



FIRSTBase User Guide

This User Guide provides users with instructions for login, MFA, account maintenance and User Management.



Table of Contents

Logging into FIRSTBase	3
Setup MFA Device	4
Logging into FIRSTBase with MFA	9
MFA Bypass	10
Reset MFA Device	11
Update Account Settings	12
Forgot Password	13
User Management	15
Add New FIRSTBase User	17
Setting User Permissions	18
Unlocking Users/Resetting Passwords	20
Reset a User's MFA Device	21
Grant MFA Bypass	22
Deleting A User	23
FIRSTBase Permissions	24



Welcome to FIRSTBase.

FIRSTBase is Kasasa's fully integrated content, lead and application management platform. Within FIRSTBase you can review and approve applications, track an agent's follow-up with applicants quickly and easily, update account disclosures update, make changes to your website and download ACH files,

Logging into FIRSTBase

A screenshot of the KASASA login interface. It features a dark teal header with the 'KASASA' logo. Below the header is a white login box with a light gray border. Inside the box, there are two input fields: 'Email' with an envelope icon and 'Password' with a lock icon. Below these fields are two links: 'Remember Me' with an unchecked checkbox and 'Forgot password?'. A large blue 'Sign In' button is positioned below the links. At the bottom of the login box, the text '©2016 Kasasa' is visible.

Navigate to <https://base.kasasaonline.com/> and enter your credentials.



Setup MFA Device

If your institution requires Multi-Factor-Authentication (MFA) and you have not registered a device, you will be prompted to enroll. If your institution is in the MFA enrollment period, the enrollment page will display upon login.

KASASA

Welcome to FIRSTBase: Multi-Factor Authentication

Your institution is adding multi-factor authentication (MFA) to all of its FIRSTBase accounts. Each time you sign into FIRSTBase, in addition to your password, you'll be asked for a verification code.

22 days left to configure MFA for your account

After June 20, 2017, any FIRSTBase accounts not configured for MFA will be locked and will require help from your institution's administrator to unlock and configure.

[I'll do this later.](#) [Set Up My Device](#)

If the MFA enrollment period has not passed you can click the **I'll do this later** link to continue with your FIRSTBase session or click **Set Up My Device** to enroll and setup your MFA device.

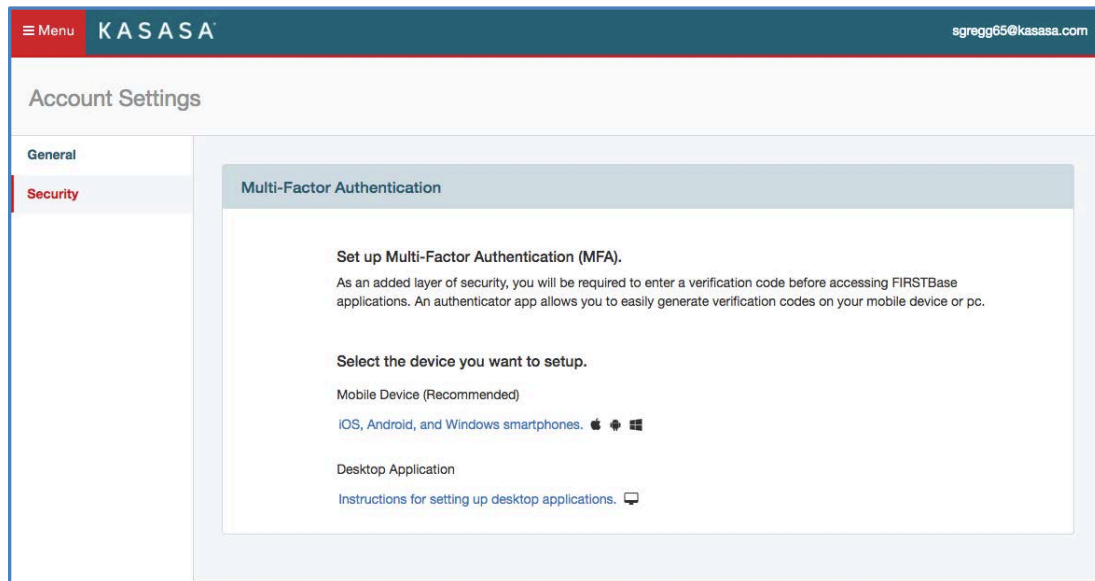
Note: Once you enroll and register an MFA device, you will be prompted for a verification code when you log into FIRSTBase. If you forget to enroll before the enrollment period expires, your FIRSTBase account will be locked and will need to contact your institution's FIRSTBase Administrator for assistance.

KASASA

Click **Set Up My Device**.

The *Multi-Factor Authentication Setup* page displays the device setup options.

Select the device you would like to use for MFA. *Note: Mobile is recommended.*



KASASA

For a Mobile Device:

1. Download an authentication app.
2. Scan the QR code presented on the page.
3. Enter the 6-digit code from your authenticator app.
4. Click **Verify**.

Menu KASASA sgregg55@kasasa.com

Account Settings

General

Security

Multi-Factor Authentication

1. Setup your iOS, Android or Windows smartphones.

- Get a mobile authenticator app for your smartphone:
 - iOS: Google Authenticator app from App Store.
 - Android: Google Authenticator app from Google Play.
 - Windows Phone: Microsoft Authenticator app from Windows Phone Store.
- In the app, select Set up account.

2. Choose Scan barcode, and scan this:

I can't scan the barcode?

3. Enter the 6-digit passcode you got from the authenticator app to activate.

Cancel Verify

If your mobile device can't scan the code, click the **I can't scan the barcode?** link and follow the instructions provided on the page.

