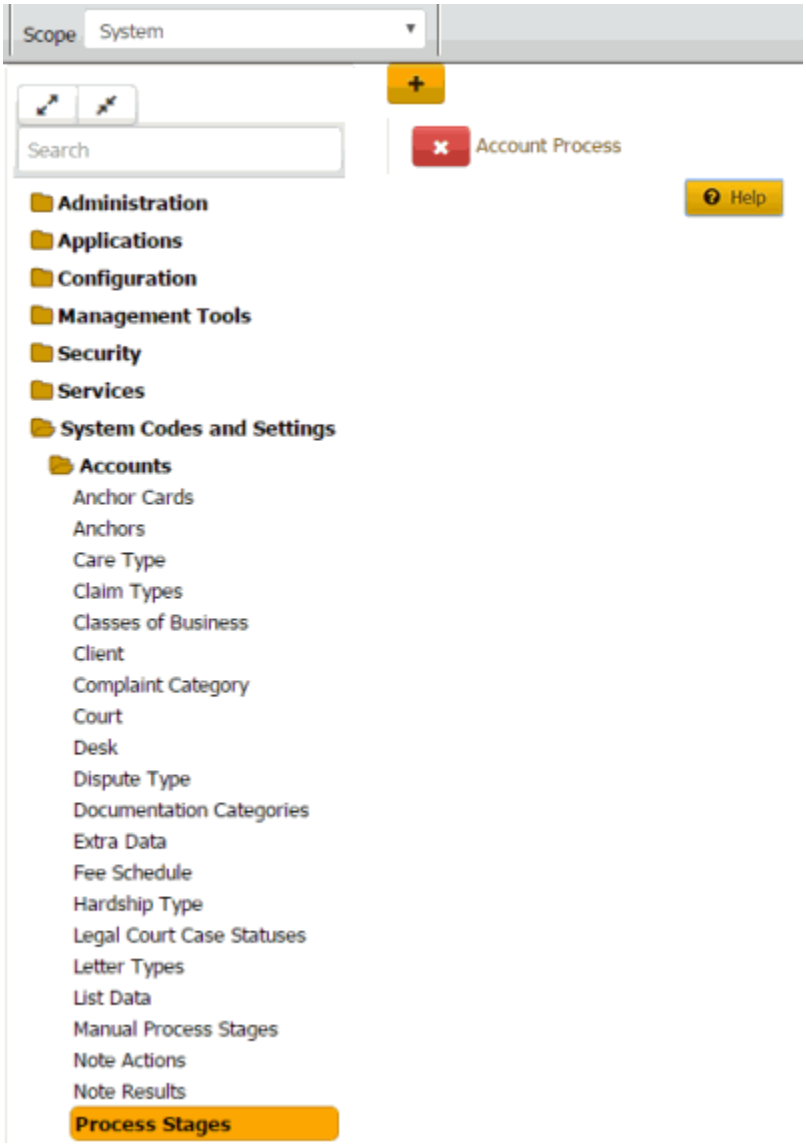
4. Modify the information and then click **Done**.
5. Click **Save**.

Delete a Process Stage

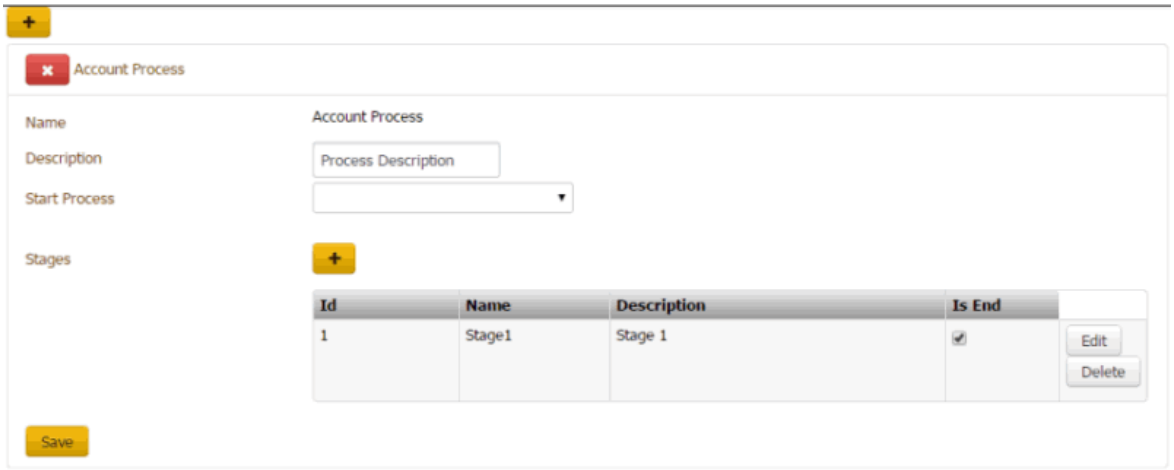
Use the **Process Stages** panel to delete a process stage.

To delete a process stage

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Process Stages**.



2. Click the process from which to delete a stage. The process expands.



3. In the data grid, click **Delete** and then click **OK**.

Queue Levels

Queue Levels

Queue levels manage workflow to ensure the most efficient routing and working of accounts. Every account in Latitude has a queue level. Queue levels change based on account activity or condition. Queue logic doesn't force a queue level change when business logic prevents it. For example, when a user creates a promise payment arrangement on the account, Latitude assigns queue level 820 (future promise). When the credit bureau returns a requested credit report for the account. The queue level remains at 820 instead of changing to 200 (returned with credit report) because the business logic has priority.

Queue level code management

Users with the System Codes and Settings Permission can add, modify, and delete queue level codes. The system reserves queue levels 425-499, 600-699, and 700-799 to allow you to create queues for accounts that require special attention. Though allowed, we don't recommend the following actions without consulting with Latitude by Genesys Support:

- Modifying the descriptions for system- and user-defined queue levels.
- Modifying the "should queue" setting for system- and user-defined queue levels.
- Deleting system- and user-defined queue levels.

Queue level assignment

Automated queue level assignment is based on account activity and condition. When certain events occur or conditions exist on an account, Latitude or Custodian changes the queue level accordingly. For example, when a user sets a follow-up date on an account or a supervisor dismisses an account from the Supervisor queue. Users can move accounts manually to Custom, Clerical, or Supervisor queues. For a list of queue levels and their description, see Queue Level Codes.

Latitude updates some account queue levels immediately while others update during Custodian processing. Your organization can change the queue levels on accounts as needed using Custodian, WorkFlow, Job Manager, Exchange, or an SSIS package. For more information about Custodian; WorkFlow; Job Manager; or Exchange, see the corresponding documentation. If you need assistance, contact Latitude by Genesys Support.

Work queues

There are four work queues in Latitude that are available based on your permissions. Each queue contains accounts assigned to a specific queue level. For more information about working accounts in queues, see Work Queues.

- **Collector queue:** Contains accounts assigned to a queue level that is less than 599.
- **Custom queue:** Contains accounts assigned to queue levels 425-499 that require a specific type of work (for example, skip tracing).
- **Clerical queue:** Contains accounts assigned to queue levels 600-699 that require clerical support (for example, verification of a direct payment).

- **Supervisor queue:** Contains accounts assigned to queue levels 700-799 that require supervisor support (for example, approval of a payment arrangement).

Queue level issues and challenges

Queue levels present certain issues and challenges. For example:

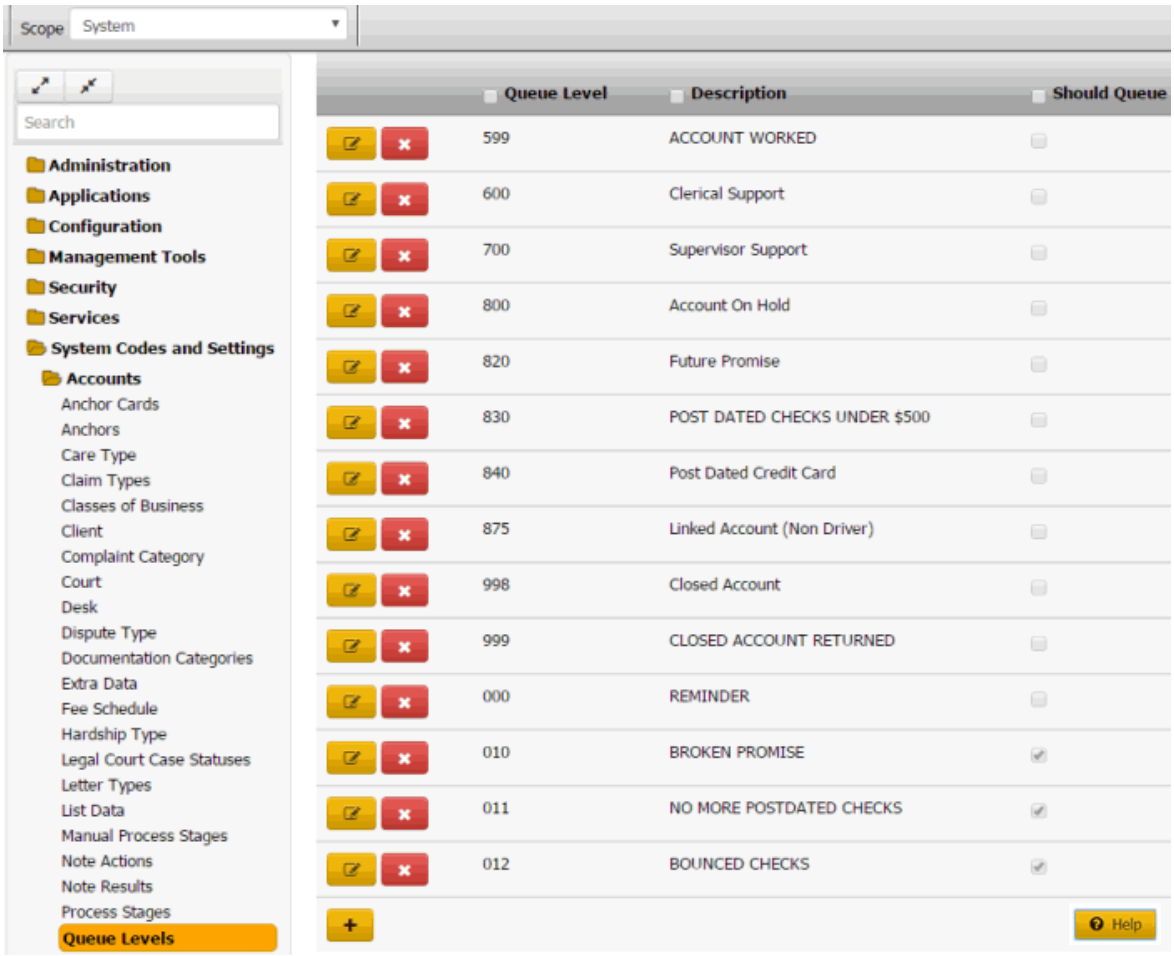
- **Workflow:** Some queue levels determine the workflow priority for presenting accounts to users in work queues. The smaller the queue level number, the higher the priority for working those accounts.
- **Work queues:** Some queue levels identify a group of accounts that require special processing, after-hours work, clerical support, or supervisor support.
- **Immediate assignment:** Latitude assigns accounts to queue levels immediately based on account activities and conditions.
- **Nightly assignment:** Custodian assigns accounts to queue levels during nightly processing when accounts qualify.
- **Planned assignment:** Your organization can change queue level assignments at any time using Custodian, WorkFlow, Job Manager, Exchange, or an SSIS package.
- **User-defined assignment:** Users can assign accounts to user-defined queue levels that define the Custom, Clerical, and Supervisor queues.

Add a Queue Level

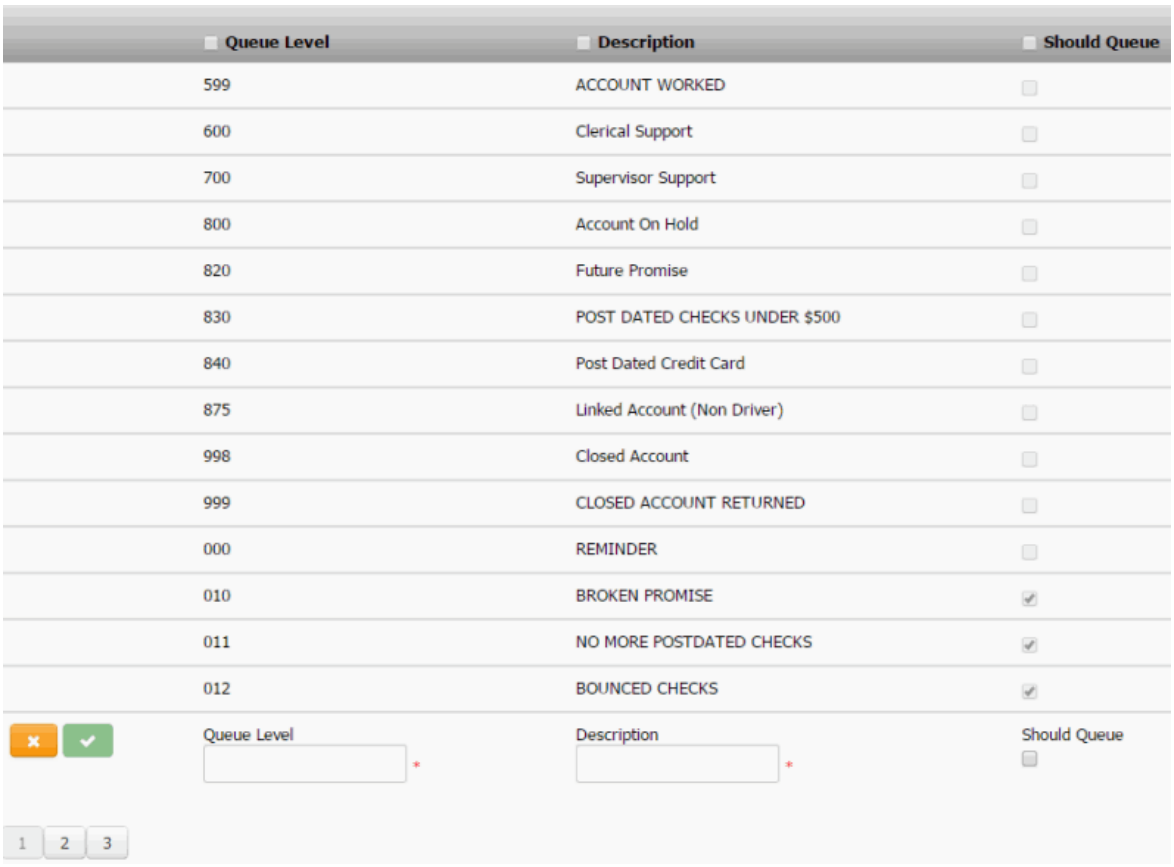
Use the **Queue Levels** panel to add a queue level.

To add a queue level

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Queue Levels**.



2. Click the plus sign (+). A blank row appears in the data grid.



Queue Level	Description	Should Queue
599	ACCOUNT WORKED	☐
600	Clerical Support	☐
700	Supervisor Support	☐
800	Account On Hold	☐
820	Future Promise	☐
830	POST DATED CHECKS UNDER $500	☐
840	Post Dated Credit Card	☐
875	Linked Account (Non Driver)	☐
998	Closed Account	☐
999	CLOSED ACCOUNT RETURNED	☐
000	REMINDER	☐
010	BROKEN PROMISE	☑
011	NO MORE POSTDATED CHECKS	☑
012	BOUNCED CHECKS	☑
✖ ✔	Queue Level *	Description *

1 2 3

Queue Level: Unique three-digit code that identifies the queue level.

Description: Description of the queue.

Should queue: If selected and the queue level is between 600-799 (clerical or supervisor), accounts assigned to this queue appear in the users' queue. If the user has the **Accounts – Change Continue Queuing** permission, you can override this setting when assigning an account to a support queue.

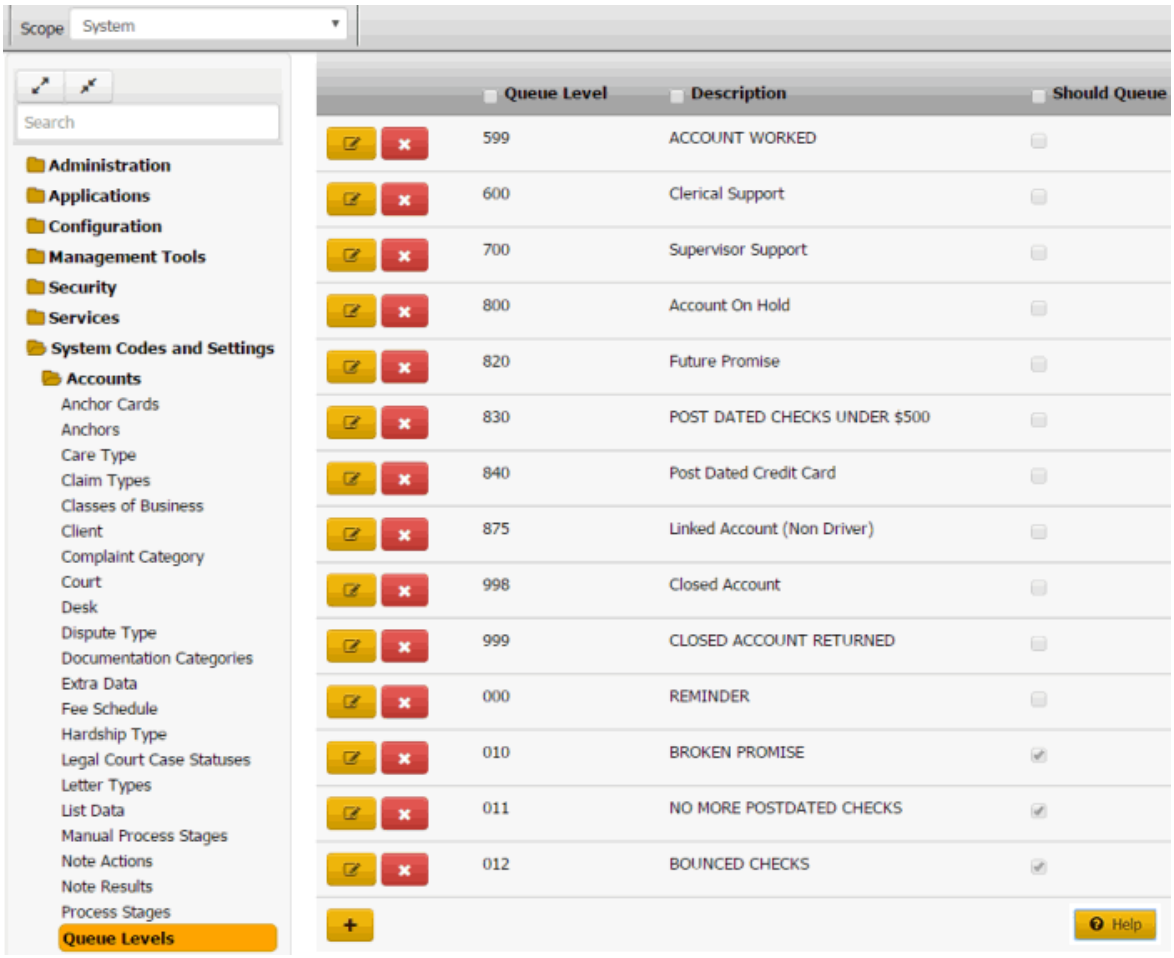
3. Complete the information and then click the check mark.

Modify a Queue Level

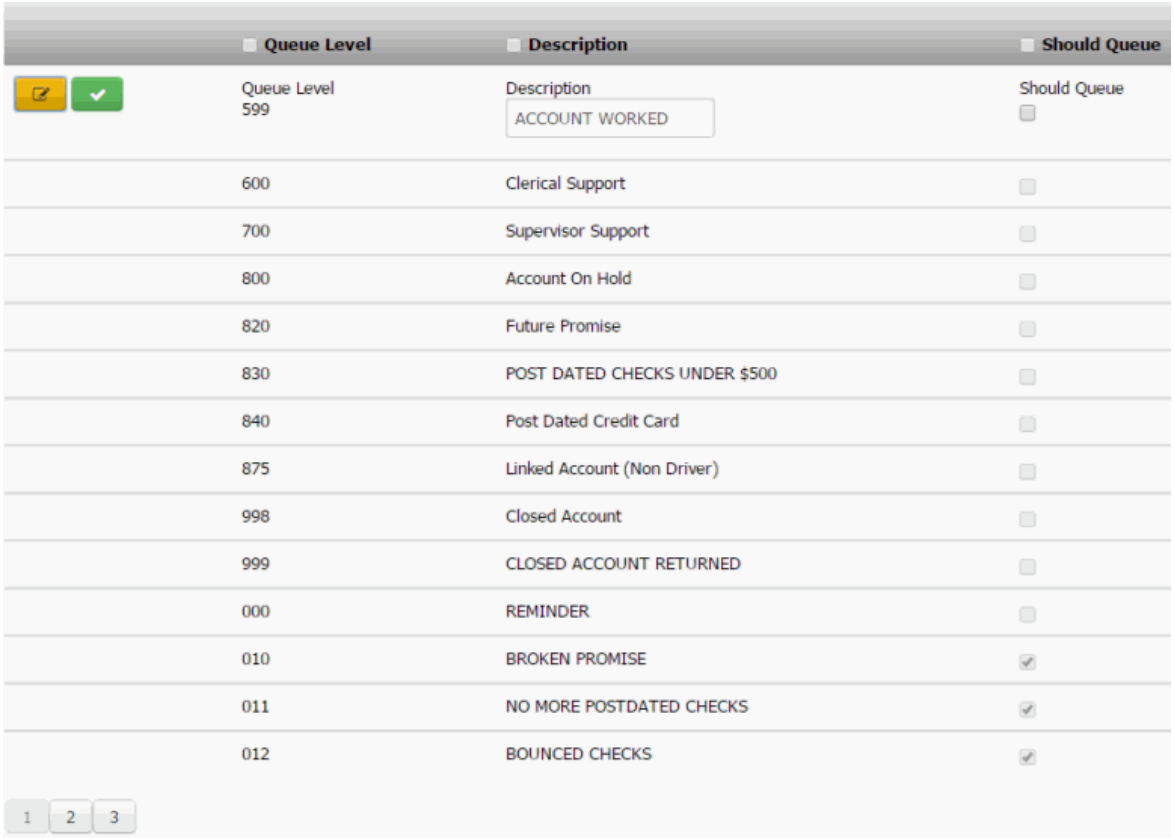
Use the **Queue Levels** panel to modify a queue level.

To modify a queue level

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Queue Levels**.



2. Click the Edit icon. The queue level appears in edit mode.



Queue Level	Description	Should Queue
Queue Level 599	Description ACCOUNT WORKED	Should Queue
600	Clerical Support	
700	Supervisor Support	
800	Account On Hold	
820	Future Promise	
830	POST DATED CHECKS UNDER $500	
840	Post Dated Credit Card	
875	Linked Account (Non Driver)	
998	Closed Account	
999	CLOSED ACCOUNT RETURNED	
000	REMINDER	
010	BROKEN PROMISE	
011	NO MORE POSTDATED CHECKS	
012	BOUNCED CHECKS	

1 2 3

Queue Level: Unique three-digit code that identifies the queue level.

Description: Description of the queue.

Should queue: If selected, accounts assigned to this queue appear in work queues. If the user has the **Accounts – Change Continue Queuing** permission, you can override this setting when assigning an account to a support queue.

3. Modify the information and then click the check mark.

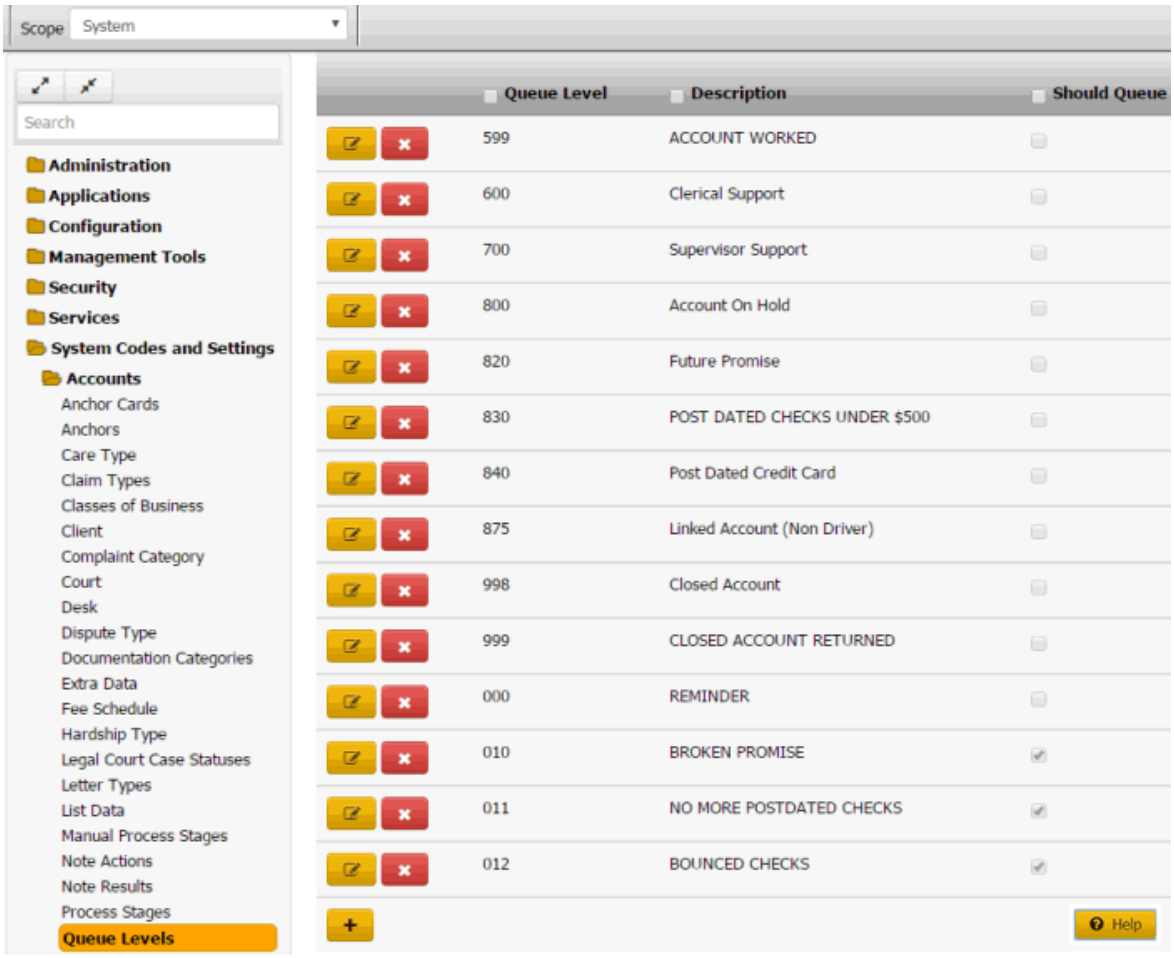
Note: For system-level queues, you cannot modify the code.

Delete a Queue Level

Use the **Queue Levels** panel to delete a queue level code.

To delete a queue level

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Queue Levels**.



2. Click the Delete icon and then click **Yes**.

Queue Level Codes

Latitude releases with several queue level codes, as described in the following table. Most queue levels represent events or conditions that trigger a queue level change. The queue levels flagged with an asterisk (*) in the following table represent repositories for accounts that require special attention.

> **Note:** The names associated to the queue levels may differ, depending on how you or Latitude by Genesys configured your system. The remaining information applies regardless of the queue level name.

Queue Level	Name	Assignment	Queues for Work?	Reassignment
000	Reminder	Latitude assigns this queue level when a user creates a reminder or follow-up on an account.	No	For a follow-up, when a user works the account, Latitude reassigns the account to the queue level that applies based on account activity or condition.

Queue Level	Name	Assignment	Queues for Work?	Reassignment
		Note: If an account has a reminder set, the reminder appears for the desk at the designated date and time. If an account has a follow-up set, the account appears in the **Work Form** on the designated day when a user attempts to move to the next account in a work queue.		For a reminder, when a user dismisses the reminder, Latitude reassigns the account to the queue level that applies based on account activity or condition. **Note:** If a user doesn't dismiss a reminder, accounts can remain at this queue level indefinitely. To avoid or correct this issue, do one of the following: • At the desk level, set the maximum number of days ahead that a user can set a reminder. After the number of days pass and a user hasn't dismissed the reminder, Custodian reassigns the account to the previous queue level. • Use a Custodian task to identify accounts assigned to queue level 000 for more than a specific number of days. Set the task to force dismissal of the reminders and reassign the accounts to the previous queue level. • Use the Account Analysis tool to identify accounts assigned to queue level 000. When users work these accounts, Latitude or Custodian reassigns the accounts to the queue level that applies based on account activity or condition.
010	Broken Promise	Custodian assigns this queue level when an account has a promise arrangement due on the current day but no payment posted to the account. Custodian places future payments on hold.	Yes	After a user receives a payment or negotiates a new payment arrangement, Custodian reassigns the account to the queue level that applies based on account activity or condition. Custodian also removes the hold on future payments.

Queue Level	Name	Assignment	Queues for Work?	Reassignment
		Note: If a grace period exists for the account, Custodian delays assigning this queue level and placing payments on hold until the grace period expires without a payment posting on the account.		
011	No More Postdated Checks	Custodian assigns this queue level when an account completes a post-dated payment arrangement successfully but a balance remains on the account.	Yes	After a user negotiates a new payment arrangement or otherwise works the account, Custodian reassigns the account to the queue level that applies based on account activity or condition.
012	Bounced Checks	Custodian assigns this queue level when an account has a payment reversal because the check bounced and there are no future payments in the arrangement.	Yes	After a user receives payment or negotiates a new payment arrangement, Custodian reassigns the account to the queue level that applies based on account activity or condition.
013	No More Promises	Custodian assigns this queue level when an account completes a promise payment arrangement successfully but a balance remains on the account.	Yes	After a user negotiates a new payment arrangement, Custodian reassigns the account to the queue level that applies based on account activity or condition.
015	New Accounts	Custodian assigns this queue level when you import a new account into Latitude that is either not a linked account or is the link driver. If the new account is not the link driver, Custodian assigns the account to queue level 875.	Yes	If a user accesses but doesn't work the account, Custodian reassigns the account to queue level 016. If a user accesses and works the account, Custodian reassigns the account to queue level 599.
016	NewBiz Followup	Custodian assigns this queue level when a user accesses but doesn't work a new account	Yes	After a user works the account the same day or the set number of days allowed, Custodian reassigns the account to the queue level that applies

Queue Level	Name	Assignment	Queues for Work?	Reassignment
		that is either not a linked account or is the link driver.		based on the account activity or condition. **Note:** If your organization configured the desk to allow users to work a new account for a specific number of days, the account remains at this queue level until that time passes.
018	PDC over $500	Latitude assigns this queue level when an account has a post-dated check or ACH payment arrangement with payments that are $500 or more each.	Yes	After a user contacts the customer regarding the upcoming deduction of funds, Custodian reassigns the account to the queue level that applies based on the account activity or condition.
019	NSF With PDCs	Custodian assigns this queue level when an account has a payment reversal because the check bounced and there are future payments in the payment arrangement. Custodian places the future payments on hold.	Yes	After a user receives a payment or renegotiates the payment arrangement, Custodian reassigns the account to the queue level that applies based on account activity or condition. Custodian also removes the hold on future payments.
020	Accounts 0 - 30 Days Old	Custodian assigns this queue level when an account has been in Latitude less than 31 days since the date received.	Yes	If a user works the account before 30 days pass, Custodian reassigns the account to the queue level that applies based on account activity or condition. If 30 days pass and a user hasn't worked the account, Custodian reassigns the account to queue level 030.
025	Accounts W Payment	No longer in use.	N/A	N/A
030	Accounts 30 – 60 Days Old	Custodian assigns this queue level when an account has been in Latitude between 30 and 60 days since the date received.	Yes	If a user works the account before 60 days pass, Custodian reassigns the account to the queue level that applies based on account activity or condition.

Queue Level	Name	Assignment	Queues for Work?	Reassignment
				If 60 days pass and a user hasn't worked the account, Custodian reassigns the account to queue level 060.
060	Accounts 60 – 90 Days Old	Custodian assigns this queue level when an account has been in Latitude between 60 and 90 days since the date received.	Yes	If a user works the account before 90 days pass, Custodian reassigns the account to the queue level that applies based on account activity or condition. If 90 days pass and a user hasn't worked the account, Custodian reassigns the account to queue level 090.
090	Accounts 90 – 120 Days Old	Custodian assigns this queue level when an account has been in Latitude between 90 and 120 days since the date received.	Yes	If a user works the account before 120 days pass, Custodian reassigns the account to the queue level that applies based on account activity or condition. If 120 days pass and a user hasn't worked the account, Custodian reassigns the account to queue level 120.
100	Account Reassigned	Custodian assigns this queue level when an account that is not new business moves from one desk to another.	Yes	After a user works the account, Custodian reassigns the account to the queue level that applies based on account activity or condition.
120	Over 120 Days Old	Custodian assigns this queue level when an account has been in Latitude for more than 120 days since the date received.	Yes	After a user works the account, Custodian reassigns the account to the queue level that applies based on account activity or condition.
200	Returned With Credit Report	Latitude assigns this queue level when a user receives a requested credit report and adds it to an account.	Yes	After a user updates the account to reflect the information in the credit report, Custodian reassigns the account to the queue level that applies based on account activity or condition.
400*	Late Night Queue (1)	Users assign this queue level initially when an account requires after-hours follow-up. Custodian assigns this queue level when an account reaches	Yes	If a user works the account on the current day, Custodian reassigns the account to the queue level that applies based on account activity or condition.

Queue Level	Name	Assignment	Queues for Work?	Reassignment
		queue level 403 without a user working it.		If a user doesn't work the account on the current day, Custodian reassigns the account to queue level 401.
401*	Late Night Queue (2)	Custodian assigns this queue level when a user didn't work an account while it was at queue level 400.	Yes	If a user works the account on the current day, Custodian reassigns the account to the queue level that applies based on account activity or condition. If a user doesn't work the account on the current day, Custodian reassigns the account to queue level 402.
402*	Late Night Queue (3)	Custodian assigns this queue level when a user didn't work an account while it was at queue level 401.	Yes	If a user works the account on the current day, Custodian reassigns the account to the queue level that applies based on account activity or condition. If a user doesn't work the account on the current day, Custodian reassigns the account to queue level 403.
403*	Late Night Queue (4)	Custodian assigns this queue level when a user didn't work an account while it was at queue level 402.	Yes	If a user works the account on the current day, Custodian reassigns the account to the queue level that applies based on account activity or condition. If a user doesn't work the account on the current day, Custodian assigns the account to queue level 400.
425-499*	Custom Queue Levels	Users can assign accounts to Custom queues. Custom queues are work queues that your organization can create to hold accounts that require special follow-up work (for example, skip tracing; probate activity, bankruptcy). For more information, see Queue Levels.	Yes	After a user removes an account from a Custom queue, Custodian reassigns the account to the queue level that applies based on account activity or condition.

Queue Level	Name	Assignment	Queues for Work?	Reassignment
599	Account Worked	Latitude assigns this queue level when a user works an account on the current day.	No	Accounts remain at this queue level until the end of the day to ensure compliance with Federal and State collection laws. Custodian reassigns the account to the queue level that applies based on account activity or condition.
600-699*	Clerical Support	Users and Latitude can assign accounts to Clerical queues. For example, when a user requests a letter for an account and the user doesn't have permissions to print letters, Latitude assigns the account to a Clerical queue. Clerical queues are work queues that your organization can create to hold accounts that require clerical support (for example, direct payment verification with a customer). For more information, see Queue Levels.	Yes	After a user removes an account from a Clerical queue, Custodian reassigns the account to the queue level that applies based on account activity or condition.
700-799*	Supervisor Support	Users and Latitude can assign accounts to Supervisor queues. For example, when a user creates a payment arrangement on an account but doesn't have permissions to approve payment arrangements, Latitude assigns the account to a Supervisor queue. Supervisor queues are work queues that organization can create to hold accounts that require supervisor action (for example, payment arrangement approval). For more information, see Queue Levels.	Yes	After a user removes an account from a Supervisor queue, Custodian reassigns the account to the queue level that applies based on account activity or condition.

Queue Level	Name	Assignment	Queues for Work?	Reassignment
800	Account on Hold	Latitude assigns this queue level when an account has a customer-level or account-level hold.	No	After a user or Latitude removes the hold on the account, Custodian reassigns the account to the queue level that applies based on account activity or condition.
820	Future Promise	Latitude assigns this queue level when an account has a new promise payment arrangement.	No	When Custodian identifies a broken or complete payment arrangement, Custodian reassigns the account to the queue level that applies based on account activity or condition.
830	Post-dated Checks Under $500	Latitude assigns this queue level when an account has a post-dated check or ACH payment arrangement with payments that are less than $500 each.	No	When Custodian identifies a broken or complete payment arrangement, Custodian reassigns the account to the queue level that applies based on account activity or condition.
840	Post-dated Credit Card	Latitude assigns this queue level when an account has a post-dated credit card payment arrangement with payments that are less than $500 each.	No	When Custodian identifies a broken or complete payment arrangement, Custodian reassigns the account to the queue level that applies based on account activity or condition.
875	Linked Account (Non Driver)	Custodian assigns this queue level when an account is a linked account but isn't the link driver account. Users work these accounts when the link driver account queues for work.	No	If Custodian identifies the account as closed, Custodian reassigns the account to queue level 998. If Custodian identifies the account as closed and returned, Custodian reassigns the account to queue level 999.
998	Closed Account	Latitude assigns this queue level when an account has a closed status.	No	If Custodian identifies the account as closed and returned, Custodian reassigns the account to queue level 999.
999	Closed Account Returned	Latitude assigns this queue level when an account has a closed and returned status.	No	If a user reopens the account, Custodian reassigns the account to the queue level that applies based on account activity or condition.

Responsible Party Codes

Responsible Party Codes

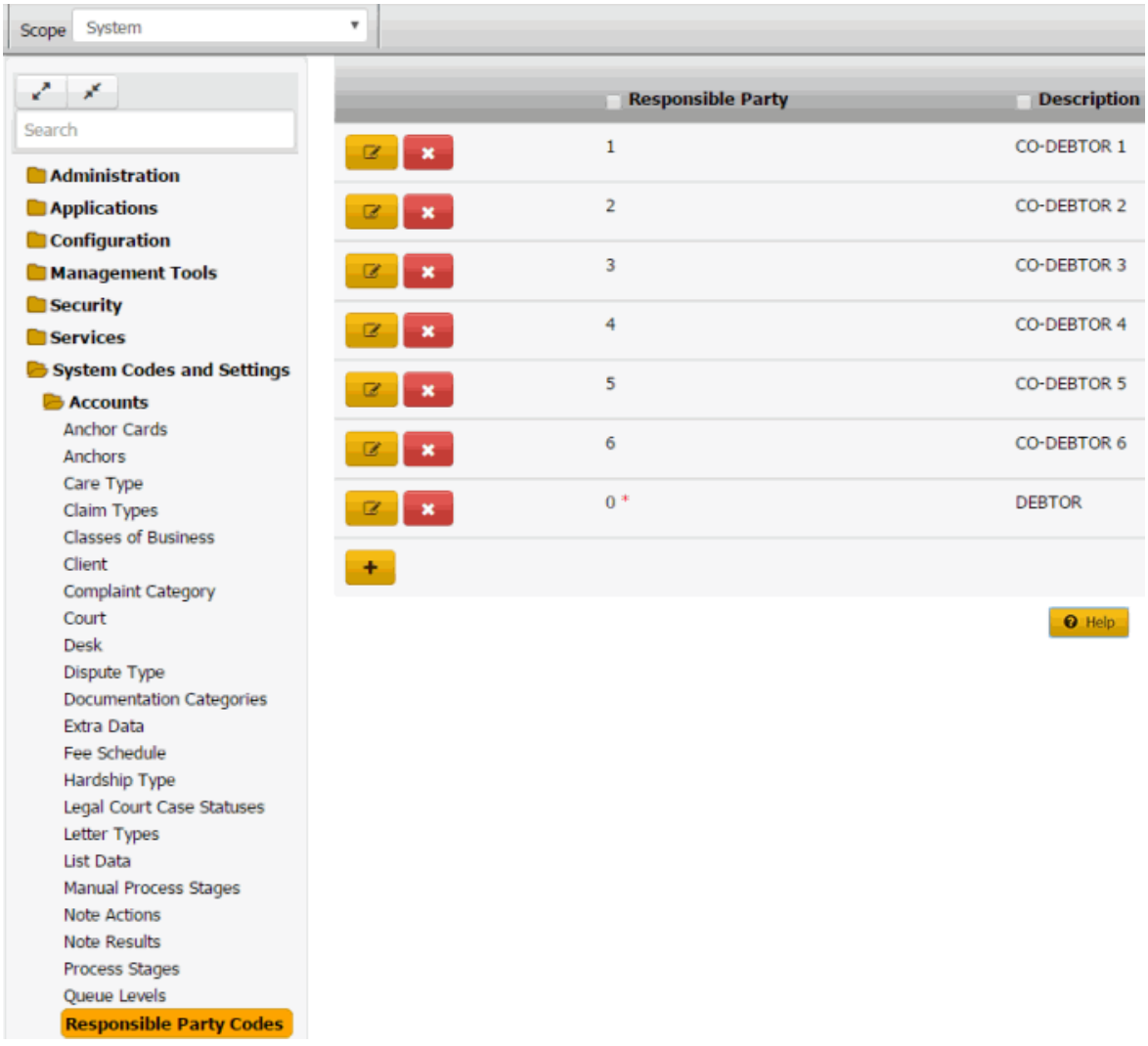
You can search for, add, modify, and delete responsible party codes that represent the relation of a party to an account (for example, co-debtor). Your organization can set up an unlimited number of responsible party codes, and record separate demographic information for each party associated to an account. Users specify a responsible party code when adding a party to an account. For more information, see Add a Party to an Account.

