LICENSE TERMS FOR JACK HENRY/ENTERPRISE PAYMENT SOLUTIONS PRIVATE LABEL MATERIALS

Jack Henry & Associates, Inc., acting through its Enterprise Payment Solutions division ("JHA"), by providing documentation to you the licensee ("You") for private labeling (the "Materials"), grants a limited license (the "License") to You to publish and distribute the Materials under Your private label, solely in connection with Your promotion, marketing, and support to Your customers of the applicable JHA solutions purchased and/or licensed by You from JHA. Your use of the Materials indicates your acceptance of the terms of this License.

This License does not convey any rights to alter the content of the Materials other than to apply Your private labels.

The Materials covered by this License include only items that are provided to You in a word processing format appropriate for revision; such items do not include files provided in the secured portable document format (PDF). All other documentation and materials provided to You by JHA are not covered by this License and may not be altered or privately labeled by You without JHA's prior written permission.

JHA retains all ownership rights to the Materials, including, but not limited to, in accordance with U.S. Code Title 17—Copyrights. Accordingly, You have no rights with regard to the Materials other than those rights specifically granted to You under this License. Without limiting the generality of the foregoing, JHA reserves the right to:

(a) require You to cease publication, distribution, and use of any Materials that JHA determines in its sole discretion can no longer be used due to content-related issues, including, but not limited to, outdated and inaccurate content;

(b) create new versions of the Materials and require You to replace prior versions of the Materials with the new versions;

(c) create derivatives of, or new versions of, the Materials without Your private labels for publication elsewhere without notifying You or obtaining Your permission; and

(d) monitor Your publication, distribution, and use of the Materials for compliance with the terms of this License, and take any action deemed necessary by JHA in its sole discretion to stop and/or remedy any conduct by You that violates the terms of this License, including, but not limited to, revoking the rights granted herein.

Nothing contained herein shall be construed as creating any agency, legal representative, partnership, or other form of joint enterprise between You and JHA, and neither You nor JHA shall have the authority to contract for or bind the other in any matter.

JHA warrants that it owns all copyright and other proprietary rights to the Materials, that JHA is authorized to grant the rights granted to You under this License. EXCEPT FOR THE FOREGOING WARRANTIES, JHA MAKES NO OTHER REPRESENTATIONS OR WARRANTIES OF ANY KIND, NATURE, OR DESCRIPTION, EXPRESS OR IMPLIED, WITH RESPECT TO THE MATERIALS, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR AS TO THE RESULTS TO BE OBTAINED BY YOU AS A RESULT OF YOUR USE OF THE MATERIALS IN YOUR BUSINESS, AND JHA HEREBY DISCLAIMS THE SAME.

The terms of this License apply to all Materials in Your possession or control now and in the future.

jack henry™

Enterprise Payment Solutions (EPS)

JHA SmartPay Business^{SM}

- April 2023

SmartPay Business (SPB) – User Administrator Handbook – Word version

Open-Source Statements

Some Jack Henry & Associates, Inc. ("JH") solutions incorporate open-source software ("OSS") pursuant to generally agreed upon open-source software protocols. JH's notice of use and attribution of OSS appears on this page of the *For Clients* site. Verified users may also request access to a copy of JH's notice of use and attribution of OSS by emailing legalintake@jackhenry.com with an email subject line titled, "Open Source Software Attribution."

Introduction

An administrator creates and maintains user profiles for employees within an organization and grants certain privileges and roles allowing users to perform tasks in the system.

An admin performs the following:

- Setting up employee user profiles
- Enabling or disabling users
- Editing user profiles
- Unlocking user profiles
- Deleting user profiles
- Resetting passwords and providing new temporary passwords
- Assigning specific roles or functions
- Designating certain users as authorized callers for support-related questions
- Enabling access to any and all accounts (locations) for employees to process

Based on roles assigned by an admin, users process transactions, generate reports, research historical transactions, edit transactions, and contact support.

For questions about the application, contact your first line of support. For a complete guide on how to run reports, see the *User Reports Handbook.*

User Terminology

This manual refers to certain parties and their responsibilities when managing your customers with this application. The following terms define who perform tasks in the system.

User Admin and FI/Partner Admin – Responsible for setting up user profiles. User Admins establish privileges and roles for users, allowing them to complete tasks within the application. These administrators have the ability to:

- Creating, deleting, enabling, or disabling a user.
- Resetting a password and providing a temporary password to a user.
- Unlocking a user.
- Assigning specific privileges and roles to a user.

NOTE: If the User Admin needs to perform tasks in managing customers or transactions, it is strongly recommended a separate user profile is created with the appropriate privileges and roles. Using a user profile helps specify which users are performing tasks and prevents miscommunication.

