



Remote Deposit Capture Company Administration Guide

Contents

Introduction to Remote Deposit Capture.....	1
Overview of Roles	1
Session Timeouts and Maintenance.....	1
System Login	2
Standalone Login to RDC.....	2
Single-Sign-On from Online Banking Services.....	3
Online Banking.....	3
Treasury Management Services.....	3
mRDC App	3
User Management.....	4
Adding Users.....	4
Unlock a User.....	6
Removing a User.....	7
Adding New Deposit Accounts (Locations).....	8

Introduction to Remote Deposit Capture

Welcome to Mission Bank!

Our remote deposit capture (RDC) service allows you to make deposits from the convenience of your office. All you need is a computer with a compatible operating system, browser, scanner, and a high-speed internet connection. There is also a companion mobile deposit app (mRDC) for businesses that receive a small number of checks, or for payments collected outside of your office.

Since the RDC program was designed for business use, users can be allowed to make deposits to the business's accounts, but account transactions and/or account balances are not visible from the RDC site.

Overview of Roles

One or more company administrators ("admins") are established by Mission Bank. Admins will establish privileges and roles for persons within your organization, allowing users to complete tasks within the application.

Admins are able to:

- Create, delete, enable, or disable users
- Reset passwords and provide temporary passwords to users
- Unlock a user who has been locked out of the application
- Assign specific privileges and roles to a user

Based on the assigned role(s) provided by the admin, users will have the ability to:

- Set up customer profile information
- Process transactions
- Generate reports
- Research historical transactions
- Edit transactions
- Make deposits on a mobile device

Session Timeouts and Maintenance

RDC will automatically log off a user who has been inactive for 15 minutes. A *Session Timeout Warning* appears two minutes before the user is set to be logged out to give them an opportunity to remain logged in. If the user clicks anywhere on the screen the session will stay active.

You may occasionally see notices that the system will shut down temporarily for maintenance. This notice will appear as a bar at the top of the menu panel and will indicate the time and date when the system will shut down.

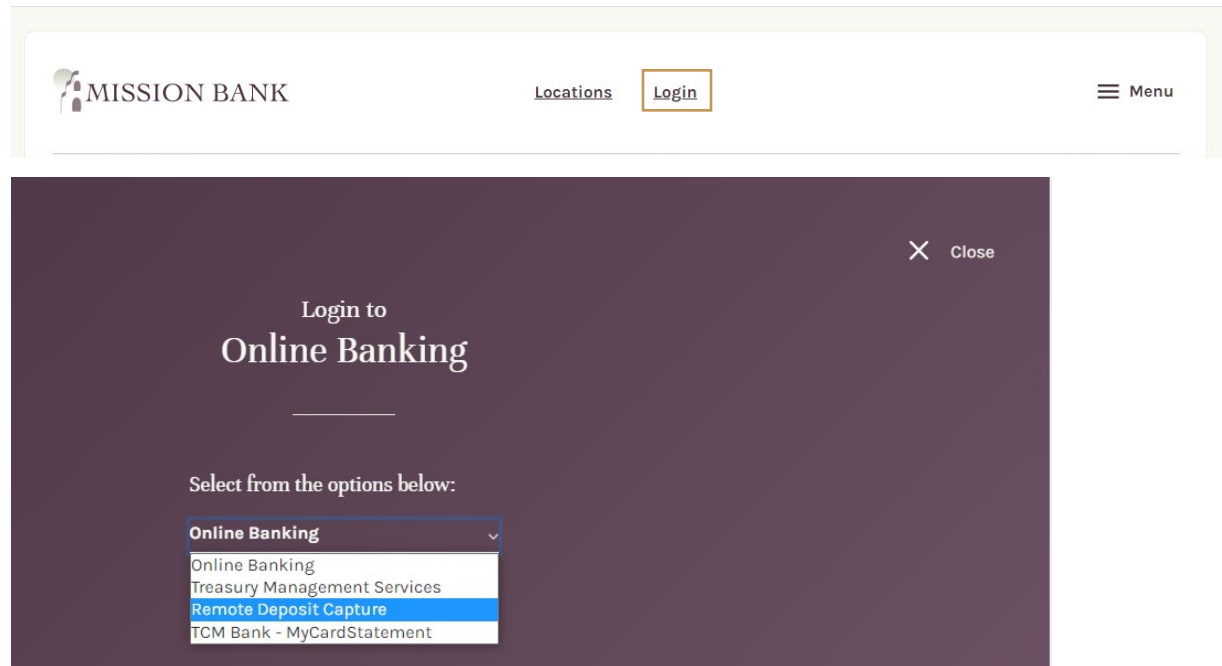
There may also be notices for changes or updates to the RDC system that will appear in the News panel on the dashboard screen.

