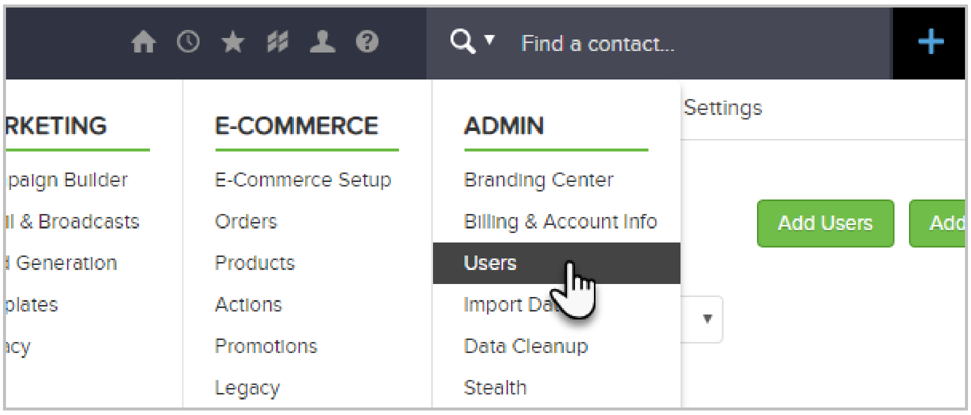
User Permissions - Application

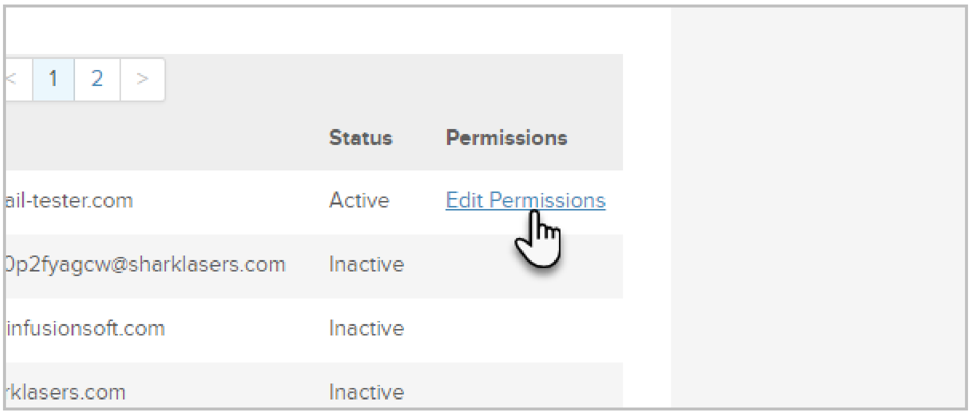
This article applies to:

These user profile permissions are used in the administration of Keap to control the ability to access various account level functions.

1. As an admin, go to **Admin** > **Users** in the main menu.



2. Click **Edit Permission** next to the user that you want to modify.



	Status	Permissions
ail-tester.com	Active	Edit Permissions
0p2fyagcw@sharklasers.com	Inactive	
infusionsoft.com	Inactive	
rklasers.com	Inactive	

Application

These permissions control the ability to access various "account level" functions that are not associated with one particular component of Keap.

