



(THE FUTURE OF
FINANCE IS **OPEN**

Fusion NetCapture

Portal User Guide

Version 8.3
May 2018

Copyright

© 2018 Finastra International Limited, or a member of the Finastra group of companies ("Finastra"). All Rights Reserved. Confidential - Limited Distribution to Authorized Persons Only, pursuant to the terms of the license agreement by which you were granted a license from Finastra for the applicable software or services and this documentation. Republication or redistribution, in whole or in part, of the content of this documentation or any other materials made available by Finastra is prohibited without the prior written consent of Finastra. The software and documentation are protected as unpublished work and constitute a trade secret of Finastra International Limited, or a member of the Finastra group of companies, Head Office: One Kingdom Street, Paddington, London W2 6BD, United Kingdom.

Trademarks

Finastra, NetCapture, and their respective sub-brands, and the logos used with some of these marks, are trademarks or registered trademarks of Finastra International Limited, or a member of the Finastra group of companies ("Finastra") in various countries around the world. All other brand and product names are trademarks, registered trademarks, or service marks of their respective owners, companies, or organizations, may be registered, and should be treated appropriately.

Disclaimer

Finastra does not guarantee that any information contained herein is and will remain accurate or that use of the information will ensure correct and faultless operation of the relevant software, services or equipment. This document contains information proprietary to Finastra. Finastra does not undertake mathematical research but only applies mathematical models recognized within the financial industry. Finastra does not guarantee the intrinsic theoretical validity of the calculation models used.

Finastra, its agents, and employees shall not be held liable to or through any user for any loss or damage whatsoever resulting from reliance on the information contained herein or related thereto. The information contained in this document and the general guidance of Finastra staff does not take the place of qualified compliance personnel or legal counsel within your institution. FINASTRA CANNOT RENDER LEGAL, ACCOUNTING OR OTHER PROFESSIONAL SERVICES TO YOUR INSTITUTION. THE INFORMATION CONTAINED HEREIN IS GENERAL IN NATURE AND DOES NOT CONSTITUTE LEGAL ADVICE OR A LEGAL OPINION. CONSULT YOUR LEGAL COUNSEL FOR LEGAL ADVICE SPECIFIC TO YOUR SITUATION OR CIRCUMSTANCES OR TO ANSWER ANY LEGAL QUESTIONS.

This document is not intended as a substitute for formal education in the regulatory requirements of banking, banking operations, lending, lending operations, or other topics generally applicable to financial institutions. Your financial institution is solely responsible for configuring and using the software or services in a way that meets policies, practices, and laws applicable to your institution, including, without limitation: (1) options and selections made on prompts; (2) entries in the software program; (3) program setup; and (4) documents produced by the software or services. It is the obligation of the customer to ensure that responsible decisions are taken when using Finastra products. Information in this document is subject to change without notice and does not represent a commitment on the part of Finastra.

Feedback

Do you have comments about our guides and online help? Please address any comments and questions to your local Finastra representative.

Need more information? Read more about our products at <http://www.finastra.com> or contact your local Finastra office at <http://www.finastra.com/contact>.

Printed to PDF on 5/2/2018.

THIRD-PARTY SOFTWARE ACKNOWLEDGMENTS

Apache software acknowledgement:

This product includes software developed by the Apache Software Foundation ([http:// www.apache.org/](http://www.apache.org/)).

DOM4J binary inclusion acknowledgement:

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain copyright statements and notices. Redistributions must also contain a copy of this document.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name "DOM4J" must not be used to endorse or promote products derived from this Software without prior written permission of MetaStuff, Ltd. For written permission, please contact dom4j-info@metastuff.com.

Products derived from this Software may not be called "DOM4J" nor may "DOM4J" appear in their names without prior written permission of MetaStuff, Ltd. DOM4J is a registered trademark of MetaStuff, Ltd.

Due credit should be given to the DOM4J Project (<http://dom4j.org/>).

THIS SOFTWARE IS PROVIDED BY METASTUFF, LTD. AND CONTRIBUTORS "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL METASTUFF, LTD. OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright 2001 (C) MetaStuff, Ltd. All Rights Reserved.

Oracle JDBC driver binary inclusion disclaimer:

The Oracle Software in the Finastra system is provided by Oracle "As Is" without warranty of any kind. Oracle disclaims all warranties, express and implied, including without limitation, any implied warranties of merchantability, fitness for a particular purpose or non-infringement.

In no event shall Oracle be liable for any indirect, incidental, special, punitive or consequential damages, or damages for loss of profits, revenue, data or data use, incurred by any third party, whether in an action in contract or tort, even if Oracle has been advised of the possibility of such damages. Oracle's entire liability for damages shall in no event exceed one thousand dollars. All warranties for the Finastra software including the use of Oracle software within the Finastra software are contained in their entirety within the License Agreement between Finastra and its customers using the Finastra system.

Hibernate-GNU Library binary inclusion acknowledgement and disclaimer:

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Library General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Library General Public License for more details.

You should have received a copy of the GNU Library General Public License along with this library; if not, write to the Free Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

Finastra hereby disclaims all copyright interest in this Library.

J2SSH-GNU Library binary inclusion acknowledgement and disclaimer:

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Library General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Library General Public License for more details.

You should have received a copy of the GNU Library General Public License along with this library; if not, write to the Free Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

Finastra hereby disclaims all copyright interest in this Library.

OpenOCES OpenSign-GNU Library binary inclusion acknowledgement and disclaimer:

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Library General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Library General Public License for more details.

You should have received a copy of the GNU Library General Public License along with this library; if not, write to the Free Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

Finastra hereby disclaims all copyright interest in this Library.

itext-GNU Library binary inclusion acknowledgement and disclaimer:

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Library General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Library General Public License for more details.

You should have received a copy of the GNU Library General Public License along with this library; if not, write to the Free Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

Finastra hereby disclaims all copyright interest in this Library.

TABLE OF CONTENTS

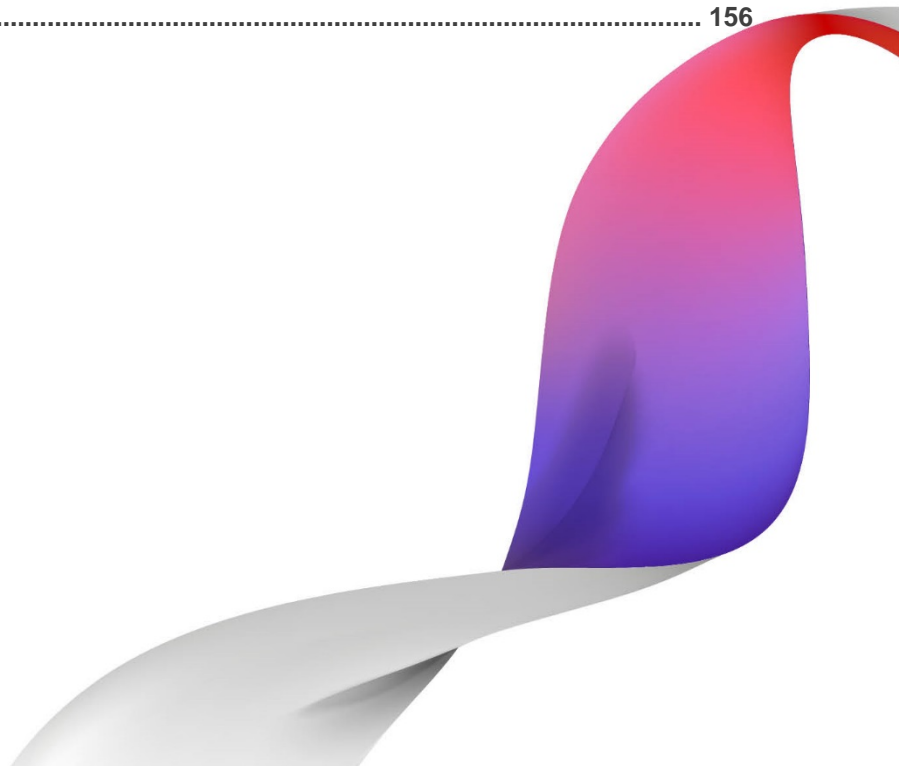
1 INTRODUCTION	1
Getting Started with NetCapture Portal	1
System Requirements	1
Support	2
Logging In	2
Changing Your Password	3
Logging Out	3
2 COMPLETING INITIAL SETUP	4
Understanding the System Manager Window	4
Left Panel	5
Right Panel	6
Icons in System Manager	7
Entering Text in System Manager	7
Understanding the Organizational Hierarchy	7
Understanding User Roles and Privileges	8
Role Inheritance and Assignability	9
Available Roles	10
Choosing Roles for Users	11
Default Roles and Privileges Matrix	11
Privileges and User Interface Access Matrix	16
Usage Examples	33
Suggested Operational Guidelines	35
Initial Setup	36
Requirements	36
Initial Setup Checklist	36
Typical Setup Tasks	39
Adding Customers	39
Typical Maintenance	40
3 USING SYSTEM MANAGER	41
Configuring Applications	41
Requirements	42

Steps	48
Additional Steps for Installing Multiple Application Instances	49
Creating New Organizations	49
Requirements	49
Steps	50
Editing Organization General Information	62
Requirements	62
Steps	62
Editing Organization Operational Parameters	63
Requirements	63
Steps	63
Configuring the Client System Message	63
Requirements	64
Steps	64
Creating Users	65
Requirements	65
Steps	66
Searching for a User	70
Searching for a User on the Users Tab	70
Browsing Through Users for an Organization	71
Editing User Settings	72
Changing a User's Password	72
Changing a User's Deposit Limit	73
Changing a User's Status	73
Assigning a New Security Profile to a User	73
Changing a User's Role Assignments	73
Creating Custom Roles	75
Requirements	75
Steps for Creating a New Role	75
Steps for Modifying an Existing Role	76
Steps for Deleting a Role	76
Configuring Adjustments	77
Edit Adjustments General Configuration	78

Edit Debit and Credit Adjustment Configuration.....	79
Edit Credit Record Configuration	81
Configuring Adjustment Notification Emails.....	82
Requirements	83
Steps	83
Configuring User-Defined Fields.....	84
Requirements	84
Steps to Configure Custom Field Data.....	84
Steps to Configure Payment Data Fields	85
Creating and Managing Templates.....	86
Requirements	86
Steps to Create a New Organization Template.....	87
Steps to Modify an Existing Organization Template	87
Steps to Create a New User-Defined Field Template.....	88
Steps to Modify an Existing User-Defined Field Template.....	90
Managing Scrutiny Rules	91
Scrutiny Rules Hierarchy.....	91
Valid Rule Combinations	92
Requirements	98
Creating New Scrutiny Rules	98
Setting Scrutiny Rule Status.....	99
Configuring Deposit Confirmation Email Contents	100
Configuring Branding	102
Requirements	102
Steps	102
Configuring Report Branding	105
Requirements	106
Steps	106
Configuring Report Parameters	107
Requirements	107
Steps	108
Configuring Security Profiles.....	108
Requirements	109

Steps	109
Assigning a Security Profile to an Organization.....	112
Requirements	113
Steps	113
Configuring Dual Control.....	113
Requirements	113
Steps	114
Creating Account Groups.....	115
Creating Groups	115
Adding Accounts to the Group	116
Adding Users to the Group.....	117
Viewing Group details	118
Adding/Editing Locations	119
Requirements	119
Steps	119
Adding/Editing Contacts.....	120
Requirements	121
Steps	121
Adding/Editing Accounts	123
Requirements	123
Steps	123
Forcing a Client User Logout	126
Managing Licenses	127
Requirements	127
Steps for Adding Licenses.....	127
Steps for Changing License Distribution	128
4 USING DEPOSIT REVIEW	129
Introducing Deposit Review	129
Deposit Review User Privileges	129
Deposit Review Overview	129
Understanding the Deposit Review Window	130
Reviewing Deposits in Deposit Review	130
Reviewing and Modifying Items.....	131

Selecting an Item for Review.....	131
Adding Item or Deposit Comments	140
Setting Item Status	141
Submitting Completed Deposits	142
Referring a Deposit	143
Rejecting a Deposit	143
Suspending a Deposit	143
Examples of Adjustment and Rejections Notices.....	144
Managing Queues in Deposit Review.....	144
Changing the Priority of Unassigned Queued Deposits.....	146
Assigning Deposits to Specific Reviewers	146
Removing an Assignment from a Deposit.....	147
5 TROUBLESHOOTING.....	148
Login Issues	148
General Issues	150
Troubleshooting System Manager	150
User Interface Issues	151
Privileges Issues	151
Data Validation Issues.....	152
Troubleshooting Deposit Review	154
Deposit Issues	154
Item Editing Issues	154
FINASTRA SUPPORT	156



1 Introduction

NetCapture Portal provides single sign-on access to the NetCapture Business system web-based applications. NetCapture Portal includes the following applications:

- System Manager is used to administer the NetCapture Business environment; providing service organizations with the tools to create customer-specific processing and business rules, risk and security parameters, user profiles, and access control.
- Deposit Review provides a wide range of utilities for monitoring, adjusting, and managing incoming deposits. For a supervisor, Deposit Review serves as a workflow management tool to support multiple review agents. Deposits that fail business rules are pushed to review agents for review and adjustment, as necessary.
- Reporting provides authorized users access to reports about deposits and items, deposit status, and desktop client (NetCapture Business Pro) and web client (NetCapture Business) seat licenses.

This guide includes information about the NetCapture Portal, including the following:

For information about reporting, see the *Reporting and Deposit Management User Guide*.

Getting Started with NetCapture Portal

This section includes information about the following:

- System Requirements
- Support
- Logging In
- Changing Your Password
- Logging Out

System Requirements

Following are the minimum system requirements to run NetCapture Portal:

Minimum System Requirements	
Operating System	One of the following: <ul style="list-style-type: none">• Microsoft Windows Vista Business• Microsoft Windows 7 Professional or Ultimate• Microsoft Windows 8 Pro or Enterprise (desktop mode only)
Internet Browser	<ul style="list-style-type: none">• Microsoft Internet Explorer version 7.x or higher• Internet Explorer 10 supported in compatibility mode only• Ensure Internet Explorer security is not set to High. (If security is set to High, JavaScript is automatically disabled. Either manually enable Javascript, or set security to Medium or Low.)• If you have pop-up blocking software installed, ensure you configure it to allow pop-ups from the web site that hosts NetCapture Portal. Deposit Review and System Manager both make use of pop-up windows.

Minimum System Requirements	
Authentication	If your organization is using user certificate-based client authentication, procure a digital certificate issued by a commercial Certificate Authority and install it in Internet Explorer.
Network Connectivity	Network connectivity to the web server, via Internet or Intranet.

Support

You can get support through the NetCapture Portal online help or from your Service Representative.

Online Help

Click the Help link to get online help from any window. The Help link appears just below the tabs in NetCapture Portal.

Technical Support

Contact your local system administrator or Service Representative for additional help with NetCapture Portal.

Logging In

Depending on how your service organization has configured the access days and times for NetCapture Portal, it may or may not be available to you when you attempt to log in. Contact your Service Representative for information about the times when the application is available to you.

Before you log in to the system for the first time, make sure you have received the following information from your Service Representative:

- URL for accessing NetCapture Portal
- Valid user name and password

To log in:

1. Launch a browser and go to the URL provided by your Service Representative for accessing NetCapture Portal. Be sure to enter the correct URL.

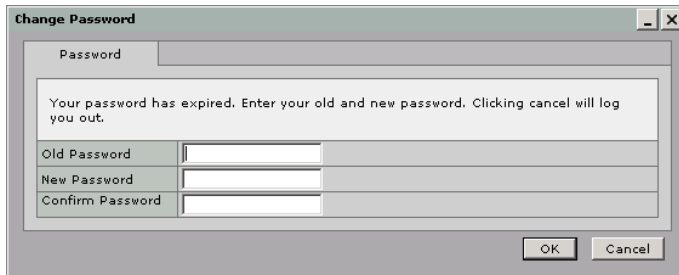
The Login window appears.

2. In the User Name field, enter your user name exactly as it was provided to you by your Service Representative.
3. In the Password field, enter your password exactly as it was provided to you by your Service Representative. Passwords are case sensitive.
4. Click Submit.
5. If your NetCapture Portal is configured to use digital certificates (external authentication) and multiple digital certificates are available on your workstation, the Choose a digital certificate box appears. Choose the certificate you will use for this session and click OK.

You are now logged into the system. If this is your first login, or if your password has expired, you are prompted to change your password.

Changing Your Password

If this is the first time you have logged in or if your password has expired, after logging into the system the Change Password window appears. You must change your password when you see this window to be able to log into the application in the future.

A screenshot of a 'Change Password' dialog box. The window has a title bar with 'Change Password' and standard window controls. Inside, there's a 'Password' label above a text input field. Below that, a message states: 'Your password has expired. Enter your old and new password. Clicking cancel will log you out.' Under the message are three input fields labeled 'Old Password', 'New Password', and 'Confirm Password'. At the bottom right are 'OK' and 'Cancel' buttons.

In addition, you can change your password at any time by clicking the Change Password link on the Main tab of NetCapture Portal.

Do the following to change your password:

1. In the Old Password field, enter your current password.
2. In the New Password and Confirm Password fields, enter a new password. You will use this password every time you log into the system.

Your password must comply with certain restrictions as defined by your service organization. Contact your Service Representative for details.
3. Click OK.

Your password has now been changed. Use your new password the next time you log in to NetCapture Portal.

Logging Out

You should always exit NetCapture Portal by clicking the Logout tab. If you are reviewing a deposit in Deposit Review and do not complete the deposit before logging out, it will be saved in its current state.

2 Completing Initial Setup

System Manager is the central configuration point for the NetCapture Business system. Use System Manager to manage user preferences, organizations, applications, and define rules for receiving and processing deposits.

This section includes the following information:

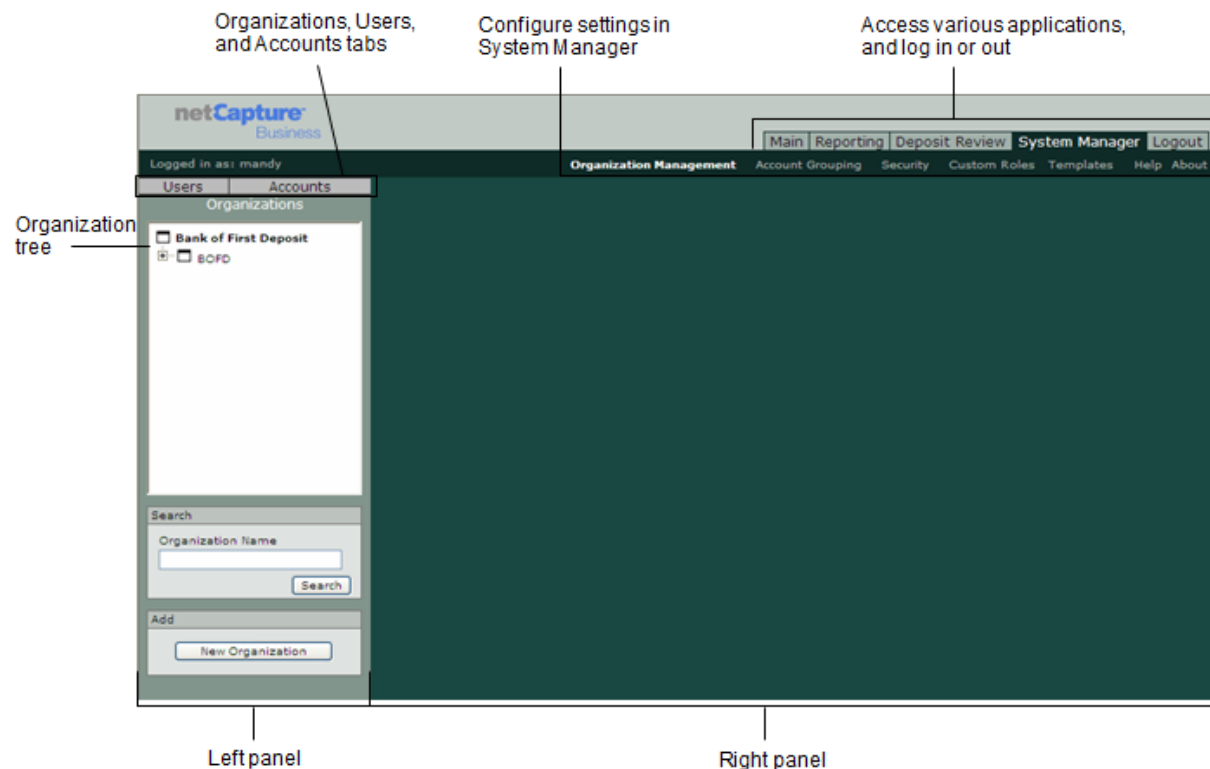
- Understanding the System Manager Window
- Understanding User Roles and Privileges
- Suggested Operational Guidelines
- Initial Setup
- Typical Setup Tasks

Understanding the System Manager Window

To access System Manager, log in to NetCapture Portal and click the System Manager tab. In System Manager you will have access to the screens and dialog boxes you are authorized to use. Functions you are not authorized to use may not be visible or may be grayed out.

Note: For more information about system access, see *Understanding User Roles and Privileges*.

Following is a view you may typically expect to see when you first access System Manager. By default, most users will see the Organization Management area inside System Manager. If you do not have rights to configure organization settings, your view will default to one of the other areas of System Manager, depending on your privileges.

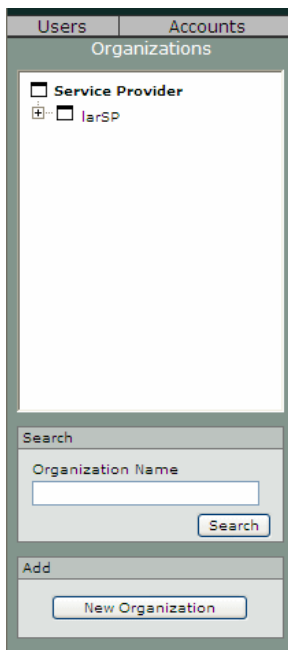


There are two main areas in the System Manager window, the left panel and the right panel.

Left Panel

The left side of the window has three tabs—Organizations, Users, and Accounts.

Organizations Tab

The screenshot shows the 'Organizations' tab selected in a window with 'Users' and 'Accounts' tabs. The main area displays a tree view under 'Service Provider' with a sub-item 'IarSP'. Below the tree is a 'Search' section with a text field for 'Organization Name' and a 'Search' button. At the bottom is an 'Add' section with a 'New Organization' button.

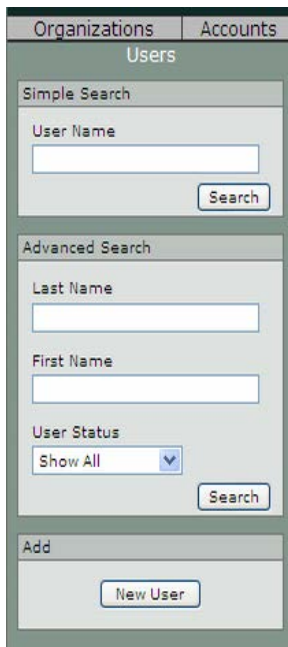
The Organizations tab lets you search for and select an organization. It contains a list of organizations existing in your system. The way organizations are displayed illustrates the hierarchical structure configured in the system. For more information, see *Understanding the Organizational Hierarchy*.

Click the [+] next to an organization to display that organization's child organizations. Click on an organization to select it.

Alternately, you can search for an organization by name. You can use partial names or single letters to search for an organization by name in the Name field. You do not need to use * in the search criteria. The search results include all organizations with names containing the characters you used for the search criteria.

If you are logged in as a user with Create Organization permissions, you can also add a new organization by clicking the New Organization button. See *Creating New Organizations* for details about creating new organizations.

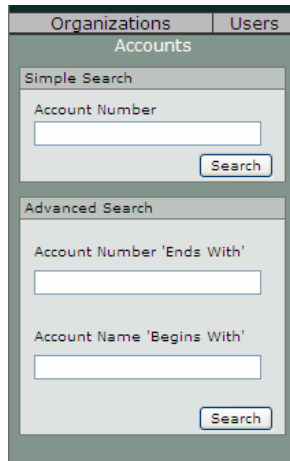
Users Tab

The screenshot shows the 'Users' tab selected in a window with 'Organizations' and 'Accounts' tabs. The main area has a 'Simple Search' section with a 'User Name' text field and a 'Search' button. Below that is an 'Advanced Search' section with 'Last Name' and 'First Name' text fields, a 'User Status' dropdown menu set to 'Show All', and a 'Search' button. At the bottom is an 'Add' section with a 'New User' button.

The Users tab lets you search for and select a user. You can perform a simple search by user name, or an advanced search by first or last name, or status. When you use a text field to search for a user's name, you can use partial names or single letters. You do not need to use * in the search criteria. The search results include all users with names containing the characters you used for the search criteria.

If you are logged in as a user with Create User permissions, you can also add a new user by clicking the New User button. See *Creating Users* for details about creating new users.

Accounts Tab



The Accounts tab lets you search for and select an account. You can perform a simple search by providing a complete account number, or you can perform an advanced search by providing one or both of the following:

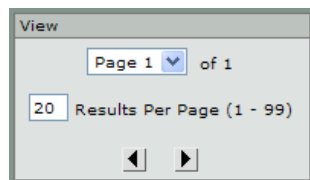
- Account Number 'Ends With': Specify the last number(s) of an account number to return a list of all accounts ending with those numbers.
- Account Name 'Begins With': Specify the first letter(s) of an account name to return a list of accounts with names that begin with those letters.

You must enter data to perform a search—if you do not specify any search criteria, the search will return no results. If you are logged in as a user with permissions to edit accounts, you can select an account from the list of results to edit.

Note: Accounts associated with inactive organizations will NOT be included in search results. However, inactive accounts associated with active organizations will be included.

Navigation

When you complete a search for an organization, user, or account, a navigation aid appears at the bottom of the tab. You can navigate the results using the Page drop-down box or the arrow buttons, and you can determine how many results appear on a page by editing the Results Per Page field.



Right Panel

The right side of the window contains either search results for searches performed using the Organizations, Users, and Accounts tabs, or links to various system configuration options. The following links and tabs may or may not appear depending on your privileges:

- The Organization Management link lets you configure and manage the organizations, accounts, and users in the system. Once you select an organization, you may see the following tabs:
 - The General tab contains basic information about the organization such as its name, type, and related organizations.
 - The Branding tab contains information about any custom branding set up for the selected organization's Web Client applications.
 - The Operational Parameters tab contains information about the way the Web Client applications for the selected organization operate. It also includes information about customer notification emails settings.
 - The User-Defined Fields tab lets you define additional fields that appear in Desktop Client and Web Client applications so that depositors can enter extra information that is useful to their organization. The Web Client only uses the first 12 custom fields, and does not use payment data fields.
 - The Locations & Contacts tab contains information about the organization's office locations and personnel contacts.
 - The Accounts tab contains information about the accounts set up for this organization for processing deposits in the system. This tab appears only for Customer type organizations.

- The Rules tab contains information about the rules that determine how items are routed for processing in the system.
- The Users tab contains information about the users belonging to the selected organization.
- The Security tab lets you specify which security profile is associated with the selected organization.
- The Applications tab contains information about NetCapture Portal applications.
- The License Mgmt tab contains information about the licenses your organization has purchased and is using at Web Client sites.
- The Adjustment Processing tab contains information about settings for debit adjustments, credit adjustments, and credit records generated by the system.
- The Custom Roles link lets you create and manage custom roles for managing user privileges in the system.
- The Account Grouping link lets you set up account groups that allow you to group together organizations and accounts for reporting purposes. Setting up groups makes it simple to generate cumulative report data for the group.
- The Security link contains information about security parameters for system users and applications.
- The Templates link lets you create and manage templates that you can use to create new organizations or user-defined field groups:
 - The Org Templates tab lets you create and manage templates that contain pre-defined settings for organizations. You can apply templates when creating new organizations in the system to save time and enforce consistency.
 - The Defined Field Group and Defined Field Templates tabs let you create and manage templates that contain pre-defined custom and payment data fields. You can apply user-defined field templates to new organizations to save time and enforce consistency.

Icons in System Manager

The following icons are used throughout System Manager:



Add: Click to add a new object, such as a user or organization



Edit: Click to edit an existing object



Delete: Click to delete an object

Entering Text in System Manager

As a general rule, text fields in System Manager accept only basic ASCII characters, or those characters found on your keyboard. The exception to this is the Branding window, which supports the copyright (©) and trademark (™) symbols. Some fields have additional restrictions; for example, they may accept only numeric characters. Any such restrictions are specified in the instructions for editing those fields.

Understanding the Organizational Hierarchy

The following types of organizations can be defined in the system:

- Service Provider
- Bank of First Deposit
- Correspondent Bank
- Customer

The system allows for flexible configuration of the hierarchy to match your organizational structure. The following rules dictate how you can set up the organization hierarchy:

- The top-level organization in the system may be either the Bank of First Deposit or a Service Provider.
- There must be one Bank of First Deposit.
- If the top-level organization is a Service Provider, then the Bank of First Deposit resides below it in hierarchy.
- Under the Bank of First Deposit there may be optional Correspondent Banks.
- Customer Organizations can exist under the Bank of First Deposit or Correspondent Banks. They CANNOT exist below other Customer organizations in the hierarchy.
- Organizations running Desktop Client or Web Client applications must be specified as Customer type organizations.

The system relies on the concept of parent and child organizations.

- A parent organization is one that has other organizations residing below it in hierarchy.
- A child organization is one that has other organizations residing above it in hierarchy.

For example, the following illustrates a potential hierarchy of organizations where at least one of each type of organization is represented.

> (Level 1) Service Provider

>> (Level 2) Bank of First Deposit

>>>> (Level 4) Customer 1

>>> (Level 3) Correspondent Bank

>>>> (Level 4) Customer 2

In this hierarchy, the Bank of First Deposit is a child of the Service Provider. Customer 1 is a child of the Bank of First Deposit. The Correspondent Bank is a child of the Bank of First Deposit and a parent to customer 2.

Another possible hierarchy might look like this:

> (Level 1)

>> (Level 2) Customer 1

>> (Level 2) Customer 2

>> (Level 2) Customer 3

In this hierarchy, there is no Service Provider or Correspondent Bank, just Customers of the Bank of First Deposit. Each Customer is a child of the Bank of First Deposit, which is the parent.

Understanding User Roles and Privileges

In order to understand how access is granted to users in the system, you need to understand two key concepts:

- Privileges: Privileges dictate a specific level of access to an application.
- Roles: Roles are groups of privileges that are assigned to users.

The role assigned to a user determines the user's level of access to the system and the types of activities the user is allowed to perform.

Roles are assigned to users for a particular organization. For example:

- A user is associated with both Customer A and Customer B.
- The user is assigned the Remote User role and the Reporting Viewer role for Customer A, but only the Remote User role for Customer B.
- The user can submit deposits for both Customer A and Customer B.
- The user can access reporting information for Customer A's accounts but NOT for Customer B's accounts.

Roles cannot be assigned to users independently of organizations. In other words, you cannot assign a role to a user without also specifying which organization the role is associated with. However, if you specify that the role is inheritable when assigning it to a user for an organization, the user will inherit that role for all of that organization's child organizations. For more information, see the next section, *Role Inheritance and Assignability*.

To understand roles and privileges in System Manager and how they determine system access, see the following sections:

- Role Inheritance and Assignability
- Available Roles
- Choosing Roles for Users
- Default Roles and Privileges Matrix
- Privileges and User Interface Access Matrix
- Usage Examples

Role Inheritance and Assignability

When you assign roles to users, you can flag them to be executable, inheritable, or assignable.

Executable

Executable means that when a role is assigned to a user and flagged as Execute, the role can be executed by the user.

Inheritable

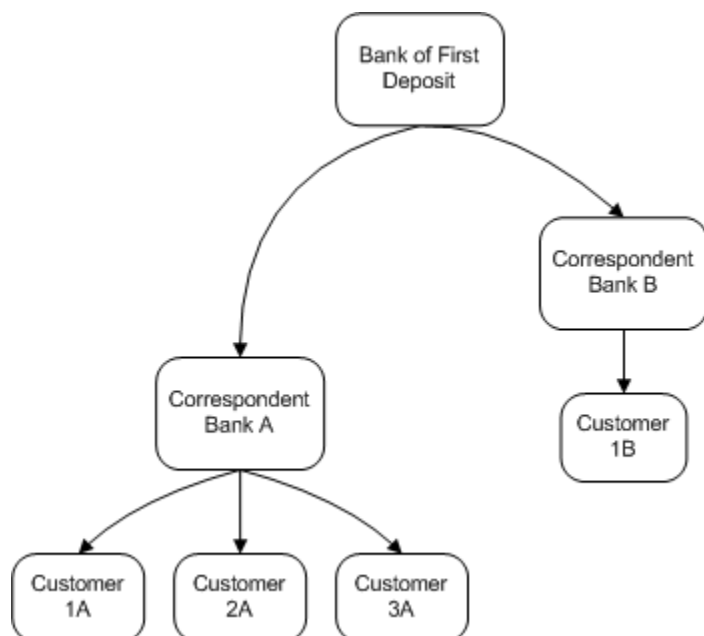
Inheritable means that when a role is assigned to a user at a parent organization level and flagged as Inherit, the role will be inherited by the user for any of that organization's child organizations.

Assignable

Assignable means that when a role is assigned to a user and flagged as Assign, the user has rights to assign that role to other users. Users can assign the role to any users associated with organizations for which they have that role (for example, if you have the role Remote User for Customer 1 marked as assignable but you do NOT have Remote User for Customer 2, you can assign that role to other users only for Customer 1).

Examples of Assignable and Inheritable Usage

Let's use the following diagram as an example.



If a user is assigned a role for the Correspondent Bank B organization and that role is flagged as inheritable, that user will have the same role for Customer 1B, but will not have the role for Correspondent Bank A or Customers 1A, 2A, or 3A.

If the user has a role assigned for the Bank of First Deposit organization that is flagged as inheritable, then the user has the role for all organizations.

If a user is assigned the Bank Operations role for Correspondent Bank A and it is flagged as assignable but NOT inheritable, then that user can assign that role to users only for Correspondent Bank A, and NOT for any of the associated customer organizations.

If a user is assigned the Bank Operations role for Correspondent Bank A and it is flagged as both assignable and inheritable, then that user can assign that role to users for Correspondent Bank A, Customer 1A, Customer 2A, or Customer 3A. That user CANNOT assign that role to users for Correspondent Bank B or Customer 1B.

For more examples, see *Usage Examples*.

Warning about Inheritable and Assignable Flags

You should be aware of the effects of setting the assignable or inheritable flag for a role assignment. When you mark a role assignment as inheritable for a high-level organization, the user will receive the same role assignment for ALL organizations below that organization in the hierarchy. For example, if you assign a user the Banking Operations role for the Bank of First Deposit and mark it as inheritable, that user will have the Banking Operations role for the Bank of First Deposit and ALL organizations beneath it in the hierarchy, including all Correspondent Bank and Customer organizations. If you are not careful when assigning roles to users, you could grant levels of access that should not be given to them. Be careful when setting the inheritable flag to avoid inadvertently giving user's access to accounts and deposits to which they should not have access, and be careful when setting the assignable flag to avoid inadvertently giving users the rights to re-assign roles to other users that they should not be able to re-assign.

Available Roles

Following is a list of the default roles available in the system:

- NCB Super System Administrator
- System Administrator
- Banking Operations
- Help Desk Technician
- Customer Service
- Security Administrator
- Template Administrator
- Role Administrator
- Deposit Review Agent
- Customer Administrator
- Bank of First Deposit Administrator
- Correspondent Bank Administrator
- Remote User
- Remote Reviewer
- Reporting Viewer
- Account Groups Administrator

Note that roles can be deleted and added, so it is possible that the list of roles available in your system is different.

You can also create custom roles that contain whatever groupings of privileges your organization needs. See *Privileges and User Interface Access Matrix* for a complete list of the privileges available in the system, and see *Creating Custom Roles* for information about how to create custom roles.

Choosing Roles for Users

You should decide how to assign a role to a user by determining what types of activities you want the user to be able to perform, and which portion of the user interface will allow the user to perform those activities.

Use the *Default Roles and Privileges Matrix* and the *Privileges and User Interface Access Matrix* to determine which roles you want to assign to users. Consider the privileges you do NOT want the user to have in addition to the privileges that you DO want the user to have when making your decision. You can also create custom roles that contain the privileges you want a particular user to have.

In order to complete most activities in the system, a role must have the execute type privilege in addition to either the create, update, or delete type privilege. The execute privilege is what allows the user to access the specified area of the user interface. The create, update, and delete privileges, as a general rule, are what allow the user to complete actions in System Manager. For more information about which privileges provide access to which portions of the user interface, see *Privileges and User Interface Access Matrix*.

IMPORTANT! When the system is installed, there is a default user with the NCB Super System Administrator role assigned to the top-level organization. This role has all available privileges in the system. You can get the initial user's user name and password from your Service Representative. Once new users have been configured and all system privileges have been parceled out to other users, it is highly recommended that you either disable the initial super user's account (by setting it to inactive or deleted), or limit the super user's system access by removing privileges from the NCB Super System Administrator role according to your organization's security policies.