System Login

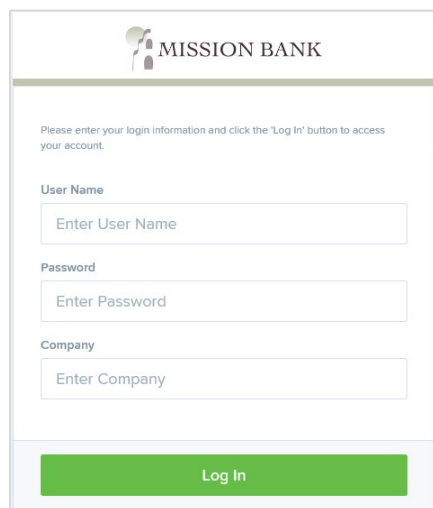
The RDC program can be reached two different ways:

1. A standalone login page to remote deposit is available for users without online banking access or for customers using our standard, single-user, online banking.
2. Online Banking or Treasury Management Services users can log in with single-sign-on to RDC through online banking.

There are login links on our website, www.missionbank.bank, for the options above.



Standalone Login to RDC

The image shows a screenshot of a standalone login form for RDC. At the top, the Mission Bank logo is on the left. Below the logo, there is a heading 'Please enter your login information and click the "Log In" button to access your account.' The form contains three input fields: 'User Name' with the placeholder text 'Enter User Name', 'Password' with the placeholder text 'Enter Password', and 'Company' with the placeholder text 'Enter Company'. At the bottom of the form, there is a green 'Log In' button.

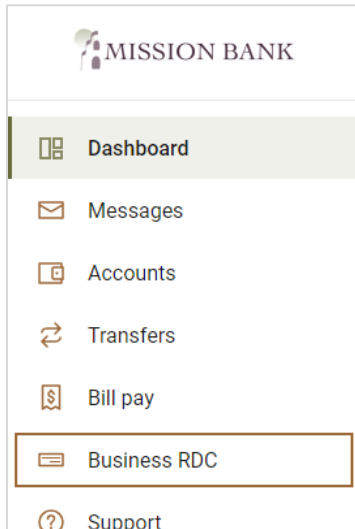
The menu option for Remote Deposit Capture, shown above, will take a user directly to the RDC program's login page. As stated above, this login page is most commonly used for users without online banking access, or for customers that do not have a multi-user online banking service.

You will be provided with the user name(s), temporary password(s), and company name that must be entered. The *User Name* and *Company* fields are not case sensitive; the *Password* field is case sensitive.

Single-Sign-On from Online Banking Services

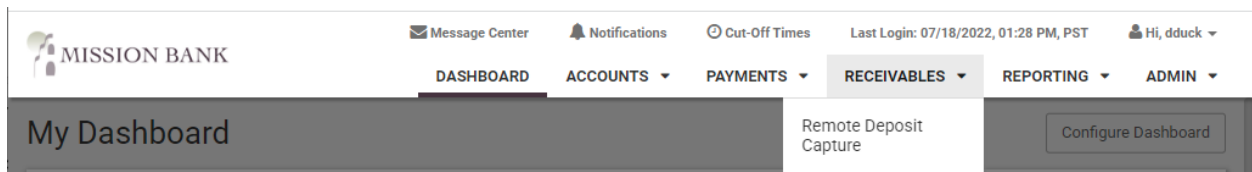
Online Banking

Users will log in using “Online Banking” (shown in the screen above). Once they are fully logged in, there is a link to “Business RDC” on the user’s dashboard that will allow access to RDC without a separate login.



