User Setup

Overview

As an administrator, you have the ability to create new user accounts for use within your branch. If your company has sub-branches, you may also administer the users in those branches.

User List

You can access the User Setup page from the desktop by clicking on "User Setup" under the "Tools" section.

User Setup

Add Show USER ACCOUNTS Show locked user accounts Generate Auth Code

Name	Login	Email	Locked	Admin	See Credit	Bill Separately	Report Ordering	Supplement Ordering	Department	Teams	Restrictions	Last Login
DOC ADMIN	docadmin	test@test.com	NO	YES	YES	NO	ALL	ALL				8/25/2016 1:18:43 PM
DOCUMENTATION	Doc	test@test.com	NO	NO	YES	NO	ALL	ALL				8/24/2016 4:54:32 PM

Add a User

Click the "Add" button to add a new user. If you need to edit an existing user, click their hyperlinked Name under the user accounts table. The screen for adding new users will look very much like the one for editing an existing user.

User Accounts Table

Field	Description

Field	**Description**
Name	This is the full name of the user. Clicking this value will bring you to the User Edit Page.
Login	This is the user's login name. This is used to access the system.
Email	The user's email address associated with their account.
Locked	Either a NO or a red YES will populate this column. If a user's account is locked, an administrator will have to unlock it for them.
Admin	Administrators have elevated access to configure company and user settings. A NO or a YES will appear here.
See Credit	A NO or a YES will appear here. If a YES is displayed, then this user is allowed to see credit files belonging to other users.
Bill Separately	A NO or a YES will appear here. If a YES is displayed, the user is configured to have their own invoices generated, as opposed to having their transactions included on the company invoice.
Report Ordering	Indicates the user's report ordering access. NONE - User does not have access to order any reports. SELF - User has access to order reports only for themselves. ALL - User has access to order reports on behalf of other users.
Supplement Ordering	Indicates the user's supplement ordering access. NONE - User does not have access to order any supplements. SELF - User has access to order supplements only for themselves. ALL - User has access to order supplements on behalf of other users.
Department	This column is filled with whatever text is entered in the User's Edit screen. Examples: SALES or MANAGEMENT
Teams	Lists any teams the user is assigned to. Teams allow administrators to group users with regards to file accessibility.
Restrictions	Any restrictions that the user may possess is displayed here. The list of restrictions can be found under the "Restrictions" tab of the user's edit screen.
Last Login	This will show the timestamp of the user's last successful login.

Generate Auth Code

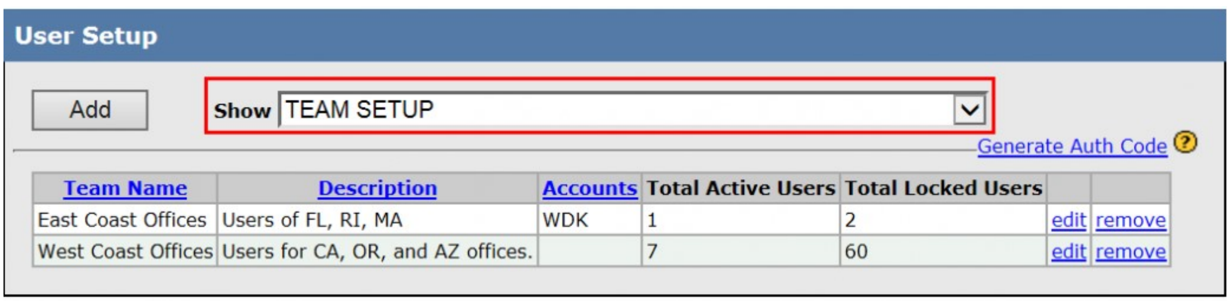
Occasionally, users will be prompted for an authentication code upon logging into the website. This link can be clicked to generate such a code.

- When the code is generated using this method, it will immediately appear in a pop-up window. The code will be vaild for 2 hours.
- Authentication codes can normally be requested by the user and sent via email or text message. Manually generating an authentication code for a user is only done under a handful of circumstances (e.g. client does not have access to their cell phone or email at the moment).

Teams

The system allows for the configuration of complex file access permissions via a concept referred to as "teams". It's the middle point between giving a user access to view files belonging to all other company users and giving a user access to none of them. "Teams" allows for a setup where users are able to view files belonging to other users, but only those users who are part of the same team.