User – A person within your organization who is responsible for completing tasks within the application, as designated by the User Admin. Responsibilities for a user include:

- Setting up customer profile information.
- Editing transaction details.
- Generating reports.
- Processing transactions.

Customer – A client within your organization wishing to make deposits/donations.

Session Timeouts & Maintenance

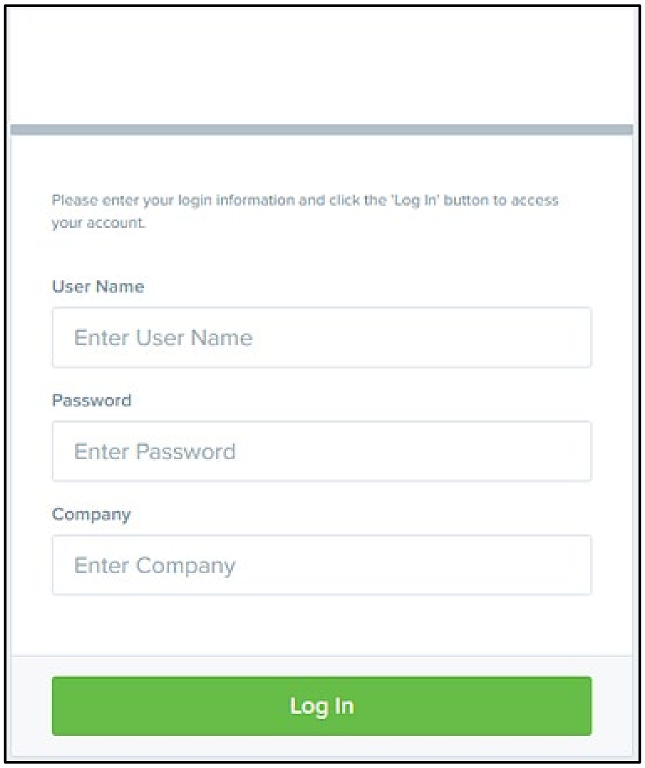
The system automatically logs off users who are inactive for at least 15 minutes. You receive a two-minute *Session Timeout Warning*. Click anywhere on the screen to remain logged in.

When the system shuts down for maintenance, find the notice at the top of your page. It appears as a bar. This notice indicates the time and date of the shutdown.

Admin: Getting Started

You are provided with your site's URL address, an admin user name, a temporary password, and a company name to enter the first time you log in to the system. Save the URL for future use, as it is a route of access into the system.

1. Once at the provided URL address, complete the **User Name**, **Password**, and **Company** fields. Select **Log In**.



Please enter your login information and click the 'Log In' button to access your account.

User Name

Enter User Name

Password

Enter Password

Company

Enter Company

FIGURE 1: LOGIN PAGE

2. The system prompts you to change your password. Passwords expire every 90 days and are case-sensitive. Use the following guidelines when creating a new password:
   - At least one uppercase letter
   - At least one lowercase letter
   - At least one number
   - 8–50 characters in length
3. Click **Update Password**.

Password Security

To help protect users' authentication credentials, each user needs a unique set of credentials. It is best to choose hard-to-guess passwords, including a mix of upper- and lowercase letters, numbers, and special characters. Take steps to protect passwords. Never write down a password or share it with anyone. Do not store passwords where they might be found.

Passwords reset every 90 days, and the previous four passwords cannot be reused.

If you suspect your password has been compromised, change it immediately. Five unsuccessful login attempts cause a user account to temporarily lock. To unlock an account, see the *Unlocking a User* section.

Creating a Secret Question

Your profile must include an email address where a new temporary password is sent if you forget your password. The email also allows you to make changes to your password unless you are locked out of your profile.

You must set up a secret question as a security measure before you can create a new password.

If you answer the secret question correctly, you receive an email with a new temporary password. Secret questions do not need to be a complete question or contain a question mark. The secret question and answer are not case-sensitive.

NOTE: Single sign-on users do not need to set up a secret question, but they do need to set up an authorized caller question.

1. Log in to the system.
2. Select **User menu | My Settings**.

IMPORTANT: Screenshots are provided for general orientation. Your screens and menu options may differ from the examples pictured in this document.