Menu KASASA sgregg55@kasasa.com

Account Settings

General

Security

Multi-Factor Authentication

1. Setup your iOS, Android or Windows smartphones.

- Get a mobile authenticator app for your smartphone:
 - iOS: Google Authenticator app from App Store.
 - Android: Google Authenticator app from Google Play.
 - Windows Phone: Microsoft Authenticator app from Windows Phone Store.
- In the app, select Set up account.

2. Chose Manual Entry and enter the following information:

- Enter your FIRSTBase email address and this key (spaces don't matter):

jwnr ffu5 3amx 4lkk xnlj rb3x vltj cn62

Back to barcode.

3. Enter the 6-digit passcode you got from the authenticator app to activate.

Cancel Verify

Click **Verify**.



If the code entered is correct, the page will refresh and show your Authenticator App is Verified.

Multi-Factor Authentication

Your device has been successfully configured. When prompted, you'll verify your identity by entering a code from your authenticator app.

Authenticator App **Verified**

Note: Upon successful MFA device setup, the mobile app should list your FIRSTBase email address along with the provider tag of "Kasasa".

For a Desktop Application:

1. Have your IT department install an approved desktop authenticator app.
2. Follow the setup instructions provided on the page.
3. Enter the 6-digit code from your authenticator app.
4. Click **Verify**.

Menu KASASA sgregg65@kasasa.com

Account Settings

General

Security

Multi-Factor Authentication

Please contact your institution's IT department to install an approved desktop authenticator app. Once an authenticator is installed, follow the steps below.

1. Setup your Multi-Factor desktop client:

- Enter your name or issuer, for example, Kasasa.
- If a username is required, use your FIRSTBase login email address.
- Select a "time-based" option (if required).
- Type or copy/paste the secret key shown below to setup authentication.

celu dixh njab havv 56i5 yjji rty2 jp3x

2. Enter the 6-digit passcode you got from the authenticator app to activate.

Cancel Verify



If the code entered is correct, the page will refresh and show your Authenticator App is *Verified*.

Multi-Factor Authentication

Your device has been successfully configured. When prompted, you'll verify your identity by entering a code from your authenticator app.

Authenticator App	Verified
--------------------------	-----------------

Note: Upon successful MFA device setup, the mobile app should list your FIRSTBase email address along with the provider tag of "Kasasa".



Logging into FIRSTBase with MFA

Once you have a registered MFA device, to log into FIRSTBase you will be required to enter a verification code from your authentication app when prompted.

After correctly entering your credentials, you may be prompted to enter the verification code from your authentication app.

To obtain your verification code, open your app and use the six-digit code associated with your FIRSTBase account.

A screenshot of the KASASA mobile application's MFA verification screen. The screen has a dark teal header with the 'KASASA' logo in white. Below the header, the text 'Get verification code from your Authentication app.' is centered. Underneath this text is a light grey input field with the placeholder text 'Enter the 6-digit code' and a small mobile phone icon on the right. Below the input field is a solid blue button with the word 'Verify' in white text.

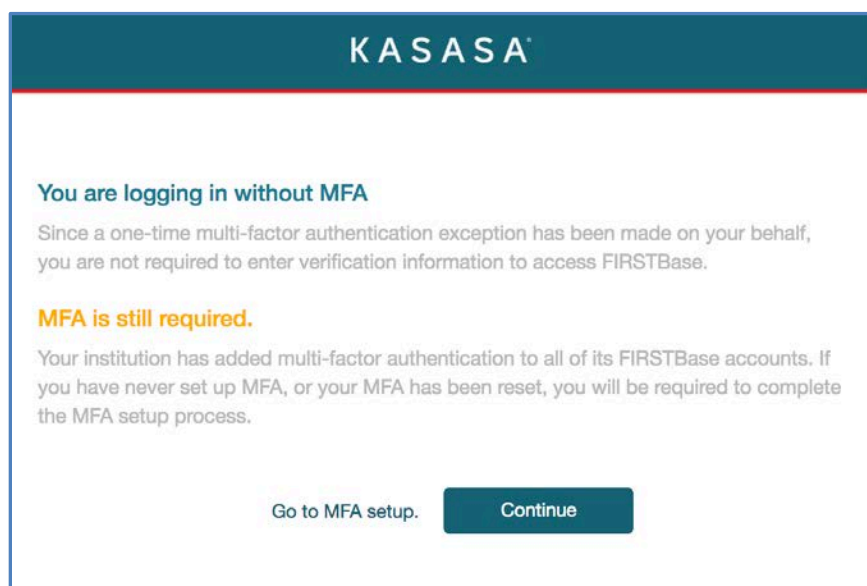


MFA Bypass

If you temporarily misplace your registered MFA device and need to log into FIRSTBase, contact your institution's Administrator and request a one-time MFA Bypass.

Once the administrator has granted the one-time MFA Bypass, after entering your credentials you will be presented with the MFA Bypass message.

Click **Continue**.



If you need to register a new device, click the **Go to MFA Setup** link.

Note: You will have 4 hours from the time the Bypass is granted to log in without being required to MFA.

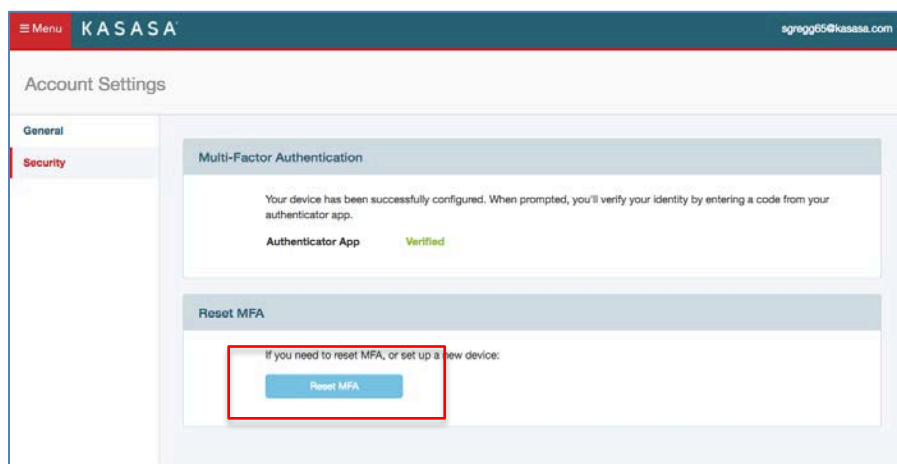


Reset MFA Device

If you get a new MFA device, you will need to delete the current device and setup the new one.