To see your company's team setup, set the "Show" dropdown to "TEAM SETUP", as highlighted below.



Team Name	Description	Accounts	Total Active Users	Total Locked Users		
East Coast Offices	Users of FL, RI, MA	WDK	1	2	edit	remove
West Coast Offices	Users for CA, OR, and AZ offices.		7	60	edit	remove

Adding / Editing a Team

To add a team, click the "Add" button. To edit an existing team, click the team's corresponding "edit" link. Note that you might not have access to add or remove teams, depending on your permissions. Below, we will briefly explain the team configuration page that will appear when adding or editing a team.

Field	Description
Name	The team's name. This is what will appear throughout the system when a team name is displayed.
Branch	Admins on the Master Account will have a "Branch" option. This allows Admins access to add teams to Sub-accounts.
Description	A brief description of the team. This is optional.
User Name	This column will show the names of all users under the customer account. If the team being added/edited belongs to a master account, then sub-accounts will also appear in the list, as shown in the above screenshot. Checking the box next to the name of the company will automatically include all existing and future users under that account to be included in the team.
Existing Team Membership	If the user is part of any teams, it will be shown here.

Once the team settings are complete, click "Save" to save your changes.

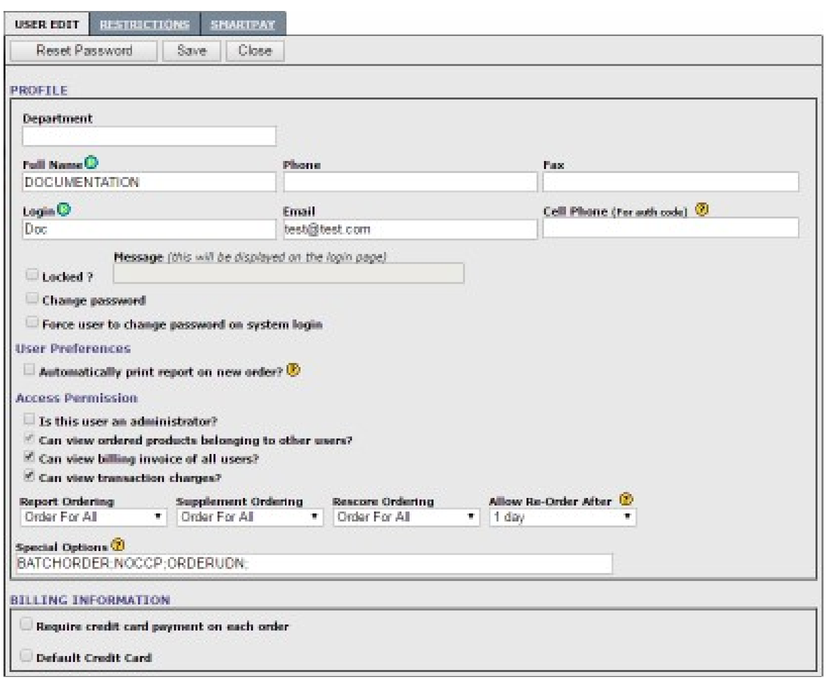
Team Rules to Remember

- Administrators are exempt from team restrictions. They can view files belonging to all users in the customer account (and in any sub-accounts, if applicable), regardless of their team assignments.
- By default, users belonging to a master account who can "view products belonging to other users" can also view products belonging to sub-account users.
- Any users who are part of mutual teams can see files belonging to each other. Users can be

part of multiple teams to support complex file-access configurations.
- You can add a specific user or an entire sub-account to a team. Including an entire sub-account account will automatically include users created later on.
- Users in a sub-account cannot view files belonging to users in other sub-accounts, regardless of team configurations. A rule of thumb is that "teams" does not allow users more access to files than they normally would have--"teams" is a feature that restricts access. Sub-account users normally do not have access to view files belonging to other sub-accounts so it isn't possible to configure teams in such a way that would remove this restriction.

User Edit Tab

- The system requires each account to have a login name, a full name, and a password.
- The login name must be unique to the system.
    - If the login name you want to use already exists in the system try adding a number at the end.
- An e-mail address is recommended to receive notification of when supplement requests are completed and for password resets.
- If the *Department* field is filled out, it can be used in the Activity Summary to group the total balances by Departments.
- A phone and fax number is recommended so the Credit Reporting Agency can contact the user if they have questions on the user's supplement request.
- The Cell Phone can be used by the user to generate an auth code in case they are logging in from a new location.