Default Roles and Privileges Matrix

The following table depicts the privileges that each default role defined in the system has. You can create new roles and assign any combination of these privileges to the new roles. You can also change the privileges that are associated with the default roles.

The Role Administrator and Template Administrator roles are new in the 5.2 release. If you are upgrading from version 5.1, these roles will automatically be assigned to any existing users that are assigned the System Administrator role. These users can then assign the new roles/privileges to other users as appropriate. For more information about how roles are assigned to existing users after upgrading the system, see the *NetCapture Platform System Manual*.

For information about the conditions that must be met before a user can assign roles to other users, see *Changing a User's Role Assignments*.

In addition to these roles, you can set up custom roles. See *Creating Custom Roles* for more information.

#	Privilege	NCB Super System Administrator	System Administrator	Banking Operations	Help Desk Technician	Customer Service	Security Administrator	Template Administrator	Role Administrator	Deposit Review Agent	Customer Administrator	Bank of First Deposit Admin	Correspondent Bank Admin	Remote User	Remote Reviewer	Reporting Viewer	Account Group Admin
1	Execute System Manager	X	X	X	X	X	X			X	X	X	X				
2	Create Top Orgs	X										X					
3	Update Top Orgs	X										X					
4	Create Bank	X											X				
5	Update Bank	X									X						
6	Create Customer	X									X						
7	Update Customer	X									X						
8	Execute Account	X	X	X	X	X	X			X							
9	Create Account	X	X	X													
10	Update Account	X	X	X													
11	Execute Contact	X	X	X	X	X	X			X							
12	Create Contact	X	X	X		X											
13	Update Contact	X	X	X		X											
14	Delete Contact	X	X	X		X											

#	Privilege	NCB Super System Administrator	System Administrator	Banking Operations	Help Desk Technician	Customer Service	Security Administrator	Template Administrator	Role Administrator	Deposit Review Agent	Customer Administrator	Bank of First Deposit Admin	Correspondent Bank Admin	Remote User	Remote Reviewer	Reporting Viewer	Account Group Admin
15	Execute User	X	X	X	X	X	X										
16	Create User	X	X	X	X	X											
17	Update User	X	X	X	X	X											
18	Execute Roles	X							X								
19	Create Roles	X							X								
20	Update Roles	X							X								
21	Delete Roles	X							X								
22	Execute Rules	X		X						X							
23	Create Rules	X		X													
24	Update Rules	X		X													
25	Execute Security Profile	X	X				X										
26	Create Security Profile	X					X										
27	Update Security Profile	X					X										
28	Delete Security Profile	X					X										
29	Execute Templates	X						X									
30	Create Templates	X						X									
31	Update Templates	X						X									
32	Delete Templates	X						X									

#	Privilege	NCB Super System Administrator	System Administrator	Banking Operations	Help Desk Technician	Customer Service	Security Administrator	Template Administrator	Role Administrator	Deposit Review Agent	Customer Administrator	Bank of First Deposit Admin	Correspondent Bank Admin	Remote User	Remote Reviewer	Reporting Viewer	Account Group Admin
33	Execute App Parameter	X	X		X												
34	Create App Parameter	X	X														
35	Update App Parameter	X	X														
36	Create Parent Org Brand	X	X														
37	Update Parent Org Brand	X	X														
38	Delete Parent Org Brand	X	X														
39	Create Child Org Brand	X		X													
40	Update Child Org Brand	X		X													
41	Delete Child Org Brand	X		X													
42	Update Licenses	X										X	X				
43	Execute Reports	X														X	
44	Execute Account Groups	X															X
45	Create Account Groups	X															X
46	Delete Account Groups	X															X
47	Update Account Groups	X															X

#	Privilege	NCB Super System Administrator	System Administrator	Banking Operations	Help Desk Technician	Customer Service	Security Administrator	Template Administrator	Role Administrator	Deposit Review Agent	Customer Administrator	Bank of First Deposit Admin	Correspondent Bank Admin	Remote User	Remote Reviewer	Reporting Viewer	Account Group Admin
48	Adjustment Processing	X									X	X	X				
49	Create Deposit	X												X			
50	Review Remote Deposit	X													X		
51	Execute Deposit Review	X		X						X							
52	Update Deposit Review	X		X						X							
53	Update Deposit Queue	X		X													
54	Manage Web Client Settings	X	X														
55	Manage Web Client Deposits	X		X													
56	Execute Support Util	X	X														
57	Create Provisioned User *																
58	Update Provisioned User *																
59	Create Consumer Deposit																
60	Create Desktop Deposit																

#	Privilege	NCB Super System Administrator	System Administrator	Banking Operations	Help Desk Technician	Customer Service	Security Administrator	Template Administrator	Role Administrator	Deposit Review Agent	Customer Administrator	Bank of First Deposit Admin	Correspondent Bank Admin	Remote User	Remote Reviewer	Reporting Viewer	Account Group Admin
61	Create Mobile Deposit																
62	Create Receivable Deposit																
63	Create Web Client Deposit																
64	Execute SendMoney Report																
65	Execute Swipe Card																
66	Execute Transact Express																
67	Execute Transact Express Report																
68	Execute Virtual Terminal																
69	Manage Email Configurations	X		X													

* There are no default roles for the Create Provisioned User and Update Provisioned User privileges.

Privileges and User Interface Access Matrix

The table below specifies which user interface components (tabs, links, buttons, etc.) are available with each privilege. For example, according to this matrix, if you grant someone a role that has the Execute System Manager and Create Customer privileges, then they will have access to the Organization Management link and the New Organization button in System Manager.

Some privileges have restrictions on the types of organizations for which they can be assigned. For example, you can only assign a user a role that has the Create Templates privilege for the Service Provider or Bank of First Deposit. The system does not allow you to assign a role containing this privilege for a Correspondent Bank or Customer type organization.

Other privileges are unrestricted in how they can be assigned, but once assigned are only applicable to certain organization types. For example, if you assign a role to a user that has the Create Account privilege, the privilege applies only to Customer type organizations since accounts are associated with Customer type organizations, not any other organization types.

See the notes for each privilege for details about usage and restrictions.

The table also provides cross-references to the most common procedures related to the privilege/user interface component.

#	Privilege	Interface Component	Notes	Cross Reference to Procedures
1	Execute System Manager	System Manager - Organization search tab System Manager - Organization Management link: <ul style="list-style-type: none"> • General tab • Branding tab • Operational Parameters tab (for all but Service Providers) • User Defined Fields (for Customers) • Locations & Contacts tab 	IMPORTANT! Roles that include any privileges with access to interface components inside the System Manager Organization Management link also require this privilege to be present. This is a view-only privilege.	Logging In Understanding the System Manager Window
2	Create Top Orgs	System Manager - Create Top Level Org dialog box	This privilege allows only for the one-time setup of the top-level organization(s) (Service Provider and/or Bank of First Deposit).	Creating New Organizations
3	Update Top Orgs	System Manager - Organization Management link: <ul style="list-style-type: none"> • Edit Organization General Information Icon • Edit Operational Parameters Icon • Add Location Icon • Edit Location Icon • Delete Location Icon • Security tab 	This privilege only applies to Service Provider and Bank of First Deposit type organizations.	Editing Organization General Information Editing Organization Operational Parameters Adding/Editing Locations
4	Create Bank	System Manager - Organization Management link: <ul style="list-style-type: none"> • New Organization Button • Security tab 	This privilege only applies to Correspondent Bank type organizations.	Creating New Organizations

#	Privilege	Interface Component	Notes	Cross Reference to Procedures
5	Update Bank	System Manager - Organization Management link: <ul style="list-style-type: none"> Edit Organization General Information Icon Edit Operational Parameters Icon Add Location Icon Edit Location Icon Delete Location Icon Security tab 	This privilege only applies to Correspondent Bank type organizations.	Editing Organization General Information Editing Organization Operational Parameters Adding/Editing Locations
6	Create Customer	System Manager - Organization Management link: <ul style="list-style-type: none"> New Organization Button Security tab 	This privilege only applies to Customer type organizations.	Creating New Organizations
7	Update Customer	System Manager - Organization Management link: <ul style="list-style-type: none"> Edit Organization General Information Icon Edit Operational Parameters Icon Add Location Icon Edit Location Icon Delete Location Icon Add User Defined Fields Icon Edit User Defined Fields Icon Delete User Defined Fields Icon Security tab 	This privilege only applies to Customer type organizations.	Editing Organization General Information Editing Organization Operational Parameters Adding/Editing Locations

#	Privilege	Interface Component	Notes	Cross Reference to Procedures
8	Execute Account	System Manager - Account search tab System Manager - Organization Management link: <ul style="list-style-type: none"> Accounts tab Show Account Locations & Contacts Icon Account Locations & Contacts Tab 	This privilege only applies to Customer type organizations. This is a view-only privilege	NA
9	Create Account	System Manager - Organization Management link: <ul style="list-style-type: none"> Add Account Icon 	This privilege only applies to Customer type organizations. This privilege is not required for setup of the initial account in the Create Organization dialog box. You must also assign the Execute Account privilege to any roles that contain this privilege in order for users to be able to access these functions.	Adding/Editing Accounts
10	Update Account	System Manager - Organization Management link: <ul style="list-style-type: none"> Edit Account Icon Add Account Location Icon Edit Account Location Icon Delete Account Location Icon 	This privilege only applies to Customer type organizations. You must also assign the Execute Account privilege to any roles that contain this privilege in order for users to be able to access these functions.	Adding/Editing Accounts
11	Execute Contact	System Manager - Organization Management link: <ul style="list-style-type: none"> Show Contacts Icon Show Account Contact Icon 	This is a view-only privilege.	NA

#	Privilege	Interface Component	Notes	Cross Reference to Procedures
12	Create Contact	System Manager - Organization Management link: <ul style="list-style-type: none"> • Add Contact Icon • Add Account Contact Icon 	This privilege is not required for setup of the primary contact in the Create Organization dialog box. You must also assign the Execute Contact privilege to any roles that contain this privilege in order for users to be able to access these functions.	Adding/Editing Contacts
13	Update Contact	System Manager - Organization Management link: <ul style="list-style-type: none"> • Edit Contact Icon • Edit Account Contact Icon 	You must also assign the Execute Contact privilege to any roles that contain this privilege in order for users to be able to access these functions.	Adding/Editing Contacts
14	Delete Contact	System Manager - Organization Management link: <ul style="list-style-type: none"> • Delete Contact Icon • Delete Account Contact Icon 	You must also assign the Execute Contact privilege to any roles that contain this privilege in order for users to be able to access these functions.	Adding/Editing Contacts
15	Execute User	System Manager - User search tab System Manager - Organization Management link: <ul style="list-style-type: none"> • User Tab 	This is a view-only privilege.	NA
16	Create User	System Manager - Organization Management link: <ul style="list-style-type: none"> • Add User Icon 	In order to assign roles to a user, you must have either this privilege or the Update User privilege, and you must have the roles assigned to you and marked assignable. You must also assign the Execute User privilege to any roles that contain this privilege in order for users to be able to access these functions.	Creating Users

#	Privilege	Interface Component	Notes	Cross Reference to Procedures
17	Update User	System Manager - Organization Management link: <ul style="list-style-type: none"> Edit User Icon Assign Multiple Roles for Single Organization Icon Delete Role Icon 	<p>In order to assign roles to or remove roles from a user, you must have either this privilege or the Create User privilege, <i>and</i> you must have the roles assigned to you and marked assignable.</p> <p>You must also assign the Execute User privilege to any roles that contain this privilege in order for users to be able to access these functions.</p>	<p>Creating Users</p> <p>Changing a User's Role Assignments</p> <p>Editing User Settings</p>
18	Execute Roles	System Manager - Custom Roles link	<p>This privilege can only be assigned for Service Provider or Bank of First Deposit type organizations. The system does not allow you to assign a role that contains this privilege to a user for a Correspondent Bank or Customer.</p> <p>This is a view-only privilege.</p>	NA
19	Create Roles	System Manager - Custom Roles link: <ul style="list-style-type: none"> Add Role Icon 	<p>This privilege can only be assigned for Service Provider or Bank of First Deposit type organizations. The system does not allow you to assign a role that contains this privilege to a user for a Correspondent Bank or Customer.</p> <p>You must also assign the Execute Roles privilege to any roles that contain this privilege in order for users to be able to access this function.</p>	Creating Custom Roles

#	Privilege	Interface Component	Notes	Cross Reference to Procedures
20	Update Roles	System Manager - Custom Roles link: <ul style="list-style-type: none"> Edit Role Icon 	<p>This privilege can only be assigned for Service Provider or Bank of First Deposit type organizations. The system does not allow you to assign a role that contains this privilege to a user for a Correspondent Bank or Customer.</p> <p>You must also assign the Execute Roles privilege to any roles that contain this privilege in order for users to be able to access this function.</p>	Creating Custom Roles
21	Delete Roles	System Manager - Custom Roles link: <ul style="list-style-type: none"> Delete Role Icon 	<p>This privilege can only be assigned for Service Provider or Bank of First Deposit type organizations. The system does not allow you to assign a role that contains this privilege to a user for a Correspondent Bank or Customer.</p> <p>You must also assign the Execute Roles privilege to any roles that contain this privilege in order for users to be able to access this function.</p>	Creating Custom Roles
22	Execute Rules	System Manager - Organization Management link: <ul style="list-style-type: none"> Rules Tab Show Account Rules Icon Account Rules Tab 	<p>This privilege applies to all organization types except Service Provider.</p> <p>This is a view-only privilege.</p>	NA
23	Create Rules	System Manager - Organization Management link: <ul style="list-style-type: none"> Add Account Rule Icon Add Rule Icon 	<p>This privilege applies to all organization types except Service Provider.</p> <p>You must also assign the Execute Rules privilege to any roles that contain this privilege in order for users to be able to access these functions.</p>	Adding/Editing Accounts Managing Scrutiny Rules

#	Privilege	Interface Component	Notes	Cross Reference to Procedures
24	Update Rules	System Manager - Organization Management link: <ul style="list-style-type: none"> Edit Account Rule Icon Edit Rule Icon 	This privilege applies to all organization types except Service Provider. You must also assign the Execute Rules privilege to any roles that contain this privilege in order for users to be able to access these functions.	Adding/Editing Accounts Managing Scrutiny Rules
25	Execute Security Profile	System Manager - Security link	This privilege can only be assigned for Service Provider or Bank of First Deposit type organizations. The system does not allow you to assign a role that contains this privilege to a user for a Correspondent Bank or Customer. This is a view-only privilege.	NA
26	Create Security Profile	System Manager - Security link: <ul style="list-style-type: none"> Add Security Profile Icon 	This privilege can only be assigned for Service Provider or Bank of First Deposit type organizations. The system does not allow you to assign a role that contains this privilege to a user for a Correspondent Bank or Customer. You must also assign the Execute Security Profile privilege to any roles that contain this privilege in order for users to be able to access this function.	Configuring Security Profiles

#	Privilege	Interface Component	Notes	Cross Reference to Procedures
27	Update Security Profile	System Manager - Security link: <ul style="list-style-type: none"> Edit Security Profile Icon 	<p>This privilege can only be assigned for Service Provider or Bank of First Deposit type organizations. The system does not allow you to assign a role that contains this privilege to a user for a Correspondent Bank or Customer.</p> <p>You must also assign the Execute Security Profile privilege to any roles that contain this privilege in order for users to be able to access this function.</p>	<p>Configuring Security Profiles</p> <p>Assigning a Security Profile to an Organization</p>
28	Delete Security Profile	System Manager - Security link: <ul style="list-style-type: none"> Delete Security Profile Icon 	<p>This privilege can only be assigned for Service Provider or Bank of First Deposit type organizations. The system does not allow you to assign a role that contains this privilege to a user for a Correspondent Bank or Customer.</p> <p>You must also assign the Execute Security Profile privilege to any roles that contain this privilege in order for users to be able to access this function.</p>	Configuring Security Profiles
29	Execute Templates	System Manager - Templates link	<p>This privilege can only be assigned for Service Provider or Bank of First Deposit type organizations. The system does not allow you to assign a role that contains this privilege to a user for a Correspondent Bank or Customer.</p> <p>This is a view-only privilege.</p>	NA

#	Privilege	Interface Component	Notes	Cross Reference to Procedures
30	Create Templates	System Manager - Templates link: <ul style="list-style-type: none"> • Add Organization Template Icon • Add Defined Field Template Icon • Add Defined Field Group Icon • Add Custom Data Field dialog box - Save as Template button • Add Payment Data Column dialog box - Save as Template button 	<p>This privilege can only be assigned for Service Provider or Bank of First Deposit type organizations. The system does not allow you to assign a role that contains this privilege to a user for a Correspondent Bank or Customer.</p> <p>You must also assign the Execute Templates privilege to any roles that contain this privilege in order for users to be able to access these functions.</p>	Creating and Managing Templates
31	Update Templates	System Manager - Templates link: <ul style="list-style-type: none"> • Edit Organization Template Icon • Edit Defined Field Template Icon • Edit Defined Field Group Icon • Edit Custom Data Field dialog box - Save as Template button • Edit Payment Data Column dialog box - Save as Template button 	<p>This privilege can only be assigned for Service Provider or Bank of First Deposit type organizations. The system does not allow you to assign a role that contains this privilege to a user for a Correspondent Bank or Customer.</p> <p>You must also assign the Execute Templates privilege to any roles that contain this privilege in order for users to be able to access these functions.</p>	Creating and Managing Templates

#	Privilege	Interface Component	Notes	Cross Reference to Procedures
32	Delete Templates	System Manager - Templates link: <ul style="list-style-type: none"> Delete Organization Template Icon Delete Defined Field Template Icon Delete Defined Field Group Icon 	<p>This privilege can only be assigned for Service Provider or Bank of First Deposit type organizations. The system does not allow you to assign a role that contains this privilege to a user for a Correspondent Bank or Customer.</p> <p>You must also assign the Execute Templates privilege to any roles that contain this privilege in order for users to be able to access these functions.</p>	Creating and Managing Templates
33	Execute App Parameter	System Manager - Organization Management link: <ul style="list-style-type: none"> Applications Tab 	<p>This privilege only applies to Service Provider, Bank of First Deposit, and Correspondent Bank type organizations.</p> <p>This is a view-only privilege.</p>	NA
34	Create App Parameter	System Manager - Organization Management link: <ul style="list-style-type: none"> Add Application Icon 	<p>This privilege only applies to Service Provider, Bank of First Deposit, and Correspondent Bank type organizations.</p> <p>You must also assign the Execute App Parameter privilege to any roles that contain this privilege in order for users to be able to access these functions.</p>	Configuring Applications
35	Update App Parameter	System Manager - Organization Management link: <ul style="list-style-type: none"> Edit Application Icon 	<p>This privilege only applies to Service Provider, Bank of First Deposit, and Correspondent Bank type organizations.</p> <p>You must also assign the Execute App Parameter privilege to any roles that contain this privilege in order for users to be able to access these functions.</p>	Configuring Applications

#	Privilege	Interface Component	Notes	Cross Reference to Procedures
36	Create Parent Org Brand	System Manager - Organization Management link: <ul style="list-style-type: none"> Add Brand Icon 	This privilege only applies to Service Provider, Bank of First Deposit, and Correspondent Bank type organizations.	Configuring Branding
37	Update Parent Org Brand	System Manager - Organization Management link: <ul style="list-style-type: none"> Edit Brand Icon 	This privilege only applies to Service Provider, Bank of First Deposit, and Correspondent Bank type organizations.	Configuring Branding
38	Delete Parent Org Brand	System Manager - Organization Management link: <ul style="list-style-type: none"> Delete Brand Icon 	This privilege only applies to Service Provider, Bank of First Deposit, and Correspondent Bank type organizations.	Configuring Branding
39	Create Child Org Brand	System Manager - Organization Management link: <ul style="list-style-type: none"> Add Brand Icon 	This privilege only applies to Customer type organizations.	Configuring Branding
40	Update Child Org Brand	System Manager - Organization Management link: <ul style="list-style-type: none"> Edit Brand Icon 	This privilege only applies to Customer type organizations.	Configuring Branding
41	Delete Child Org Brand	System Manager - Organization Management link: <ul style="list-style-type: none"> Delete Brand Icon 	This privilege only applies to Customer type organizations.	Configuring Branding
42	Update Licenses	System Manager - Organization Management link: <ul style="list-style-type: none"> License Mgmt Tab 	This privilege only applies to Bank of First Deposit and Correspondent Bank type organizations.	Managing Licenses
43	Execute Reports	<ul style="list-style-type: none"> NetCapture Portal Reporting tab Server Reports button in Desktop Client All customer-facing reports in Web Client Server Side Reporting 	The inheritable flag does not apply to this privilege. If you assign this privilege to a user for a bank, the user will have access to reports for all other correspondent bank and customer organizations below that bank in the hierarchy regardless of whether or not the inheritable flag is set.	<i>Reporting and Deposit Management User Guide</i>

#	Privilege	Interface Component	Notes	Cross Reference to Procedures
44	Execute Account Groups	System Manager - Account Grouping link	<p>This privilege can only be assigned for Service Provider or Bank of First Deposit type organizations. The system does not allow you to assign a role that contains this privilege to a user for a Correspondent Bank or Customer.</p> <p>This is a view-only privilege.</p>	NA
45	Create Account Groups	System Manager - Account Grouping link <ul style="list-style-type: none"> Add Account Group Icon 	<p>This privilege can only be assigned for Service Provider or Bank of First Deposit type organizations. The system does not allow you to assign a role that contains this privilege to a user for a Correspondent Bank or Customer.</p> <p>You must also assign the Execute Account Groups privilege to any roles that contain this privilege in order for users to be able to access this function.</p>	Creating Account Groups
46	Delete Account Groups	System Manager - Account Grouping link <ul style="list-style-type: none"> Delete Account Group Icon 	<p>This privilege can only be assigned for Service Provider or Bank of First Deposit type organizations. The system does not allow you to assign a role that contains this privilege to a user for a Correspondent Bank or Customer.</p> <p>You must also assign the Execute Account Groups privilege to any roles that contain this privilege in order for users to be able to access this function.</p>	Creating Account Groups

#	Privilege	Interface Component	Notes	Cross Reference to Procedures
47	Update Account Groups	System Manager - Account Grouping link <ul style="list-style-type: none"> Edit Account Group Icon 	<p>This privilege can only be assigned for Service Provider or Bank of First Deposit type organizations. The system does not allow you to assign a role that contains this privilege to a user for a Correspondent Bank or Customer.</p> <p>You must also assign the Execute Account Groups privilege to any roles that contain this privilege in order for users to be able to access this function.</p>	Creating Account Groups
48	Adjustment Processing	System Manager - Organization Management link: <ul style="list-style-type: none"> Adjustment Processing Tab 	This privilege only applies to Bank of First Deposit, Correspondent Bank, and Customer type organizations.	Configuring Adjustments
49	Create Deposit	<ul style="list-style-type: none"> Desktop Client Web Client Users Deposit Status report in Web Client Server Side Reporting 	<p>This privilege only applies to Customer type organizations.</p> <p>This privilege is required to access Web Client applications.</p> <p>You can assign roles that contain this privilege at the account level if you want to limit the number of accounts to which the user can make deposits. See <i>Changing a User's Role Assignments</i>. However, the account-level assignment will not take effect for the Users Deposit Status report. The report will still contain all deposits submitted by the user, regardless of which account they were submitted to.</p>	<i>Web Client User Guide</i> <i>Desktop Client User Guide</i>

#	Privilege	Interface Component	Notes	Cross Reference to Procedures
50	Review Remote Deposit	Desktop Client	<p>This privilege only applies to Customer type organizations.</p> <p>This privilege does not apply to Web Client, only to Desktop Client.</p> <p>You can assign roles that contain this privilege at the account level if you want to limit the number of accounts for which the user can approve deposits. See <i>Changing a User's Role Assignments</i>.</p>	<p>Configuring Dual Control</p> <p><i>Desktop Client User Guide</i></p>
51	Execute Deposit Review	Deposit Review tab	<p>This privilege only applies to Customer type organizations.</p> <p>This is a view-only privilege.</p>	Introducing Deposit Review
52	Update Deposit Review	Deposit Review - Review Deposits	<p>This privilege only applies to Customer type organizations.</p> <p>Users with this privilege do NOT also need the Execute Deposit Review privilege. This privilege provides access to the Deposit Review tab and all functionality within the Review Deposits screen.</p>	Reviewing Deposits in Deposit Review
53	Update Deposit Queue	Deposit Review - Manage Queue	<p>This privilege only applies to Customer type organizations.</p> <p>Users with this privilege do NOT also need the Execute Deposit Review privilege. This privilege provides access to the Deposit Review tab and all functionality within the Manage Queue screen.</p>	Managing Queues in Deposit Review

#	Privilege	Interface Component	Notes	Cross Reference to Procedures
54	Manage Web Client Settings	Web Manager - System Settings tab	This privilege can only be assigned for Service Provider or Bank of First Deposit type organizations. The system does not allow you to assign a role that contains this privilege to a user for a Correspondent Bank or Customer.	<i>NetCapture Web Client Gateway System Manual</i>
55	Manage Web Client Deposits	Web Manager - Deposit tab	This privilege can only be assigned for Service Provider, Bank of First Deposit, or Correspondent Bank type organizations. The system does not allow you to assign a role that contains this privilege to a user for a Customer.	<i>Reporting and Deposit Management User Guide</i>
56	Execute Support Util	Capture Gateway, Extractor, and Portal support info generation web pages	This privilege is only usable by admins who have access to the NetCapture Platform server environment.	<i>NetCapture Platform System Manual</i>
57	Create Provisioned User		<p>In order to assign roles to a provisioned user, you must have either this privilege or the Update Provisioned User privilege, AND you must have the roles assigned to you and marked assignable.</p> <p>You must also assign the Execute User privilege to any roles that contain this privilege in order for users to be able to access these functions.</p> <p>Note: This privilege is not associated with any default roles.</p> <p>This privilege is used during custom User Provisioning applications. Contact your Service Representative for details.</p>	

#	Privilege	Interface Component	Notes	Cross Reference to Procedures
58	Update Provisioned User		<p>In order to assign roles to or remove roles from a user, you must have either this privilege or the Create Provisioned User privilege, <i>and</i> you must have the roles assigned to you and marked assignable.</p> <p>You must also assign the Execute User privilege to any roles that contain this privilege in order for users to be able to access these functions.</p> <p>Note: This privilege is not associated with any default roles.</p> <p>This privilege is used during custom User Provisioning applications. Contact your Service Representative for details.</p>	
59	Create Consumer Deposit	Entry Portal - Small Business tab	Applies to the entry.	<i>NetCapture Portal User Guide</i>
60	Create Desktop Deposit	Desktop Client	Applies to the entry.	Not Used
61	Create Mobile Deposit	Entry Portal - Mobile Deposit	Applies to the entry.	Not Used
62	Create Receivable Deposit	Entry Portal - Receivable	Applies to the entry.	Not Used
63	Create Web Client Deposit	Entry Portal - Web Client tab	Applies to the entry.	Not Used
64	Execute SendMoney Report	Entry Portal - SendMoney tab	Applies to the entry.	Not Used
65	Execute Swipe Card	Entry Portal - Swipe Card tab	Applies to the entry.	Not Used
66	Execute Transact Express	Entry Portal - Transact Express	Applies to the entry.	Not Used
67	Execute Transact Express Report	Entry Portal - Reporting tab	Applies to the entry.	Not Used

#	Privilege	Interface Component	Notes	Cross Reference to Procedures
68	Execute Virtual Terminal	Entry Portal - Virtual Terminal tab	Applies to the entry.	Not Used
69	Manage Email Configurations	System Manager – Email Configuration tab	This privilege only applies to Bank of First Deposit and Correspondent Bank type organizations.	Configuring Deposit Confirmation Email Contents

Usage Examples

Following are some scenarios describing how you can use privileges along with the assignable and inheritable flags to control system access using the organizational hierarchy depicted in the figure in *Examples of Assignable and Inheritable Usage*.

The purpose of these examples is to provide context about how the assignable and inheritable flags work with privileges to restrict system access. As such, the examples are simplified. You likely will want to provide more privileges to certain users whose job functions include many system configuration tasks.

Case 1: User Who Manages Accounts

Need: You want a user named John to be able to create accounts for all of the Customers of a Correspondent Bank A.

Configuration: In this case, you assign John a role containing at least these privileges for Correspondent Bank A and mark it as Execute and Inherit:

- Execute System Manager
- Execute Account
- Create Account
- Update Account

Result: John will have access to create accounts for all of the organizations under Correspondent Bank A in the hierarchy, but he will *not* have access to assign this role to other users.

Case 2: User who Administer the Organization Hierarchy

Need: You want a user named Jane to be able to set up and maintain organizations in the system.

Configuration: In this case, you assign Jane a role containing at least these privileges for the Bank of First Deposit and mark it as Execute and Inherit:

- Execute System Manager
- Update Top Orgs
- Create Bank
- Update Bank
- Create Customer
- Update Customer

If you want Jane to be able to create and manage organization templates, you must ensure she also has these privileges:

- Execute Templates
- Create Templates

- Update Templates
- Delete Templates

Result: Jane will have access to create and modify Correspondent Bank and Customer type organizations, and to modify the Bank of First Deposit's general organization settings and operational parameters. Jane also has access to assign security profiles to organizations. If you granted template privileges, she also has access to create and modify organization templates.

Case 3: Users who Manages Other Users

Need: You want a user named Alice to be able to set up all of the other users in the system and assign them roles as appropriate.

Configuration: In this case, you assign Alice a role containing at least these privileges for the Bank of First Deposit and mark it as Execute and Inherit:

- Execute System Manager
- Execute User
- Create User
- Update User

In addition, you must assign Alice any of the existing roles in the system that you want to be assigned to other users and ensure they are all marked as assignable.

Result: Alice will have access to create new users at any level in the organization, and can assign them all of the roles that she holds and that are marked as assignable. Alice also has access to assign security profiles to users. However, Alice does NOT have access to assign the role containing Execute, Create, and Update User privileges to other users since it was not marked as assignable.

Case 4: Users who Manages System Security

Need: You want a user named Bob to be able to define the security settings restricting system access, including password settings, access times, and roles available in the system.

Configuration: In this case, you assign Bob a role containing at least these privileges for the Bank of First Deposit and mark it as Execute and Inherit:

- Execute System Manager
- Execute Security Profile
- Create Security Profile
- Update Security Profile
- Delete Security Profile
- Execute Roles
- Create Roles
- Update Roles
- Delete Roles

Result: Bob will have access to create and modify the roles available in the system. He will also have access to create and modify security profiles that contain password settings, access control settings, and session control settings.

IMPORTANT! Notice that duties are segregated in cases 3 and 4 so that the user who creates roles is not the same as the user who assigns roles to other users. Bob cannot assign the roles he created because he does not have the Update User privilege. Alice can assign roles since she has this privilege. However, before Alice can assign the roles that Bob created, Bob must assign the new roles to Alice and mark them as assignable.

Suggested Operational Guidelines

Before you begin working in System Manager, you should understand what potential problems may occur when administering Web Client applications in the system. System configuration changes only take effect in Web Client applications when users log in to the application. They do not take effect during sessions that are already open on the workstation. Your organization should set up operational policies and procedures that will help mitigate the following potential processing issues.

Field	Description	Suggested Procedural Guidelines
Configuration Changes during Deposit Processing	<p>When an administrator changes configuration for customers, accounts, applications, rules, or user privileges in System Manager, these changes will be carried to Web Client applications ONLY when a user logs in to the application. If a user is logged in to the Web Client when changes are made in System Manager, the Web Client application will not have access to the configuration changes until the user logs out and then logs back in. Because of this, there is a possibility that deposits may be processed inadvertently through the Web Client application.</p> <p>Scenario: A user accesses System Manager and deactivates an account. At the same time, a Web Client user is in the process of preparing a deposit for the (now inactivated) account. The Web Client user will be able to submit the deposit to the inactivated account.</p>	<p>Identify times for making configuration changes in System Manager that will ensure that all deposits are completed and no Web Client users are logged in to the system. You may want to set operational procedures for System Manager users that ensure that all configuration changes are completed outside the allowable login times for Web Client users.</p> <p>Using System Manager, you can configure the days and times at which Web Client users are allowed to log in to the system. See <i>Configuring Security Profiles</i> for information on how to configure allowed login times.</p>
Suspended Deposits and Configuration Changes	<p>When a customer or account is inactivated in System Manager, there is a possibility that suspended deposits for the inactivated customer/account already exist at a Web Client workstation.</p> <p>Scenario: A Web Client workstation is holding a suspended deposit for an account. An administrator in System Manager inactivates the account. A Web Client user later logs in to complete the deposit, but the deposit is not presented to the user for completion since the account has been inactivated.</p>	
Inactivating System Components	<p>When you inactivate an organization, account, user, or application in System Manager, all its associated data remains in its current state—in other words, it is not automatically set to an inactive status.</p> <p>Scenario: You inactivate a Customer organization. The accounts, users, and applications that are associated with the organization remain active.</p>	<p>When inactivating data in System Manager, make it a policy to also inactivate the appropriate associated organizations, accounts, users, or applications. For example, to completely inactivate all the data for an organization, you must also locate its accounts, users, and applications in System Manager and set their statuses to inactive.</p>

Field	Description	Suggested Procedural Guidelines
Adding Roles for Logged-In Users	<p>When you add roles for a user that is currently logged in to the system, the role's privileges are not granted until that user logs out and then logs back in.</p> <p>Scenario: Two different System Manager users are logged in at the same time. User A grants user B the privileges to edit an organization. User B can see the new organization, but when attempting to access the organization, error messages appear. User B must log out and then log back in to be able to access the organization.</p>	Identify times for making configuration changes in System Manager that will ensure that no other users are logged in to the system. Also, make it a policy to notify Portal users when their privileges have changed.

Initial Setup

As a general rule, you must complete a basic set of configurations before the system can process deposits. Use the instructions in the following sections to complete the configuration.

- Requirements
- Initial Setup Checklist

Requirements

IMPORTANT! Before beginning any configuration tasks in System Manager, your system administrator must complete configuration of the top-level organization(s), applications, and initial users as described in the Net-Capture Platform System Manual. The System Administrator will provide you with a user name and password for the system.

This checklist walks you through the high-level initial setup steps. These steps are recommended for successful operation of the system—they will help you create the typical types of organizations and users that are required to run Desktop Client and Web Client applications. This checklist describes the most typical setup scenario. Your organization's structure may vary, so use the checklist only as a guideline.

Initial Setup Checklist

Perform the following REQUIRED and OPTIONAL steps to complete initial setup in System Manager:

Log In... (REQUIRED)

1. Log in to Portal using the user name and password provided to you by your system administrator.
After logging in for the first time, you will be forced to change your password.
2. Change your password.

For step-by-step instructions, see *Logging In* and *Changing Your Password*.

Create Correspondent Banks and Customers... (REQUIRED)

1. Click the System Manager tab.
2. Click the Organization Management link.
3. Create the Customer organizations that will host Desktop Client or Web Client applications to process deposits. If you are using any Correspondent Banks, create those organizations as well.

For step-by-step instructions, see *Creating New Organizations*.

Create Users... (REQUIRED)

1. In the organization tree, select the organization under which you want to create users.

You will likely want to create some of the following users under the top-level organization and other users (specifically, those with the Remote User role) under specific Customer organizations. Be sure you have reviewed *Understanding User Roles and Privileges* carefully before you start creating users and assigning roles.

2. Click the Users tab.
3. Create the following users.

Requirement	Value
User with Banking Operations, Correspondent Bank Admin, Customer Admin, BOFD Admin, and Template Administrator roles	Name: User name: Password:
User with Customer Admin and Banking Operations roles	Name: User name: Password:
User with Customer Service role	Name: User name: Password:
User with Account Groups Administrator role	Name: User name: Password:
User with Security Admin, System Admin, Help Desk Technician, and Role Administrator roles	Name: User name: Password:
User with Banking Operations role	Name: User name: Password:
User with Deposit Review Agent role	Name: User name: Password:
User(s) with Reporting Viewer role	Name: User name: Password:
User(s) with Remote User role You need to configure this for each user who will access Desktop Client or Web Client to make deposits.	Name: User name: Password:

If you desire, you can also create your own custom roles and assign users to those roles. See *Understanding User Roles and Privileges* and *Creating Custom Roles* for more information.

IMPORTANT! You are responsible for providing the users with the user names and passwords you create. The password is not stored in a visible format after you enter it. You should keep track of it elsewhere, or

provide it to the user immediately upon setup. Otherwise, a Help Desk Technician will have to reset the user's password before the user will be able to log in.

For step-by-step instructions, see *Creating Users*.

Configure Adjustments... (REQUIRED)

Complete this configuration to specify how adjustments are constructed by the system, including which route/transit numbers, account numbers, and transaction codes to use for adjustments.

1. Click the Organization Management link.
2. Select the Bank of First Deposit organization in the organization tree.
3. In the Adjustment Processing tab, edit the adjustment setup according to your organization's policies.

For step-by-step instructions, see *Configuring Adjustments*.

Configure Adjustment Email Notifications... (REQUIRED)

1. In the Locations & Contacts tab for your organization, set the primary contact. The primary contact receives email notifications.
2. In the Operational Parameters tab for your organization, select Send Reviewer Email.
3. In the Applications tab, ensure the correct SMTP server address is specified for your instance of Portal.