You can reset your MFA device from the Security tab in Account Settings.

Click **Reset MFA**.



The *Multi-Factor Authentication* setup page displays the device setup options (see page 4). Be sure to complete the setup process to avoid getting locked out.

As an alternative, you can have your institution's administrator perform a Reset MFA and Bypass MFA (see page 21) for you.

Note: iOS users may need to delete previous "Kasasa" accounts from Google Authenticator when resetting MFA to avoid duplicate accounts.



Update Account Settings

You can update your name, email address and password on the Account Settings, General page. *(Note: Always use a valid email address so that you can receive system notifications).*

To locate this page, click **Menu** in the top left corner of the page. At the bottom of the menu, click **Settings**.

A screenshot of the KASASA Account Settings page. The page has a dark teal header with a "Menu" button on the left, the "KASASA" logo in the center, and the email address "sally.test@fi.com" on the right. Below the header, the page title "Account Settings" is displayed. On the left side, there is a sidebar with two options: "General" (highlighted in red) and "Security". The main content area is divided into two columns. The left column is titled "Personal Information" and contains three input fields: "First Name" with the value "Sally", "Last Name" with the value "Tester", and "Email" with the value "sally.test@fi.com". The right column is titled "Change Password" and contains a list of password requirements, three input fields for "Current Password", "New Password", and "Confirm New Password", and a "Save" button at the bottom right.



Forgot Password

If you can't remember your password, you can click the **Forgot Password** link on the FIRSTBase login page.

A screenshot of the KASASA login interface. At the top is a dark teal header with the 'KASASA' logo in white. Below the header are two input fields: 'Email' with an envelope icon and 'Password' with a lock icon. Under the password field is a checkbox labeled 'Remember Me' and a blue link labeled 'Forgot password?' which is highlighted with a red rectangular box. At the bottom is a large blue button labeled 'Sign In'.

Enter the email address associated with your FIRSTBase account and click **Submit**. A temporary password will be emailed to you.

A screenshot of the 'Forgot Password' form. It has a dark teal header with a back arrow icon and the text 'Forgot Password'. The main content area has the text 'We'll send you a temporary password to your email address.' followed by an 'Email' input field with an envelope icon. At the bottom is a large blue button labeled 'Submit'.


Note: Temporary passwords are good for 24 hours.




If you enter your password incorrectly too many times your account will be locked. You can wait 24 hours or contact your institution's FIRSTBase administrator to unlock your account and reset your password.

KASASA[®]

You've been locked due to too many failed attempts. Please wait 24 hours or contact an Administrator.





☐ Remember Me [Forgot password?](#)

Sign In

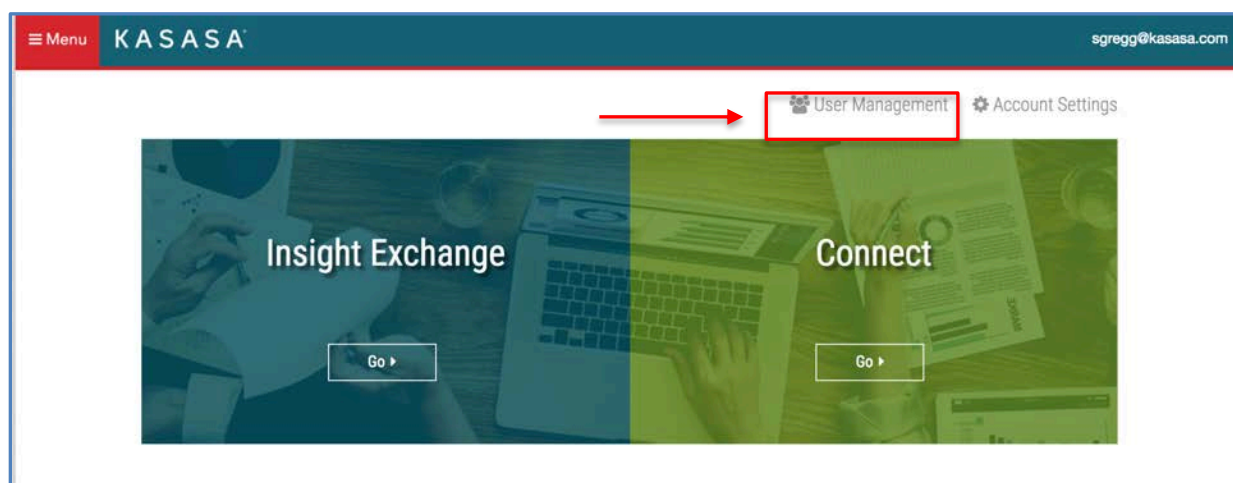


User Management

The User Management tool allows you to manage your institution's FIRSTBase users and perform common administrative functions. Pages 15 – 23 below only apply to FI Administrators.