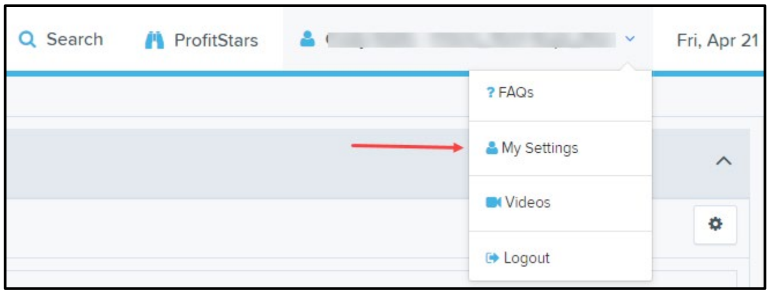
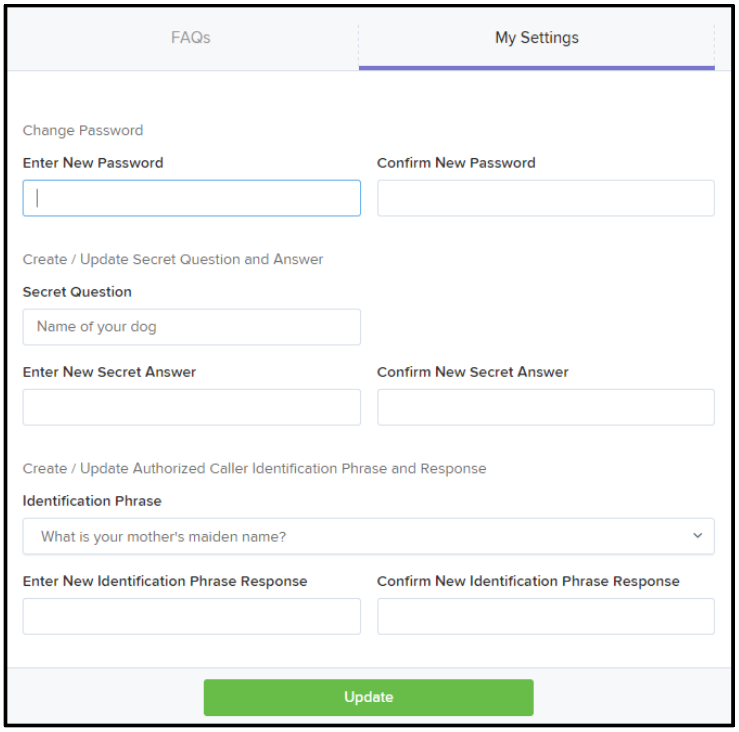


FIGURE 2: MY SETTINGS

The system prompts you for your current login password to reach the *My Settings* page. Once there, make changes to the sections regarding passwords, secret question and answer, and authorized caller, as needed.

Select **Update** when finished.



FAQs | My Settings

Change Password

Enter New Password

Confirm New Password

Create / Update Secret Question and Answer

Secret Question: Name of your dog

Enter New Secret Answer

Confirm New Secret Answer

Create / Update Authorized Caller Identification Phrase and Response

Identification Phrase: What is your mother's maiden name?

Enter New Identification Phrase Response

Confirm New Identification Phrase Response

Update

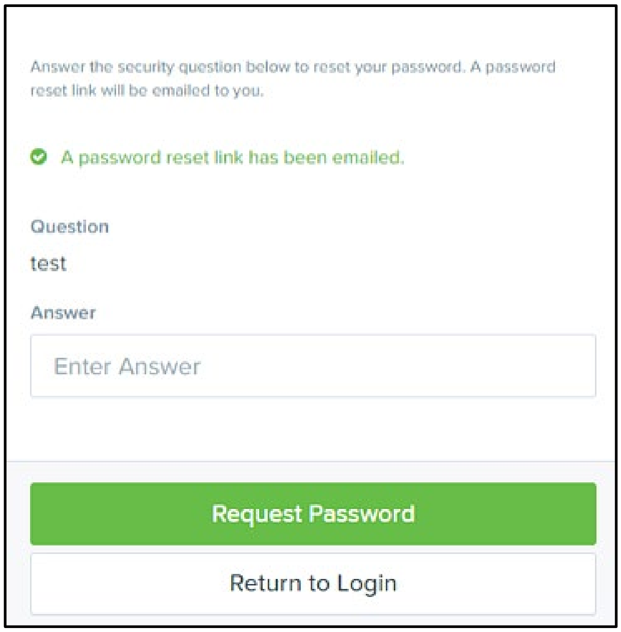
FIGURE 3: MY SETTINGS PAGE

3. Enter an answer in the **Enter New Secret Answer** field and again in the **Confirm New Secret Answer** field. Make changes to your password if needed.
4. Click **Update** when finished.

Self-Service Password Reset

Users reset passwords using the password rest link. To reset a password:

1. Click **Request Password**.
2. Answer the security question.
3. Click **Request Password**. A notification window appears, to confirm that a password is being emailed to you.



Answer the security question below to reset your password. A password reset link will be emailed to you.

✓ A password reset link has been emailed.

Question

test

Answer

Enter Answer

FIGURE 4:RESETTING PASSWORD LINK NOTIFICATION

4. From your email, click the provided link. Existing users have one hour to use the link. New users have one day.
5. After the *Security Challenge* page opens in your browser, answer the security question a second time.
6. Click **Submit Answer**.
7. On the next page, complete the **New Password** and **Confirm Password** fields.
8. Click **Update Password**. A *Password Update Complete* notification appears.
9. Return to the *Login* page to submit your updated password.