For step-by-step instructions, see *Configuring Adjustment Notification Emails*.

Configure Branding... (OPTIONAL)

Note: This step is optional. If you choose not to customize branding, the default settings will be used.

1. In the Branding tab for your organization, enter any custom branding information to be used in your Desktop Client and Web Client applications.
2. Edit the Report Branding to enter any custom branding information to be used in server reports.

For step-by-step instructions, see *Configuring Branding* and *Configuring Report Branding*.

Create Scrutiny Rules... (OPTIONAL)

Note: This step is optional. If you choose not to edit scrutiny rules, the default settings will be used.

In the Rules tab for your organization, create scrutiny rules for the Bank of First Deposit. These rules will apply to all child organizations, unless you set up rules for a particular organization, which will override these rules.

For step-by-step instructions, see *Managing Scrutiny Rules*.

Configure Report Parameters... (OPTIONAL)

Note: This step is optional. If you choose not to edit the report parameters, the default settings will be used.

In the Operational Parameters tab, under Report Parameters, use the information you gathered for server report parameters to set limits for the amount of data included in reports.

For step-by-step instructions, see *Configuring Report Parameters*.

Configure Security Parameters... (OPTIONAL)

Note: This step is optional. If you choose not to edit the report parameters, the default settings will be used.

1. In the Security tab, create a new security profile that determines how access to applications in the system is granted.
2. Click the Organization Management tab.
3. Select an organization in the organization tree.
4. On the Security tab, choose the security profile you want to assign to this organization.

For step-by-step instructions, see *Configuring Security Profiles*.

Set up Organization Templates... (OPTIONAL)

Note: This step is optional.

If many of the settings you will use are the same for each organization you create in the system, you may want to create a template to capture those settings. The template can then be applied each time you create a new organization, saving setup time and ensuring consistency across the organizations in the system.

For step-by-step instructions, see *Creating and Managing Templates*.

You have now completed initial setup of the system. In order to begin processing items, you need to complete some additional setup to add customers and Web Client seats. Continue with the next section, *Typical Setup Tasks*.

Typical Setup Tasks

Following are some typical setup tasks you will need to complete on an ongoing basis.

- Adding Customers
- Typical Maintenance

Adding Customers

Following are the steps you will need to complete when adding new customer organizations that will host Web Client seats. There are both required and optional steps.

1. Create customer organizations (required). See *Creating New Organizations*.
2. Create users for the customer organization (required). See *Creating Users*.
3. Configure dual control (optional). See *Configuring Dual Control*.
4. Configure user-defined fields (optional). See *Configuring User-Defined Fields*.
5. Configure customer organization branding (optional). See *Configuring Branding* and *Configuring Report Branding*.
6. Add customer locations and contacts (optional). See *Adding/Editing Locations* and *Adding/Editing Contacts*.
7. Add accounts for the customer (optional). See *Adding/Editing Accounts*.
8. Set customer and account level scrutiny rules (optional). See *Managing Scrutiny Rules*.
9. Configure customer security parameters (optional). See *Configuring Security Profiles*.
10. Configure adjustments for the customer (optional). See *Configuring Adjustments*.

When adding a new customer, make sure that all servers and applications are installed and running and users have their system user names and passwords.

Typical Maintenance

Following are some tasks you will need to complete on a periodic basis to manage organizations, users, and operational settings.

- Force user logout: You will need to do this if a user's session is interrupted unexpectedly (for example, if there is a power outage) and they are unable to log back into the system. See *Forcing a Client User Logout*.
- Change user passwords: You will need to do this if users forget their passwords, or if they believe their passwords have been compromised. See *Editing User Settings*.
- Edit the client system message: You may want to edit this message if you want to notify your Web Client users about planned system downtime or provide updated support contact information. See *Configuring the Client System Message*.
- Add/remove roles from users: You will need to do this if you need to change the roles assigned to a user that govern their level of system access. See *Changing a User's Role Assignments*.
- Edit user settings: You will need to do this if you need to change a user's maximum deposit limit, if you need to revoke a user's system access by changing their status, or if you want to change the security profile assigned to a user. See *Editing User Settings*.
- Edit existing organizations: You will most likely need to do this if you need to set an organization so it is no longer active in the system. You may also need to do this if an organization name or customer reference ID changes. See *Editing Organization General Information*.
- Edit or delete branding: You will need to do this if any of your organizations' branding information changes. See *Configuring Branding* and *Configuring Report Branding*.
- Edit operational parameters: You will need to do this if you want to change the way that Web Client applications operate. This includes settings for export files, image type, duplicate checking, CAR thresholds, etc. See *Editing Organization Operational Parameters*.
- Edit or delete user-defined fields (customers only): You will need to do this if you need to change any of the customized data that you gather from your customer organizations. See *Configuring User-Defined Fields*.
- Create, edit, or delete locations and contacts: You will need to do this if any of the individuals listed as contacts for an organization or account change, or if an organization's location changes. See *Adding/Editing Contacts*.
- Edit or inactivate accounts (customers only): You will need to do this if you make any changes to the bank accounts you are using in the system. See *Adding/Editing Accounts*.
- Edit or inactivate scrutiny rules: You will need to do this if you need to change the rules used to validate scanned items. See *Managing Scrutiny Rules*.
- Edit security parameters: You will need to do this if your organization wants to change the way session timeout occurs, modify the times users are allowed to access the systems, or change password restrictions. See *Configuring Security Profiles* and *Assigning a Security Profile to an Organization*.
- Manage licenses: You will need to manage licenses on an ongoing basis by uploading licenses received from Finastra to help you track seat usage. See *Managing Licenses*.
- Edit adjustments: You will need to do this if the account numbers, route/transit numbers, aux on-us numbers, or transaction codes you are using in adjustments changes, or if you want to add a new adjustment type. See *Configuring Adjustments*.

3 Using System Manager

This section contains instructions for using System Manager to complete configuration tasks. For checklists that will help you understand what configuration needs to be done for initial setup, when adding customers, or as ongoing maintenance, see *Completing Initial Setup*.

You can use System Manager to do the following:

- Configuring Applications
- Creating New Organizations
- Editing Organization General Information
- Editing Organization Operational Parameters
- Configuring the Client System Message
- Creating Users
- Searching for a User
- Editing User Settings
- Creating Custom Roles
- Configuring Adjustments
- Configuring Adjustment Notification Emails
- Configuring User-Defined Fields
- Creating and Managing Templates
- Managing Scrutiny Rules
- Configuring Deposit Confirmation Email Contents
- Configuring Branding
- Configuring Report Branding
- Configuring Report Parameters
- Configuring Security Profiles
- Assigning a Security Profile to an Organization
- Configuring Dual Control
- Creating Account Groups
- Adding/Editing Locations
- Adding/Editing Contacts
- Adding/Editing Accounts
- Forcing a Client User Logout
- Managing Licenses

Configuring Applications

Use System Manager to add Platform applications that are run by the Bank of First Deposit or Service Provider, such as the NetCapture Portal, Capture Gateway, Extractor, or Web Client Server Reporting.

* There is no need to add Web Client or Desktop Client applications in System Manager.

- Adding application configurations in System Manager allows installed applications to communicate with each other properly. You must also install the applications in the appropriate physical locations

before they will be operational. You can install the applications before or after you configure them in System Manager.

The following applications are pre-configured for the default organization (either the Bank of First Deposit or Service Provider):

- Capture Gateway Server
- Extractor
- NetCapture Portal

* The Web Client Server Reporting application (called Server Side Reporting in System Manager) is for the Web Client only (NOT Desktop Client). It is not pre-configured for the default organization. If you are using Web Client, you must add this application manually. After setting up the application in System Manager, you must reboot the server for the changes to take effect.

Requirements for Configuring Applications

Before you configure applications in System Manager, you must work with the administrator of the applications to determine how the applications should be configured. Use the following tables to obtain the information you will need before you begin.

All NetCapture Platform Applications

Gather the following information for each component of the NetCapture Platform (Capture Gateway, Portal, Extractor, and Web Client Server Reporting). Required information is marked with an asterisk (*). You can choose to leave the default values for the remaining parameters if you wish.

Property	Description	Values, Examples	Default	My Value
Type*	The type of application you are adding/editing.	Capture Gateway Portal Extractor Server Side Reporting	NA	<ul style="list-style-type: none">• Capture Gateway• Portal• Extractor• Server Side Reporting
Application Name*	A unique name for the application. You can use the default if you are installing only one instance of the component. If you are configuring multiple instances of an application, you will need unique names for each one to distinguish them from each other. The application name is case sensitive. This name must be the same as the name specified in the web.xml file for the application.	CG NDPortal Extractor SSReporting	blank	Capture Gateway: Portal: Extractor: Server Side Reporting:
Description	A description of the application. This is optional.		blank	

Property	Description	Values, Examples	Default	My Value
SMTP Host*	The IP address for the SMTP mail server used for email communication.	Example: 10.200.1.1	blank	Capture Gateway: Portal: Extractor: Server Side Reporting:
Status*	This can be active or inactive. If you select active, users are able to access the application and process items in the system. If you select inactive, the application is not currently active and users are not able to access it.	Active Inactive	Active	<ul style="list-style-type: none"> Active Inactive

Capture Gateway

Gather the following information for each Capture Gateway you plan to configure. Required information is marked with an asterisk (*). You can choose to leave the default values for the remaining parameters if you wish.

Property	Description	Values, Examples	Default	My Value
Authentication Type*	This option sets the required method of authentication for the applications associated with this server. Select External to use certificate-based authentication or select Internal to use simple password-based authentication.	External Internal		<ul style="list-style-type: none"> External Internal
Plug-in Class*	This field appears only if you have selected External for the Authentication Type. If you are using external authentication, enter the plug-in class to enable it. Contact your Service Representative for this value.			
Compatible Client Version	Indicates which versions of Desktop Client this Capture Gateway will support. You can change this value if you want to force Desktop Client users to upgrade to a newer version and not allow them to continue to use previous versions.	9 (5.0 Patch 8) 10 (5.1) 11 (5.2) 12 (6.4+) 13 (7.1) 14 (8.0) 15 (8.1) 16 (8.3)		<ul style="list-style-type: none"> 9 10 11 12 13 14 15 16

Property	Description	Values, Examples	Default	My Value
URL to download updates for client	The URL of the server your organization uses to push automatic updates of the Desktop Client software out to client workstations.	www.example.com	CONFIGURE_ME	

Portal and Server-Side Reporting

Gather the following information for each Portal or Server-Side Reporting application you plan to configure. Required information is marked with an asterisk (*).

Property	Description	Values, Examples	Default	My Value
Authentication Type*	This option sets the required method of authentication for the applications associated with this server. Select External to use certificate-based authentication or select Internal to use simple password-based authentication.	External Internal	Internal	<ul style="list-style-type: none"> External Internal
Plug-in Class*	This field appears only if you have selected External for the Authentication Type. If you are using external authentication, enter the plug-in class to enable it. Contact your Service Representative for this value.			
Web App Name	This name must be the same as the name you gave the application when you deployed it in WebLogic.		NA	

Extractor

Gather the following additional information for each Extractor you plan to configure. You can choose to leave the default values for the parameters if you wish. Required information is marked with an asterisk (*).

Property	Description	Values, Examples	Default	My Value
Sleep Time*	The Extractor sleep time, specified in seconds.		60	
Temp Directory*	The temp directory for storing data and image files during processing. Specify an absolute path name (relative paths will not work). This directory <i>cannot</i> be the same as the Temp Image Directory.		temp	
Temp Image Directory*	The temp directory for storing individual image files during processing. This directory <i>cannot</i> be the same as the Temp Directory.		temp/ images	

Property	Description	Values, Examples	Default	My Value
Archive Directory*	The directory where processed extract files will be stored for archiving. Specify an absolute path name (relative paths will not work).		CONFIGURE_ME	
Days to Archive*	<p>The number of days to store extract files in the archive directory.</p> <p>The directories within the archive directory that exceed this number (configured number of days + 1) are deleted on startup, and also at about midnight, assuming a small value for the sleep.time property.</p> <p>If this setting is set to 0, the extract files are deleted after the file transfer to the DG is successful, without being archived.</p>	0-365	14	
Sequence Number Size*	<p>Specifies whether you want to generate 10-digit or 15-digit item sequence numbers (this is dependent on the version of Decision Gateway you are using).</p> <p>If this value is 10, the item number will be a 10-digit number at position 31 in the detail record.</p> <p>If this value is 15, the item number will be a 15-digit number at position 558 in the detail record.</p>	10 15	15	<ul style="list-style-type: none"> • 10 • 15
Extractor Plugin	<p>Specifies whether 15-digit or 10-digit item numbers are generated by the Extractor.</p> <p>This setting is not required if the Sequence Number Size is set to 10.</p>	com.netdeposi. extractor.impl .N DExtractorFacadeImpl	com.netdeposit. extractor.impl.N DExtractorFacadeImpl	NA
Send ACH Opt Out*	<p>Specifies whether you plan to use ACH opt-out functionality in Web Client. This flag indicates you intend to send ACH opt-out information to the Decision Gateway.</p> <p>This applies to Decision Gateway version 2.0 only, as the functionality is not available for previous versions.</p> <p>Note: If this parameter is set to true, Sequence Number Size must be set to 15; otherwise setting this value to true has no effect.</p>	true false	true	<ul style="list-style-type: none"> • True • False
<p>Image Conversion Configuration Settings</p> <p>By default, image conversion settings match the image format required by Decision Gateway version 1.6 or higher. It is recommended that you do not change the default settings.</p>				

Property	Description	Values, Examples	Default	My Value
Image Type*	If the incoming image type is different from the specified value, the image type will be converted to the specified value. If you specify other than TIFF, you will encounter errors.	TIFF	TIFF	TIFF
Image Compression Type*	If the incoming image compression is different from the specified value, the image will be compressed using the specified value.	G4 PACKBITS DEFLATE NONE	G4	<ul style="list-style-type: none"> • G4 • PACKBITS • DEFLATE • NONE
Front Image Bit Depth*	<p>If the incoming front image bit depth is different from the specified value, the front image bit depth will be converted to the specified value.</p> <p>If the value is 1, ImageType must be TIFF and compression must be G4, DEFLATE, PACKBITS or NONE or you will encounter errors.</p> <p>If the value is 8, ImageType must be TIFF and compression must be DEFLATE, PACKBITS or NONE or you will encounter errors.</p>	1 8	1	<ul style="list-style-type: none"> • 1 • 8
Back Image Bit Depth*	<p>If the incoming back image bit depth is different from the specified value, the back image bit depth will be converted to the specified value.</p> <p>If the value is 1, ImageType must be TIFF and compression must be G4, DEFLATE, PACKBITS or NONE or you will encounter errors.</p> <p>If the value is 8, ImageType must be TIFF and compression must be DEFLATE, PACKBITS or NONE or you will encounter errors.</p>	1 8	1	<ul style="list-style-type: none"> • 1 • 8
Image Cutoff Threshold*	<p>The cutoff threshold for down sampling of 8-bit images to 1-bit images. The value must be between 0 and 0.99. If you specify 0, the image will not be downsampled.</p> <p>It is recommended that you leave the default value of 0.125 for CTS scanners. This value may be changed if a better image quality can be achieved using another value.</p>	a value <i>between</i> 0.0 and 0.99	0.125	

Property	Description	Values, Examples	Default	My Value
RSS ID*	The component ID assigned to this NetCapture Platform installation at the Decision Gateway. In order to facilitate messaging, this ID must match an ESS ID as configured at the Decision Gateway (receive this value from your Decision Gateway administrator).	your component ID	NA	
DG Host Address*	Fully qualified domain name or IP address of the Decision Gateway host to which extract files will be transferred.	your DG address	CONFIGURE_ME	
DG User Name*	User name for FTP as used to transfer extract files to the Decision Gateway.	username	CONFIGURE_ME	
DG Password*	Password for FTP as used to transfer extract files to the Decision Gateway. <i>You must change the default value when you configure the application, or you will receive an error message.</i>	password	CONFIGURE_ME (displayed as asterisks)	
Confirm DG Password*	Re-enter the password you entered in the DG Password field.	password	CONFIGURE_ME (displayed as asterisks)	
DG FTP Directory*	Directory on the Decision Gateway to which extract files will be transferred via FTP.	your FTP directory	CONFIGURE_ME	
DG FTP Protocol*	Specifies the file transfer protocol used to transfer extract files to the Decision Gateway. If you want to use a protocol other than FTP or SFTP, contact your Service Representative for more information.	FTP SFTP Other	FTP	<ul style="list-style-type: none"> • FTP • SFTP • Other_____
Duplicate Check*	Determines whether the Extractor checks for duplicates.	on off	on	<ul style="list-style-type: none"> • On • Off

Property	Description	Values, Examples	Default	My Value
Allow 8 Digit RT*	Indicates whether the Extractor needs to add a check digit to 8-digit route/transit numbers to convert them to 9-digit numbers. If you are using a Decision Gateway prior to version 2.1, set this to true. If you are using Decision Gateway version 2.1 or later, you may set it to false since later versions of the Decision Gateway accept 8-digit route/transit numbers for internal items (credit items, debit adjustments, credit adjustments).	true false	false	<ul style="list-style-type: none"> • True • False

Steps for Configuring Applications

To create a new application configuration, do the following:

1. In System Manager, click the Organization Management link.
2. In the organization tree, select the organization for which you want to configure a new application.
3. Click the Applications tab.
4. Click the Add icon.

The Add Application dialog box appears.

On the Application Configuration tab, complete the fields for this application using the information you gathered using the table in *All NetCapture Platform Applications*.

5. On the More Configuration tab, complete the fields for this application using the information you gathered using the appropriate table for the type of application you are configuring:
 - Capture Gateway: See the table in *Capture Gateway* for information required to configure Capture Gateway.
 - NetCapture Portal: See the table in *Portal and Server-Side Reporting* for information required to configure NetCapture Portal.
 - Extractor: See the table in *Extractor* for information required to configure Extractor.

Note: You must select the application Type on the Application Configuration tab before you can complete the More Configuration tab.

6. Click OK to save the application.

Note: If you added the Server Side Reporting application, you must restart the server that is hosting the application for the changes to take effect.

Additional Steps for Installing Multiple Application Instances

If you are installing multiple instances of any component, you must ensure the application name you assign in System Manager and the application name specified in the web.xml file for the application match. For example, if you are installing two instances of the Extractor, you must do the following:

1. Set up two applications of the same type in System Manager using the steps above.
For example, if you want to set up two Extractors, you might configure two Extractor-type applications in System Manager and name the first instance Extractor1 and the second instance Extractor2.
2. Modify the web.xml file for each application (located on the server where the application is installed, at <app install dir>/WEB-INF/ web.xml) so that the application names match what you configured in System Manager.

For example, for Extractor1, the web.xml file would look like this:

```
<init-param>
  <param-name>AppName</param-name>
  <param-value>Extractor1</param-value>
</init-param>
```

For Extractor2, the web.xml file would look like this:

```
<init-param>
  <param-name>AppName</param-name>
  <param-value>Extractor2</param-value>
</init-param>
```

3. After completing this setup, restart the servers that are hosting the applications.

Creating New Organizations

Use System Manager to complete initial setup of the Service Provider or Bank of First Deposit organization, create Correspondent Bank and Customer organizations that are related to a Bank of First Deposit, and then manage those organizations on an ongoing basis.

Requirements for Creating a New Organization

Before you begin, make sure you have read Understanding the Organizational Hierarchy. Once you understand how the organizational hierarchy works in System Manager, continue with *Steps for Creating a New Organization*.

The first time you log in to System Manager, you will be prompted to create the highest-level organization(s) in the hierarchy, the Service Provider or Bank of First Deposit (BOFD). This should have already been completed by the system administrator who installed the system. You can then create new Correspondent Banks or Customer organizations that belong to the Bank of First Deposit.

Before you begin creating a new Correspondent Bank or Customer organization, do the following:

- Contact your Decision Gateway Administrator to get the Decision Gateway Customer Reference ID and Account Reference ID for the organization you want to add.
- Obtain the organization's address and phone information.
- Obtain address and telephone information for the primary contact at the organization.

- Obtain account information for the organization.
- Obtain the desired operational parameters for customer organizations. In *Steps for Creating a New Organization*, see the first table in Step 6 for more details.

Steps for Creating a New Organization

To create a new organization in System Manager, do the following:

1. In System Manager, click the Organization Management link.
2. In the organization tree, select the appropriate parent organization (Bank of First Deposit or Correspondent Bank) for the new organization you are creating.
3. On the main window beneath the organization tree, click the New Organization button.

The Create Organization dialog box appears.

4. On the General tab, complete the following fields (fields marked with an asterisk [*] are required):

Field	Description
Apply Template	The template you want to apply to this organization, if any. Choosing a template will pre-populate the fields with any information that has been defined as part of the template. You can also choose to leave this blank and manually fill in each required field for the organization.
User Defined Field Group	Select the group you want to apply to this organization, if any. This field only appears if user-defined field groups are defined in the system.
Organization Name*	A descriptive name for the organization. The name can be up to 50 characters. Be sure to use unique names for all the organizations you configure in the system in order to avoid confusion.
Organization Type	This can be Customer or Correspondent Bank.

Field	Description
Parent Organization*	The parent organization is the organization directly above the one you are adding to the hierarchy structure. If you are adding a Correspondent Bank, the parent must be the BOFD. If you are adding a Customer, the parent can be the BOFD or a Correspondent Bank.
Customer Reference ID*	This is the ID you received from your Decision Gateway Administrator that links this customer to the customer set up in the Decision Gateway database. The ID must be a six-digit number, padded with zeroes if necessary (for example, 000050).
Status	This may be active or inactive. Active means the organization is actively using the system to process items. Inactive means the organization is not actively using the system to process items.
Location Name*	A name for this location, for example, Corporate Headquarters. Note: This will be the primary location for this organization. You can add additional locations later.
Country	The country where the organization is located.
Address 1	The street address for the organization.
Address 2	Additional address information for the organization, such as a suite number.
Address 3	Additional address information for the organization.
Address 4	Additional address information for the organization.
City	The city where the organization is located.
State/Province	The state or province where the organization is located.
Zip/Postal Code	The ZIP or postal code for the organization.
Description	An optional description for the organization.

- When you are finished, click the Next button.
The Operational Parameters tab opens.

Create Organization

General | **Operational Parameters** | Account | Contact

ACH Opt Out: ☒ true

Require Control Balance: ☐

Export Data and Images: ☐

Export File Format: ASCII FILE

Use Image Watermark: ☐

Check Duplicates on Server for: days

Image Quality: Front Image

Image Format: Black and White (TIFF)

Image CAR Confidence Threshold *: 0

Enter Payer: ☐

Mask Account Number: ☐ Yes ☐ No ☒ Use Parent Org's Setting

Remove Customer Name: ☐ Yes ☐ No ☒ Use Parent Org's Setting

Remove Report Download: ☐ Yes ☐ No ☒ Use Parent Org's Setting

Required Payment Data Enforcement: ☒ Relaxed Enforcement ☐ Strict Enforcement
(The default value is the same as the selected parent organization. Selecting a different parent organization may change this value.)

Disable Scanner Spray Text: ☐

Custom Data 1:

Custom Data 2:

Custom Data 3:

Disable Virtual Endorsement: ☐

* required

Next >> OK Cancel

6. Complete the fields (fields marked with an asterisk [*] are required).

The options that appear here depend on the type of organization you are creating. The following fields appear for Customer type organizations.

Note: These fields may or may not be applicable depending on whether you are using Desktop Client, Web Client, Receivables Client or Small Business/Consumer Client. The settings for fields labeled not applicable in this table are not used for that type of client.

Field	Used	Not Applicable	Description
ACH Opt Out	<ul style="list-style-type: none"> Desktop Client Web Client Receivables Client 	<ul style="list-style-type: none"> Small Business/Consumer Client DNC 	If this is set to true, users are able to mark items as ineligible for ACH processing in Web Client. If this is set to false, the function is unavailable in the application.
Require Control Balance	<ul style="list-style-type: none"> Desktop Client Web Client Receivables Client Small Business/Consumer Client DNC 		Indicates whether or not the Web Client application will require users to enter a control balance for use in balancing their deposits. If the check box is selected, the control balance is required.
Export Data and Images	<ul style="list-style-type: none"> Desktop Client 	<ul style="list-style-type: none"> Web Client Receivables Client Small Business/Consumer Client DNC 	If the check box is selected, deposit data and check images are exported from the Desktop Client application to a flat file for use in other systems.

Field	Used	Not Applicable	Description
Export File Format	<ul style="list-style-type: none"> Desktop Client 	<ul style="list-style-type: none"> Web Client Receivables Client Small Business/Consumer Client DNC 	If you selected the check box for Export Data and Images, choose the file format for the exported data, either ASCII File (.dat format) or Comma Delimited File (.csv format).
Use Image Watermark	<ul style="list-style-type: none"> Desktop Client 	<ul style="list-style-type: none"> Web Client Receivables Client Small Business/Consumer Client DNC 	<p>If the check box is selected, images included in the export file in Desktop Client applications are watermarked with VOID as a security measure.</p> <p>This option is available only if Export Data and Images is selected.</p>
Check Duplicates on Server for ____ days	<ul style="list-style-type: none"> Desktop Client Web Client Receivables Client Small Business/Consumer Client 	<ul style="list-style-type: none"> DNC 	<p>The number of days of deposits that will be checked for possible duplicate items.</p> <p>The maximum number of days is 180. Keep in mind that large numbers may affect the performance of the system.</p> <p>Not only does this value need to be greater than 0 for duplicate checking to be used, but the Duplicate Checking on Server scrutiny rule also needs to be active for this customer. See <i>Managing Scrutiny Rules</i> for details.</p>
Image Quality	<ul style="list-style-type: none"> Desktop Client Web Client Receivables Client Small Business/Consumer Client DNC 		<p>Select which images will be analyzed for image quality in Web Client:</p> <ul style="list-style-type: none"> None All Front Image Back Image <p>In order for this setting to take effect, you must also configure an IQA Threshold scrutiny rule. Images that do not meet the configured IQA Threshold scrutiny rule(s) will be flagged or rejected. If no scrutiny rules are set, the image quality will not be checked.</p> <p>IMPORTANT! IQA is only used if you configure the organizations Desktop Client applications with a separate CAR/IQA toolkit, or if you install and configure the IQA/CAR server for the organization's Web Client applications.</p>

Field	Used	Not Applicable	Description
Image Format	<ul style="list-style-type: none"> Desktop Client 	<ul style="list-style-type: none"> Web Client Receivables Client Small Business/Consumer Client DNC 	<p>Select the format in which images will be captured at the Desktop Client—Black & White (TIFF) or Gray Scale (JPEG).</p> <p>UEC 7011 scanners can only scan in TIFF format. If JPEG format is selected but a user scans an item with a UEC 7011 scanner, it will generate a TIFF image.</p> <p>Note: You should choose to capture images using the same format that is configured at the Extractor (TIFF) in order to avoid degrading image quality.</p>
Image CAR Confidence Threshold*	<ul style="list-style-type: none"> Desktop Client Web Client Receivables Client Small Business/Consumer Client DNC 		<p>Provide a number from 1-100 to indicate the level at which you will accept the confidence value returned by the CAR (courtesy amount recognition) application in the Web Client. CAR will be applied (in other words, the courtesy amount will be read) for items whose CAR confidence value exceeds the threshold configured here.</p> <p>You can also enter 0 (zero) to turn off CAR functionality. The application will not use CAR to read the courtesy amount.</p> <p>IMPORTANT! CAR is only used if you configure the organization's Desktop Client applications with a separate IQA/CAR toolkit, or if you install and configure the IQA/CAR server for the organization's Web Client applications.</p>
Enter Payer	<ul style="list-style-type: none"> Web Client 	<ul style="list-style-type: none"> Desktop Client Receivables Client Small Business/Consumer Client DNC 	<p>If the check box is selected, the Check Payer name will be captured and displayed during the check capture process.</p>

Field	Used	Not Applicable	Description
Mask Account Number	<ul style="list-style-type: none"> • Desktop Client • Web Client • Receivables Client • Small Business/Consumer Client 	<ul style="list-style-type: none"> • DNC 	<p>If Yes is selected, the account number is masked (for example, xxxx-1234) throughout the application for users who are associated with this organization: the account selection screen, the deposit slip, credit records, and when printed on items.</p> <p>If Use Parent Org's Setting is selected, then the setting for this organization will be the same as the setting for the parent organization.</p>
Remove Customer Name	<ul style="list-style-type: none"> • Web Client • Receivables Client • Small Business/Consumer Client 	<ul style="list-style-type: none"> • Desktop Client • DNC 	<p>If Yes is selected, the customer name does not appear in the account selection, Deposit, and Item Detail screens in the application for users who are associated with this organization.</p> <p>If Use Parent Org's Setting is selected, then the setting for this organization will be the same as the setting for the parent organization.</p>
Remove Report Download	<ul style="list-style-type: none"> • Web Client • Receivables Client 	<ul style="list-style-type: none"> • Desktop Client • Small Business/Consumer Client • DNC 	<p>If Yes is selected, reports cannot be downloaded or exported as .pdf or .csv files by users who are associated with this organization.</p> <p>If Use Parent Org's Setting is selected, then the setting for this organization will be the same as the setting for the parent organization.</p>
Required Payment Data Enforcement	<ul style="list-style-type: none"> • Desktop Client 	<ul style="list-style-type: none"> • Web Client • Receivables Client • Small Business/Consumer Client • DNC 	<p>Choose Relaxed Enforcement to allow users to determine whether or not to enter payment data. Under this model, required Payment Data fields are required only if the user has clicked the Add Row button on the Payment Data spreadsheet.</p> <p>Choose Strict Enforcement to require users to enter at least one row of payment data if there are any required payment data fields for items at Desktop Client.</p> <p>Note: This setting made at a Customer organization level will override the setting at the bank level.</p>

Field	Used	Not Applicable	Description
Disable Spray Scanner Text	<ul style="list-style-type: none"> • Web Client • DNC 	<ul style="list-style-type: none"> • Receivables Client • Small Business/ Consumer Client 	<p>If the Disable Spray Scanner Text is selected, then bank level settings will be ignored and the spray scanner text feature will be disabled for the client. If the bank level is set to Not Configured, then this check box will be disabled.</p> <p>If spray text is not configured or disabled, the user will have the option to configure it in the User Preferences tab.</p>
Disable Virtual Endorsement	<ul style="list-style-type: none"> • Desktop Client • Web Client • Receivables Client • Small Business/ Consumer Client • DNC 		<p>If the Disable Virtual Endorsement check box is selected, then virtual endorsement will be disabled for the customer.</p>
Custom Data Fields 1-3	<ul style="list-style-type: none"> • NA 	<ul style="list-style-type: none"> • NA 	<p>Up to three custom data fields can be added for service organizations to use. Use this field to track any additional data about your customers. Enter up to 100 alpha numeric characters. These three fields are available in the Customer Info Report.</p>

The following fields appear for Correspondent Bank type organizations:

Create Organization

General | Operational Parameters | Contact

Send Reviewer Email ☐

Default Route/Transit

Check Duplicates on Server for days

Mask Account Number ☐ Yes ☐ No ☒ Use Parent Org's Setting

Remove Customer Name ☐ Yes ☐ No ☒ Use Parent Org's Setting

Remove Report Download ☐ Yes ☐ No ☒ Use Parent Org's Setting

Required Payment Data Enforcement ☒ Relaxed Enforcement ☐ Strict Enforcement
(The default value is the same as the selected parent organization. Selecting a different parent organization may change this value.)

Scanner Spray Text

Scanner Spray Custom String

Virtual Endorsement ☒ Business Name

* required

None
Customer Name
Account Name
Both Customer and Account names

Field	Description
Send Reviewer Email	<p>If the check box is selected, the system sends adjustment notification emails to the primary contact for each customer organization when adjustments are created. If the check box is not selected, the system does not send emails.</p> <p>You can set an amount threshold for triggering adjustment email notifications in the Adjustment Processing tab. See <i>Configuring Adjustments</i>.</p>
Default Route/Transit	<p>Provide a route/transit number that will be used to pre-populate the route-transit field when setting up new accounts for this organization.</p> <p>The route/transit number you specify here will be used as the default route/transit number for all accounts created under this organization.</p>
Check Duplicates on Server for ____ days	<p>The number of days of deposits that will be checked for possible duplicate items.</p> <p>The maximum number of days is 180. Keep in mind that large numbers may affect the performance of the system.</p> <p>Not only does this value need to be greater than 0 for duplicate checking to be used, but the Duplicate Checking on Server scrutiny rule also needs to be active for this organization. See <i>Managing Scrutiny Rules</i> for details.</p>
Mask Account Number	<p>If Yes is selected, the account number is masked (for example, xxxx-1234) throughout the Web Client applications: account selection, the deposit slip, credit reports, and when printed on items.</p> <p>Note that this setting made at a Customer organization level will override the setting at the bank level.</p>
Remove Customer Name	<p>If Yes is selected, the customer name does not appear in the account selection screens in Desktop Client or in the Deposit and Item Detail screens in Web Client.</p> <p>Note that this setting made at a Customer organization level will override the setting at the bank level.</p>
Remove Report Download	<p>If Yes is selected, reports cannot be downloaded, exported as PDFs or .csv files.</p> <p>Note that this setting made at a Customer organization level will override the setting at the bank level.</p>
Required Payment Data Enforcement	<p>Choose Relaxed Enforcement to allow users to determine whether or not to enter payment data. Under this model, required Payment Data fields are required only if the user has clicked the Add Row button on the Payment Data spreadsheet.</p> <p>Choose Strict Enforcement to require users to enter at least one row of payment data if there are any required payment data fields for items at the Desktop Client.</p> <p>Note that this setting made at a Customer organization level will override the setting at the bank level.</p>

Field	Description
Scanner Spray Text	<p>If Not Configured is chosen in the drop-down menu, then no scanner spray text will be applied at client locations unless those clients have configured print text in the User Preferences tab of web client.</p> <p>If Standard is chosen in the drop-down menu, the customer name and account number will be printed on the back of the check.</p> <p>If Customized is chosen in the drop-down menu, a custom string of up to 40 characters will be printed on the back of the check.</p> <p>If Mixed is chosen in the drop-down menu, the customer name, account number, and custom string will be printed on the back of the check. The combination of the customer name, account number, and custom string cannot exceed 40 characters.</p> <p>Note that Digital Check scanners are unable to print the percentage (%) or ampersand (&) symbols correctly on the back of items. You should avoid using these two symbols in the data to be printed.</p>
Virtual Endorsement	<p>If this setting is enabled, then an endorsement will appear on the Payee endorsement area on the back of the check. Virtual endorsement is only applied on the server side and will only be visible on images in server side reporting.</p> <p>No single line of text can exceed 36 characters. If more than 36 characters are included in the data to be used in the virtual endorsement, it will be truncated after the 36 character.</p> <p>To enable virtual endorsement, select the Virtual Endorsement check box and the following options will be available in the Business Name drop-down menu:</p> <p>If None is chosen in the drop-down menu, then neither the customer nor account name will be configured in the endorsement. The endorsement will look like this:</p> <p style="text-align: center;">American National Bank 012345678 For Deposit Only Account: 12345678901234567890</p> <p>If Customer Name is chosen in the drop-down menu, then the customer name will appear in line 3 of the endorsement. The endorsement will look like this:</p> <p style="text-align: center;">American National Bank 012345678 For Deposit Only Peterson Coffee and Tea Account: 12345678901234567890</p> <p>If Account Name is chosen in the drop-down menu, then the account name will appear in line 4 of the endorsement. The endorsement will look like this:</p> <p style="text-align: center;">American National Bank 012345678 For Deposit Only Account: 12345678901234567890 SF Downtown - Operational account</p> <p>If Both Customer and Account names is chosen in the drop-down menu, then the customer name will appear in line 3 and the account name will appear in line 5 of the endorsement. The endorsement will look like this:</p>

Field	Description
	<p>American National Bank 0123456789</p> <p>For Deposit Only</p> <p>Peterson Coffee and Tea</p> <p>Account: 12345678901234567890</p> <p>SF Downtown - Operational account</p> <p>Note that if there is already an endorsement or other text on the back of the check, then virtual endorsement will be applied over the top of it.</p>

7. Click Next.

The Account tab opens if you are creating a Customer type organization.

Create Organization

General | Operational Parameters | **Account** | Contact

Account Number * []

Account Name []

Route/Transit Number * []
(The default route/transit number is the same as the selected parent organization's route/transit number. Selecting a different parent organization may change this value.)

Aux On-Us []

Account Reference ID * []

Status: Active ▼

Deposit Slip: Optional ▼

New Account: ☒ (When checked, if the New Account scrutiny rule is enabled, all deposits will be reviewed for this account.)

Clear New Account Flag * 10 days after first deposit (0 means it will never expire)

* required

Next >> OK Cancel

The Account tab lets you save information about a depository account for the organization. You can add more accounts for the organization later.