Profile

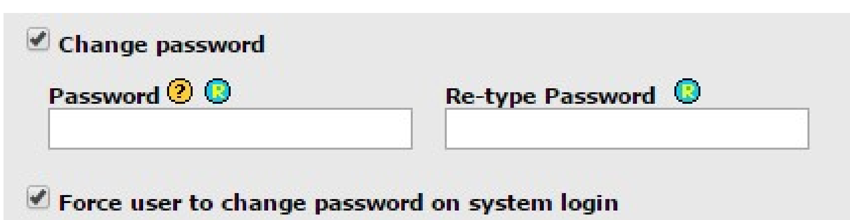
- **Department:** If the *Department* field is filled out, it can be used in the Activity Summary to group the total balances by Departments.

- **Full Name:** The first and last name of the user.
- **Phone & Fax:** A phone and fax number is recommended so the Credit Reporting Agency can contact the user if they have questions on the user's supplement request.
- **Login:** The login name must be unique to the system. If the login name you want to use already exists in the system try adding a number at the end.
- **Email:** An e-mail address is recommended to receive notification of when supplement requests are completed and for password resets. An auth-code can also be received by e-mail when no cell phone number is registered.
- **Cell Phone:** The Cell Phone can be used by the user to receive an auth code in case they are logging in from a new location.
- **Pointservices User ID:** (Not pictured) You will find this field on each user within a customer who is enabled for the Pointservices Interface.
    - The Pointservices User ID is a value from PitchPoint that determines what products a user can order and view when they use the Pointservices interface.
    - There is also a Default User ID that can be configured in the customer setup. If no Pointservices User ID is configured in the user setup, the Default User ID is used when the user accesses the Pointservices interface.

Locked?

- To lock or unlock an account, select or deselect the *Locked?* checkbox.
- A user cannot log into MCL with a locked account.
- When you lock an account, it is a good idea to include a brief description to explain why you did so in the *Message* field.
- The message will appear on the login screen when the user tries to log into MCL with the locked account.
- If a user tries to log in with the wrong password five consecutive times, their account will lock automatically.
    - The reason given will be *Too many logon attempts*. An administrator must unlock the account before the user can log in again

Change Password



Checking the *Change password* this will allow a new password to be setup manually. You will have to enter the password twice as confirmation.

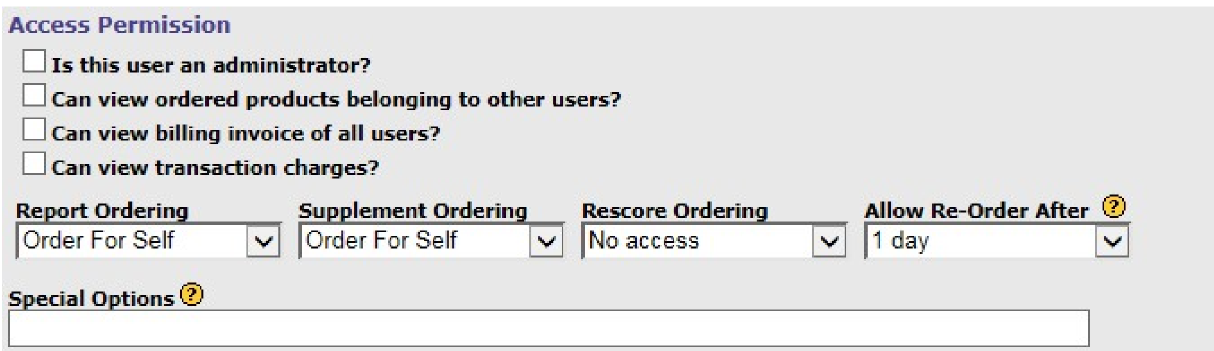
- **Force user to change password on system login:** When creating a password for a user it is recommended that the option *Force user to change password* is checked so when the user logs in they will be prompted to change their password. This will enforce that only the user knows their password.