Updating a User Profile

As the User Admin, you need to update your profile with an email address where a new temporary password can be sent.

1. Log in to the system.
2. Select **Admin | Users** from the left main menu.

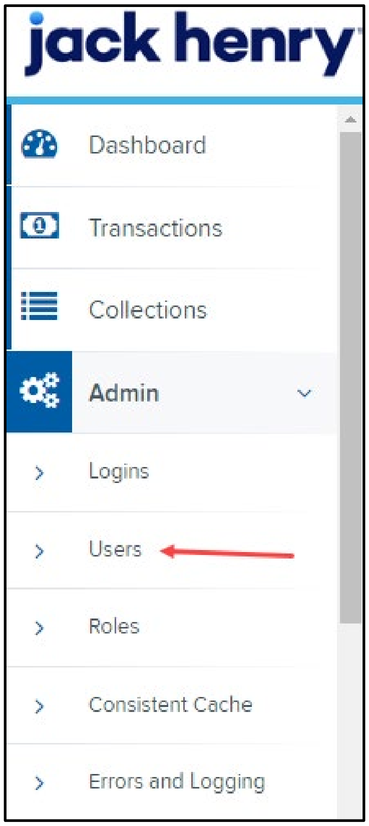
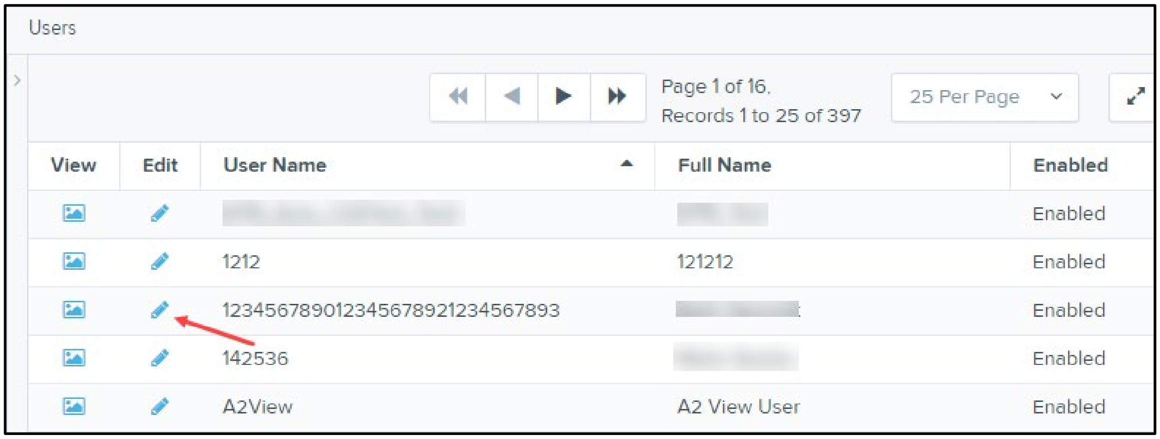


FIGURE 5: ADMIN TAB, USERS SUB-OPTIONS

3. Select ✎ **Edit** to choose the user profile to update.


Users

Page 1 of 16.
Records 1 to 25 of 397

25 Per Page

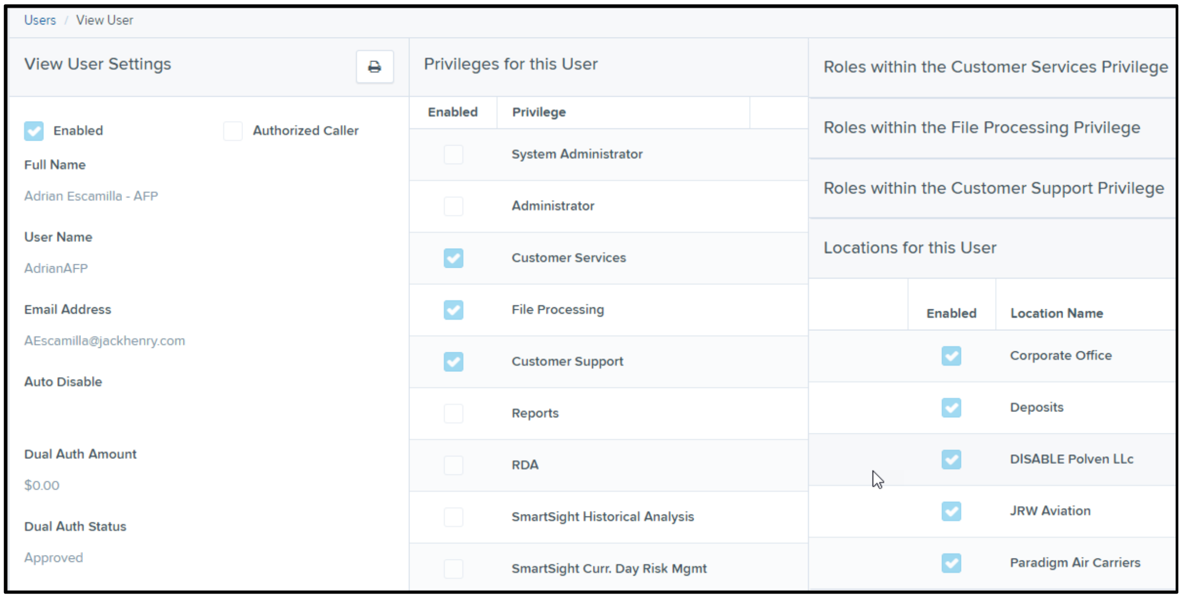
View	Edit	User Name	Full Name	Enabled
🖼	✎	[redacted]	[redacted]	Enabled
🖼	✎	1212	121212	Enabled
🖼	✎	123456789012345678921234567893	[redacted]	Enabled
🖼	✎	142536	[redacted]	Enabled
🖼	✎	A2View	A2 View User	Enabled

