

RDC SmartPay Business User Maintenance

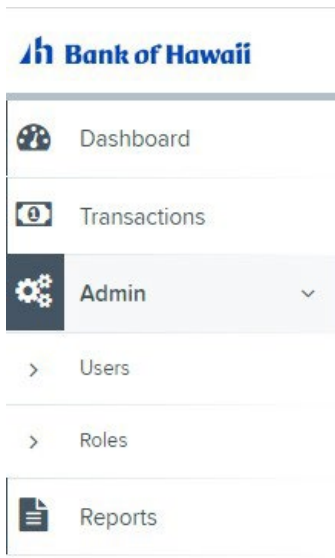
QUICK REFERENCE GUIDE

Admin users are responsible for creating user profiles for those completing tasks with the SmartPay Business application on a daily basis. The admin user is also responsible for updating user profiles, providing new passwords, unlocking users if they become locked out of the system, and deleting a user's profile if needed.

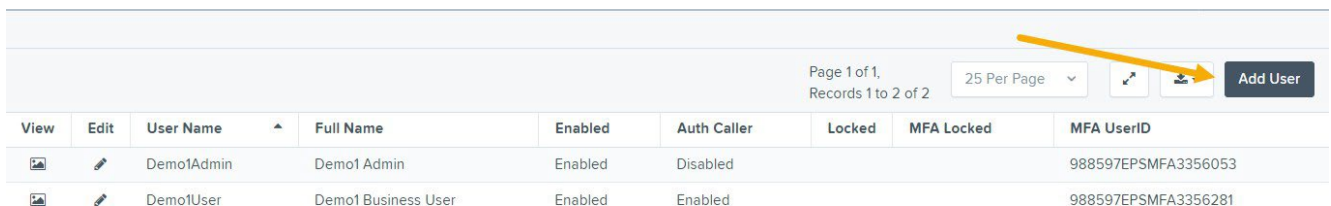
Accessing the Application

To access the RDC application, you must log in to the application with the proper URL and login credentials supplied by your organization admin user. Your admin user will receive their credentials from BOH Cash Management. To get to the proper URL, [please go to Remote Deposit Capture - Bank of Hawaii \(boh.com\)](#), and click on the RDC link. You can also find the most up to date contact information, in case you have any questions.

1. Once you log in to the Remote Deposit Now site, it will bring you to the home page. Here you would click on Admin.



2. Select **Add User**.

A screenshot of a user management table. 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 data. An orange arrow points to an 'Add User' button in the top right corner of the table area.

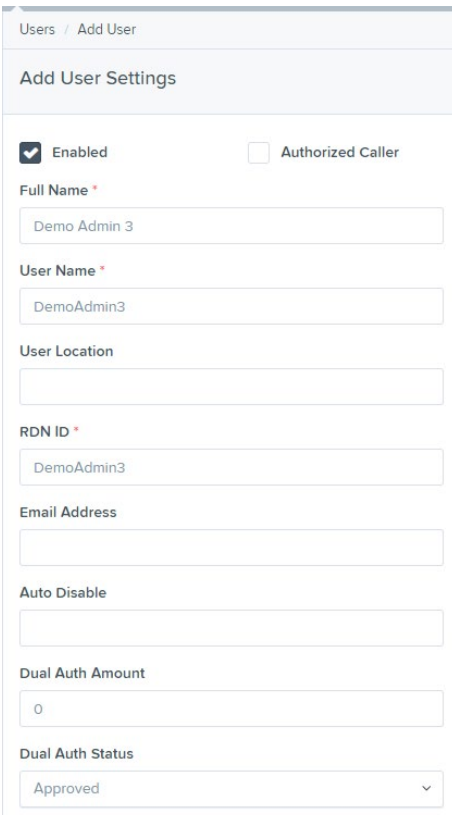
View	Edit	User Name	Full Name	Enabled	Auth Caller	Locked	MFA Locked	MFA UserID
		Demo1Admin	Demo1 Admin	Enabled	Disabled			988597EPSMFA3356053
		Demo1User	Demo1 Business User	Enabled	Enabled			988597EPSMFA3356281

3. Fill in the following required fields.

- **Full Name** – The first and last name of the user.
- **User Name** – The user's login name. This field is not case-sensitive.
- **RDN ID** – This field will create the RDN user on the backend. It can be the same as the profile user name. To avoid duplication of the user profiles, do not update this field after the original setup.
- **Email Address** – **This is not a required field, but is recommended, in case the user needs to reset their own password it sends them an email.**

Non-required fields:

- **User Location** – Optional informational field to describe the user.
- **Auto Disable** – Leave this field blank.
- **Dual Auth Amount** – Leave this field set to 0.
- **Dual Auth Status** – Leave this field set to Approved.