8. Complete the following information (fields marked with an asterisk [*] are required):

Field	Description
Account Number*	The account number for the organization's account to which deposits can be made.
Account Name	A name to help you and users of the Web Client identify this account.
Route/Transit Number*	The route/transit number for the account you are adding.
Route/Transit Number Verified*	<p>This field appears only if you have entered an invalid route/transit number. Select the check box if you want to accept the route/transit number and use it for the account even though it has failed validation.</p> <p>If you do not want to accept the invalid route/transit number, re-enter a valid route/transit in the Route/ Transit Number field.</p>

Field	Description
Aux On-Us	<p>This aux on-us value is inserted into the aux on-us field of the automatically generated credit item when a deposit is completed without a deposit slip.</p> <p>When a deposit slip is used, users see this value in a message box.</p>
Account Reference ID*	<p>This is the ID you received from your Decision Gateway Administrator that links this account to the account set up in the Decision Gateway database. This ID may be up to 20 alphanumeric characters.</p>
Status	<p>This may be active or inactive. Active means the account is actively being used in the system. Inactive means the account is not actively being used in the system.</p> <p>The default is active.</p>
Deposit Slip	<p>This determines how the Web Client will handle deposit slips for this account. Required means a deposit slip is required to be submitted for each deposit. Not Used means deposit slips cannot be submitted. Optional means users can choose whether or not to use a deposit slip for each deposit they submit.</p> <p>The default is Optional.</p> <p>The deposit slips users submit with deposits must match the account number specified for this account.</p> <p>If you choose to use deposit slips, you may also want to set a scrutiny rule to flag deposits in which users have changed an item's type (from deposit slip to debit item, or vice versa). See <i>Managing Scrutiny Rules</i> for more information.</p>
New Account	<p>Indicates that this is a new account, and that Deposit Review Agents are required to review all deposits made to this account in Deposit Review. If the check box is selected, all deposits for this account will be flagged for review.</p> <p>This check box is selected by default.</p> <p>To use this option, the account must have the Is New Account scrutiny rule configured. See <i>Managing Scrutiny Rules</i> for details.</p>
Clear New Account Flag	<p>The number of days the New Account flag will remain active on a depository account. This can be 0-999 days. If it's set to zero (0), the New Account flag will never be cleared.</p> <p>The time period calculation will begin at the time the first deposit is made. For instance, if the New Account check box is selected, the inactivation date is set to 10, and the user begins making deposits at 1 p.m. on the 1st of the month, then the New Account flag will be cleared on the 10th at 1 p.m. MT.</p> <p>Note: The inactivation time will always be displayed in Mountain Time.</p>

9. Click Next.

The Contact tab opens.

The Contact tab lets you save information about the primary contact person for the organization. You can add additional contacts later.

10. Complete the contact information fields (fields marked with an asterisk [*] are required):

Field	Description
First Name*	The contact person's first name.
Last Name*	The contact person's last name.
Contact Type*	Indicate the type of contact.
Email Address	<p>The email address at which this contact person can be reached. For customer and bank type organizations, this is also the email address from which adjustment notifications will be sent.</p> <p>You can enter multiple email addresses for the contact by separating them with semicolons. For example: john@example.com;john@bankabc.com.</p>
Deposit Review Notifications	Select this box if you want this contact to receive notification of item adjustments and rejections by email. The check box is selected by default for the primary contact.
Account Level Only	Select this box if you want contacts that are set up at the depository account level to receive notifications only for deposits made to that account.
Deposit Confirmation Notifications	Select the check box if you want the contact to receive email notifications confirming that deposits have successfully been submitted. Note that if you check this box, this individual will receive an email message for every deposit submitted on behalf of this customer organization.

Field	Description
Use organization address [Copy]	Click the copy button if you want to copy the address you specified on the general tab for the organization to be used as the address for this contact.
Country	The country in which the contact is located.
Address Line 1	The street address at which this contact person may be reached.
Address Line 2	Additional address information at which this contact person may be reached, such as a suite number.
Address Line 3	Additional address information for this contact person.
Address Line 4	Additional address information for this contact person.
City	The city in which the contact is located.
State/Province	The state or province in which the contact is located.
Zip/Postal Code	The ZIP or postal code for the contact.
Phone	The phone number at which the contact can be reached, including an extension. Enter only numeric characters. For customer and bank type organizations, this is the contact phone number that will be included in adjustment notifications.
Fax	The fax number at which the contact can be reached, including an extension. Enter only numeric characters.

When the required fields in all the tabs are populated, the OK button becomes active.

11. Click OK to save the new organization information.
12. Repeat this procedure to create more organizations.

To add users to the organization, continue with the section see *Creating Users*. To edit organizational information, see *Editing Organization General Information*.

Editing Organization General Information

System Manager lets you edit the information related to organizations previously created in the system. You cannot delete organizations.

Requirements for Editing General Information for an Organization

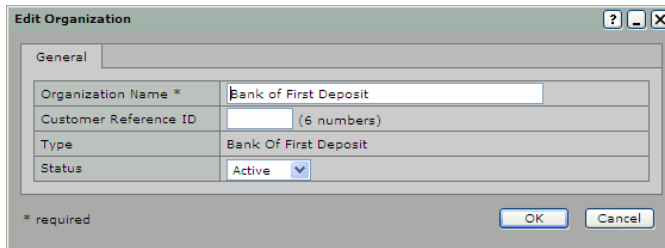
You can edit an existing Correspondent Bank or Customer organization. However, you cannot change the hierarchy of existing organizations. The organizations you are allowed to edit depend on your role in the system. See *Understanding User Roles and Privileges* for details.

Steps for Editing General Information for an Organization

To edit general information for an organization, do the following:

1. In System Manager, click the Organization Management link.
2. In the organization tree, select the organization you want to edit.
3. Click the General tab.
4. Click the Edit icon for the organization.

The Edit Organization dialog box appears.



5. Modify the desired fields according to the information from the table in Step 4 of *Steps for Creating a New Organization*.

You cannot change the organization type.

6. Click OK to save the information.

Editing Organization Operational Parameters

You can edit an existing Bank of First Deposit, Correspondent Bank, or Customer organization's operational parameters.

Requirements for Editing Operational Parameters for an Organization

The organizations you are allowed to edit depend on your role in the system. See *Understanding User Roles and Privileges* for details.

Steps for Editing Operational Parameters for an Organization

To edit operational parameters for an organization, do the following:

1. In System Manager, click the Organization Management link.
2. In the organization tree, select the organization you want to edit.
3. Click the Operational Parameters tab.
4. Click the Edit icon.

The Edit Operational Parameters dialog box appears.

- a. If you are editing the information for a customer organization, modify the desired fields according to the information from the first table in Step 6 in *Steps for Creating a New Organization*.

Note: The options that appear depend on what is configured for the parent organization.

- b. If you are editing the information for a correspondent bank or Bank of First Deposit, modify the desired fields according to the information from the second table in Step 6 in *Steps for Creating a New Organization*.

There are two additional fields if you are editing the Bank of First Deposit. For information about how to configure those two fields, see *Configuring the Client System Message*.

5. Click OK to save the information.

Configuring the Client System Message

You can configure a message that will appear to Desktop Client, Web Client and Small Business/Consumer Client users after they log into the application. You can use this message to inform users of scheduled downtime or to present marketing information. You can also configure how often this message will appear to users.

In addition to the configured display frequency, this message will also be displayed to users if at any time they are unable to connect to the Capture Gateway. As such, you may also want to use it to provide support contact information or a link to your organization's support web site.

Requirements for Configuring the Client System Message

This message can only be configured for the Bank of First Deposit. As such, all organizations under the Bank of First Deposit in the hierarchy will receive the same message.

Steps for Configuring the Client System Message

Do the following to configure the client system message:

1. In System Manager, click the Organization Management link.
2. In the organization tree, select the Bank of First Deposit.
3. Click the Operational Parameters tab.
4. Click the Edit icon.

The Edit Operational Parameters dialog box appears.

5. Complete the first two fields (fields marked with an asterisk [*] are required):

Field	Description
Client System Message	<p>This text will appear as a message displayed to users when they log in to Web Client, Desktop Client, Small Business/Consumer Client, or DNC.</p> <p>You can enter up to 500 alphanumeric characters, including spaces. You can also use hard returns to insert blank lines between paragraphs.</p> <p>You can enter a single URL starting with http:// or https://. The URL will be displayed as a hyperlink that users can click on to launch a browser and visit the URL.</p>

Field	Description
Client Message Display	<p>This setting determines when the message will be displayed to users.</p> <ul style="list-style-type: none"> • Select Always if you want the message to appear every time a user logs in. • Select Once if you want the message to appear the first time a user logs in and, subsequently, the first time a user logs in after the message is changed. • Select Offline if you want the message to appear only when users are unable to connect to the Capture Gateway.

6. Click OK to save the message.

Creating Users

After creating an organization, you must add users to the organization. When you create users, you create all pertinent information such as user names and passwords so the users can be authenticated in the system.

When you add new users, you also set the user's home organization. The home organization is the organization that you select in the organization tree when you choose to add a new user. The home organization determines how certain settings like branding and license messaging appear to users.

When you create a user, you must also assign roles to the user so the user can access system applications and perform the appropriate tasks.

Requirements for Creating Users

An organization must be created before users can be added to that organization. Depending on your privileges, you may or may not be able to add users. The types of users you are allowed to add and the roles you are allowed to assign to those users depend on your privileges in the system.

Before you begin, gather the user's name and desired user name and password information.

Before you begin assigning user roles, you should understand which privileges are granted for each role. Be sure to assign the appropriate roles to individuals in your organization so that they will have the minimum level of access required to complete their tasks. You also have the option of creating customized roles that contain the privileges you want your users to have. See *Understanding User Roles and Privileges* for a detailed discussion of roles and privileges before you begin assigning user roles, and *Creating Custom Roles* details about creating custom roles. When assigning roles, be careful to assign the appropriate roles to the appropriate people to ensure you do not inadvertently grant access to areas to which users should not have access.

Role assignment is subject to the following restrictions:

- You must have the Create User or Update User privilege in order to make role assignments.
- You can only assign roles to or remove roles from other users that you yourself have and that are marked as assign. For example, to assign the Remote User role to another user, you must have the Create User or Update User privilege, you must hold the Remote User role, and that role must be marked as assign. The same conditions must be met in order for you to remove this role assignment from another user.
- You can only assign roles that contain privileges that are available for the selected organization. For example, if you have selected a Correspondent Bank organization, any roles that contain privileges that are not allowed to be assigned for Correspondent Banks will NOT appear in the list as available for assignment.
- You can assign roles that contain the Create Deposit and Review Remote Deposit privileges at either the organization level or the account level. You may want to do this if you want a Web Client

user to have access to a sub-set of accounts for an organization. If you assign the role at the organization level, the user will have access to make deposits to all of that organization's accounts; if you assign the role at the account level, the user will have access to make deposits only to the assigned accounts.

- Role assignments at the organization level take precedence over role assignments at the account level. In order for account-level privileges to be effective, you should ensure that the role is assigned to a user only at the account level, and is NOT assigned for an organization to which the account belongs. For example, if Customer 1 has Account A and Account B, and the Remote User role is assigned to a user for Customer 1, then the user has access to submit deposits to both Account A and Account B. If you want to restrict the user's access to Account A, you must remove the role assignment for Customer 1 and then assign the role to the user for only Account A.

Important Note about Account-Level Assignments and Custom Roles: Be mindful when creating custom roles that combine the Create Deposit and Review/Approve Deposit privileges with other privileges. If either of these two privileges is present in a role, the role can be assigned at the account level—however, the account-level restriction will only apply for these two privileges, it will not apply for the other privileges associated with the role. In addition, any other privileges included in this role are ignored (for example, the user will not have access to those functions) unless the role is also assigned for an organization. For example:

- If you create a custom role that contains the Create Deposit privilege and the Execute Reports privilege and assign the role to a user at the account level, the user will have access to submit deposits for the assigned accounts. However, the user will not have access to server reports in Desktop Client because the role has not been assigned at the organization level.
- If you create a custom role that contains the Review/Approve Deposit privilege and the Execute Deposit Review privilege, and assign the role to a user at the account level, the user will have access to review and approve deposits in Distributed Print Server User Guide Client for the assigned accounts. However, the user will not have access to review deposits in Deposit Review because the role has not been assigned at the organization level.

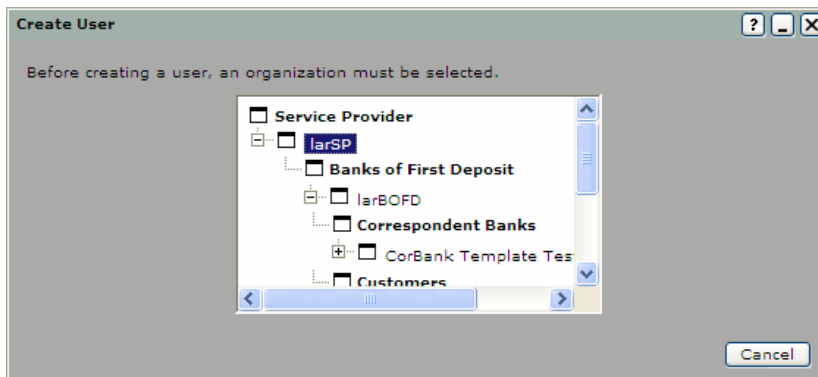
For more information about the specific levels of access granted with each privilege, see *Privileges and User Interface Access Matrix*.

Steps for Creating Users

To add a user to an organization, do the following:

1. In System Manager, click the Organization Management link.
2. Click the Users tab.
3. Click the New User button.

An organization selection dialog box appears.



4. Select the organization to which you want to add a user, then click OK.

The Add User dialog box appears.

Add User

User Roles

User Name *
First Name *
Last Name *
Password *
Confirm Password *
Status Active Status
Deposit Amount Limit * \$ 99999999.99
(Do not use a comma or any other special Character. Only two decimal places are allowed (e.g. 10000.25). If this limit is set and "Deposit Amount" rule is enabled, all deposits will be subject to this limit.)
User Level Aux On-Us
Email Address (required for mobile customers)
Phone Number (required for mobile customers)
Phone Type iPhone (required for mobile customers)
Language English (required for mobile customers)
Assign Security Profile profile1

* required

Apply Reset OK Cancel

5. Enter the following information in the fields (fields marked with an asterisk [*] are required):

Field	Description
User Name*	The name the user will use to log in to the system applications. The user name maximum length is 100 characters, cannot contain spaces, and can contain letters, numbers, and special characters. Note: User names are not case sensitive in the database, but they are case sensitive in the UI. For example, the database recognizes Jsmith and jsmith as the same user name. However, if the user name Jsmith was set up, then the user must enter Jsmith. If the user types in jsmith, the UI will give them an error.
First Name*	The user's first name.
Last Name*	The user's last name.
Password*	Provide a password for the user that complies with your organization's password requirements.
Confirm Password*	Re-enter the user's password a second time, for verification. The system validates that the password is not on the disallowed password list, and that it conforms to formatting requirements. The user's password expiration date is set to the current date and time. (The system will force the user to reset the password after the new user logs in for the first time.)
IMPORTANT! You are responsible for providing the user with the user name and password you supply here. The password is not stored in a visible format after you enter it. You should keep track of it elsewhere, or provide it to the user immediately upon setup. Otherwise, a Help Desk Technician will have to reset the user's password before the user will be able to log in.	
Status	<ul style="list-style-type: none"> Active Status (Default): The user is able to use the system applications to process items in the system. Inactive Status: The user is not currently active and is unable to log in to the system applications. This can be manually set or automatically set because the user unsuccessfully tried to authenticate to a system application multiple times.

Field	Description
Deposit Amount Limit*	<p>The maximum amount of a single deposit that this user is allowed to submit in Desktop Client. This field only applies to users with the Create Deposit privilege. The deposit limit maximum amount is \$99,999,999.99.</p> <p>Deposits that exceed this amount will require review by a user with the Review Remote Deposit privilege.</p> <p>Note: This limit does NOT determine which deposits users with the Review Remote Deposit privilege can review. Users with this privilege can review and approve deposits of any amount.</p> <p>IMPORTANT! To use this option, the organization must have the Dual Control Deposit Amount scrutiny rule configured. See <i>Managing Scrutiny Rules</i> for details.</p>
User Level Aux On-Us	<p>A unique aux on-us for a user that can be applied to the credit and adjustment records for items deposited by that user. The user level aux on-us can contain up to 15 numeric characters.</p> <p>Note: The user level aux on-us may also be referred to as the unique reference ID in some implementations.</p> <p>This field will only be present if the Use user level aux on-us check box is selected in the Adjustment Processing tab for the customer. If a value is present in the field, it will be used in place of the account-level aux on-us for credit and adjustment records. If the field is empty, then the aux on-us specified for the account will be used.</p> <p>Note: This field will only be displayed if a parent organization is configured for User Level Aux On-Us. See <i>Configuring Adjustments</i> for details.</p>
Email Address	The user's email address. An email address is required for mobile users.
Phone Number	<p>The mobile user's phone number. The phone number cannot contain dashes -, parenthesis (), or plus + characters.</p> <p>Note: To use this option, the organization must have mobile RDC configured.</p>
Phone Type	<p>The type of phone used.</p> <ul style="list-style-type: none"> • iPhone • Android <p>Note: To use this option, the organization must have mobile RDC configured.</p>
Language	<ul style="list-style-type: none"> • English • Spanish • Chinese <p>Note: To use this option, the organization must have mobile RDC configured.</p>
Assign Security Profile	<p>Select the security profile to assign to this user. The security profile dictates when and how the user can access applications. By default, the parent organization's security profile is selected.</p> <p>For more information, see <i>Configuring Security Profiles</i>.</p>

6. Click the Roles tab.

7. Make the appropriate selections to assign a role to the user (fields marked with an asterisk [*] are required).

Note: If you do not have the Create User or Update User privilege, the fields on this screen are not editable.

Field	Description
Organization*	<p>Select the organization for which you want to assign the user a particular role.</p> <p>If you want to change the organization that is selected, click the Edit icon. A dialog box with the organization tree appears. Click the organization for which you want to make the role assignment.</p>
Role*	<p>Select the role you want to assign to the user for the selected organization.</p> <p>Only the roles you have privileges to assign for the selected organization appear in the list. If you have roles assigned to you that are not associated with an organization (this may happen if you create custom roles), then those roles appear in the list for all organizations.</p>
Account	<p>If you want Web Client users to be able to submit or approve deposits only for specific accounts, and not for all the accounts configured for an organization, select the desired account.</p> <p>This drop-down box only becomes active if you have selected a Customer-type organization and a role that contains the Create Deposit or Review Remote Deposit privilege.</p> <p>Note: The Execute, Assign and Inherit check boxes do not apply to role assignments at the account level.</p>
Execute	<p>If you want this user to be able to execute this role, select the Execute check box.</p> <p>This option is not available for account-level assignments.</p>
Assign	<p>If you want this user to be able to assign this role to other users, select the Assign check box.</p> <p>This option is not available for account-level assignments.</p>
Inherit	<p>If you want this user to have this role for all child organizations below the selected organization in the hierarchy, Inherit check box.</p> <p>This option is not available for account-level assignments.</p>

- Click the Add icon to add this role assignment for the user.

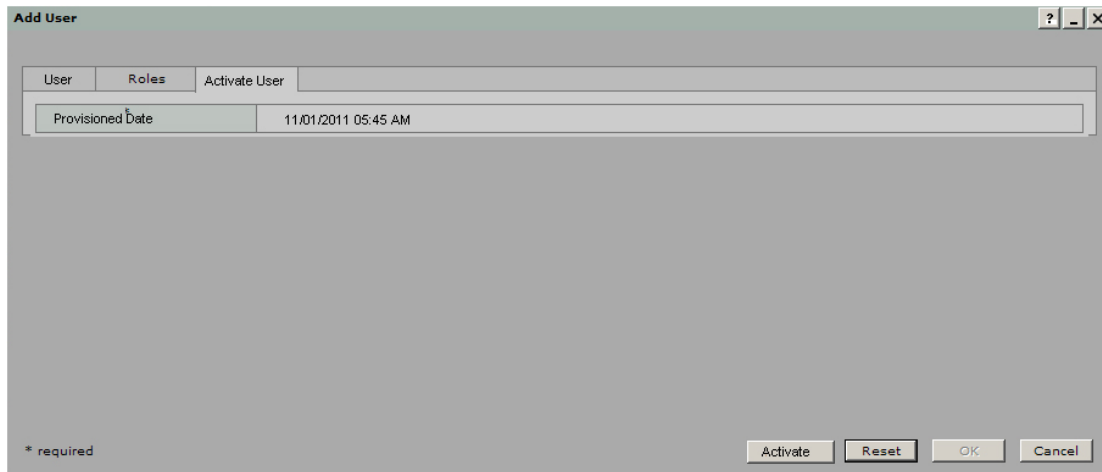
The assignment appears in the table below the drop-down boxes.

- If desired, repeat Steps 7 and 8 to add more roles to the user.

- Click OK to save the user.

- Click the Activate User tab if you are activating a new mobile RDC user.

Note: You can only see the Activate User tab if your service organization has been configured for mobile RDC.



Field	Description
Provisioned Date	The date and time the mobile user was activated.

- Click Activate to activate the new mobile user.

The newly created user's information is displayed in the user list for the organization.

- Repeat this procedure if you need to create more users.

Searching for a User

There are two methods you can use to search for a user in the system:

- Searching for a User on the Users Tab
- Browsing Through Users for an Organization

Searching for a User on the Users Tab


Do the following to search for a user on the Users tab in the left pane of System Manager:

- In System Manager, click the Organization Management link.
- On the Users tab, search for the user to whom you want to assign a new role or remove a role.

The search results appear in the right pane.

Search Results

<input type="checkbox"/>	User Name	Name	Status	Organization
<input type="checkbox"/>	admin	System Admin	Active Status	BofD
<input type="checkbox"/>	jasonanderson@abccomp...	Jason Anderson	Active Status	ABC Company
<input type="checkbox"/>	john.doe@abccompany.c...	john doe	Active Status	ABC Company
<input type="checkbox"/>	johnsmith	john smith	Active Status	ABC Company
<input type="checkbox"/>	vlademirkumar@abccomp...	Vladimir Kumar	Active Status	ABC Company



Assign Multiple Roles for Single Organization

- Click the check box for the user(s) you want to edit. To select all the users in the search results, click the check box at the top of the column.

You can change role assignments for multiple users by selecting them in this list and then clicking the Assign Multiple Roles for Single Organization icon. See *Assigning Roles to Multiple Users*.

Browsing Through Users for an Organization

Do the following to browse through the users for an organization to locate the user whose settings you want to edit:

- In System Manager, click the Organization Management link.
- In the organization tree, select the organization to which the user belongs.
- Click the Users tab.







A list of users that have roles for this organization or any of its accounts appears.

ABC Company

General	Branding	Operational Parameters	User Defined Fields	Locations & Contacts	Accounts	Rules	Users	Security	Adjustment Processing
---------	----------	------------------------	---------------------	----------------------	----------	-------	-------	----------	-----------------------

View all Users assigned to this organization

All Users with roles for this organization or its accounts

	User Name	Name	Status	Security Profile	Deposit Amount Limit	Roles
	admin	System Admin	Active	profile1	\$99,999,999.99	Show Roles
	jasonanderson@abccomp...	Jason Anderson	Active	profile1	\$99,999,999.99	Show Roles
	john.doe@abccompany.c...	john doe	Active	profile1	\$99,999,999.99	Show Roles
	johnsmith	john smith	Active	profile1	\$99,999,999.99	Show Roles
	remoteuser	remote user	Active	profile1	\$99,999,999.99	Show Roles
	vlademirkumar@abccomp...	Vladimir Kumar	Active	profile1	\$99,999,999.99	Show Roles

Results: 1 - 6 of 6

Records Per Page * 10

Update

You can view the roles assigned to a particular user by clicking Show Roles. This allows you to see which roles the user has for which organizations, and whether they are assignable or inheritable.

You can also view the users for whom this is the home organization (the organization under which they were created) by clicking the View All Users assigned to this organization button. The view changes to display all users for whom this is the home organization, and the button changes to read View all Users with roles for this organization or its accounts. You can click the button to return to the original view.

Note: If the number of users for the organization exceeds the number specified in the Records Per Page field, you will need to increase the number in that field or browse to the remaining results using the arrow buttons in order to see all the users for the organization.

Editing User Settings

You can edit a user's settings to accomplish any of the following:

- Changing a User's Password
- Changing a User's Deposit Limit
- Changing a User's Status
- Assigning a New Security Profile to a User
- Changing a User's Role Assignments

To edit a user's settings, do the following:

1. In System Manager, click the Organization Management link.
2. Search for the user whose settings you want to edit.

For information about how to locate a user, see *Searching for a User*.

3. Depending on how you completed the search, click the user name or the Edit icon for the user you want to edit.

The Edit User dialog box appears.

Edit User

User Login Roles

User Name * mccuser1

First Name *

Last Name *

Password *

Confirm Password *

Status Active Status

Deposit Amount Limit * \$ 99999999.99
(Do not use a comma or any other special Character. Only two decimal places are allowed (e.g. 10000.25). If this limit is set and "Deposit Amount" rule is enabled, all deposits will be subject to this limit.)

User Level Aux On-Us

Email Address (required for mobile customers)

Phone Number (required for mobile customers)

Phone Type iPhone (required for mobile customers)

Language English (required for mobile customers)

Assign Security Profile profile1

* required

Apply Reset OK Cancel

4. Complete one of the following procedures to edit the user's settings:
 - Changing a User's Password
 - Changing a User's Deposit Limit
 - Changing a User's Status
 - Assigning a New Security Profile to a User
 - Changing a User's Role Assignments

Changing a User's Password

To change the user's password, do the following:

1. On the User tab, enter the desired new password for the user in the Password and Confirm Password fields. The passwords must match.
2. Click OK.

The user's password is updated. The user will be required to provide the new password the next time they log in.

Changing a User's Deposit Limit

To change the user's deposit limit, do the following:

1. On the User tab, enter the desired new deposit amount limit for the user in the Deposit Amount Limit field. The deposit amount cannot exceed \$99,999,999.99
2. Click OK.

The user's deposit limit is updated. The change will take effect the next time the user logs in.

Changing a User's Status

If you do not want a user to have access to the system, you can either set the user to inactive or delete the user. You should set the user inactive when you want to temporarily revoke access. You should delete the user when you want to permanently remove the user from the system.

When you delete a user account, the user is no longer able to log in to the system. A user account cannot be re-set to active or any other status after it has been deleted. The deleted user account information is not included in any reports.

You can also configure the system to automatically delete inactive user accounts. In *Steps for Configuring Security Profiles*, see the table in Step 3 for more information.

To change the user's status, do the following:

1. On the User tab, select the desired status in the Status drop-down box.
 - Select Inactive Status to temporarily revoke system access for the user.
 - Select Deleted Status to remove the user from the system.
2. Click OK.

The user's status is updated. The change will take effect the next time the user logs in.

Assigning a New Security Profile to a User

By default, users are assigned the security profile that is associated with the organization under which they are created. However, you can change the security profile that is assigned to a user at any time. The profile assigned at the user level will override the profile assigned at the organization level.

To change the security profile assigned to the user, do the following:

1. On the User tab, choose a profile in the Assign Security Profile drop-down box.
2. Click OK.

The new profile will apply to the user the next time the user logs in to the system.

Changing a User's Role Assignments

When you create a user, you assign roles to the user so the user can access the applications and perform the appropriate tasks. You may need to add or remove roles for users after the users have been created. Users can have multiple role assignments granting them access to various areas of the system for different organizations.

- Editing a Role Assignment
- Deleting a Role Assignment

Editing a Role Assignment

To modify the existing role assignments for a user, do the following:

1. On the Roles tab, click the Edit icon next to the role assignment.
2. Modify the role assignment(s) as desired. You can change the organization association, the role, the account association, and whether the role(s) are executable, assignable or inheritable.

In *Steps for Creating Users*, see the table in Step 7 for detailed information about each option.

3. When you have finished making updates, click OK to save your changes and exit.

Note: If you want to make further changes, you can click Apply and the Edit User dialog box will remain open. If you decide you do not want to save your changes, click Reset. The settings will revert back to what they were before you started making changes (when you opened the Edit User dialog box, or the last time you clicked Apply).

Deleting a Role Assignment

To delete a role assignment, do the following:

1. On the Roles tab, select the Delete check box next to the role you want to delete in the role assignment table.

To delete multiple role assignments, check multiple boxes. You can use the Select All button to select all role assignments in the table.

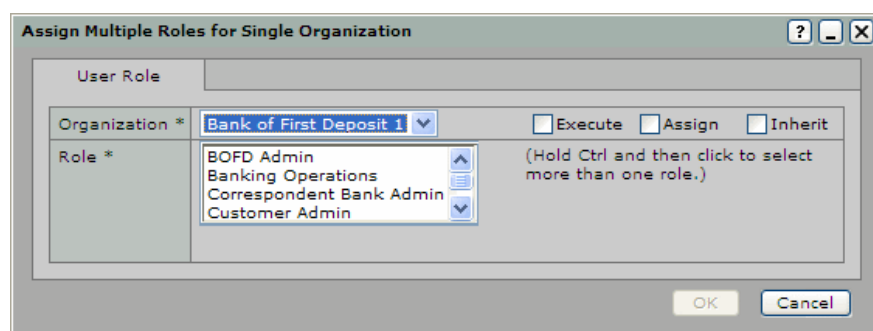
2. Click Apply.

The role assignment(s) are removed from the table.

Assigning Roles to Multiple Users

You can make role assignment(s) for multiple users at one time. Do the following:

1. Using the steps in *Searching for a User on the Users Tab*, select the check boxes for the users to whom you want to assign roles.
2. Click the Assign Multiple Roles for Single Organization icon.



3. In the Organization drop-down box, select the organization for which you want to assign the role(s).
4. In the Role list, select the role(s) you want to assign to the user(s). To select multiple roles, hold down the Ctrl key.
5. If you want this user to be able to execute this role, select the Execute check box.
6. If you want this user to be able to assign this role to other users, select the Assign check box.
7. If you want this user to have this role for all child organizations below the selected organization in the hierarchy, select the Inherit check box.
8. Click OK to save your changes.

Creating Custom Roles

If you want to create new roles that have specific sets of privileges, you can create custom roles. You should create custom roles if the default roles provided in the system do not meet the needs of your organization.

Requirements for Creating Custom Roles

Before you start creating or modifying roles, you should understand which privileges provide access to which areas of the system. See *Privileges and User Interface Access Matrix* for more information. Some privileges can only be assigned for certain organization levels, so be sure that the combination of privileges you assign to a role make sense for the users and organizations for which you intend to use the role.

In order to complete most activities in the system, a role must have the execute type privilege in addition to either the create, update, or delete type privilege. The execute privilege is what allows the user to access the specified area of the user interface. The create, update, and delete privileges are what allow the user to complete actions in System Manager.

When you create a new role, it is automatically assigned to you and marked as assign and inherit. This allows you to assign the role to other users. However, the role is not associated with an organization. This means you cannot actually use the role to complete any actions in the system. If you want to be able to use the role yourself, you must have another user re-assign it to you so it is associated with an organization. See *Changing a User's Role Assignments* for more information.

Important Note about Account-Level Assignments and Custom Roles: Be mindful when creating custom roles that combine the Create Deposit and Review/Approve Deposit privileges with other privileges. If either of these two privileges is present in a role, the role can be assigned at the account level—however, the account-level restriction will only apply for these two privileges, it will not apply for the other privileges associated with the role. In addition, any other privileges included in this role are ignored (for example, the user will not have access to those functions) unless the role is also assigned for an organization. For example:

- If you create a custom role that contains the Create Deposit privilege and the Execute Reports privilege and assign the role to a user at the account level, the user will have access to submit deposits for the assigned accounts. However, the user will not have access to server reports in Desktop Client because the role has not been assigned at the organization level.
- If you create a custom role that contains the Review/Approve Deposit privilege and the Execute Deposit Review privilege, and assign the role to a user at the account level, the user will have access to review and approve deposits in Distributed Print Server User Guide Client for the assigned accounts. However, the user will not have access to review deposits in Deposit Review because the role has not been assigned at the organization level.

For more information about the specific levels of access granted with each privilege, see *Privileges and User Interface Access Matrix*.

Steps for Creating a New Role

To create a new role, do the following:

1. In System Manager, click the Custom Roles link.
2. Click the Add icon.

The Add Role dialog box appears.

3. In the Role Name field, enter a name for the role.
This cannot exceed 100 alphanumeric characters. You must enter a unique name for the role. If you enter a name that is the same as a name used for an existing role, an error appears when you try to save the new role.
4. Select the default value for the execute check box for the new role.
5. In the Available Privileges list, select the privilege(s) you want to assign to the user. To select multiple privileges, hold down the Ctrl key while clicking on privileges. To select all privileges, click the Select all in list check box.
6. Click the arrow [>] button to move the privilege to the Current Privileges list.
You can also remove privileges from the Current Privileges list by selecting the privilege and clicking the arrow [<] button to move it back to the Available Privileges list.
7. Click OK to save the role.

Steps for Modifying an Existing Role

You can edit the privileges assigned to an existing role. To locate and edit an existing role, do the following:

1. In the Custom Roles area, click the Edit icon for the role you want to modify.
2. Edit the data for the role and change the privilege assignments using the instructions in *Steps for Creating a New Role*.

If you change the name of an existing role, the previous role name is replaced with the new name. For example, if you create a role named Test Role and then edit the role and change the name to Test Role 2, Test Role no longer exists in the system—it is replaced by Test Role 2.

3. Click OK to save your changes.

Steps for Deleting a Role

You can delete roles that are not currently assigned to any users in the system, or that are only assigned to users without an organization association (this may happen in the case where a new custom role is assigned to the person who created it, or when certain roles are automatically assigned to users after upgrade).

To delete a role, go to the Custom Roles area and click the Delete icon for the role you want to delete.

If a role is assigned to a user, you will receive an error message and will not be allowed to delete the role.

Configuring Adjustments

The Adjustment Processing tab lets you configure default and alternate settings for credit and debit adjustments, adjustment email notification settings, and credit record and deposit slip settings.

The settings you configure here are automatically inherited by any new child organizations that are created under this organization. However, if you change this configuration for a parent organization, existing child organizations are not automatically updated. If you want to change these settings for existing child organizations, you must manually edit them. This does not apply to dynamic image data. See *Edit Adjustments General Configuration* and *Edit Credit Record Configuration*.

Bobs Printing

General Branding Operational Parameters User Defined Fields Locations & Contacts Accounts Rules Users Security Adjustment Processing

General

Deposit Channel: RDC
RDC
Mobile RDC

☐ Use this configuration

☐ Only send email notification for adjustment over: \$0.00

☐ Use user level aux on-us

Debit Adjustment

Default Configuration	Alternate Configuration <input type="checkbox"/> Use this if adjustment amount is less than: \$0.00
Route/Transit: <input checked="" type="radio"/> From Credit Record <input type="radio"/> Custom:	Route/Transit: <input checked="" type="radio"/> From Credit Record <input type="radio"/> Custom:
Account: <input checked="" type="radio"/> From Credit Record <input type="radio"/> Custom:	Account: <input checked="" type="radio"/> From Credit Record <input type="radio"/> Custom:
<input type="checkbox"/> Append Tran Code starts at 13	<input type="checkbox"/> Append Tran Code starts at 13
Aux On-Us: <input checked="" type="radio"/> From Credit Record <input type="radio"/> Custom:	Aux On-Us: <input checked="" type="radio"/> From Credit Record <input type="radio"/> Custom:

Credit Adjustment

Default Configuration	Alternate Configuration <input type="checkbox"/> Use this if adjustment amount is less than: \$0.00
Route/Transit: <input checked="" type="radio"/> From Credit Record <input type="radio"/> Custom:	Route/Transit: <input checked="" type="radio"/> From Credit Record <input type="radio"/> Custom:
Account: <input checked="" type="radio"/> From Credit Record <input type="radio"/> Custom:	Account: <input checked="" type="radio"/> From Credit Record <input type="radio"/> Custom:
<input type="checkbox"/> Append Tran Code starts at 13	<input type="checkbox"/> Append Tran Code starts at 13
Aux On-Us: <input checked="" type="radio"/> From Credit Record <input type="radio"/> Custom:	Aux On-Us: <input checked="" type="radio"/> From Credit Record <input type="radio"/> Custom:

Credit Record Configuration

Deposit Slip	Credit Record
Route/Transit: <input checked="" type="radio"/> From Credit Record <input type="radio"/> Custom:	Route/Transit: <input checked="" type="radio"/> From Credit Record <input type="radio"/> Custom:
<input type="checkbox"/> Append Tran Code starts at 13	<input type="checkbox"/> Append Tran Code starts at 13

To configure adjustment and credit record settings, do the following:

1. In System Manager, click the Organization Management link.
2. In the organization tree, select the organization for which you want to modify adjustment settings.
3. Click the Adjustment Processing tab.
4. In the Deposit Channel drop-down box, select the channel to which the configured settings apply. There are two channels to choose from.

- RDC: Select this channel to configure settings for deposits received from all non-mobile RDC channels.
 - Mobile RDC: Select this channel to configure settings for deposits received from mobile RDC. Note that if you are not using mobile RDC, these settings will be ignored.
5. Click the Edit icon on the left side of the information that you want to configure. An Edit dialog box appears.
 6. Configure the information as described in the appropriate section below:
 - Edit Adjustments General Configuration
 - Edit Debit and Credit Adjustment Configuration
 - Edit Credit Record Configuration
 7. Click OK.