Add a Responsible Party Code

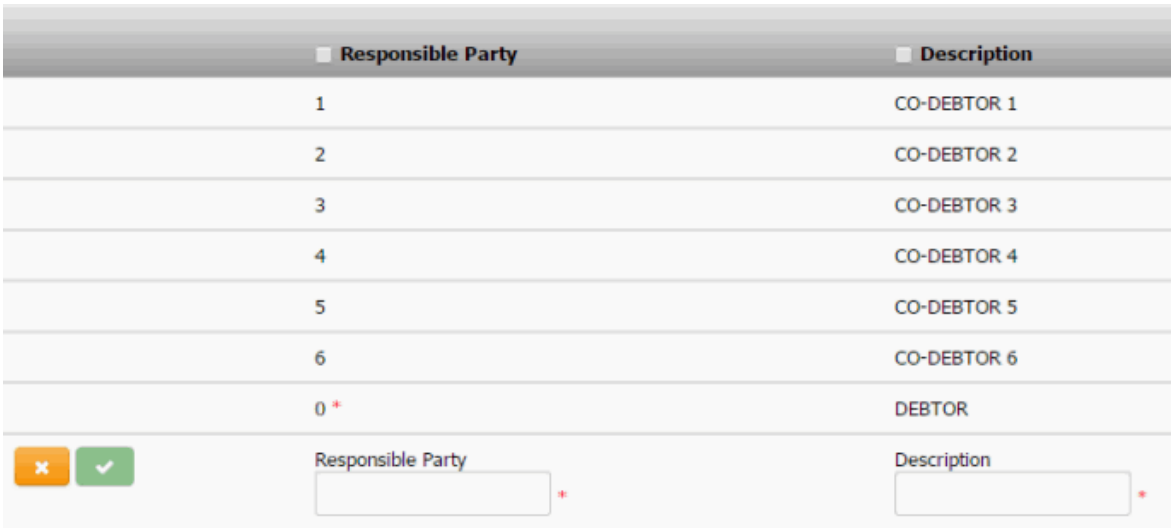
Use the **Responsible Party Codes** panel to add a responsible party code.

To add a responsible party code

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Responsible Party Codes**.



2. Click the plus sign (+). A blank row appears in the data grid.



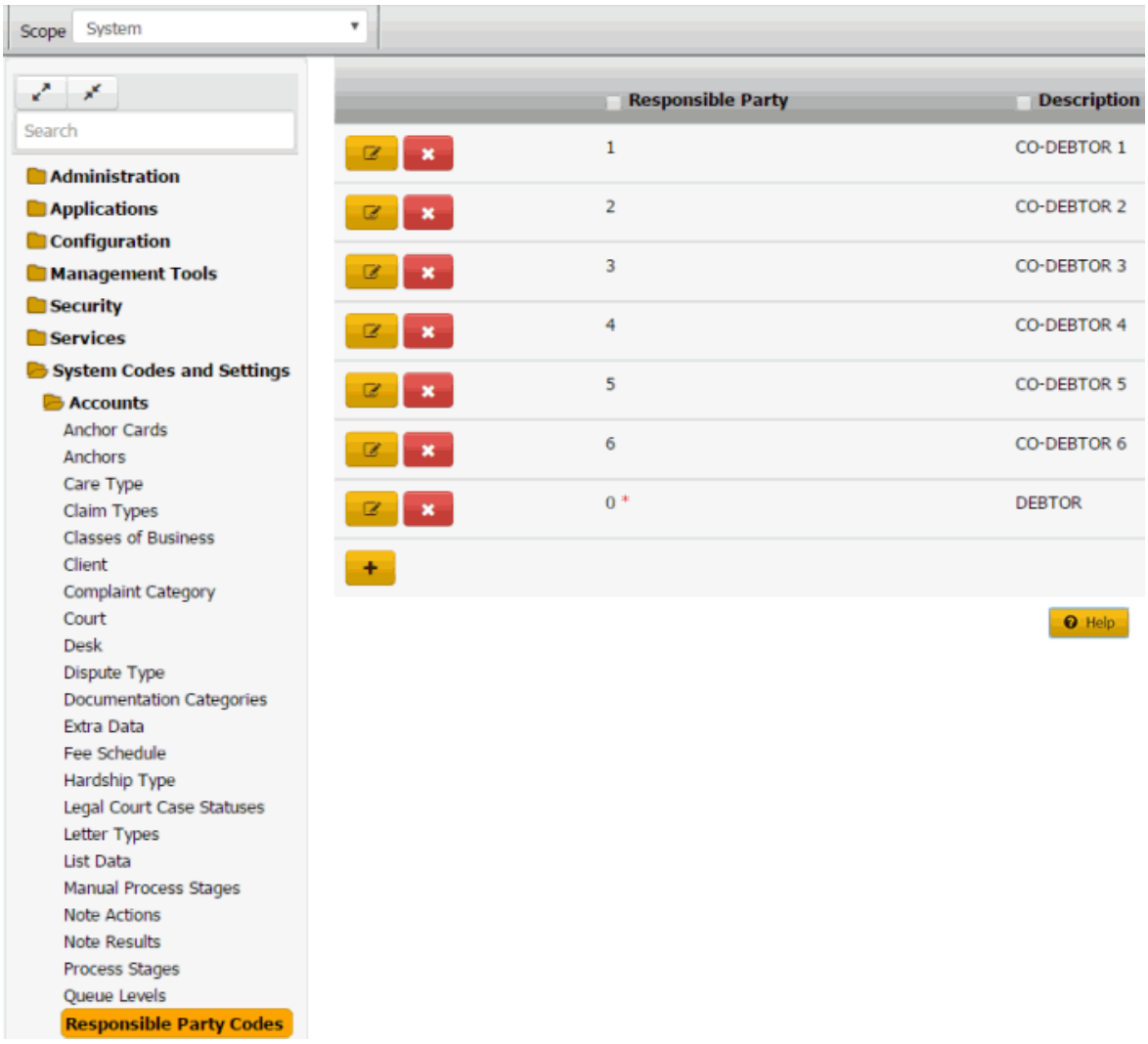
3. In the **Code** box, type a unique code for the responsible party code.
4. In the **Description** box, type a description of the responsible party code.
5. Click the check mark.

Modify a Responsible Party Code

Use the **Responsible Party Codes** panel to modify a responsible party code.

To modify a responsible party code

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Responsible Party Codes**.



2. Click the Edit icon. The responsible party code appears in edit mode.

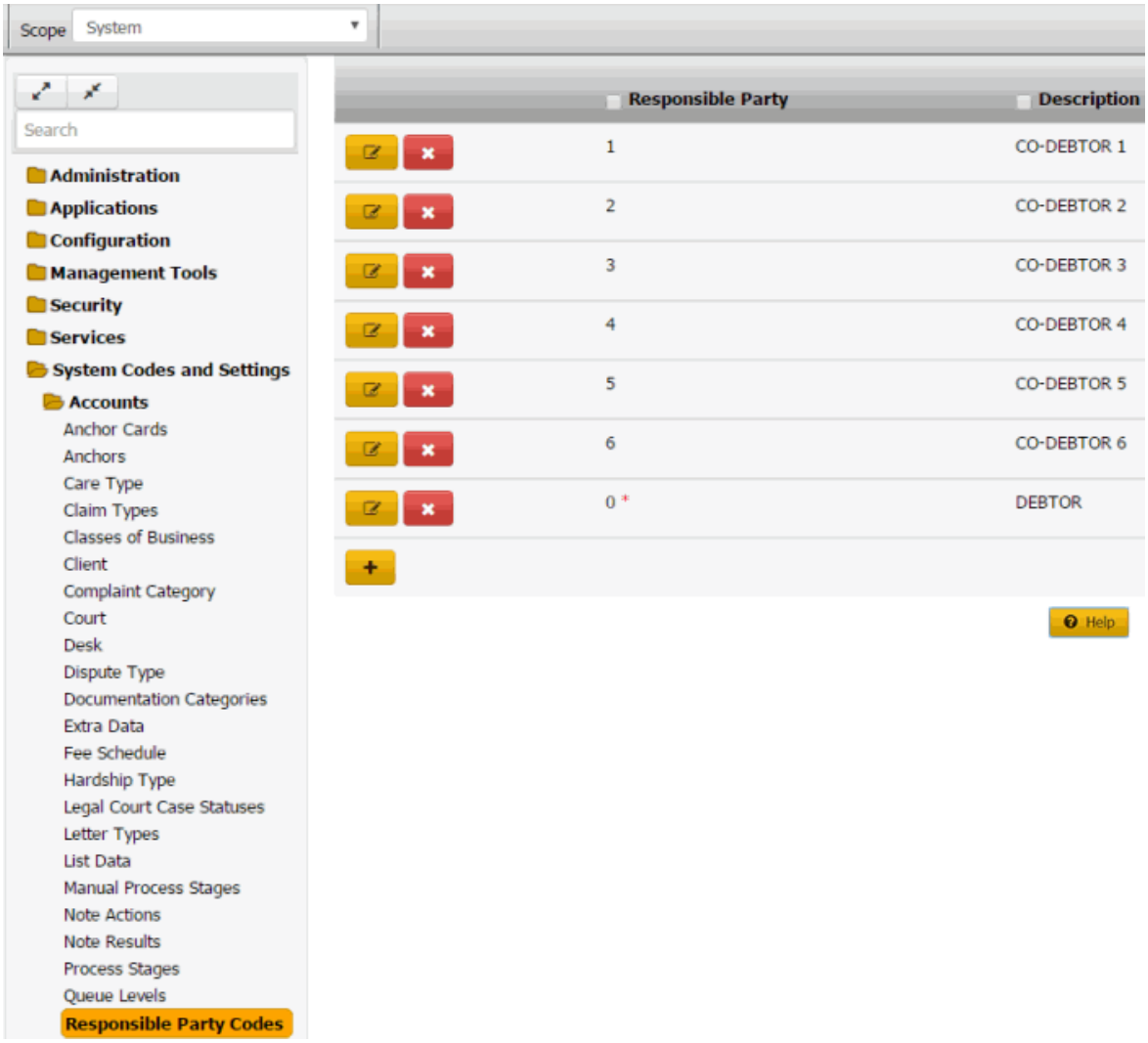
3. Modify the information and then click the check mark.

Delete a Responsible Party Code

Use the **Responsible Party Codes** panel to delete a responsible party code.

To delete a responsible party code

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Responsible Party Codes**.



2. Click the Delete icon and then click **Yes**.

Status Codes

Status Codes

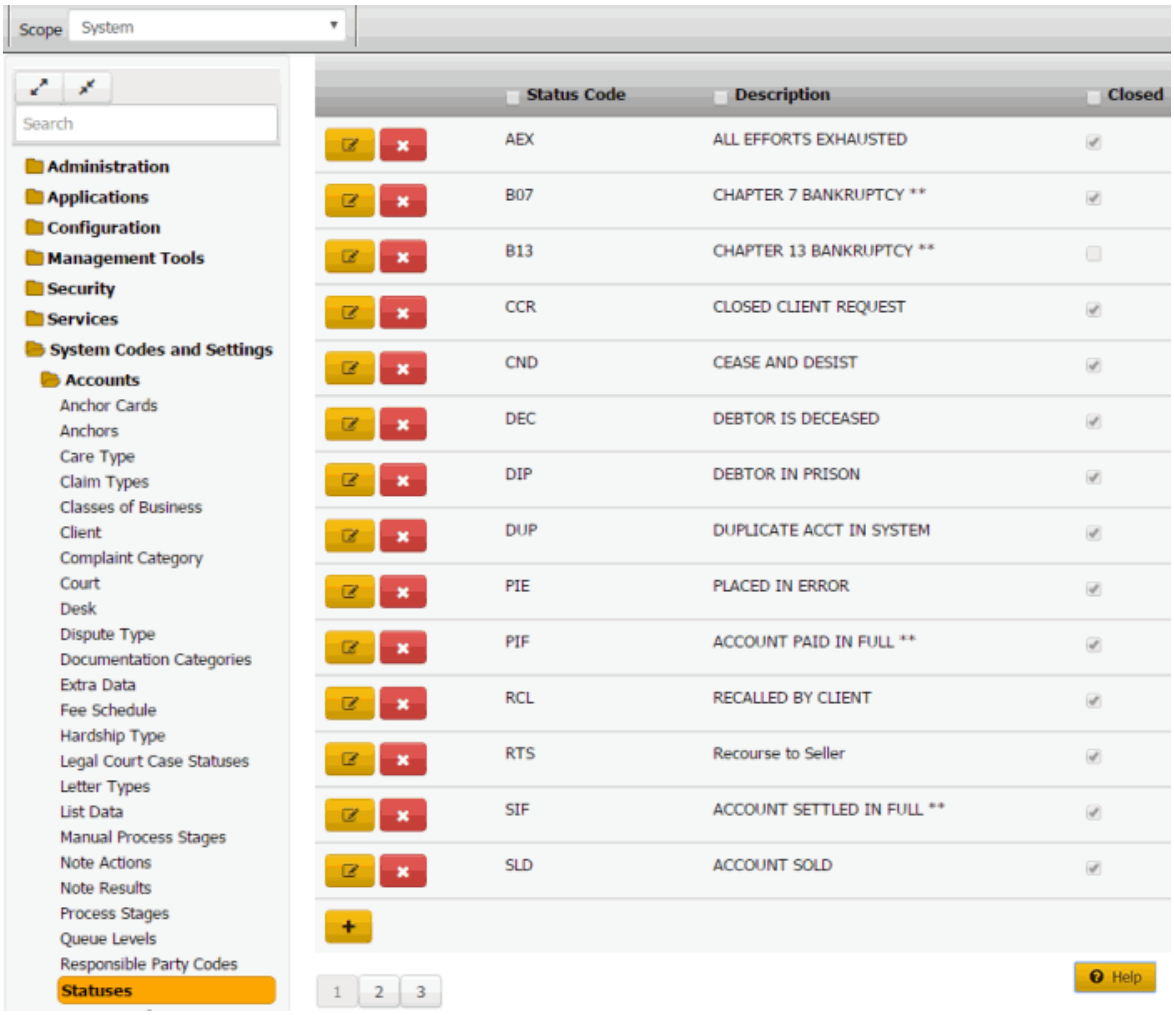
You can search for, add, modify, and delete status codes. Status codes represent the state of an account and whether it is active or closed. Latitude releases with several standard status codes.

Add a Status Code

Use the **Status** dialog box to add a status code.

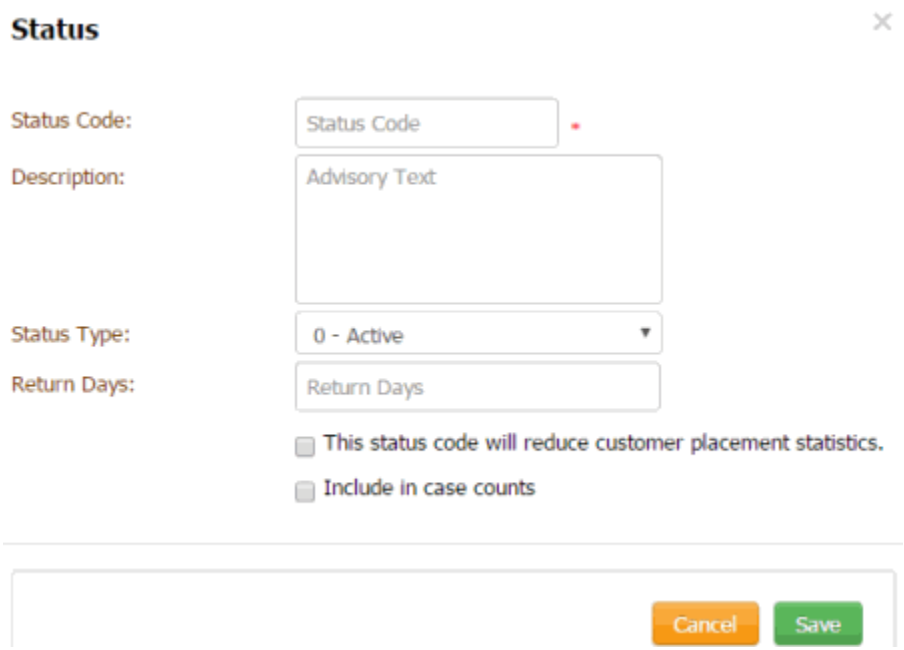
To add a status code

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Statuses**.



1.

2. Click the plus sign (+). The **Status** dialog box appears.



Status Code: Unique code that identifies the status.

Description: Description of the status.

Status Type: Type of status that the status code applies to, such as active or closed. Accounts with a closed status type code don't appear in work queues.

Return Days: Number of days to hold an account assigned to this status before returning the account to the customer.

This status code will reduce customer placement statistics: If selected, Latitude excludes accounts assigned to this status code from customer account placement statistics.

Include in case counts: If selected, the Desk Mover program includes accounts in this status when determining whether the case count exceeds the case limit set for the desk.

> **Note:** To configure credit bureau reporting options for a status code, use Credit Bureau Reporting Console. For more information, see the *Credit Bureau Reporting Console* documentation.

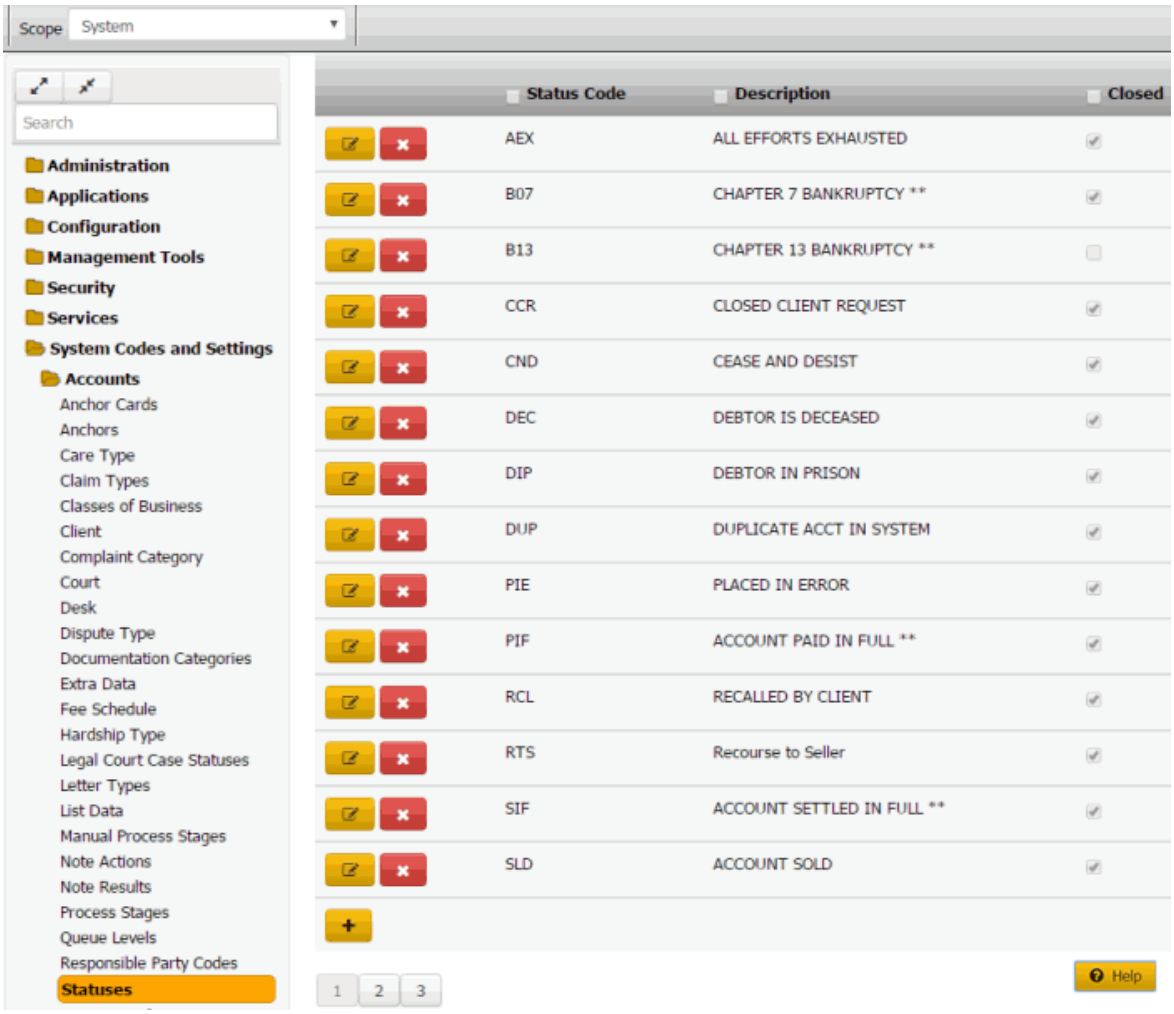
3. Complete the information and then click **Save**.

Modify a Status Code

Use the **Status** dialog box to modify a status code.

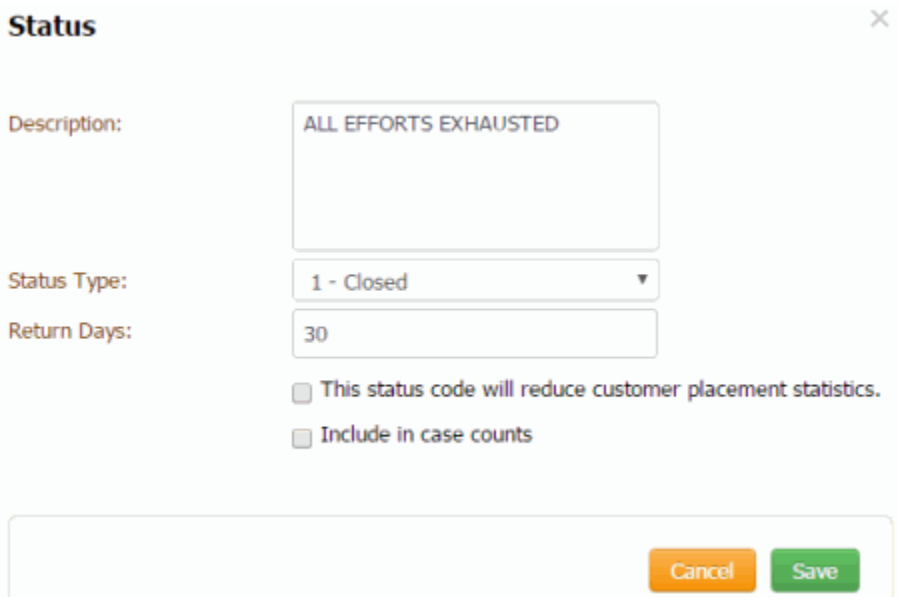
To modify a status code

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Statuses**.



1.

2. Click the Edit icon. The status code appears in edit mode.



Description: Description of the status.

Status Type: Type of status that the status code applies to, such as active or closed. Accounts with a closed status type code don't appear in work queues.

Return Days: Number of days to hold an account assigned to this status before returning the account to the customer.

This status code will reduce customer placement statistics: If selected, Latitude excludes accounts assigned to this status code from customer account placement statistics.

Include in case counts: If selected, the Desk Mover program includes accounts in this status when determining whether the case count exceeds the case limit set for the desk.

> **Note:** To configure credit bureau reporting options for a status code, use Credit Bureau Reporting Console. For more information, see the *Credit Bureau Reporting Console* documentation.

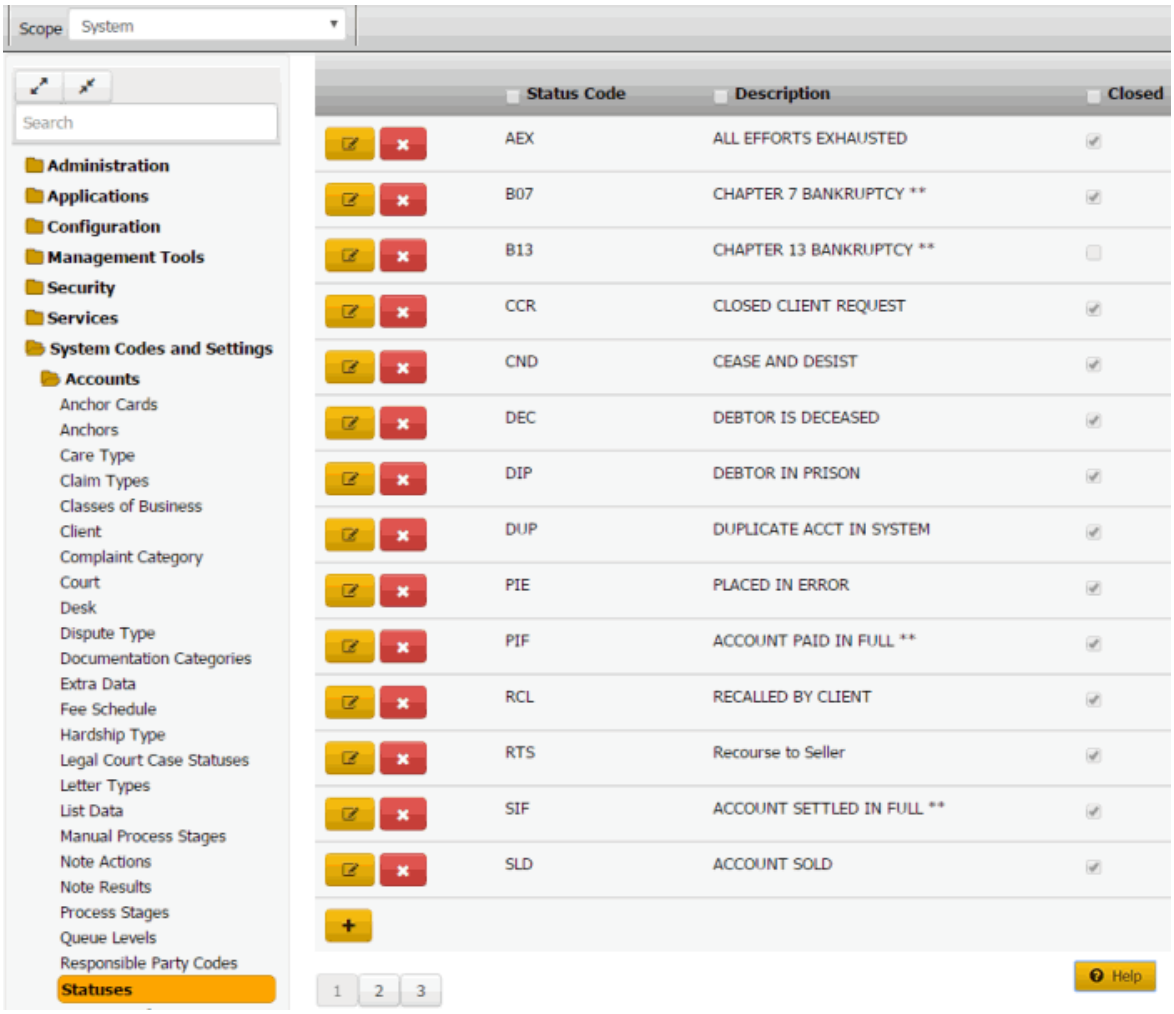
3. Modify the information and then click **Save**.

Delete a Status Code

Use the **Statuses** panel to delete a status code.

To delete a status code

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **Statuses**.



2. Click the Delete icon and then click **Yes**.

System Configuration

System Configuration

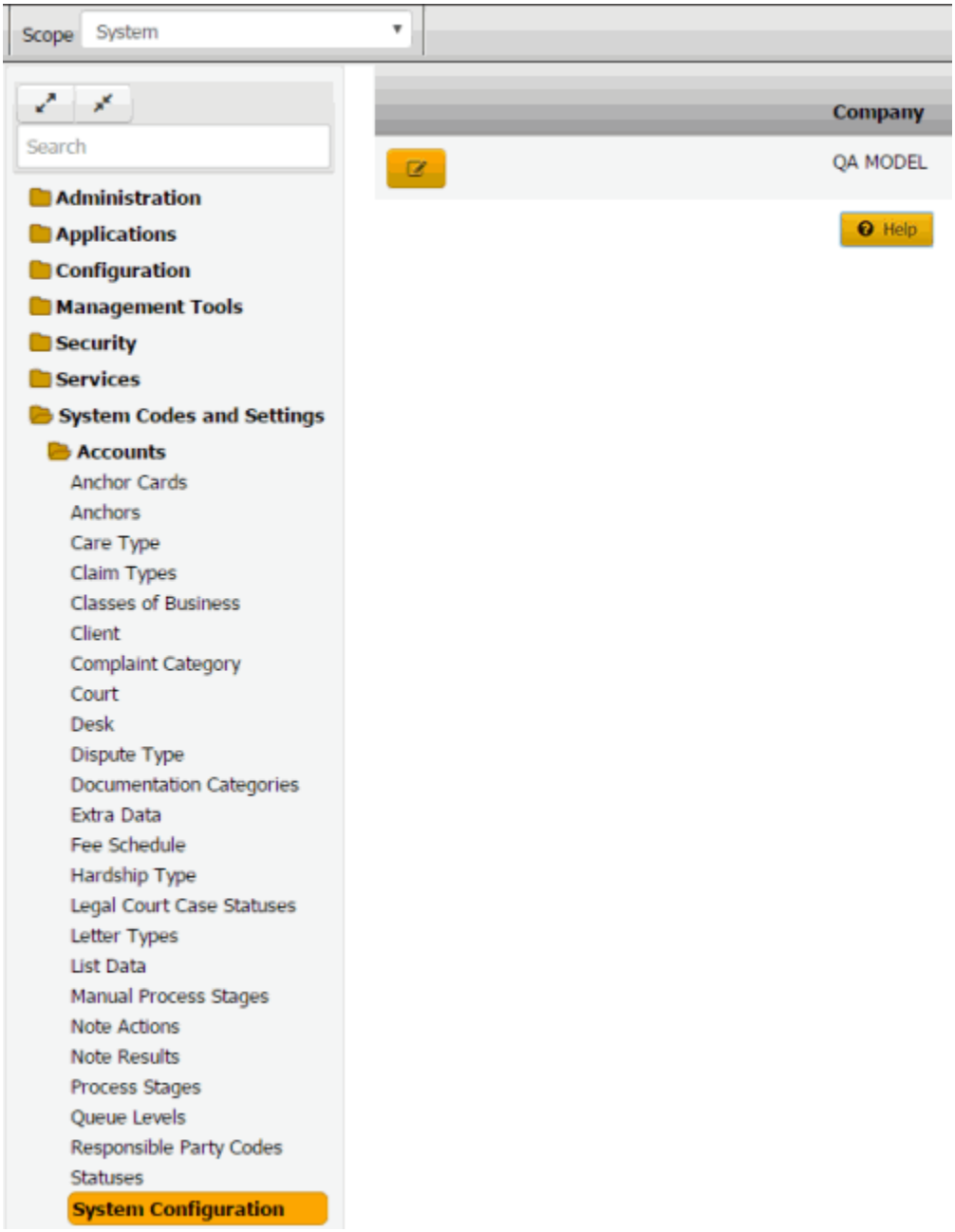
You can view and maintain settings for your organization that apply globally across Latitude. These settings include company information, money titles, letter defaults, system settings, account titles, client titles, file paths, and miscellaneous settings. You must have the System Configuration Permission to modify the settings.

Maintain Company Information

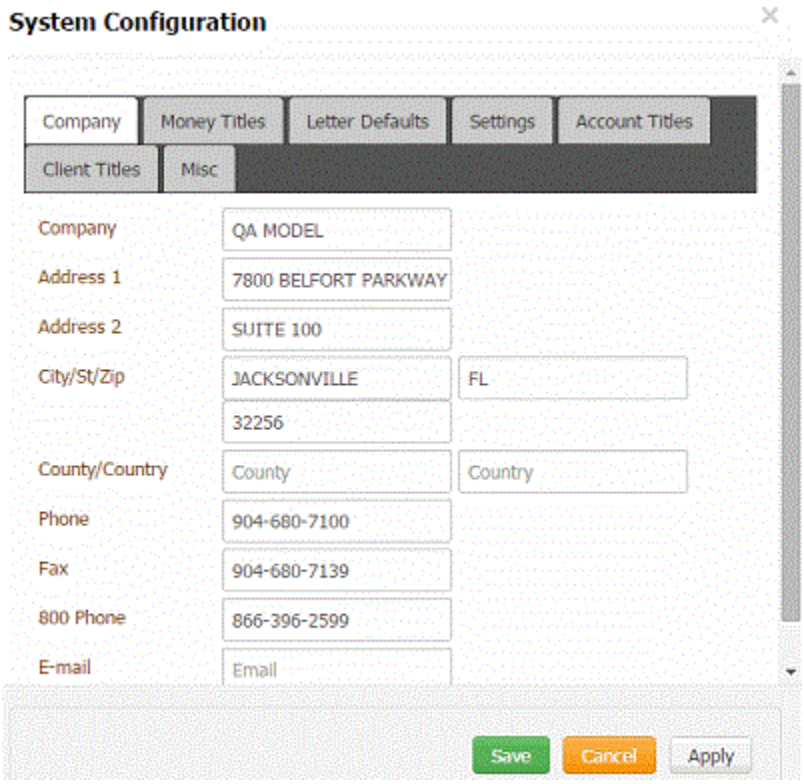
Use the **Company** tab to maintain information about your organization.

To maintain company information

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **System Configuration**.



2. Click the Edit icon and then click the **Company** tab.



Company: Name of your organization.

Address 1: First line of your organization's street address.

Address 2: Second line of your organization's street address.

City/State/ZIP: Your organization's city, state, and postal code.

County/Country: Your organization's county and country.

Phone: Your organization's phone number.

Fax: Your organization's fax number.

800 Phone: Your organization's 1-800 phone number.

Email: Your organization's email address.

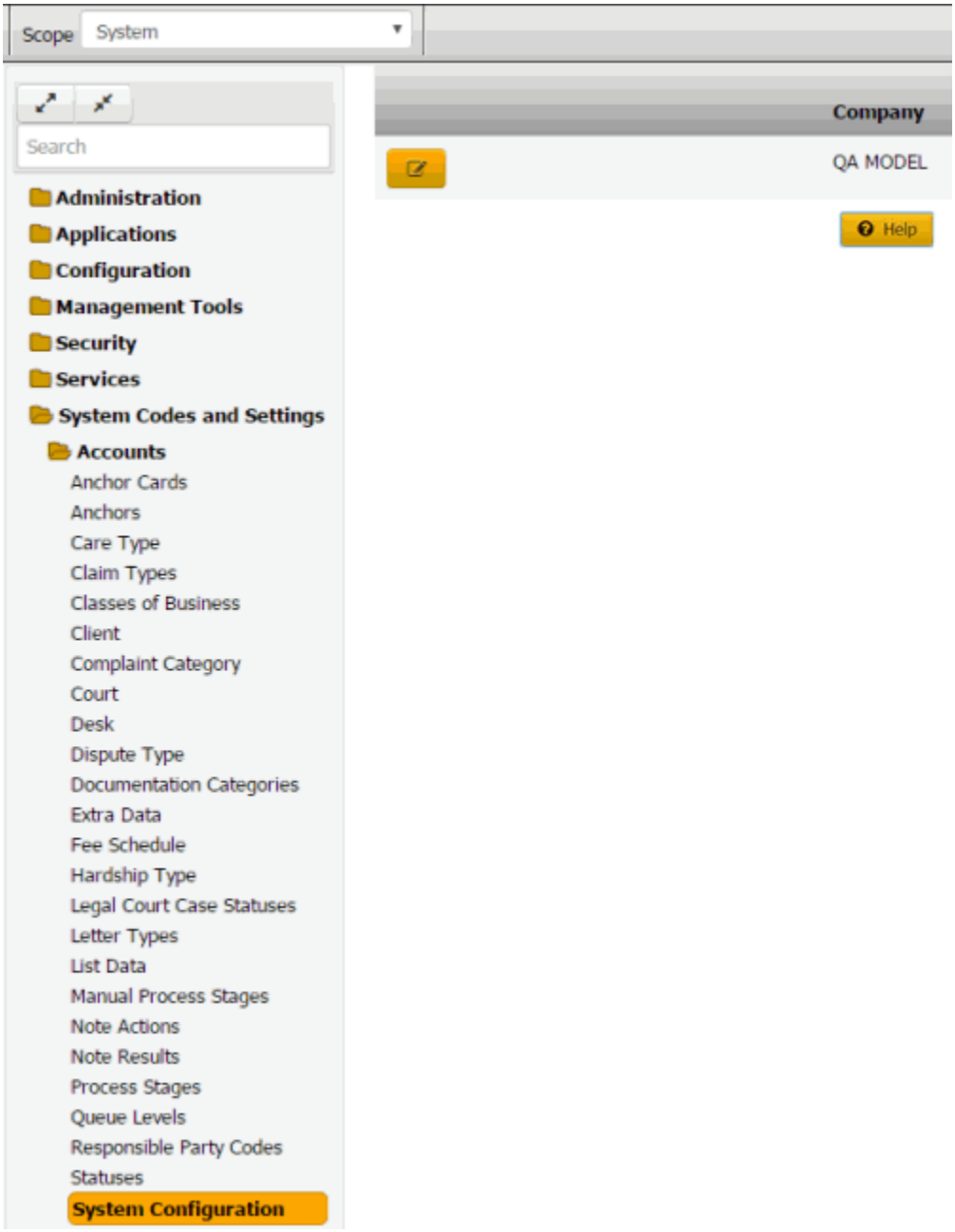
3. Complete the information and then click **Save**.

Maintain Money Titles

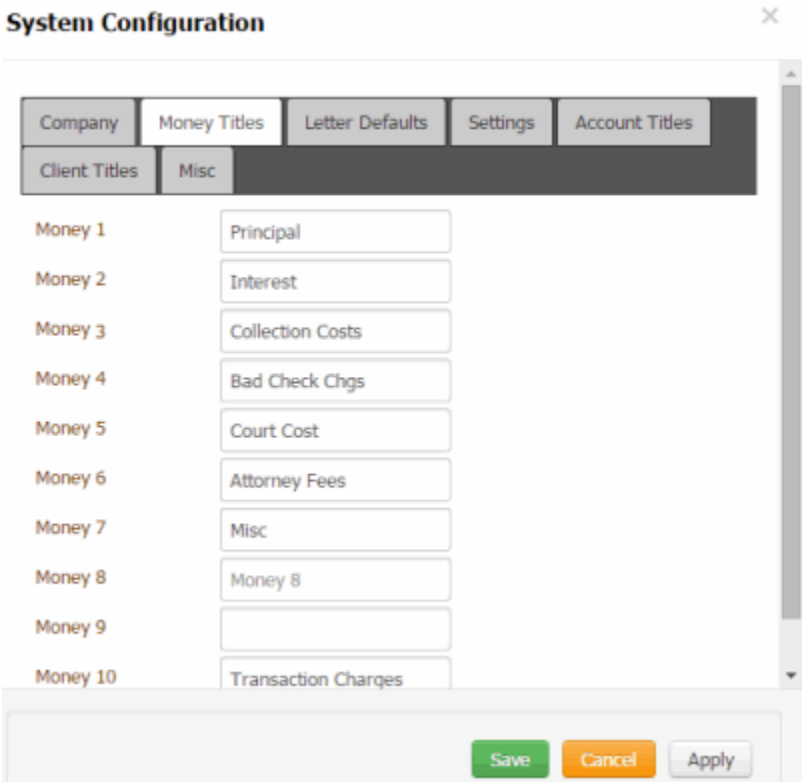
Use the **Money Titles** tab to specify labels for the money buckets that store money amounts for accounts.

To maintain money titles

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **System Configuration**.



2. Click the Edit icon and then click the **Money Titles** tab.



Money 1: Latitude reserves this money bucket for principal.

Money 2: Latitude reserves this money bucket for interest.

Money 10: Latitude reserves this money bucket for transaction charges.

Money 3 through **Money 9:** You can use these money buckets to store whatever money amounts you want. The values you provide in these boxes become the labels for these amounts when they appear in other areas of the system (for example, the **Balance Details** panel).