- **Can add tag**: This permission controls the ability to create and use tags throughout the application. If it is set to No, the user will not able to create new tags in the system. They also cannot see the Tag tab or the Edit Tags button when viewing a contact record. They will not be able to apply tags to contacts and can only remove tags from a contact record using the Tags option in the interactive panel. They will be able to use the tag objects in the campaign builder and set up actions to apply / remove tags, if their marketing permissions allow access to these features.
- **Can see app account management page**: This permission controls the ability to access the Keap account page in the Admin area of the main navigation menu. This page provides summary account usage information and allows you to upgrade your account, manage billing, and purchase plug-ins or services. If it is set to *No*, the user will not see the Keap *Account* option in the main menu.
- **Can go to billing info management page**: This permission controls the ability to view the billing summary on the Keap *Account* page. If it is set to *No*, the user will be able to access the account page to upgrade and purchase add-on products or services; however, they will not see the next bill date or be able to log into the customer center to update the credit card on file.
- **Can import records**: This permission controls a user's ability to upload a spreadsheet of records into Keap (e.g., contacts, products, tags, etc...) If it is set to *No*, the user will not see the *Import Contacts* option in the *Contacts* menu and will receive an *access denied* message if they try an update import (Modify Existing Records) through **Admin > Data Cleanup**.
- **Can dup check and merge records**: This permission controls a user's ability to run the automated duplicate checking process and merge the duplicate contact records. If it is set to *No* the user will not see the *Data Cleanup* option in the main navigation menu.
- **Can rollback imports**: This permission controls a user's ability to delete (rollback) an entire import. If it is set to *No* the user can view previous imports (if *can import* is set to *Yes*), but cannot see the link required to rollback the import.
- **Can view company files**: This permission controls the ability to access the application file box from the user toolbar. They will receive an *access denied* message if they select the *Files* option from the *Home* icon on the toolbar. The user is still able to add files to contact file boxes.
- **Can delete company files**: This permission controls the ability to delete files from the application file box. If it is set to No, the user can view the company files but cannot delete them.
- **Can export lists**: This permission controls the ability to export any kind of data (e.g., contacts, orders, etc...) from your system. If it is set to No, the user will not see the Export option on any of the Action menus throughout the system.
- **Can edit Misc. Settings**: This permission controls access to various settings throughout the system. If it is set to No, then the user will not see the link to the marketing, e-commerce, or admin settings from the master nav. They will have limited access to CRM settings (like tags and scores). This permission will also limit the ability to access settings through the E-Commerce setup page.
- **Can see other users**: This permission controls the ability to view the list of users throughout the system. If it is set to *No*, the user will not see the *Owner* field on a contact or opportunity record. It also limits the ability to see the user list when performing a search. They cannot assign tasks, appointments, or notes to other users or view other's calendars.
- **Can delete app data in bulk**: This permission restricts a user's ability to batch-delete various records throughout the system. If it is set to *No*, the user will not see the *Delete* option in the *Actions* drop down menus.

- **Can change field data in bulk**: This permission controls a user's ability to mass update various records throughout the system. If it is set to *No*, the user will not see the *mass update* options in the *Actions* drop down menus throughout the system (e.g., mass update contacts, opportunities, referral partners, etc.)
- **Can add items to the top nav**: This permission controls a user's ability to add custom menu items to the area dropdown navigation (e.g., add a custom search to the Contacts menu within the CRM area). If it is set to *No*, the user will not see the *Main Nav* menu option under **Admin > Settings**.
- **Can reveal credit card data**: This permission is no longer valid.
- **Can Manage Scores**: This permission controls the ability to set up scoring criteria. If it is set to *No*, the user is not able to see the *Scores* menu option under **CRM > Settings**.

Action

These permissions control the ability to set up, use, or manage action sets.

- **Can apply actions**: This controls the ability to run actions on a list of contacts or an individual contact or opportunity record. If it is set to *No*, the user will not see the *Apply Action Set* option in the *Actions* drop down menus throughout the system or the *Apply Actions* option on the contact actions list. They also will not see the *Actions* drop-downs when setting up web forms, order forms, etc...
- **Can see all action sets**: This permission controls the ability to view the list of all existing action sets. If it is set to *No*, the user will receive an *access denied* message when trying to access *Action Sets* through **CRM > Settings or Marketing > Settings**.
- **Can share action sets**: This permission controls the ability to share a new action set created through the *Action Set* settings screen with other users. If it is set to *No*, the user will not see the *Visible To* tab when creating a new action set through **CRM > Settings** or **Marketing > Settings**. Action sets are visible to all users by default. The visibility filter allows users to hide action sets for users so they will not see them when applying actions, copying actions, or running another action set.
- **Can change priority of scheduled actions**: This permission controls the ability to rearrange actions through the *Scheduled Actions* admin report. If it is set to *No*, the user will not be able to re-prioritize the actions.

Reports

These permissions control access to reports by system area. If any of these permissions are set to *Yes*, the related report menu options are visible in the main navigation menu. If it is set to *No*, the user will not see the menu option to the related reports:

- Can view Marketing Reports
- Can view Sales Reports
- Can view Order Reports
- Can view Affiliate Reports
- Can view Administrative Reports

Fulfillment

Can see all fulfillment jobs: This permission only applies to the legacy *Day* or *Agenda* home page views. It does not apply to the customizable User Dashboard.

- If this permission is set to *Yes* the user is able to see the queued fulfillment and order fulfillment jobs assigned to all users.
- If it is set to *No*, the user will only see their own jobs.

Mobile

Can access mobile application: This permission controls access through the mobile application.

- If set to Yes, the user will be able to connect through the mobile application and have full access to the Mobile app. The other permissions set here (Desktop Application) do not carry over into the mobile app.
- If set to No, the user will not be able to access any data through the mobile application.