Users / Add User

Add User Settings

Enabled Authorized Caller

Full Name *

Demo Admin 3

User Name *

DemoAdmin3

User Location

RDN ID *

DemoAdmin3

Email Address

Auto Disable

Dual Auth Amount

0

Dual Auth Status

Approved



4. Check off any *Privileges for this User* sections.
 - a. *Privileges for this User* can now be assigned. Select the checkbox to each applicable role for the user and click the green **Update** button at the bottom of the page.
 - i. *Administrator* allows a user to add/modify/delete other users and reset other user passwords
 - ii. *Customer Services* allows a user to make deposits and see transactions

Privileges for this User	
Enabled	Privilege
<input checked="" type="checkbox"/>	Administrator
<input checked="" type="checkbox"/>	Customer Services

- b. Once you have selected privileges to provide to this user, click the green **Add** button. The system will create the user and allow you to select roles for each of the privileges assigned to them.
- c. Note that a **Temporary Password** is displayed at the bottom of the page—provide this password to the user you are creating along with their username and your Company login ID (ex. BOH0123).

Reset Password	Temporary Password <input type="text"/>	Copy Password	Copy Password Reset Link	Delete User	Update
--------------------------------	---	-------------------------------	--	-----------------------------	------------------------

5. Once privileges have been assigned to a user, you can now assign roles within each privilege as well as Locations the user is entitled to.
 - a. If you have created a user with the Administrator privilege, select the drop-down for *Roles within the Administrator Privilege* and select the *Admin* role.
 - b. If you have created a user with Customer Services privilege, select the drop-down for *Roles within the Customer Service* privilege, select the *Accounting* role for the user to run reports in the application. Select the *Remote Deposit Now* role for the user to scan checks to submit for deposit using RDN. Select *mRDC* role for the user to be able to use the mobile app to scan checks to submit for deposit through RDN. *Please note that the mRDC functionality is not available at this time. An update will be provided on the release of this functionality after our conversion to the new platform is completed.* All other roles are not applicable.
 - c. Select the drop down for *Locations for this User* and select appropriate check boxes to enable locations for which the user will have access to.

RDC SmartPay Business User Maintenance

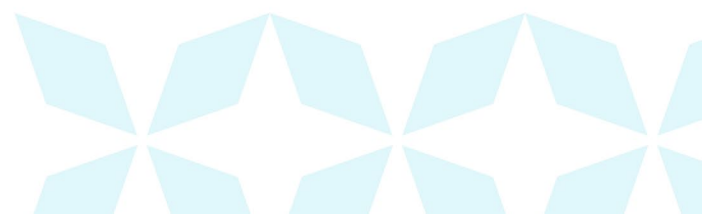
Roles within the Administrator Privilege		
Enabled	Role Name	Description
<input checked="" type="checkbox"/>	Admin	Merchant Administrator

Roles within the Customer Services Privilege		
Enabled	Role Name	Description
<input checked="" type="checkbox"/>	Accounting	All Reporting Functionality
<input type="checkbox"/>	RTG User / SERVER ONLY	Real Time Gateway, server to server activity only
<input checked="" type="checkbox"/>	Remote Deposit Now	Remote Deposit Now
<input type="checkbox"/>	Reconciliation Report	Allow User to view Reconciliation Report
<input type="checkbox"/>	Customer Data Privacy	User can view the page, generate report, and forget customer
<input checked="" type="checkbox"/>	mRDC	Mobile RDC

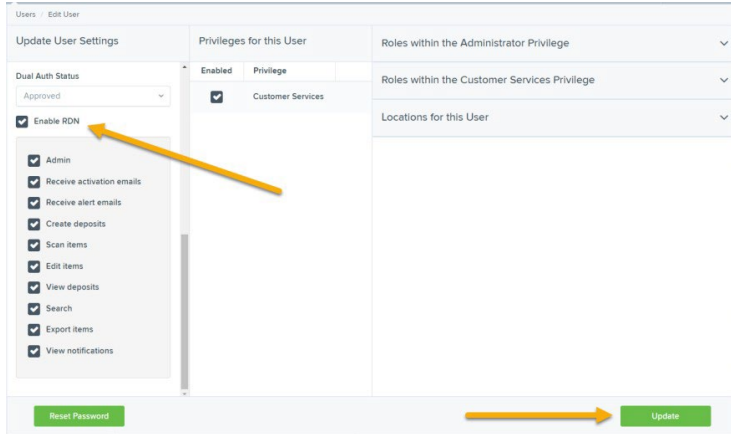
Locations for this User		
Enabled	Location Name	Location Enabled
<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/>	0000000123 BOH Demo RDN Location 10 LOC 96706	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	0000000124 BOH Demo RDN Location 1 LOC 96813	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	0000000456 BOH Demo RDN Location 2 LOC 96701	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	0000000789 BOH Demo RDN Location 3 LOC 96825	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	0000001234 BOH Demo RDN Location 4 LOC 96701	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	0001234567 Test Location LOC 4567	<input checked="" type="checkbox"/>