3. Add up to seven labels and then click **Save**.

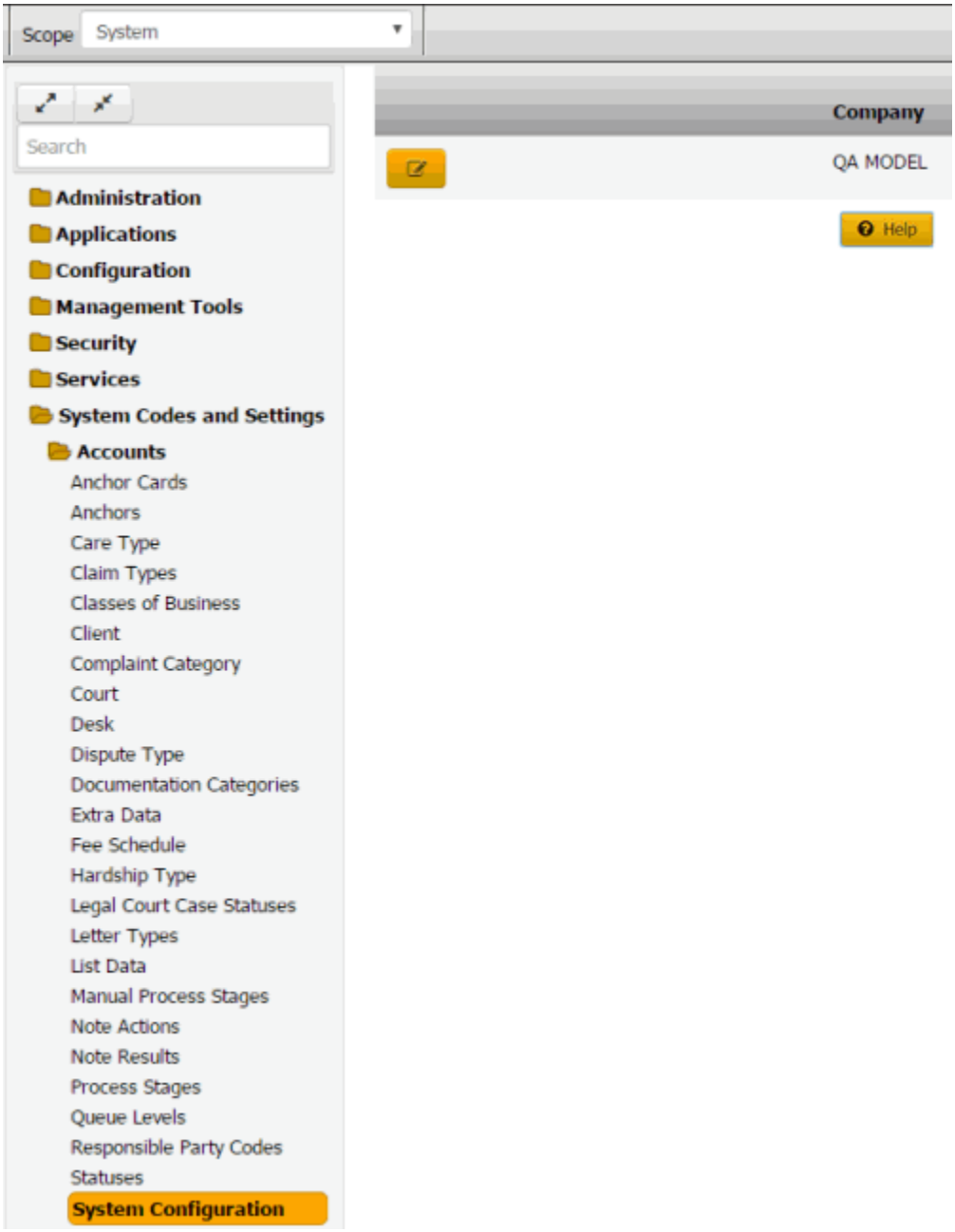
> **Note**: We recommend that you don't change the money buckets after you set them up and add accounts to Latitude.

Maintain Letter Defaults

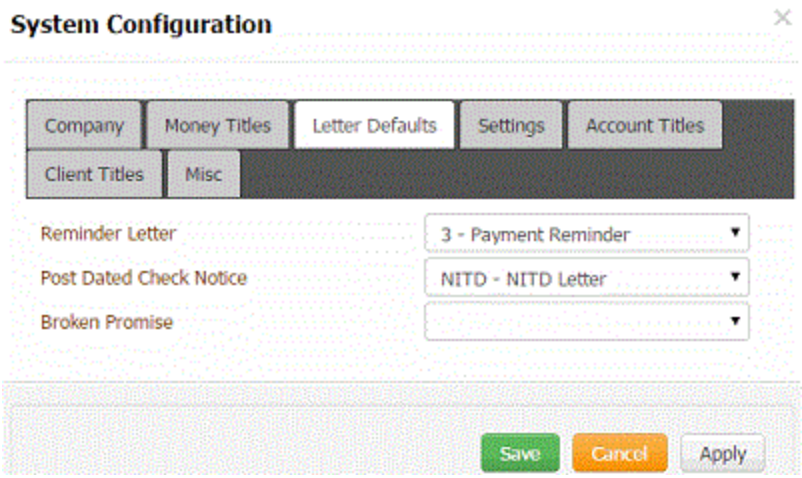
Use the **Letter Defaults** tab to specify the default letter to generate for specific transactions. You generate letters using Letter Console. For more information about Letter Console, see the *Letter Console* documentation.

To maintain letter defaults

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **System Configuration**.



2. Click the Edit icon and then click the **Letter Defaults** tab.



Reminder Letter: Letter to remind customers of their payment promise due date and amount due. Latitude generates this letter when a user adds a promise to an account.

Post Dated Check Notice: Letter to notify the customer of the deposit date. Latitude generates this letter when a user adds a post-dated check or credit card payment to an account.

Broken Promise: Letter to notify the customer that the date they promised to pay has passed. Latitude generates this letter when a promise becomes past due without receiving a payment.

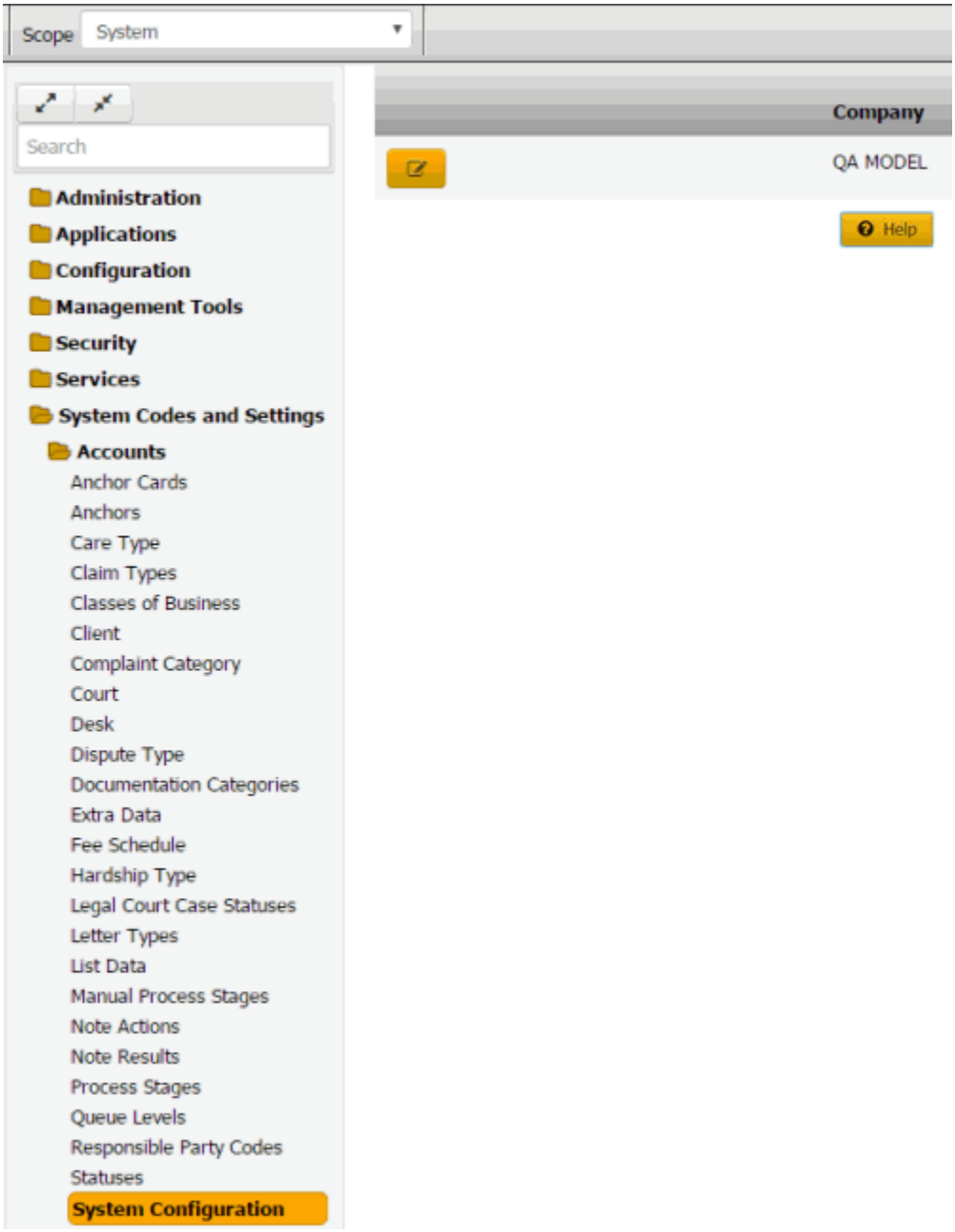
3. Complete the information and then click **Save**.

Maintain System Settings

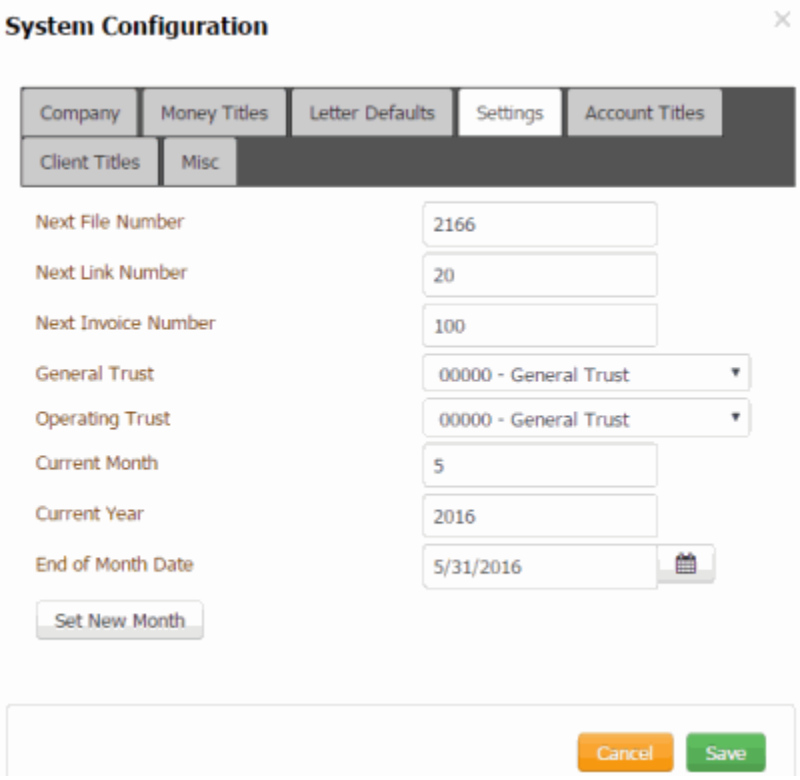
Use the **Settings** tab to specify system-wide default settings.

To maintain system settings

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **System Configuration**.



2. Click the Edit icon and then click the **Settings** tab.



Next File Number: Unique number to assign to the next new account. Latitude assigns the next sequential file number to each account added thereafter. We recommend that you don't change this number after importing accounts initially.

Next Link Number: Unique number to assign to the next link created. A link number identifies a group of linked accounts. Latitude assigns the next sequential link number to each link created thereafter.

Next Invoice Number: Unique number to assign to the next invoice generated using the Invoices program. Latitude assigns the next sequential invoice number to each invoice created thereafter.

General Trust: Account used for deposits when the customer doesn't have a trust account assigned. The account assigned as the General Trust account initially (upon upgrade or conversion) is the bank account with the lowest code number assigned.

Operating Trust: Account used for transaction surcharge deposits. You can use the same bank as the General Trust account. The account assigned initially (upon upgrade) is the bank account with the lowest code number assigned.

Current Month: Current processing month for Latitude. Only change the month using this list box during system implementation or when directed by Latitude by Genesys Support. All other times, click **Set New Month** instead.

Current Year: Current processing year for Latitude. Only change the year using this list box during system implementation or when directed by Latitude by Genesys Support. All other times, click **Set New Month** instead.

End of Month Date: Last posting day for the current month. This date isn't necessarily the last calendar day of the month.

Set New Month: Advances the accounting period to the next month and, if applicable, year.

> **Note**: Process payments, adjustments, invoices, new business imports, and reports for the current month and year before changing the accounting period. For example, you can process June business in July as long as you haven't changed the accounting period to July.

3. To set the next accounting period after your organization has completed monthly processing, do the following:

a. Click **Set New Month** and in the confirmation dialog box, click **Yes**. Latitude advances the current month to the next month. If it's the end of the year, Latitude advances the current year to the next year.

b. Verify the end of month date. If the date is incorrect, in the **End Of Month Date** box, type or click the correct date.

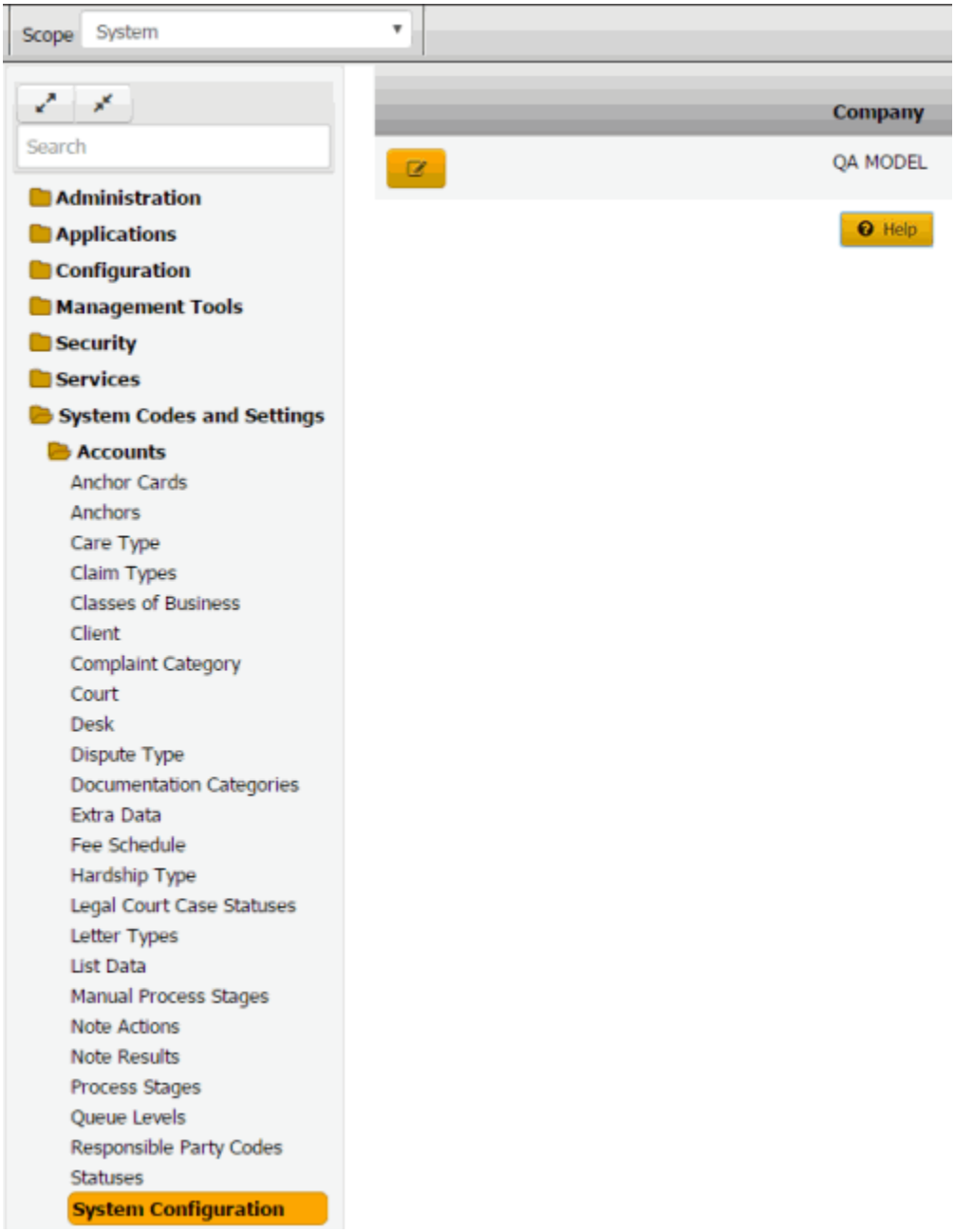
4. Complete the information in the dialog box and then click **Save**.

Maintain Account Titles

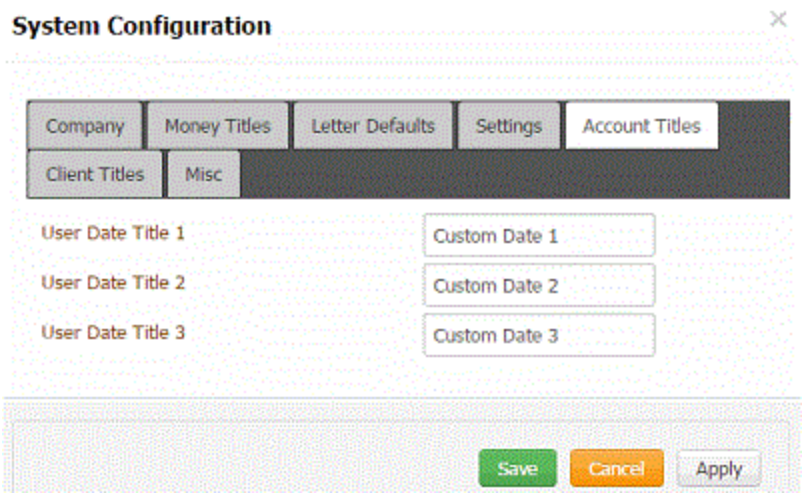
Use the **Account Titles** tab to specify labels for miscellaneous dates you want to record on accounts.

To maintain account titles

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **System Configuration**.



2. Click the Edit icon and then click the **Account Titles** tab.



User Date Title 1 through **User Date Title 3:** The values you provide in these boxes become the labels for dates you want to appear on the **Account Dates** panel. For example, if you type "Date First Billed" in the **User Date Title 1** box, "Date First Billed" appears as a label next to an input box on the **Account Dates** panel. For more information, see View or Modify Account Dates.

3. Add up to three labels and then click **OK**.

Client Titles

Client Titles

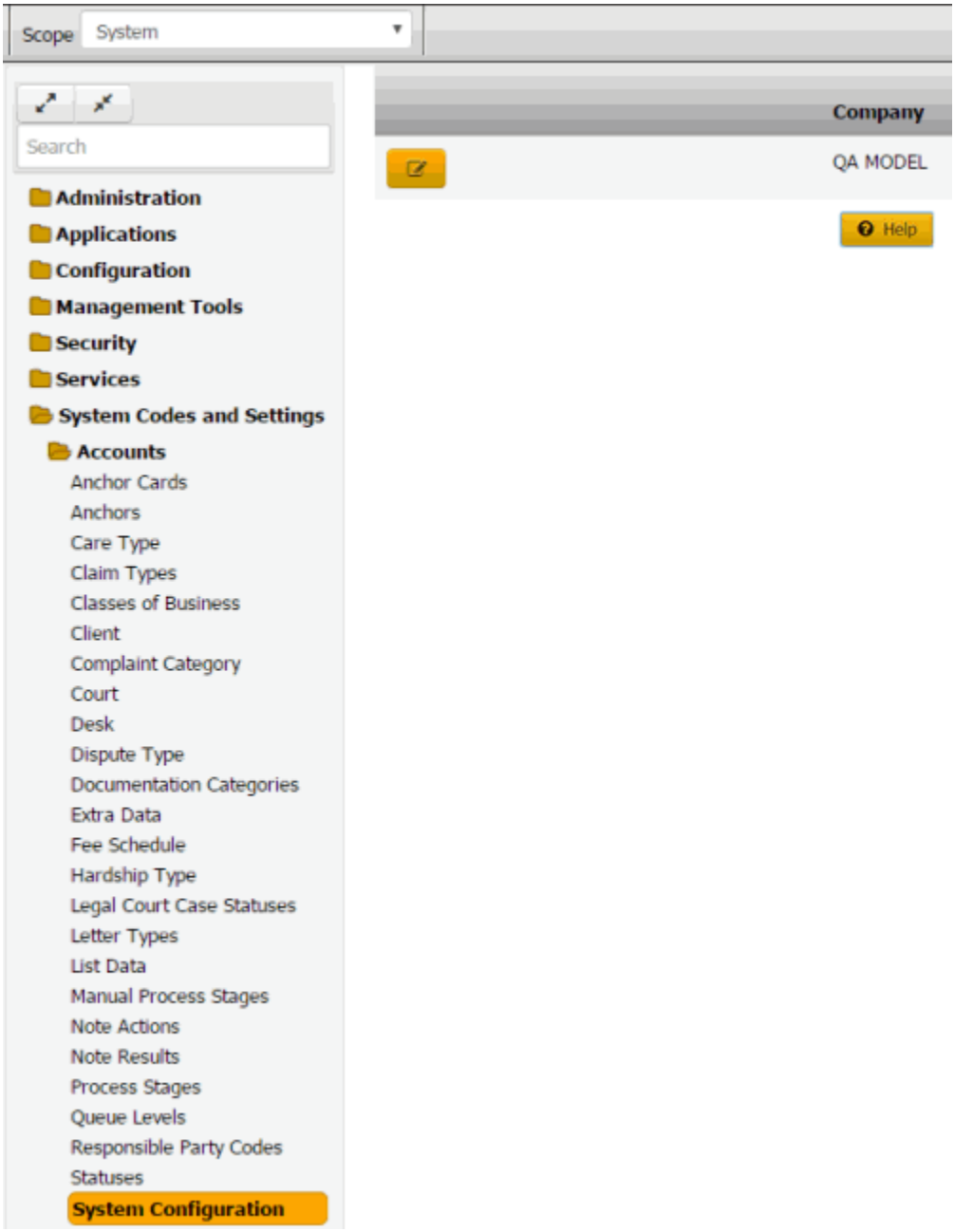
You can specify labels for data that you want users to record when adding or modifying clients. For more information, see Custom Data.

Maintain Client Date Titles

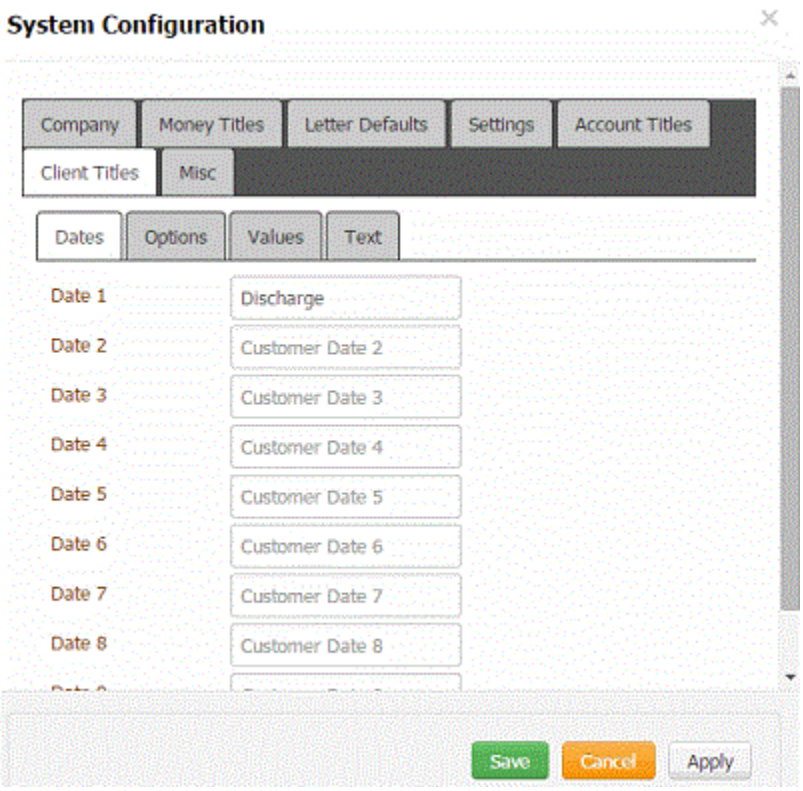
Use the **Dates** tab to specify up to nine labels for dates to display when adding or modifying client accounts.

To maintain client date titles

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **System Configuration**.



2. Click the Edit icon.
3. Click the **Customer Titles** tab and then click the **Dates** tab.



Date 1 through **Date 9:** The values you provide in these boxes become the labels for dates you want to appear when adding a client. For example, if you type "Discharge" in the **Date 1** box, "Discharge" appears as a label next to an input box on the **Custom** tab. For more information, see Maintain Custom Dates.

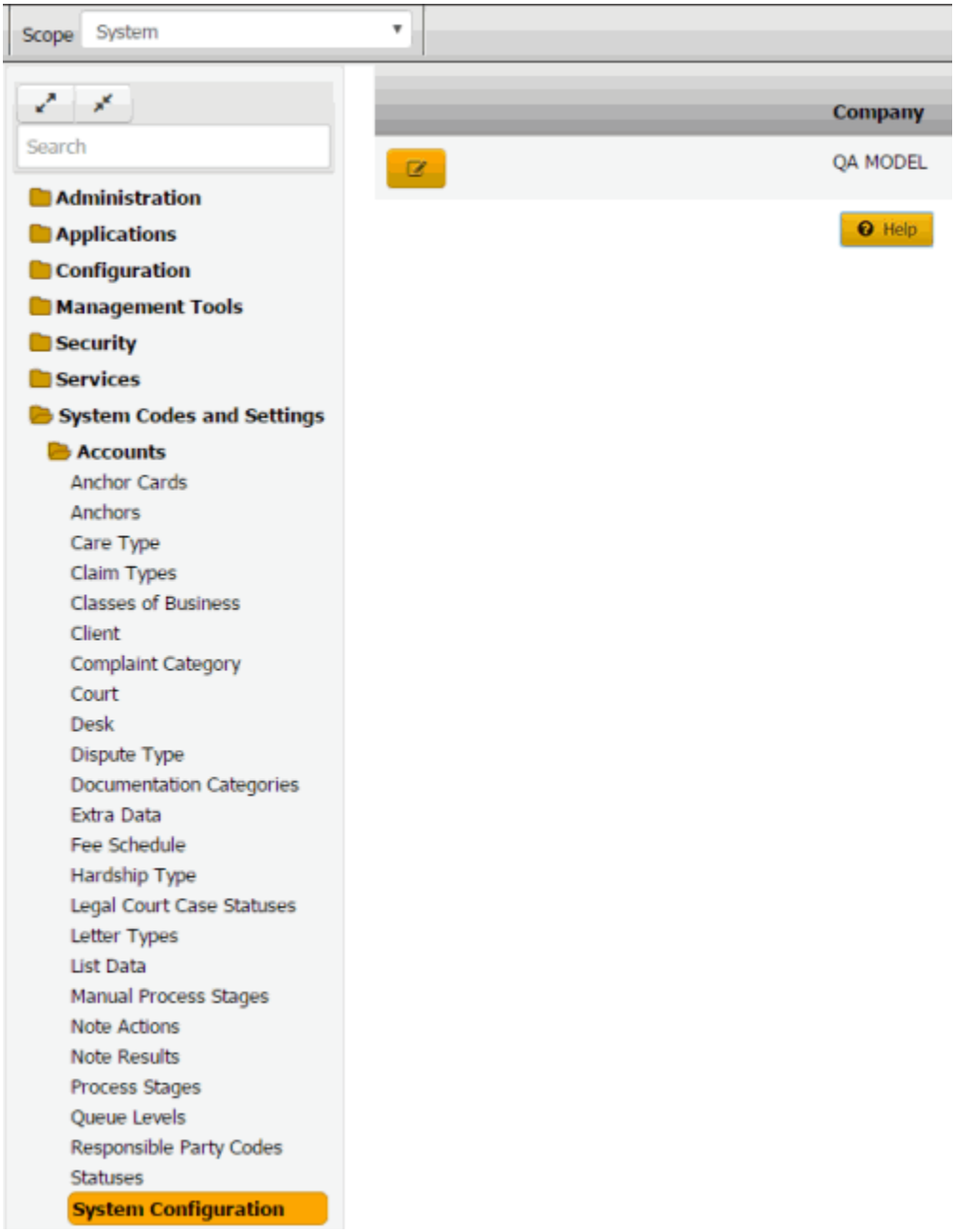
4. Complete the information and then click **Save**.

Maintain Client Option Titles

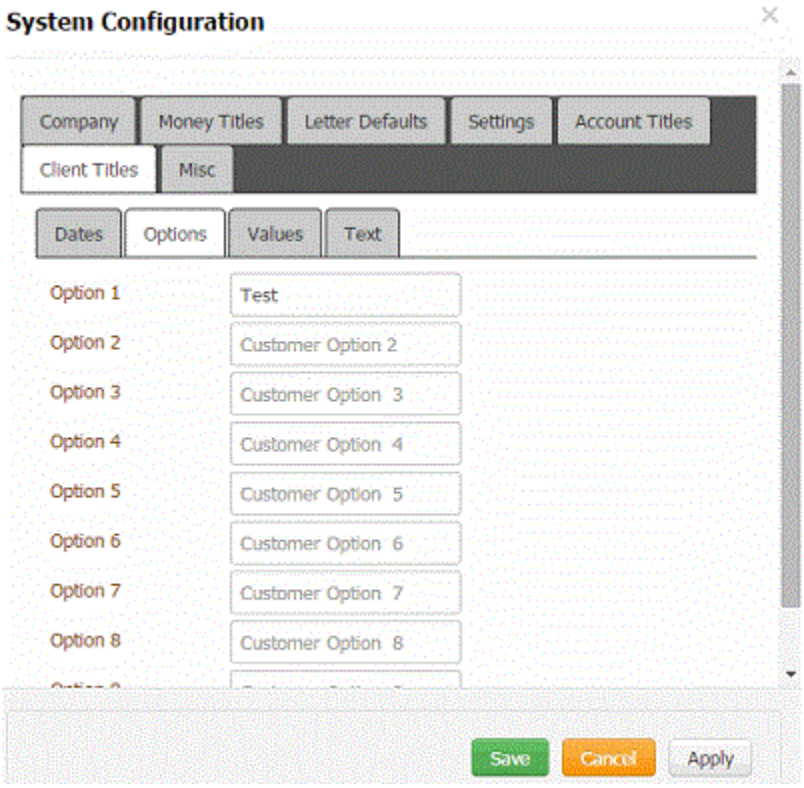
Use the **Options** tab in the **Client Titles** panel to specify up to nine labels for check box options to display when adding or modifying clients.

To maintain client option titles

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **System Configuration**.



2. Click the Edit icon.
3. Click the **Customer Titles** tab and then click the **Options** tab.



Option 1 through **Option 9:** The values you provide in these boxes become the labels for options you want to appear on the **Custom** tab in the **Client** dialog box. For example, if you type "Filed Bankruptcy" in the **Option 1** box, "Filed Bankruptcy" appears as a label next to an input box on the **Custom** tab. For more information, see Maintain Custom Options.

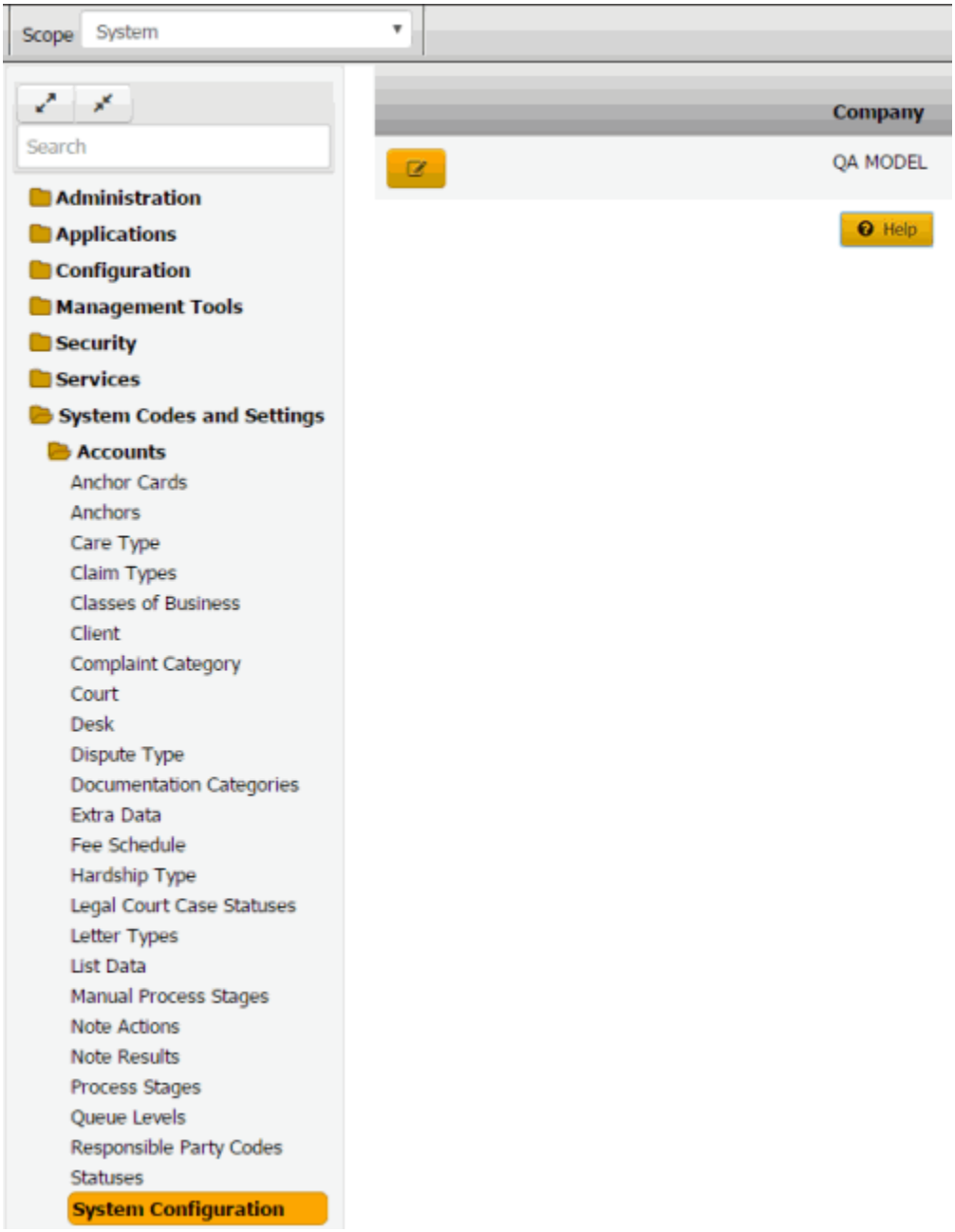
4. Complete the information and then click **Save**.

Maintain Client Text Titles

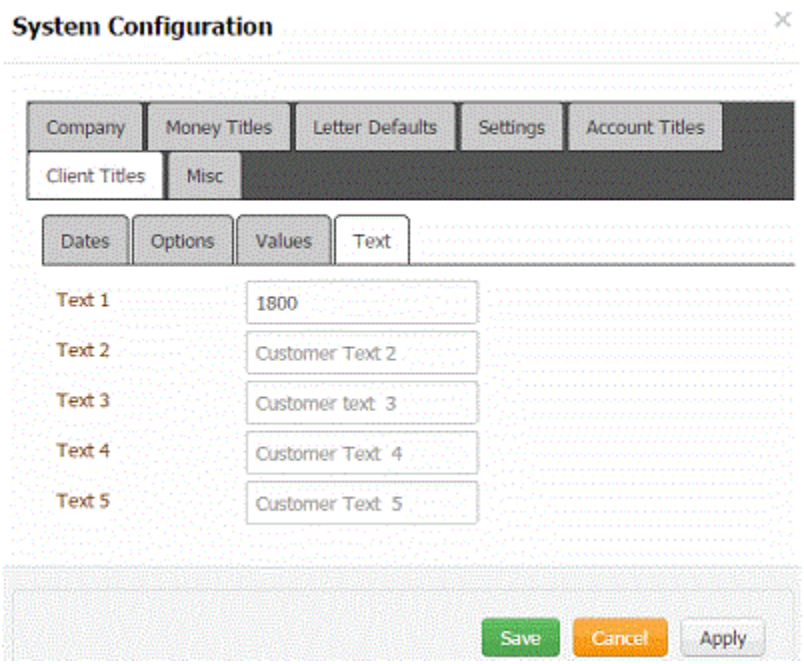
Use the **Text** tab in the **Client Titles** panel to specify up to nine labels for text to display when adding or modifying clients.

To maintain client text titles

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **System Configuration**.



2. Click the Edit icon.
3. Click the **Customer Titles** tab and then click the **Text** tab.



Text 1 through **Text 9:** The values you provide in these boxes become the labels for text you want to appear on the **Custom** tab in the **Client** dialog box. For example, if you type "Bankruptcy Status" in the **Text 1** box, "Bankruptcy Status" appears as a label next to an input box on the **Custom** tab. For more information, see Maintain Custom Text.

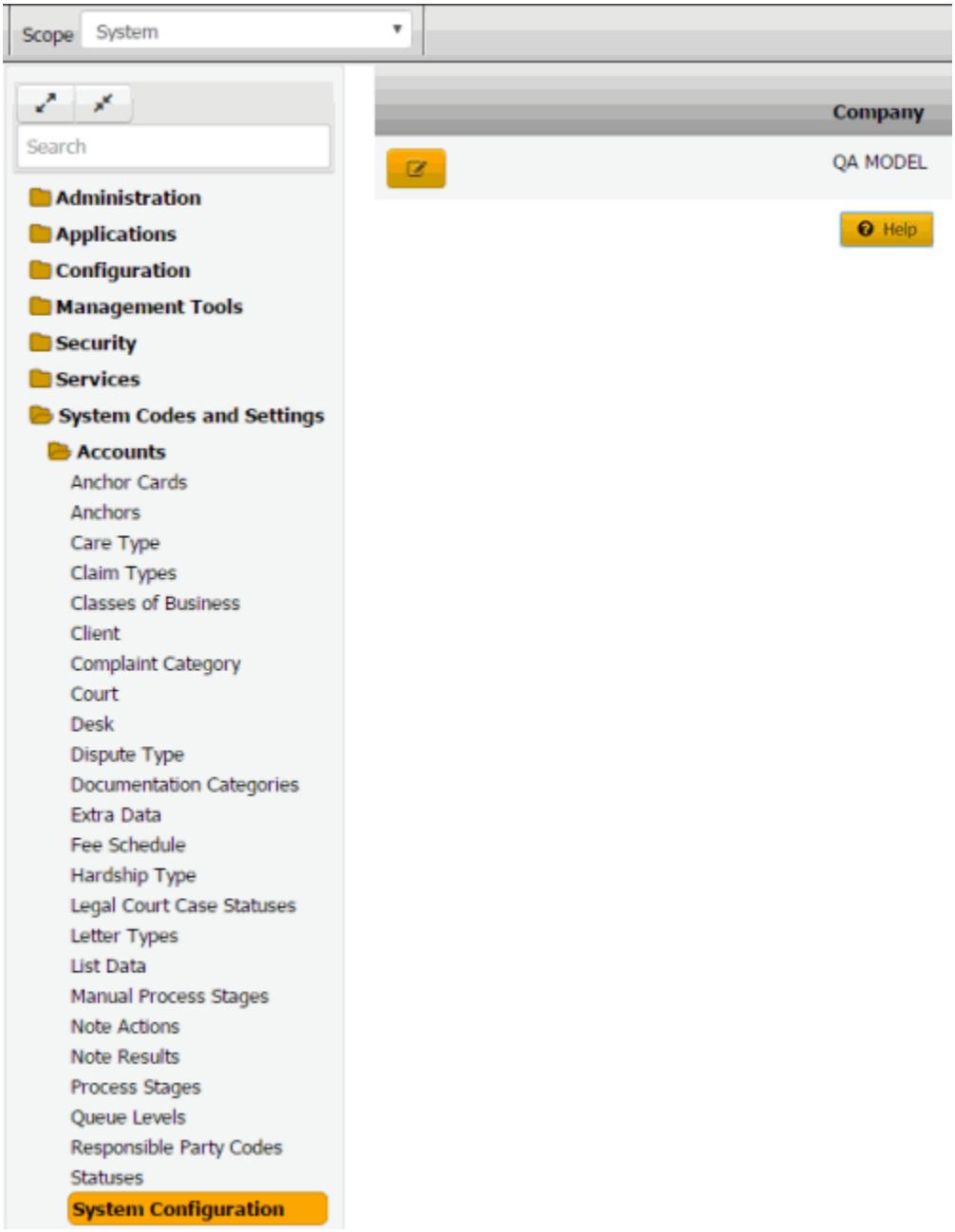
4. Complete the information and then click **Save**.