Treasury Management Services

Treasury Management users can locate the single-sign-on link to RDC by clicking Receivables on the top menu bar.



mRDC App

mRDC is the companion mobile app for RDC and is used by customers with standalone RDC access or single-sign-on access through Online Banking. The app is available for iPhones or Android devices and can be found under *Mission Bank Business mRDC* in the app stores.

Users logging into the mRDC app must use their RDC user name, password, and company name, similar to the standalone login shown above.

Customers using Mission Bank’s Treasury Management Services do not need to use the separate mRDC app – the deposit functionality is built into the Treasury Management Services’ mobile app.

***Please Note:** A mobile device can be used in place of a scanner, but the RDC online program must be used to manage users, to research deposits, add new locations (accounts), and to run reports.*

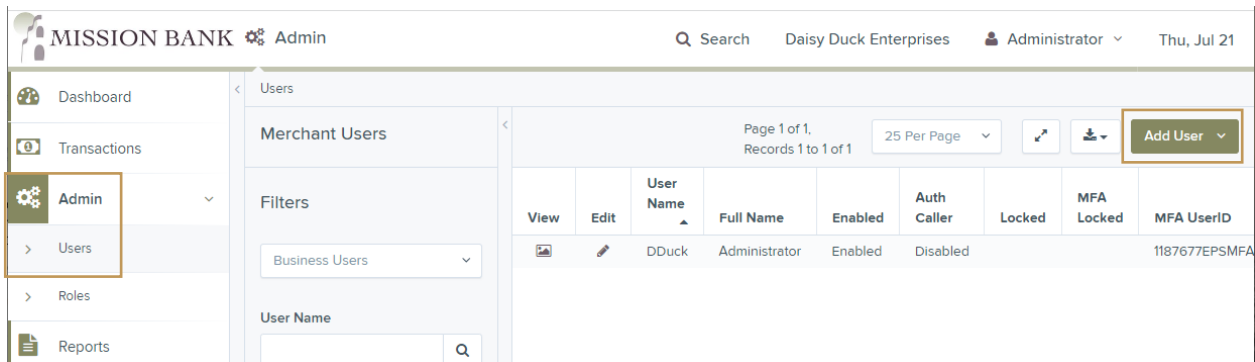
User Management

Admins are responsible for managing their company's users in RDC and/or mRDC. It is highly recommended that more than one admin be established for back-up purposes.