[Delete User](#) [Update](#)

6. Click the green **Update** button at the bottom of the page.



7. Enabling Remote Deposit Now (RDN) Features for a User Profile



Note: Remote Deposit Now (RDN) is the tool within SmartPay Business used to scan check deposits. To specify the permissions this user will have with RDN, select the check box next to the *Enable RDN* option on the *Update User Settings* page, and select green **Update** at the bottom of the page. You may need to scroll down within the *Update User Settings* pane to view this option. The page refreshes, and the various permissions to give a user profile appear.

- a. Select which RDN permissions the user will need from the options displayed.
 - **Admin Permission** – Separate from the account administrator role. This role is required to access the *Tools* tab, which allows the user to delete an existing batch.
 - **Receive Alert Emails** – Allows the user to receive deposit alert emails upon deposit.
 - **Scan Items** – Allows the user to scan items through RDN.
 - **View Deposits** – Allows the user to view deposits in RDN.
 - **Export Deposits** – Allows the user to export items.
 - **Receive Activation Emails** – Not applicable, do not check this box.
 - **Create Deposits** – Check this box to allow the user to make deposits to EPS.
 - **Edit Items** – Check this box to allow the user to be able to modify/fix their batches in RDN.
 - **Search** – This allows the user to perform searches in RDN on the Search page.
- b. **View Notifications** – This allows the user to view any deposit messages coming from EPS, such as exceeded transaction limits. Make any other changes to this profile and select green **Update** at the bottom of the page to finish and save changes.



Troubleshooting Tips

There are instances that may generate duplicate RDN alert emails. See below for two examples and ways to avoid those situations.

Duplicated email addresses – For every instance of the same email address that is entered into the merchant user's profiles in SmartPay Business, the application will send an email. For example, using the same email address for both the Admin profile and the merchant user will cause two identical emails to be sent to that address.

Updating the RDN ID – When the original RDN ID is created in the user profile, the application creates an RDN profile on the backend. If the RDN ID is changed after the initial setup, another RDN profile that is not visible to the customer will be created. This new RDN profile will contain the same information as the original profile, including the email address. This will result in multiple emails sent to the same address. To avoid this, do not make changes to the RDN ID.

Updating a User Profile


As the admin user, you also have the responsibility of enabling/disabling users, deleting a user, resetting a user's password, editing/updating user profiles, and designating authorized callers.

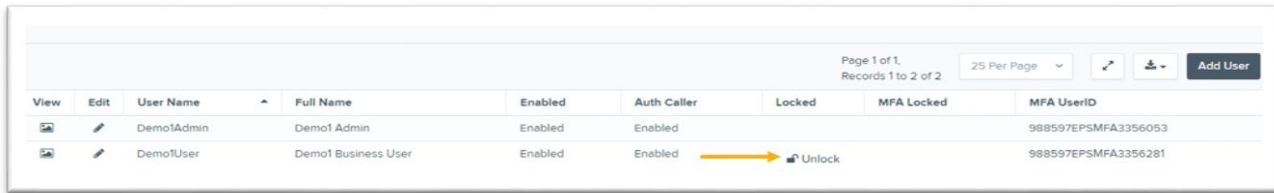
1. Log in and then select **Admin | Users** from the left main menu.
2. Select the **Edit** icon for the user profile to be updated (in this case, a user). You may also use the Filters bar to search by User Name or Full Name.
3. The *Update User Settings* page displays. Make any changes necessary to the user profile, privileges, roles, or locations for the user.
4. Click **Update** at the bottom of the page.

Unlocking a User Profile

Users can be locked out of the system for keying their password incorrectly five times or answering the secret question incorrectly when requesting a new temporary password.

As the admin user, you are responsible for unlocking an employee's profile. If an admin user is locked out, contact your first line of support for assistance. Follow the steps below to unlock a user's profile.