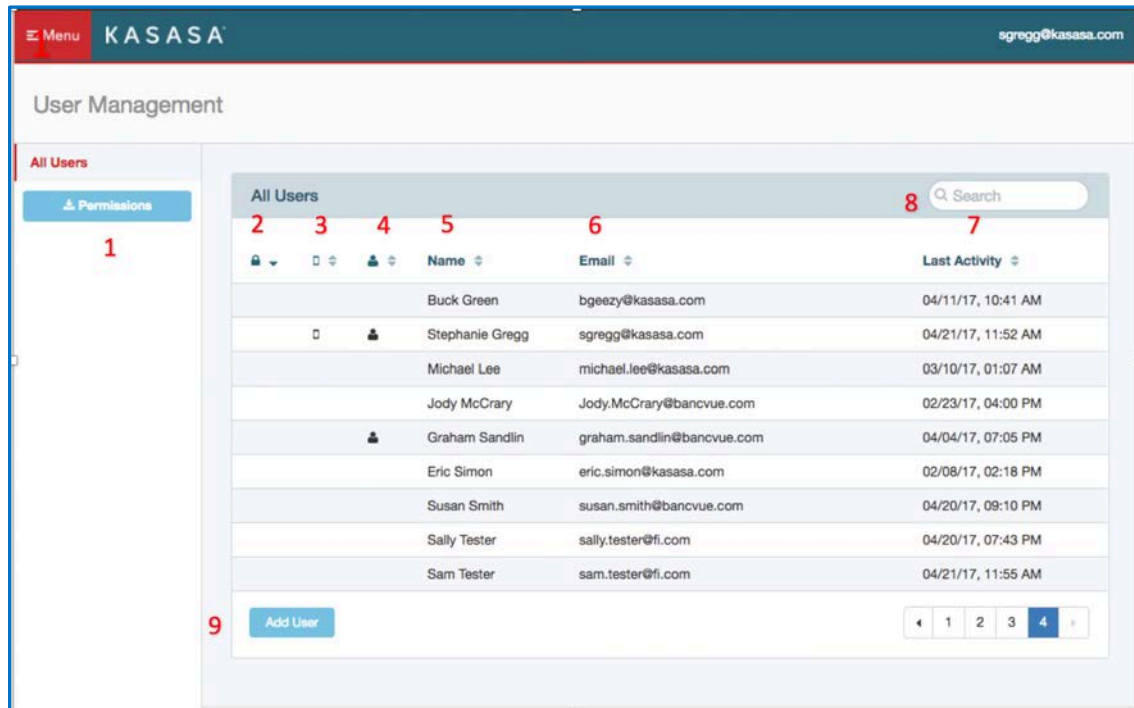
To access User Management, click on **User Management**.

Note: If you don't see User Management you will need the Users permission added by your FIRSTBase Administrator.



KASASA

The *User Management* page displays all FIRSTBase users for your institution

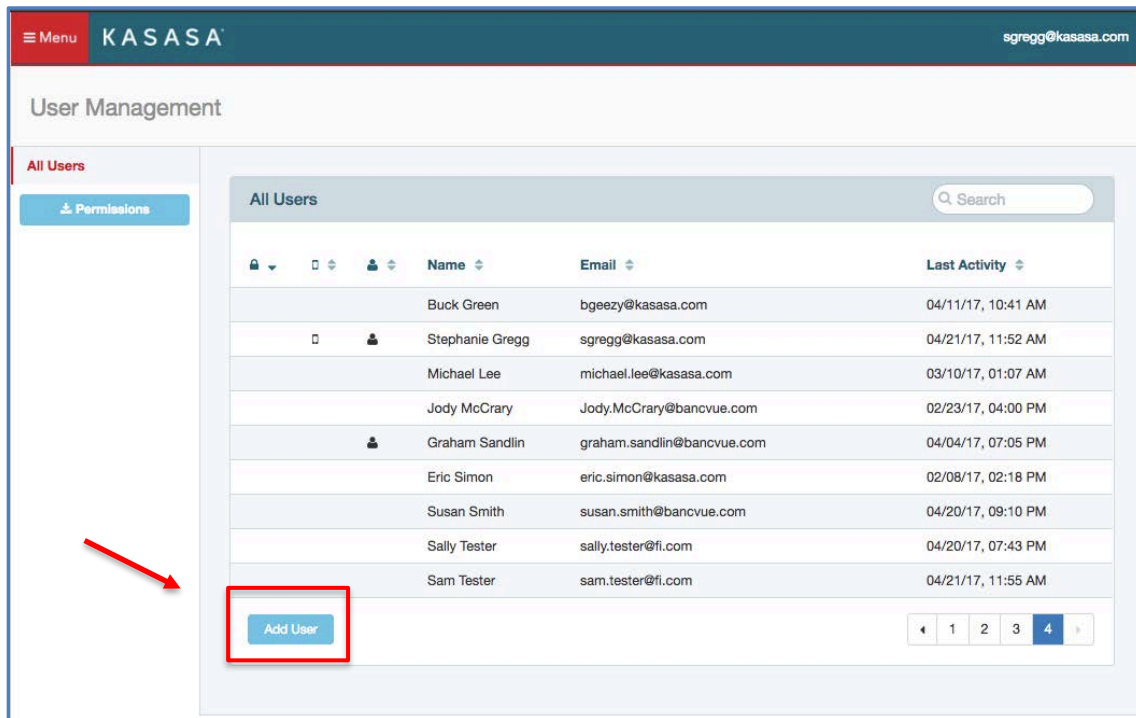


1. **Permissions** – Downloads a CSV that contains all users and their permissions.
2. **Lock** – A lock icon will display if the user's account has been locked.
3. **Phone Icon** – A phone icon will display if the user has registered an MFA device.
4. **Admin Icon** – If the admin icon displays next to the individual's name, they can add/edit user permissions.
5. **Name** – Shows the user's name. You can also sort by name.
6. **Email** – Shows the user's email address. This can be changed by the user after they login.
7. **Last Activity** – Shows the last time the user logged into the system.
8. **Search** – Quickly search for a user by name or email.
9. **Add User** – This button will only display for Administrators (those users with the icon from #4 above). From here a new user and permissions can be added to FIRSTBase.