- **Password Requirements:** Passwords must be at least eight characters long and must contain at least one digit (0-9) and one alphabetical character (A-Z). Passwords may not include commonly used phrases or passwords that have been breached in publicly available databases. Users may change their own passwords by using the *My Account* feature in the *Others* section of the desktop; administrative access is not required to change a password this way.

User Preferences

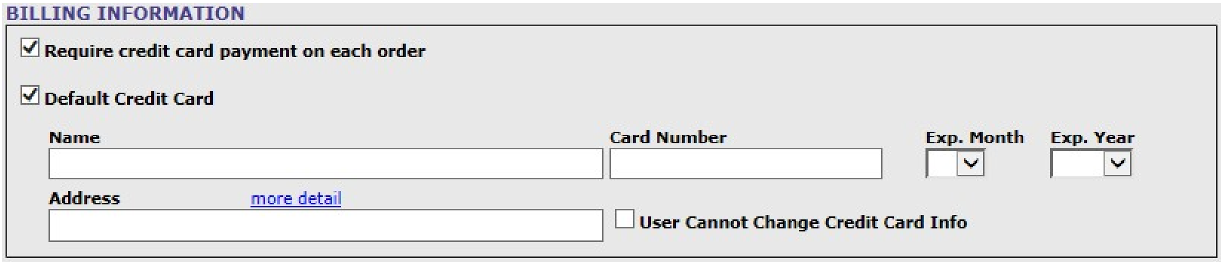
- **Automatically print report on new order?:** The only user preference at this time is the *automatic print* option. You may choose to select or deselect this option for a user, but the user does have control of this option from the *My Account* screen.

Access Permissions



- **Access Permission:** These options set viewing privileges for this account. These options determine whether or not a user is an administrator, whether the user can view other users' credit files, whether a user can see billing invoices, and whether the user can view the Activity Summary. If you elect to make this user an administrator, all of these other options will be overridden (grayed out) and forced to be true.
- **Ordering Options:** These options control whether a user can order reports and supplements for herself/himself or everyone. The values can be:
  - **Order for Self:** Allows a user to order reports, supplements, or rescore requests on their own behalf.
  - **Order for all:** Allows a user to order reports, supplements, or rescore requests on another user's behalf. A loan processor is usually give *Order for all* permission on these fields.
  - **No Access:** Prevents a user from ordering a new report, supplement, or score request.
- **Allow Re-Order After:** Specifies how many days the user must wait before he/she can re-order a new report using the same borrower information. It is recommended to put 30 days. If a user is an administrator, your selections for these options will be overridden and locked.
- **Special Options:** In the *Special Options* field you specify keywords to activate special user options offered by MCL. Each keyword entered manually must end with a semicolon.

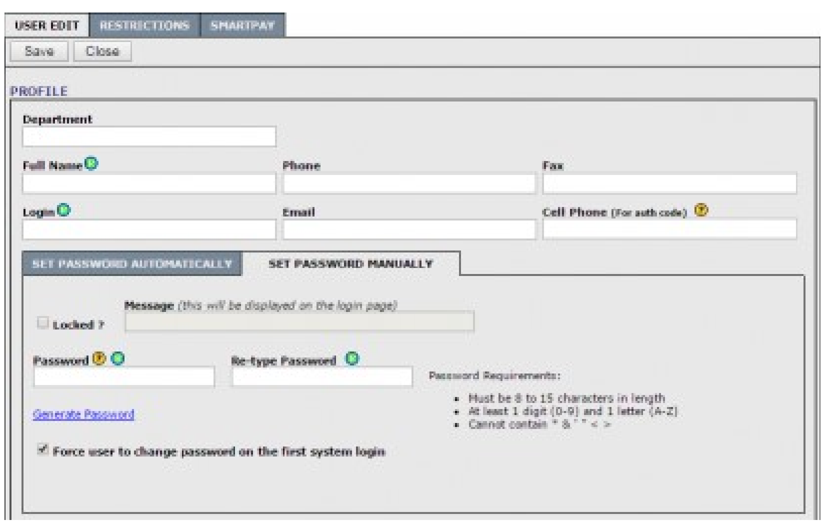
Billing Information



- **Require credit card payment before ordering?:** Option requires users to pay for report orders using a credit card before they can order the reports. You will then need to choose whether they need to pay all related additional charges before viewing a report.
- **Default Credit Card:** The stored credit card information will automatically populate into the credit card payment screen when a user pays for the report. Press *Save* at the top to save the data and exit, deselect and save to clear the fields, and *Cancel* to exit without saving. The credit card number will not be visible to the user; they will see only the last four digits of the card number.