Edit Adjustments General Configuration

The General section of the Adjustment Processing tab allows you to specify whether you want to use the default system behavior or the configuration you specify on the Adjustment Processing tab, set a threshold for adjustment email notifications, and enable dynamic data embedding for both adjustment record images.

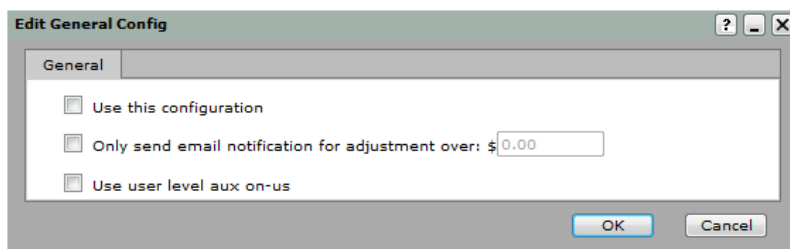
About Dynamic Adjustment Images

When a debit or credit adjustment is created in the NetCapture Platform, an image for the adjustment items is generated which contains dynamically embedded data. This dynamic image configuration can be set only at the Bank of First Deposit organization level. Inheritance rules are not applied.

The adjustment image will contain the following dynamic data:

- Account name (if available)
- Account number
- Deposit Date/Time (time in UTC format)
- Deposit ID
- Credit/Debit indicator
- MICR line—which includes the aux on-us, routing number, bank on-us and adjustment amount

For more information on dynamic adjustment images and how to view them in Server Reporting, see the *Reporting User Guide* or the *Reporting and Deposit Management User Guide*.



Field	Description
Use this configuration	<p>Select this box to use the configuration specified in the Adjustment Processing tab instead of the default system behavior.</p> <p>Note: The default values in the Adjustment Processing tab and the default system behavior are the same. Both configurations generate adjustments and credit records using the information from the depository account. You only need to select this box if you want to change any of the default settings, or if you want to set a threshold for email notifications (as configured in the field below).</p>
Only send email notification for adjustment over: ____	<p>Select this box to suppress the email notification when an adjustment is created for an amount less than the amount specified in the field.</p> <p>In order for this to take effect, you must also select the Use this configuration box.</p>
Use user level aux on-us	<p>Select this box to enable use of a user level aux on-us in place of the aux on-us specified for the depository account when generating credit and adjustment records.</p> <p>When this box is selected, then the User level aux on-us field appears in the Add/Edit User dialog box.</p> <p>Note: This check box is only present on the Adjustment Processing tab for Customer organizations, not at the BOFD or Correspondent Bank level.</p>
Enable Adjustment Dynamic Image	<p>Select this box to enable the credit and debit images generated by the NetCapture Platform to be shown with dynamically embedded data specific to the current deposit.</p> <p>In order for this to take effect, you must also select the Use this configuration box.</p> <p>Note: This check box is only available at the BOFD or Correspondent Bank level.</p>
Enable Adjustment Back Image	<p>Select this box to enable the back image of a credit or debit adjustment item generated by the NetCapture Platform to be shown as a standard, blank image with no dynamic data.</p> <p>In order for this to take effect, you must also select the Use this configuration box.</p> <p>Note: This check box is only available at the BOFD or Correspondent Bank level.</p>

Edit Debit and Credit Adjustment Configuration

The Debit and Credit Adjustment configuration sections of the Adjustment Processing tab allow you to configure the information that is used when creating adjustments to deposits.

You can set up two types of adjustments—a default configuration and an alternate configuration that is used when an adjustment is less than a specified amount. Specify the default configuration in the fields on the left, and specify the alternate configuration in the fields on the right.

Field	Description
Route/Transit	<p>Select From Credit Record to use the route/transit number from the credit record or deposit slip associated with the deposit in adjustments.</p> <p>Select Custom to use a custom route/transit number in adjustments, and enter the route/transit number in the text box.</p>
Account	<p>Select From Credit Record to use the account number from the credit record or deposit slip associated with the deposit in the bank on-us field of adjustments.</p> <p>Select Custom to use a custom account number the bank on-us field of adjustments, and enter the account number in the text box.</p>
Append Tran Code	<p>Select the check box to append a tran code to the adjustment's bank on-us field, then enter the tran code in the text box.</p> <p>Tran codes can be up to 6 characters long and can contain numbers, spaces, dashes, and forward slashes.</p> <p>In the field after the words start at, specify the starting position in the MICR line where the tran code will be placed. This must be between 32 and 13.</p> <p>For more information, see <i>About the MICR Line and Tran Codes</i>.</p>
Aux On-Us	<p>Select From Credit Record to use the aux on-us number from the credit record or deposit slip associated with the deposit in adjustments.</p> <p>Select Custom to use a custom aux on-us number in adjustments, and enter the aux on-us number in the text box; or leave it blank if you do not want to use an aux on-us number in adjustments.</p> <p>If the User Level Aux On-Us is configured for a specific organization, it will override other aux on-us settings. See <i>Edit Adjustments General Configuration</i> for details.</p>
Use this if adjustment amount is less than \$____	<p>Select this box to use the Alternate Configuration for items that are less than the amount specified in the text field.</p> <p>If you do not enter an amount or if the check box is not selected, the Default Configuration will be used.</p>

About the MICR Line and Tran Codes

Each character in a MICR line is given a numerical value to represent the placement of the character on the document. The values start with 1 at the far right side of the MICR line and increment as you move to the left.

The bank on-us field starts in position 32 of the MICR line and is written to the right, up to position 13. You can configure tran codes to start in any position between 32 and 13. This means that if an item already has a bank on-us number, and you specify a tran code, there is the potential that the tran code you specify could overlap/overwrite the existing bank on-us number.

By default, tran codes are configured to start in position 13. You should specify the starting position of the tran code by determining what the bank on-us values of adjustments are likely to be, and what the length of the tran code you have specified is.

For example:

- An adjustment has a bank on-us value that is 9 characters long. This value will occupy positions 32 to 24 of the MICR line.
- You have configured a 3-digit tran code that starts at position 15. The tran code will occupy positions 15 to 13 of the MICR line.
- Positions 23 to 16 of the MICR line will be blank.

Edit Credit Record Configuration

The Credit Record configuration section of the Adjustment Processing tab allows you to configure the content of credit records that are sent to the Decision Gateway and enable dynamic credit record. The values you configure here are used on all credit items generated by the Extractor in place of the values generated by Web Client or scanned from a deposit slip.

- To configure the values for scanned deposit slips, modify the values in the section labeled Deposit Slip.
- To configure the values for system-generated credit records, modify the values in the section labeled Credit Record.

About Dynamically Generated Credit Records

In the Edit Credit Record section, you can enable a dynamic image and back image for credit records. This dynamic image configuration can be set only at the Bank of First Deposit organization level. Inheritance rules are not applied.

During image capture in both the Web Client and Web Client, when a deposit ticket is not scanned as the first item, the system generated credit record or deposit ticket will include dynamic data specific to the current deposit. The deposit ticket image will include dynamic deposit and account data which will be viewable in Server Reporting in the NetCapture Platform system. The dynamically embedded credit record will contain the following dynamic data:

- Account name (if available)
- Account number
- Deposit amount
- Deposit date and time received
- Deposit ID
- Credit indicator
- MICR line—which includes the aux on-us, routing number, bank on-us and adjustment amount based on preconfigured adjustment creation rules

For more information on dynamically generated credit records and how to view them in Server Reporting, see the *Reporting User Guide* or the *Reporting and Deposit Management User Guide*.

Field	Description
Route/Transit	Select From Credit Record to use the route/transit number from the credit record or deposit slip associated with the deposit. Select Custom to use a custom route/transit number, and enter the route/transit number in the text box.
Append Tran Code	Select the check box to append a tran code to the credit record's bank on-us field, then enter the tran code in the text box. Tran codes can be up to 6 characters long and can contain numbers, spaces, dashes, and forward slashes. In the field after the words start at, specify the starting position in the MICR line where the tran code will be placed. This must be between 32 and 13. For more information, see <i>About the MICR Line and Tran Codes</i> .
Credit Records	
Enable Dynamic Image	Select this box to enable the credit record images generated by the NetCapture Platform to be shown with dynamically embedded data specific to the current deposit.
Enable Back Image	Select this box to enable the back image of credit record item generated by the NetCapture Platform to be shown as a standard, blank image with no dynamic data.

Configuring Adjustment Notification Emails

Use System Manager to configure adjustment notification emails that are automatically sent when deposits or items are rejected or adjusted in Deposit Review. Adjustment notification emails look similar to this:

Joe's Auto Repair,

For Account A xxxxx-1234 in deposit number 32, submitted on 04/26/ 2007 12:38:15 for \$1563.12, a CREDIT adjustment of \$1.00 will be posted to the following item(s) for the following reason(s):

Item 72 - Adjusted for Encoded Amount Error

If you have any questions or concerns, please contact 800-387-7884.

Thank you,

Sample Bank

Note: The notifications sent by your system may differ from the example if your service organization has modified the default email text in the database. For more information, see the *NetCapture Platform System Manual*.

The name of the organization in the salutation is the name of the parent organization that is hosting NetCapture Portal. The address from which the message is sent and the contact phone number in the message are the email address and phone number of the configured primary contact for the customer's parent organization (Bank of First Deposit or Correspondent Bank).

Requirements for Configuring Adjustment Notification Emails

Obtain the following information before you configure adjustment notifications in System Manager (coordinate this information with the administrator of the application):

- Name and email address of the intended sender of adjustment notification emails
- The SMTP server host address for the Portal
- The name of the parent organization from which the adjustment notification emails should be sent
- The customer support phone number for questions or concerns about adjustments

Steps for Configuring Adjustment Notification Emails

Do the following to configure adjustment notification emails:

1. In System Manager, click the Organization Management link.
2. In the organization tree, select the Customer's parent organization (you can find the name of the parent organization on the General tab for the Customer). This is the organization from which the emails will be addressed.
3. Click the Locations & Contacts tab.
4. Expand the list to view the contacts for a particular organization by clicking [+] next to Show contacts.
5. Find the primary location and the primary contact at that location. The primary contact has a check mark under the Primary column.
6. Ensure the primary contact at the primary location is the person/email address from which you want adjustment notifications to be sent. If you want the notifications to be sent from another address, change the primary contact for the organization—see *Adding/Editing Contacts* for instructions.
7. Ensure the primary contact has the correct customer support phone number as it will be listed in the adjustment notification messages.
8. Click the Operational Parameters tab.
9. Ensure that the Send Reviewer Email column has a check mark under it. If it doesn't, click the Edit icon and enable Send Reviewer Emails by selecting the check box next to it, and then clicking the OK button.
10. In the organization tree, select the Service Provider (or Bank of First Deposit if no Service Provider is present) that hosts the NetCapture Portal application servers.
11. Click the Applications tab.
12. Locate the NetCapture Portal application and click the Edit icon.
13. In the SMTP Host field, provide the URL for the SMTP mail server that will be sending adjustment notification emails.
14. Repeat Steps 12 and 13 for each Portal application hosted by the organization.
15. OPTIONAL: If you want to suppress email notifications for adjustments of less than a certain dollar amount, see *Edit Adjustments General Configuration*.

Configuring User-Defined Fields

User-defined fields are extra fields that you can add in Desktop Client and Web Client for your customers to use to enter information about the deposited items. The fields you configure here are added to each item in the deposit, so you can capture whatever additional information each organization needs, such as accounts receivable information.

There are two types of fields you can configure here—custom data fields and payment data fields.

- Custom Data fields can be used to capture any type of information that is not normally included on an item but that would be useful for your organization to have. There are two types of custom data fields—item-level fields and deposit-level fields.
 - Desktop Client: The first two item-level custom data fields you configure appear on the Item Data tab in Desktop Client. Any other custom data fields appear on the Custom Data tab. Up to four deposit-level fields you configure appear on the Deposit-Level Data tab in Desktop Client.
 - Web Client: Up to 21 item-level custom data fields are used in Web Client.
- Payment Data fields are used to capture detailed information about a specific item, such as an itemized listing of charges included on the item amount. The fields can be summed and balanced against the item amount. These fields appear on the Payment Data tab in Desktop Client. Web Client does not support payment data fields.

You can configure user-defined fields for a specific organization by using these steps, or you can create templates that can then be applied to organization templates you can use when creating customer organizations. For more information about templates, see *Creating and Managing Templates*.

Requirements for Configuring User-Defined Fields

Before you begin, obtain information about the user-defined fields you want to configure.

For custom data fields, obtain the following for each field:

- Whether the field should be available at the deposit or item level
- The field label (up to 20 alphanumeric characters)
- Whether the field is required or optional
- The type of data that can be entered in the field—alphanumeric, numeric, date, or currency data.
- Whether or not you want the field to be auto-populated based on previous entries.
- Whether or not you want the field to be used as a cross-reference in a downstream system.

For payment data fields, obtain the following in addition to the information listed above for custom fields:

- Which information should be summed for balancing against the item total

Steps for Configuring Custom Field Data

To configure custom data fields, do the following:

1. In System Manager, click the Organization Management link.
2. In the organization tree, select the organization for which you want to configure custom data.
3. Click the User-Defined Fields tab.
4. Under Custom Data Fields, click the Add icon.

The Add Custom Data Field dialog box appears.

5. Edit the following settings as desired (fields marked with an asterisk [*] are required):

Field	Description
Label*	This is the text label that describes the field in the Web Client. This can be up to 20 alphanumeric characters.
Deposit Level	Select this box to make this field a deposit-level field, which means it must be entered only once for the entire deposit and not for every item. You can configure up to 4 fields as deposit-level fields.
Required?	Select this box if the field is required to be completed. Leave the check box clear if the field is optional and can be left blank.
Data Type	The type of data allowed to be entered in the field. This can be Alphanumeric, Currency, Date, Drop- Down, or Numeric.
Auto-Populate?	Select this box to look up previous transactions and auto-populate custom fields. The system will save a history of items captured and the values entered for custom fields. As new items are scanned, if the system finds a match, it will auto-populate the custom fields using the previously-entered values.
Drop-down values?	If you have chosen drop-down as the custom field type, use this field to enter the values you want to appear in the drop-down list. Separate the entries with hard returns.
X-Ref?	Select this box to designate a custom field as the primary cross-reference for a customer.

6. Click OK to save the custom data fields.

Steps for Configuring Payment Data Fields

To configure payment data fields, you will configure the columns to be included in a table of fields. Do the following:

Note: Web Client does not support payment data fields.

1. In System Manager, click the Organization Management link.
2. In the organization tree, select the organization for which you want to configure payment data fields.
3. Click the User-Defined Fields tab.

Under Define Payment Data Columns, click the Add icon. The Add Payment Data Column dialog box appears.

4. Edit the following settings as desired (required fields are marked with an asterisk [*]):

Field	Description
Label*	This is the text that is in the column heading in the Desktop Client Payment Data tab. This can be up to 20 alphanumeric characters.
Required?	Select this box if the field is required to be completed. Leave the check box clear if the field is optional and can be left blank.
Data Type	The type of data allowed to be entered in the field. This can be Alphanumeric, Currency, Date, or Numeric.
Is Included in Payment Total?	Select the check box to include this field in a sum of payment data fields that is balanced against the item amount. Leave the check box clear to exclude the field from the payment data total. This option only applies to fields for which the Data Type is set to be Currency.

5. Click OK to save the payment data fields.

Creating and Managing Templates

If many of the settings you will use are the same for each organization you create in the system, you may want to create templates to capture those settings. The templates can then be applied each time you create a new organization, saving setup time and ensuring consistency across the organizations in the system.

There are two types of templates: organization templates and user-defined field templates. You can apply both types of templates when creating a new organization.

For example, if your policy is that all Customer type organizations use the same operational parameters and user-defined fields for Web Client applications, then you may want to create an organization template and a user-defined field template that define those settings. You can then apply those templates each time you create a new Customer organization.

Requirements for Creating and Managing Templates

Before creating templates, gather the information you want to use in the template.

- See *Creating New Organizations* for information about the fields available in the organization template.
- See *Configuring User-Defined Fields* for information about the fields available in the user-defined field template.

Once you create an organization using a template, it is no longer linked to the template. You cannot dynamically update existing organizations in the system by modifying a template. When you modify a template, only new organizations you apply the template to will receive the new settings. Therefore, be sure you define the correct settings in the template before you begin adding organizations.

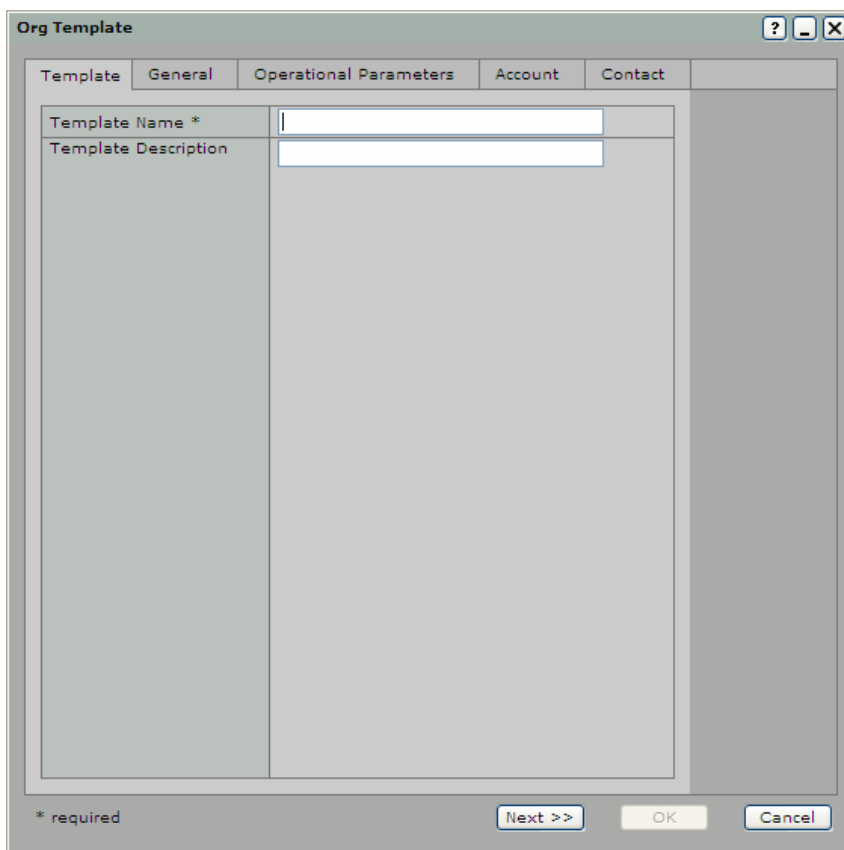
Steps for Creating a New Organization Template

To create a new organization template, do the following:

1. In System Manager, click the Templates link.
2. Click the Org Templates tab.
3. Click the Add icon.

If you want to use an existing template as the basis for a new template, you can instead click the Edit icon and then save your changes as a new template—see the next section, *Steps to Modify an Existing Organization Template*.

The Org Template dialog box appears.



4. Enter a name for the template.
This is the name users will see when they choose the template to apply to a new organization. The name can be up to 50 characters long.
5. If desired, enter a description for the template.
6. On the remaining tabs, complete the fields that you want to include in the template using the instructions in Creating New Organizations.
You can complete as many or as few fields as you wish. Ensure you complete the fields accurately since they will be pre-populated for any new organizations created using this template.
7. When you are finished entering the template information, click OK to save the template.

Steps for Modifying an Existing Organization Template

Do the following to modify an existing organization template:

1. In System Manager, click the Templates link.

2. Click the Org Templates tab.
3. Locate the template you want to update and click the Edit icon.

The Org Template dialog box appears.

4. Ensure the option Update Existing Template is selected.
If you instead want to create a new template, you can select Create New Template.
5. Modify the template name or description, if desired.
6. On the remaining tabs, make any desired changes to the information in the template.
You can complete as many or as few fields as you wish. Ensure you complete the fields accurately since they will be pre-populated for any new organizations created using this template.
7. Click OK to save the template.

Steps for Creating a New User-Defined Field Template

To create a new user-defined field template, you must first create templates for each individual user-defined field, and then you must group them together. The template group is what you will apply when creating a new organization.

- Creating Individual Field Templates
- Creating Template Groups

Creating Individual Field Templates

To create the individual user-defined field templates, do the following:

1. In System Manager, click the Templates link.
2. Click the Defined Field Templates tab.

- If you want to add a custom data field template, click the Add icon under Custom Data Field Templates.
- If you want to add a payment data field template, click the Add icon under Payment Data Field Templates.
- If you want to use an existing template as the basis for a new template, you can instead click the Edit icon and then save your changes as a new template—see *Steps to Create a New User-Defined Field Template*.

Depending on the selection you made, the Add Custom Data Field Template or Add Payment Data Field Template dialog box appears.

3. Complete the fields using the instructions in Configuring User-Defined Fields.

Ensure you complete the fields accurately since they will be used for any new organizations to which you apply this template.

4. When you are finished entering the template information, click the Save as Template Field button.

A dialog box appears prompting for a template name and description.

5. Enter a name for the template.

This is the name you will see when you choose the template to add to a template group. The name can be up to 50 characters long. It is recommended that you name the template in a way that will help you easily identify it.

6. If desired, enter a description for the template.
7. Click OK to save the template.

Creating Template Groups

To create a user-defined field template group, do the following:

1. In System Manager, click the Templates link.
2. Click the Defined Field Groups tab.
3. Click the Add icon.

The Defined Field Group dialog box appears.

4. Enter a name for the template group. The name can be up to 50 characters long.
5. If desired, enter a description for the template group.
6. In the Available list, select the user-defined field template(s) that you want to include in this group.
Note: To select multiple templates, hold down the Ctrl key while you click on the templates. To select all available templates, select the Select all in list check box.
7. Click the arrow key [>] to move the template(s) to the Current list.
8. Click OK.

Steps for Modifying an Existing User-Defined Field Template

You can modify either the individual user-defined field templates you have created or the template groups.

- Modifying an Individual Field Template
- Modifying a Template Group

Modifying an Individual Field Template

Do the following to modify an existing user-defined field template:

1. In System Manager, click the Templates link.
2. Click the Defined Field Templates tab.
3. Locate the field you want to edit and click the Edit icon.
 Depending on which type of field you chose to edit, the Edit Custom Data Field Template dialog box or the Edit Payment Data Field Template dialog box appears.
4. Make any desired changes to the information in the template.
 Ensure you complete the fields accurately since they will be pre-populated for any new organizations created using this template and click the Save as Template button.
 A save as dialog box appears.

5. Ensure the option Update Existing Template is selected.

If you instead want to create a new template, you can select Create New Template.

6. Modify the template name or description, if desired.

If you change the name of an existing template, the new template name will replace the previous template name. The old template name will no longer be available to users when creating organizations.

7. Click OK to save the template.

Modifying a Template Group

Do the following to modify an existing user-defined field template group:

1. In System Manager, click the Templates link.
2. Click the Defined Field Groups tab.
3. Locate the group you want to edit and click the Edit icon.
4. Make any desired changes to the information in the template.

Ensure you complete the fields accurately since they will be pre-populated for any new organizations created using this template.

If you change the name of an existing template, the new template name will replace the previous template name. The old template name will no longer be available to users when creating organizations.

5. Click OK to save the group.

Managing Scrutiny Rules

Scrutiny rules are used to evaluate deposited items to determine whether they should be accepted, rejected, or flagged for review at Deposit Review before being processed.

Scrutiny Rules Hierarchy

To make the most efficient use of the system, Banks of First Deposit should add scrutiny rules that suit their organizations (Service Providers will never have scrutiny rules). Correspondent Banks and Customers inherit a default set of scrutiny rules from their parent organizations, and they can add rules for their own use.

In addition to the organization-level scrutiny rules, you can also create rules at the account level. Account-level rules override child organization rules, and child organization rules override parent organization rules. That is, when evaluating items, the system uses any available account-level rules first, then any available child organization rules, then any available parent organization rules. The one exception to this is for the Route/Transit Number type rule, where the rule as defined at the parent organization overrides any rules that may be defined for its child organizations.

See the section *Adding/Editing Accounts* for details about creating account-level scrutiny rules.

If multiple instances of the same rule are defined for an organization, any rules that are set to reject items override the rules set to flag items. For example, a Bank of First Deposit has defined the following two Item Amount Threshold rules:

- IF Item Amount Threshold IS GREATER THAN 100 THEN Reject
- IF Item Amount Threshold IS GREATER THAN 10 THEN Set Flag

In this case, the first rule (the one with the Reject action) will override the second rule when applicable. For example, if more than 10 deposits are received, it will be flagged. But if more than 100 deposits are received, it will be rejected.

Valid Rule Combinations

The following table contains the valid rule conditions and actions. You may want to refer to this table when creating rules. All of these rules apply to Web Client applications except for the Duplicate Item on Server rule, which applies to the Extractor.

Rule	Valid Conditions	Valid Actions	Description
Route/Transit Number	Is Between* * Commonly excluded RT number ranges include: <ul style="list-style-type: none"> • 00000051-00000051 Government checks • 80000000-89999999 Travelers checks • 00000050-00000050 Government checks 	Reject	Items possessing route/transit numbers that fall within the specified range of numbers will be rejected.
Item Scanned MICR Line	Is Empty	Reject Set Flag	Items that are missing a scanned MICR line will be flagged for review or rejected. Note: This rule does not apply to mobile transactions.
RT Number Check Digit	Fails	Reject Set Flag	Items with route/transit numbers that failed the check digit calculation will be flagged for review or rejected. The check digit calculation ensures the route/transit number is valid.
Scanned MICR Amount	Is Found	Reject Set Flag	Items with amounts encoded in the MICR line will be flagged for review or rejected.
Item Amount Threshold	Is Equal To	Reject Set Flag	Items with amounts equal to, greater than, or less than the specified amount will be flagged for review or rejected.
	Is Greater Than Or Equal To	Reject Set Flag	
	Is Greater Than	Reject Set Flag	
	Is Less Than Or Equal To	Reject Set Flag	

Rule	Valid Conditions	Valid Actions	Description
	Is Less Than	Reject Set Flag	
Capture Duplicate Item	Is Found	Reject Set Flag	Items that may be duplicates of items previously submitted at the capture point will be flagged for review or rejected. Note: This rule does not apply to mobile transactions.
Scanned Route/Transit	Is Changed	Reject Set Flag	A depositor edited the initial scanned route/ transit number for an item, so the item will be flagged for review or rejected. Note: This rule does not apply to mobile transactions.
Scanned Bank On-Us	Is Changed	Reject Set Flag	A depositor edited the initial scanned bank on-us field for an item, so the item will be flagged for review or rejected. Note: This rule does not apply to mobile transactions.
Scanned Aux On-Us	Is Changed	Reject Set Flag	A depositor edited the initial scanned aux on-us field for an item, so the item will be flagged for review or rejected. Note: This rule does not apply to mobile transactions.
Scanned Amount	Is Changed	Reject Set Flag	A depositor edited the initial scanned encoded amount for an item, so the item will be flagged for review or rejected. Note: This rule does not apply to mobile transactions.
	Increased By More Than	Set Flag	An item amount that has been increased by more than the specified threshold will be flagged for review. If you use this condition, item amounts that are decreased will NOT be flagged for review. Note: This rule does not apply to mobile transactions.
Entered Amount	Is Changed	Reject Set Flag	An item amount that was initially entered was changed before the deposit was completed by the depositor, so the item will be flagged for review or rejected.
	Increased By More Than	Set Flag	An item amount that has been increased by more than the specified threshold will be flagged for review. If you use this condition, item amounts that are decreased will NOT be flagged for review.

Rule	Valid Conditions	Valid Actions	Description
Scanned Item * This rule is not supported.	Is not stamped	Reject Set Flag	Note: This rule is not supported. Set the Status field to Inactive. This rule does not apply to mobile transactions.
Deposit Amount Threshold	Is Equal To	Set Flag	Deposits with total amounts equal to, greater than, or less than the specified amount will be flagged for review.
	Is Greater Than Or Equal To	Set Flag	
	Is Greater Than	Set Flag	
	Is Less Than Or Equal To	Set Flag	
	Is Less Than	Set Flag	
Daily Total Deposit Amount	Is Greater Than Or Equal To	Don't Accept Report Only Set Flag	When deposits submitted for the designated customer or account reach the daily limit specified here, they will trigger the rule. For the purposes of this rule, a day is defined as a 24-hour period from midnight to midnight.
	Is Greater Than	Don't Accept Report Only Set Flag	If you choose Don't Accept, deposits triggering the rule will be stopped at the client and users will not be allowed to submit them until the 24-hour period is up. If you choose Report Only, deposits that trigger the rules will be included in over limit reports, but no further action will be taken on them. If you choose Set Flag, deposits triggering the rule will be sent to Deposit Review. These deposits will also be included in over limit reports. Note: This rule can only be applied to customers and accounts. Bank-level limits are not supported.
Daily Number of Items	Is Greater Than Or Equal To	Don't Accept Report Only Set Flag	When deposits submitted for the designated customer or account reach the daily number of items specified here, they will trigger the rule. For the purposes of this rule, a day is defined as

Rule	Valid Conditions	Valid Actions	Description
	Is Greater Than	Don't Accept Report Only Set Flag	<p>a 24-hour period from midnight to midnight.</p> <p>If you choose Don't Accept, deposits triggering the rule will be stopped at the client and users will not be allowed to submit them until the 24-hour period is up.</p> <p>If you choose Report Only, deposits that trigger the rules will be included in over limit reports, but no further action will be taken on them.</p> <p>If you choose Set Flag, deposits triggering the rule will be sent to Deposit Review. These deposits will also be included in over limit reports.</p> <p>Note: This rule can only be applied to customers and accounts. Bank-level limits are not supported.</p>
7-Day Total Deposit Amount	Is Greater Than Or Equal to	Don't Accept Set Flag	<p>Mobile deposits that exceed the configured limit, which is calculated using a 7-day rolling time period, will either be rejected or flagged for review.</p>
	Is Greater Than	Don't Accept Set Flag	<p>The 7-day time period is calculated by looking back exactly 7 days from the time at which the deposit is attempted. For example, if a user submits a deposit at 10:00 a.m. on March 12, then the application looks back 7 days to 10:00 a.m. on March 5, calculates the total, and takes action on the deposit based on the total of all deposits submitted between 10:00 a.m. on March 5 and 10:00 a.m. on March 12.</p> <p>For this rule, the UTC time zone is used with no offset, which makes the user's time zone irrelevant. Each deposit timestamp is stored at the server in UTC time and that is used to calculate the rolling limits.</p> <p>Note: This rule can only be applied to mobile customers and accounts. Bank-level limits are not supported.</p>
30-Day Total Deposit Amount	Is Greater Than Or Equal to	Don't Accept Set Flag	<p>Mobile deposits that exceed the configured limit, which is calculated</p>

Rule	Valid Conditions	Valid Actions	Description
	Is Greater Than	Don't Accept Set Flag	<p>using a 30-day rolling time period, will either be rejected or flagged for review. The 30-day time period is calculated by looking back exactly 30 days from the time at which the deposit is attempted. For example, if a user submits a deposit at 10:00 a.m. on March 30, then the application looks back 30 days to 10:00 a.m. on March 1, calculates the total, and takes action on the deposit based on the total of all deposits submitted between 10:00 a.m. on March 1 and 10:00 a.m. on March 30.</p> <p>For this rule, the UTC time zone is used with no offset, which makes the user's time zone irrelevant. Each deposit timestamp is stored at the server in UTC time and that is used to calculate the rolling limits.</p> <p>Note: This rule can only be applied to mobile customers and accounts. Bank-level limits are not supported.</p>
Account Number	Is New	Set Flag	<p>Deposits made to accounts that are marked as new accounts will be flagged for review.</p> <p>To use this rule, you must also enable the New Account option for the account. See <i>Adding/Editing Accounts</i> for details.</p>
Percent of Deposits to Review	Is Applied	Set Flag	A random selection of deposits that meets the specified percentage of all deposits made will be flagged for review.
Bank On-Us	Is Empty	Reject Set Flag	<p>No bank on-us number was scanned for the item, so it will be flagged for review or rejected.</p> <p>Note: This rule does not apply to mobile transactions.</p>
Scanned or Edited EPC	Is Found	Reject Set Flag	An EPC number was scanned or edited for the item, so it will be flagged for review or rejected.
Scanned or Edited Aux On-Us	Is Empty	Reject Set Flag	<p>An aux on-us field was scanned or edited for the item, so it will be flagged for review or rejected.</p> <p>Note: This rule does not apply to mobile transactions.</p>
Control Balance	Is Changed	Set Flag	The control balance for the deposit was changed before submitting the deposit, so it will be flagged for review.

Rule	Valid Conditions	Valid Actions	Description
Item Type	Is Changed	Set Flag	<p>This item's type (DR-debit, DS-deposit slip) was changed after the initial scan, so it will be flagged for review.</p> <p>Note: It is recommended that you set this rule for all accounts using deposit slips in order to ensure that scrutiny rules are applied properly for items that have their types changed after initial scanning at Web Client.</p> <p>This rule does not apply to mobile transactions.</p>
Dual Control Deposit Amount	Is Greater Than the Deposit Limit	Review	<p>When this rule is active, Remote Users with deposit limits will be prompted to have any deposits that exceed the limit reviewed by a Remote Reviewer before they can be submitted.</p> <p>Note: In order for this rule to take effect, Remote users associated with the organization that has this rule set must also have deposit limits assigned. See <i>Creating Users</i>. Deposits will only require review if this rule is set and the deposit exceeds the deposit limit for the user making the deposit.</p> <p>This rule does not apply to mobile transactions.</p>
IQA Threshold	Is Less Than	Reject Set Flag	<p>Provide a number from 1 to 100 to indicate the acceptable level of quality for scanned images. Images that receive a quality grade below this number will be flagged for review or rejected.</p> <p>Web Client evaluates scanned check images for their level of quality and assigns a grade to each image. The better the quality, the higher the grade the image receives. The image quality grade is a composite of several factors, such as image sharpness and clarity, darkness or lightness, readability, etc. The higher the number you provide here, the more items will <i>fail</i> to meet quality standards and will require re-scanning or adjustment.</p> <p>Enter 0 (zero) to turn off IQA functionality. The application will not analyze the quality of images.</p> <p>IMPORTANT! IQA is only used if you configure the organization's Desktop Client applications with a separate CAR/IQA toolkit, or if you install and configure the IQA/CAR server for the organization's Web Client applications.</p>

Rule	Valid Conditions	Valid Actions	Description
Duplicate Item on Server	Is Found	Set Flag	<p>Items that may be duplicates of items previously submitted to the server will be flagged for review.</p> <p>Note: This rule must be set here for the Extractor and also defined for each Customer organization in its operational parameters. The number of days in the Check Duplicates For field must be set to greater than 0 (zero) to specify the number of days the server will check for duplicates. This number should not exceed the number of days the images are available on the server (images should not be purged according to a schedule that is shorter than this setting).</p>

Requirements for Creating Scrutiny Rules

Before you create scrutiny rules, make sure you have completed a risk analysis and you understand your organization's requirements for routing items.

You cannot delete scrutiny rules. If your organization no longer wants to use a rule, you must set its status to inactive.

You can do either of the following:

- Creating New Scrutiny Rules
- Setting Scrutiny Rule Status

Creating New Scrutiny Rules

To create scrutiny rules, do the following:

1. In System Manager, click the Organization Management link.
2. In the organization tree, select the organization for which you want to create scrutiny rules.
3. Click the Rules tab.
4. Click the Add icon.

The Add Rule dialog box appears.

Rule	
Application Type *	Remote
Rule *	Deposit Amount Threshold
Condition **	Is Greater Than or Equal to
Start Value **	1000.00
Action *	Set Flag
Status	active

* required

OK Cancel

The options that appear in the Add Rule dialog box depend on the selections you make. The available options change dynamically to match your selections. See *Valid Rule Combinations* for details about the rule conditions and actions that are available for each type of rule.

5. Provide the following information (fields marked with an asterisk [*] are required):

Field	Description
Application Type*	Select the application to which this rule will apply. The application will use this rule when validating items. <ul style="list-style-type: none">• Select Remote if the rule applies to Desktop Client and Web Client applications.• Select Extractor if the rule applies to the Extractor component of the NetCapture Platform.• Select Mobile if the rule should apply to mobile transactions.
Rule*	Select the type of rule.
Condition*	The condition for the rule. For example, the condition determines whether each deposit's value is greater than, less than, or equal to the threshold value.
Value*	The value for the rule. For example, the value determines the cutoff point for deposits being evaluated. If the rule allows a range, there will be both a Start Value and an End Value.
Action*	The appropriate action to take when the rule criteria are met. The actions available for each rule vary, but they include Reject, Set Flag, Review, and Don't Accept. Reject means items are rejected at the Web Client. Set Flag means items/deposits will be reviewed at Deposit Review before further processing. Review means the deposits may be reviewed by a second user at the Desktop Client before being submitted. Don't Accept means the deposit will be stopped at the client and the user will be unable to submit it until some condition is met.
Account Level Only	Select this check box to apply the rule at the account level. When this box is selected, the total will not be aggregated at the customer level — rather, it will be applied to each account belonging to this customer. Note: This check box is only available when Mobile is selected in the Application Type.
Status	The rule may be active (in use) or inactive (not currently in use).