KASASA

Add New FIRSTBase User

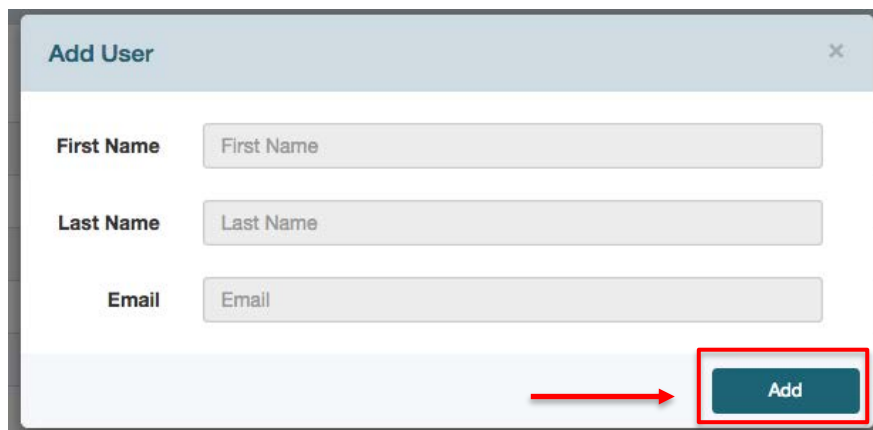
Click the **Add User** button at the bottom of the *User Management* page. (Note: You must have Admin User permissions to see the Add User button.)



The screenshot shows the KASASA User Management interface. On the left, there is a sidebar with 'All Users' and 'Permissions' options. The main area displays a table of users. At the bottom left of the table, there is a blue 'Add User' button, which is highlighted with a red box and a red arrow pointing to it.

Name	Email	Last Activity
Buck Green	bgeezy@kasasa.com	04/11/17, 10:41 AM
Stephanie Gregg	sgregg@kasasa.com	04/21/17, 11:52 AM
Michael Lee	michael.lee@kasasa.com	03/10/17, 01:07 AM
Jody McCrary	Jody.McCrary@bancvue.com	02/23/17, 04:00 PM
Graham Sandlin	graham.sandlin@bancvue.com	04/04/17, 07:05 PM
Eric Simon	eric.simon@kasasa.com	02/08/17, 02:18 PM
Susan Smith	susan.smith@bancvue.com	04/20/17, 09:10 PM
Sally Tester	sally.testers@fi.com	04/20/17, 07:43 PM
Sam Tester	sam.testers@fi.com	04/21/17, 11:55 AM

The *Add User* page is displayed.



The 'Add User' form is shown with three input fields: 'First Name', 'Last Name', and 'Email'. At the bottom right, there is a blue 'Add' button, which is highlighted with a red box and a red arrow pointing to it.

Enter the new user's first name, last name and email address. (Note: The email address needs to be valid in order for the user to receive system notifications).

Click the **Add** button. The page will refresh, ready for you to set the user's permissions.

KASASA

Setting User Permissions

User Management

Back

Profile

Audit Log

1 Sam Tester added. Now set the permissions below.
Their temporary password is: gome6943. The user will be required to change their password the first time they sign in.

FIRSTBase Account

Name Sam Tester

2 Permissions Template None

Email sam.teste@fi.com

Last Activity 04/21/17

Security

3 Reset Password Resets password, emails the user a temporary password.

4 Reset MFA Removes MFA, preventing login.

5 Bypass MFA Allows 1-time MFA bypass, prompts for MFA enrollment if unenrolled.

Best Practices

Forgot Device? Bypass MFA

New Device? Reset MFA and Bypass MFA

Lost Device? Reset MFA, Bypass MFA & Reset Password

Client Permissions

Permission Group	Can Modify	Can Approve
Archive		
Blurbs		

6

1. **Temporary Password** – Anytime a new user is added the system will generate a temporary password. This password should be provided to the new user. Either send the password to the new user manually or follow the directions for Unlocking/Resetting Passwords on the next page. The temporary password is only good for 24 hours.
2. **Permissions Template** – You can give someone a base set of permissions or you can add them individually below. See how to manage permissions on page 24 for more information.
3. **Reset Password** – This is usually used after a user is setup in the event the user gets locked out. This will unlock the user and send them a temporary password. Temporary passwords are good for 24 hours.
4. **Reset MFA** – Removes a user's MFA device, preventing them from logging in.
5. **Bypass MFA** – Grants a 1-time MFA bypass so that the user can log in without MFA.
6. **Permissions** – This is where you set what the user will have access to when the user logs into FIRSTBase. Be sure to click **Save** at the bottom of the page after setting permissions.
7. **Audit Log** – The audit log shows when permissions were added and by whom.

KASASA

After setting a user's permissions, be sure to click the **Save** button at the bottom of the page.

Connect Permissions

Permission Group	Can Modify	Can Approve
<input type="checkbox"/> Marketing Admin		
<input type="checkbox"/> Marketing User		

Delete

Save

Note: When a new user is added after the MFA enrollment period has passed, upon initial login, the user will be prompted to set up their MFA device. If the user clicks CONTINUE, logs out or allows their FIRSTBase session to time-out prior to setting up their MFA device their account will automatically be locked. Please instruct your new users to setup their MFA device upon initial login.



Unlocking Users/Resetting Passwords

Users can lock themselves out of FIRSTBase if they enter their password incorrectly too many times. Users can also become locked if they have not signed in for 90 days.