Maintain Client Value Titles

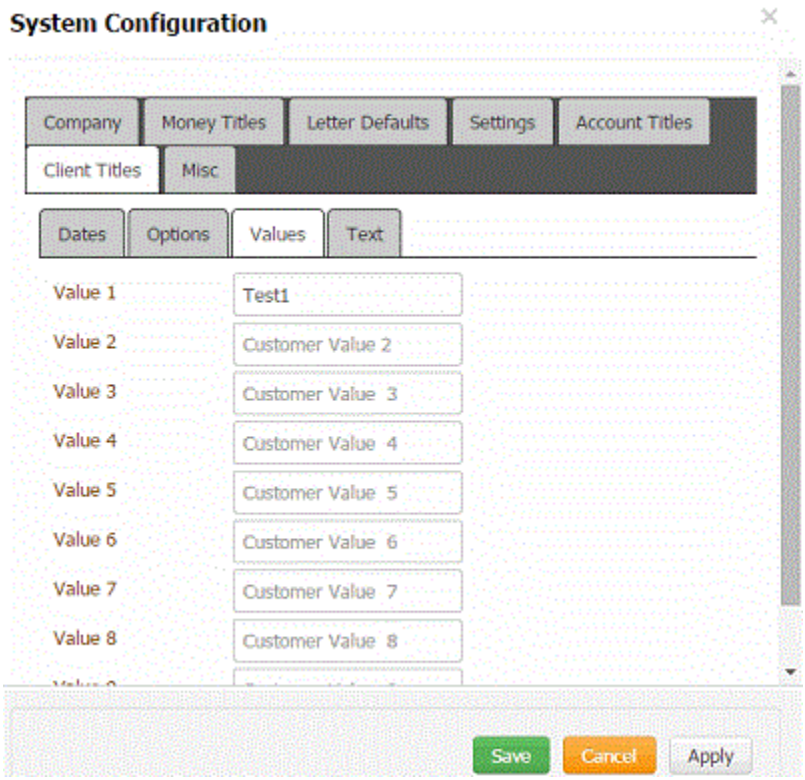
Use the **Values** tab in the **Client Titles** panel to specify up to nine labels for numeric values to display when adding or modifying clients.

To maintain client value titles

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **System Configuration**.



2. Click the Edit icon.
3. Click the **Customer Titles** tab and then click the **Values** tab.



Value 1 through **Value 9:** The values you provide in these boxes become the labels for numeric values you want to appear on the **Custom** tab in the **Client** dialog box. For example, if you type "Number of Bankruptcies Filed" in the **Value 1** box, "Number of Bankruptcies Filed" appears as a label next to an input box on the **Custom** tab. For more information, see Maintain Custom Values.

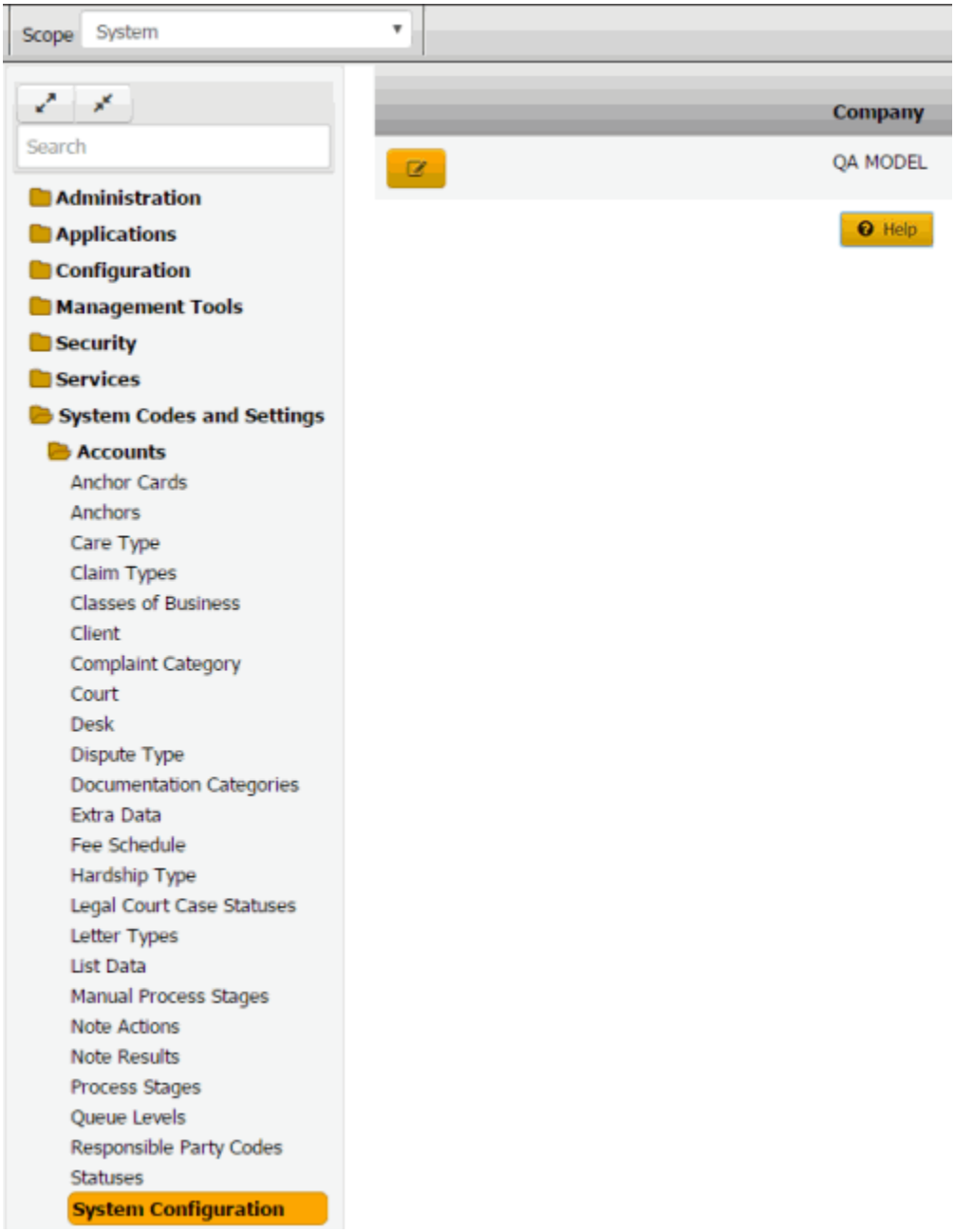
4. Complete the information and then click **Save**.

Maintain Miscellaneous Settings

Use the **Misc** tab to specify the "You've Got Claims" identification number, the name of your outgoing email server, and the path to your custom reports.

To maintain miscellaneous settings

1. In the **Navigation** pane, click **System Codes and Settings** > **Accounts** > **System Configuration**.



2. Click the Edit icon and then click the **Misc** tab.

You Got Claims ID: "You've Got Claims" identification number used for accounts placed with an attorney.

Mail Server (Out): Network name of the outgoing email server. If this setting is incorrect, email letter functions fail.

Crystal Reports Path: Path to the custom reports your organization creates.

3. Complete the information and then click **OK**.

Financial Codes

Financial Codes

You can set up and configure system codes that users can assign to financial transactions for an account.

ABA Routing Numbers

ABA Routing Numbers

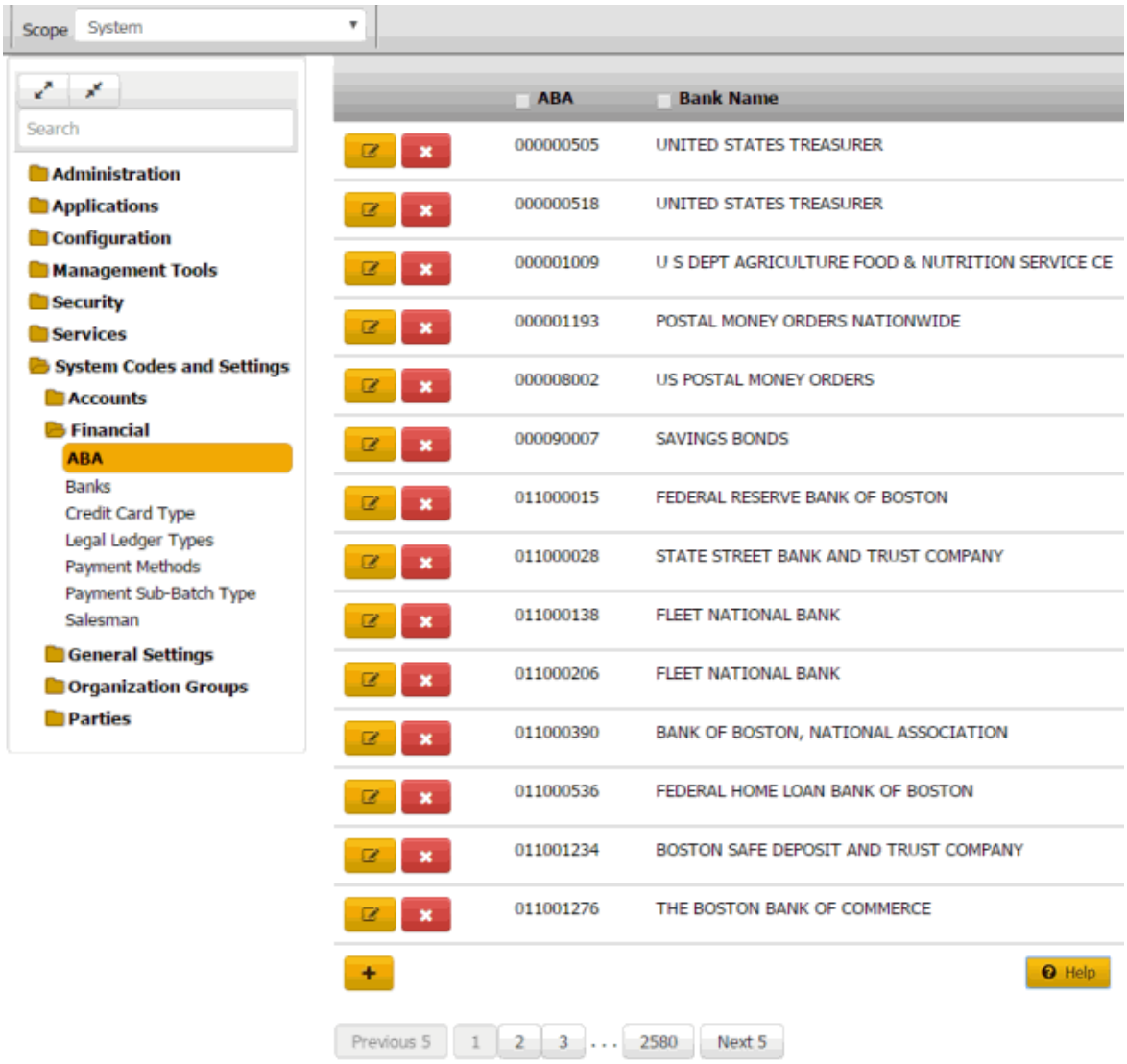
You can search for, add, modify, and delete American Bankers Association (ABA) routing numbers. Latitude uses these numbers to verify the financial institution when users submit a check, ACH, electronic funds transfer, or online banking transaction. Users specify a routing number when adding an ACH or paper draft account to a customer's account. For more information, see Add an ACH or Paper Draft Account.

Add an ABA Routing Number

Use the **ABA** dialog box to add an ABA routing number.

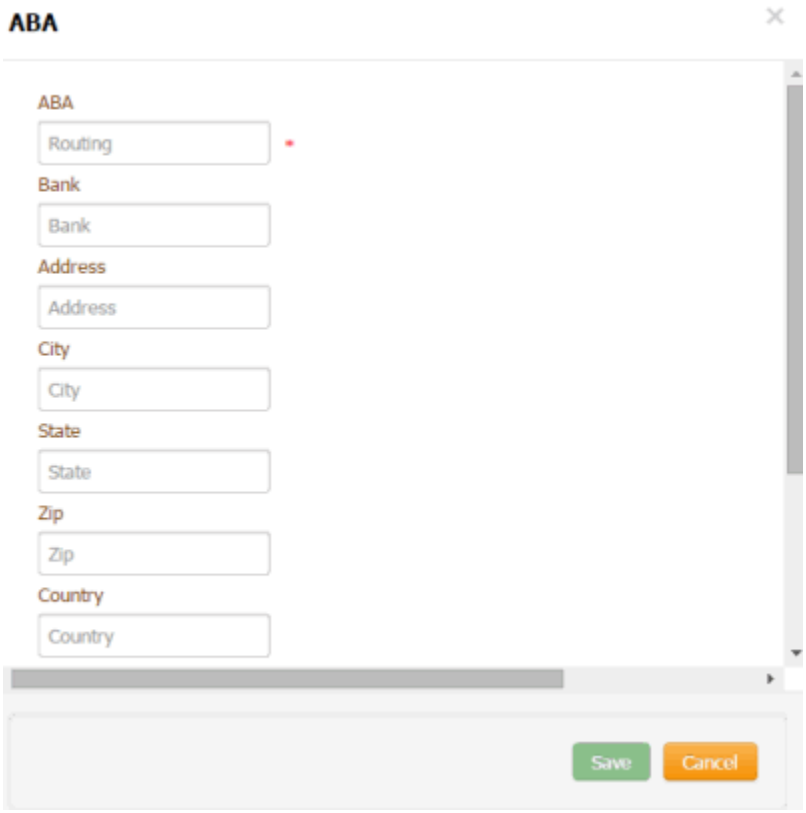
To add an ABA routing number

1. In the **Navigation** pane, click **System Codes and Settings** > **Financial** > **ABA**.



> **Tip:** To limit the records that display in the data grid, click one or more check boxes next to a column heading. In the **Filter** box, type one or more characters and then press **Enter**. To clear a filter, clear the check boxes and then click the Refresh icon.

2. Click the plus sign (+). The **ABA** dialog box appears.



ABA: Routing number that identifies the bank.

Bank: Name of the bank.

Address: Bank's street address.

City: Bank's city.

State: Bank's state.

Zip: Bank's ZIP Code.

Country: Bank's country.

County: Bank's county.

Phone: Bank's phone number.

Fax: Bank's fax number.

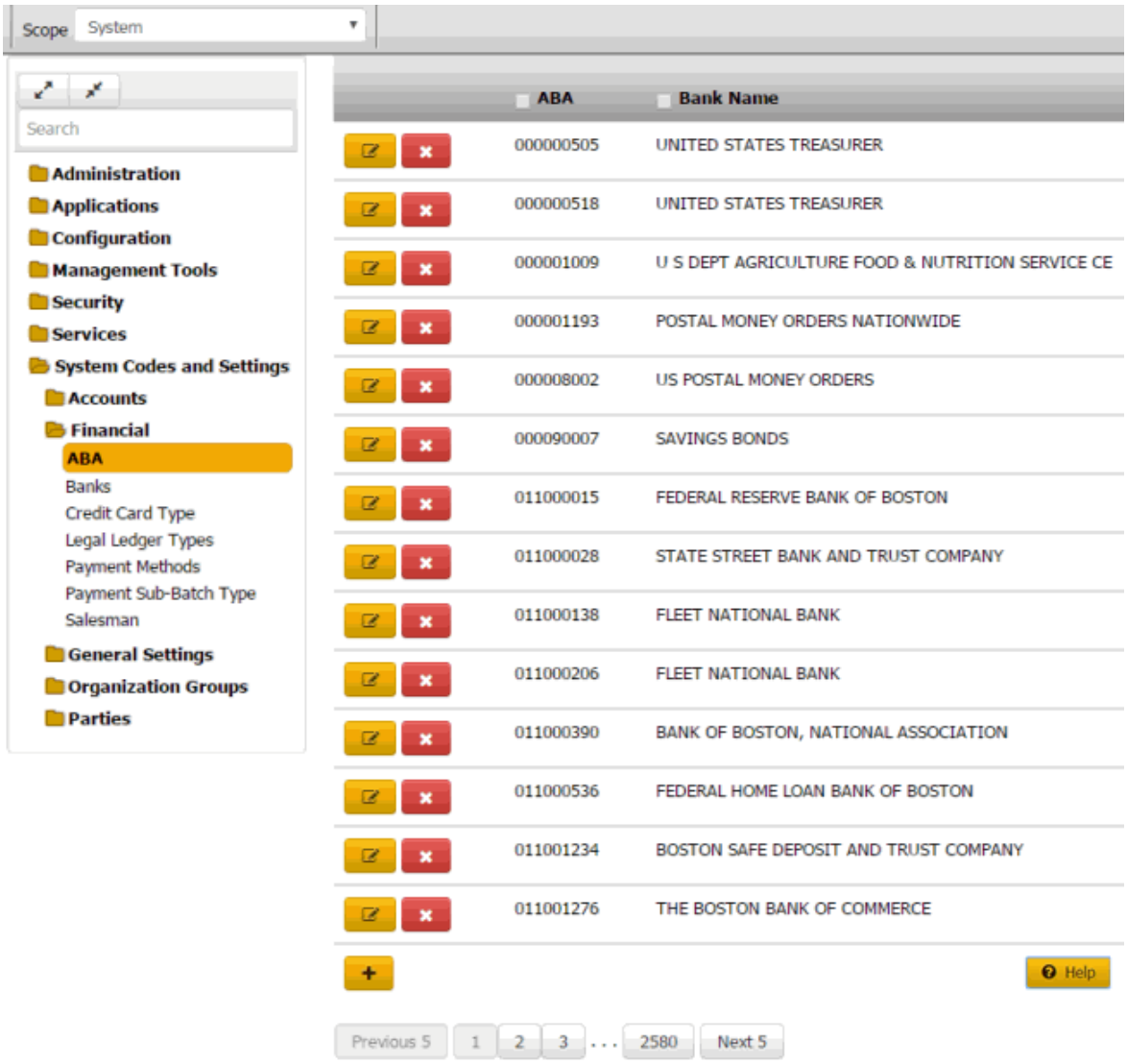
3. Complete the information and then click **Save**.

Modify an ABA Routing Number

Use the **ABA** dialog box to modify an ABA routing number.

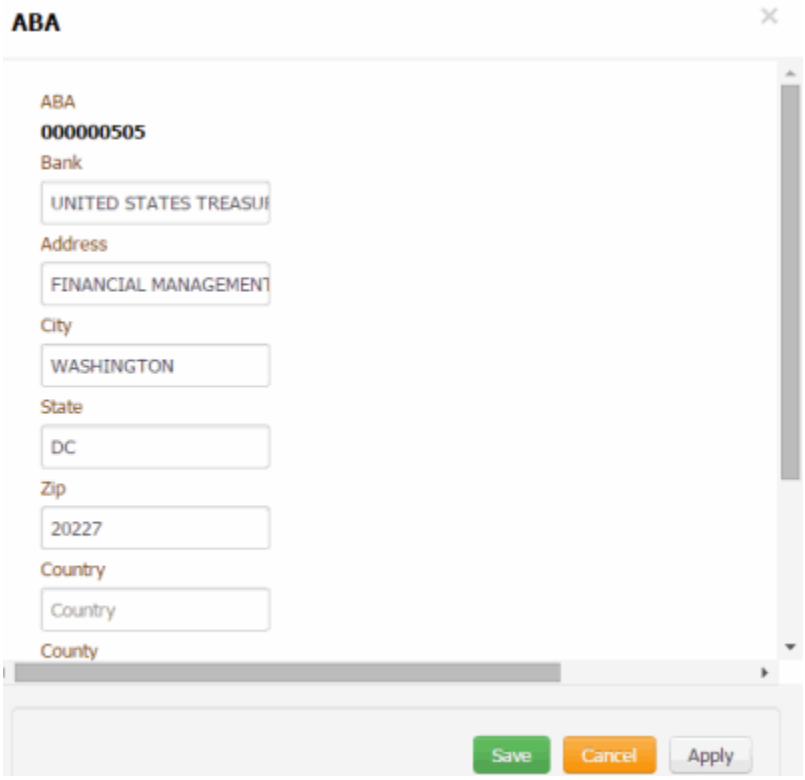
To modify an ABA routing number

1. In the **Navigation** pane, click **System Codes and Settings** > **Financial** > **ABA**.



> **Tip:** To limit the records that display in the data grid, click one or more check boxes next to a column heading. In the **Filter** box, type one or more characters and then press **Enter**. To clear a filter, clear the check boxes and then click the Refresh icon.

2. Click the Edit icon. The **ABA** dialog box appears.



ABA: Routing number that identifies the bank.

Bank: Name of the bank.

Address: Bank's street address.

City: Bank's city.

State: Bank's state.

Zip: Bank's ZIP Code.

Country: Bank's country.

County: Bank's county.

Phone: Bank's phone number.

Fax: Bank's fax number.

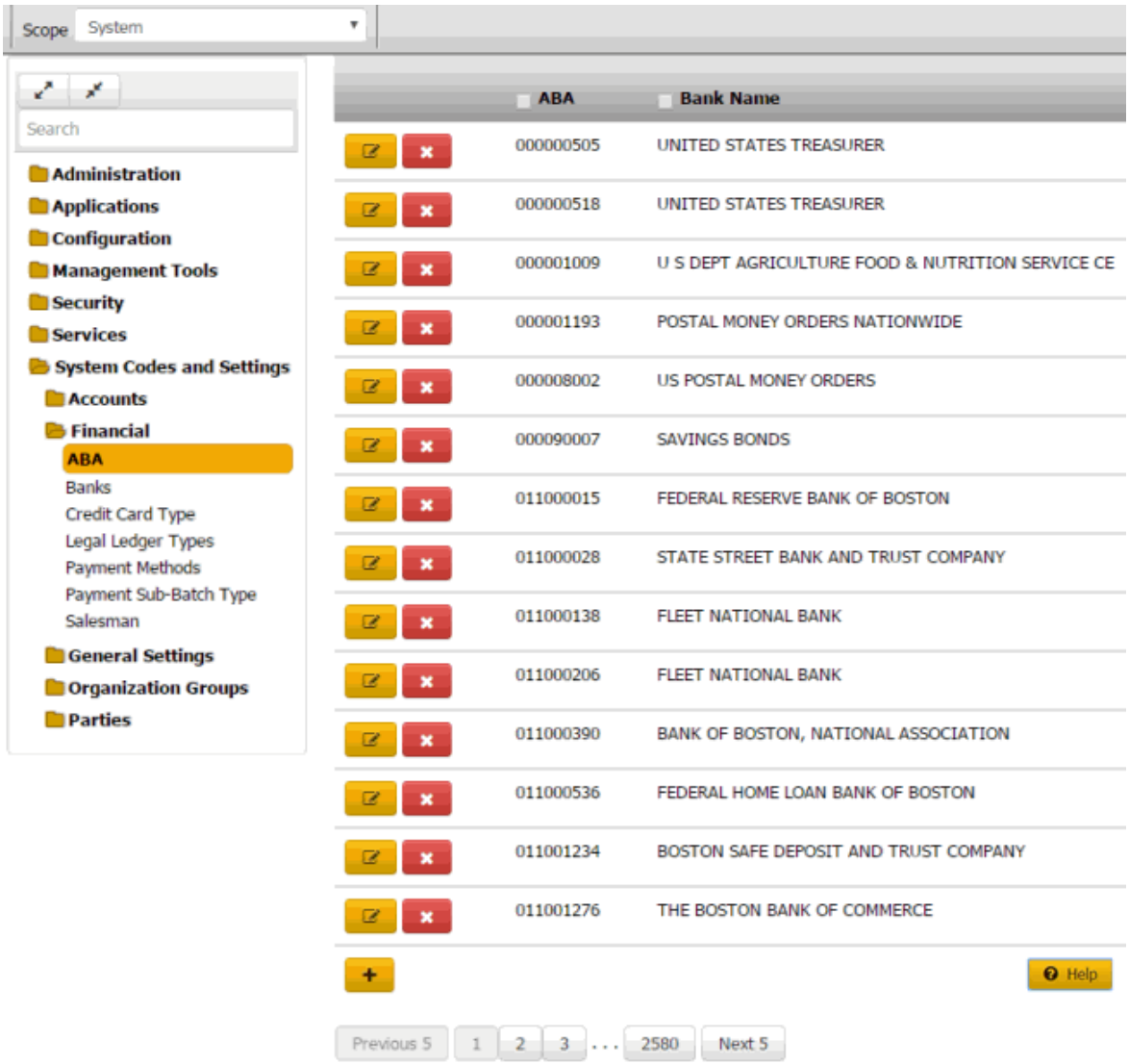
3. Modify the information and then click **Save**.

Delete an ABA Routing Number

Use the **ABA** panel to delete an ABA routing number.

To delete an ABA routing number

1. In the **Navigation** pane, click **System Codes and Settings** > **Financial** > **ABA**.



> **Tip:** To limit the records that display in the data grid, click one or more check boxes next to a column heading. In the **Filter** box, type one or more characters and then press **Enter**. To clear a filter, clear the check boxes and then click the Refresh icon.

2. Click the Delete icon and then click **Yes**.

Banks

Banks

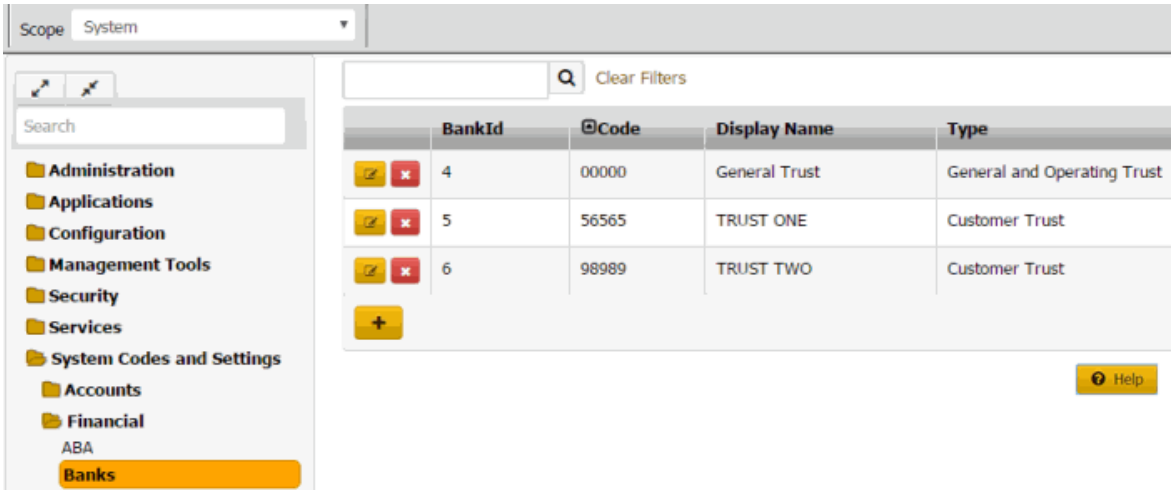
You can search for, add, modify, and delete bank codes. Bank codes allow you to set up separate records for each trust account that accepts deposits of funds from your organization.

Search for a Bank

Use the **Bank** panel to search for a bank.

To search for a bank

1. In the **Navigation** pane, click **System Codes and Settings** > **Financial** > **Banks**.



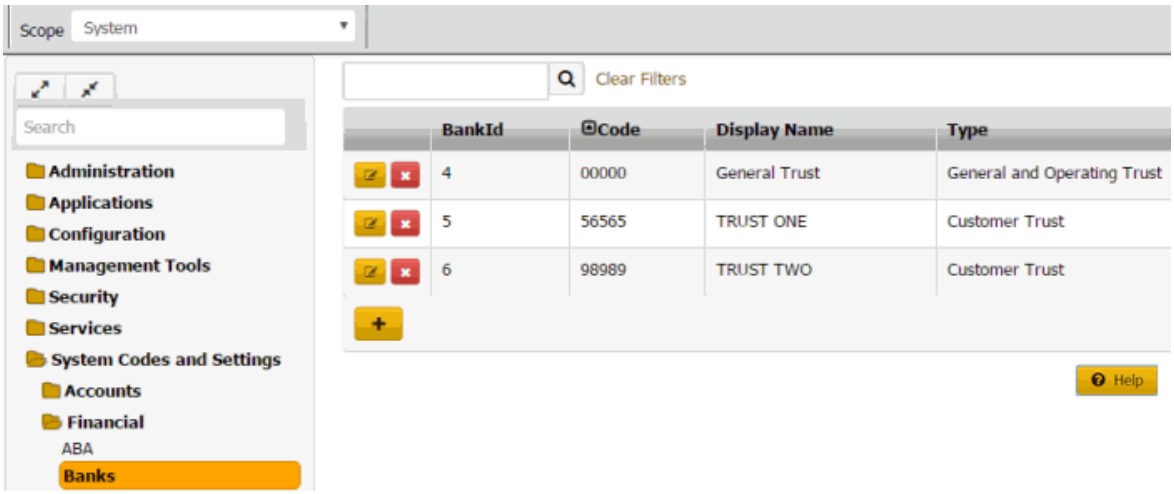
2. In the **Search** box in the **Bank** panel, type one or more characters to search and then press **Enter** or click the Search icon. The system searches the bank code, display name, and bank type for a match. It displays only the banks that match your search criteria.
3. To clear the search criteria, click **Clear Filters**. The system displays all banks.

Add a Bank

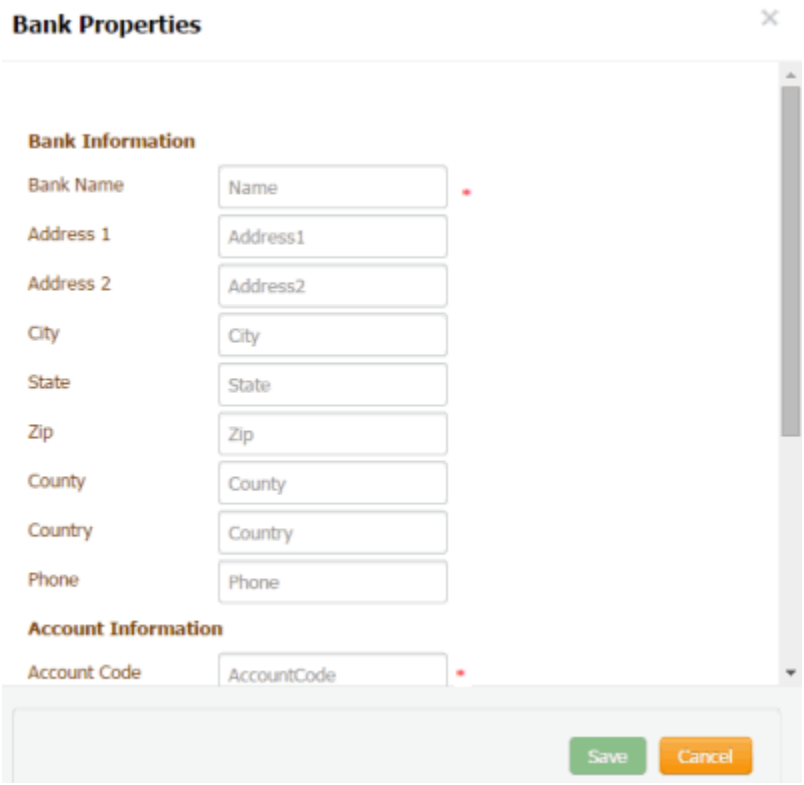
Use the **Bank Properties** dialog box to add a bank.

To add a bank

1. In the **Navigation** pane, click **System Codes and Settings** > **Financial** > **Banks**.



2. Click the plus sign (+). The **Bank Properties** dialog box appears.



Bank Name: Name of the financial institution.

Address 1: First line of the financial institution's street address.

Address 2: Second line of the financial institution's street address.

City: Financial institution's city.

State: Financial institution's state.

ZIP: Financial institution's postal code.

County: Financial institution's county.

Country: Financial institution's country.

Phone: Financial institution's phone number.

Account Code: A numeric code up to five digits in length, that your organization uses to identify the account internally.

Account Title: Title for the account (could include a customer name).

ABA Routing: Nine-digit code that identifies the financial institution.

Checking Account Number: Your organization's checking account number for the trust account.

Starting Check Number: (optional) If your organization is printing checks using the Invoices program, type the first check number to use.

ISO Currency Code: Code that identifies the currency type and country. For example, the currency code for the United States is USD, which signifies United States dollar.

Permit Deposit to General Trust Account: Allows money collected and split between linked accounts having different banks to deposit to the **General Trust** initially. Latitude only includes in the same payment arrangement accounts that deposit to the same trust or general trust.

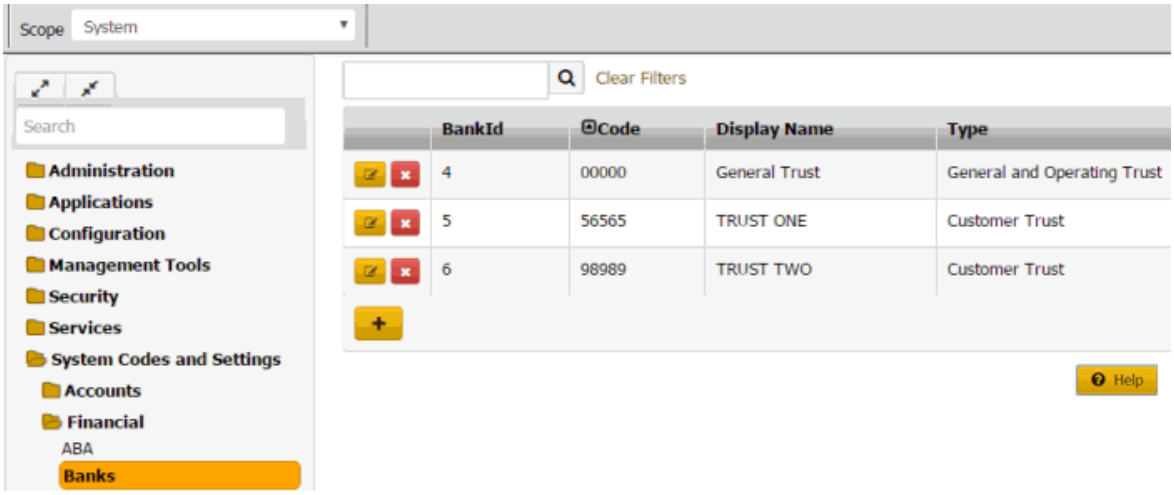
3. Complete the information and then click **Save**.

Modify a Bank

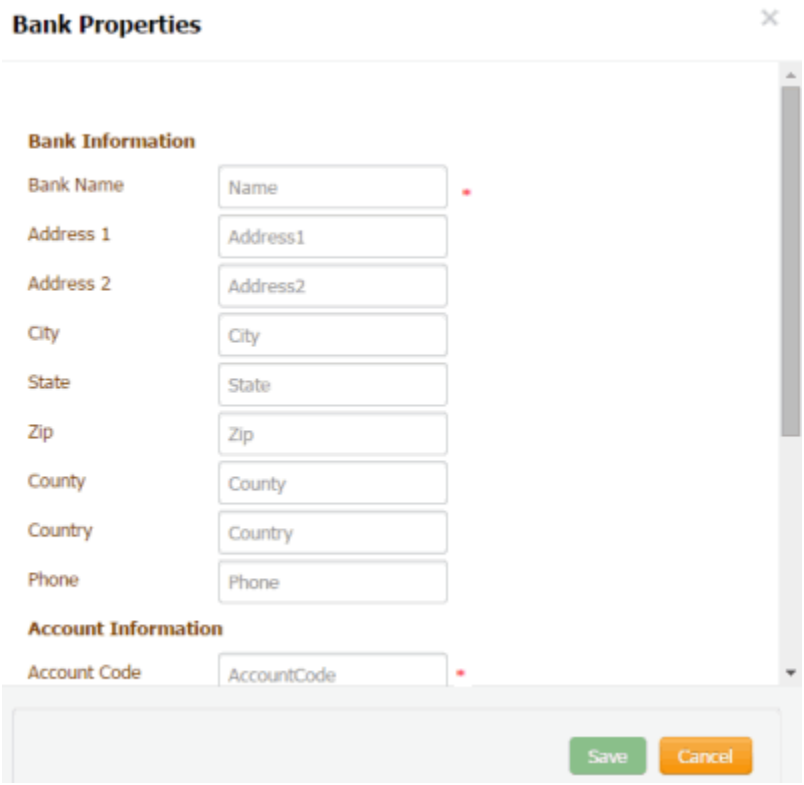
Use the **Bank Properties** dialog box to modify a bank.

To modify a bank

1. In the **Navigation** pane, click **System Codes and Settings** > **Financial** > **Banks**.



2. Click the Edit icon. The **Bank Properties** dialog box appears.



Bank Name: Name of the financial institution.

Address 1: First line of the financial institution's street address.

Address 2: Second line of the financial institution's street address.

City: Financial institution's city.

State: Financial institution's state.

ZIP: Financial institution's postal code.

County: Financial institution's county.

Country: Financial institution's country.

Phone: Financial institution's phone number.

Account Code: A numeric code up to five digits in length, that your organization uses to identify the account internally.

Account Title: Title for the account (could include a customer name).

ABA Routing: Nine-digit code that identifies the financial institution.

Checking Account Number: Your organization's checking account number for the trust account.

Starting Check Number: (optional) If your organization is printing checks using the Invoices program, type the first check number to use.

ISO Currency Code: Code that identifies the currency type and country. For example, the currency code for the United States is USD, which signifies United States dollar.

Permit Deposit to General Trust Account: Allows money collected and split between linked accounts having different banks to deposit to the **General Trust** initially. Latitude only includes in the same payment arrangement accounts that deposit to the same trust or general trust.

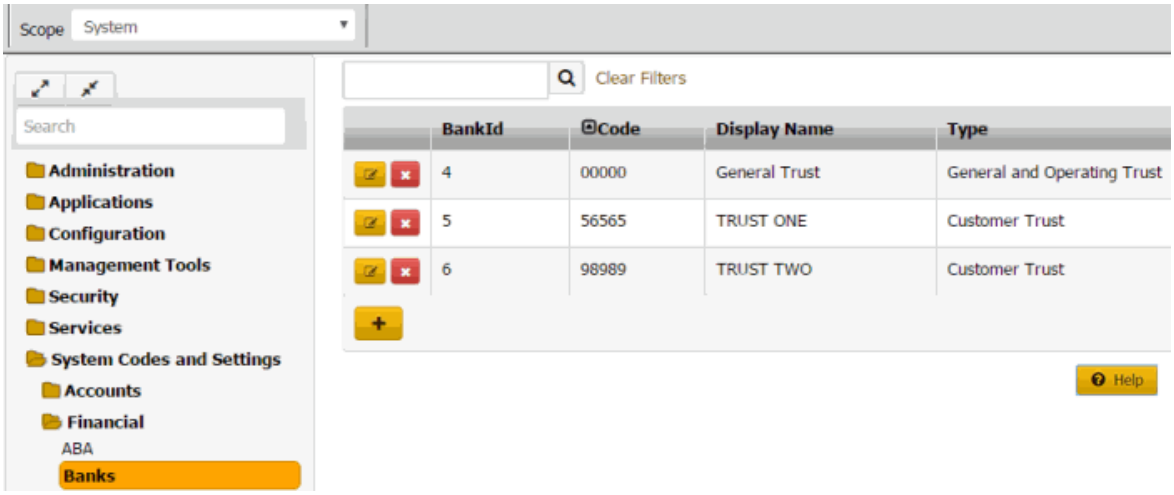
3. Modify the information and then click **Save**.

Delete a Bank

Use the **Banks** panel to delete a bank.