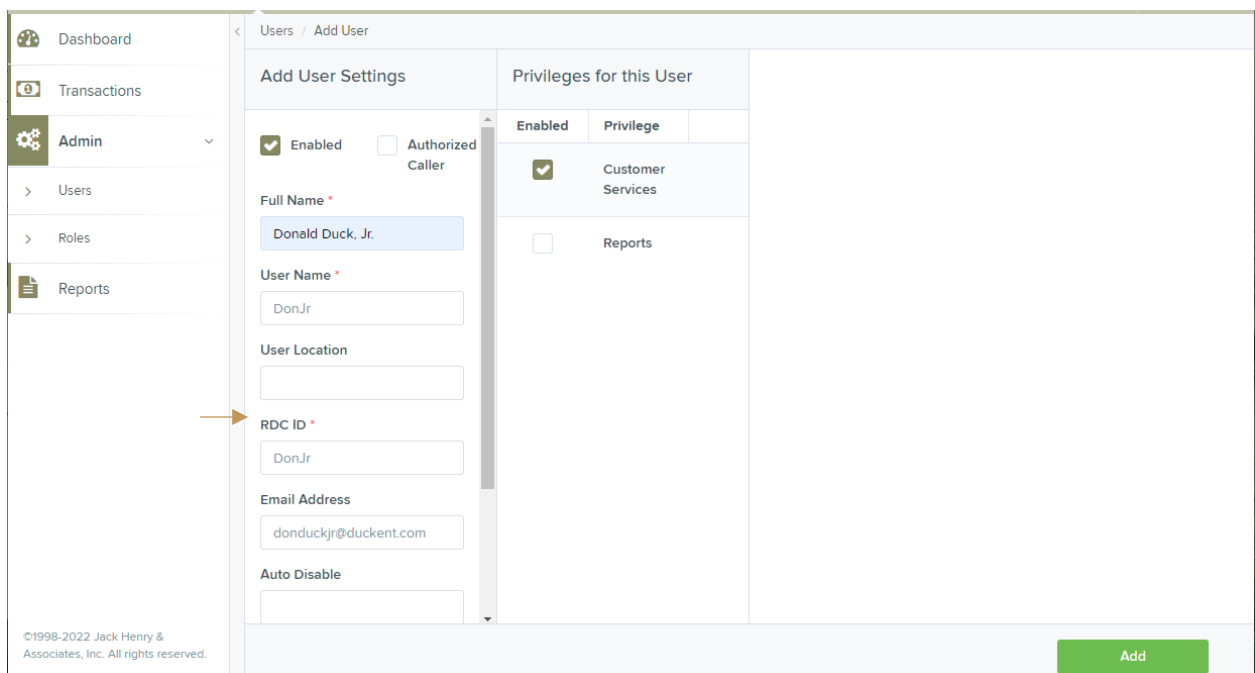
Adding Users

For security purposes, a user profile must be set up for each employee with access to RDC.

- Choose *Admin > Users* from the left navigation bar
- Then *Add User* in the upper right corner of the screen > *Business User*



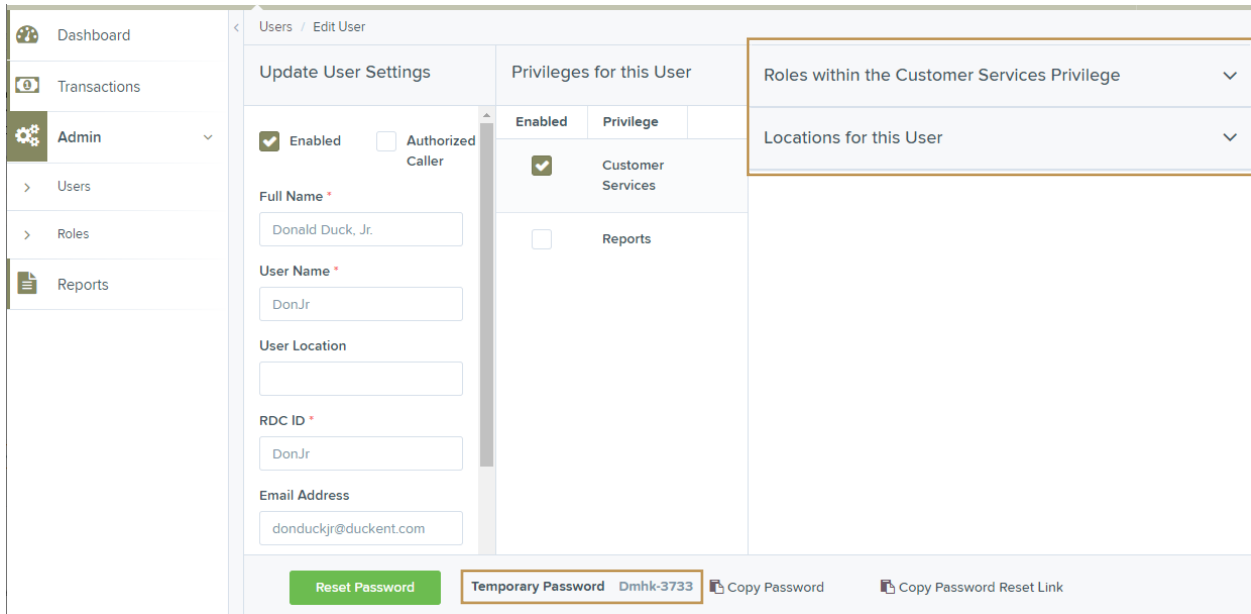
Next, complete the profile information for the user and select Customer Services under Privileges for this User. If you want to assign admin rights or single-sign-on from Online Banking to a new user, please call your Business Banker for assistance.



