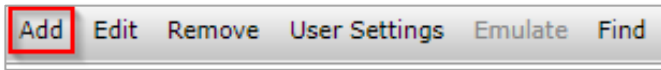
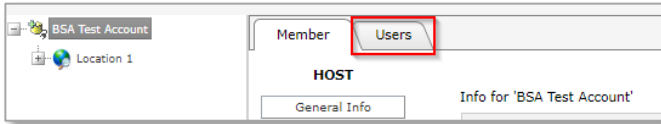


CLIENT USER ADMIN – GUIDE TO USER SET UP AND MAINTENANCE

This guide provides instructions on how to add, modify, and enable/disable Remote Deposit Capture system users. The guide will also provide instruction on how to lock or unlock users and reset their passwords.



Adding user to [BSA Test Account]

Login:

Full name:

Password:

Confirm:

Email Address:

Confirm Email Address:

Mobile Phone Number:
 Enter a valid mobile phone number

Password Profile:
 ▼

<input checked="" type="checkbox"/>	ZB - Image Research
<input checked="" type="checkbox"/>	ZB - Mobile
<input checked="" type="checkbox"/>	ZB - RDC Business
<input type="checkbox"/>	ZB - RDC Treasury
<input checked="" type="checkbox"/>	ZB - User Admin
<input checked="" type="checkbox"/>	ZB - View Reports

OK Cancel

ADDING A USER

STEP 1: ADDING A USER

- Select the Users tab and select *Add* at the bottom of the screen.
- Enter a **Unique Login ID** that is 4-20 characters long. Login ID must be unique across the entire Remote Deposit Capture system, if not, you will receive an error.
- Enter the user's full name. Full name can contain a maximum of 21 alphanumeric characters.
- Enter a temporary password and re-enter to confirm. Password must be at least 8 digits in length, must include at least one alpha character, one numeric character, and one upper case character.
- Enter the user's email address and re-enter to confirm.
- Do not change the Password Profile value.

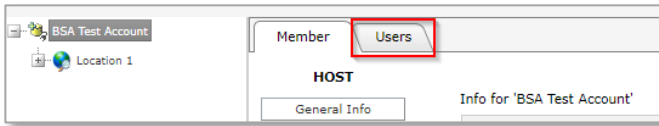
STEP 2: ASSIGN USER ROLES

- Roles should be assigned based on functions the user should perform in the system.
- Assign the user at least one of these roles: User Admin, Business or Treasury Remote Deposit Capture (based on application being used), View Reports, Image Research, and Mobile.
- Click on the box next to each role the user should have.
- Click *OK* to save the user profile.

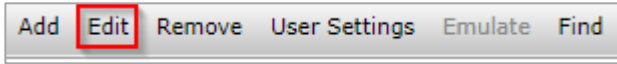
USER PROFILE MAINTENANCE

STEP 1: EDIT A USER PROFILE

- Select the **Users** Tab
- Click on the user to be modified.
- Click *Edit* at bottom of the screen to update user information.
- Change assigned roles by clicking on the box next to each role to add or remove the role.
- Click the *Enabled* box to enable or disable a user who should no longer have access to the system.
- Click the *Locked* box to unlock a user who is locked due to failed login attempts.
- Click *OK* to save the user profile changes.



Andreaabt	Andrea Test
Darrenabt	Darren Test
Eeshaabt	Eesha Test



<input type="checkbox"/>	ZB - Image Research	<input checked="" type="checkbox"/>	ZB - Image Research
<input type="checkbox"/>	ZB - Mobile	<input checked="" type="checkbox"/>	ZB - Mobile
<input checked="" type="checkbox"/>	ZB - RDC Business	<input checked="" type="checkbox"/>	ZB - RDC Business

Enabled:

Locked:

Enabled: <input type="checkbox"/>	Enabled: <input type="checkbox"/>
Locked: <input checked="" type="checkbox"/>	Locked: <input checked="" type="checkbox"/>