To delete a bank

1. In the **Navigation** pane, click **System Codes and Settings** > **Financial** > **Banks**.



2. Click the Delete icon and then click **Yes**.

Credit Card Types

Credit Card Types

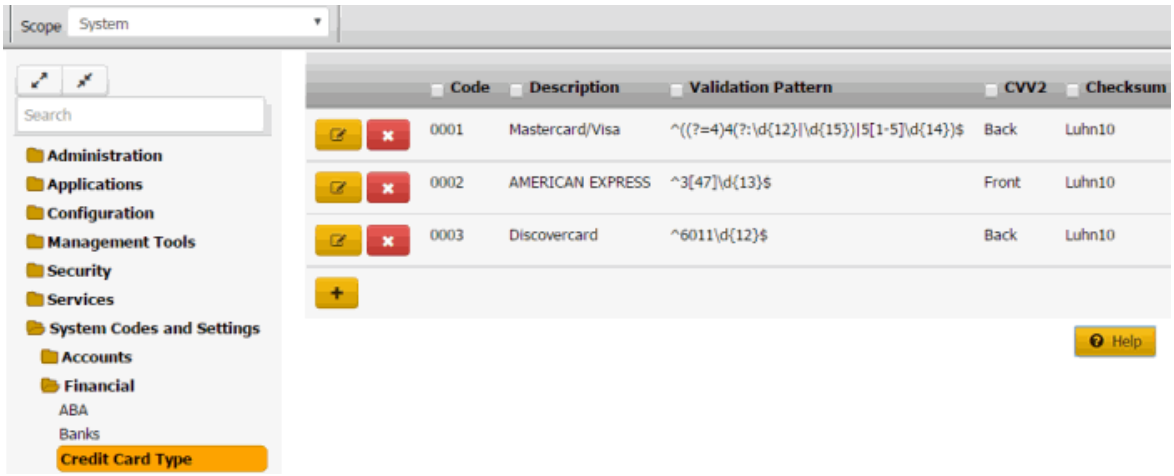
You can search for, add, modify, and delete credit card types that your organization accepts for payment transactions. Users specify a credit card type when adding a credit card to a payment arrangement. For more information, see Add a Credit Card. The algorithm for the credit card determines whether it is a valid card.

Add a Credit Card Type

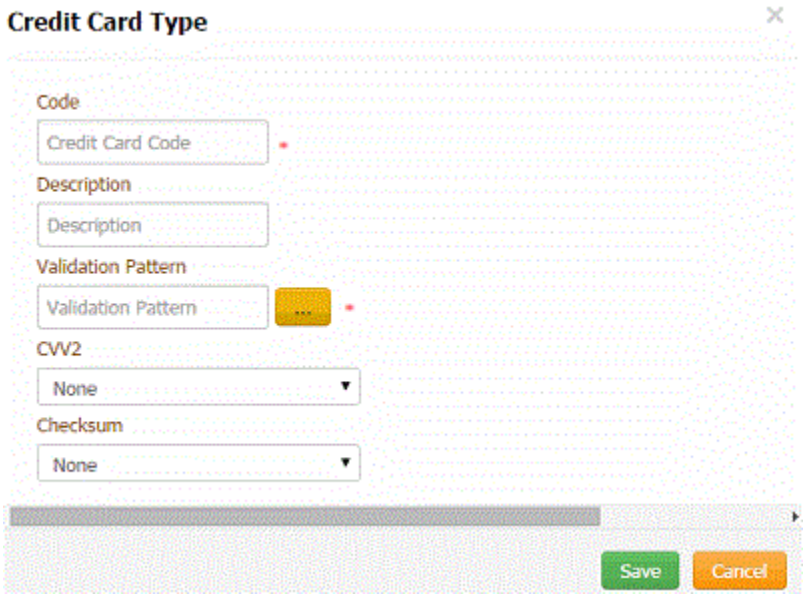
Use the **Credit Card Type** dialog box to add a credit card type.

To add a credit card type

1. In the **Navigation** pane, click **System Codes and Settings** > **Financial** > **Credit Card Type**.



2. Click the plus sign (+). The **Credit Card Type** dialog box appears.



Code: Unique code that identifies the credit card type.

Description: Commonly used name for the credit card type.

Validation Pattern: Expression used to identify the card. Click the ellipsis (**...**) and select a standard card type from the list.

CVV2: Indicates the location of the security code on the credit card.

Checksum: Formula to use to validate the credit card.

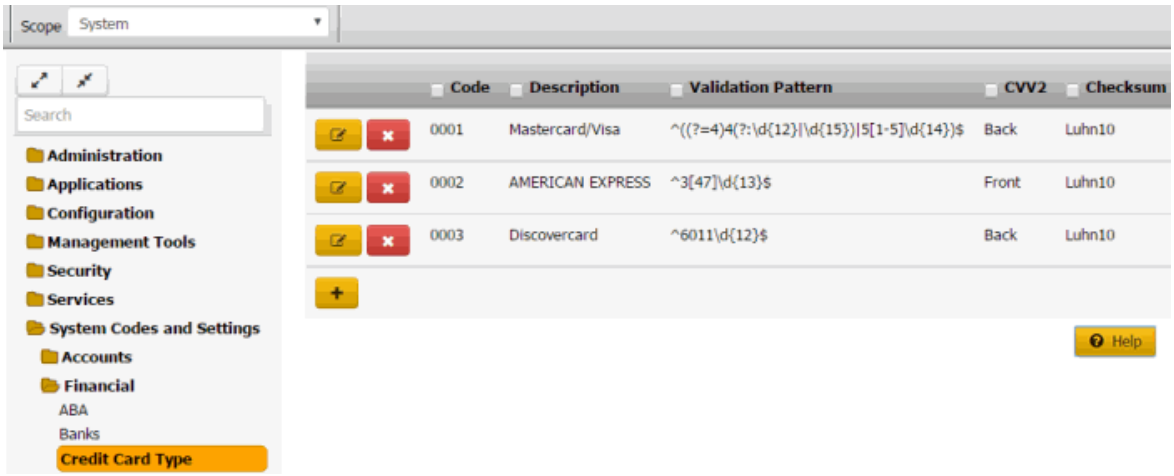
3. Complete the information and then click **Save**.

Modify a Credit Card Type

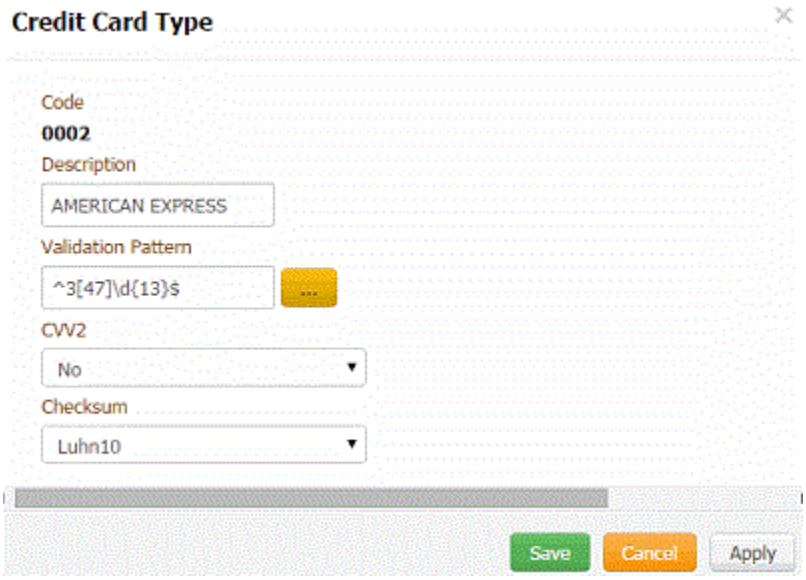
Use the **Credit Card Type** dialog box to modify a credit card type.

To modify a credit card type

1. In the **Navigation** pane, click **System Codes and Settings** > **Financial** > **Credit Card Type**.



2. Click the Edit icon. The **Credit Card Type** dialog box appears.



Code: Unique code that identifies the credit card type.

Description: Commonly used name for the credit card type.

Validation Pattern: Expression used to identify the card. Click the ellipsis (**...**) and select a standard card type from the list.

CVV2: Indicates the location of the security code on the credit card.

Checksum: Formula to use to validate the credit card.

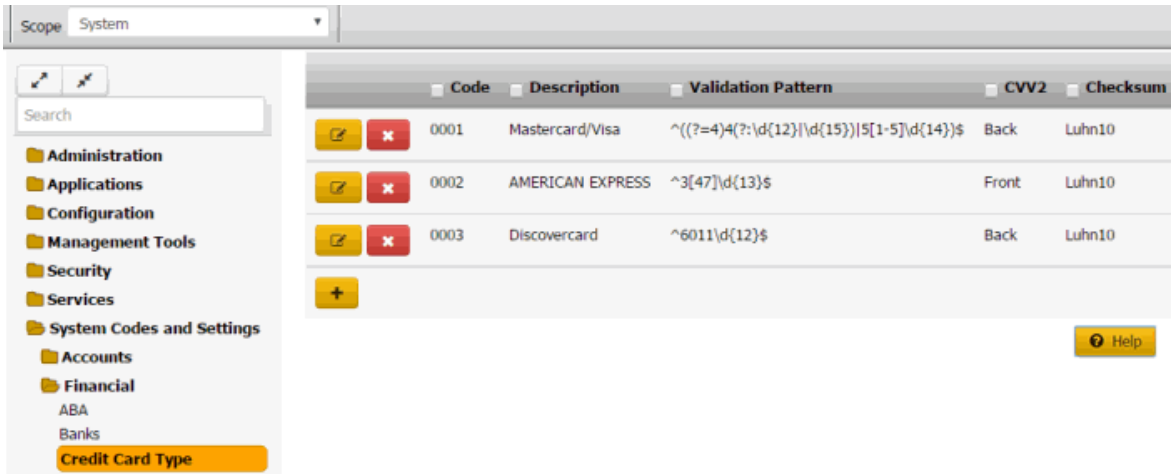
3. Modify the information and then click **Save**.

Delete a Credit Card Type

Use the **Credit Card Type** panel to delete a credit card type.

To delete a credit card type

1. In the **Navigation** pane, click **System Codes and Settings** > **Financial** > **Credit Card Type**.



2. Click the Delete icon and then click **Yes**.

Legal Ledger Types

Legal Ledger Types

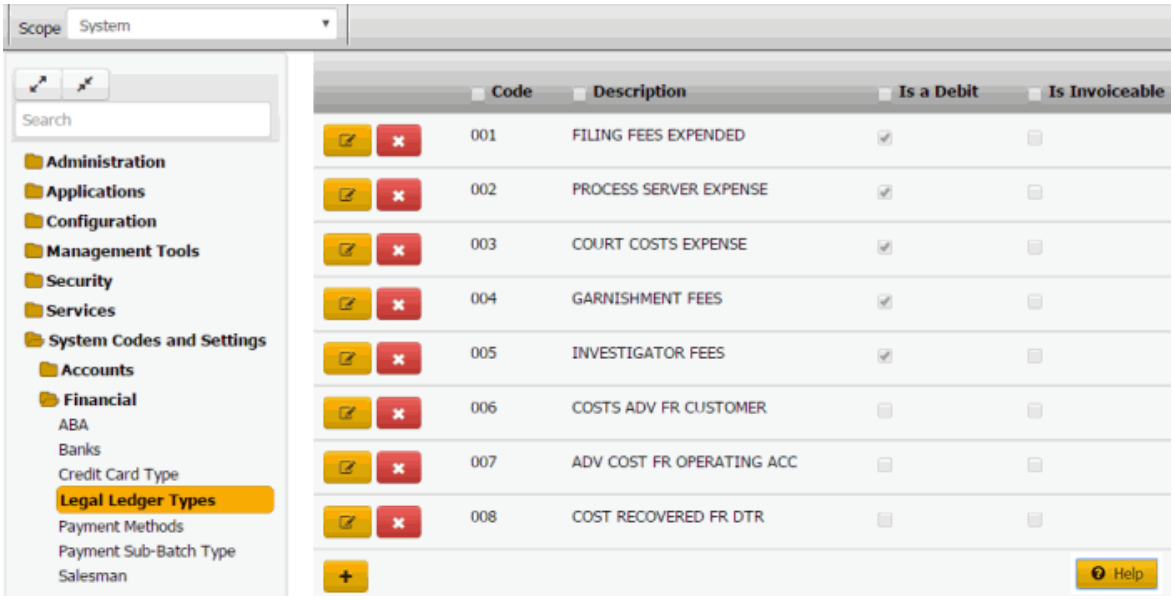
You can search for, add, modify, and delete legal ledger types. Legal ledger types allow your organization group legal accounting ledger entries. You specify whether transactions assigned to a type apply as debits or credits, and whether invoices include the transactions. Users specify a ledger type when adding a legal ledger item to a legal case. For more information, see Add a Legal Ledger Item.

Add a Legal Ledger Type

Use the **Legal Ledger Types** panel to add a legal ledger type.

To add a legal ledger type

1. In the **Navigation** pane, click **System Codes and Settings** > **Financial** > **Legal Ledger Types**.



2. Click the plus sign (+). A blank row appears in the data grid.

Code	Description	Is a Debit	Is Invoiceable
001	FILING FEES EXPENDED	☑	☐
002	PROCESS SERVER EXPENSE	☑	☐
003	COURT COSTS EXPENSE	☑	☐
004	GARNISHMENT FEES	☑	☐
005	INVESTIGATOR FEES	☑	☐
006	COSTS ADV FR CUSTOMER	☐	☐
007	ADV COST FR OPERATING ACC	☐	☐
008	COST RECOVERED FR DTR	☐	☐
	Code *	Description *	Is a Debit ☐	Is Invoiceable ☐

Code: Unique code that identifies the legal ledger type.

Description: Description of the legal ledger type.

Is a Debit: If selected, the legal ledger type represents a debit transaction. If cleared, transactions assigned to this legal ledger type apply as a credit. These transactions do not affect the account balances in Latitude.

Is Invoiceable: If selected, the legal ledger type represents a transaction that you can invoice. These transactions appear on a separate Exchange AIM invoice. These transactions do NOT appear on standard Latitude invoices.

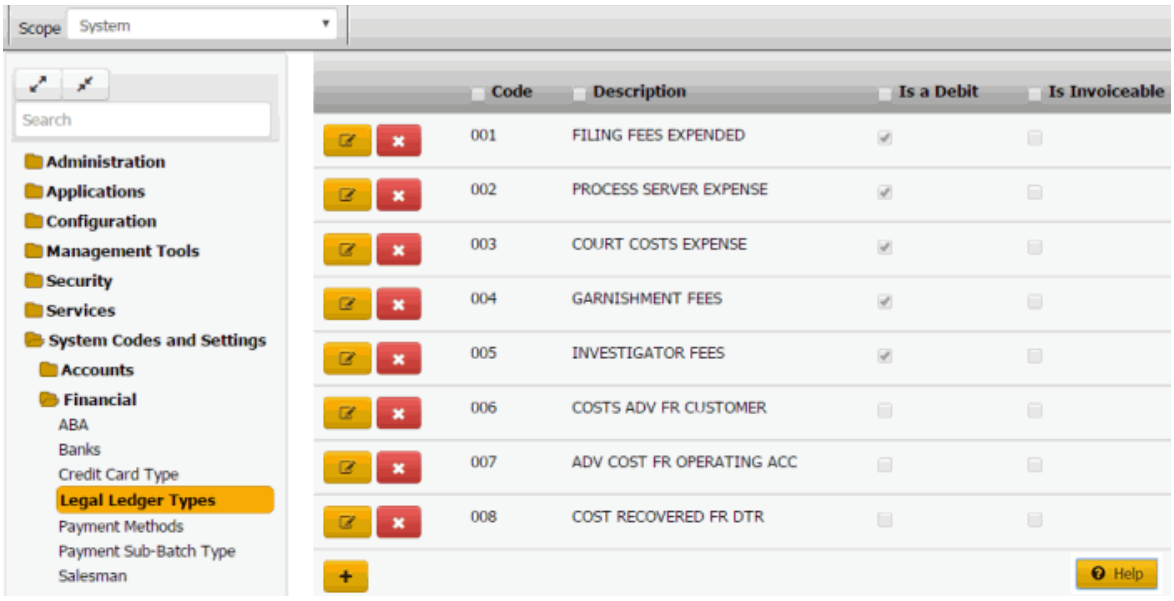
3. Complete the information and then click the check mark.

Modify a Legal Ledger Type

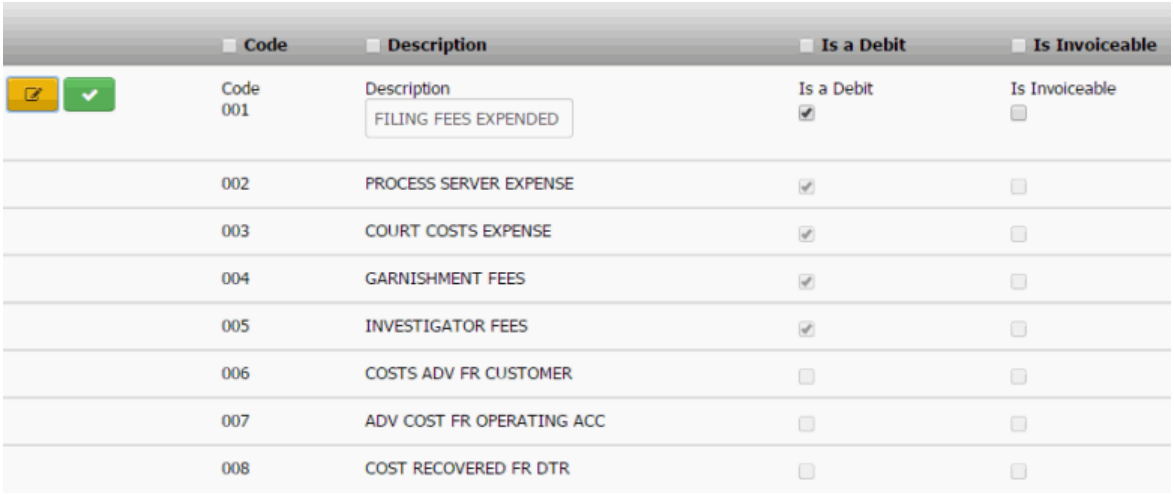
Use the **Legal Ledger Types** panel to modify a legal ledger type.

To modify a legal ledger type

1. In the **Navigation** pane, click **System Codes and Settings** > **Financial** > **Legal Ledger Types**.



2. Click the Edit icon. The legal ledger type appears in edit mode.



Code: Unique code that identifies the legal ledger type.

Description: Description of the legal ledger type.

Is a Debit: If selected, the legal ledger type represents a debit transaction. If cleared, transactions assigned to this legal ledger type apply as a credit. These transactions do not affect the account balances in Latitude.

Is Invoiceable: If selected, the legal ledger type represents a transaction that you can invoice. These transactions appear on a separate Exchange AIM invoice. These transactions do NOT appear on standard Latitude invoices.

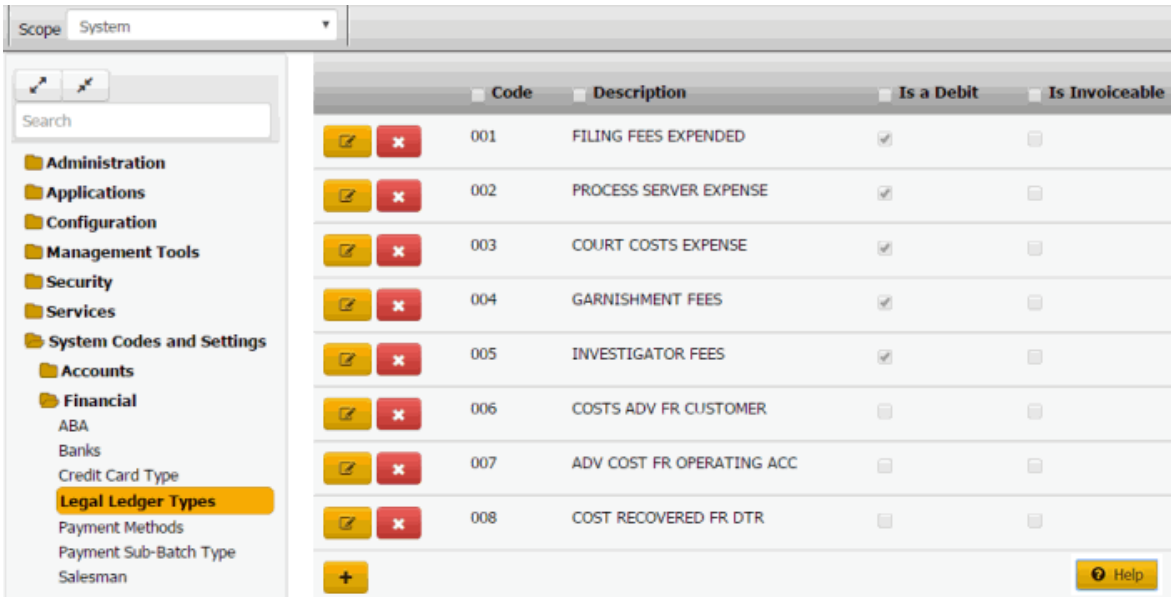
3. Modify the information and then click the check mark.

Delete a Legal Ledger Type

Use the **Legal Ledger Types** panel to delete a legal ledger type.

To delete a legal ledger type

1. In the **Navigation** pane, click **System Codes and Settings** > **Financial** > **Legal Ledger Types**.



2. Click the Delete icon and then click **Yes**.

Payment Methods

Payment Methods

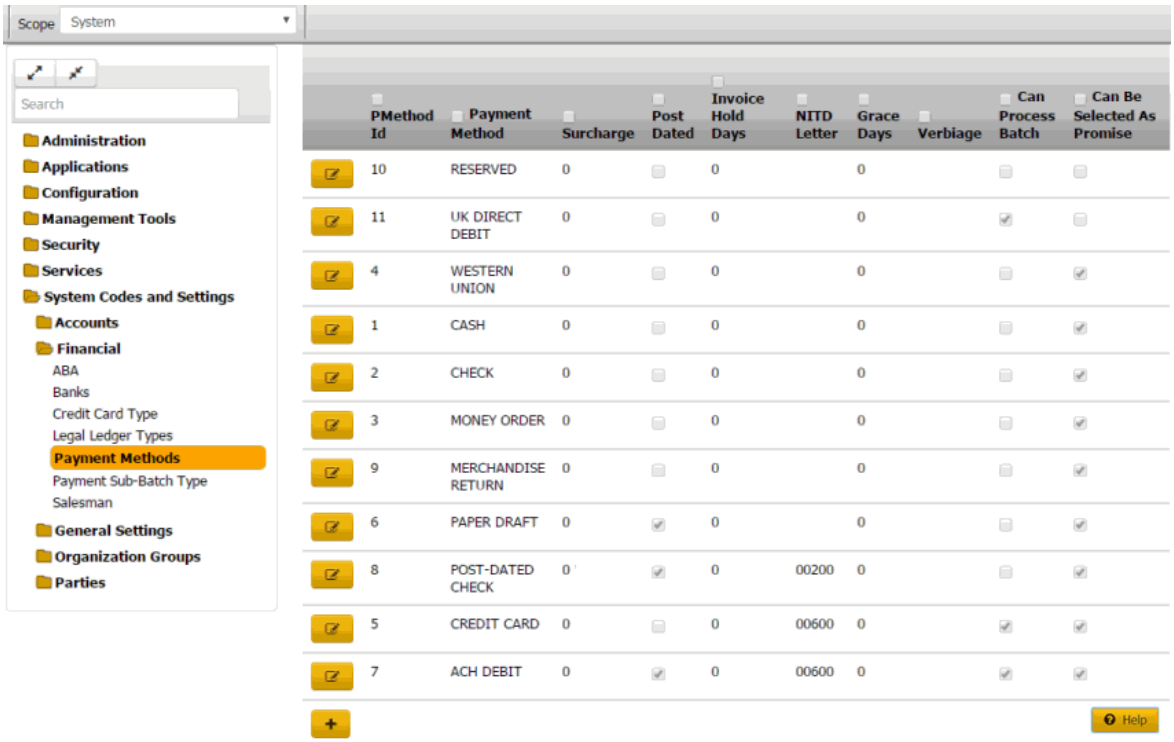
You can search for, add, and modify payment methods. Users specify a payment method when creating a payment arrangement. For more information, see Propose a Payment Arrangement.

Add a Payment Method

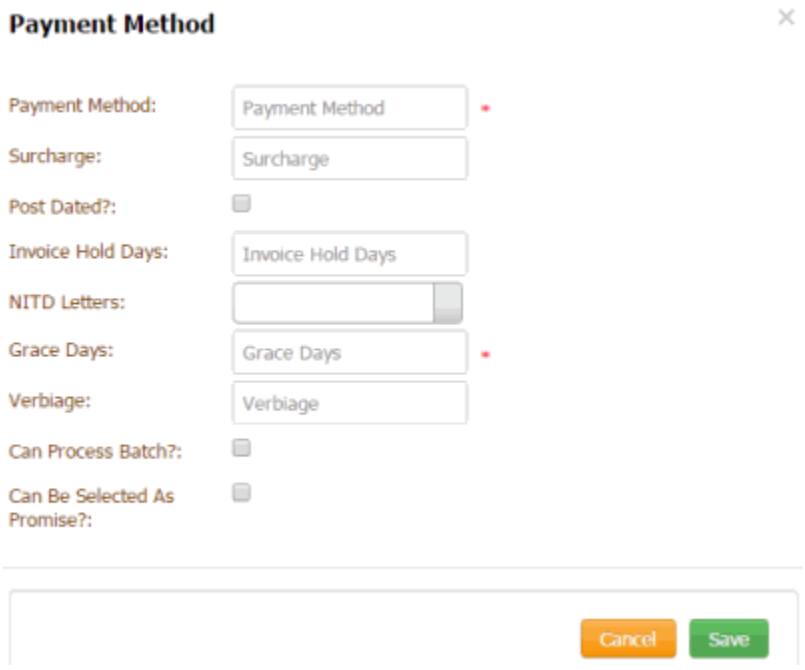
Use the **Payment Method** dialog box to add a payment method.

To add a payment method

1. In the **Navigation** pane, click **System Codes and Settings** > **Financial** > **Payment Methods**.



2. Click the plus sign (+).



Payment Method: Means of payment in a payment arrangement.

Surcharge: Amount your organization adds to the account for payments received using this payment method (not applicable for MA accounts). Latitude adds this amount to bucket 10 when users add a payment to an account. For more information, see Surcharge Rules.

Post Dated?: If selected, this payment method is a post-dated entry. This option is available when adding post-dated check information for an account.

Invoice Hold Days: Number of days to wait before posting payments received to the client's invoice using this payment method.

NITD Letters: Notice of Intent to Deposit letters. Code that identifies the letter to generate when users add payments using this method. The letters available are based on the letters your organization configured using Letter Console.

Grace Days: Maximum number of days after the payment due date that the customer can submit a payment before the payment is considered late.

Verbiage: Text to display to the user when using this payment method in a payment arrangement.

Can Process Batch?: If selected, this payment method is available for selection as a batch type when processing payment batches using the Batch Processor.

Can Be Selected as Promise?: If selected, this payment method is available for selection when scheduling a payment promise.

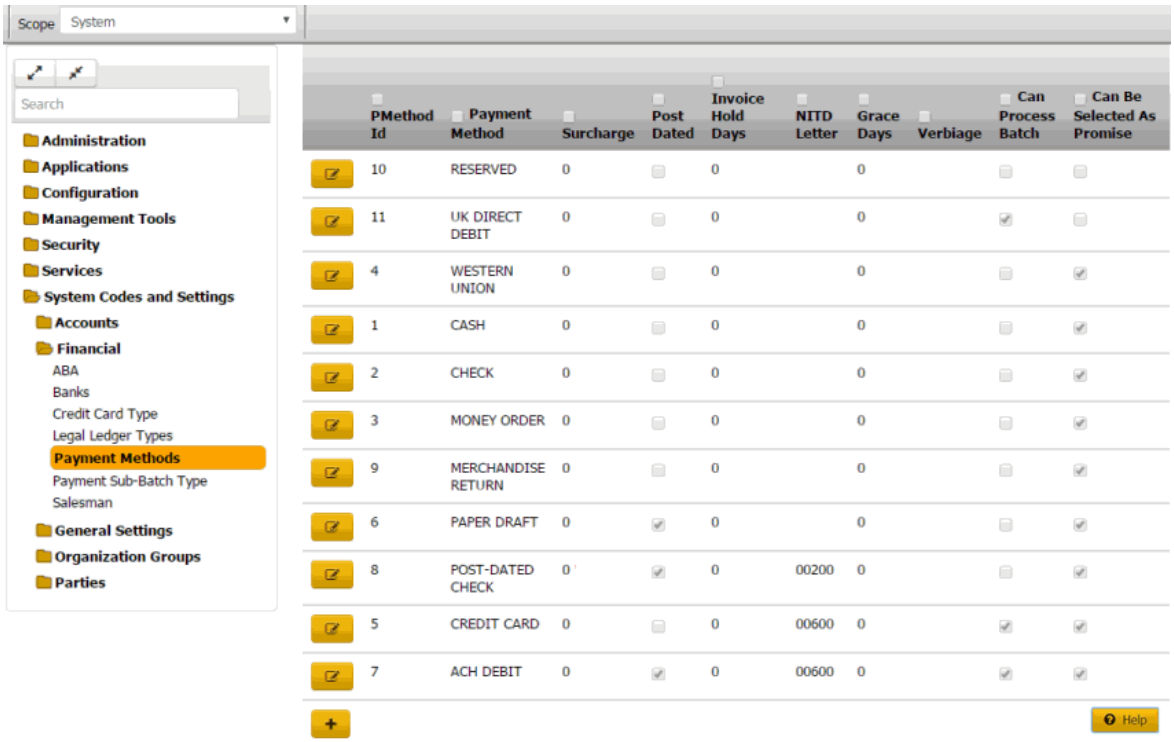
3. Complete the information and then click **Save**.

Modify a Payment Method

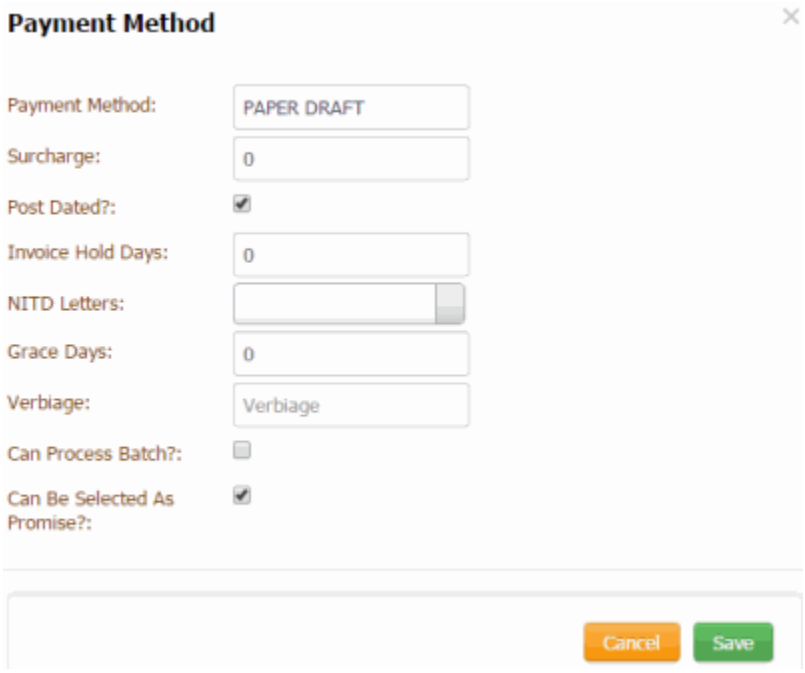
Use the **Payment Method** dialog box to modify a payment method.

To modify a payment method

1. In the **Navigation** pane, click **System Codes and Settings** > **Financial** > **Payment Methods**.



2. Click the Edit icon.



Payment Method: Means of payment in a payment arrangement.

Surcharge: Amount your organization adds to the account for payments received using this payment method (not applicable for MA accounts). Latitude adds this amount to bucket 10 when users add a payment to an account.

Post Dated?: If selected, this payment method is a post-dated entry. This option is available when adding post-dated check information for an account.

Invoice Hold Days: Number of days to wait before posting payments received to the client's invoice using this payment method.

NITD Letters: Notice of Intent to Deposit letters. Code that identifies the letter to generate when users add payments using this method. The letters available are based on the letters your organization configured using Letter Console.

Grace Days: Maximum number of days after the actual payment due date that the customer can submit a payment before the payment is considered late.

Verbiage: Text to display to the user when using this payment method in a payment arrangement.

Can Process Batch?: If selected, this payment method is available for selection as a batch type when processing payment batches using the Batch Processor.

Can Be Selected as Promise?: If selected, this payment method is available for selection when scheduling a payment promise.

3. Modify the information and then click **Save**.

Payment Sub-Batch Types

Payment Sub-Batch Types

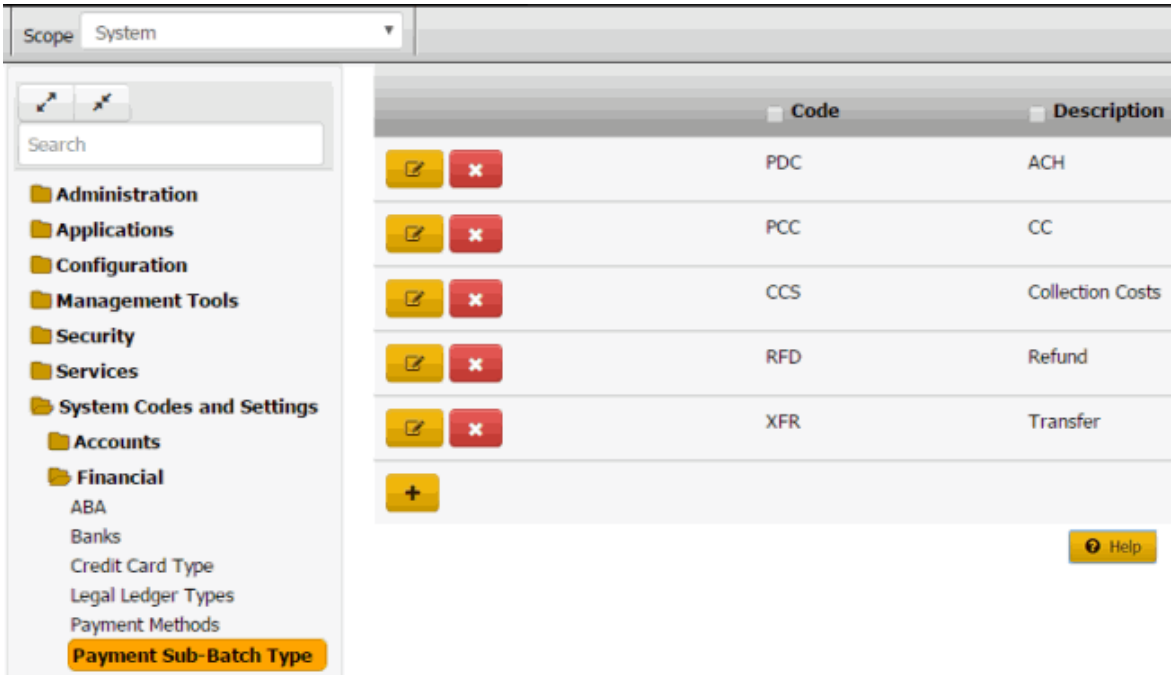
You can search for, add, modify, and delete payment sub-batch types. Sub-batches allow you to further categorize payment types.

Add a Payment Sub-Batch Type

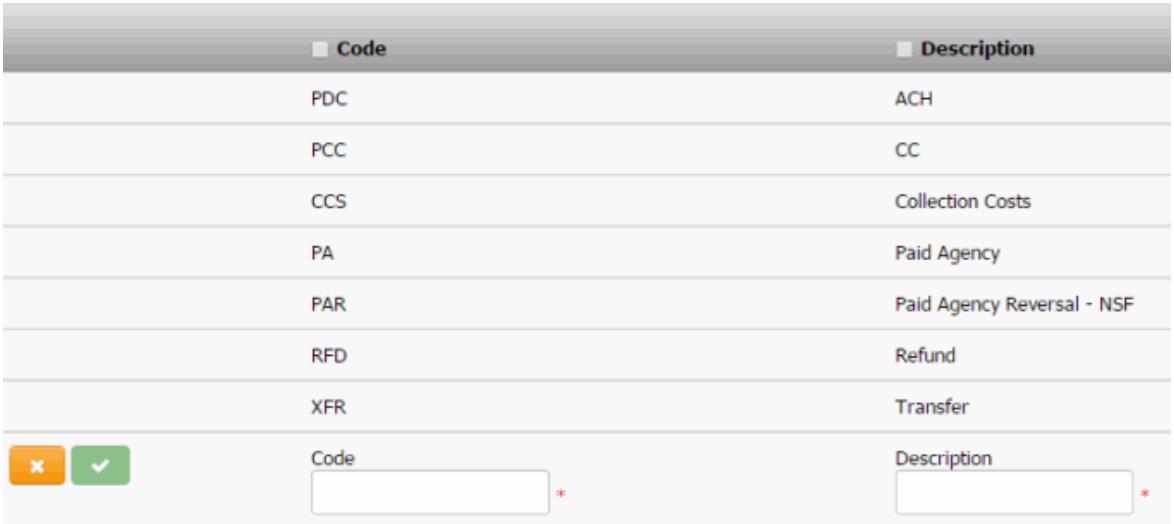
Use the **Payment Sub-Batch Type** panel to add a payment sub-batch type.

To add a payment sub-batch type

1. In the **Navigation** pane, click **System Codes and Settings** > **Financial** > **Payment Sub-Batch Type**.



2. Click the plus sign (+). A blank row appears in the data grid.



Code: Unique three-character code that identifies the payment sub-batch.

Description: Description of the payment sub-batch.

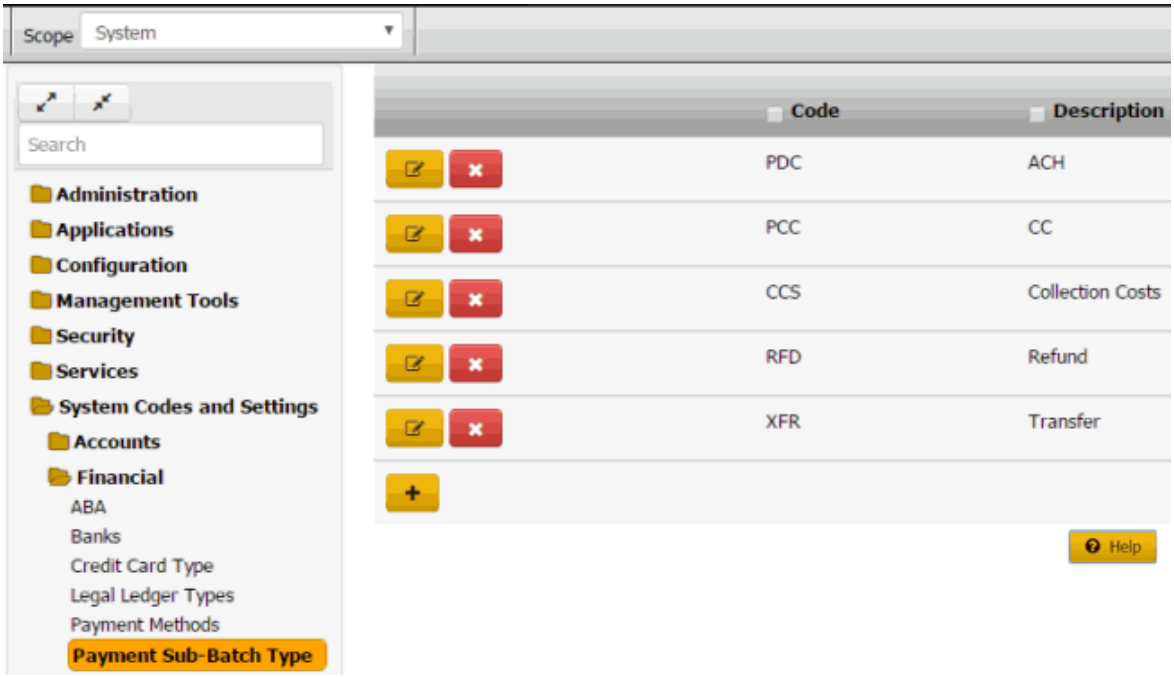
3. Complete the information and then click the check mark.

Modify a Payment Sub-Batch Type

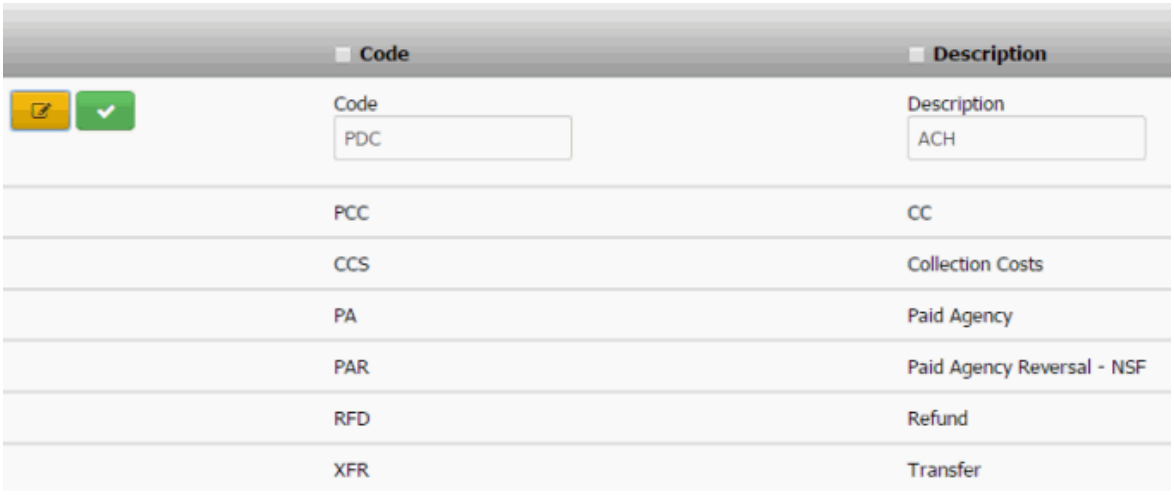
Use the **Payment Sub-Batch Type** panel to modify a payment sub-batch type.