User Edit when Adding a User

When creating a user for the first time you must enter in a name, login and generate a password. We have two options to generate passwords. You can input an email address and an email will be sent to the client asking them to login and set a password. You can also manually generate a password.



Set Password Automatically

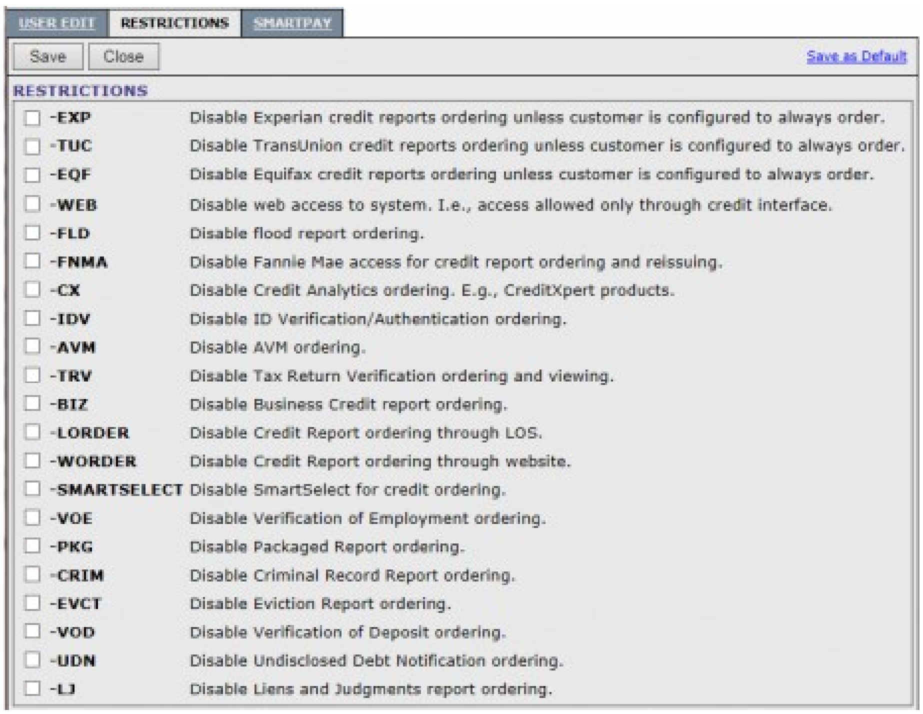
If you choose not to generate a password manually you will need to include an email address. Once you save the account information two separate emails will be sent to the client. The first email will include the client's new login. The second email will contain a link to generate their password.

If the client has access to view other user's credit files then they will also need to use an auth code to enter the system. This auth code cannot be generated via email and must be given to them directly or can be sent to the cell phone if it has been included.

Set Password Manually

By clicking the Set Password Manually tab you will see the location to enter in a password. There will also be a link to generate a random password that will auto fill. We recommend you force the user to change their password on the first system login.

Restrictions Tab



- These options allow you to prevent a user from ordering credit reports from individual credit repository, from ordering other products or to deny a user access to MCL's Web interface.
- A user without Web access is restricted to your custom CreditAPI interface, and cannot use the standard MCL interface.
- **Check the box next to the options that you want to restrict.**
- **Press *Save* to save and close the dialog; press *Close* to close it without saving.**
- Contact your Credit Reporting Agency if you have questions about other options.

Save as Default

This link is located on the top right of the User's Restriction tab. Clicking on it will save the current restrictions as a template. When new users are created, they will default to the options you saved. The following are the options that can be defaulted:

- Everything under the *Access Permission* section under the *User Edit* tab.

- Special Options
- The restrictions under the *Restrictions* tab.
- The *Credit Limit* under the *Restrictions* tab.
- The *Team Settings* under the *Restrictions* tab.

The *IP Restrictions*, *Billing Information*, and *Credit Order Limit* currently are not defaulted via the Save as Default feature.