FIGURE 6: EDIT USER OPTION

4. Change any of the *Update User Settings*, *Privileges for this User, Roles,* and *Locations for this User* sections.

NOTE: The **Email Address** field is in the *Update User Settings* section.

5. Click **Update** to save all changes.



Users / View User

View User Settings

☑ Enabled ☐ Authorized Caller

Full Name

Adrian Escamilla - AFP

User Name

AdrianAFP

Email Address

AEscamilla@jackhenry.com

Auto Disable

Dual Auth Amount

$0.00

Dual Auth Status

Approved

Privileges for this User

Enabled	Privilege
☐	System Administrator
☐	Administrator
☑	Customer Services
☑	File Processing
☑	Customer Support
☐	Reports
☐	RDA
☐	SmartSight Historical Analysis
☐	SmartSight Curr. Day Risk Mgmt

Roles within the Customer Services Privilege

Roles within the File Processing Privilege

Roles within the Customer Support Privilege

Locations for this User

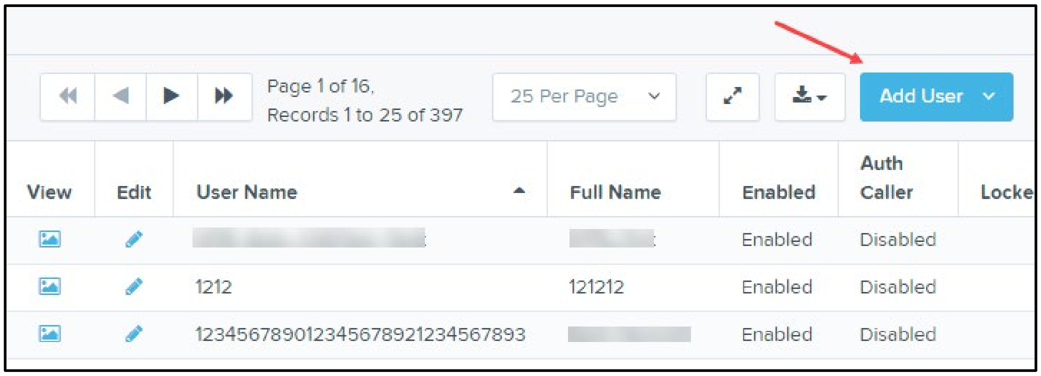
Enabled	Location Name
☑	Corporate Office
☑	Deposits
☑	DISABLE Polven LLc
☑	JRW Aviation
☑	Paradigm Air Carriers

FIGURE 7: EMAIL ADDRESS ON UPDATE USER SETTINGS PAGE

Creating a User

Administrators create users who work with transactions, reports, or other tasks within the system on a daily basis. The Admin also updates a user's profile, provides new passwords, unlocks a user's profile, and deletes a user's profile.

1. Log in to the system.
2. Select **Admin | Users** from the left main menu.
3. From the left navigational bar, under the *User Admin* heading, select **Add User**.