1. Log in and then select **Admin | Users** from the left main menu.
 2. Under the Locked column, select the **Unlock** option for that user. The Unlock will disappear, and the user profile will be unlocked.
- 

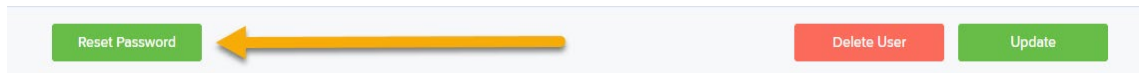


View	Edit	User Name	Full Name	Enabled	Auth Caller	Locked	MFA Locked	MFA UserID
		Demo1Admin	Demo1 Admin	Enabled	Enabled			988597EPSMFA3356053
		Demo1User	Demo1 Business User	Enabled	Enabled			988597EPSMFA3356281

NOTE: If the user needs a new password, you will need to reset the password (detailed below).

Resetting a Password Users may forget their password and ask you to provide them with a new, temporary one. The steps below explain how to reset a user's password.

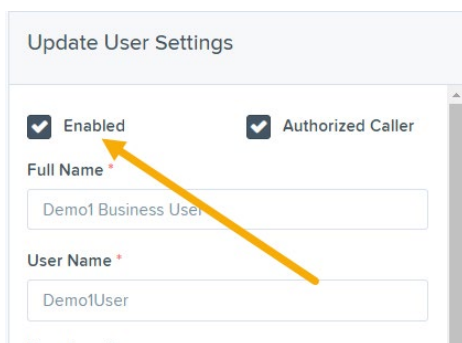
1. Log in and then select **Admin | Users** from the left main menu.
2. Select **Edit** for the user profile to update.
3. Select **Reset Password** button from the bottom of the page. The user's profile will have a case-sensitive temporary password generated. Carefully record this password and provide it to the user.



Disabling a user profile

Disabling a user keeps the profile intact until access is re-enabled by the admin user. The admin may want to disable a user if they are on leave for a long time before working with the application again.

1. Log in to the system, and then select **Admin | Users** from the left main menu.
2. Select **Edit** for the user profile you wish to disable.
3. Uncheck the **Enabled** box in the *Update User Settings* section.



Update User Settings

Enabled Authorized Caller

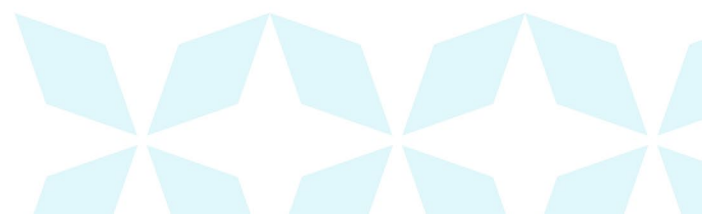
Full Name *

Demo1 Business User

User Name *

Demo1User

4. Select green **Update** to save all changes.

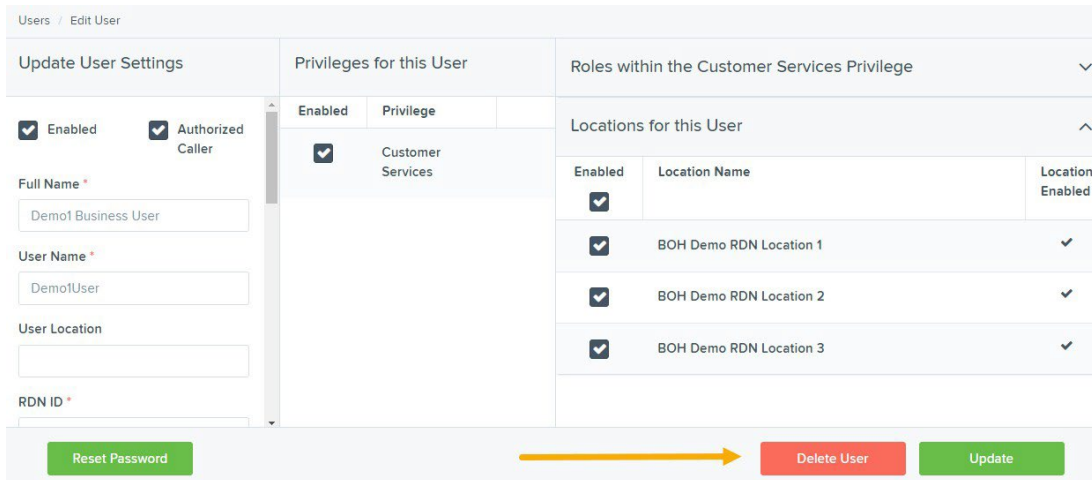


Deleting a User Profile

Deleting a user profile will remove it from the list of users and make it inaccessible. The *User Name* for that profile cannot be utilized again for a different user. The profile will be categorized as a deleted user.