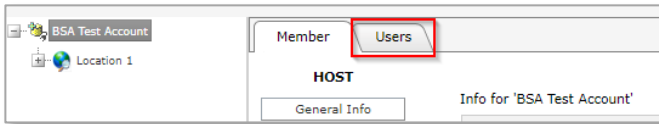
<input checked="" type="checkbox"/>	ZB - Image Research
<input checked="" type="checkbox"/>	ZB - Mobile
<input checked="" type="checkbox"/>	ZB - RDC Business
<input type="checkbox"/>	ZB - RDC Treasury
<input type="checkbox"/>	ZB - User Admin

OK Cancel

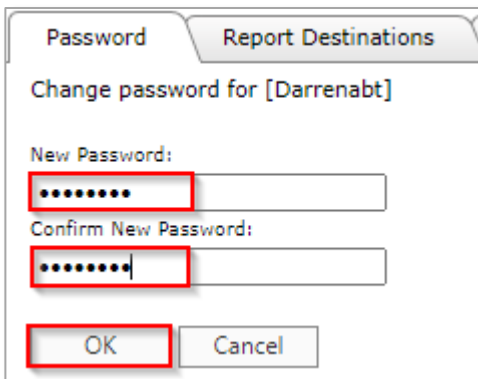
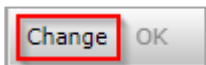
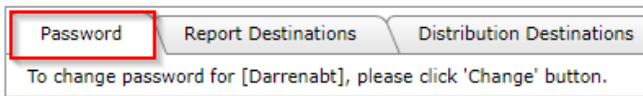
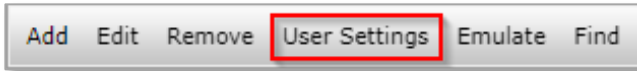
RESETTING USER PASSWORDS

STEP 1: TO RESET A USER PASSWORD

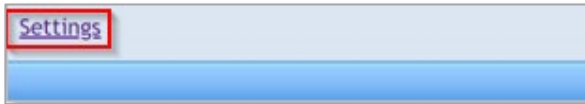
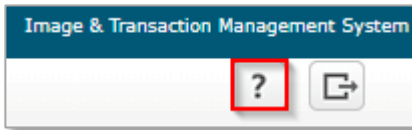
- Select the *Users Tab*
- Find and click on the user who needs to have their password reset.
- Select *User Settings* at the bottom of the screen.
- Select the *Password tab*.
- Click *Change* at the bottom of the screen.
- Enter a temporary password and re-enter to confirm. Password must be at least 8 digits in length, must include at least one alpha character, one numeric character, and one upper case character.
- Click *OK* when finished and click *OK* again to complete and acknowledge changes.
- Provide the user the temporary password to use the next time they log into the system.
- Upon their next login, the user will be prompted to create a new password.



Andreaabt	Andrea Test
Darrenabt	Darren Test
Eeshaabt	Eesha Test



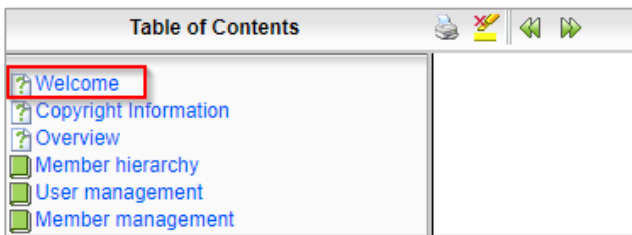
NOTE: These are some of the more common tasks you will perform as the remote deposit capture user administrator for your company. Additional information is available in the Administration guide located in the online help feature in the system.