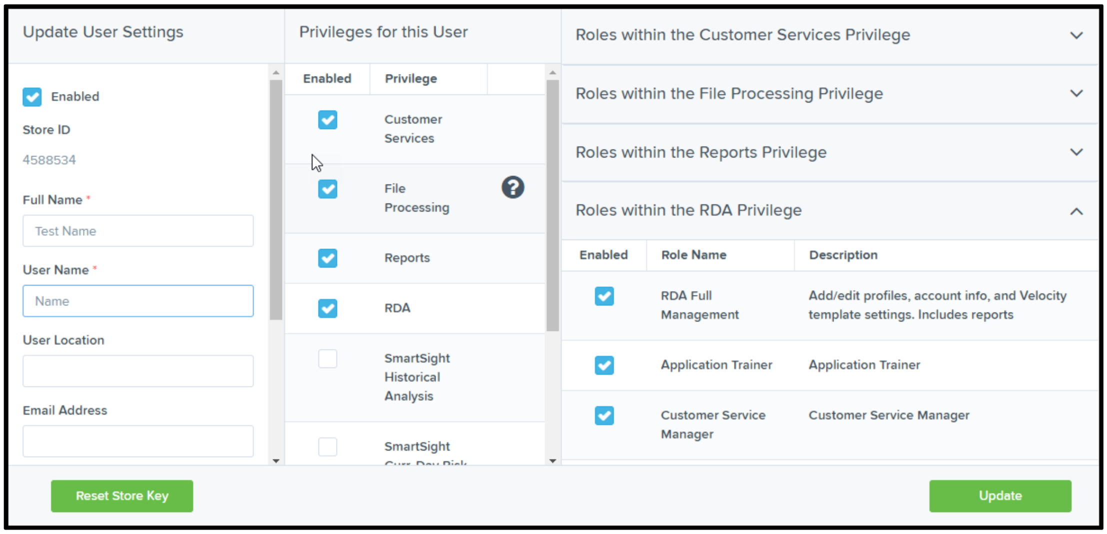
View	Edit	User Name	Full Name	Enabled	Auth Caller	Locke
🖼	✎	[redacted]	[redacted]	Enabled	Disabled	
🖼	✎	1212	121212	Enabled	Disabled	
🖼	✎	123456789012345678921234567893	[redacted]	Enabled	Disabled	

FIGURE 8: ADD USER OPTION

4. Fill out the *Add User Settings* and the *Privileges for this User* sections. Note that a temporary password appears at the bottom of the page. Provide this password to the user you create.
5. Select the **Authorized Caller** check box to allow a user to contact EPS for support. Once enabled, the user must establish an **Authorized Caller Identification Phrase** the EPS Customer Support representative uses to verify authorization. Callers who cannot answer their identification phrase are directed to their financial institution for further assistance.
6. After you select privileges for this user, click **Add**.

The system creates the user and allows you to select roles underneath each of the privileges assigned to them. For a complete list, see *Appendix A: Privileges and Roles*.

7. Select roles for this user
8. Select the locations for this user.
9. Click **Update** to finish assigning privileges and roles for this user.



Update User Settings

☑ Enabled

Store ID

4588534

Full Name *

Test Name

User Name *

Name

User Location

Email Address

Privileges for this User

Enabled	Privilege
☑	Customer Services
☑	File Processing
☑	Reports
☑	RDA
☐	SmartSight Historical Analysis
☐	SmartSight

Roles within the Customer Services Privilege

Roles within the File Processing Privilege

Roles within the Reports Privilege

Roles within the RDA Privilege

Enabled	Role Name	Description
☑	RDA Full Management	Add/edit profiles, account info, and Velocity template settings. Includes reports
☑	Application Trainer	Application Trainer
☑	Customer Service Manager	Customer Service Manager

FIGURE 9: UPDATING A USER

Assigning Privileges and Roles

The administrator assigns the appropriate privileges and subsequent roles to users' profiles. Users must be given a privilege before roles under that privilege are assigned.

The following table lists the most common roles associated with the *Customer Services* privilege.

Role	Definition
Accounting	Allows a user to run reports, balance all checking and credit card transactions, look at transaction details, edit transactions, view check images, and monitor and research transactions.
Accounting – Approve Check Only	In conjunction with the Dual Authorization feature within a user's profile, this role designates the user as the second person who approves a transaction in the *Awaiting Approval* status. The different user made the transaction.
Accounting – User Role	A user with this role cannot access the *Transaction Status Summary* on the home page of the application.
Credit Card	Allows a user to process scanned and card-not-present transactions.

Credit Card View Only	Allows a user to view payment screens concerning credit card information but not to process a payment.
Edit ACH Opt Out	Allows a user to edit the ACH Opt Out list.
Preauthorized Recurring Credit	Allows a user to set up recurring ACH credits that customers use to pay creditors. **NOTE:** This feature is not used for payroll.
Preauthorized Single Credits	When enabled, a user creates a one-time manual ACH credit or partial refund. Alternatively, the customer creates a payment to their creditor.
Preauthorized Single Debits	Allows a user to create a one-time customer-authorized ACH debit transaction.
QB Admin	Allows a user to set up the link to the QuickBooks® account and export transaction files to QuickBooks®.
Refund	Allows a user to create refunds (complete reversals) of already-processed ACH transactions.
RDC Admin	Allows a user to create, scan, and submit items as a transaction.
RDC User	Allows a user to create and scan items, but not submit them as a transaction.
RDS User	Allows a user to create, scan, and submit an item as a transaction.
RTG User	If enabled, third-party vendor files are sent through Real Time Gateway.
Telephone Payment	Allows a user to create a customer-authorized ACH payment received via the telephone.
View ACH Opt Out	Allows a user to view a list of customers who have opted not to have their transactions processed as ACH items.
View ACH Opt Out Account	Allows a user to view, add to, and edit the ACH Opt Out list, and view a customer’s complete account number instead of just the last four digits.