Please Note: the field above labeled "RDC ID" will appear for customers using Treasury Management Services, if using Online Banking the field title will be

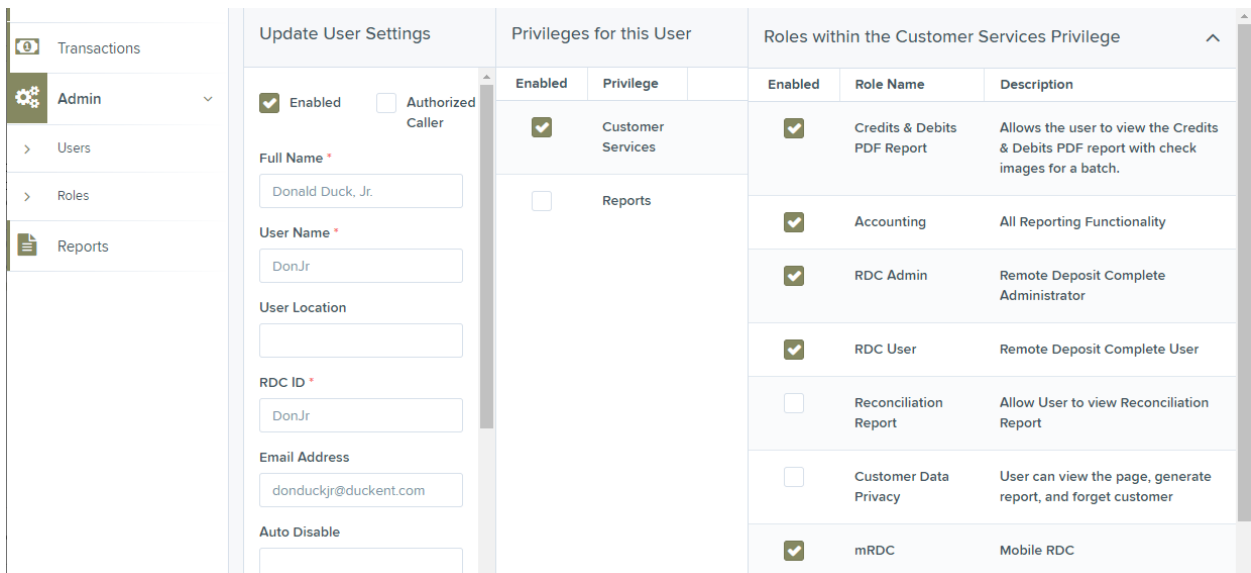
“Cash Mgmt ID”. This ID must exactly match their ID in either Treasury Management Services or Online Banking, or single-sign-on will not work. Contact your Business Banker for assistance.

After the user profile is added you will see *Roles within the Customer Services Privilege* and *Locations for this User*. A temporary password will also be generated – make note of it for the user’s first login if the user will be using the standalone login or mRDC.



Expand the Roles within the Customer Services Privilege and assign the user the necessary entitlements. The entitlements shown checked below will allow the user to scan and close a deposit, access the reporting that is available, and use the mobile app.

***Please Note:** The RDC Admin role below is needed for the user to release a deposit to the bank, they cannot manage other users.*



If desired, the deposit function can be placed in dual control, so that one user scans the checks and a different user releases deposits to the bank. To enforce dual control, assign either *RDC Admin* (this allows the user to release a deposit to the bank, but they cannot manage other users), or *RDC User* (allows the user to scan checks), but not both, to users.

The new user will also need accounts assigned under *Locations for this User*. Update the profile to save the changes.

Unlock a User

Users can get locked out of RDC when they enter their password incorrectly at least four times; or when requesting a new temporary password, they answer their secret question incorrectly.

If a user has forgotten their password they can request a new password directly from the RDC login screen (this must be done from a computer, it is not available on the mRDC app) and they will have to answer their secret question. A password reset link will be emailed.

The image shows two screenshots of the Mission Bank user interface. The left screenshot is the login page, featuring the Mission Bank logo at the top. Below the logo, there is a message: "Please enter your login information and click the 'Log In' button to access your account." A red error message states: "Invalid login. Please note that passwords are case sensitive. Did you forget your password? To request a new one, click 'Request Password'." The login form includes fields for "User Name" (containing "donjr"), "Password" (with the placeholder "Enter Password"), and "Company" (containing "daisy duck ent"). At the bottom, there are two buttons: a green "Log In" button and a white "Request Password" button with a green border. The right screenshot is the "Request Password" screen. It has a title "Request Password" and a message: "Answer the security question below to reset your password. A password reset link will be emailed to you." The form includes a "Question" field with the text "who's the boss" and an "Answer" field with the placeholder "Enter Answer". At the bottom, there are two buttons: a green "Request Password" button and a white "Return to Login" button with a green border.