To modify a payment sub-batch type

1. In the **Navigation** pane, click **System Codes and Settings** > **Financial** > **Payment Sub-Batch Type**.



2. Click the Edit icon. The payment sub-batch appears in edit mode.



Code: Unique three-character code that identifies the payment sub-batch.

Description: Description of the payment sub-batch.

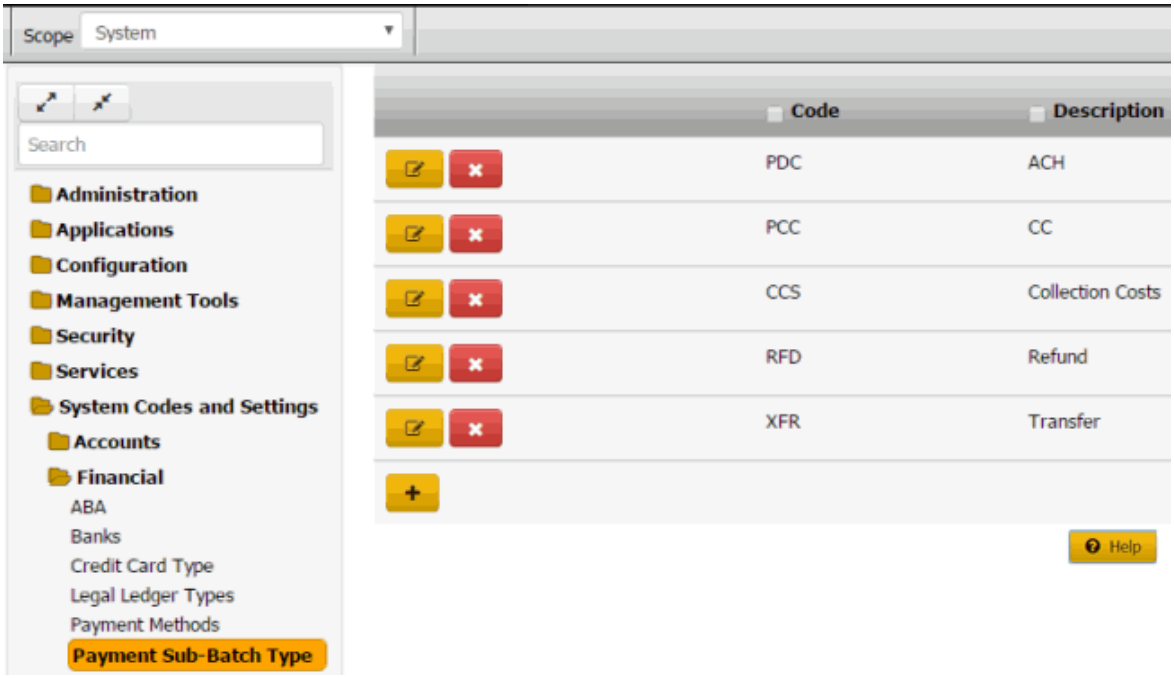
3. Modify the information and then click the check mark.

Delete a Payment Sub-Batch Type

Use the **Payment Sub-Batch Type** panel to delete a payment sub-batch type.

To delete a payment sub-batch type

1. In the **Navigation** pane, click **System Codes and Settings** > **Financial** > **Payment Sub-Batch Type**.



2. Click the Delete icon and then click **Yes**.

Salesman Codes

Salesman Codes

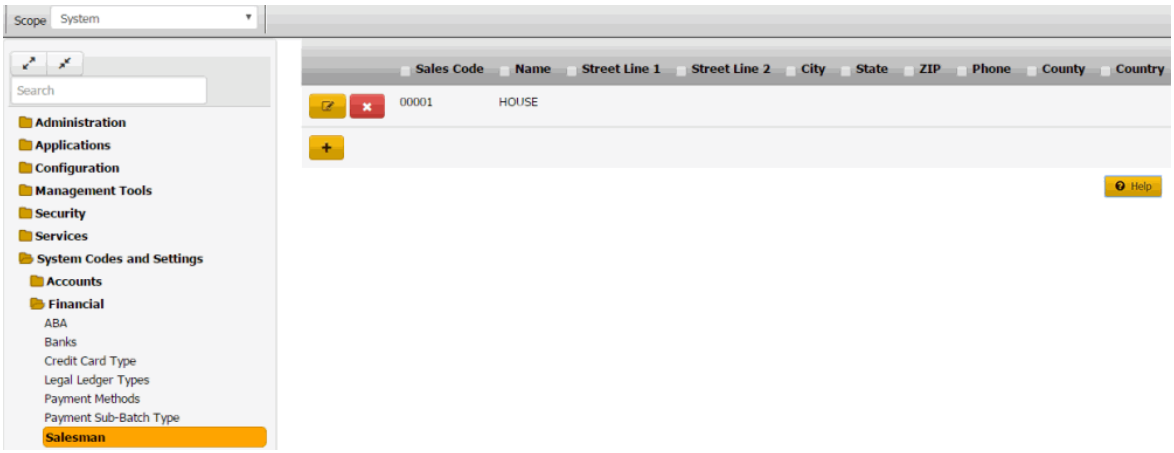
You can search for, add, modify, and delete salesmen. Users can assign an individual salesman to each client to track the number and value of accounts placed. The system also tracks the money collected and fees placed against accounts for each salesman in an office. For more information, see Maintain Client Account Information.

Add a Salesman

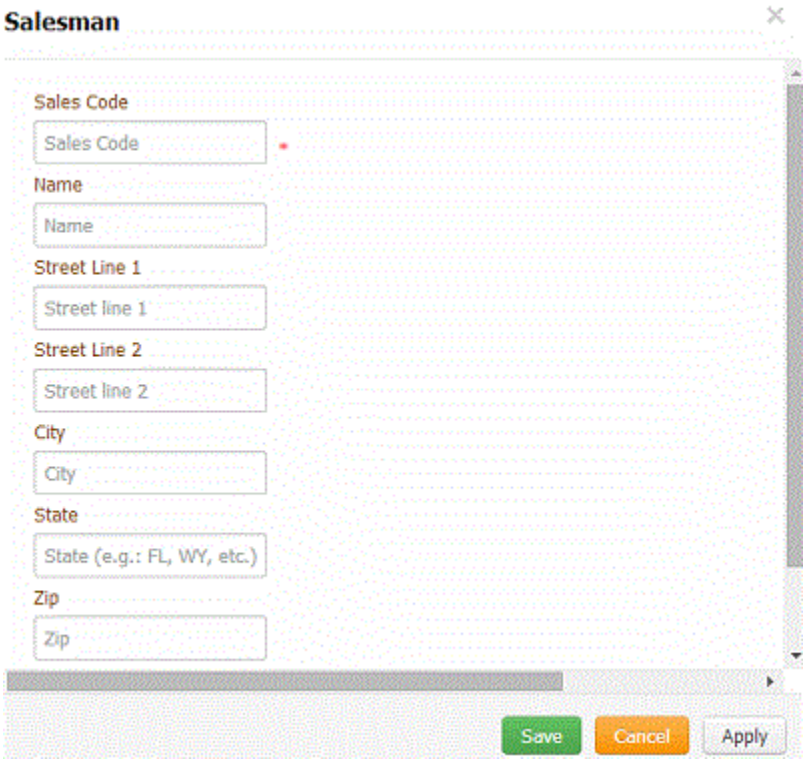
Use the **Salesman** dialog box to add a sales person.

To add a salesman

1. In the **Navigation** pane, click **System Codes and Settings** > **Financial** > **Salesman**.



2. Click the plus sign (+). The **Salesman** dialog box appears.



Sales Code: Unique code that identifies the sales person.

Name: Sales person's full name, including first name, last name, and suffix.

Street Line 1: First line of the sales person's street address.

Street Line 2: Second line of the sales person's street address.

City: Sales person's city.

State: Sales person's state.

ZIP: Sales person's postal code.

Phone: Sales person's phone number, including area code.

County: Sales person's county.

Country: Sales person's country.

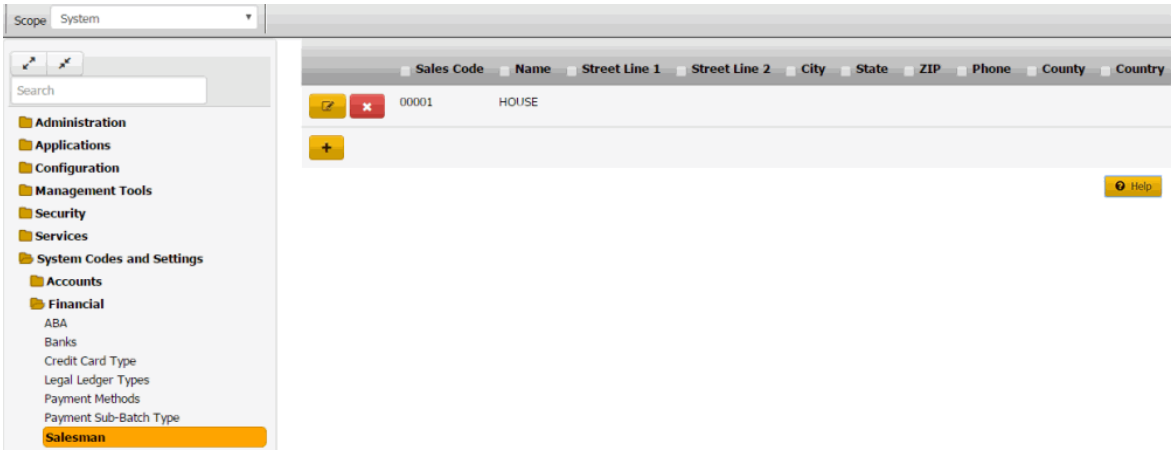
3. Complete the information and then click **Save**.

Modify a Salesman

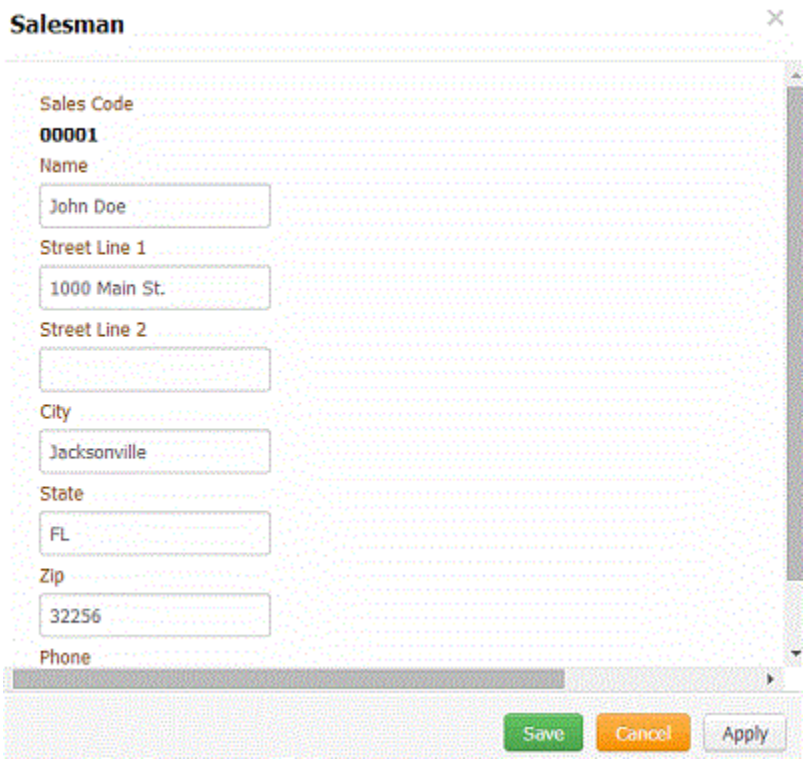
Use the **Salesman** dialog box to modify a sales person.

To modify a salesman

1. In the **Navigation** pane, click **System Codes and Settings** > **Financial** > **Salesman**.



2. Click the Edit icon. The **Salesman** dialog box appears.



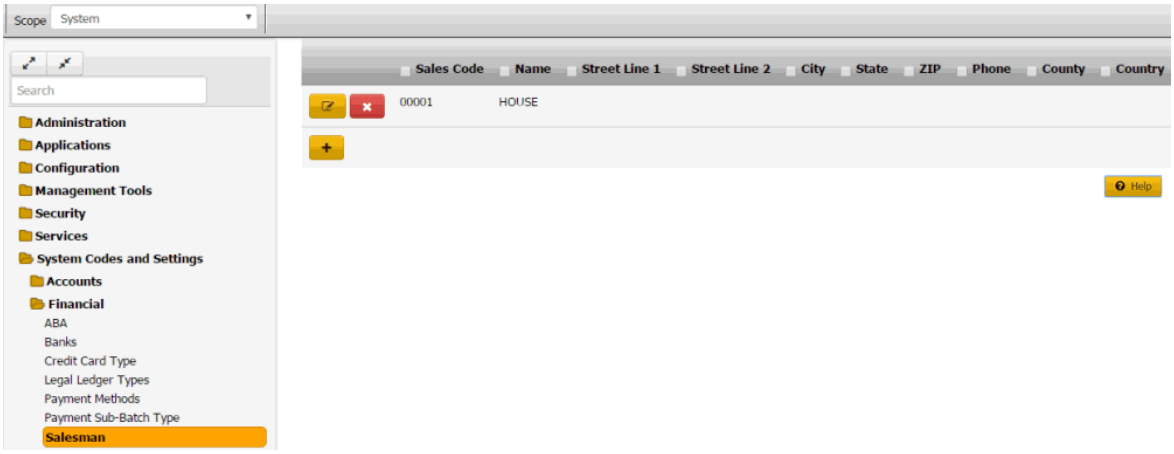
3. Modify the information and then click **Save**.

Delete a Salesman

Use the **Salesman** panel to delete a sales person.

To delete a salesman

1. In the **Navigation** pane, click **System Codes and Settings** > **Financial** > **Salesman**.



2. Click the Delete icon and then click **Yes**.

General Settings

General Settings

You can set up and configure law lists and state restrictions.

Law Lists

Law Lists

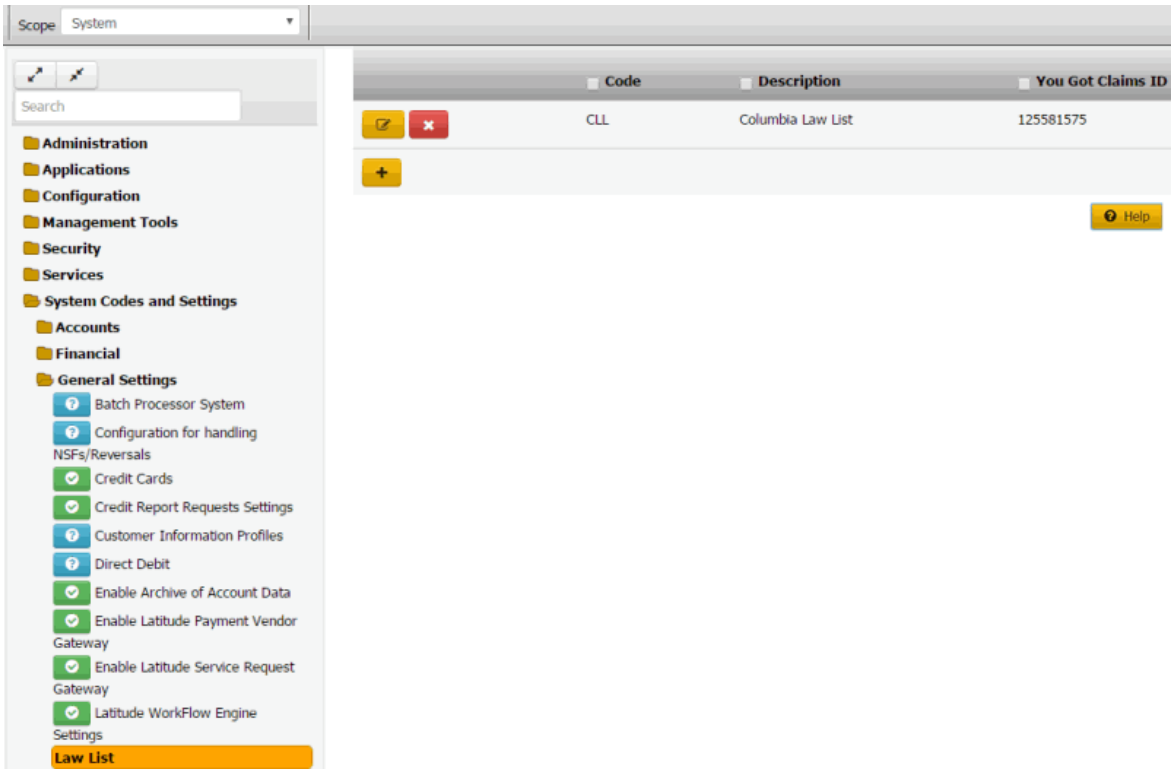
You can search for, add, modify, and delete law lists that your organization references when seeking the services of a collection attorney.

Add a Law List

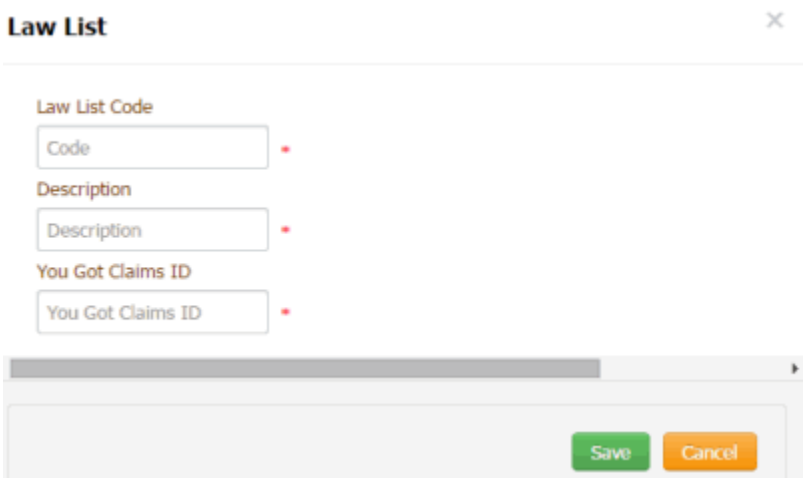
Use the **Law List** dialog box to add a law list code.

To add a law list

1. In the **Navigation** pane, click **System Codes and Settings** > **General Settings** > **Law List**.



2. Click the plus sign (+). The **Law List** dialog box appears.



Law List Code: Code that identifies the law list.

Description: Description or name of the law list.

You Got Claims ID: You've Got Claims identifier.

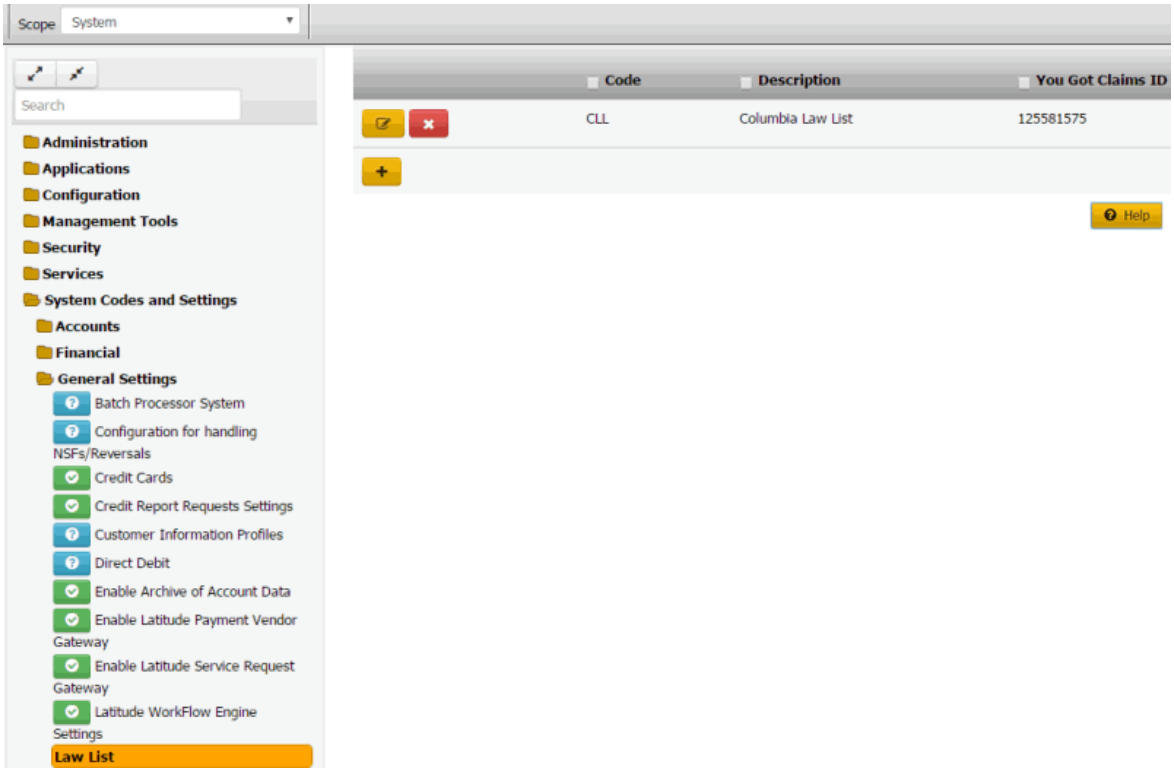
3. Complete the information and then click **Save**.

Modify a Law List

Use the **Law List** dialog box to modify a law list code.

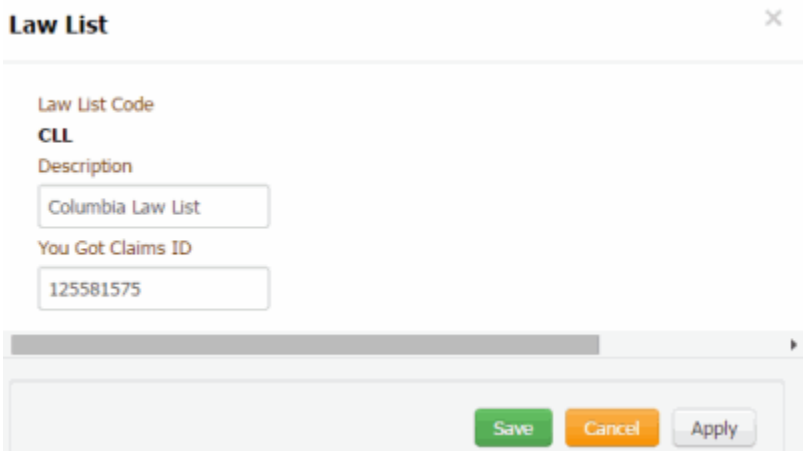
To modify a law list

1. In the **Navigation** pane, click **System Codes and Settings** > **General Settings** > **Law List**.



You Got Claims ID: You've Got Claims identifier.

2. Click the Edit icon. The **Law List** dialog box appears.



Law List Code: Code that identifies the law list.

Description: Description or name of the law list.

You Got Claims ID: You've Got Claims identifier.

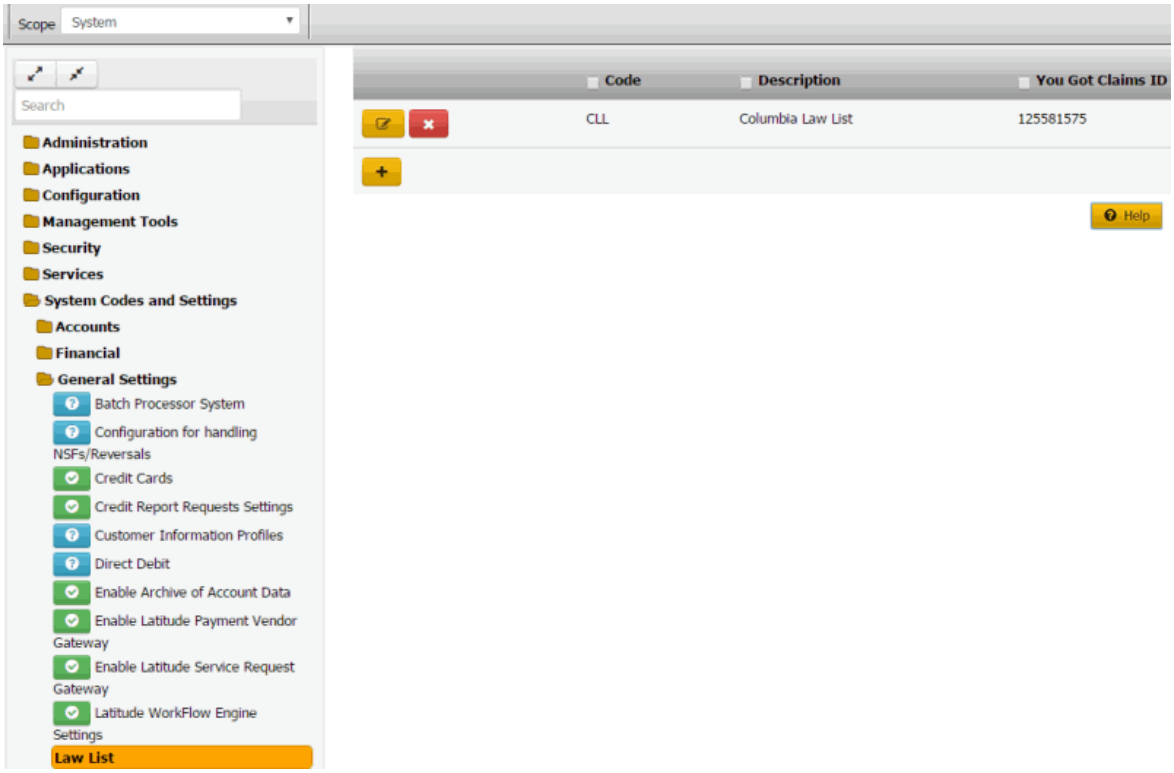
3. Modify the information and then click **Save**.

Delete a Law List

Use the **Law List** panel to delete a law list code.

To delete a law list code

1. In the **Navigation** pane, click **System Codes and Settings** > **General Settings** > **Law List**.



2. Click the Delete icon and then click **Yes**.

State Restriction

State Restriction

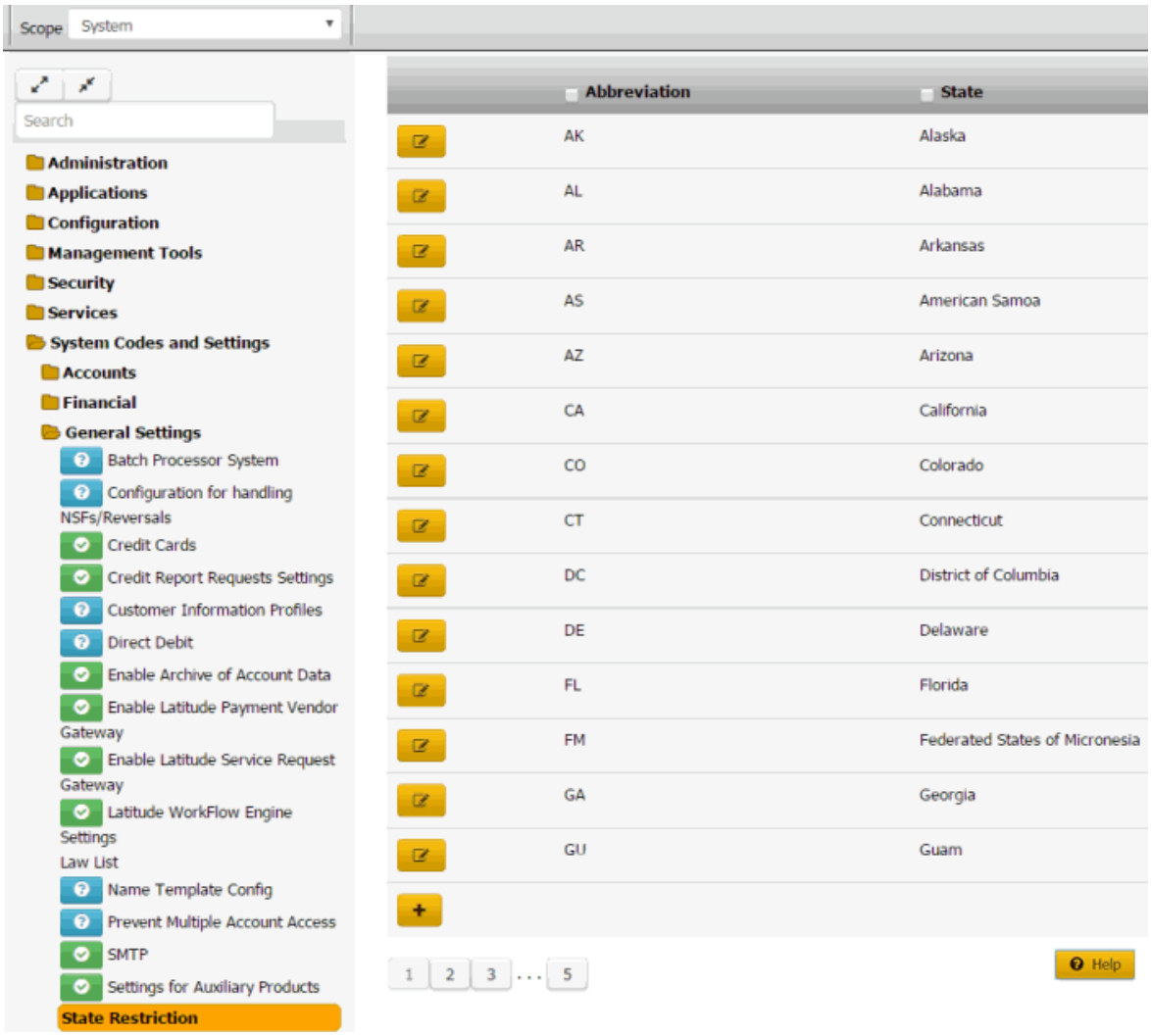
You can add and modify state restrictions that control how the system handles accounts within specific states. For example, letter restrictions, printed advisories, warnings, and surcharges.

Add a State Restriction

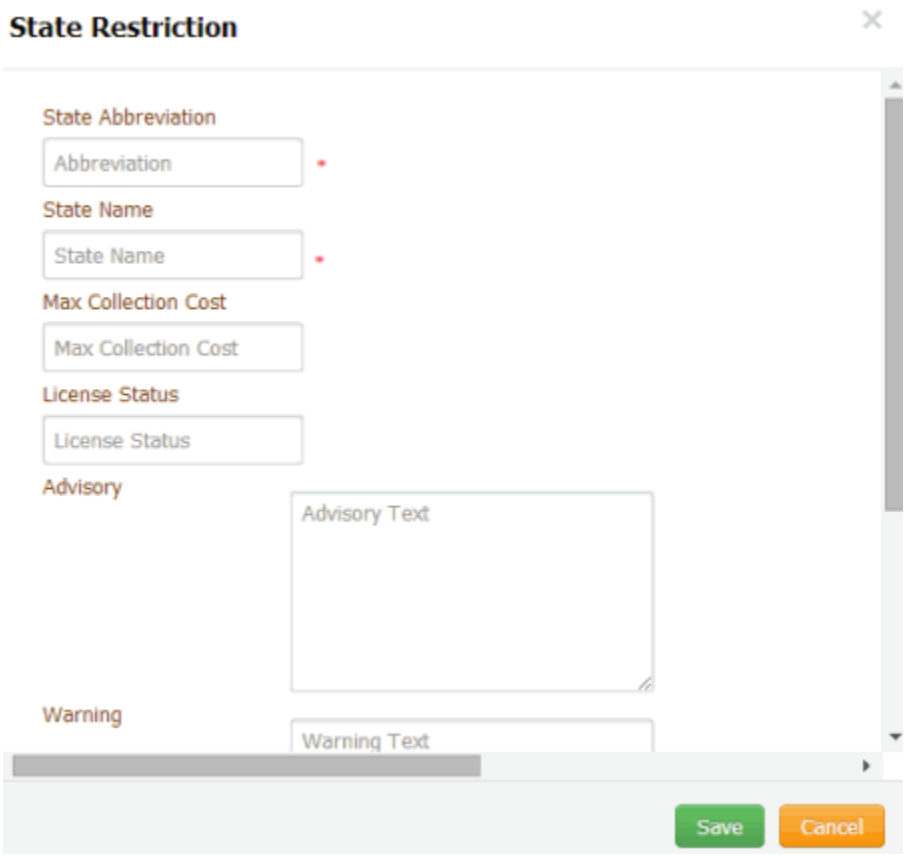
Use the **State Restriction** dialog box to add a state restriction.

To add a state restriction

1. In the **Navigation** pane, click **System Codes and Settings** > **General Settings** > **State Restriction**.



2. Click the plus sign (+). The **State Restriction** dialog box appears.



State Abbreviation: Unique code that identifies the state.

State Name: Full name of the state.

Max Collection Cost: Maximum collection cost percent the state allows. You can configure the client record to allow agents to override this percent for customers residing in the state.

License Status: Optional place to store licensing information.

Advisory: Advisory information to print on letters for customers residing in the state. The system inserts this information in letters when you include the **State_Legal_Advisory** merge field in the letter body.

Warning: Warning information to display in the **Warnings** dialog box when the account first appears in the **Work Form** for customers residing in the state.

Restrict Letters: If selected, the state restricts the letters you can send to customers residing in the state.

Permit a Wage Garnishment: If selected, the state allows administrative wage garnishment.

Permit Surcharge: If selected, the state allows collection of surcharges for customers residing in the state. If cleared, the surcharge option isn't available when creating payment arrangements.

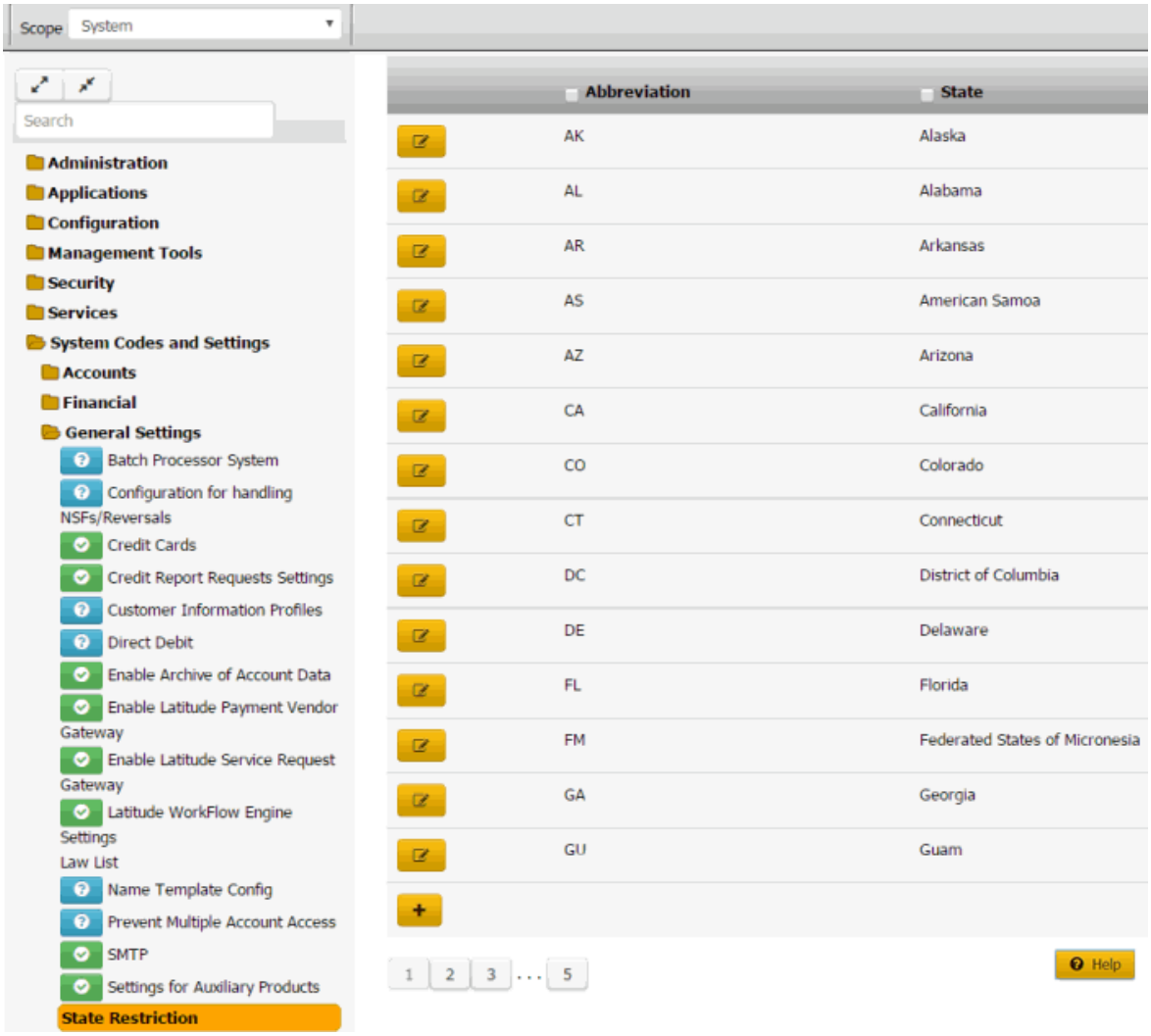
3. Complete the information and then click **Save**.

Modify a State Restriction

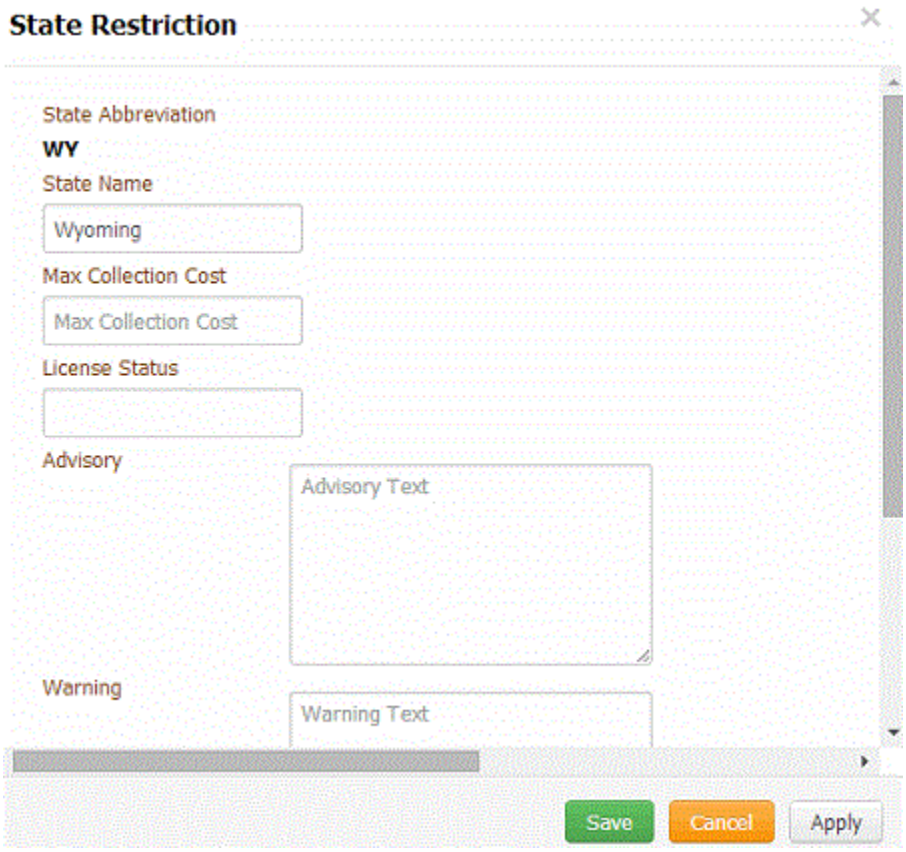
Use the **State Restriction** dialog box to modify a state restriction.

To modify a state restriction

1. In the **Navigation** pane, click **System Codes and Settings** > **General Settings** > **State Restriction**.



2. Click the Edit icon. The **State Restriction** dialog box appears.



State Abbreviation: Unique code that identifies the state.

State Name: Full name of the state.

Max Collection Cost: Maximum collection cost percent the state allows. You can configure the client record to allow agents to override this percent for customers residing in the state.

License Status: Optional place to store licensing information.

Advisory: Advisory information to print on letters for customers residing in the state. The system inserts this information in letters when you include the **State_Legal_Advisory** merge field in the letter body.

Warning: Warning information to display in the **Warnings** dialog box when the account first appears in the **Work Form** for customers residing in the state.