To delete an admin, you must first remove the *Administrator* privilege from the user's profile before completing the following steps.

1. Log in to the system and then select **Admin | Users** from the left main menu.
2. Select **Edit** for the user profile to delete.
3. Select **Delete User**, as shown below.



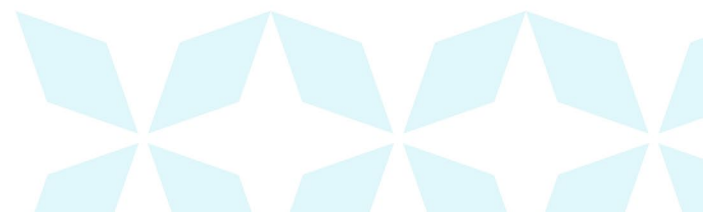
The screenshot shows the 'Edit User' page with the following sections:

- Update User Settings:** Includes checkboxes for 'Enabled' and 'Authorized Caller', and input fields for 'Full Name' (Demo1 Business User), 'User Name' (Demo1User), 'User Location', and 'RDN ID'.
- Privileges for this User:** A table with columns 'Enabled' and 'Privilege'. One entry is checked: 'Customer Services'.
- Roles within the Customer Services Privilege:** A dropdown menu.
- Locations for this User:** A table with columns 'Enabled', 'Location Name', and 'Location Enabled'. Three entries are checked: 'BOH Demo RDN Location 1', 'BOH Demo RDN Location 2', and 'BOH Demo RDN Location 3'.
- Buttons:** 'Reset Password' (green), 'Delete User' (red, highlighted with a yellow arrow), and 'Update' (green).

4. A prompt will ask you to confirm deleting the user. Select **Yes**.



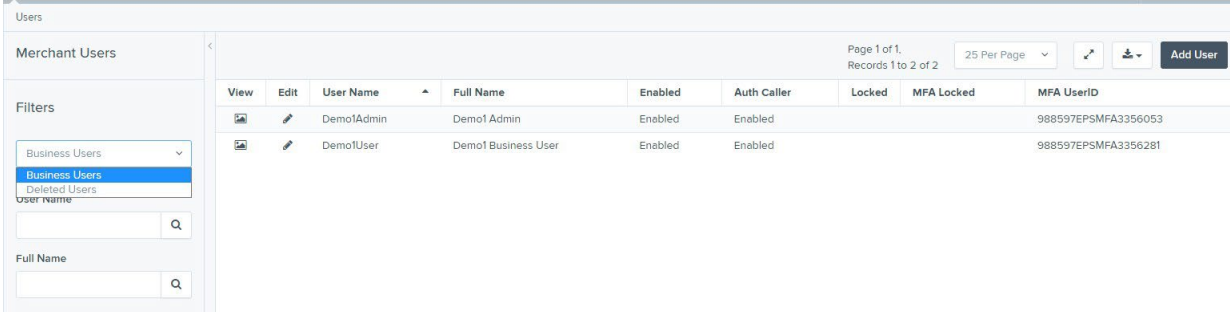
The dialog box is titled 'Confirm Delete' and contains the text: 'Are you sure you want to delete this user?'. At the bottom right, there are two buttons: 'Yes' (red) and 'No' (white).



Listing Deleted Profiles

A list of the user profiles that you have deleted is available if you need to refer to a previous user's profile information. This list will also provide the profile's audit history and any updates that may have been made to it.

1. Log in and then select **Admin | Users** from the left main menu.
2. In the *Merchant Users* section, select the **Deleted Users** option under *Filters*. The list of users will automatically update to display only deleted users.
 - a. Select **Clear Filters** to strip any filters from the list of users.



The screenshot shows the 'Users' management interface. On the left, there is a 'Merchant Users' section with a 'Filters' dropdown menu. The 'Filters' menu is open, showing 'Business Users' and 'Deleted Users' options. Below the menu are search fields for 'User Name' and 'Full Name'. The main area displays a table of users. The table has columns for 'View', 'Edit', 'User Name', 'Full Name', 'Enabled', 'Auth Caller', 'Locked', 'MFA Locked', and 'MFA UserID'. Two users are listed: 'Demo1Admin' and 'Demo1User'. The 'Demo1User' row is highlighted, indicating it is the selected user.

View	Edit	User Name	Full Name	Enabled	Auth Caller	Locked	MFA Locked	MFA UserID
		Demo1Admin	Demo1 Admin	Enabled	Enabled			988597EPSMFA3356053
		Demo1User	Demo1 Business User	Enabled	Enabled			988597EPSMFA3356281