When a user is unable to reset their password the company admin can unlock them.

The image shows a screenshot of the "Merchant Users" admin interface. On the left, there is a sidebar with "Admin" selected, and sub-items for "Users" and "Roles". The main area shows a table of users. The table has columns for "View", "Edit", "User Name", "Full Name", "Enabled", "Auth Caller", "Locked", "MFA Locked", and "MFA UserID". There are two rows of users. The first row is for "DDuck" (Administrator), and the second row is for "DonJr" (Donald Duck, Jr.). The "Locked" column for "DonJr" has a green "Unlock" button with a padlock icon. The table also shows "Page 1 of 1" and "Records 1 to 2 of 2".

View	Edit	User Name	Full Name	Enabled	Auth Caller	Locked	MFA Locked	MFA UserID
		DDuck	Administrator	Enabled	Disabled			1187677EPSM
		DonJr	Donald Duck, Jr.	Enabled	Disabled			1187677EPSM

If a new password is needed, click the edit symbol for that user and choose the *Reset Password* button at the bottom of the screen to generate a temporary password.

If MFA (multi-factor authentication) is locked, contact your Business Banker for assistance.

Removing a User

There are two ways to deactivate a user profile:

1. Disable it by unchecking the *Enabled* box
2. Delete the user profile

Disabling a profile allows you the ability to re-enable it should the user need access to RDC again in the future.

Deleting a profile removes it from view and it cannot be reactivated and the user name cannot be used again.

The screenshot shows the 'Edit User' form with the following details:

- Update User Settings:** Enabled, Authorized Caller
- Full Name:** Donald Duck, Jr.
- User Name:** DonJr
- User Location:** (empty)
- RDC ID:** DonJr
- Email Address:** donduckjr@duckent.com
- Auto Disable:** (empty)
- Privileges for this User:** Customer Services, Reports
- Roles within the Customer Services Privilege:** (empty)
- Locations for this User:** (empty)
- Buttons:** Reset Password, Delete User (highlighted), Update

A list of deleted user profiles is available, if needed.

The screenshot shows the 'Merchant Users' list with the following details:

- Filters:** Deleted Users (highlighted)
- Table:**

User Name	Full Name	Status
DipDuck	Dipsy Duck	Deleted

Adding New Deposit Accounts (Locations)

When a new account is opened your Business Banker needs to add it to your company's RDC profile.

After the account has been added to the company profile the admin can add the new account to themselves and/or each user that needs access for depositing.

The new account will be listed in the *Locations for this User* entitlement section and checking the box to the left of the account name enables it for the user. Once the profile is updated users will see the new location when they are creating new deposits.

The screenshot displays the 'Edit User' interface in the RDC Company Admin system. The left sidebar contains navigation options: Dashboard, Transactions, Admin (selected), Users, Roles, and Reports. The main content area is titled 'Users / Edit User' and is divided into three sections: 'Update User Settings', 'Privileges for this User', and 'Roles within the Administrator Privilege'.

Update User Settings: This section includes a 'Full Name' field with the value 'Administrator', a 'User Name' field with 'DDuck', a 'User Location' field, an 'RDC ID' field with 'DDuck', an 'Email Address' field with 'daisyduck@duckent.com', and an 'Auto Disable' field. There are checkboxes for 'Enabled' (checked) and 'Authorized Caller' (unchecked). A 'Reset Password' button is located at the bottom left of this section.

Privileges for this User: This section shows a table of privileges for the user:

Enabled	Privilege
<input checked="" type="checkbox"/>	Customer Services
<input checked="" type="checkbox"/>	Reports

Roles within the Administrator Privilege: This section lists three roles: 'Roles within the Administrator Privilege', 'Roles within the Customer Services Privilege', and 'Roles within the Reports Privilege', each with a dropdown arrow.

Locations for this User: This section shows a table of locations for the user:

Enabled	Location Name	Location Enabled
<input type="checkbox"/>	New Account #1	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Operating	<input checked="" type="checkbox"/>

An 'Update' button is located at the bottom right of the interface. A copyright notice '©1998-2022 Jack Henry & Associates, Inc. All rights reserved.' is visible in the bottom left corner.