Restrict Letters: If selected, the state restricts the letters you can send to customers residing in the state.

Permit a Wage Garnishment: If selected, the state allows administrative wage garnishment.

Permit Surcharge: If selected, the state allows collection of surcharges for customers residing in the state. If cleared, the surcharge option isn't available when creating payment arrangements.

3. Modify the information and then click **Save**.

Organization Groups

Organization Groups

You can set up and configure various groups in Latitude. These groups allow you to streamline the process of granting permissions and assigning accounts. You can grant permissions to:

- An individual user.
- A role that you assigned to one or more users.
- A branch in your organization that you assigned to one or more users.
- A desk that you assigned to a user.
- A department in your organization.
- A team in your organization.

Branches

Branches

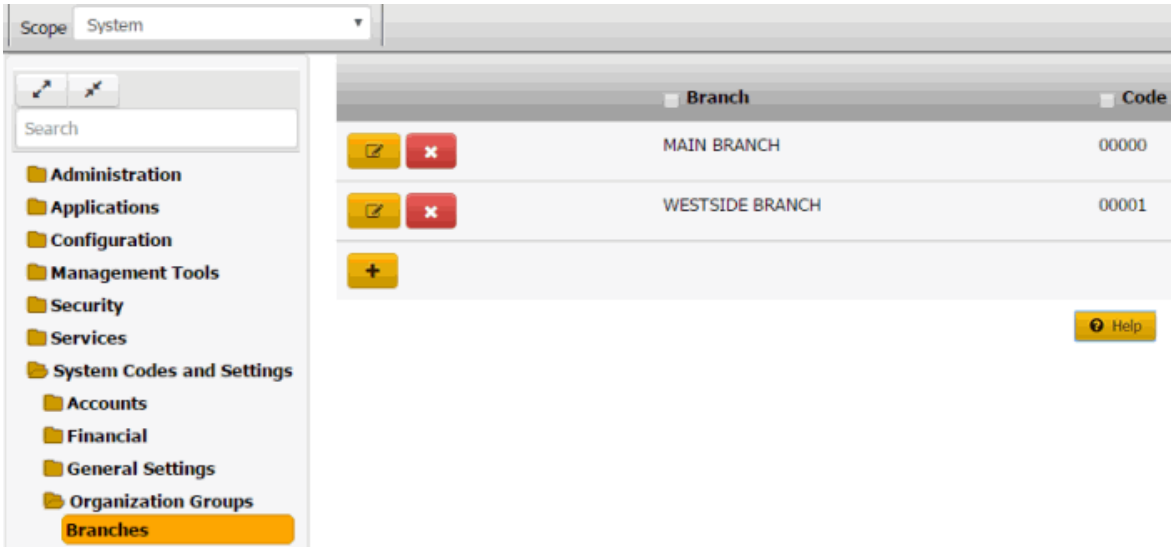
You can search for, add, modify, and delete branches. If you have more than one office (or branch), you can set up a branch and assign it to accounts to provide inventory separation by location.

Add a Branch

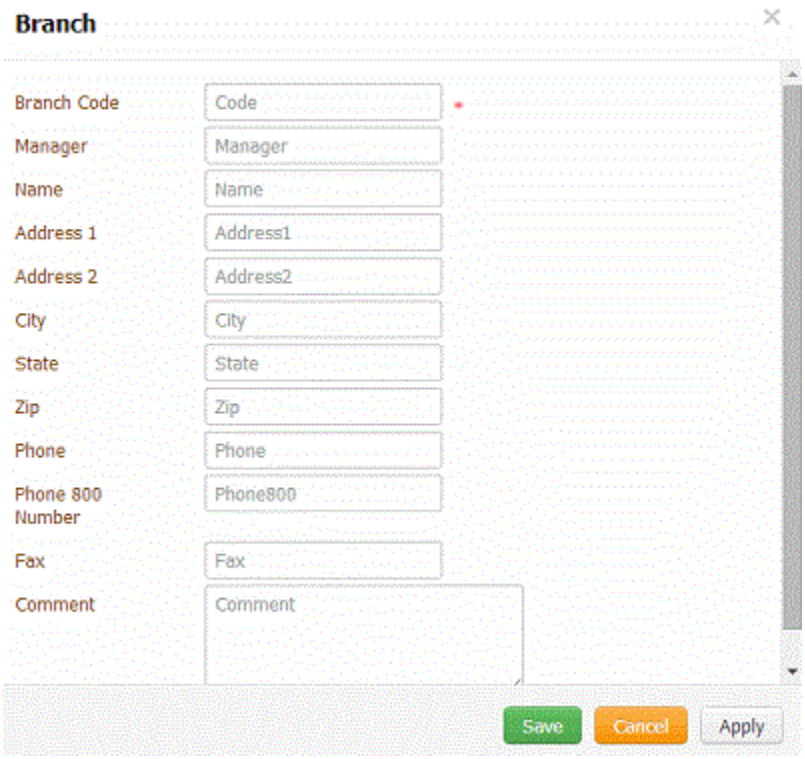
Use the **Branch** dialog box to add a branch.

To add a branch

1. In the **Navigation** pane, click **System Codes and Settings** > **Organization Groups** > **Branches**.



2. Click the plus sign (+). The **Branch** dialog box appears.



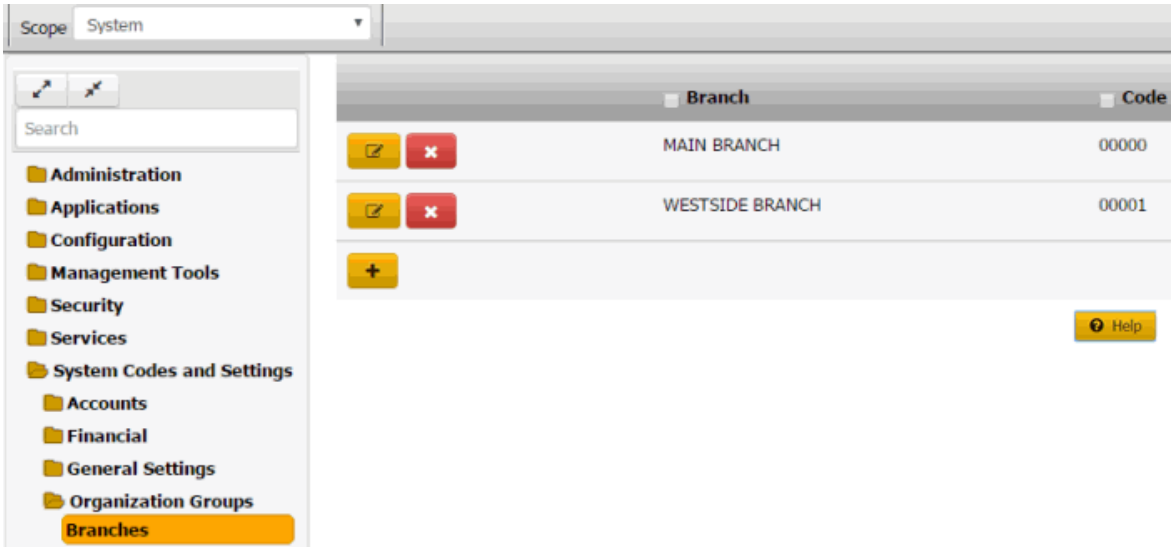
3. Complete the information and then click **Save**.

Modify a Branch

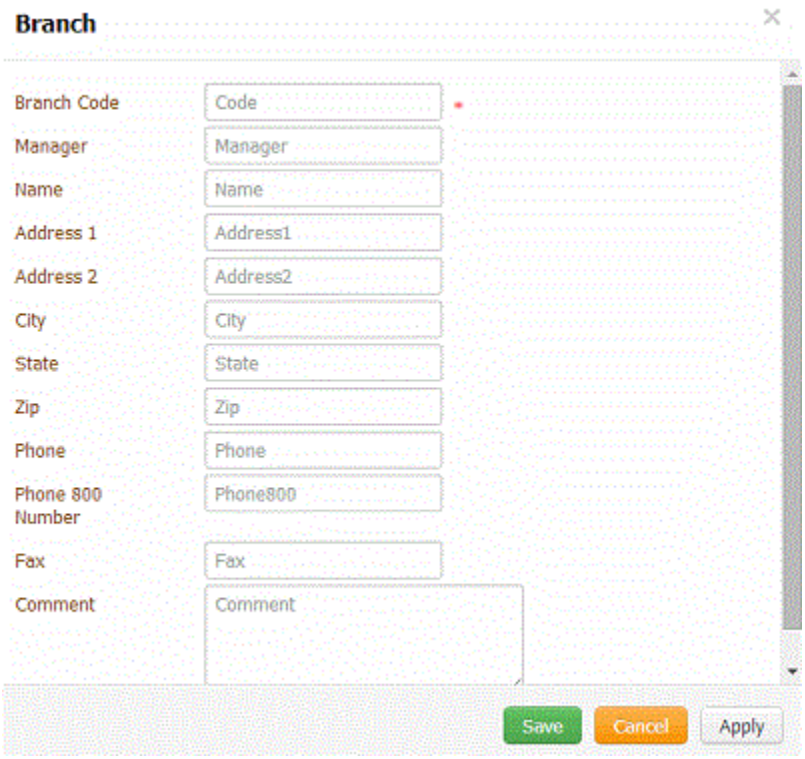
Use the **Branch** dialog box to modify a branch.

To modify a branch

1. In the **Navigation** pane, click **System Codes and Settings** > **Organization Groups** > **Branches**.



2. Click the Edit icon. The **Branch** dialog box appears.



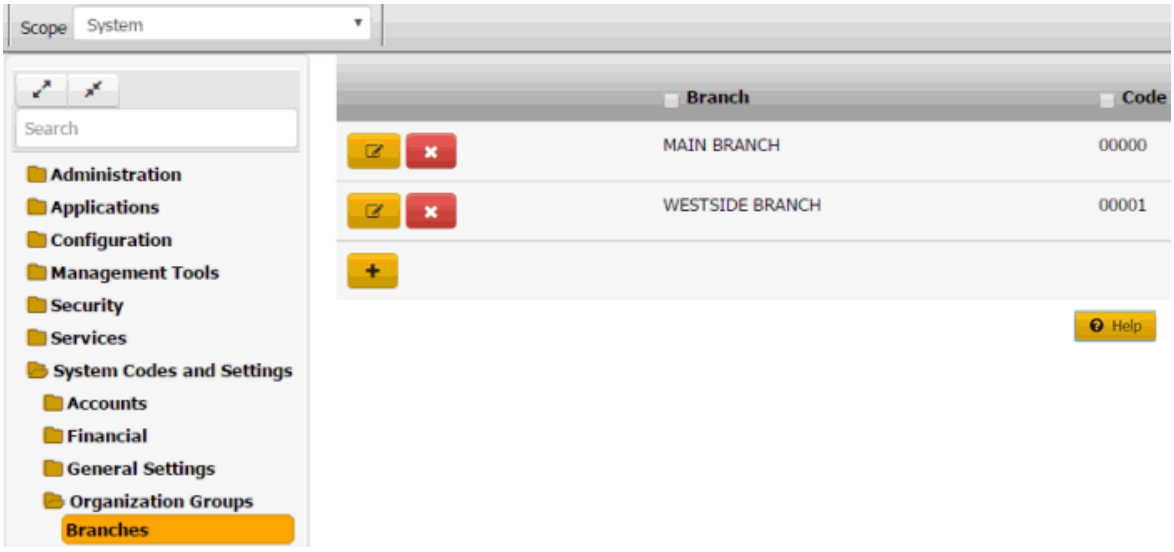
3. Modify the information and then click **Save**.

Delete a Branch

Use the **Branches** panel to delete a branch that your organization didn't assign to another entity, such as a user, department, or account.

To delete a branch

1. In the **Navigation** pane, click **System Codes and Settings** > **Organization Groups** > **Branches**.



2. Click the Delete icon and then click **Yes**.

Departments

Departments

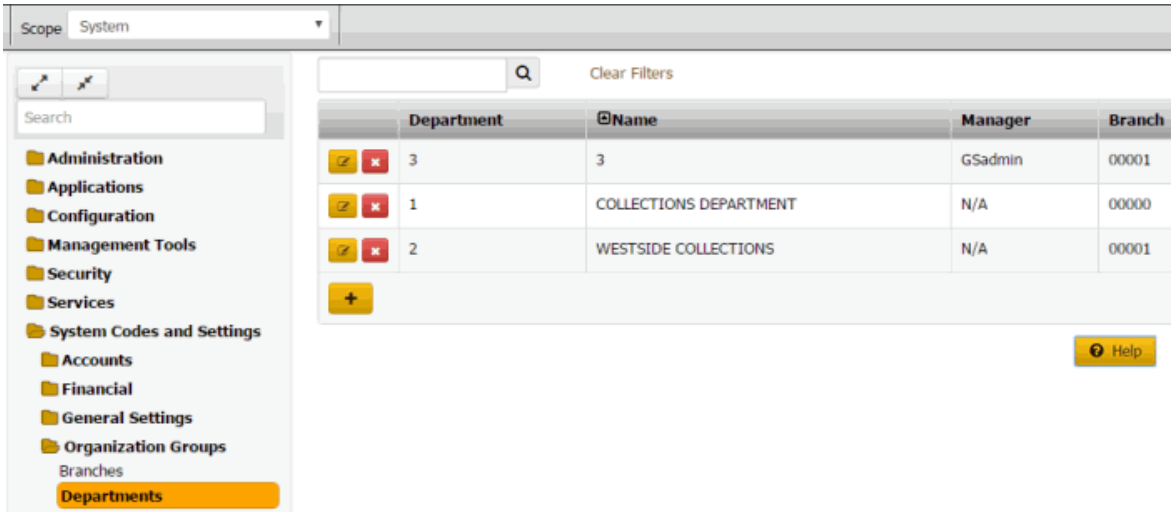
You can search for, add, modify, and delete departments. You assign departments to a specific branch.

Search for a Department

Use the **Departments** panel to search for a department.

To search for a department

1. In the **Navigation** pane, click **System Codes and Settings** > **Organizational Groups** > **Departments**.



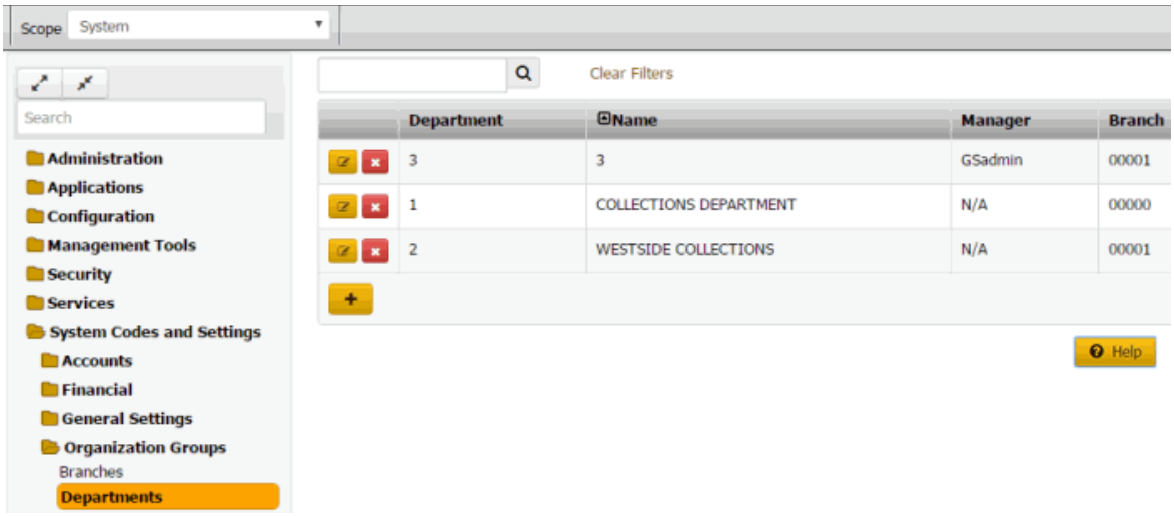
2. In the **Search** box in the **Departments** panel, type one or more characters to search and then press **Enter** or click the Search icon. The system searches the department code, name, manager, and branch for a match. It displays only the departments that match your search criteria.
3. To clear the search criteria, click **Clear Filters**. The system displays all departments.

Add a Department

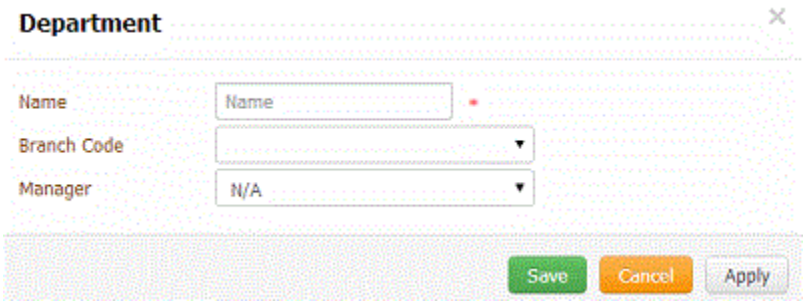
Use the **Department** dialog box to add a department.

To add a department

1. In the **Navigation** pane, click **System Codes and Settings** > **Organization Groups** > **Departments**.



2. Click the plus sign (+). The **Department** dialog box appears.



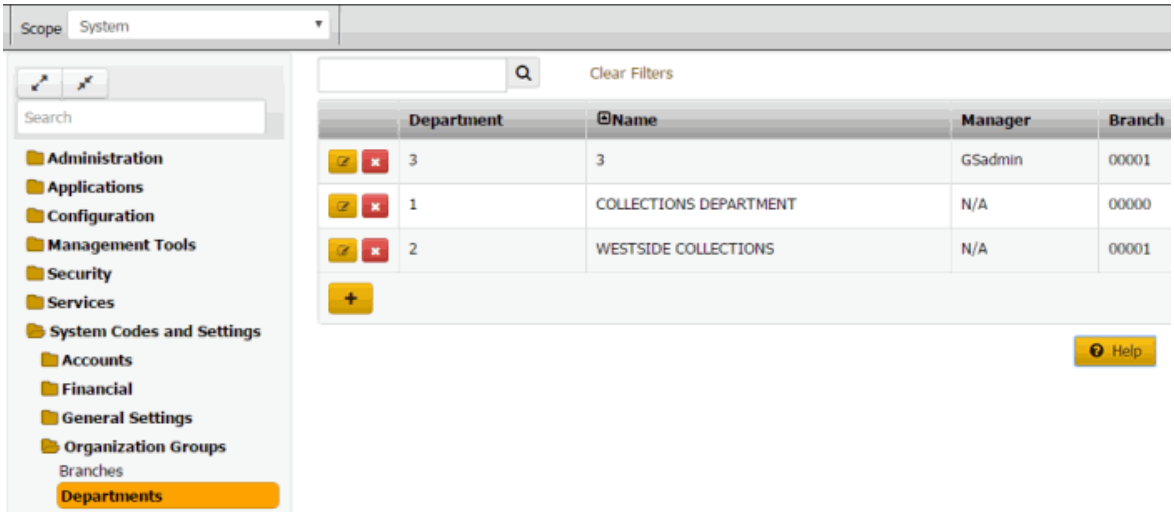
3. Complete the information and then click **Save**.

Modify a Department

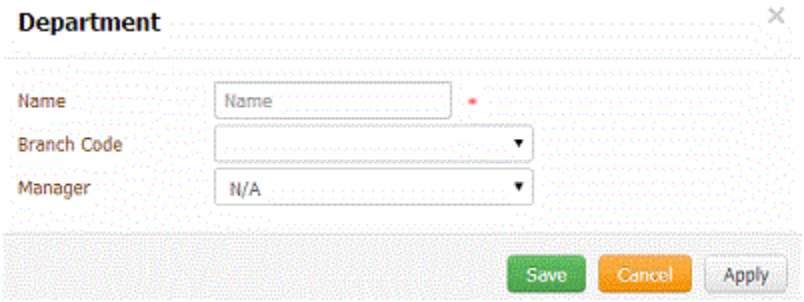
Use the **Department** dialog box to modify a department.

To modify a department

1. In the **Navigation** pane, click **System Codes and Settings** > **Organization Groups** > **Departments**.



2. Click the Edit icon. The **Department** dialog box appears.



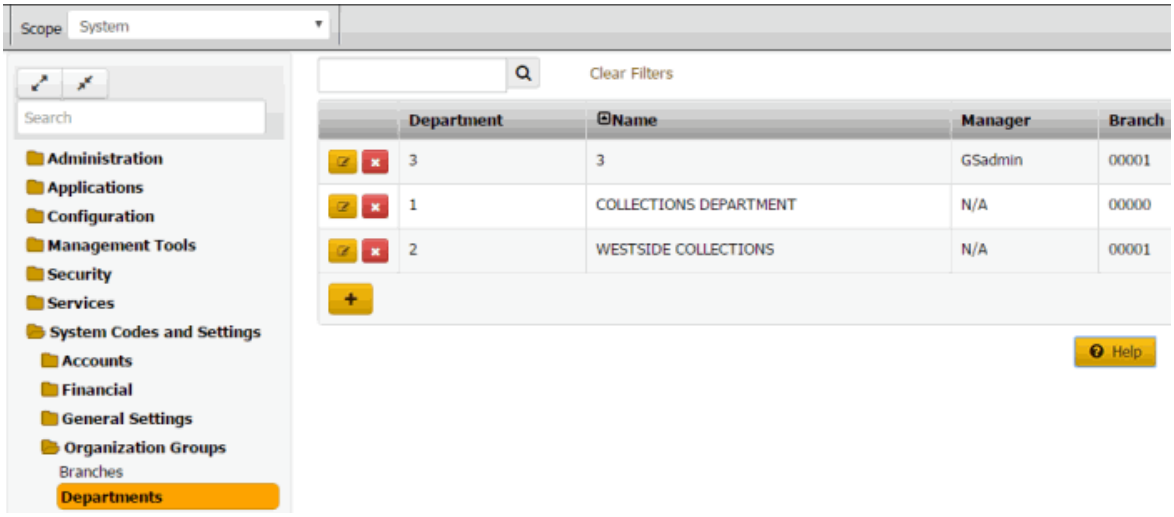
3. Modify the information and then click **Save**.

Delete a Department

Use the **Departments** panel to delete a department.

To delete a department

1. In the **Navigation** pane, click **System Codes and Settings** > **Organization Groups** > **Departments**.



2. Click the Delete icon and then click **Yes**.

Roles

Roles

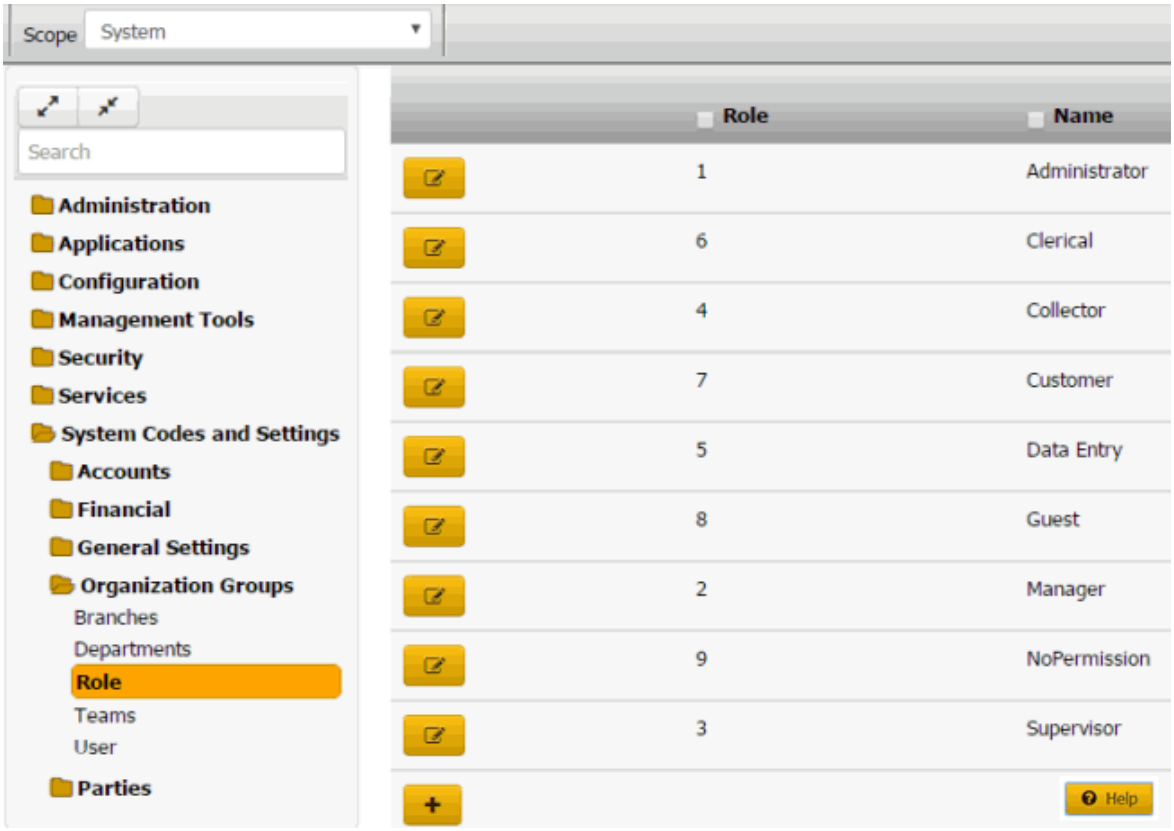
You can search for, add, modify, copy, and delete roles. Roles facilitate granting multiple permissions to multiple users who require the same permissions. For more information about permissions and policies for roles, see Permissions and Policies.

Add a Role

Use the **Role** dialog box to add a role. After adding a role, assign permissions to the role and assign the role to one or more users.

To add a role

1. In the **Navigation** pane, click **System Codes and Settings** > **Organization Groups** > **Role**.



2. Click the plus sign (+). The **Role** dialog box appears.

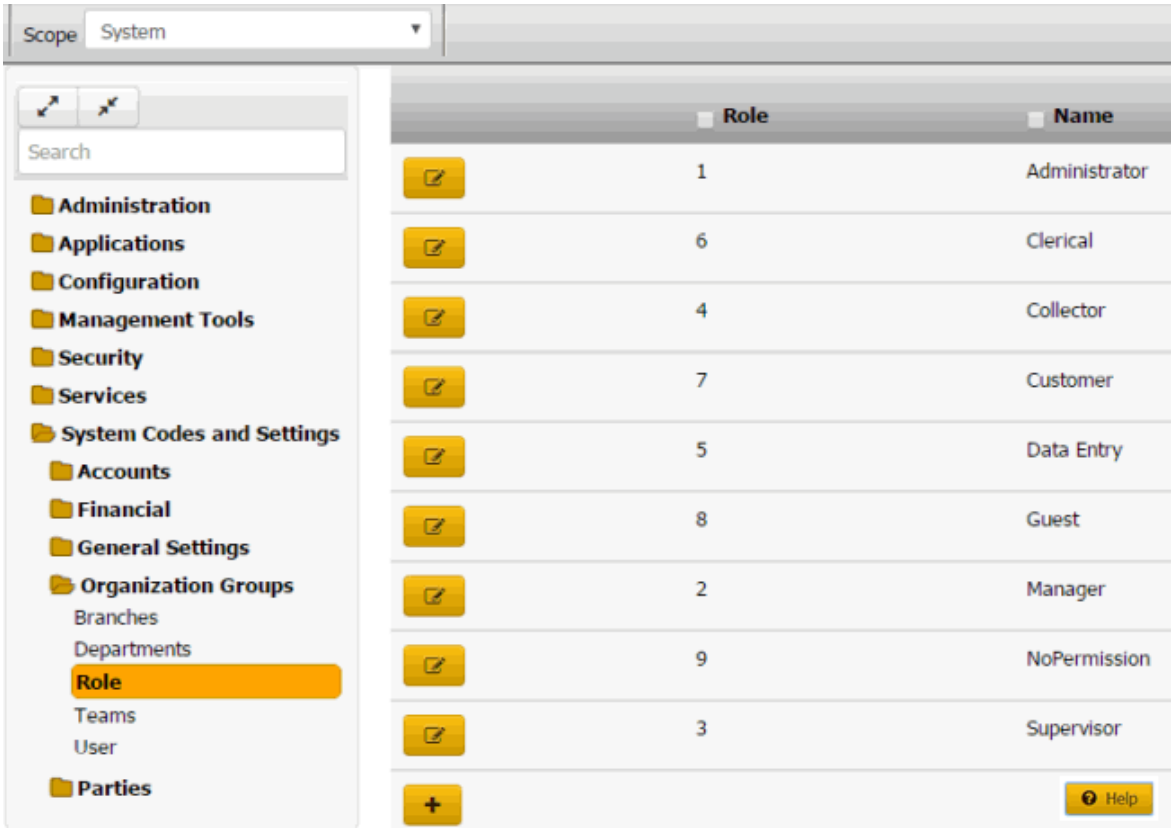
3. In the **Name** box, type the name of the new role and then click **Save**.

Modify a Role

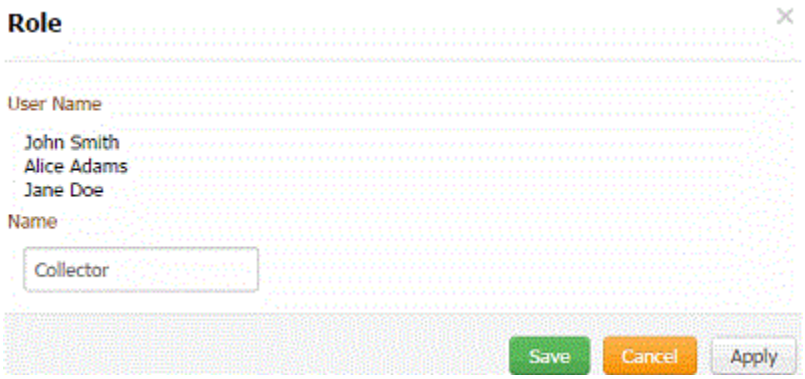
Use the **Role** dialog box to modify the name of a role or view the users assigned to a role.

To modify a role

1. In the **Navigation** pane, click **System Codes and Settings** > **Organization Groups** > **Role**.



2. Click the Edit icon. The **Role** dialog box appears.



User Name: Users assigned to the role.

3. In the **Name** box, modify the name of the role and then click **Save**.

Teams

Teams

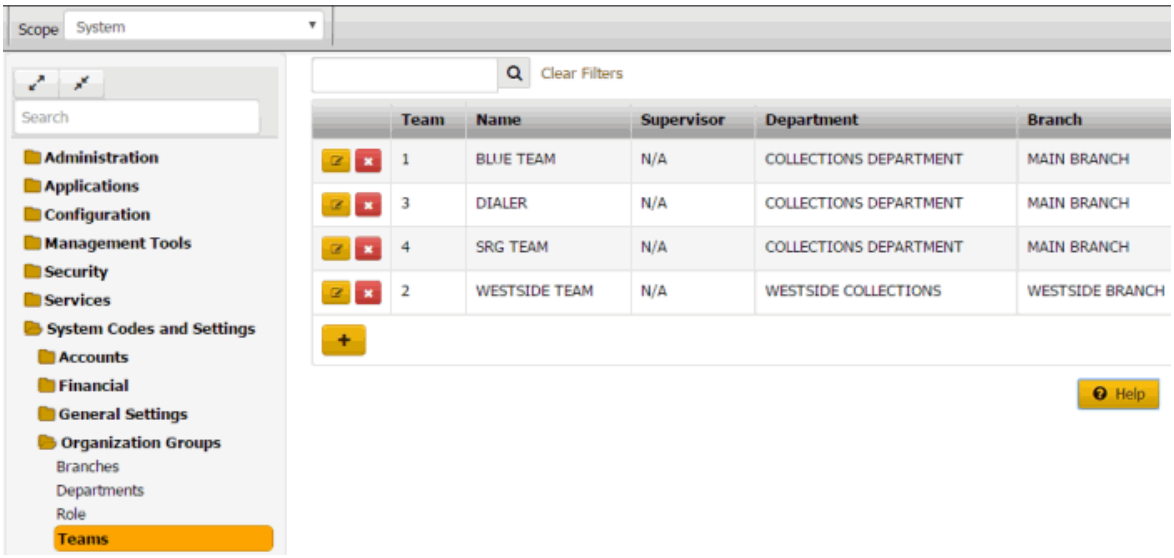
You can search for, add, modify, and delete teams. You assign teams to a specific department.

Search for a Team

Use the **Teams** panel to search for a team.

To search for a team

1. In the **Navigation** pane, click **System Codes and Settings** > **Organizational Groups** > **Teams**.



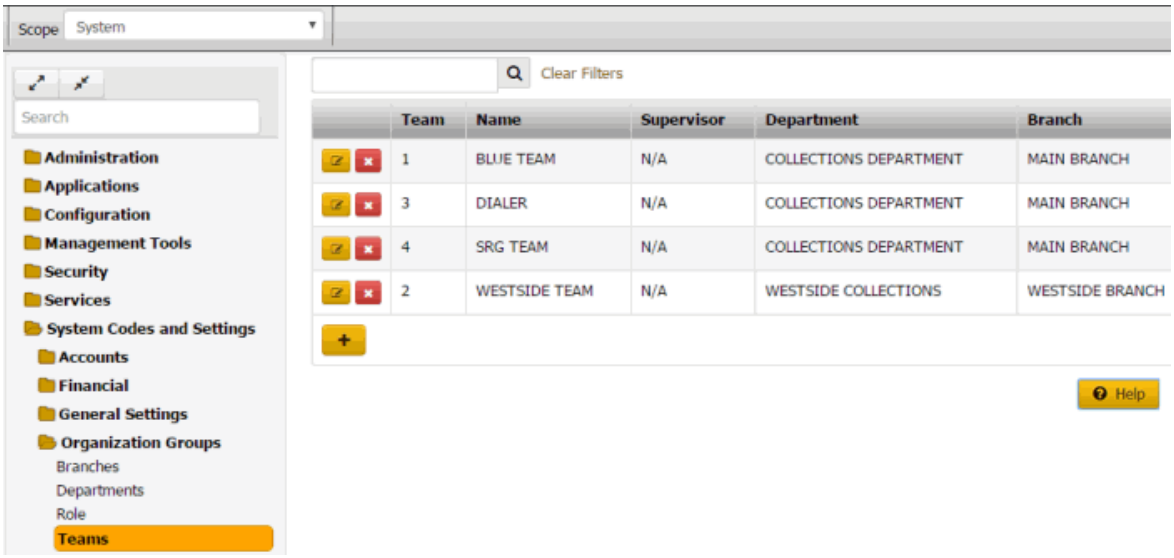
2. In the **Search** box in the **Teams** panel, type one or more characters to search and then press **Enter** or click the Search icon. The system searches the team code, name, supervisor, department, and branch for a match. It displays only the teams that match your search criteria.
3. To clear the search criteria, click **Clear Filters**. The system displays all teams.

Add a Team

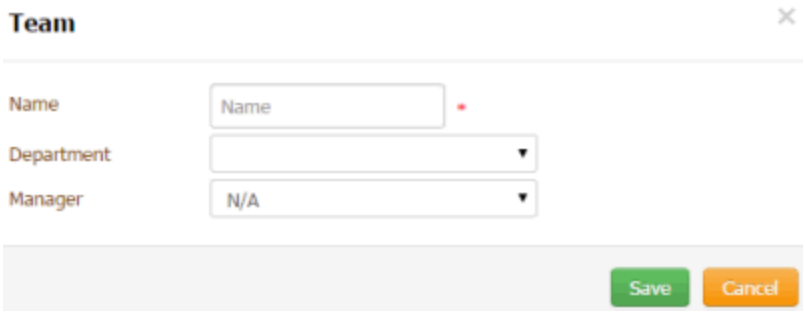
Use the **Team** dialog box to add a team code.

To add a team code

1. In the **Navigation** pane, click **System Codes and Settings** > **Organization Groups** > **Teams**.



2. Click the plus sign (+). The **Team** dialog box appears.



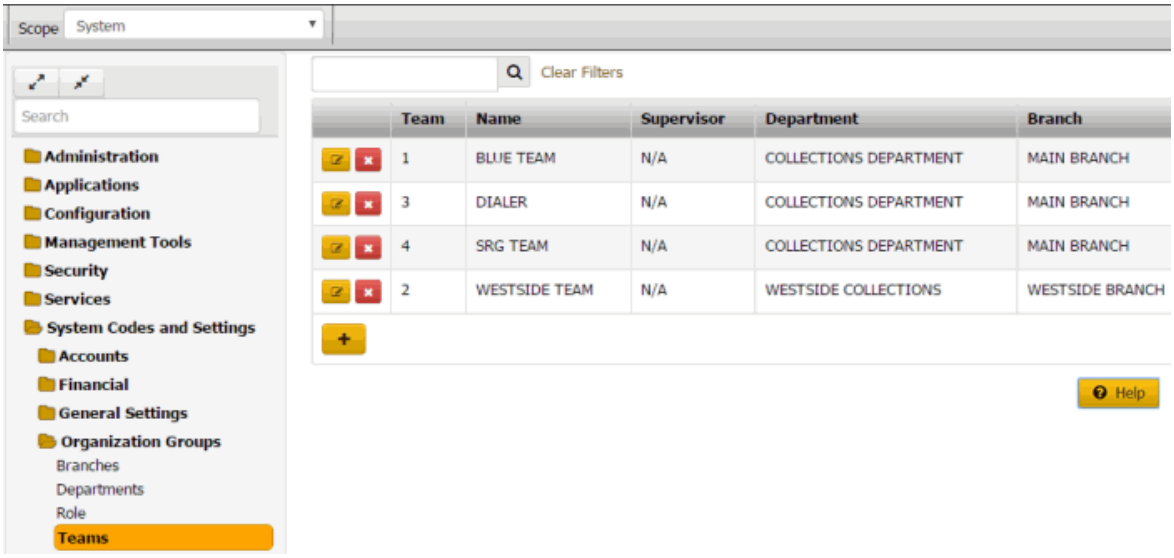
3. Complete the information and then click **Save**.

Modify a Team

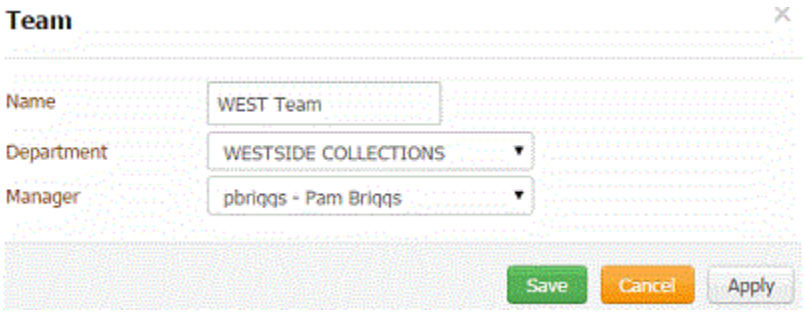
Use the **Team** dialog box to modify a team code.

To modify a team code

1. In the **Navigation** pane, click **System Codes and Settings** > **Organization Groups** > **Teams**.



2. Click the Edit icon. The **Team** dialog box appears.



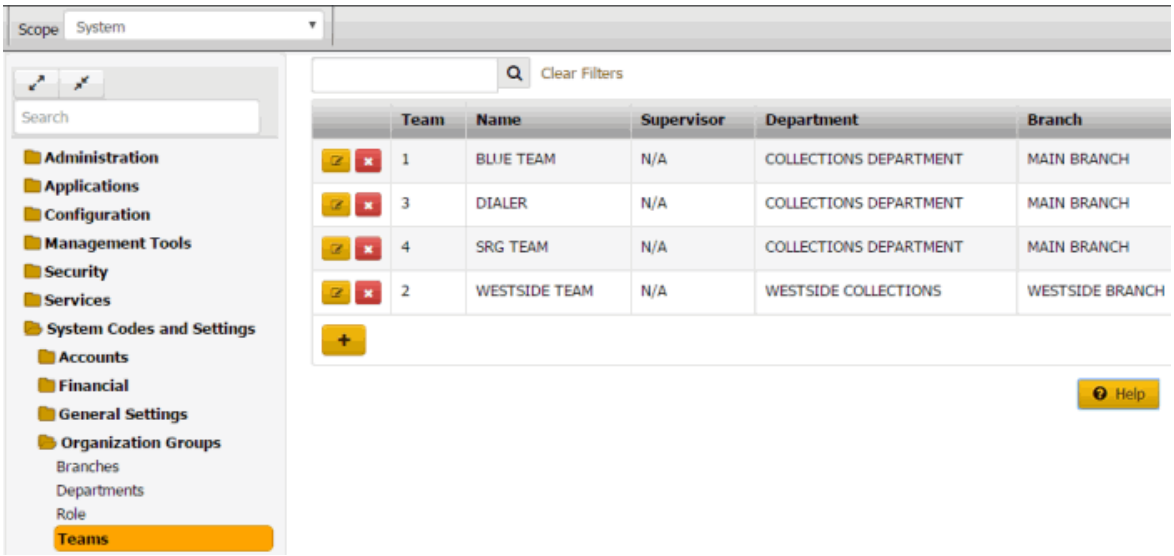
3. Modify the information and then click **Save**.