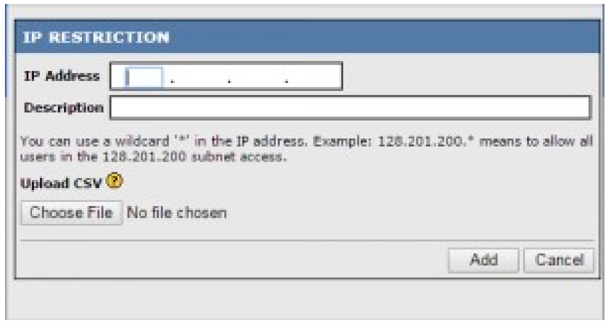
Please note that the *-TRV* option will always be checked when creating a new user regardless of whether you saved a default with -TRV unchecked.

IP Restrictions

- As an added security precaution, MCL now allows administrators to restrict access by IP address.
- An IP address is like a street address, but for your computer.
- With this feature, you can restrict access to a particular network, or even to a specific computer.
- This type of IP address filtering is most effective if you have a network with a predetermined range of IP addresses.
- To determine your IP address, speak with your IT personnel.
  - Alternatively, you can go to a third party website, such as http://www.ip-adress.com or http://www.whatismyip.com, to easily identify your IP Address.
- If you leave this list blank, then you will not restrict access for this user.
- Your CRA also has access to this list, and can edit your changes or add new restrictions.
- Additionally, your CRA has the capability of restricting access for your company as a whole, and those settings are not reflected here.

Add a Single IP Address

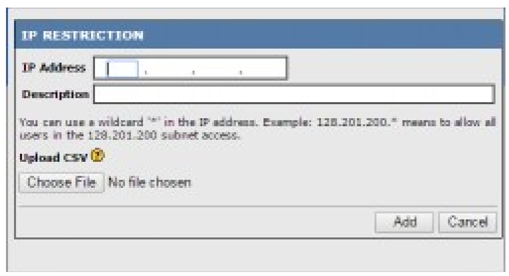
1. **Right-click anywhere on the IP Restriction table.** This will bring up a pop-up menu.
2. **Click the *Add* option from the menu.** A new window will display where you can input the IP Restriction into the IP Address field and add a description if desired.



3. **Enter the IP address and a description, then press the *Add* button.** This will close the pop-up and add IP address to the IP Restriction Table.
4. **Click the Save button at the top of the Restrictions tab to save all your changes.**

Add Multiple IP Addresses

1. **Right-click anywhere on the IP Restriction table.** This will bring up a pop-up menu.
2. **Click the *Add* option from the menu.** A new window will display where you can input the IP Restriction into the IP Address field and add a description if desired.

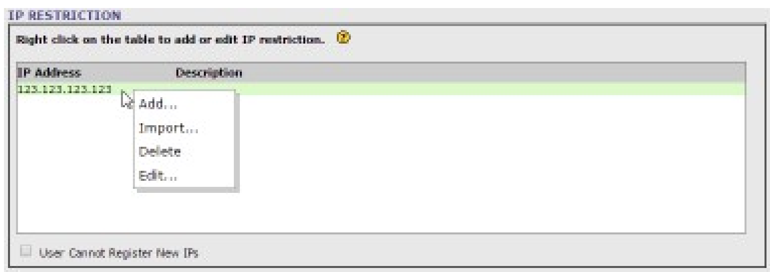


3. **Upload a CSV file.** In order to accommodate specifying several IP Addresses or ranges of IP Addresses without using the wildcard (*) symbol, you may upload a CSV file with the following formatting:
    - No header row.
    - Each row must contain a different IP Address.
    - Column A should be populated with IP Addresses.
    - Column B should contain a description of the IP address in column A. If no description is needed, leave the cell in column B blank.
    - There must be no blank row in between two populated rows.
4. **Click on the *Add* button.** This will batch add all the IP addresses from the CSV file into the setup.
5. **Click the Save button at the top of the Restrictions tab to save all your changes.**

Edit an IP Address

1. **Right-click on an existing IP address in the IP Restriction table.** This will bring up a pop-up menu.
2. **Click on the *Edit* option from the menu.** A new window will display where you can input the IP Restriction into the IP Address field and add a description if desired.
3. **Modify the IP address and the description, then press the Save button.** This will close the pop-up and add IP address to the IP Restriction Table.
4. **Click the Save button at the top of the Restrictions tab to save all your changes.**