6. Click OK to save the rule.
7. Repeat this procedure to create additional rules.

Setting Scrutiny Rule Status

To set the status of existing scrutiny rules, do the following:

1. In the organization tree, select the organization for which you want to set the status of scrutiny rules.
2. Click the Rules tab.

The list of scrutiny rules for the organization appears.

Bobs Printing									
General	Branding	Operational Parameters	User Defined Fields	Locations & Contacts	Accounts	Rules	Users	Security	Adjustment Processing
Show Active Rules ▼									
Application	Org Name	Org Type	Rule	Status	Condition	Start Value	End Value	Action	
MOBILECLIENT	DNow	Bank Of First Deposit	Daily Total Deposit Amount	Active	Is Greater Than or Equal to	10000		Set Flag	
REMOTE	DNow	Bank Of First Deposit	Route/Transit Number	Active	Is Between	00000000	00000000	Reject	
MOBILECLIENT	DNow	Bank Of First Deposit	Account Number	Active	Is New			Set Flag	
REMOTE	DNow	Bank Of First Deposit	RT Number Check Digit	Active	Fails			Set Flag	
REMOTE	Bobs Printing	Customer	Daily Number of Items	Active	Is Greater Than or Equal to	10		Do not Accept	
REMOTE	Bobs Printing	Customer	Daily Total Deposit Amount	Active	Is Greater Than or Equal to	100		Do not Accept	

Note: You can filter the list of rules using the drop-down box on the right side of the screen. You can view all rules, only active rules, or only inactive rules.

- Locate the rule you want to change, then click the Edit icon for that rule.

Note: The Edit icon is available only for those rules that you have permission to change. For example, in the figure above the rules list includes rules inherited from the Bank of First Deposit and rules that have been customized for the selected customer. You can change only the rules for the selected customer. To change the rules for the Bank of First Deposit, you must first select it in the organization tree.

The Edit Rule dialog box appears.

Edit Rule

Rule

Application Type	REMOTE
Rule	No Scanned MICR Line Found
Condition	Is Empty
Action	Set Flag
Status	active ▼

OK

Cancel

- In the Status drop-down box, select active (rule is in use) or inactive (rule is not currently in use).
- Click OK to save the rule.
- Repeat this procedure for each rule whose status you want to update.

Configuring Deposit Confirmation Email Contents

The email configuration settings determine how bank organizations customize the content of deposit confirmation email messages.

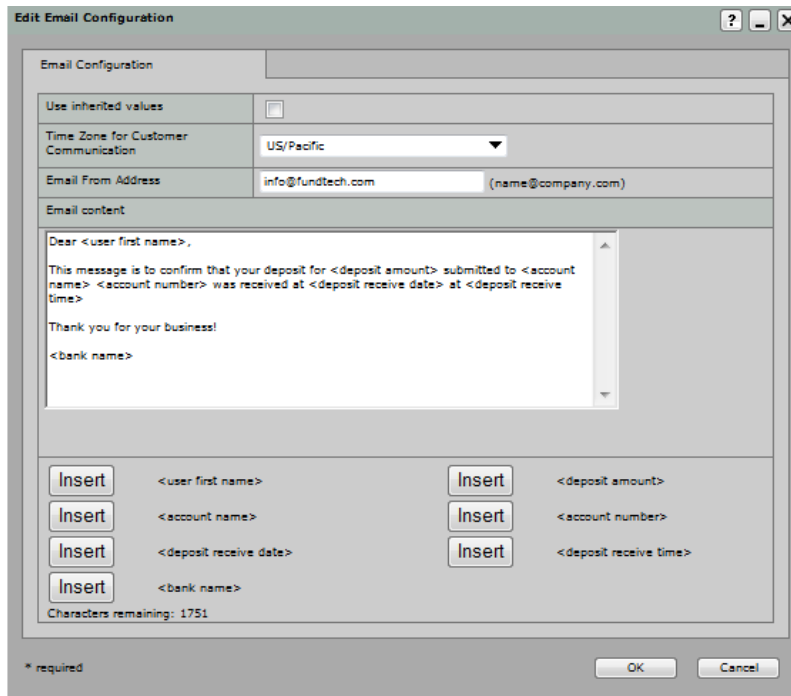
To access email configuration, do the following:

- In System Manager, click the Organization Management link.
- In the Organization tree, select the Bank of First Deposit or Correspondent Bank for which you want to configure the email message.
- Click the Email Configuration tab.

Test Bank										
General	Branding	Operational Parameters	Locations & Contacts	Rules	Users	Security	Applications	License Mngmt	Adjustment Processing	Email Configuration
Inherited Settings		Email "From" Address	Time Zone	Email Content						
		info@fundtech.com	US/Pacific	Dear <user first name>, This message is to confirm ...						

- Click the Edit icon.

The Edit Email Configuration dialog box appears.



The dialog box titled "Edit Email Configuration" contains the following fields and controls:

- Use inherited values:** A checkbox.
- Time Zone for Customer Communication:** A dropdown menu currently showing "US/Pacific".
- Email From Address:** A text field containing "info@fundtech.com" with a placeholder "(name@company.com)".
- Email content:** A large text area containing the following text:

Dear <user first name>,
 This message is to confirm that your deposit for <deposit amount> submitted to <account name> <account number> was received at <deposit receive date> at <deposit receive time>
 Thank you for your business!
 <bank name>
- Dynamic Tags:** A section with eight "Insert" buttons, each corresponding to a tag:
 - <user first name>
 - <account name>
 - <deposit receive date>
 - <bank name>
 - <deposit amount>
 - <account number>
 - <deposit receive time>
- Characters remaining:** A label showing "1751".
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

- Complete the following fields:

Field	Description
Use inherited values	By default, Correspondent Banks are configured to inherit the setting for the Bank of First Deposit. To override the Bank of First Deposit settings and customize the email for a Correspondent Bank, clear the Use inherited values check box.
Time Zone for Customer Communication	The time zone for which you want the email sent to.
Email From Address	The email address from which the email is being sent to.
Email content	<p>The content for the email deposit confirmation that will be sent to end users. Content can be entered as free-form text up to 2000 characters, and will retain spaces and hard returns. The following dynamic tags can be used:</p> <ul style="list-style-type: none"> • user first name • deposit amount • account name • account number • deposit receive date • deposit receive time • bank name

6. Click Ok to save the message settings.

Configuring Branding

Use System Manager to modify branding that appears in Web Client and Desktop Client applications for the selected organization.

You can customize branding for any organization, whether it be a Service Provider, Bank of First Deposit, Correspondent Bank, or Customer. For example, if a Bank of First Deposit has 200 customers who will all use the same branding information, you can set the brand at the Bank of First Deposit level and it will apply to all of the bank's customer organizations.

If you do not customize branding in System Manager, Web Client applications will use the default Finastra branding provided in the system.

Requirements for Configuring Branding

Obtain the information specified from the table in Step 5 in *Steps for Configuring Branding* before you edit branding in System Manager.

Note: The Branding window supports the copyright (©) and trademark (™) symbols.

Steps for Configuring Branding

You can add a new brand or edit the settings for a brand that already exists. To add or edit a brand, do the following:

1. In System Manager, click the Organization Management link.
2. In the organization tree, select the organization for which you want to configure branding.
3. Click the Branding tab.
4. Click the Add icon to create a new brand, or locate an existing brand that you want to modify and click the Edit icon.

Note: You can view the current branding settings by clicking the Show links in the columns for license message, splash screen, small icon, and web client logo. You can delete a brand by clicking the Delete icon.

The Add or Edit Brand dialog box appears.

Add Brand

Brand

Brand Name * (Do not enter special characters)

Title Text * (Do not enter special characters)

License Message *

Splash Screen Image * Browse...

Maximum viewable size: 515 x 150 pixels

Required filename is "splash screen image.gif"

Small Windows Icon * Browse...

Size is 16 x 16
Required filename is "small windows icon.gif"

License Requires Acceptance by User ☐

* required

OK Cancel

5. Modify the desired fields (fields marked with an asterisk [*] are required).

Field	Desktop Client	Web Client	Receivables Client	Consumer Client	Description
Brand Name*	Used	Used	Used	Used	A unique name for this brand. This is only used internally to distinguish it from other brands. This can be up to 30 characters.
Title Text*	Used	Not Applicable	Not Applicable	Not Applicable	The text that is in the title bar of Desktop Client for this organization. This can be up to 300 alphanumeric characters.
License Message*	Used	Used	Used	Used	<p>The message text that displays on the first startup of Web Client and Desktop Client (for example, a licensing agreement or privacy policy). This can be up to 25,000 alphanumeric characters. You can also use hard returns to insert blank lines between paragraphs.</p> <p>This text is displayed to users only one time unless you edit it. Each time you change this text, it is displayed to users once.</p>

Field	Desktop Client	Web Client	Receivables Client	Consumer Client	Description
Splash Screen Image*	Used	Not Applicable	Not Applicable	Not Applicable	<p>The image that appears when the Desktop Client application starts up, in the Help > About window, and in the Scan window when no check images are being displayed. Provide the full path to the image or click Browse to navigate to the image on your system.</p> <p>This image must have the same file name and dimensions as the default image.</p> <p>splash screen image.gif</p> <p>Min: 515 x 150 pixels</p> <p>Max: 555 x 550 pixels</p> <p>Less than or equal to 1MB in size</p>
Small Windows Icon*	Used	Not Applicable	Not Applicable	Not Applicable	<p>The small icon that appears in the Desktop Client title bar and file management applications. Provide the full path to the image or click Browse to navigate to the image on your system.</p> <p>This image must have the same file name and dimensions as the default image:</p> <p>small windows icon.gif</p> <p>16 x 16 pixels. The image will be converted to a small Windows icon on the client.</p> <p>Less than or equal to 1MB in size.</p>

Field	Desktop Client	Web Client	Receivables Client	Consumer Client	Description
Web Client Logo	Not Applicable	Not Applicable	Used	Used	<p>The logo that appears in the header of Web Client. Provide the full path to the image or click Browse to navigate to the image on your system.</p> <p>This image must have the same file name and dimensions as the default image:</p> <p>wk. logo.gif</p> <p>182 x 38 pixels</p> <p>Less than or equal to 1MB in size</p> <p>The organization can choose either to use the logo specified here, or if they prefer to make the branded logo available on the login page, they can work with their service representative to provide a logo that will be used during the deployment process.</p>
License Requires Acceptance by User	Used	Used	Used	Used	<p>Select the check box to require that users acknowledge the License Message text before continuing. When this box is selected, Accept and Decline buttons appear on the License Message in the application.</p>

- Click OK to save the information.

Configuring Report Branding

Use System Manager to modify the branding that appears in the NetCapture Portal server reports for the selected organization. Server report branding options include background colors and the logo.

You can customize branding for any organization, whether it be a Service Provider, Bank of First Deposit, Correspondent Bank, or Customer. Child organizations do not inherit report branding settings from their parent organizations. If you want a Customer organization to have server report branding, you must define the branding for that particular Customer.

If you do not customize branding in System Manager, the server reports will use the default Finastra branding provided in the system.

Report branding applies only to the reporting accessed through NetCapture Portal, it does not apply to the Web Client Server Reporting application.

Requirements for Configuring Report Branding

You must define the Web Client branding before you can edit the branding for reports. For information about Web Client branding, see *Configuring Branding*.

Obtain the information specified from the table in Step 5 in *Steps for Configuring Report Branding* before you configure report branding in System Manager.

Steps for Configuring Report Branding

To configure report branding, do the following:

1. In System Manager, click the Organization Management link.
2. In the organization tree, select the organization for which you want to configure branding.
3. Click the Branding tab.
4. Locate the brand that you want to modify and under the Report Branding column heading, click the Edit link.

The Edit Report Branding dialog box appears.

Report Branding

Logo
Size is 199 x 32
Required filename is logo.gif
Note: To see the new image in the example page to the right, you must first save your changes you have made to this page.

Banner Background
Tab Background
Menu Background
Info Background
Content Background

netCapture Business
Main Reporting Logou

Logged in as: Reporting

Report: *
Deposit By Customer

Customer: *
Selected Organization:
Customer 2

Select Start Date & Time: *
1/13/2005 0:01 AM
(mm/dd/yyyy hh:mm AMPM)

Select End Date & Time: *
1/13/2006 4:49 PM
(mm/dd/yyyy hh:mm AMPM)

Records Per Page: * 20

Submit

* required

Report Detail:

Account	Account #
Account 2	123456

Results: 1 - 1 of 1

* required

OK Cancel

5. Modify the desired fields (fields marked with an asterisk [*] are required).

Note: The changes you make appear in the sample page on the right side of the dialog box. You can use the sample page to experiment until you achieve the look you want. Make sure you view the results before finalizing the branding to ensure the page is readable with the colors you have chosen.

Field	Description
Logo	<p>The logo that appears in the upper left corner of the server reports window. Provide the full path to the image or click Browse to navigate to the image on your system.</p> <p>This image must have the same file name and dimensions as the default image: logo.gif 199 x 32 pixels</p> <p>Note: To see the logo in the sample page on the right, you must first save the changes you have made by clicking OK.</p>
Background Color Fields:	<p>You can select a color using two different methods:</p> <ul style="list-style-type: none"> Enter # and then the six-digit hexadecimal value for the color you want. Click the [...] button to display a color palette from which you can select a color. <p>When you choose a color, the color is on the sample page on the right side of the screen.</p>
Banner Background	The color of the background at the top of the page behind the logo.
Tab Background	The color of the background on the tabs in the Portal Reporting area.
Menu Background	The color of the background on the currently-selected tab in the Portal Reporting area.
Info Background	The color of the background of the area where the user enters report search criteria.
Content Background	The color of the background of the report content area. This is the color behind the actual report.

6. Click OK to save the information.

Configuring Report Parameters

You can define the maximum number of days' worth of data included in each type of report. These parameters are defined for the Bank of First Deposit and apply to all child organizations associated with the Bank of First Deposit.

Requirements for Configuring Report Parameters

Before you begin, decide how many days' worth of data you want to appear in each type of report. The maximum is 31 days. You should set these values to the minimum required by your organization's business policies and procedures. For example, if your policy is to print a report of all deposits made by a customer once each business day, then you should set the Deposit by Customer report limit to 1 day. Keeping these values as small as possible will help minimize the impact that reporting has on system performance.

Reports with a maximum of 31 days are summary reports and do not include detailed information. Reports with a maximum of 5 days include detailed information (for example, Deposit by Customer includes the high-level deposit information as well as details about all the deposits and items for that customer that meet the report criteria).

You can define a different maximum value for the following two versions of the reports:

- Reports generated as PDF files

- Reports as viewed on the screen or saved as CSV files

Note: For descriptions of the available types of reports, see the *Reporting User Guide*.

Steps for Configuring Report Parameters

To edit the report parameters, do the following:

1. In System Manager, click the Organization Management link.
2. In the organization tree, select the Bank of First Deposit.
3. Click the Operational Parameters tab.
4. Under Report Parameters, click Edit.

The Edit Reporting Operational Parameters dialog box appears.

	PDF Date Range Limit	Report Date Range Limit
Deposit By Organization: *	31 Days	31 Days
Deposit By Bank: *	31 Days	31 Days
Deposit By Account Group: *	5 Days	31 Days
Deposit By Customer: *	5 Days	31 Days
Deposit Status: *	31 Days	31 Days
Customer Deposit Status: *	31 Days	31 Days
Users Deposit Status: *	31 Days	31 Days
Item Research: *	1 Days	31 Days
Audit and Billing Report: *	31 Days	31 Days

5. Modify the desired fields.

Field	Description
PDF Date Range Limit	For each type of report, enter the number of days' worth of data you want to appear in the reports generated as PDF files. The maximum is 31 days.
Report Date Range Limit	For each type of report, enter the number of days' worth of data you want to appear in the reports generated on screen or saved as .csv files. The maximum is 31 days.

6. Click OK to save the information.

Configuring Security Profiles

Security profiles are groups of settings that define the restrictions that determine how and when applications can be accessed by users. You can assign a particular profile to an organization or user.

This section describes how to configure security profiles. For information about assigning profiles to organizations, see *Assigning a Security Profile to an Organization*.

Requirements for Configuring Security Profiles

Before you begin, obtain information about how your organization wants to restrict access to applications, including the following:

- Application timeout requirements
- Access time requirements
- Password requirements
- User deletion requirements

For information about how default security settings are configured when upgrading from 5.1 to 5.2, see the *NetCapture Platform System Manual*.

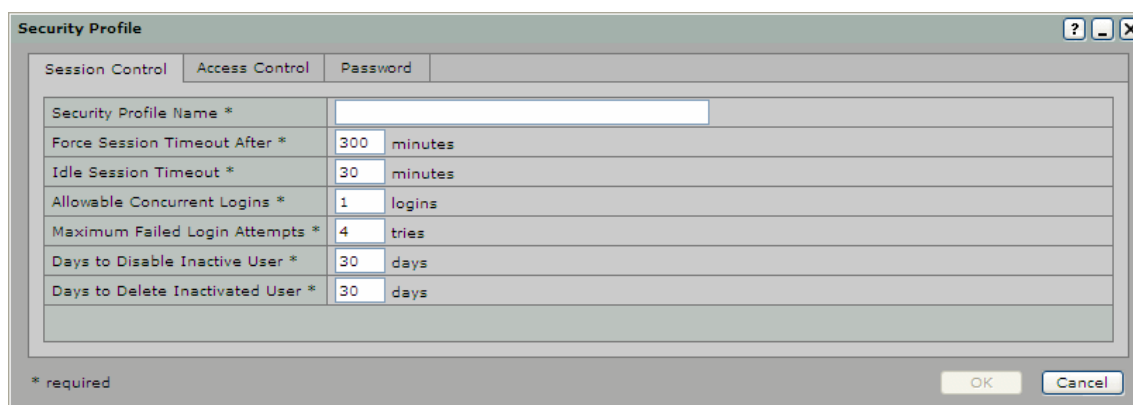
Steps for Configuring Security Profiles

To configure a security profile, do the following:

1. In System Manager, click the Security link.
2. Click the Add icon, or locate an existing security profile that you want to modify and click the Edit icon.

Note: You can also delete a security profile by clicking the Delete icon for the profile.

The Security Settings dialog box appears.



3. On the Session Control tab, edit the following settings as desired.

Field	Description
Security Profile Name*	Provide a unique name for the security profile. The name can be up to 100 characters long. Users who are assigning this profile to organizations or to other users will identify profiles by the name you specify here.
Force Session Time-out After*	A period of time after which users are required to re-enter log in information, in minutes.
Idle Session Time-out*	A period of time where there is no discernible mouse or keyboard activity after which users are required to re-enter log in information, in minutes.
Allowable Concurrent Logins*	The number of additional times a user may be logged in to the Desktop Client application, after the initial login. For example, if this value is set to two, the user may log in for three concurrent sessions. The Desktop Client supports 0 - 9 concurrent logins. Web Client does not allow concurrent logins.

Field	Description
Maximum Failed Login Attempts*	The number of times users are allowed to attempt to log in to an application unsuccessfully, after which their statuses are changed to Inactive and they are not allowed access. Note: If you are using an external authentication plug-in, then this setting is ignored and accounts are not deactivated. The plug-in is expected to handle repeated failed login attempts.
Days to Disable Inactive User	The number of days a user cannot log in to the system before the user's status is automatically changed to inactive. This can be anywhere from 0 to 365 days. If the number of days is set to zero, inactive users will not be disabled. If your organization has chosen not to install this feature in the database, this setting is non-functional.
Days to Delete Inactivated User	The number of days a user's status in the system can be inactive before the user is automatically deleted. This can be anywhere from 0 to 360 days. If your organization has chosen not to install this feature in the database, this setting is non-functional. Once a user account is deleted from the system, it cannot be recovered.

- Click the Access Control tab.

The screenshot shows the 'Security Profile' dialog box with the 'Access Control' tab selected. At the top, there are tabs for 'Session Control', 'Access Control', and 'Password'. Below these, a dropdown menu shows 'Allowable Login Times for GMT-06:00 Mountain Daylight' with a 'Select Time Zone' button. A note states: '(Use military time in hh:mm format for start and end times)'. The main area is a grid for days of the week (Sunday through Saturday). Each day has two rows of 'Start' and 'End' time slots. For Monday through Friday, the first row is checked and set to 08:00 and 20:00. The second row is empty. For Sunday and Saturday, both rows are empty. At the bottom left, it says '* required'. At the bottom right are 'OK' and 'Cancel' buttons.

- On the Access Control tab, edit the following settings as desired (fields marked with an asterisk [*] are required):

Note: These times define the days/hours during which users are allowed to log in to the system. Users who are already logged in to the system when an allowable login time expires are not forced to log out. For example, if the end time is 5:00 p.m., a user who logged in at noon and remains logged in will not be forced out of the system at 5:00 p.m.

Field	Description
Allowable Login Times for ____ Select Time Zone	Select the time zone for which you are defining access times. This should be the time zone of the organization or user for which you are defining the security profile.

Field	Description
Start and End times	<p>You can define up to two access time periods per day by defining a start time and an end time for each access period. Select the check box to activate the text fields.</p> <p>Specify times using military time format. Do not use a colon.</p> <p>Example 1: A user's shift is from 9:00 p.m. until 6 a.m. each business day. You would define a start time of 2100 for each day, starting with Sunday and ending with Thursday, and an end time of 0600 for each day, starting with Monday and ending with Friday.</p> <p>Example 2: A user works Monday through Friday from 8:00 a.m. until 5:00 p.m. with an hour lunch break. You can define two time periods for each day: a start time of 0800 and an end time of 1200, and a start time of 1300 and an end time of 1700.</p> <p>Note: Selecting a check box without entering specific times in the text fields will grant all-day access (00:00 to 23:59). Clearing a check box will clear any times defined in the text fields.</p>

- Click the Password tab.

- On the Password tab, edit the following settings as desired (fields marked with an asterisk [*] are required):

Note: These settings apply only to the passwords created in System Manager. These settings do not apply to any passwords created and used by an external authentication server.

Field	Description
Minimum Password Characters Length*	<p>The minimum number of characters users are required to include in their passwords. The default is 6. The minimum allowable value for this field is 5, and the maximum is 15.</p> <p>Note that the minimum allowable value for DNC is 8, and the maximum is 15.</p>
Minimum Alphabetic Characters in Passwords*	<p>The minimum number of alphabetic characters users are required to include in their passwords.</p> <p>The default is 1. If you specify 0 (zero), then users do not have to include alphabetic characters in their passwords.</p>

Field	Description
Minimum Numeric Characters in Password*	The minimum number of numeric characters users are required to include in their passwords. The default is 1. If you specify 0 (zero), then users do not have to include numeric characters in their passwords.
Minimum Special Characters in Password*	The minimum number of special characters users are required to include in their passwords. The default is 0. If you specify 0 (zero), then users do not have to include special characters in their passwords.
Days to Keep User Password History*	The number of days for which the system stores users' previously-used passwords, to enforce rules that do not allow users to repeat the use of passwords. The default is 30.
Password Expiration*	The number of days after which users' passwords expire and must be changed. The default is 90.
Password Expiration Notice*	The number of days prior to expiration of the user's password that the user will be notified of the pending expiration. The default is 7.
Password Change Allowed	Specifies whether or not users can change their own passwords. If this is set to no, then users can only change their passwords when prompted by the system to do so.
Maximum Password Change Attempts*	The maximum number of times a user is allowed to unsuccessfully attempt to change their password in a single session. The default is 4.
Disallowed Passwords	You can add words to the default disallowed password list. Disallowed passwords are words/phrases that users are not allowed to specify as passwords for authentication to the system. There is no limit on the number of disallowed password entries you add to the system. Disallowed password entries cannot exceed 15 characters in length. <ul style="list-style-type: none"> To add words, type or paste the words into the Add Disallowed Passwords text field, ensuring there is a hard return after each word (so each word appears on its own line). Click the arrow button [>] to move the words to the Disallowed Password List text field. To delete words, select them in the Disallowed Password List text field (use the Shift or Ctrl keys to select multiple passwords), then click the Delete button.

- Click OK to save the security profile.

Assigning a Security Profile to an Organization

Once you have configured security profiles, you can assign them to organizations. If you do not specify a security profile for an organization, it will by default use its parent organization's profile. If you do not specify a security profile for the parent organization, it will use the default security profile that is configured in the system.

You can also assign security profiles to specific users. The profile assigned at the user level will override the profile assigned at the organization level. For more information, see *Editing User Settings*.

Requirements for Assigning a Security Profile to an Organization

Before you assign security profiles to organizations, you should understand how the profiles are configured. Security profiles control system access and password requirements. Make sure you assign the correct profile to each organization according to your organization's security policies.

Steps for Assigning a Security Profile to an Organization

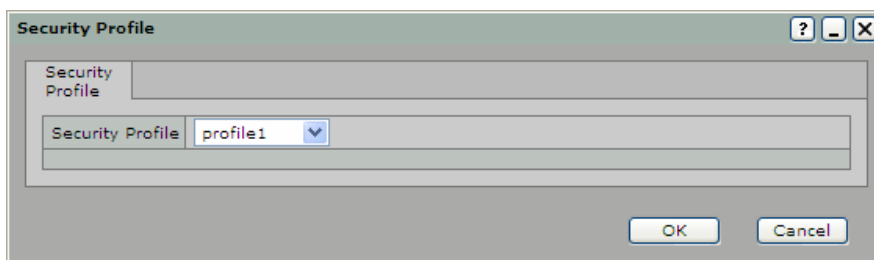
Do the following to assign a security profile to an organization:

1. In System Manager, click the Organization Management link.
2. In the organization tree, select the organization for which you want to assign a security profile.
3. Click the Security tab.

The screen shows the profile that is currently assigned to the selected organization.

4. To change the assigned security profile, click the Edit icon.

The Security Settings dialog box appears.



5. In the drop-down box, select the profile you want to assign to the selected organization.
6. Click OK.

Configuring Dual Control

Use System Manager to configure the dual control feature. When this feature is configured, Remote Users that have a deposit limit set must have any deposits they make in Desktop Client that exceed that limit reviewed and approved by a Remote Reviewer before the deposit can be submitted.

Note: This procedure refers to the default roles Remote User and Remote Reviewer. If you are not using the default roles in the system, then instead of the Remote User role, you must assign a role that has the Create Deposit privilege, and instead of the Remote Reviewer role, you must assign a role that has the Review Remote Deposit privilege.

Dual control can be set up at the bank or customer organization level. If the rule is set up at the bank level, the Dual Control Deposit Amount rule will apply to all child organizations of that bank. For the Dual Control Deposit Amount Rule to take effect, Remote Users must have deposit limits set.

Note: Dual control does not apply to Web Client, only Desktop Client.

Requirements for Configuring Dual Control

Obtain the following information before you configure dual control.

- Identify an organization that will have the Dual Control Deposit Amount rule set
- Review the Default Roles and Privileges Matrix
- Identify Remote Users who will have deposit limits set
- Identify Remote Reviewers for the organization

We recommend that you create at least two Remote Reviewers in order to ensure that there is always someone available to review and approve deposits that require review before being submitted.

Steps for Configuring Dual Control

Do the following to configure dual control:

- Configuring the Dual Control Deposit Amount Rule
- Configure Remote Users for Dual Control
- Configure Remote Reviewers

Configuring the Dual Control Deposit Amount Rule

Do the following to configure the Dual Control Deposit Amount rule:

1. In System Manager, click the Organization Management link.
2. In the organization tree, select the organization for which you want to configure the Dual Control Deposit Amount rule.
3. Click the Rules tab.
4. Click the Add icon.
5. The Add Rule dialog box appears.

6. Select the following for each field (fields marked with an asterisk [*] are required):

Field	Description
Application Type*	Remote
Rule*	Dual Control Deposit Amount
Condition*	Is Greater Than the Deposit Limit (this is the only condition available under the Dual Control Deposit Amount rule)
Action*	Review (this is the only action available under the Dual Control Deposit Amount rule)
Status	Active (this field is not marked as required, but you must set the rule to active so that it will be used)

7. Click OK to save the rule.

Configure Remote Users for Dual Control

Remote Users create and submit deposits. When the Dual Control Deposit Amount rule is active and a Remote User has a deposit limit assigned, a Remote Reviewer must review deposits that exceed the Remote User's deposit limit before the deposit can be submitted.

Do the following to configure Remote Users for dual control:

1. Create a new user or edit an existing user for whom you want to set a deposit limit.
See *Creating Users* for detailed instructions.
2. In the Deposit Limit field, enter the maximum deposit limit for this user.

This is the maximum amount of a single deposit that this user is allowed to submit in the Desktop Client. Deposits that exceed this amount require review by a Remote Reviewer.

The deposit limit maximum amount is \$99,999,999.99. Setting the amount to \$0 will cause all deposits to require review. Set the deposit limit according to your institution's security policies.

Note: The Deposit Limit does not affect the ability of users who have the Remote Reviewer role to review and approve deposits. Remote Reviewers can review and approve deposits of any amount.
3. Assign the Remote User role to this user (or any role that contains the Create Deposit privilege).

Configure Remote Reviewers

Remote Reviewers review deposits that exceed a Remote User's deposit limit and approve them for submission.

Do the following to configure Remote Reviewers:

1. Create a new user or edit an existing user to whom you want to assign the Remote Reviewer role.
See *Creating Users* for detailed instructions.
2. Assign the Remote Reviewer role to the user (or any role that has the Review Deposit privilege).

Creating Account Groups

You can set up account groups that allow you to group together organizations and accounts. Setting up groups makes it simple to generate cumulative report data for the group. For example, if you want to generate a single report that contains the deposit status for all your customer organizations, you can create an account group that contains all of the accounts belonging to your customers.

You can group together any organizations or accounts that belong to the top-level organization (Bank of First Deposit or Service Provider) for which you are assigned the Account Groups Administrator role.

- Creating Groups
- Adding Accounts to the Group
- Adding Users to the Group
- Viewing Group details

Creating Groups

Do the following to create an account group:

1. In System Manager, click the Account Grouping link.
2. Click the Add icon to create a new group, or locate an existing group that you want to modify and click the Edit icon.

Note: You can also delete a group by clicking the Delete icon.

The Account Group dialog box appears.

3. Click the Group tab.
4. Enter the following information in the fields (fields marked with an asterisk [*] are required):

Field	Description
Group Name*	A name for the group. This name appears in the Reporting area to help users filter reports.
Group Description*	A description of the group.

5. Continue with the next section.

Adding Accounts to the Group

Do the following to add accounts to the account group:

1. Click the Add Accounts tab.

2. Search for the accounts you want to add to the group by doing the following:
 - a. In the Account Search field, enter the name/number or portion of the name/number associated with the accounts you want to find, based on what you selected for the Search Type.
 - b. For example, to find all accounts for a customer organization named John's Flowers, enter either the entire customer name or a portion of the name in the Account Search field. (You do not need to use * in the search criteria.)
 - c. In the Search Type field, choose the criteria you want to use to search for accounts. Choose Account Number, Account Name, or Customer Name.
 - d. Click the Search button.

The accounts matching the search criteria appear in the top panel under Account Search Results.

3. In the top panel, select the accounts you want to add to the group. You can select more than one account by pressing and holding down the Ctrl key while you select the desired accounts.
4. Click the right arrow button [>] to add the accounts to the group. The accounts now appear in the bottom panel under Account(s) Selected.

Continue with the next section, Adding Users to the Group.

Adding Users to the Group

Do the following to add users to the account group:

1. Click the Add Users tab.

The screenshot shows the 'Account Group' dialog box with the 'Add Users' tab selected. The 'User Search' field contains 'john' and the 'Search Type' is set to 'First Name'. The 'User Search Results' table shows one result: 'smith, john' with username 'johnsmith' and organization 'ABC Company'. The 'User(s) Selected' table shows one result: 'doe, john' with username 'john.doe@abccompany.com_compi...' and organization 'ABC Company'. The dialog has tabs for 'Group', 'Add Accounts', 'Add Users', 'View Accounts', and 'View Users'. It also has 'OK' and 'Cancel' buttons at the bottom right.

2. Search for the users you want to add to the group by doing the following:
 - a. In the User Search field, enter the name or portion of the name associated with the users you want to find, based on what you selected for the Search Type.
 - b. For example, to find all users whose last names begin with W, enter W in the User Search field. (You do not need to use * in the search criteria.)
 - c. In the Search Type field, choose the criteria you want to use to search for users. Choose Username, First Name, Last Name, or Customer.
 - d. Click the Search button.

The users matching the search criteria appear in the top panel under User Search Results.

3. In the top panel, select the users you want to add to the group. You can select more than one user by pressing and holding down the Ctrl key while you select the desired users.
4. Click the right arrow button [>] to add the users to the group. The accounts now appear in the bottom panel under User(s) Selected.

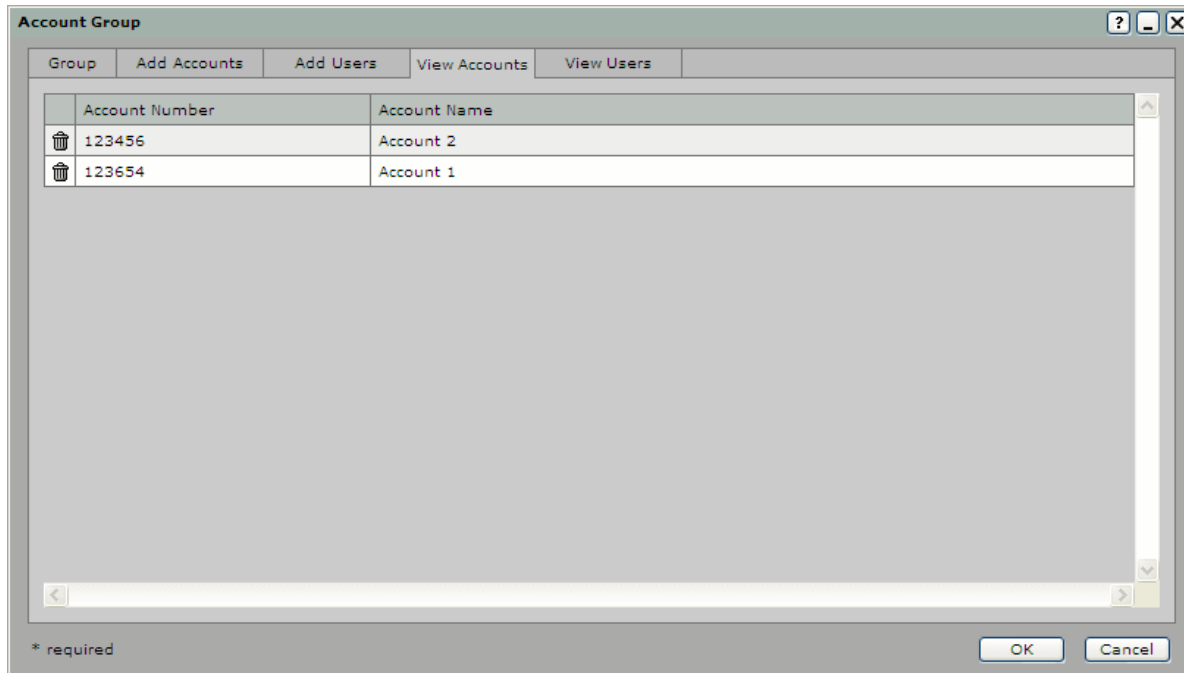
5. Click OK.

The account group is saved. It is now available to the users you assigned.

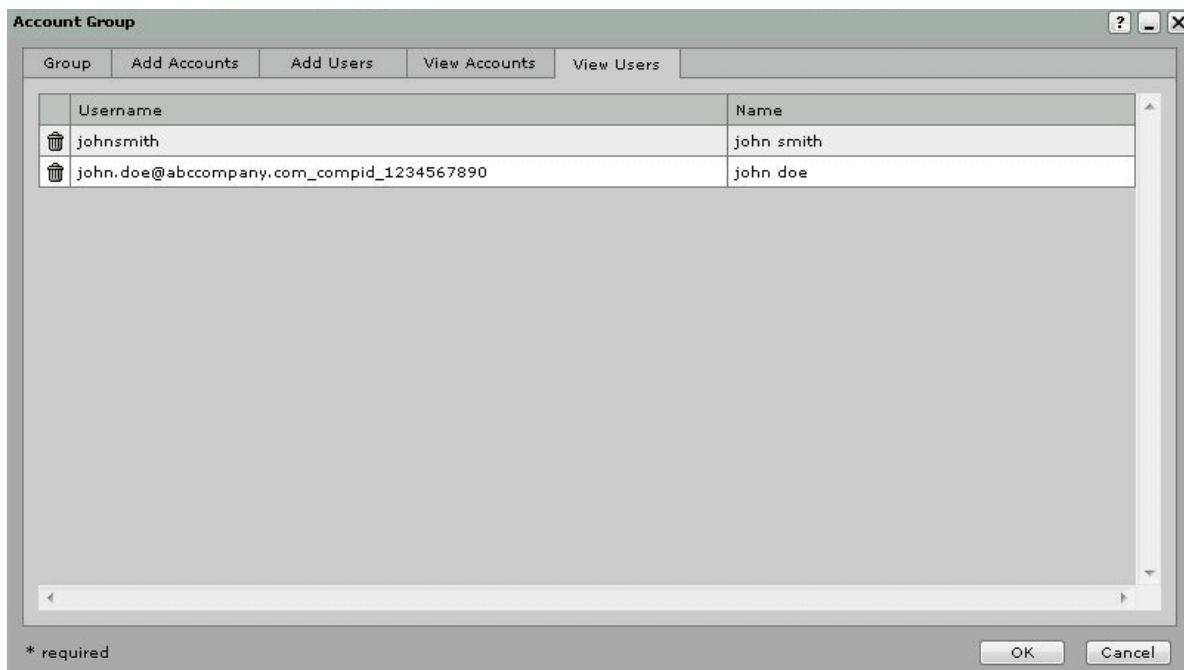
Viewing Group details

You can view the complete list of accounts and users associated with the group by clicking the View Accounts and View Users tabs in the Account Group dialog box.