View Batch Images (Debits & Credit Report)	Allows a user to access to the batch image file to print, save, or view.

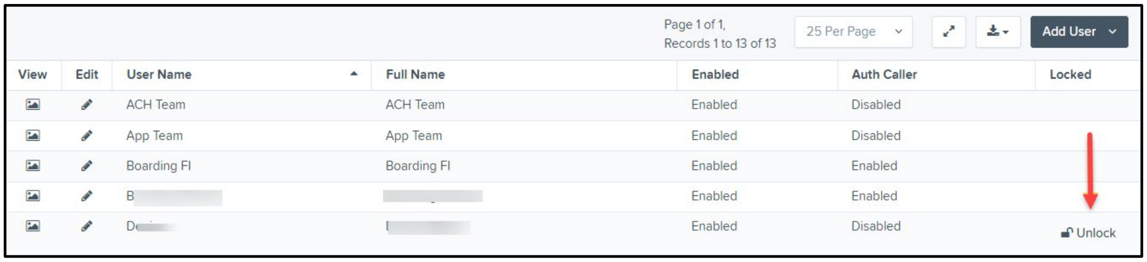
After selecting the roles you wish to enable for the user, select **Update** to save all changes.

Unlocking a User

The system locks out users who key a password incorrectly at least five times or fail to answer the secret question correctly when requesting a temporary password.

As the Admin, you are responsible for unlocking FI user profiles to allow access to the system again. If the Admin user is locked out, contact your first line of support for assistance. To unlock a user:

1. Log in to the system.
2. Select **Admin | Users** from the left main menu.
3. Under the *Locked* column, select the **Unlock** option for that user. The **Unlock** text disappears, and the user profile unlocks.



Page 1 of 1,
Records 1 to 13 of 13

View	Edit	User Name	Full Name	Enabled	Auth Caller	Locked
		ACH Team	ACH Team	Enabled	Disabled	
		App Team	App Team	Enabled	Disabled	
		Boarding FI	Boarding FI	Enabled	Enabled	
		[redacted]	[redacted]	Enabled	Enabled	
		[redacted]	[redacted]	Enabled	Disabled	Unlock

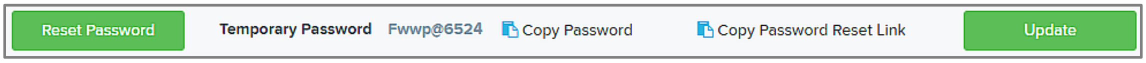
FIGURE 10: UNLOCK OPTION

NOTE: If the user needs a new password, reset the password following the steps in the *Resetting a Password* section.

Resetting a Password

1. Log in to the system.
2. Select **Admin | Users** from the left menu.
3. Select **Edit** to display the *Edit User* page.
4. Select **Reset Password** at the bottom of the page. The user's profile generates a case-sensitive, temporary password.

5. Click **Copy Password** to manually send the temporary password to a user or click **Copy Password Reset Link** to manually send the user a link.



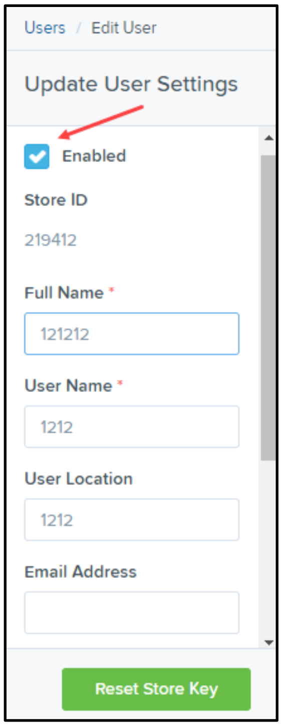
Temporary Password Fwwp@6524

FIGURE 11: SPB RESET PASSWORD BUTTON WITH COPY PASSWORD/COPY PASSWORD RESET LINK

Disabling a User

Disabling a user keeps the profile intact until the Admin re-enables the account. The Admin disables users who are on leave for an extended period of time before working with the application again.