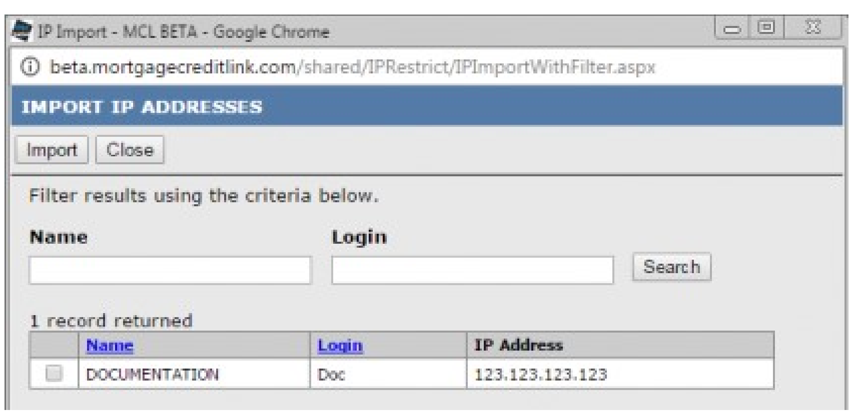
Remove an IP Address



1. **Right-click on an existing IP address in the IP Restriction table.** This will bring up a pop-up menu.
2. **Click on the *Delete* option from the menu.**
3. **Click the Save button at the top of the Restrictions tab to save all your changes.**

Import an IP address

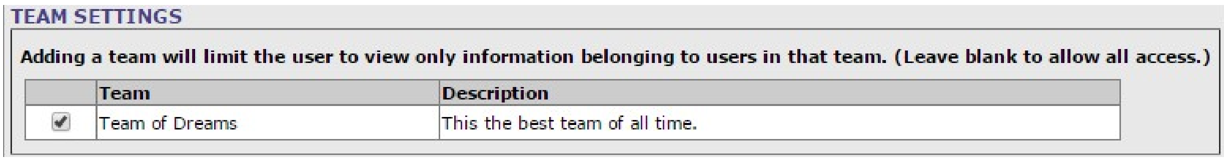
1. **To import an IP address to a user's restriction list, scroll down and right-click anywhere on the IP Restriction Table and then click the *Import* option from the drop-down menu.** This will open up a pop-up menu.



2. **Select one or more IP addresses from the list by checking the checkbox on the left.** If

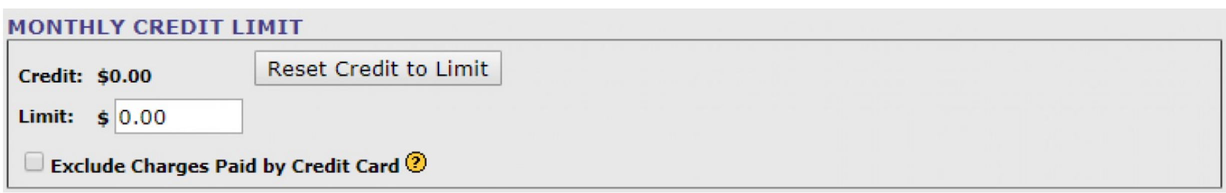
there are a lot of IP addresses, you can narrow the list down by searching by Name or Login.
3. **Click the *Import* button.** This will add the selected IP addresses to the user's setup.
4. **Click the *Save* button at the top of the Restrictions tab.** This will save all your changes.

Team Settings



If your account is setup with teams, these will be listed here. Otherwise, this section will be blank. **To add or remove a user from a team, simply check/uncheck the checkbox(es).** For more details on Teams, visit the Team Settings section below.

Monthly Credit Limit



The Monthly Credit Limit feature places a restriction on individual users which caps the amount of charges they can accrue each month. This limit will automatically reset every month. This is helpful for where the company pay for what the employee orders, but does not want to give the person unlimited usage. To use this feature:

1. Specify the limit to be set and click the *Reset Credit to Limit* button. Note that setting the limit to $0.00 means removing the limit.
2. By defalt, when the user orders a product or service and pays for it via credit card at the time of ordering, their credit limit will still be reduced. To prevent this from happening, check the *Exclude Charges Paid by Credit Card* box.
3. Click the Save button to save all changes.

The *Credit* field will show the amount of credit remaining on the user's account. This will decrease as the user orders products and services.