When you click on a user it will let you know the user is locked. You can unlock the user by clicking the **Reset Password** button. The system will send the user an email containing a temporary password.

The screenshot shows the 'User Management' interface. On the left is a sidebar with 'Back', 'Profile', and 'Audit Log'. The main content area is titled 'FIRSTBase Account' and shows user details for 'Sally Tester', including 'Permissions Template' (None), 'Email' (sally.test@fi.com), and 'Last Activity' (04/20/17). Below this is a 'Security' section with three buttons: 'Reset Password', 'Reset MFA', and 'Bypass MFA'. The 'Reset Password' button is highlighted with a red box and a red arrow points to it from the left. To the right of the buttons are descriptions: 'Resets password, emails the user a temporary password.', 'Removes MFA, preventing login.', and 'Allows 1-time MFA bypass, prompts for MFA enrollment if unenrolled.' At the bottom is a 'Best Practices' section with a table:

Forgot Device?	Bypass MFA
New Device?	Reset MFA and Bypass MFA
Lost Device?	Reset MFA, Bypass MFA & Reset Password

KASASA

Reset a User's MFA Device

There are times in which a user may need their MFA device reset.

- The user has lost their registered device.
- The user has a new device, needs to log in, reset MFA and register a new device.

After selecting the user, click the **Reset MFA** button.

The screenshot shows the KASASA User Management interface. On the left is a sidebar with 'Back', 'Profile', and 'Audit Log'. The main content area has a 'FIRSTBase Account' section with fields for Name (Sally Tester), Permissions Template (None), Email (sally.test@fi.com), and Last Activity (04/20/17). Below this is a 'Security' section containing three buttons: 'Reset Password', 'Reset MFA', and 'Bypass MFA'. A red box highlights the 'Reset MFA' button, with a red arrow pointing to it from the left. To the right of these buttons are descriptions: 'Resets password, emails the user a temporary password.', 'Removes MFA, preventing login.', and 'Allows 1-time MFA bypass, prompts for MFA enrollment if unenrolled.' Below the buttons is a 'Best Practices' section with a table:

Best Practices	
Forgot Device?	Bypass MFA
New Device?	Reset MFA and Bypass MFA
Lost Device?	Reset MFA, Bypass MFA & Reset Password

At the bottom of the interface, a yellow banner reads: 'MFA reset. The user's MFA has been reset. They will be required to register a new device.' Below this banner is the 'FIRSTBase Account' section again, showing the Name (Sally Tester).

Note: Resetting MFA locks the user out of their FIRSTBase account, preventing login. If the user needs to register a new MFA device, you will also need to grant an MFA Bypass.

KASASA

Grant MFA Bypass

There will be times in which a user may need to be granted a one-time MFA bypass to log in.

- A new user forgot to register their MFA device upon initial login.
- The user's device is temporarily unavailable.
- The user has a new device, needs to log in, reset MFA and register a new MFA device.

The screenshot shows the 'User Management' interface for a user named 'Sally Tester'. The interface is divided into two main sections: 'FIRSTBase Account' and 'Security'.

Account Information:

- Name: Sally Tester
- Permissions Template: None
- Email: sally.test@fi.com
- Last Activity: 04/20/17

Security Options:

- Reset Password:** Resets password, emails the user a temporary password.
- Reset MFA:** Removes MFA, preventing login.
- Bypass MFA:** Allows 1-time MFA bypass, prompts for MFA enrollment if unenrolled. (This option is highlighted with a red box and a red arrow points to it.)

Best Practices:

- Forgot Device? Bypass MFA
- New Device? Reset MFA and Bypass MFA
- Lost Device? Reset MFA, Bypass MFA & Reset Password

Success Message:

Bypass granted. The user will be allowed to successfully log in one time without MFA.

Account Information (repeated):

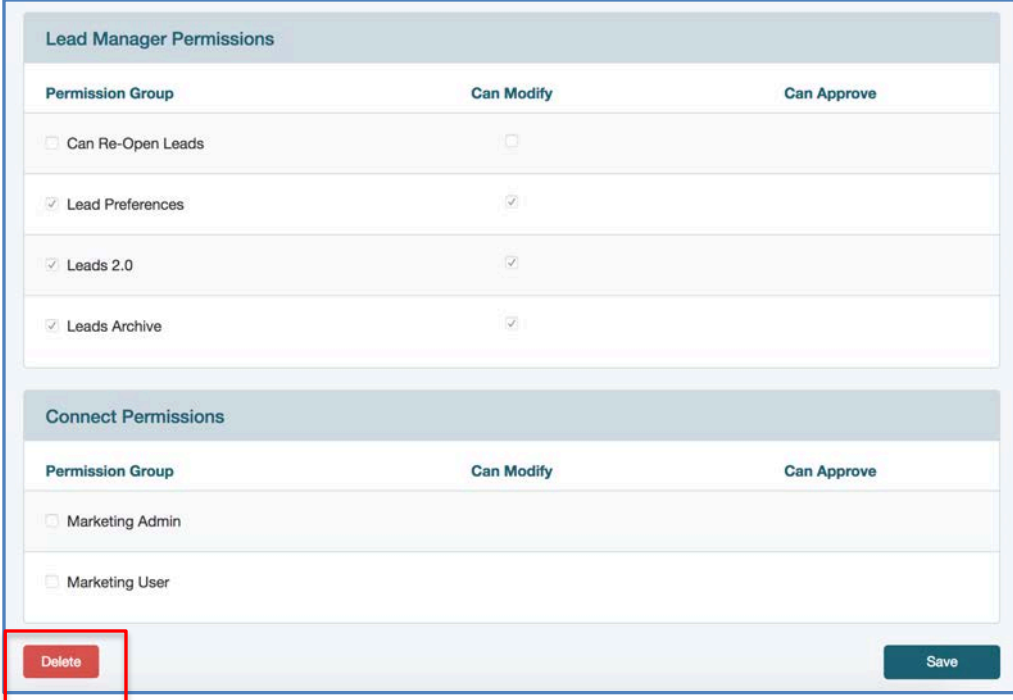
- Name: Sally Tester

Note: The user will have 4 hours from the time the Bypass is granted to log in without being required to MFA.