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



Update User Settings

☑ Enabled

Store ID

219412

Full Name *

121212

User Name *

1212

User Location

1212

Email Address

FIGURE 12: DESELECTING THE ENABLED CHECK BOX

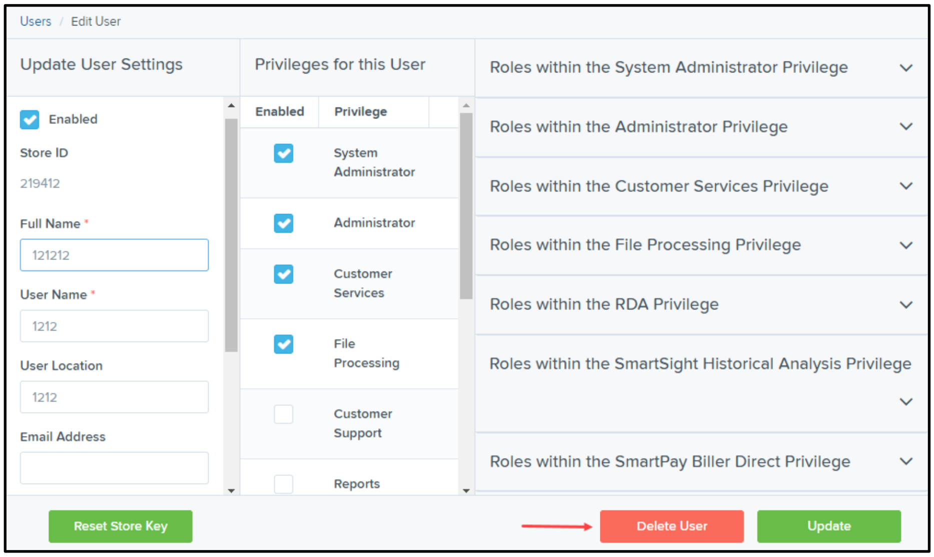
5. Click **Update** to save all changes.

Deleting a User's Profile

Deleting a user profile removes it from the list of users and makes it inaccessible. The user name for that profile cannot be used again. The profile is categorized as a deleted user.

To delete an admin, you must first remove the *Administrator* role from the user's profile. Then:

1. Log in to the system.
2. Select **Admin | Users** from the left main menu.
3. Select ✏ **Edit** for the user profile to delete.
4. Select **Delete User**.


Users / Edit User
Update User Settings
Privileges for this User
Roles within the System Administrator Privilege
Roles within the Administrator Privilege
Roles within the Customer Services Privilege
Roles within the File Processing Privilege
Roles within the RDA Privilege
Roles within the SmartSight Historical Analysis Privilege
Roles within the SmartPay Biller Direct Privilege
Reset Store Key
Delete User
Update

☑ Enabled

Store ID

219412

Full Name *

121212

User Name *

1212

User Location

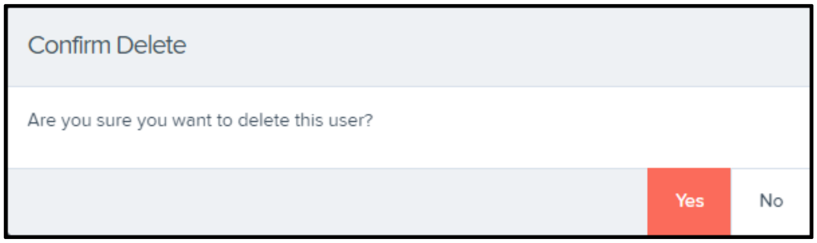
1212

Email Address

Enabled	Privilege
☑	System Administrator
☑	Administrator
☑	Customer Services
☑	File Processing
□	Customer Support
□	Reports

FIGURE 13: DELETE USER OPTION

When the confirmation prompt appears, select **Yes**.



Are you sure you want to delete this user?

FIGURE 14: DELETE USER CONFIRMATION

Listing Deleted User 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 also provides the profile's audit history and any updates made to it.

1. Log in to the system.
2. Select **Admin | Users** from the left main menu.
3. In the *Merchant Users* section, select the **Deleted Users** option under *Filters*. The list of users automatically updates to display only deleted users.

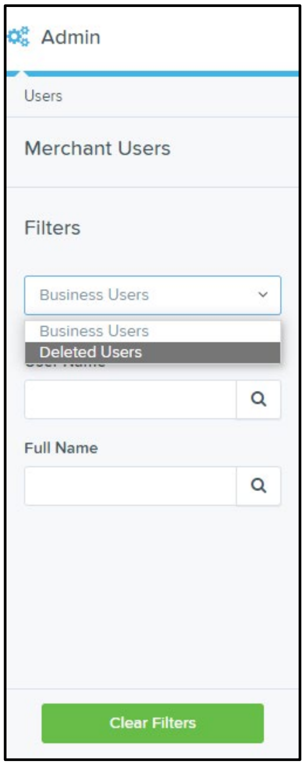


FIGURE 15: DELETED USERS FILTER

4. Click **Clear Filters** to remove any filters from the list of users.