Delete a Team

Use the **Teams** panel to delete a team code.

To delete a team code

1. In the **Navigation** pane, click **System Codes and Settings** > **Organization Groups** > **Teams**.



2. Click the Delete icon and then click **Yes**.

Users

Users

You can search for, add, and modify users; and activate or deactivate user accounts. However, you cannot delete user accounts.

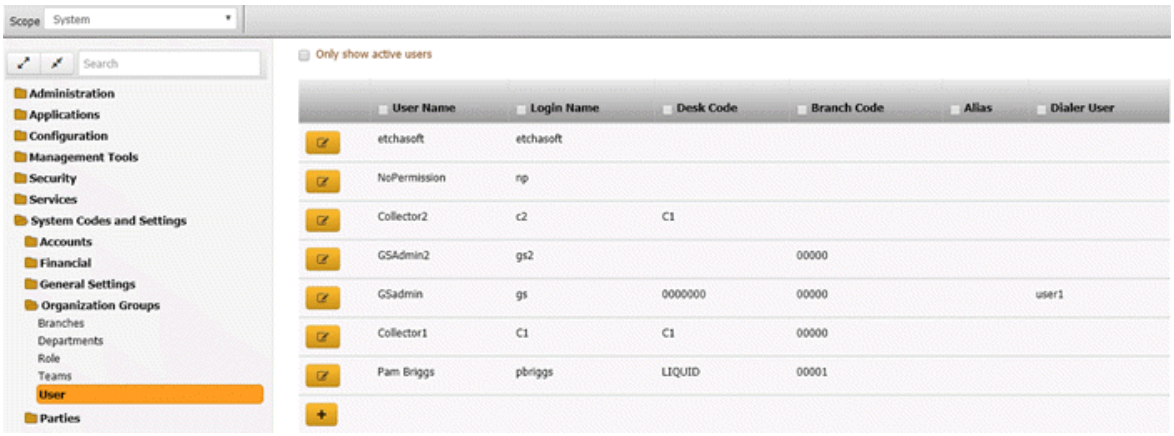
You can modify permissions and policies for a user after assigning the user to a role. If you change the permission or policy for a role, the change affects the users assigned to that role, unless you set the permission or policy at the user level. For more information about permissions and policies for users, see Permissions and Policies.

Add a User

Use the **User** dialog box to add a user. You cannot set a user's password through the add feature. To set the user's password, add the user and then use the edit feature.

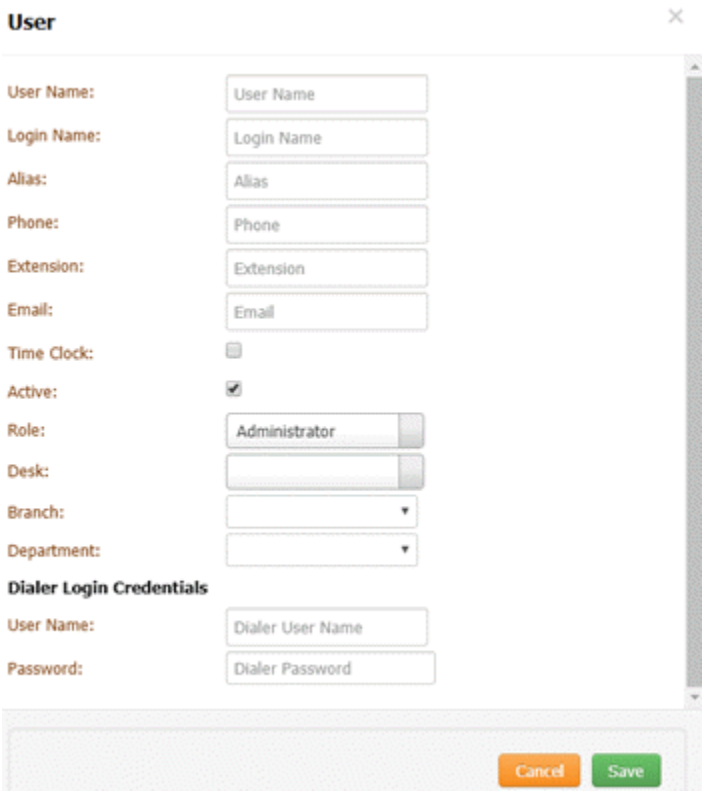
To add a user

1. In the **Navigation** pane, click **System Codes and Settings** > **Organization Groups** > **User**.



Tip: To display active users only in the data grid, click **Only show active users**.

2. Click the plus sign (+). The **User** dialog box appears.



User Name: User's first and last name.

Login Name: User's logon name.

Alias: User's alias name such as a shortened version of the first name or a nickname.

Phone: User's telephone number

Extension: User's telephone extension number.

Email: User's email address (for example, jdoe@mycompany.com).

Time Clock: If selected, the system includes the user's logon and logoff times on the User Logon report.

Active: If selected, the user can log on to the system. If cleared, the user cannot log on to the system.

Role: User's role.

Desk: User's desk.

Branch: User's branch.

Department: User's department.

Dialer Login Credentials: Latitude uses these credentials to log on the user to Dialer automatically.

User Name: User's logon name for Interaction Dialer.

Password: User's password for Interaction Dialer.

Windows ID: User's Windows authentication ID. If you specify a Windows ID, the user can choose to log on to Latitude using Windows authentication.

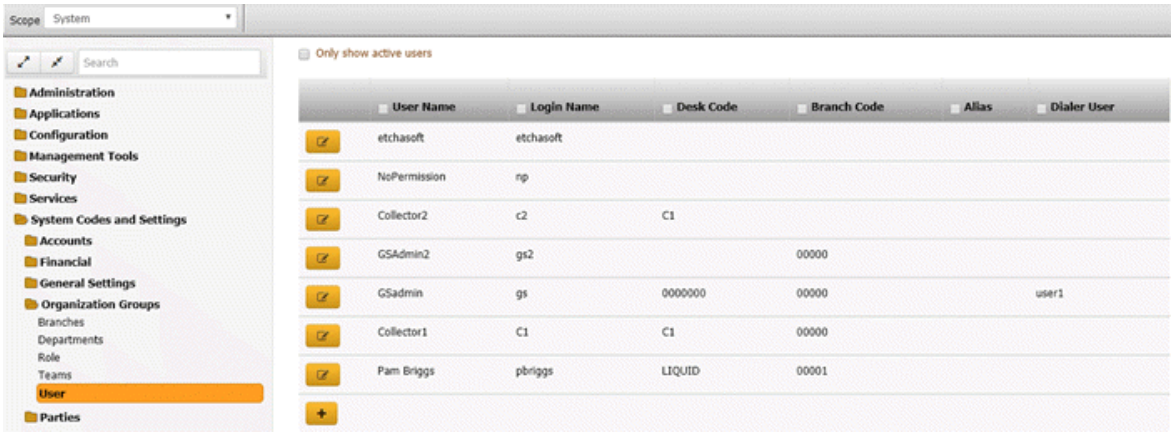
3. Complete the information and then click **Save**.

Modify a User

Use the **User** dialog box to modify a user.

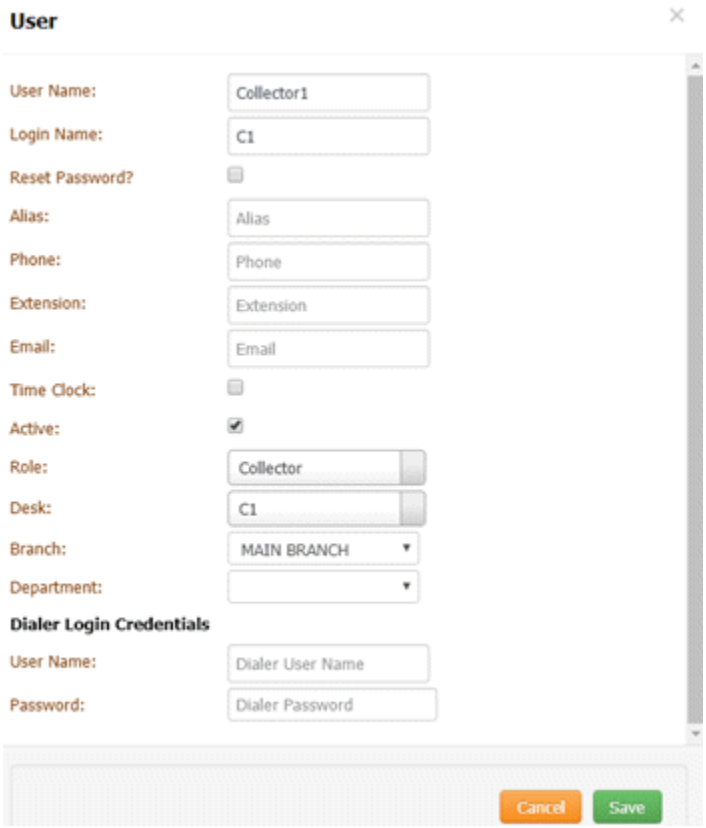
To modify a user

1. In the **Navigation** pane, click **System Codes and Settings** > **Organization Groups** > **User**.



Tip: To display active users only in the data grid, click **Only show active users**.

2. Click the Edit icon for the user account to modify. The **User** dialog box appears.



User Name: User's first and last name.

Login Name: User's logon name.

Reset Password: If selected, displays the **Password** box to allow you to change it.

Password: User's password. Periods display instead of the typed characters.

Note: Latitude uses the 512-bit Secure Hash Algorithm (SHA-512) with a randomly generated 512-bit salt that is unique per-user, per-password. Latitude stores the combined hash and salt in the user's account as a 128-character hexadecimal string.

Alias: User's alias name such as a shortened version of the first name or a nickname.

Phone: User's telephone number

Extension: User's telephone extension number.

Email: User's email address (for example, jdoe@mycompany.com).

Time Clock: If selected, the system includes the user's logon and logoff times on the User Logon report.

Active: If selected, the user can log on to the system. If cleared, the user cannot log on to the system.

Role: User's role.

Desk: User's desk.

Branch: User's branch.

Department: User's department.

Dialer Login Credentials: Latitude uses these credentials to log on the user to Dialer automatically.

User Name: User's logon name for Interaction Dialer.

Password: User's password for Interaction Dialer.

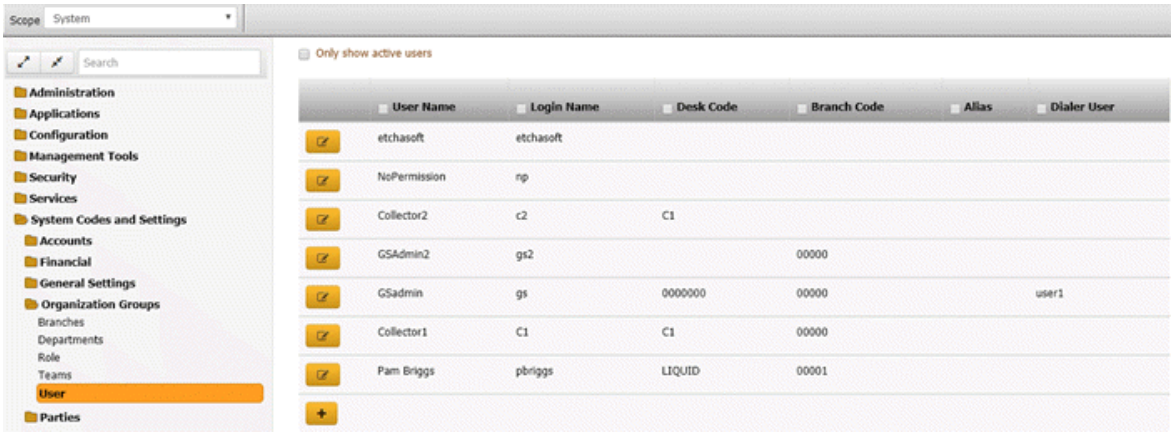
3. Modify the information and then click **Save**.

Activate or Deactivate a User Account

Use the **User** dialog box to activate or deactivate a user account, which determines whether a user can log on to Latitude.

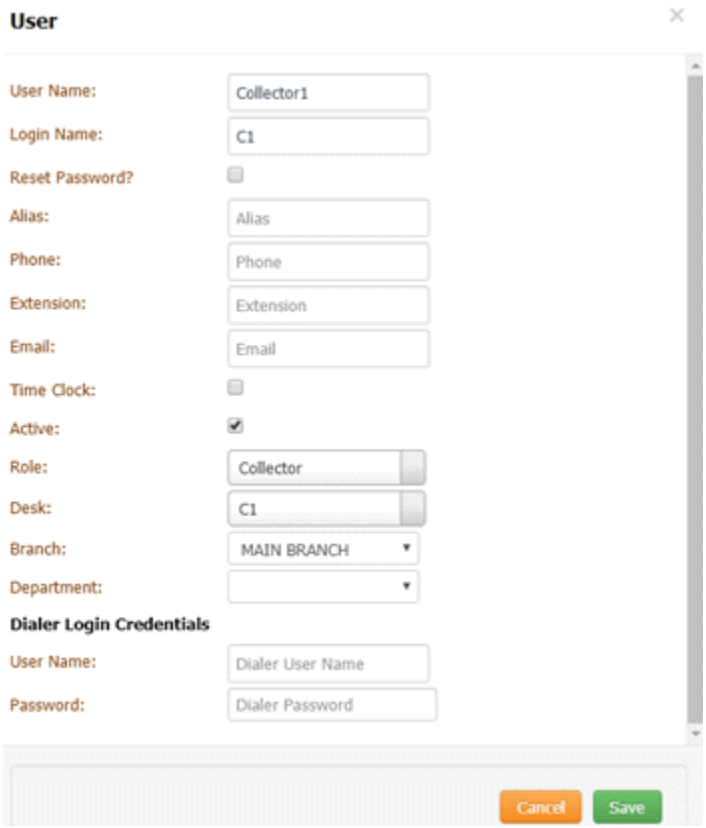
To activate or deactivate a user account

1. In the **Navigation** pane, click **System Codes and Settings** > **Organization Groups** > **User**.



Note: To display active users only in the data grid, click **Only show active users**.

2. Click the Edit icon. The **User** dialog box appears.



3. Do one of the following:
    - To activate the user account, select the **Active** check box.
    - To deactivate the user account, clear the **Active** check box.

Party Codes

Party Codes

You can set up and configure system codes that users can assign to parties associated to an account.

Asset Types

Asset Types

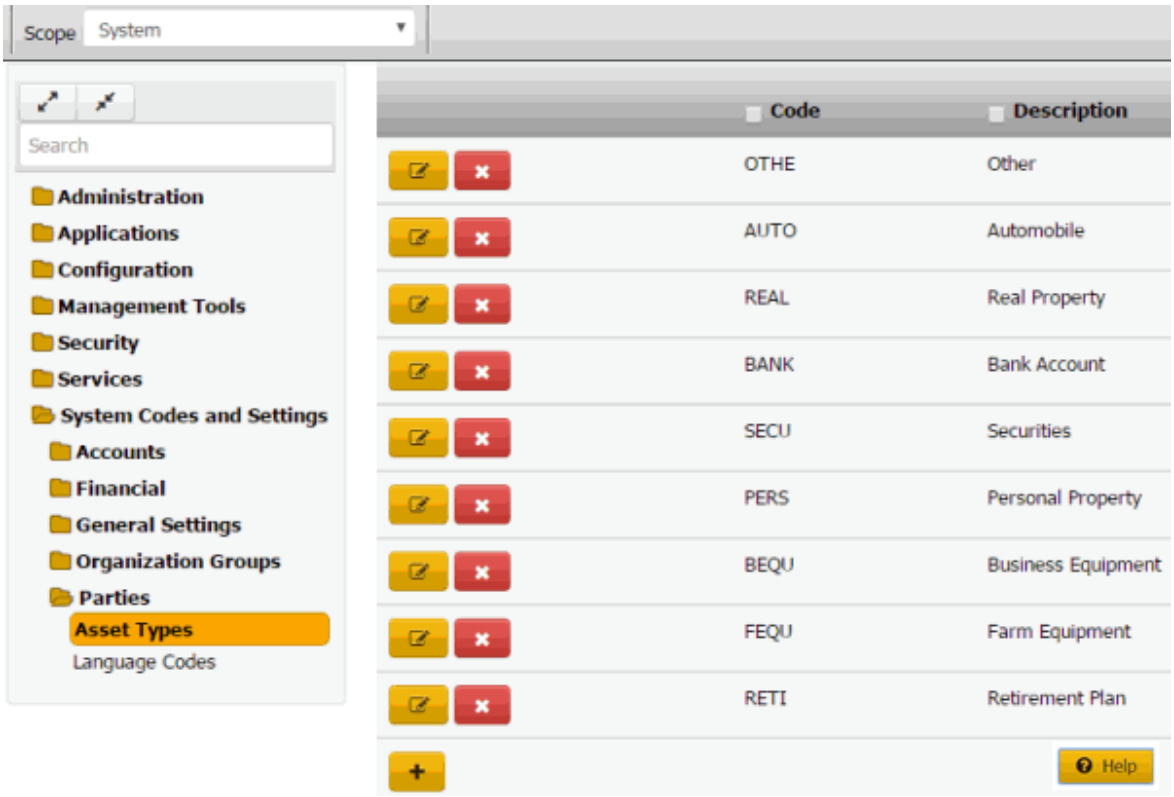
You can search for, add, modify, and delete asset types. Users specify an asset type when maintaining assets for a party on an account. For more information, see Maintain Assets.

Add an Asset Type

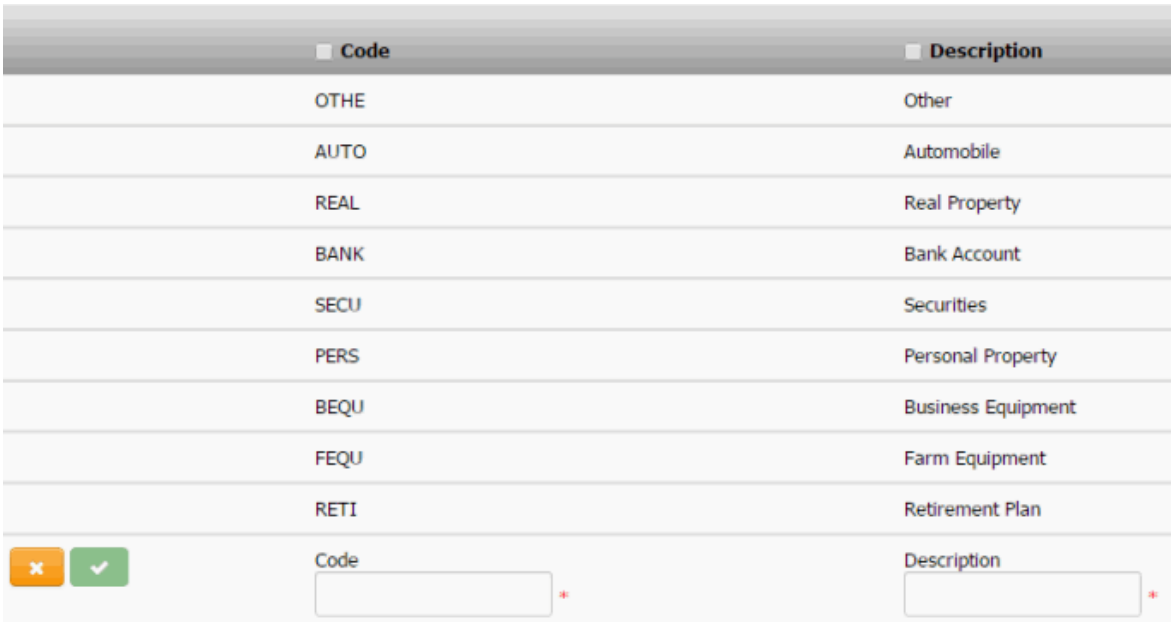
Use the **Asset Types** panel to add an asset type.

To add an asset type

1. In the **Navigation** pane, click **System Codes and Settings** > **Parties** > **Asset Types**.



2. Click the plus sign (+). A blank row appears in the data grid.



Code: Unique code that identifies the asset type.

Description: Description of the asset type.

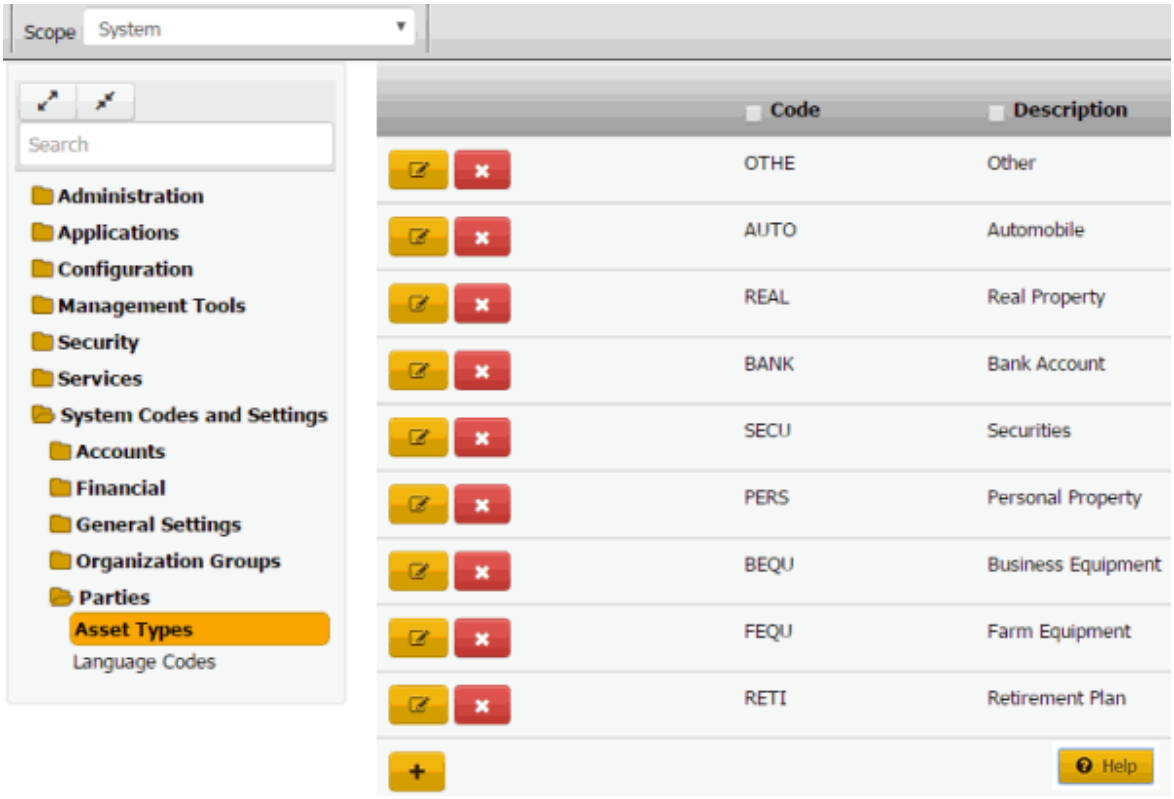
3. Complete the information and then click the check mark.

Modify an Asset Type

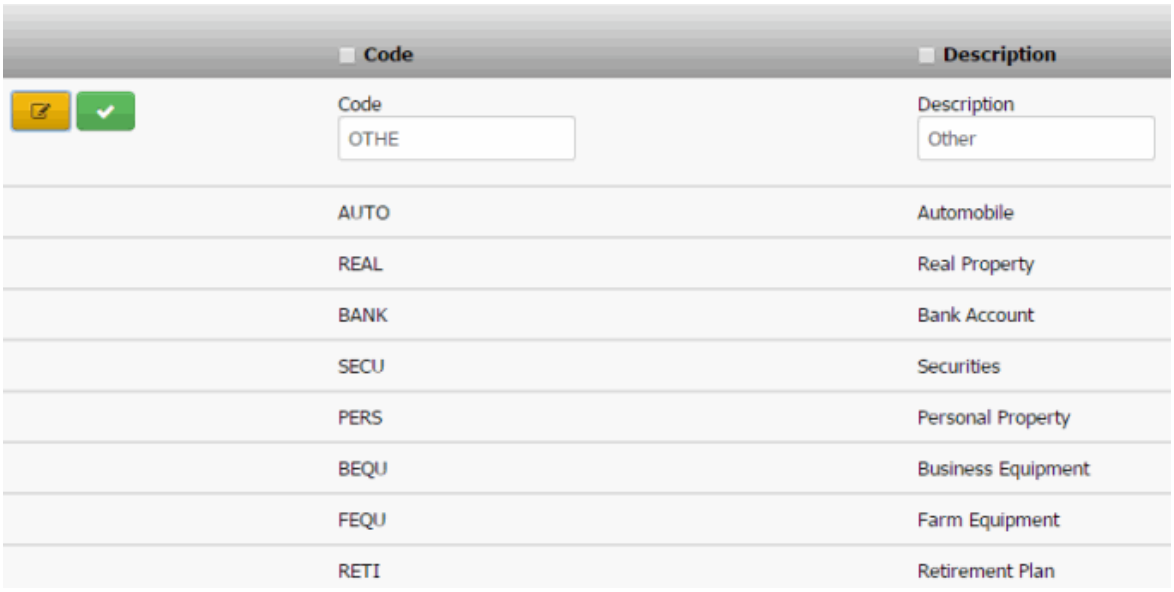
Use the **Asset Types** panel to modify an asset type.

To modify an asset type

1. In the **Navigation** pane, click **System Codes and Settings** > **Parties** > **Asset Types**.



2. Click the Edit icon. The asset type appears in edit mode.



Code: Unique code that identifies the asset type.

Description: Description of the asset type.

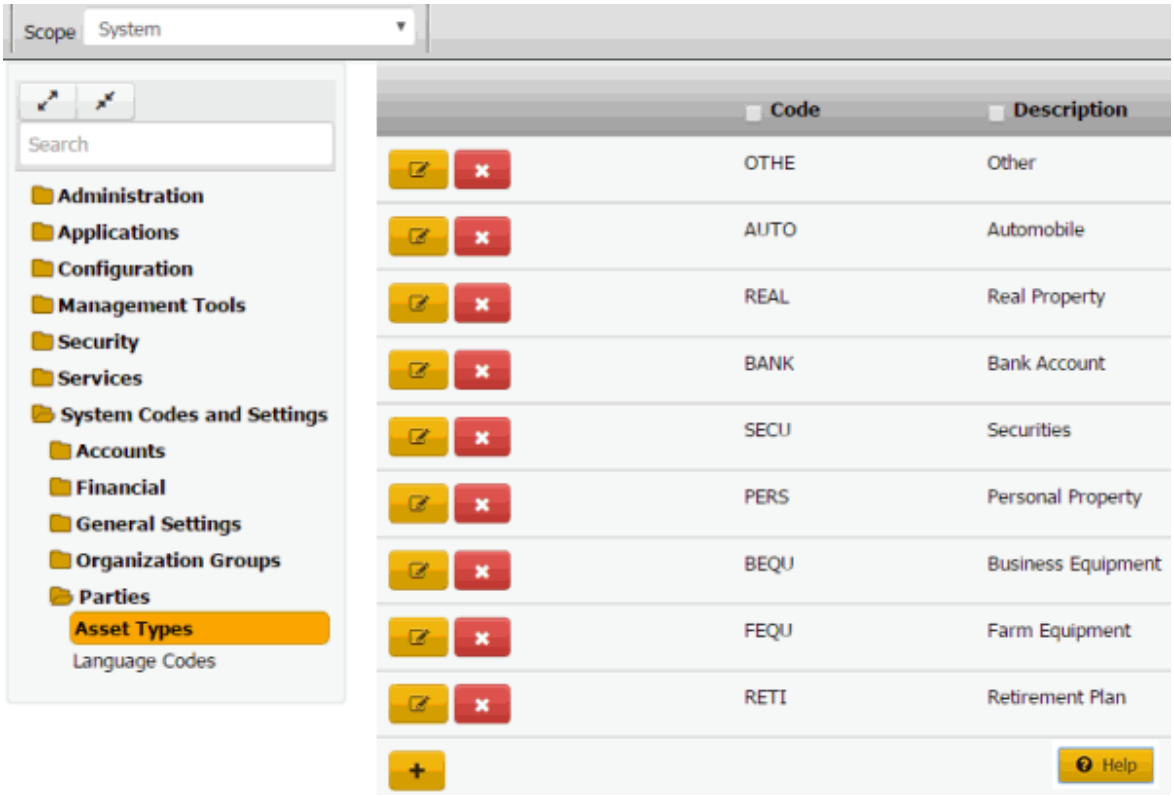
3. Modify the information and then click the check mark.

Delete an Asset Type

Use the **Asset Types** panel to delete an asset type.

To delete an asset type

1. In the **Navigation** pane, click **System Codes and Settings** > **Parties** > **Asset Types**.



2. Click the Delete icon and then click **Yes**.

Language Codes

Language Codes

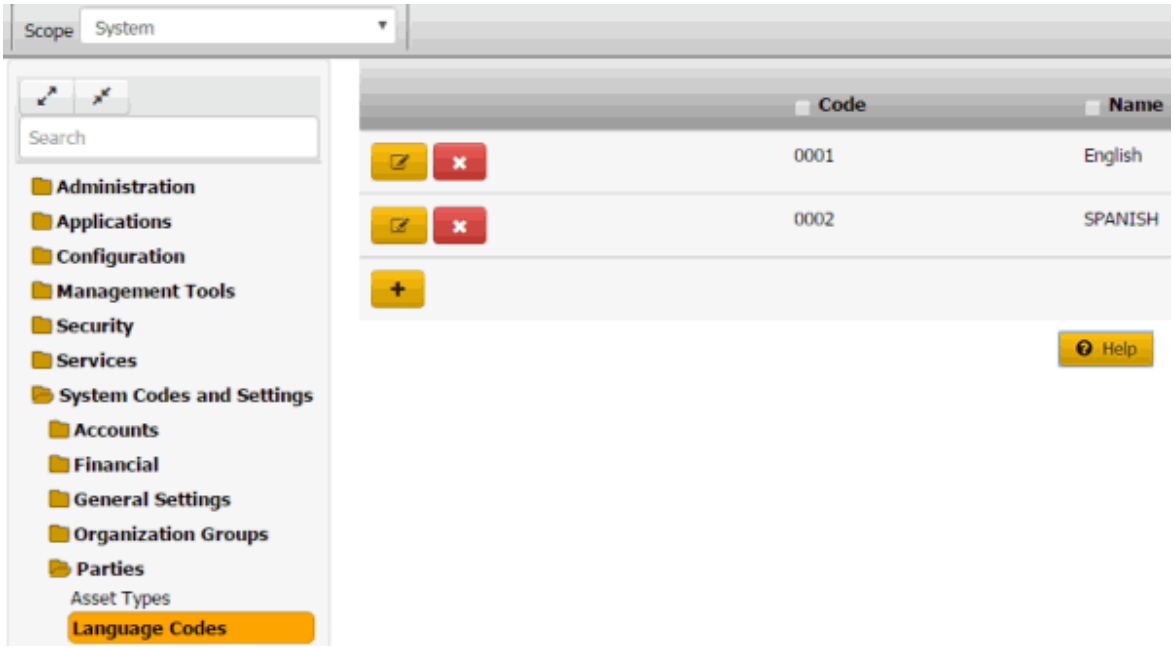
You can search for, add, modify, and delete language codes. Users can assign language codes when maintaining a party on an account. For more information, see Maintain Contact Information.

Add a Language Code

Use the **Language Codes** panel to add a language code.

To add a language code

1. In the **Navigation** pane, click **System Codes and Settings** > **Parties** > **Language Codes**.



2. Click the plus sign (+). A blank row appears in the data grid.

Code: Unique code that identifies the language type.

Name: Name of the language.

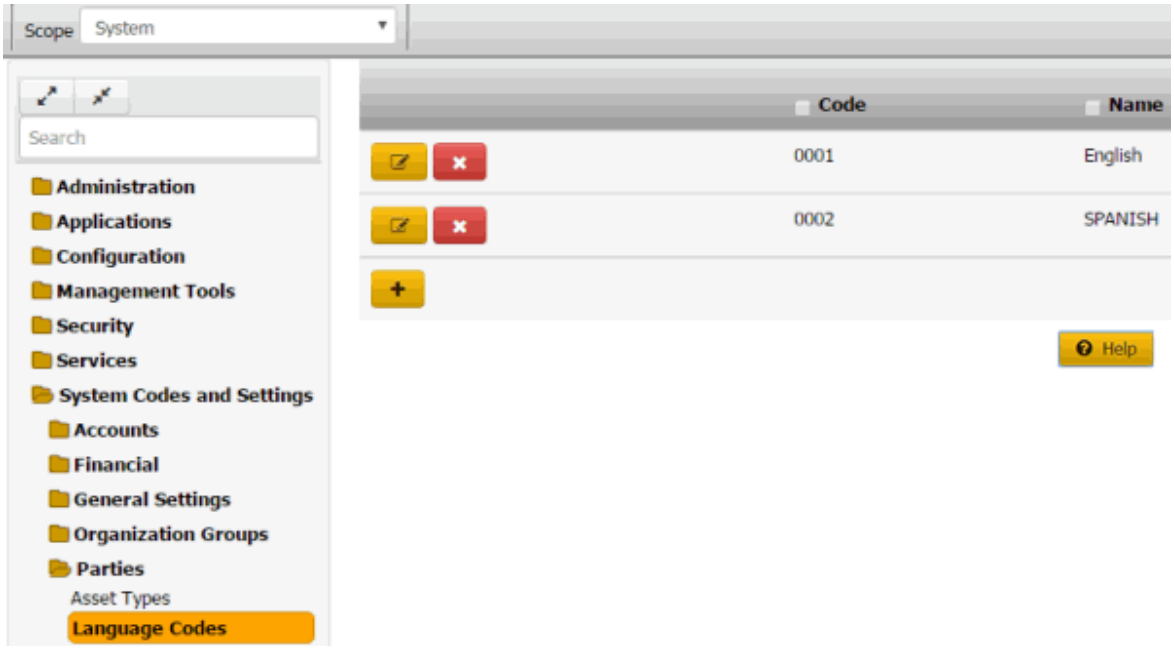
3. Complete the information and then click the check mark.

Modify a Language Code

Use the **Language Codes** panel to modify a language code.

To modify a language code

1. In the **Navigation** pane, click **System Codes and Settings** > **Parties** > **Language Codes**.



2. Click the Edit icon. The language code appears in edit mode.

Code: Unique code that identifies the language type.

Name: Name of the language.

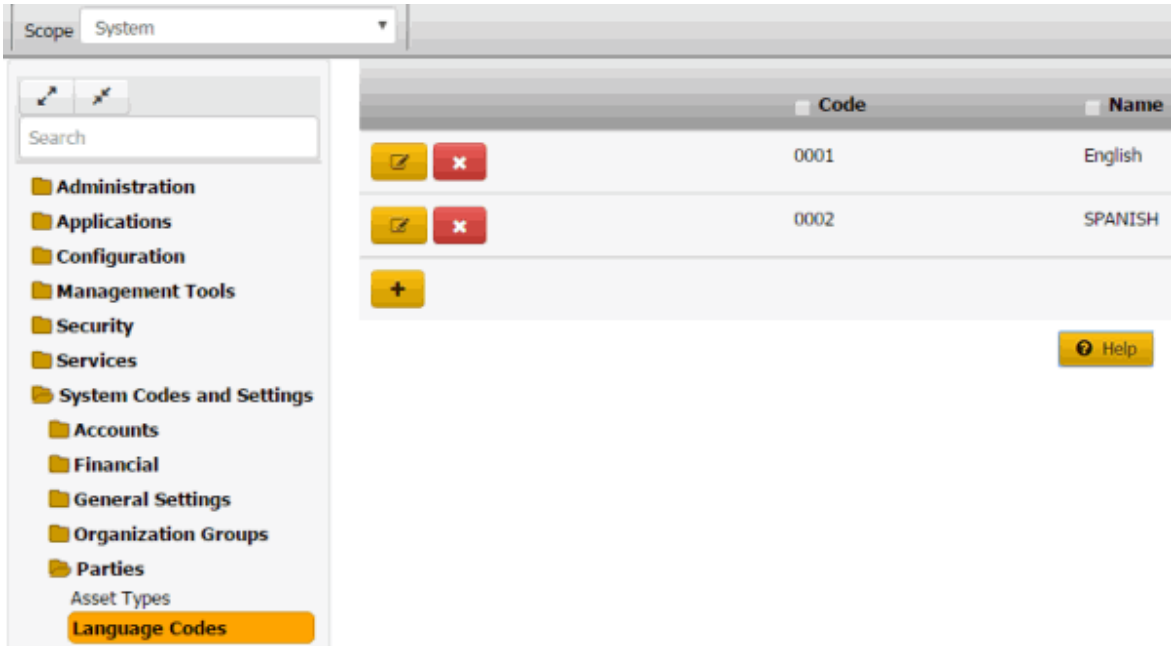
3. Modify the information and then click the check mark.

Delete a Language Code

Use the **Language Codes** panel to delete a language code.

To delete a language code

1. In the **Navigation** pane, click **System Codes and Settings** > **Parties** > **Language Codes**.



2. Click the Delete icon and then click **Yes**.

Data Grids

Data Grids

A data grid displays information in a table format (rows and columns). Each row represents a single record and each column represents a single data item. If a column in a data grid contains no data, either the user or the system didn't provide that data. If the number of records in a data grid exceeds the maximum allowed to display on a single page, a navigation bar appears at the bottom of the data grid.

Some data grids allow you to:

- Sort the data by a single column in ascending or descending order. For more information, see Sort Data in a Data Grid.
- Limit the data that displays based on one or more criteria you specify. For more information, see Filter Data in a Data Grid.

Sort Data in a Data Grid

Some data grids allow you to sort the data by a single column in ascending or descending order.

To sort data in a data grid

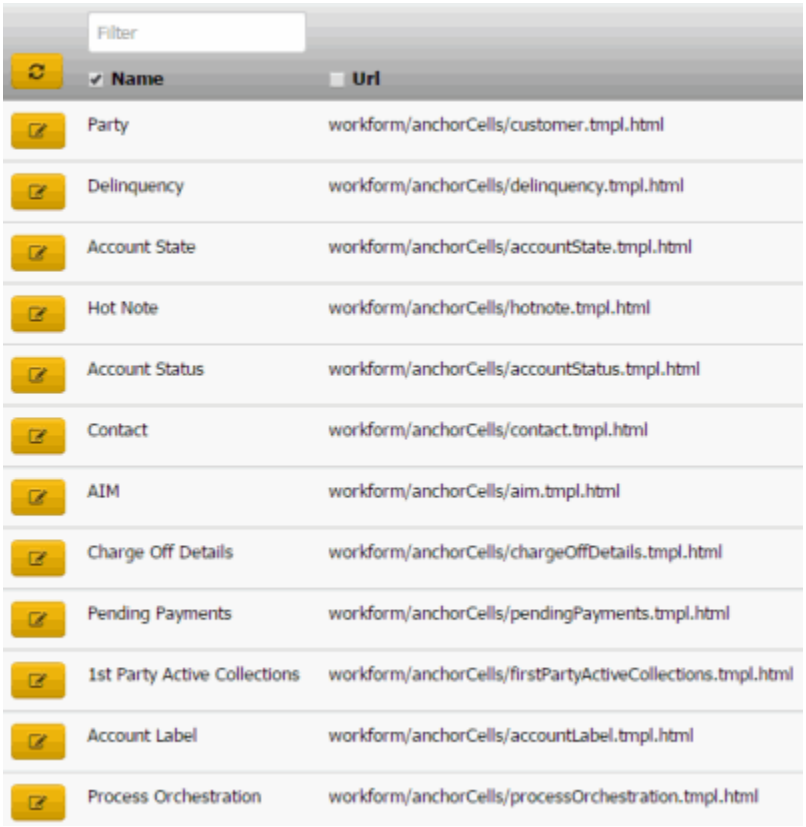
1. Click a column heading to sort the data grid in ascending order by that column. An "up" arrow appears next to the column heading.
2. Click the column heading again to sort the data grid in descending order by that column. A "down" arrow appears next to the column heading.

Filter Data in a Data Grid

Some data grids allow you to limit the data that displays based on one or more criteria. If you set a filter for a column, the filter icon has a white background color. You can set a filter for more than one column at a time.

To filter data in a data grid

1. Select the check box for the column to set limits. A **Filter** box appears.



2. In the **Filter** box, type one or more characters and then click the Refresh icon. The system only displays the rows that match the specified criteria.
3. To set more filters, select a check box and specify the criteria in the corresponding **Filter** box.
4. To remove a filter, clear the check box and then click the Refresh icon.

Move Between Pages of a Data Grid

Sometimes the number of records in a data grid exceeds the maximum allowed to display on a single page. In that case, the system displays a navigation bar at the bottom of the data grid to allow you to move between pages of the data grid.

To move between pages of a data grid

1. Click a page number to display that specific page.
2. Click **Previous** to display the previous page.

3. Click **Next** to display the next page.