KASASA

Deleting A User

As part of your institutions employee exit process you should delete their FIRSTBase account. Select a user, scroll down to the bottom and click the **Delete** button to remove the user completely from FIRSTBase.



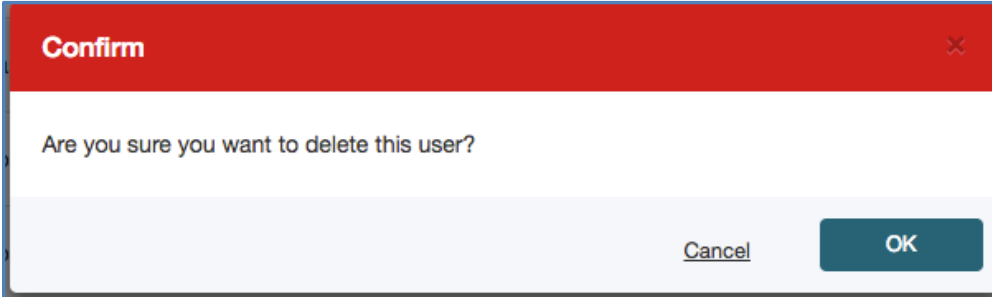
The screenshot shows a user management interface with two sections: 'Lead Manager Permissions' and 'Connect Permissions'. Each section contains a table with columns for 'Permission Group', 'Can Modify', and 'Can Approve'. Below these tables, a red 'Delete' button is highlighted with a red box and a red arrow pointing to it. A 'Save' button is also visible at the bottom right.

Permission Group	Can Modify	Can Approve
<input type="checkbox"/> Can Re-Open Leads	<input type="checkbox"/>	
<input checked="" type="checkbox"/> Lead Preferences	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> Leads 2.0	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> Leads Archive	<input checked="" type="checkbox"/>	

Permission Group	Can Modify	Can Approve
<input type="checkbox"/> Marketing Admin		
<input type="checkbox"/> Marketing User		

Delete **Save**

A *Confirm* pop-up message will display, requesting you confirm you would like to delete the user. Click **OK** to confirm.



The screenshot shows a 'Confirm' pop-up message with a red header bar. The text inside asks 'Are you sure you want to delete this user?'. At the bottom, there are two buttons: 'Cancel' and 'OK'.

Confirm

Are you sure you want to delete this user?

Cancel **OK**



FIRSTBase Permissions

This portion of the guide identifies the permissions available in the FIRSTBase. Included are the definitions of the individual permissions as well as recommended practices in setting each permission. This is an important process, as it will determine the ability of users to accomplish tasks and follow up on leads.

Overview of all possible Client Permissions:

This section includes general permissions such as KCMS, disclosures, certain reports and various administration permissions.

- Archive: view archived version of a FIRSTBranch
- Blurbs: Kasasa Internal Use Only
- Compliance Portal: access RegGen, the associated support material and other compliance information.
- Consumer Profile Manager: view and edit your users' Kasasa login profile information
- Consumers: view the Consumers tool in FIRSTBase
 - Can Modify – ability to add/modify consumers
- Documents: view disclosures
 - Can Modify – ability to upload and edit disclosures
- Funding Admin: there are 2 distinct functions this permission allows.
 - New Accounts - access Funding Admin to download INMO ACH files and/or view debit card settled funding transactions. *Note: Users with this permission will receive email notifications when a new ACH file ready to be processed and/or when debit card transactions have settled and the summary report of these transactions is available for download.*
 - Add-Ons - access Funding Admin to download Builder ACH files on the 3rd of each month. *Note: Users with this permission will receive email notifications when a new ACH file is ready to be processed and can view a summary report of those transactions.*
 - Loans - access the Funding Admin module to download Kasasa Loans ACH files for processing.
 - Can Modify – To access the Funding Admin portal, the user must have both levels of permissions. The left checkbox alone will not allow the user to access the Funding Admin section. If someone attempts to access Funding Admin without the Can Modify it will display a "Not Authorized" message.
- Insight: ability to view monthly Kasasa consulting reports
- Insight Exchange: ability to view monthly Kasasa consulting reports
- Kasasa: Kasasa Internal Use Only
- Kasasa Loans: access the basic components of the Kasasa Loans Admin System
 - Can Modify: able to record transactions and download system outputs such as transaction details, statements, and reports.
- Kasasa Loans – Collections: able to access collections tab within Kasasa Loans Admin System to view delinquent borrowers