The image below shows the View Accounts tab.



The image below shows the View Users tab.



Remove accounts or users from the group by clicking the Delete icon .

Adding/Editing Locations

You can edit an existing Bank of First Deposit, Correspondent Bank, Customer, or account's location information, and you can add new locations for an organization.

Note that you can create locations for both organizations and accounts. When viewing locations, the column **Belongs To** specifies whether the location was created for an organization or an account.

Requirements for Adding/Editing Locations






The organizations you are allowed to edit depend on your role in the system. See *Understanding User Roles and Privileges* for details.

Note: Locations are informational only. Users and deposits are not associated with the configured locations. Users are associated with the Customer organization and deposits are associated with the Customer organization and depository account.


Steps for Adding/Editing Locations

To add a new location or edit an existing location's information, do the following:

1. In System Manager, click the Organization Management link.
2. In the organization tree, select the organization for which you want to add or edit a location.
3. To add or edit a location for an organization, click the Locations & Contacts tab.

Bobs Printing									
General	Branding	Operational Parameters	User Defined Fields	Locations & Contacts	Accounts	Rules	Users	Security	Adjustment Processing
	Name	Primary	Location Address	Description	Contacts	Belongs To			
	Park City	<input checked="" type="checkbox"/>	USA		 Show contacts	Account			
	Primary	Name	Contact Address	Email	Phone/Fax	Type			
	<input checked="" type="checkbox"/>	Jane Smith	USA	jane@here.com		Business			

The primary location has a check mark under the Primary column.

4. To add or edit a location for an account, click the Accounts tab, then click the  icon for Account Locations & Contacts. See the figure above.
5. To add a new location, click the Add icon.
6. To edit an existing location, locate the one you want to edit and click the Edit icon for the location.

Note: You can delete a location by clicking the Delete icon. Deleting a location also deletes all the contacts associated with that location. You cannot delete the primary location.

The Add/Edit Location dialog box appears.

7. Modify the desired fields (fields marked with an asterisk [*] are required):

Field	Description
Location Name*	A name for this location; for example, corporate headquarters.
Primary	Indicates whether this is the primary location for the organization. Each organization must have one primary location. If the current location is designated as the primary location, you cannot remove this setting. To change the primary location, open a non-primary location for editing and select the Primary box for that location. The primary designation will automatically be removed for all other locations.
Country	The country where the organization is located.
Address 1	The street address for the organization.
Address 2	Additional address information for the organization, such as a suite number.
Address 3	Additional address information for the organization.
Address 4	Additional address information for the organization.
City	The city where the organization is located.
State/Province	The state or province where the organization is located.
Zip/Postal Code	The ZIP or postal code for the organization.
Description	An optional description for the organization.

8. Click OK to save the location information.

Adding/Editing Contacts

You can edit an existing Bank of First Deposit, Correspondent Bank, Customer, or account's contact information, and you can add new contacts for an organization.

Note that you can create contacts associated with locations for either organizations or accounts. When viewing locations, the column *Belongs To* specifies whether the location was created for an organization or an account.

Requirements for Adding/Editing Contacts

The organizations you are allowed to edit depend on your role in the system. See *Understanding User Roles and Privileges* for details.

Steps for Adding/Editing Contacts

To add a new contact or edit existing contact information, do the following:

1. In System Manager, click the Organization Management link.
2. In the organization tree, select the organization for which you want to add or edit a contact.
3. To add or edit a location for an organization, click the Locations & Contacts tab.

Bobs Printing									
General	Branding	Operational Parameters	User Defined Fields	Locations & Contacts	Accounts	Rules	Users	Security	Adjustment Processing
	Name	Primary	Location Address	Description	Contacts	Belongs To			
	Park City	<input checked="" type="checkbox"/>	USA		Show contacts	Account			
	Primary	Name	Contact Address	Email	Phone/Fax	Type			
	<input checked="" type="checkbox"/>	Jane Smith	USA	jane@here.com		Business			

Note: Expand the list to view the contacts for a particular location by clicking [+] next to Show contacts.

The primary contact has a check mark under the Primary column.

4. To add or edit a location for an account, click the Accounts tab, then click the icon for Account Locations & Contacts. See the figure above.
5. To add a new contact for a location, click the Add icon for that location.
6. To edit an existing contact, locate the one you want to edit, then click the Edit icon for the contact.

Note: You can delete a contact by clicking the Delete icon. You cannot delete the primary contact.

The Add/Edit Contact dialog box appears.

Edit Account Contact

Contact

First Name * Jane

Last Name * Smith

Contact Type Business

Primary Contact ☒

Deposit Review Notifications ☒ Account Level Only ☒

Email jane@here.com (name@company.com)

Country UNITED STATES

Address 1

Address 2

Address 3

Address 4

City

State/Province -- select one --

Zip/Postal Code

Phone +1 ext.

Fax +1 ext.

(Numbers only - Area Code/City Code Required)

* required

OK Cancel

7. Modify the desired fields (fields marked with an asterisk [*] are required):

Field	Description
First Name*	The contact person's first name.
Last Name*	The contact person's last name.
Primary Contact	Indicates whether this is the primary contact for the location. Each location must have one primary contact. If the current contact is designated as the primary contact, you cannot remove this setting. To change the primary contact, open a non-primary contact for editing and select the Primary box for that contact. The primary designation will automatically be removed for other contacts.
Deposit Review Notifications	Select this box if you want this contact to receive notification of item adjustments and rejections by email. The check box is selected by default for the primary contact. If the Account Level Only box is selected, contacts set up at the depository account level will receive notifications only for deposits made to that account. Note that this check box only appears for account-level contacts, not for organization-level contacts. Note: When the Primary Contact check box is selected the Deposit Review Notifications check box is automatically selected and is unavailable for edit.
Account Level Only	If the Account Level Only box is selected, contacts set up at the depository account level will receive notifications only for deposits made to that account. Note that this check box only appears for account-level contacts, not for organization-level contacts.
Deposit Confirmation Notifications	Select the check box if you want the contact to receive email notifications confirming that deposits have successfully been submitted. Note that if you check this box, this individual will receive an email message for every deposit submitted on behalf of this customer organization.
Contact Type*	Indicate the type of contact this person is. This can be Billing, Business, or Technical.
Email*	The email address at which this contact person can be reached. You can enter multiple email addresses for the contact by separating them with semicolons. For example: john@example.com ; john@bankabc.com.
Country	The country in which the contact is located.
Address 1	The street address at which this contact person may be reached.
Address 2	Additional address information at which this contact person can be reached, such as a suite number.
Address 3	Additional address information for this contact person.
Address 4	Additional address information for this contact person.
City	The city in which the contact is located.
State/Province	The state or province in which the contact is located.
Zip/Postal Code	The zip or postal code for the contact.

Field	Description
Phone	The phone number at which the contact can be reached, including an extension. Enter only numeric characters.
Fax	The fax number at which the contact can be reached. Enter only numeric characters.

- Click OK to save the contact information.

Adding/Editing Accounts

You can add an account or edit an existing account for an organization.

Requirements for Adding/Editing Accounts

Note that you can edit existing accounts, but you cannot delete accounts (because they must be maintained for historical auditing purposes).

You are allowed to enter multiple accounts that have the same account number and route/transit number as long as each account has a unique account name. You may want to do this if you want multiple client locations to be able to make deposits to the same account, but you want to be able to distinguish between the locations for reporting purposes.

Steps for Adding/Editing Accounts

To add an account or edit account information for an organization, do the following:

- In System Manager, click the Organization Management link.
- In the organization tree, select the organization for which you want to add or edit an account.
- Click the Accounts tab.

The list of accounts for the organization appears.

General	Branding	Operational Parameters	User Defined Fields	Locations & Contacts	Accounts	Rules	Users	Security	Applications	Adjustment Processing
Account List										
	Account Number	Account Name	Route/Transit	Reference ID	Aux On-Us	New Account	Status	Deposit Slip	Locations/Contacts	Rules
	11223344	ABC Operating Acct	123456780	11223344		✓	Active	OPTIONAL		
	10789111	Account 10	124000052	131313			Active	NOT USED		
	121212	Account 12	124000052	131313			Active	NOT USED		
	5554789	Biltmore street	124000052	131313			Active	NOT USED		
	4325557	Branch C account	124000052	131313		✓	Active	OPTIONAL		
	15999887	Byways account	124000052	131313			Active	NOT USED		
	45687017	External	124000052	131313			Active	NOT USED		
	16489718	Highlander account	124000052	131313			Active	NOT USED		
	33366655	Incidentals	124000052	131313			Active	NOT USED		
	80001487	Internal	124000052	131313			Active	NOT USED		
Results: 1 - 10 of 17										
Next										
Records Per Page * 10 Update										

Note: If the number of accounts for the organization exceeds the number specified in the Records Per Page field, you will need to increase the number in that field or browse to the remaining results using the arrow buttons in order to see all the accounts for the organization.

- Click the Add icon to create a new account, or locate an existing account that you want to modify and click the Edit icon.

The Add or Edit Account dialog box appears.


- Modify the desired fields (fields marked with an asterisk [*] are required):





Field	Description
Account Number*	The account number for the organization's account to which deposits can be made.
Account Name	A name to help you and users of Web Client identify this account.
Route/Transit*	The route/transit number for the account you are adding. A default route/transit number is pre-populated based on the route/transit number configured for the initial account configured when the parent organization was created.
Route/Transit Number Verified*	This field appears only if you have entered an invalid route/transit number. Select the check box if you want to accept the route/transit number and use it for the account even though it has failed validation. If you do not want to accept the invalid route/transit number, re-enter a valid route/transit in the Route/ Transit Number field.
Aux On-Us	The aux on-us number for the account you are adding.
Reference ID*	This is the ID you received from your Decision Gateway Administrator that links this account to the account set up in the Decision Gateway database. This ID can be up to 20 alphanumeric characters.
Status	This can be active or inactive. Active means the account is actively being used in the system. Inactive means the account is not actively being used in the system. The default is active.

Field	Description
Deposit Slip	<p>This determines how Web Client will handle deposit slips for this account. Required means a deposit slip is required to be submitted for each deposit. Not Used means deposit slips cannot be submitted. Optional means users can choose whether to use a deposit slip for each deposit they submit.</p> <p>The default is Optional.</p> <p>If you choose to use deposit slips, you may also want to set a scrutiny rule to flag deposits in which users have changed an item's type (from deposit slip to debit item, or vice versa). See <i>Managing Scrutiny Rules</i> for more information.</p>
New Account	<p>Indicates that this is a new account, and that Deposit Review Agents should review all deposits made to this account in Deposit Review. If the check box is selected, all deposits will be flagged for review.</p> <p>This check box is selected by default.</p> <p>In order to use this option, the account must have the Is New Account scrutiny rule configured. See <i>Managing Scrutiny Rules</i> for details.</p>
Clear New Account flag	<p>The number of days the New Account flag will remain active on a depository account. This can be 0-999 days. If it's set to zero (0), the New Account flag will never be cleared.</p> <p>The time period calculation will begin at the time the first deposit is made. For instance, if the New Account check box is selected, the inactivation date is set to 10, and the user begins making deposits at 1 p.m. on the 1st of the month, then the New Account flag will be cleared on the 10th at 1 p.m. MT.</p> <p>Note: The inactivation time will always be displayed in Mountain Time.</p>

- If you are adding a new account, click Save & New to save the account but leave the Add/Edit Account dialog box open so you can create another new account. Click Save & Close to save the account and exit the Add/Edit Account dialog box.

If you are editing an existing account, click OK to save the changes.

- If you want to add or edit a location or contact for this account, click the  icon for Account Locations & Contacts or click the Account Locations & Contacts tab.

Account List		Account Locations & Contacts		Account Rules	
Locations for account number 12678941					
	Name	Location Address	Description	Contacts	
	Remote	1000 West 3477 South Salt Lake City, UT 84125 USA		<input type="checkbox"/> Show contacts	
	Primary	Name	Contact Address	Email	Phone/Fax
	<input checked="" type="checkbox"/>	Mary Hong	1000 West 3577 South Salt Lake City, UT 84125 USA	mary@branch.com	phone: 8014443333
					Type

Note: You can expand the list to view the contacts for a particular organization by clicking [+] next to Show contacts.

- Edit the locations and contacts for the account as desired.

Note: Any locations or contacts you add for the account are also displayed for the related organization. See the sections *Adding/Editing Locations* and *Adding/Editing Contacts* for details about adding and editing locations and contacts.

- If you want to edit scrutiny rules for this account, click the icon for Account Rules, or click the Account Rules tab.

ADummyCustomer

General	Branding	Operational Parameters	Locations & Contacts	Accounts	Rules	Users			
Account List		Account Locations & Contacts		Account Rules					
Rules for account number 000000001								Show All Rules	
	Application	Org Name	Org Type	Rule	Status	Condition	Start Value	End Value	Action
	Remote	Bank of First Deposit 1	BANK OF FIRST DEPOSIT	Bank On-Us	Inactive	Is Empty			Reject
	Remote	Bank of First Deposit 1	BANK OF FIRST DEPOSIT	Deposit Amount Threshold	Inactive	Is Greater Than or Equal to	10000		Set Flag
	Remote	Bank of First Deposit 1	BANK OF FIRST DEPOSIT	Capture Duplicate Item	Inactive	Is Found			Set Flag
	Remote	Bank of First Deposit 1	BANK OF FIRST DEPOSIT	Route/Transit Number	Active	Is Between	00000000	00000000	Reject
	Remote	Bank of First Deposit 1	BANK OF FIRST DEPOSIT	Route/Transit Number	Inactive	Is Between	32407950	32407960	Reject
	Remote	Bank of First Deposit 1	BANK OF FIRST DEPOSIT	Deposit Control Balance	Inactive	Does not Equal Deposit Total			Set Flag
	Remote	Bank of First Deposit 1	BANK OF FIRST DEPOSIT	Entered Amount	Inactive	Is Changed			Set Flag
	Remote	Bank of First Deposit 1	BANK OF FIRST DEPOSIT	Account Number	Inactive	Is New			Set Flag
	Remote	Bank of First Deposit 1	BANK OF FIRST DEPOSIT	Item Amount Threshold	Inactive	Is Less Than or Equal to	5000		Set Flag
	Remote	Bank of First Deposit 1	BANK OF FIRST DEPOSIT	Scanned Item	Inactive	Is Not Stamped			Set Flag

Note: You can filter the list of rules using the drop-down box on the right side of the screen. You can view all rules, only active rules, or only inactive rules.

10. Edit the rules for the account as desired.

Note: The only change you can make to existing rules is to change their status to active or inactive. See the section *Managing Scrutiny Rules* for details about editing rule status.

Forcing a Client User Logout

You can use this feature when a Desktop Client or Web Client user's session was terminated without logging out (during a power loss or network failure, for example) and the user is not allowed to log in because the session has not successfully been terminated. The Force Logout button resets the user's status at the Capture Gateway, allowing the user to log in again.

You can use this feature to force the logout of any user in the system, including NetCapture Portal users.

Note: This feature does not prevent users who are currently logged in to a client application from continuing their work. To log a user out and prevent them from using the Desktop Client or Web Client, see *Changing a User's Status*.

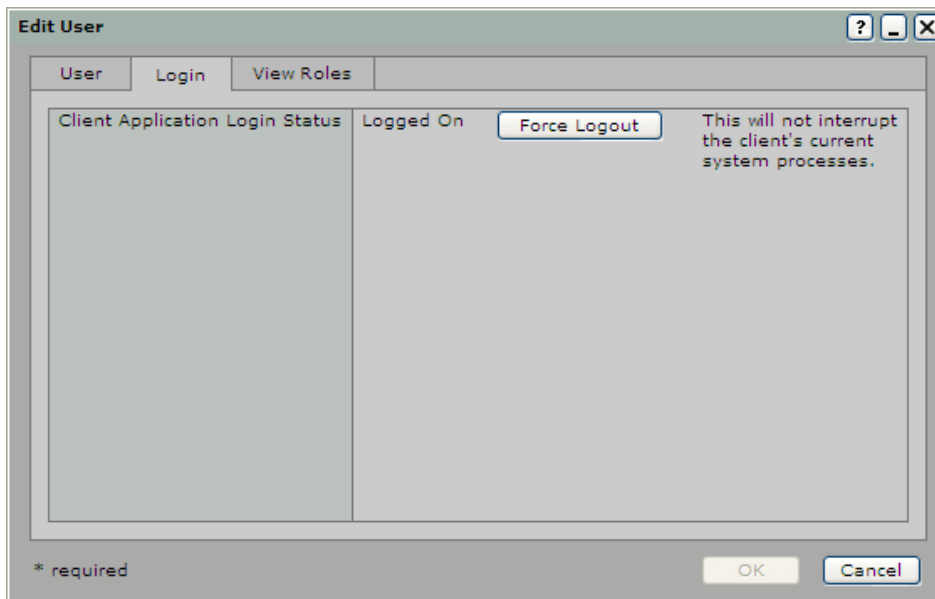
To force a logout, do the following:

1. In System Manager, click the Organization Management link.
2. Search for the user you want to force to log out.
3. Depending on how you completed the search, either click the user name or the Edit icon to edit the user.

The Edit User dialog box appears.

4. Click the Login tab.

On the Login tab, the Client Application Login Status is Logged On.



5. Click Force Logout.
6. The user is logged out of the client session.

Managing Licenses

System Manager provides a feature to help you keep track of the licenses you have purchased and distributed to customer organizations. It can also tell you how many licenses are in use and how many are free and available to use.

Requirements for Managing Licenses



Licenses can be purchased by bank organizations and distributed to any Customer organizations belonging to those banks. A license must be assigned for every Customer organization that is making deposits in the system.

Before you begin managing licenses in System Manager, you must obtain one or more license keys from Finastra. License management is available only for Service Providers, Banks of First Deposit, and Correspondent Banks.

Steps for Adding Licenses

To add seat licenses, do the following:

1. In System Manager, click the Organization Management link.
2. In the organization tree, click the bank organization for which you want to manage licenses.
3. Click the License Mgmt tab.

BOFD									
General	Branding	Operational Parameters	Locations & Contacts	Rules	Users	Security	Applications	License Mgmt	Adjustment Processing
	Org Name		Total Purchased	Total Distributed	Available				
	BOFD		500	350	150				
		Customer Name	Total Purchased	In Use	Available	Status			
		Pacific Branch	225	0	225	ACTIVE			
		South Bank	125	0	125	ACTIVE			

The License Mgmt tab displays the total number of seat licenses that your bank organization has purchased and entered into the system. When summed, the total seats for the Customer organizations will match the total seats distributed by the bank. The window also displays the number of licenses that are in use and available (not currently being used).

Note: It is possible for the number of available seats to be a negative number. This may occur if you have installed more Web Client workstations than you have purchased licenses for or if you make deposits for more Customer organizations than you have licenses for. In this case, you should comply with your billing agreement to purchase the appropriate licenses and add them to the system.

4. Click the Add icon.

The Add License Key dialog box appears.

A dialog box titled "Add License Key" with a single text input field labeled "Add License:". Below the field are "OK" and "Cancel" buttons.

5. In the Add License field, enter the license key that was provided to you by Finastra.
6. Click OK.

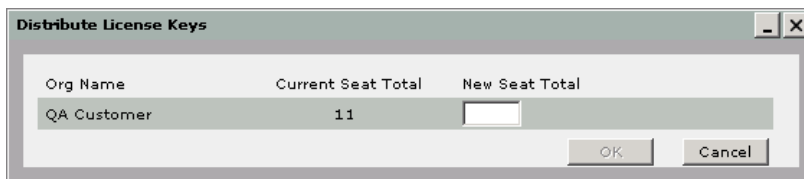
The Total Seats value is updated to add the number of seats covered by the new license key.

Steps for Changing License Distribution

To view or change the number of seats distributed to customers, do the following:

1. In System Manager, click the Organization Management link.
2. In the organization tree, click the bank organization for which you want to manage licenses.
3. Click the License Mgmt tab.
4. Under Distribution, click the Edit icon for the customer whose distribution you want to change.

The Distribute License Keys dialog box appears.

A dialog box titled "Distribute License Keys" containing a table with three columns: "Org Name", "Current Seat Total", and "New Seat Total". The first row shows "QA Customer" with a "Current Seat Total" of 11 and an empty "New Seat Total" field. "OK" and "Cancel" buttons are at the bottom right.

Org Name	Current Seat Total	New Seat Total
QA Customer	11	

The dialog box displays the number of seat licenses that are currently assigned to the customer (Current Seat Total).

5. To change the number of seat licenses assigned to the customer, enter a number in the New Seat Total field, then click OK.

The Total Seats and Available numbers are updated to reflect the change in license distribution.

4 Using Deposit Review

Deposit Review lets Deposit Review Agents and Banking Operations personnel review and approve deposits that are flagged for review before they are processed at the Decision Gateway. Deposit Review also enables the workflow management of review tasks by allowing Banking Operations personnel to manage deposit queues.

This section includes the following information:

- Introducing Deposit Review
- Reviewing Deposits in Deposit Review
- Managing Queues in Deposit Review

Introducing Deposit Review

This section includes the following information:

- Deposit Review User Privileges
- Deposit Review Overview
- Understanding the Deposit Review Window

Deposit Review User Privileges

Only qualified personnel are allowed access to Deposit Review. There are two different privileges that grant access to Deposit Review. The privileges assigned to you determine your level of access in the system:

- Update Deposit Review: Users with this privilege have access to review items and deposits. The default roles with this privilege are Deposit Review Agent and Banking Operations.
- Update Deposit Queue: Users with this privilege have access to review items and deposits that have been referred to them by users with the Update Deposit Review privilege, and to manage the queuing of deposits. The default role with this privilege is Banking Operations.

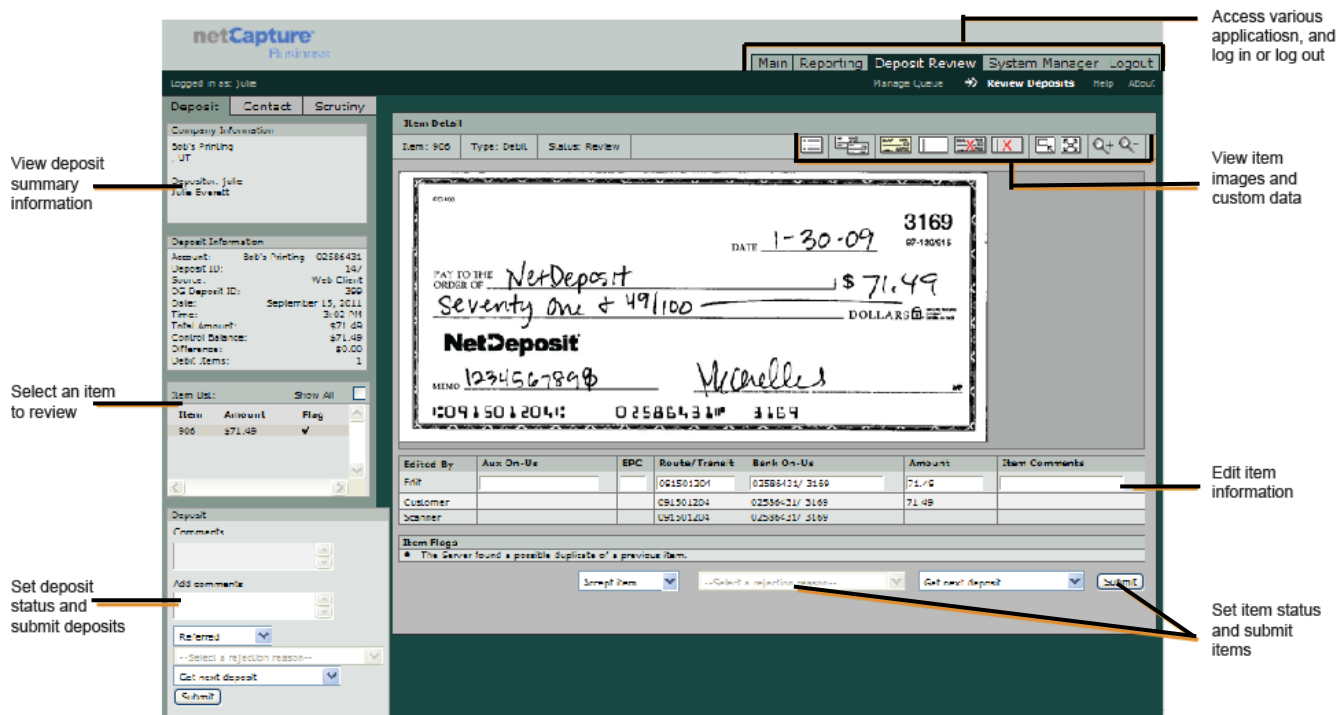
Deposit Review Overview

The Deposit Review application includes the following features:

- Allows Deposit Review Agents to review items and deposits that were flagged for review after submission.
 - Deposit Review Agents can refer items or deposits in question to users who have rights to review referred deposits.
 - Reviewers may choose to suspend the deposit for processing later.
- Performs validation on MICR fields as edited by depositors to ensure deposits will be able to be processed by the Decision Gateway.
- Allows Banking Operations personnel to review deposits, including those that were referred to them by Deposit Review Agents.
- Allows Banking Operations personnel to assign ownership of deposits to Deposit Review Agents and to adjust the priority of deposits in the work queue for effective workflow management.
- Automatically provides notification to customers when deposit adjustments occur and when deposits are rejected.

Understanding the Deposit Review Window

To access Deposit Review, log in to Portal and click the Deposit Review tab. The Deposit Review window appears with the first item of the first deposit available for review.



Note: If you have the Update Deposit Queue privilege, the Manage Queue screen appears. See *Managing Queues in Deposit Review*.

There are two main areas in the Deposit Review window:

- The left pane summarizes information about the current deposit. There are three tabs that contain information to help you in your review:
 - The Deposit tab contains information about the deposit you are currently reviewing.
 - The Contact tab contains contact information for the customer who submitted the deposit.
 - The Scrutiny tab contains definitions of all the possible flags applied to items and deposits, and details about the rules defined by your service organization.
- The right pane contains information about the selected item. This is where you will edit item information and accept, reject, or refer items in the deposit. The right pane contains the following:
 - The item image is displayed, and options are available for viewing different aspects of the image.
 - Fields for editing the item information appear below the image.
 - Options for setting the status of items appear below the item information fields.

Reviewing Deposits in Deposit Review

Some items and deposits are flagged for review by the system after they are submitted. Any items that are flagged for review appear in Deposit Review, and must be reviewed and then either approved or rejected by Deposit Review Agents. You can review and modify both monetary items (checks) and deposit slips in Deposit Review. After accepting or rejecting all the flagged items, you must accept or reject the entire deposit.

If you are unable to make an approval/rejection decision on a particular item or deposit, you can refer the item or deposit to a Banking Operations person who can then either approve or reject it. You can also suspend a deposit to save it in its current state and complete processing later.

The process of reviewing deposits may include the following:

- Reviewing and Modifying Items
- Adding Item or Deposit Comments
- Setting Item Status
- Submitting Completed Deposits
- Referring a Deposit
- Suspending a Deposit

Reviewing and Modifying Items

You must review and modify items that have been flagged for review before submitting deposits to the Decision Gateway for processing. The process of reviewing and modifying items may include the following:

- Selecting an Item for Review
- Viewing an Item's Images
- Viewing an Item's Flags
- Viewing Daily Deposit Activity
- Editing an Item's MICR Information
- Reviewing Suspected Duplicate Items

Selecting an Item for Review

The first item available for review is automatically displayed when you log in to Deposit Review. However, if you would like to select a different item, do the following:

1. In the left pane of the Deposit Review window, click the Deposit tab (if not already selected).

The scroll box lists the items available for review. By default, only flagged items are displayed for review.

2. To view all available items in the list, select the Show All check box.

The list may contain both monetary items and deposit slips, depending on which types of items have been flagged for review. Deposit slips are labeled DS in the item list.


3. Select an item in the list. The selected item appears in the right pane of the window.


Once you have selected the item you want to review, you can do the following things to help you determine whether to accept or reject the item:

- Viewing an Item's Images
- Viewing an Item's Flags
- Viewing Daily Deposit Activity
- Editing an Item's MICR Information


Viewing an Item's Images


To view an item's images, click the image icons located above the image. The selected image appears on the screen.


Custom Fields 

Duplicate: 


Appears only if the application suspects that the same item has previously been processed in the system.

Original front: 

Original back: 


Stamped front: 


Usually not available.


Stamped back: 


Usually not available.

You can change the size of the image by clicking the icons located above the image.

Actual size: 

Best fit: 

Zoom in: 

Zoom out: 

Viewing an Item's Flags

If an item or deposit is flagged for review, the flags are listed at the bottom of the screen under the headings Deposit Flags and Item Flags. Flags indicate which scrutiny rules the item failed or triggered when it was deposited. They can help you determine which areas to research further, and whether to accept or reject the item.

Viewing the Scrutiny Rules Used on the Deposit

Scrutiny rules are configured by your service organization to determine which deposited items are acceptable for processing. For example, your service organization may set a scrutiny rule that flags any items that exceed an amount of \$10,000.00. For details about how your service organization has configured scrutiny rules, click the Scrutiny tab in the left panel. The Scrutiny tab contains a listing of the active rules configured for the Bank of First Deposit, any correspondent banks, and the customer organization.

Following is a list of the scrutiny rules that may appear, depending on how your service organization has configured the scrutiny rules for deposits:

Rule	Possible Conditions	Possible Actions	Description
Route/Transit Number	<p>Is Between*</p> <ul style="list-style-type: none">Commonly excluded RT number ranges include:00000051-00000051 Government checks80000000-89999999 Travelers checks00000050-00000050 Government checks	Reject	Items possessing route/transit numbers that fall within the specified range of numbers are rejected.

Rule	Possible Conditions	Possible Actions	Description
Item Scanned MICR Line	Is Empty	Reject Set Flag	Items that are missing a scanned MICR line are flagged for review or rejected. Note: This rule does not apply to mobile transactions.
RT Number Check Digit	Fails	Reject Set Flag	Items with route/transit numbers that failed the check digit calculation are flagged for review or rejected. The check digit calculation ensures the route/transit number is valid.
Scanned MICR Amount	Is Found	Reject Set Flag	Items with amounts encoded in the MICR line are flagged for review or rejected.
Item Amount Threshold	Is Equal To	Reject Set Flag	Items with amounts equal to, greater than, or less than the specified amount are flagged for review or rejected.
	Is Greater Than Or Equal To	Reject Set Flag	
	Is Greater Than	Reject Set Flag	
	Is Less Than Or Equal To	Reject Set Flag	
	Is Less Than	Reject Set Flag	
Capture Duplicate Item	Is Found	Reject Set Flag	Items that may be duplicates of items previously submitted at the capture point are flagged for review or rejected. Note: This rule does not apply to mobile transactions.
Scanned Route/Transit	Is Changed	Reject Set Flag	A depositor edited the initial scanned route/ transit number for an item, so the item is flagged for review or rejected. Note: This rule does not apply to mobile transactions.
Scanned Bank On-Us	Is Changed	Reject Set Flag	A depositor edited the initial scanned bank on-us field for an item, so the item is flagged for review or rejected. Note: This rule does not apply to mobile transactions.
Scanned Aux On-Us	Is Changed	Reject Set Flag	A depositor edited the initial scanned aux on-us field for an item, so the item is flagged for review or rejected. Note: This rule does not apply to mobile transactions.

Rule	Possible Conditions	Possible Actions	Description
Scanned Amount	Is Changed	Reject Set Flag	A depositor edited the initial scanned encoded amount for an item, so the item is flagged for review or rejected. Note: This rule does not apply to mobile transactions.
	Increased By More Than	Set Flag	An item amount that has been increased by more than the specified threshold will be flagged for review. If you use this condition, item amounts that are decreased will NOT be flagged for review. Note: This rule does not apply to mobile transactions.
Entered Amount	Is Changed	Reject Set Flag	An item amount that was initially entered was changed before the deposit was completed by the depositor, so the item is flagged for review or rejected.
	Increased By More Than	Set Flag	An item amount that has been increased by more than the specified threshold will be flagged for review. If you use this condition, item amounts that are decreased will NOT be flagged for review.
Deposit Amount Threshold	Is Equal To	Set Flag	Deposits with total amounts equal to, greater than, or less than the specified amount are flagged for review.
	Is Greater Than Or Equal To	Set Flag	
	Is Greater Than	Set Flag	
	Is Less Than Or Equal To	Set Flag	
	Is Less Than	Set Flag	
Account Number	Is New	Set Flag	Deposits made to accounts that are marked as new accounts are flagged for review.
Percent of Deposits to Review	Is Applied	Set Flag	A random selection of deposits that meets the specified percentage of all deposits made is flagged for review.
Bank On-Ups	Is Empty	Reject Set Flag	No bank on-us number was scanned for the item, so it is flagged for review or rejected. Note: This rule does not apply to mobile transactions.
Scanned or Edited EPC	Is Found	Reject Set Flag	An EPC number was scanned or edited for the item, so it is flagged for review or rejected.
Scanned or Edited Aux On-Ups	Is Found	Reject Set Flag	An aux on-us field was scanned or edited for the item, so it is flagged for review or rejected.

Rule	Possible Conditions	Possible Actions	Description
Control Balance	Is Changed	Set Flag	The control balance for the deposit was changed before submitting the deposit, so it is flagged for review.
Item Type	Is Changed	Set Flag	This item's type (DR-debit, DS-deposit slip) was changed after the initial scan, so it is flagged for review. Note: This rule does not apply to mobile transactions.
Dual Control Deposit Amount	Is Greater Than The Deposit Limit	Review	Remote Users with deposit limits are prompted to have any deposits that exceed the limit reviewed by a Remote Reviewer before they can be submitted. Note: This rule does not apply to mobile transactions.
IQA Threshold	Is Less Than	Reject Set Flag	Indicates the acceptable level of quality for scanned images. Images that receive a quality grade below this number are flagged for review or rejected. Web Client evaluates scanned check images for their level of quality and assigns a grade to each image. The better the quality, the higher the grade the image receives. The image quality grade is a composite of several factors, such as image sharpness and clarity, darkness or lightness, readability, etc. The higher the number you provide here, the more items will <i>fail</i> to meet quality standards and will require re-scanning or adjustment.
Duplicate Item on Server	Is Found	Set Flag	Items that may be duplicates of items previously submitted to the server are flagged for review.
Daily Total Deposit Amount	Is greater than or equal to	Don't Accept Report Only Set Flag	When deposits submitted for the designated customer or account reach the daily limit specified here, they will trigger the rule. For the purposes of this rule, a

Rule	Possible Conditions	Possible Actions	Description
	Is greater than	Don't Accept Report Only Set Flag	<p>day is defined as a 24-hour period from midnight to midnight.</p> <ul style="list-style-type: none"> • If you choose Don't Accept, deposits triggering the rule will be stopped at the client and users will not be allowed to submit them until the 24-hour period is up. These deposits will also be included in over limit reports. • If you choose Report Only, deposits that trigger the rules will be included in over limit reports, but no further action will be taken on them. • If you choose Set Flag, deposits triggering the rule will be sent to Deposit Review. These deposits will also be included in over limit reports.
Daily Number of Items	Is greater than or equal to	Don't Accept Report Only Set Flag	When deposits submitted for the designated customer or account reach the daily number of items specified here, they will trigger the rule. For the purposes of this rule, a day is defined as a 24-hour period from midnight to midnight.
	Is greater than	Don't Accept Report Only Set Flag	<p>If you choose Don't Accept, deposits triggering the rule will be stopped at the client and users will not be allowed to submit them until the 24-hour period is up. These deposits will also be included in over limit reports.</p> <p>If you choose Report Only, deposits that trigger the rules will be included in over limit reports, but no further action will be taken on them.</p> <p>If you choose Set Flag, deposits triggering the rule will be sent to Deposit Review. These deposits will also be included in over limit reports.</p>
7-Day Total Deposit Amount	Is Greater Than or Equal to	Don't Accept Set Flag	Mobile deposits that exceed the configured limit, which is calculated using

Rule	Possible Conditions	Possible Actions	Description
	Is Greater Than	Don't Accept Set Flag	<p>a 7-day rolling time period, will either be rejected or flagged for review.</p> <p>The 7-day time period is calculated by looking back exactly 7 days from the time at which the deposit is attempted. For example, if a user submits a deposit at 10:00 a.m. on March 12, then the application looks back 7 days to 10:00 a.m. on March 5, calculates the total, and takes action on the deposit based on the total of all deposits submitted between 10:00 a.m. on March 5 and 10:00 a.m. on March 12.</p> <p>For this rule, the UTC time zone is used with no offset, which makes the user's time zone irrelevant. Each deposit timestamp is stored at the server in UTC time and that is used to calculate the rolling limits.</p> <p>Note: This rule can only be applied to mobile customers and accounts. Bank-level limits are not supported.</p>
30-Day Total Deposit Amount	Is Greater Than or Equal to	Don't Accept Set Flag	<p>Mobile deposits that exceed the configured limit, which is calculated using a 30-day rolling time period, will either be rejected or flagged for review.</p>
	Is Greater Than	Don't Accept Set Flag	<p>The 30-day time period is calculated by looking back exactly 30 days from the time at which the deposit is attempted. For example, if a user submits a deposit at 10:00 a.m. on March 30, then the application looks back 30 days to 10:00 a.m. on March 1, calculates the total, and takes action on the deposit based on the total of all deposits submitted between 10:00 a.m. on March 1 and 10:00 a.m. on March 30.</p> <p>For this rule, the UTC time zone is used with no offset, which makes the user's time zone irrelevant. Each deposit timestamp is stored at the server in UTC time and that is used to calculate the rolling limits.</p> <p>Note: This rule can only be applied to mobile customers and accounts. Bank-level limits are not supported.</p>

Viewing Daily Deposit Activity

For deposits that have triggered the daily velocity rule, a deposit history window will show all deposit activity for the current day.