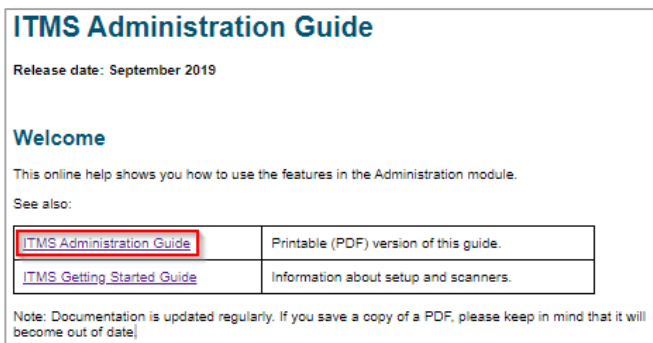
- Click the “?” icon in upper right corner (Treasury Remote Deposit Capture) or the Settings Button in the bottom left corner (Business Remote Deposit Capture)



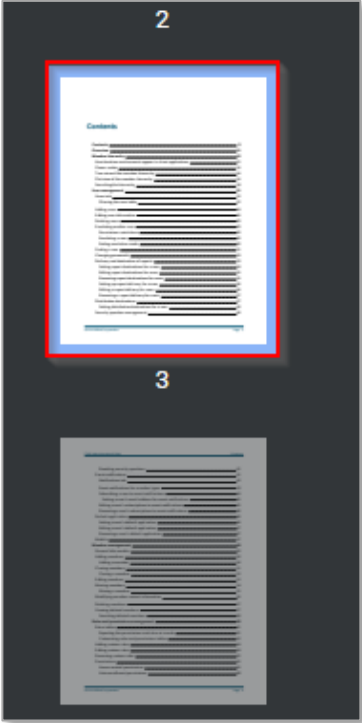
- Click the *Table of Contents* option in the bottom left margin.



- Click the *Welcome* table of contents option.



- Select the *ITMS Administration Guide* option.



- Click on the Contents page and click on User Management. Pages 21-33 cover the various tasks a User Admin may perform.

Contents

Contents	3
Overview	11
Member hierarchy	12
How locations and accounts appear in client applications	15
Owner codes	16
Tree view of the member hierarchy	16
Flat view of the member hierarchy	16
Searching the hierarchy	18
User management	21
Users tab	22
Filtering the user table	22
Adding users	24

Please reference Key Risk Mitigation Best Practices below and share with all Users who will be using the Remote Deposit Capture system.

REMOTE DEPOSIT CAPTURE KEY RISK MITIGATION BEST PRACTICES

PROCEDURAL BEST PRACTICES:

- Segregation of duties for personnel processing receipt of check payments, those preparing and submitting deposits via Remote Deposit Capture, and those reconciling accounts and statements is strongly recommended.
- Physical checks should be scanned, stored, and shredded in a secured area. Electronically captured check images, data, and any reports generated should be stored in a secured area.
- Securely store original checks between 14 days and 45 days. Immediately reconcile deposits to bank reporting and statements as they are available.
- Never share system credentials among users. Each user must be issued their own credentials for using the system.
- When processing a deposit, enter a control amount first to balance to when scanning of checks is completed.
- Confirm deposit is in balance and information is accurate before submitting each deposit.
- Routinely clean your scanner removing dust and any debris to help ensure proper performance.

DEPOSIT OF THE FOLLOWING ITEMS IS NOT PERMITTED AND COULD BE REJECTED:

- Checks drawn on foreign banks in foreign currency. Includes Canadian Checks in Canadian dollars or U.S. dollars.
- Checks payable to "Cash".
- Remotely Created Checks and Demand Drafts that do not have a maker signature.
- Checks that are irregular in any way (i.e., courtesy amount and written amount are different).
- Substitute checks (i.e., checks created from an electronic image).
- Checks you suspect are fraudulent or not properly authorized.
- Registered Government Warrants.
- Any checks that exceed transaction limitations that the bank may establish from time-to-time.
- Redeposit of Returned Checks (Must be taken to a branch).
- Check that are postdated or more than 6 months old.
- Third-party-issued-items outside the ordinary course of business" as noted in the Master Services Agreement.

CONGRATULATIONS, YOU ARE NOW READY TO BEGIN
SCANNING WITH REMOTE DEPOSIT CAPTURE.