KASASA

- Kasasa Loans – Disable Take-Backs: able to disable the “take-back” feature for an individual borrower or loan
- Kasasa Loans – Edit Profile: able to view and edit borrower profile details for an individual loan
- Kasasa Loans – Generate: able to access the Loan Import tab in the Kasasa Loans Admin System to import new loan applications or correct errors in existing loan applications
- Kasasa Loans – Loan Maintenance: view Loan Maintenance tab within the Kasasa Loans Admin system to see individual loan settings such as pausing credit bureau reporting or managing automatic payments.
 - Can Modify: able to update settings for an individual loan
- Kasasa Loans – Notes: Able to view collections notes for a delinquent loan
 - Can Modify: able to modify existing notes or submit new notes
- KCMS: update and modify information displayed on the FIRSTBranch website
- KCMS - 301 Redirect: access 301 Redirects set up for a FIRSTBranch website
 - Can Modify – ability to add/modify/delete 301 Redirects set up for a FIRSTBranch website
- Locations: view Locations set up for a FIRSTBranch website
 - Can Modify – ability to add/modify/delete locations set up for a FIRSTBranch website
- Navigation: Kasasa Internal Use Only
- Plugins: Kasasa Internal Use Only
- Product Images: Kasasa Internal Use Only
- Products: Kasasa Internal Use Only
- Security Client: For an FI Administrator to Reset MFA and Bypass MFA
- Site Alert: ability to view alerts set up on FIRSTBranch site
 - Can Modify – ability to add/modify/delete alerts set up on a FIRSTBranch website.
- Tables: Kasasa Internal Use Only
- Users: access User Management
 - Can Modify – ability to add/modify/delete users and set permissions
- Users – Reset Password: ability to reset FIRSTBase user passwords
- Web Content – ability to access to Classic CMS (flash tool)

Overview of all possible Lead Manager Permissions:

This section will be used to manage permissions for those users who will be processing leads for INMO, FIRSTBranch, Builder, Kasasa Protect and Marketing Campaigns.

- Can Re-Open Leads: ability to open an already closed lead and change the decision on that lead. This can only be done within the same day the lead was initially closed and before 11:59 PM Central time of that same day.
 - Can Modify - Both permission levels are required to re-open a closed lead.
- Lead Preferences: In the Preferences section of Leads Manager, allows the ability to view how the leads will be processed. This includes: (1) Time Zone settings for audit log tracking, (2) Response Time for leads to be moved into the Action Required folder or



KASASA

unassigned (3) the FI default setting of when email Notifications will be sent to users, (4) Status Reasons, (5) individual User notifications, and (6) Rules for incoming leads.

- Can Modify – allows the ability to make changes to all settings in this section.
 - Note: All users will have the ability to access the Preferences section to edit their own individual user preferences such as: (1) instant notification emails to override FI default setting, (2) lead summary notification emails to override FI default setting, and (3) out of office schedule. The Can Modify permission allows the person to amend everyone's individual user preferences.
- Leads 2.0: view the Leads Manager application in FIRSTBase
 - Can Modify – allows the ability to access and save changes on a lead
- Leads Archive: Kasasa Internal Use Only

For information on how to manage leads see the Leads Manager Training Guide or view eLearning training materials found at this link: <https://freedom-training.kcmspreview.com/setup-and-training/cms-leads-training.html>



KASASA

Overview of all possible Connect Permissions:

This section will be used to manage permissions for those users who will need access to Connect for marketing materials.

- Marketing Admin: Kasasa Internal Use Only
- Marketing User: ability to access Connect for Kasasa marketing materials

RECOMMENDED PERMISSION SETS:

These are the product-based recommendations for the sets of permissions that might be applicable to a certain type of user.

1. Kasasa Marketing User:

- Compliance Portal – access RegGen, the associated support material and other compliance information.
- Insight Exchange – ability to view monthly Kasasa consulting reports
- Marketing User – ability to access Connect for Kasasa marketing materials

2. FIRSTBranch User:

- KCMS – This gives full access to modify information displayed on the FIRSTBranch website that was built using Kasasa CMS.
- KCMS- 301 Redirect - access 301 Redirects set up for a FIRSTBranch website
 - Can Modify – ability to add/modify/delete 301 Redirects set up for a FIRSTBranch website
- Locations: view Locations set up for a FIRSTBranch website
 - Can Modify – ability to add/modify/delete locations set up for a FIRSTBranch website

3. INMO User:

- Documents – view disclosures
 - Can Modify – ability to upload and edit disclosures
- Funding Admin – access the Funding Admin to download INMO ACH files and/or view debit card settled funding transactions. The person with this permission will receive email notifications when there is a new ACH file ready to be processed and/or when debit card transactions have settled and they can download a summary report of those transactions.

4. Builder User:

- Consumers – view the Consumers section in FIRSTBase
 - Can Modify – ability to add/modify consumers
- Funding Admin – access Funding Admin to download Builder ACH files on the 3rd of each month. The person with this permission will receive email notifications when there is a new ACH file ready to be processed and can view a summary report of those transactions.

KASASA

5. Leads Manager (for INMO, FIRSTBranch, Builder) User:

- Can Re-Open Leads – ability to open an already closed lead and change the decision on that lead. This can only be done within the same day the lead was initially closed and before 11:59 PM Central time of that same day.
- Lead Preferences – in the Preferences section of Leads Manager, allows the ability to view how the leads will be processed. This includes: (1) time zone setting for audit log tracking, response time for leads to be moved into the Action Required folder or unassigned, (3) the default setting of when email notifications will be sent to users, (3) status bar categories, individual user notifications, and (5) rules for incoming leads.
 - Can Modify – allows the ability to make changes to all settings in this section
 - Note: All users will have the ability to access the Preferences section to edit their own individual user preferences such as: (1) instant notification emails to override default setting, (2) lead summary notification emails to override default setting, and (3) out of office schedule. The Can Modify permission allows the person to amend everyone's individual user preferences.
- Leads 2.0 – view the Leads Manager console section in FIRSTBase
 - Can Modify – allows the ability to access and save changes on a lead

6. Administrative User:

- Users – provides access to the User Management section in FIRSTBase to add new users, modify user permissions and delete users
- Users – Reset Password – ability to reset other users' passwords
- Security Client – allows one to Reset MFA and Bypass MFA

THE FOLLOWING PERMISSIONS ARE FOR KASASA INTERNAL USE ONLY

- | | |
|------------------|-------------------|
| • Blurbs | • Products |
| • Navigation | • Tables |
| • Plugins | • Leads Archive |
| • Product Images | • Marketing Admin |