1. In the Deposit Review screen, click on View Activity next to the description of the velocity rule under Deposit Flag.

A Deposit Activity window will appear, showing the summary of the rule triggered, a summary of the current deposit being reviewed, a list of deposits submitted in the current day, the customer name, the account name and number, the deposit ID, the date and time of submission, the username of the submitter, the number of items, and the deposit amount.

2. Review the deposit history from that current day and click OK.

In the Deposit Review screen, take appropriate action based on the information in the Deposit Activity window.

Viewing Item or Deposit Comments

Comments are notes that have been added to an item or deposit. You can view comments added by a reviewer (Deposit Review Agent or Bank Operations person), the customer, or the scanner. Comments can help you determine which areas to research further, and whether to accept or reject the item or deposit.

Item comments for the current item are displayed in the rows labeled Edit, Reviewer, Supervisor, Customer, and Scanner. The Reviewer and Supervisor rows only show up if a Deposit Review Agent or Banking Operations person have previously reviewed the item and made corrections.

Deposit comments for the current deposit are displayed in the Deposit Comments field in the left pane.




Editing an Item's MICR Information

Below the image display area are fields containing the item's MICR information. There are several rows of fields:

- The row labeled Edit lets you enter modified values for the item. If the item has any flags, the cursor defaults to the first field that has been flagged.
- The row labeled Reviewer contains any edited values entered by another Deposit Review Agent. This row only shows up if a Reviewer has previously reviewed the deposit and made corrections.
- The row labeled Supervisor contains any edited values entered by a Banking Operations person. This row only shows up if a Banking Operations person has previously reviewed the deposit and made corrections.
- The row labeled Customer contains any edited values entered by the depositor.
- The row labeled Scanner contains the original values scanned by the check reader.


The following fields are available for each item:

Field	Symbol	Description
Aux On-Us number	␣	This is usually the check number. It is often included on commercial checks, but never on personal checks. The format of this field varies, and may contain numbers, spaces, and dashes. If an aux on-us is present, it appears as the first piece of information in the MICR line and is denoted by the on-us symbol.
EPC number	None	This is a code assigned to the item if it has previously been processed electronically. This is usually blank, but if present, it appears between the aux on-us number and route/transit number.

Field	Symbol	Description
Route/Transit number		<p>This is the eight- or nine-digit route/transit number for the bank. This field is required.</p> <p>Eight-digit route/transit numbers are allowed only for deposit slips. Monetary items must have a nine-digit route/transit number. The route/transit number starts with a 0, 1, 2, or 3 and may contain only numbers, unless it is an eight-digit route/transit number, in which case it may contain a dash (entry of the dash is optional). The route/transit number is always present and appears after the EPC in the MICR line. It is denoted by the routing symbol.</p>
Bank On-Us number		<p>This includes the account number and in some cases the check number. Account numbers included in the bank on-us field vary in format, and may include numbers, spaces, or dashes. The account number should be entered exactly as it appears on the item. If a bank on-us is present, it consists of all the data that appears after the route/transit number and before the amount in the MICR line. It may or may not be denoted by the on-us symbol.</p> <p>The on-us symbol is displayed as a forward slash (/) in the item grid. You <i>must</i> enter a capital O or a forward slash (/) in place of the bank on-us symbol.</p>
Amount		<p>An amount for an item is required, but the amount may or may not be part of the item's MICR line. If the amount has already been encoded into the item's MICR line, it appears as the last piece of information in the MICR line (at the far right) and is denoted by the amount symbol. It is zero filled to 10 characters. The amount is displayed as a number with a decimal point, so if b0009000000c appears in the MICR line, then 90000.00 appears in the Amount field.</p> <p>If there is no decimal entered in the item amount, Deposit Review assumes a decimal is present at the end of the entered amount. For example, if you enter 1000, Deposit Review reads the amount as \$1000.00. If you enter a decimal but do not enter both digits after the decimal, Deposit Review fills in the remaining digits as zeroes. For example, if you enter 1000, Deposit Review reads the amount as \$1000.00.</p> <p>Note: This field is not editable for deposit slips.</p>

Reviewing Suspected Duplicate Items

If the current item may have already been processed through the system, then the Duplicate icon appears on the screen next to the other image icons. Before you can accept the item, you must review the suspected duplicate item(s) and determine whether or not the current item is a duplicate. Do the following to review the suspected duplicate item(s):

1. Click the Duplicate icon,  which appears next to the other image icons.
The Duplicate Check window appears.

Duplicate Check

Current Check in Review

Robert W. Andrews
123 Success Street
Anytown, USA 12345

Date 12-11-09 2339

Pay to the Order of NetDeposit, LLC \$ 99.00

Ninety-nine & 00/100 Dollars

Clarke American

For Bob Customer

24000054062 38635 4 2339

Check Details

Check Id	682
Deposit Number	164
Org User Id	35
Scanned Date	07/09/13
Status	Review
Customer	ABC Mortgage
Account	Primary Account -
Aux On-Us	
EPC	
Route/Transit	124000054
Bank On-Us	062 38635 4/ 2339
Amount	\$99.00

1 of 1 duplicate

Robert W. Andrews
123 Success Street
Anytown, USA 12345

Date 12-11-09 2339

Pay to the Order of NetDeposit, LLC \$ 99.00

Ninety-nine & 00/100 Dollars

Clarke American

For Bob Customer

24000054062 38635 4 2339


Check Details

Check Id	679
Deposit Number	163
Org User Id	35
Scanned Date	07/09/13
Status	Reject
Customer	ABC Mortgage
Account	Primary Account -
Aux On-Us	
EPC	
Route/Transit	124000054
Bank On-Us	062 38635 4/ 2339
Amount	\$0.00
Reason	Missing Endorsement

Mark Duplicate Reviewed & Close

2. Compare the two items and determine whether or not they are the same item.
The tables on the right contain information about the two items. When you hold your cursor over a field in one table, the same field in both tables is highlighted to help you more easily compare the information.
3. When you are finished reviewing the items, click Mark Duplicate Reviewed & Close to close the window.
4. If you have determined that the suspected duplicates are the same item, click Reject item to reject the current item. If you have determined that they are different items, click Accept item. If you need to research the item further, click Refer item.

Viewing Custom Fields and Payer Information

If it has been configured by your service organization, you can view custom fields and payer information by clicking on the  icon, which appears next to the other image icons. It will display the field name, field value, value type, x-reference, and whether or not it is required. Viewing custom fields and payer information may be most useful when reviewing deposits submitted through Mobile and Small Business Client applications.

Adding Item or Deposit Comments

You can add comments to any item or deposit. Comments can include any notes that will be useful to you or other reviewers in determining whether to accept or reject items or deposits. If you refer or reject an item or deposit, you may want to add comments to explain why you are referring or rejecting it.

- To add item comments, enter your comments in the Item Comments field. The comments are saved when you set the item's status (for details, see *Item Statuses* in the next section).
- To add deposit comments, enter your comments in the Deposit Comments field in the left pane. The comments are saved when you submit, refer, or suspend the deposit.

Setting Item Status

Once you have researched an item and made any necessary adjustments, you must set its status and submit it as part of the deposit. The status you choose determines whether the item will be sent to the Decision Gateway for processing.

Item Statuses

The following are the available item statuses:

- **Accept item:** If you have fixed any problems with the item so it can be processed at the Decision Gateway, you can accept the item.
- **Refer item:** There may be items for which you are unable to make an accept/reject decision. You can refer these items to a Banking Operations person for review. The Banking Operations person can then either accept or reject the item.
- **Reject item:** If you have decided that the item should not be processed further, you should reject the item.

Note: You cannot reject deposit slips.

The rejected item is removed from the deposit. The deposit is adjusted with a credit or debit adjustment to keep the deposit in balance. The system will automatically notify the customer who made the deposit of the rejected item and the adjusted deposit amount. See *Examples of Adjustment and Rejections Notices* for details.

To Set Item Status

Do the following to set an item's status and submit the item:

1. Select the appropriate item status in the drop-down box at the bottom of the screen (Accept item, Refer item, or Reject item).
- Note:** You cannot reject a deposit slip.
2. If you have selected Refer item, you may want to enter the reason for referral in the Item Comments field.

If you have selected Reject item, select the reason for rejection in the Select a rejection reason drop-down box.

The following are the available rejection reasons:

- **Encoded Amount Error:** The amount entered by the depositor does not match the amount on the item image.
- **Incomplete Image:** There is an incomplete image for the item.
- **No Signature:** The maker of the check has not signed the item.
- **Not Payable:** The item was not made payable to the depositor.
- **Stale Date:** The item's date indicates that it is too old to be processed.
- **User Error:** The depositor entered incorrect information for the item, and the item is invalid and should be rejected.
- **No Bank On-Us Value Found:** The item is missing a Bank On-Us value.
- **Duplicate Check:** The item is a duplicate of a previously submitted item.
- **Incorrect Amount (Adjusted):** The amount on the item was incorrectly adjusted by the Web Client user.
- **Illegible Image:** The check image is not clearly discernible.
- **Missing Date:** The date on the item is missing.
- **Blank Check:** The item is not filled out.
- **Post Dated:** The item has a future date that it can be deposited.

- Keyed Amount does not match Check Amount: The amount entered in the Deposit screen does not match the item amount.
- Missing Endorsement: The item is missing the endorsement on the back.
- Signature does not Match Payer: The signature on the check does not match the payer name in the Payer field.
- Unacceptable item type: Your organization has a policy that does not allow this type of item to be deposited via RDC.
- Piggyback image: A double image of two items.
- Courtesy and Legal Amounts do not match: The courtesy amount and the legal amount do not match.
- Other: Use this for any other rejection reason, and provide details in the text field that appears.

3. Click the Submit button.

The item is submitted as part of the deposit, unless it has been rejected. If you rejected the item, it is removed from the deposit, and:

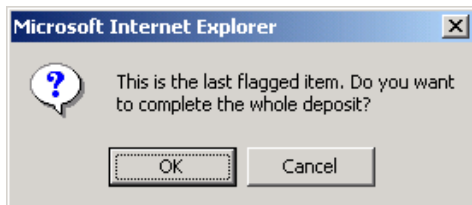
- An adjustment is automatically created to keep the deposit in balance.
- A notification message is automatically sent to contacts that have been configured to receive them and notifies them of the adjustment. See *Examples of Adjustment and Rejections Notices* for details.

The next flagged item available for review appears in the Deposit Review window. If there are no flagged items available for review, the screen continues to display the current item.

Submitting Completed Deposits

After you have reviewed and set the status of all the flagged items in a deposit, you must submit the entire deposit. If you exit the application without first completing (either submitting, referring, rejecting, or suspending) the deposit, the deposit is saved and is queued up for review the next time you log into Deposit Review.

When you have finished reviewing flagged items, the following message appears:



To submit the deposit, click OK. The deposit is sent to the Decision Gateway for processing, and one of the following occurs:

- If Get next deposit is selected in the drop-down box next to the Submit button, then the first item in the next deposit that is available for review appears.
- If Leave Deposit Review is selected in the drop-down box next to the Submit button, then the Main tab appears.

If you would like to reject the deposit or refer it to a Bank Operations person for review, click Cancel, then see the next sections, Referring a Deposit or Rejecting a Deposit.

You can also manually choose to complete a deposit by selecting Complete deposit in the field under the Comments field in the left pane, then clicking Submit. You must first complete the review of all items in the deposit before you can complete the deposit.

Referring a Deposit

There may be deposits you want to refer to a Banking Operations person for review. The Banking Operations person can then accept, reject, or refer the deposit. If you are a Banking Operations person and refer a deposit, the deposit is reinserted into the queue for Banking Operations review.

Do the following to refer a deposit at any point during the review process:

1. In the drop-down box under the Comments field in the left pane, select Refer deposit.
2. Enter the reason for referral in the Deposit Comments field (optional).
3. Click the Submit button.

The deposit is automatically reassigned to a Bank Operations person for review.

Rejecting a Deposit

If you have decided that the deposit should not be processed further, you should reject the deposit. When you reject a deposit, all the items within that deposit are also rejected. Do the following to reject a deposit at any point during the review process:

1. In the drop-down box under the Comments field in the left pane, select Reject deposit.
2. Select the reason for rejection in the Select a rejection reason drop-down box.

The following are the available rejection reasons:

- Deposit Limit Exceeded: The amount in the deposit exceeds the deposit limit amount.
- Per Customer Request: The customer who made the deposit has requested that the deposit be rejected.
- Suspected Duplicate Deposit: There is reason to believe this deposit may be a duplicate of a deposit that was already submitted.
- Suspected Fraud: There is reason to suspect that the deposit or items in the deposit are fraudulent.
- Will Not Accept Any Items: All the items in the deposit have been rejected, so the entire deposit must be rejected.
- Wrong Customer/Account: This deposit was made to the wrong account.
- Other: Use this for any other rejection reason, and provide details in the description field that appears.

3. Click the Submit button.

The system automatically notifies the customer who made the deposit of the rejected deposit and the deposit amount.

Suspending a Deposit

A suspended deposit is a deposit that is waiting for review to be completed in Deposit Review. If you need to quit reviewing the deposit before it is complete, you can select Suspend deposit in the drop-down box under the Comments field in the left pane, and then click Submit to suspend the deposit.

When a suspended deposit exists, you must complete that deposit (accept, reject, or refer the deposit) before the system will allow you to review any other deposits.

To resume a suspended deposit, log in to Portal and go to Deposit Review. The suspended deposit appears in the Deposit Review window. Continue processing the deposit as usual.

Examples of Adjustment and Rejections Notices

After you submit or reject a deposit, the application automatically sends email notifications to contacts that have been configured to receive them and notifies them of any adjusted or rejected items or deposits. Following are examples of each possible type of notification.

Note: The notifications sent by your system may differ from these examples if your service organization has modified the default email text.

Example of a Rejected Deposit Notice

John Doe

Deposit number 10, submitted on 2/15/2006 14:21:24 for \$542.44, was rejected due to the following reason:

Suspected Duplicate Deposit

If you have any questions or concerns, please contact 800-444-5555.

Thank you,

Correspondent Bank

Example of a Deposit Adjustment Notice

John Doe

In deposit number 11, submitted on 2/15/2006 14:38:28 for \$370.00, a CREDIT adjustment of \$10.00 will be posted to the following item(s) for the following reason(s):

Item 71 - Adjusted for Encoded Amount Error

Item 72 - Rejected for No Signature

Item 73 - Rejected for Other (testing reason)

Item 74 - Adjusted for Encoded Amount Error

If you have any questions or concerns, please contact 800-444-5555.

Thank you,

Correspondent Bank

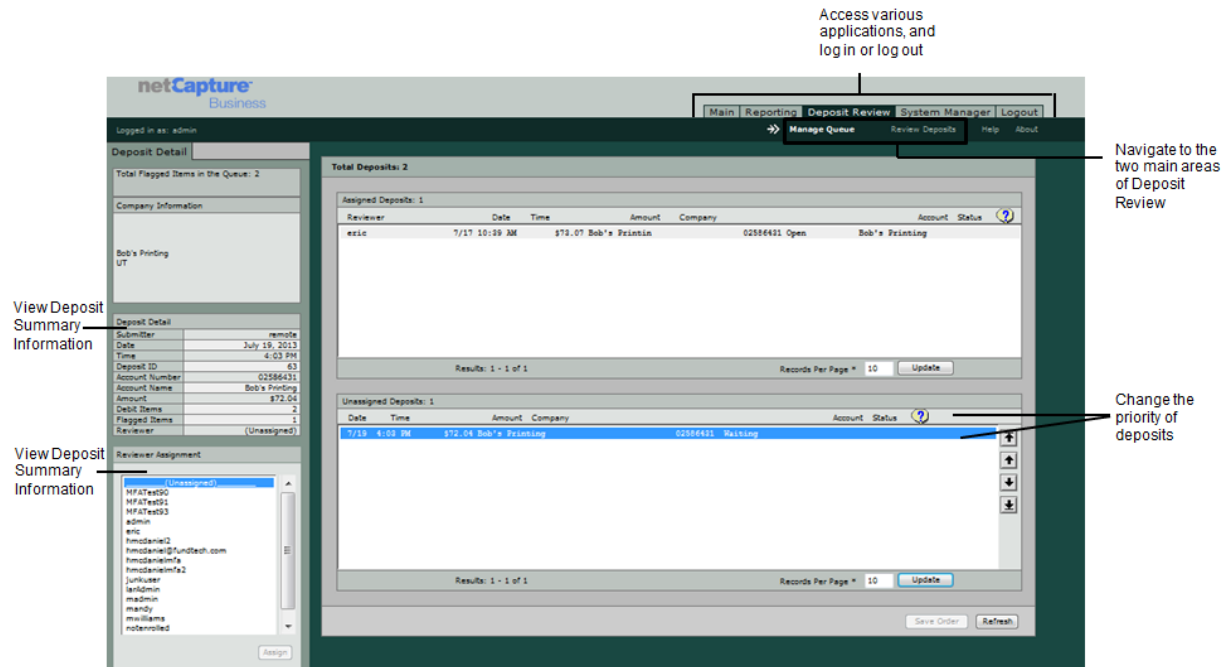
Managing Queues in Deposit Review

Banking Operations personnel have access to manage how deposits are queued for review. You can change the priority of deposits in the queue or assign deposits to specific Deposit Review Agents for review.

Deposits are automatically queued in first in, first out order, so that the first deposits submitted are also the first reviewed. You may want to change the way deposits are queued for several different reasons. For example:

- There is a high-dollar-amount deposit that needs to be processed before the other queued deposits.
- A particular reviewer has special insight into a deposit and therefore should review that deposit.
- A reviewer with assigned deposits has left on vacation, so the deposits need to be reassigned to other reviewers.

To access the deposit queue, click Manage Queue on the Deposit Review window (in the upper right corner below the tabs). This option appears only for Banking Operations personnel. The Deposit Queue window appears.



The top area of the queue lists deposits that have been assigned to a reviewer. The bottom area lists unassigned deposits. The number of deposits displayed depends on the value in the Results Per Page field. To navigate in the list, click the Previous and Next buttons: [<] [>]. To change the number of deposits that are included in the list, edit the number in the Results Per Page field and click Update.

The following information is presented for each deposit in the queue:

- **Reviewer:** The user name of the reviewer that is assigned to the deposit (this appears only for assigned deposits).
- **Date:** The date the deposit was received at your service organization.
- **Time:** The time the deposit was received at your service organization.
- **Amount:** The sum of the debit items in the deposit.
- **Company:** The name of the customer who made the deposit.
- **Account:** The account number to which the deposit is being made.
- **Status:** The status of the deposit in the Deposit Review process. Clicking the status icon at the top of the column will display an expanded definition for the abbreviated status listed. Following are the possible statuses:
 - **Receiving:** The file is being received for processing.
 - **Assigned:** The deposit has been assigned to a reviewer.
 - **Unknown:** Unknown process
 - **Error:** There is an error. Call support.
 - **Open:** The deposit is currently open and in review.
 - **Validating:** The deposit is being validated.
 - **Waiting:** The deposit is waiting for review.
 - **In Queue:** The deposit is waiting for validation.
 - **DR Done:** Deposit Review complete.

- Re-Assigned: The deposit has been assigned to an additional reviewer.
- Rejected: The deposit has been rejected in Deposit Review.
- Suspended: The deposit is suspended.
- Batch Prep: Building batch file.
- Sending: The file is being sent to the Decision Gateway.
- Processing: The deposit is being processed.
- Sent: The deposit has been sent to the bank.

The same information is presented for the selected deposit in the Deposit Detail tab in the left pane, which also includes the deposit ID and the total number of items.

You can manage the Deposit Review workflow by completing the following processes:

- Changing the Priority of Unassigned Queued Deposits
- Assigning Deposits to Specific Reviewers
- Removing an Assignment from a Deposit

Changing the Priority of Unassigned Queued Deposits

You can assign the priority of deposits in the queue for review. Deposits at the top of the queue are given the highest priority. You can only change the priority of unassigned deposits because when you assign a deposit, it is automatically given the highest priority.

Do the following to change the priority of unassigned queued deposits:

1. On the main Deposit Review window, click Manage Queue. The deposit queue window appears.
2. In the Unassigned Deposits list, select the deposit for which you want to change priority.
3. Click the up and down arrow buttons to the right of the Unassigned Deposits list to move the deposit up or down in priority.

To the top:



Up one level:



Down one level:



To the bottom:



4. Repeat Steps 2-3 for each deposit for which you want to change priority.
5. After arranging the deposit priorities, click Save Order to save the new deposit queue order.

Assigning Deposits to Specific Reviewers

You can assign deposits to specific Deposit Review Agents for review. Do the following to assign a deposit:

1. On the main Deposit Review window, click Manage Queue. The deposit queue window appears.
2. In the Assigned Deposits or Unassigned Deposits list, select the deposit you want to assign.
3. In the Reviewer Assignment drop-down box in the left pane of the window, select the user name of the person to whom you want to assign the deposit.
4. Click Assign.

If the deposit was previously unassigned, it is moved up to the Assigned Deposits list.

Removing an Assignment from a Deposit

You can also remove the assignment from a deposit so that anyone can review it. Do the following to remove the assignment from a deposit:

1. On the main Deposit Review window, click Manage Queue. The deposit queue window appears.
2. In the Assigned Deposits list, select the deposit from which you want to remove the assignment.
3. In the Reviewer Assignment drop-down box in the left pane of the window, select (Unassigned).
4. Click Assign.

The deposit is moved to the Unassigned Deposits list, and is automatically given the highest priority.

5 Troubleshooting

This chapter describes how to resolve some potential issues you may encounter in the NetCapture Portal.

- Login Issues
- General Issues
- Troubleshooting System Manager
- Troubleshooting Deposit Review

Login Issues

The following table describes possible issues you may encounter when logging in to the system.

Field	Description	Resolution
You are unable to log in to NetCapture Portal. You entered an invalid username or password.		Ensure you enter the correct user name and password as provided by your Service Representative. User names and passwords are case sensitive, and passwords must comply with certain restrictions configured by your service organization. Contact your Service Representative for details about your specific password requirements. If you continue to be denied access to the application, contact your Service Representative.
You are unable to log in at this time.	It may be outside of the configured days and times you are allowed to log in to the application. In addition, your user status may have been set to inactive.	Contact your Service Representative for information about the days and times during which the application is available, or to have your status reset.
You are unable to access Portal.		Ensure that you enter the correct URL, as provided by your Service Representative. Verify whether the URL begins with http or https.
You have exceeded the maximum number of login attempts.	Your account status is set to Inactive.	Call your Service Representative to reactivate your account.

Field	Description	Resolution
<p>The application will not allow you to set the password you desire. You may receive the following errors:</p> <ul style="list-style-type: none"> • The new password you provided is not valid. • The password you provided does not meet the length requirements configured by your service organization. • Your new password must contain at least ____ numeric characters and at least ____ alphabetic characters. • Your password cannot be the same as your username. • You cannot use the new password you provided because it has been used previously. • This password has been used recently. 	<p>Password requirements are configured by your service organization. For example, your service organization may require that your password be at least six characters in length and use a numeric value, and may use a list of excluded words that may not be used as passwords. In addition, you may not be allowed to use a password that you have used previously.</p>	<p>Contact your Service Representative for details about your specific password requirements.</p> <p>In addition to your service organization's configurable requirements, your password may not be the same as your user name and you cannot re-use any of your previous passwords.</p>
Unable to confirm current password.	The password you entered as your current password does not match what is stored in the database.	Re-enter your current password.
Your password has expired.	You must change your password before you can log in to the application.	Change your password, or contact your Service Representative to have your password reset.
Immediately after logging in to Portal and clicking on an application tab, you receive a message stating that your session has timed out.	This problem may be caused by a browser caching issue. If you have attempted to log in to Portal using different application servers (for example, WebLogic) without closing your browser between sessions, this problem may occur. This problem may also occur if Finastra Platform is running on a web server and the web server has been restarted.	<ul style="list-style-type: none"> • To clear the browser cache, close the browser and attempt to log in again. • If the above doesn't resolve the problem, contact your Service Representative, report the problem, and request that the web server be restarted again.

Field	Description	Resolution
A Web Client user receives the following error message: You cannot log in because you are already logged in to the application one or more times.	The user has attempted to log in to Web Client too many times. The maximum allowable concurrent logins are defined in System Manager in the security parameters for the organization. For example, if the Allowable Concurrent Logins value is set to two, then the user may log in for three concurrent sessions.	You can resolve this problem in one of the following ways: <ul style="list-style-type: none"> • Increase the allowable number of concurrent logins for the user's organization. <p>Note: Web Client supports 0 - 9 concurrent logins.</p> <ul style="list-style-type: none"> • Force the session to close. The user will then be able to log in.
You receive a prompt to install an updated version of the Java Runtime environment (JRE) when attempting to log in to NetCapture Portal.	Your computer does not have the latest version of the JRE installed.	Download and install the JRE as prompted by your browser. You cannot log in to NetCapture Portal unless you are using the correct version of the JRE.

General Issues

The following table describes some possible general issues you may encounter.

Field	Description	Resolution
Your session has timed out.	If the application remains idle—in other words, if you do not press any keyboard keys or move your mouse—for a period of time as configured by your service organization, the application will automatically log you out and request that you log in again.	You must log in again before you can continue working in the application. To avoid being logged out automatically, continue to use the system without significant lapses in activity. In addition, you are only allowed to remain logged in for the period of time configured by your service organization. The default is eight hours. If your login session exceeds the configured time period, the application will log you out automatically.
Access Denied. Insufficient Privileges.	You do not have sufficient privileges to view or edit this area of the application.	To gain the appropriate privileges, contact your Service Representative.
You do not have privileges to perform any action.	You do not have sufficient privileges to view or edit any NetCapture Portal applications.	To gain the privileges you need, contact your Service Representative.

Troubleshooting System Manager

This troubleshooting section covers the following types of issues:

- User Interface Issues
- Privileges Issues

- Data Validation Issues

User Interface Issues

The following table describes possible issues you may encounter with the System Manager interface.

Field	Description	Resolution
Nothing happens when you click a link for an expanding list, such as an organization tree or the Show Roles list. The list does not expand, and the browser does not respond.	Check to ensure the security settings for your Internet Explorer browser are not set to High. High security disables JavaScript, which is necessary for normal operation of System Manager.	<p>Do the following to change your security settings:</p> <ul style="list-style-type: none"> • In Internet Explorer, select Tools > Internet Options... • The Internet Options window appears. • Click the Security Tab. • Click the Custom Level button. • The Security Settings window appears. • In the Reset to: drop-down box, select Medium or Low security. • Click the Reset button. • Click OK to close the Security Settings window. • Click OK to close the Internet Options window. • Your security settings will now enable you to work in System Manager without encountering problems.

Privileges Issues

The following table describes possible issues you may encounter with privileges.

Field	Description	Resolution
A Web Client user has suspended a deposit, but can no longer access that deposit to complete and submit it for processing.	A System Manager user may have inactivated the customer or account. The deposit is not presented to the Web Client user for completion since the customer or account has been inactivated.	The Web Client user should log out and notify their system administrator of the problem. In System Manager, the administrator must re-enable the customer or account for a long enough period of time that the Web Client user is able to complete the deposit. Once the deposit has been submitted, the administrator can once again inactivate the customer or account in System Manager.

Field	Description	Resolution
When you attempt to access an organization in the organization tree, error messages appear.	Your privileges or some other configuration has been changed in System Manager while you were logged in to the system.	Log out of System Manager and then log in again. You should be able to access all organizations that are visible in your organization tree.
You do not have privileges to assign this role.		Select a different role to assign to the user, or contact your Service Representative to gain the appropriate privileges for assigning this role.

Data Validation Issues

The following table describes possible issues you may encounter with validating data.

Field	Description	Resolution
<ul style="list-style-type: none"> _____ must be a valid domain name or comply with the standard IP address format, e.g., 255.255.255.255. _____ must be between 0 and 65536 all inclusive. 	This can occur if you provide incorrect values when configuring applications in System Manager.	Provide a valid URL or IP address for the application, and provide a valid port number between 0 and 65536.
<ul style="list-style-type: none"> A primary location cannot be deleted. To continue, edit this location to be non primary. A primary contact cannot be deleted. To continue, edit this contact to be non primary. 	There must be one location or contact designated as the primary location/ contact for the organization.	To continue, leave the Primary check box selected for this location/ contact. Designate another location/ contact as primary by checking the Primary check box for that location/contact. You can then continue and delete the desired non-primary location/contact.
<ul style="list-style-type: none"> There must be at least one primary location. To continue, this location must be primary. There must be at least one primary contact. To continue, this contact must be primary. 	There must be one location or contact designated as the primary location/ contact for the organization, and currently this location or contact is designated as primary.	To continue, leave the Primary check box selected for this location/ contact to designate it as primary. If desired, you can designate another location/contact as primary by checking the Primary check box for that location/contact.
Select a different user name.	This user name has already been specified for another user.	Select a different user name for this user.
Allowable Login Time To must be in HH:mm format (e.g., 2:35 or 19:30). The Allowable Login Time From field must be earlier than Allowable Login Time To field.		In the Allowable Login Time To field, enter a valid time in HH:mm format (hours:minutes), and ensure it is a later time than that specified in the Allowable Login From field.

Field	Description	Resolution
This ____ already exists. Please check the data and try again.	The information you are trying to add already exists in the application. It may already be specified for this organization or user.	Modify the information so it is not identical to the information that already exists in the application.
____ must not be greater than 10 numeric characters and must be in the following format xxxxx-xxxx or xxxxx.		Enter a valid ZIP code or ZIP + 4 code that is less than 10 numeric characters total.
<ul style="list-style-type: none"> Contact Phone must be in the following format xxx-xxx-xxxx. Contact Fax must be in the following format xxx-xxx-xxxx. 		Enter a valid phone number or fax number in the format specified.
The percentage value must be between ____ and ____.		Enter a percentage value that falls between the values specified. Do not enter a % symbol as part of the value.
The ____ field must be greater than or equal to the accumulative values of fields ____ and ____.	The password you entered must add up to the same number of characters or a greater number of characters than specified by the minimum required numbers of alphabetic and numeric characters for passwords.	Enter a password with a length greater than the combined minimum number of alphabetic and numeric characters.
Start value must be less than or equal to End value.	When editing rules, you have specified a Start value that is greater than an End value.	Provide a Start value that is less than or equal to the End value for the rule.
____ must match the file with name _____. The file name is not case sensitive.	When editing branding for an organization, the image file name you specified does not match the required file name. The file name does not have to match the case specified.	Rename the image file to match the required file name and try again to upload the file.
Enter letters, numbers, spaces and punctuation symbols only. Only characters from the US-ASCII charset are allowed.	As a general rule, text fields in System Manager accept only basic ASCII characters, or those characters found on your keyboard. The exception to this is the Branding window, which supports the copyright (©) and trademark (™) symbols.	Edit your entry to contain only basic ASCII characters.
Image compression type cannot be G4 when a front or back image bit depth is 8.	G4 compressing can only be used in conjunction with an image bit depth of 1.	Either change the image compression type or set the front and back image bit depth to 1.
The Sequence Number Size must be set to 15 when the Send ACH Opt Out is true.	The Decision Gateway does not accept items with 10-digit sequence numbers if the option to use ACH Opt-Out is true.	Either change the sequence number size to 15 digits, or set Send ACH Opt Out to false.

Troubleshooting Deposit Review

This troubleshooting section covers the following types of issues:

- Deposit Issues
- Item Editing Issues

Deposit Issues

The following table describes possible issues you may encounter when reviewing deposits.

Field	Description	Resolution
A deposit you are reviewing is out of balance.	The deposit may not yet be fully transferred to your service organization.	Contact your Service Representative and ask them to help you determine the status of the deposit.
A deposit you are reviewing is missing images.	The deposit may not yet be fully transferred to your service organization.	Contact your Service Representative and ask them to help you determine the status of the deposit.
You are presented the same deposit for review multiple times.	When you refer a deposit, it is put back into the queue for Banking Operations review. If you are a Banking Operations person and you refer a deposit, then continue to review deposits, it is likely that the deposit you referred will once again be presented to you for review. In addition, if a referred deposit is the only one in the queue, it will continue to be presented to you or another Banking Operations person until it is completed (either accepted or rejected).	Review the deposit as usual, choosing to either reject or accept it, as appropriate.
<ul style="list-style-type: none">• The ____ adjustment of ____ exceeds the maximum allowable amount of ____.• The deposit of ____ exceeds the maximum allowable amount of ____.	The adjustment amount or deposit total amount you have specified exceeds the maximum allowable amount.	Lower the adjustment amount or deposit total amount below the specified maximum allowable amount.
Could not refer deposit, user with sufficient privileges could not be found.	You cannot refer the deposit because there are no users in the system that have the appropriate privileges to have deposits referred for their review.	Contact your Service Representative and request that users with Banking Operations privileges be added to the system.

Item Editing Issues

The following table describes possible issues you may encounter when editing items.

Field	Description	Resolution
<ul style="list-style-type: none"> The route and transit number must contain 9 numeric characters. The route and transit number appears to be invalid. This route and transit number has been configured by your service organization as invalid. 		Enter the correct nine-digit, numeric route and transit number as found on the image before accepting the item. If the route and transit number continues to be flagged as invalid, you may need to reject the item.
<ul style="list-style-type: none"> The ____ field contains non-numeric characters. The ____ field is empty or contains invalid characters. The Aux On-Us number contains non-numeric characters, or has more than 20 characters. The EPC field is invalid. 		Enter the numeric value as found on the image. All fields must contain numeric characters, except the Bank On-Us number, which can contain numbers, dashes, spaces, and the letter O or a forward slash (/) to replace the On-Us symbol. The Bank On-Us number can contain up to 20 numeric characters, and the Aux On-Us can contain up to 18 numeric characters.
The item amount you entered cannot be accepted.	The amount must be greater than \$0.00 and cannot exceed \$99,999,999.99.	Edit the amount as appropriate and accept the item again.
The length of the ____ comments field cannot be greater than ____ characters.		Shorten your entry in the specified comments field so that it contains fewer than the number of characters specified.

Finastra Support

Finastra support offers several options to help you get the most out of your software, including a self-service Case Management tool, and phone support.

Please visit the Finastra Customer Center at <https://customercenter.dh.com/> to log in to our online self-service Case Management system. If you forgot your password, simply click the [Forgot Password](#) link. Once logged in to Customer Center, you have the ability to use the Knowledge Center to troubleshoot issues and answer questions.

If your financial institution is not currently using these tools and would like to, please contact Finastra support for assistance.

Note: The Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act or GLB Act, includes provisions to protect consumers' personal financial information held by financial institutions. Therefore, Finastra support cannot accept data or screen captures that contain personal financial information via email or fax. For information about secure file transfer methods, contact Finastra support.



About Finastra

Finastra unlocks the potential of people and businesses in finance, creating a platform for open innovation. Formed in 2017 by the combination of Misys and D+H, we provide the broadest portfolio of financial services software in the world today—spanning retail banking, transaction banking, lending, and treasury and capital markets. Our solutions enable customers to deploy mission critical technology on premises or in the cloud. Our scale and geographical reach means that we can serve customers effectively, regardless of their size or geographic location—from global financial institutions, to community banks and credit unions. Through our open, secure and reliable solutions, customers are empowered to accelerate growth, optimize cost, mitigate risk and continually evolve to meet the changing needs of their customers. 48 of the world's top 50 banks use Finastra technology. Please visit finastra.com.

North American Headquarters

120 Bremner Boulevard
30th Floor
Toronto, Ontario M5J 0A8
Canada

T: +1 888 850 6656

