



## System Administration for Company Admins

This article describes the system administration functions of STASH that are available for company administrators responsible for a Vault.

As a company administrator, you have the ability to create and administer user accounts for your users, and assist your users with groups and folder permissions, as well as define company settings, company profile, and storage locations.

This article is organized according to functions available in the administration module.

- [Access Control](#)
- [Companies](#)
- [Additional Information](#)

To access the administration module, login to your Vault with your administrator account and click the “cog” in the upper right.



*Admin “Cog” and Admin Menu*

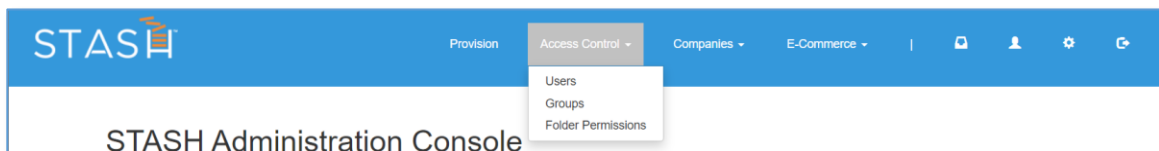


*“Cog” and Reduced Admin Menu*

Depending on the width of the browser window, you may see all the menu options displayed, or for narrow screens, the admin menu options will be displayed as a “hamburger” icon – the three horizontal dashes. Clicking the dashes will bring up the same menu options as displayed on larger screens.

The color of the background and menu items may be different than those displayed in this document due to branding and color styles in your company profile.

### Access Control



*Access Control Menu in the Administration Module*

The “Access Control” menu item allows you to create, edit and delete individual accounts, groups, and folder permissions for your company. *PLEASE SEE IMPORTANT NOTE* about passwords in this section before you change any user passwords.

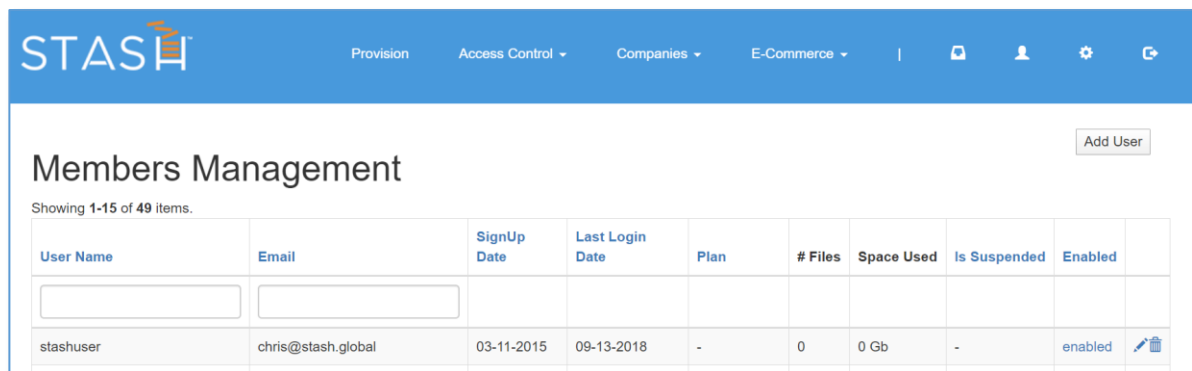
## Users

With the Users administrator module, you can create, edit, and delete user accounts within your company with up to “Company Admin” account permissions. The files, directory structure, and secure storage space is shared with all users in the company, but may be restricted by [folder permissions](#). Your plan determines the amount of secure storage space your company has in addition to any additional features or services.

**IMPORTANT NOTE ON PASSWORDS** – as the company administrator, you can change and reset passwords for any user within your company. If they forget their password, you can reset it for them, and they will not lose access to files in the shared data Vault. If the company has only a single company administrator, and forgets the login account information, all data stored in the Vault will be lost. It’s recommended to make at least two company administrator accounts and store the login information for each in a secure place. If one admin forgets their login information, the other can reset it for them, with no loss of data. Even if an admin forgets their login information, any existing user accounts will be able to access data in the shared Vault provided they have their login information.

### Listing users

From the admin module, click Access Control, then click Users. A list of the users registered to your company will be displayed. From here, you can see basic summary of the user accounts including the plan they are on, the number of files they have uploaded and the amount of storage space they have used. You can also edit and delete accounts from this screen. You can filter the list of users by entering a partial username in the box at the top of the “User Name” column or entering a partial email address in the box at the top of the “Email” column. You can sort the list by clicking any of the headings that appear as links; not all columns support sorting.



The screenshot shows the STASH Members Management interface. At the top, there is a navigation bar with the STASH logo and menu items: Provision, Access Control (selected), Companies, and E-Commerce. Below the navigation bar, the title "Members Management" is displayed, along with an "Add User" button. The interface shows a table with the following columns: User Name, Email, Sign Up Date, Last Login Date, Plan, # Files, Space Used, Is Suspended, and Enabled. The table contains one row for a user named "stashuser" with email "chris@stash.global", signed up on 03-11-2015, last login on 09-13-2018, on a "-" plan, with 0 files and 0 Gb of space used. The user is not suspended and is enabled. There are search boxes for User Name and Email above the table.

User Name	Email	Sign Up Date	Last Login Date	Plan	# Files	Space Used	Is Suspended	Enabled
stashuser	chris@stash.global	03-11-2015	09-13-2018	-	0	0 Gb	-	enabled

*User List – Available from Access Control -> Users in the Administration Module*

### Creating a new user

If your plan allows it, you can create additional users who will have shared access to the data Vault. From the admin module, click Access Control, then click Users. A list of the users registered on the system will be displayed. Click the “New User” button at the top of the list and complete the form that is displayed. Click the Create button and the user account will be created, and the user will receive an email to activate their account.

Attribute	Description
Username	The username for the account; must be unique. Used by the user to login to the Vault.
UUID	Assigned when the user account is created – this is a universally unique identifier that represents the user in the backend across all STASH instances
Company ID	Select the company the user will belong to. If the company doesn't exist, you must create it first (see <a href="#">provisioning</a> or <a href="#">company</a> sections of this article)
Password	This is a temporary password for the user account to login to the vault. If creating a new account, it is highly recommended you select the "Force Password Reset" option as well. Required for login to the Vault.
Force Password Reset	Forces the user to change their password on next login to the system
Email	The email address for the user; all system generated notices relevant for this account will be sent to this address.
MFA/2FA Enabled	If checked, will require the user to enroll a mobile device into the selected MFA provider and will require its use as part of the login process
MFA/2FA Enrolled	READ-ONLY, if checked, indicates the user has successfully enrolled with the MFA provider
Is Locked	If checked, indicates the user account is locked (most often because it has exceeded the number of failed logins). May be used by administrators to temporarily deactivate an account or prevent a user from logging in or using STASH services with this account.
Dash Enabled	If checked, allows the user to use the DASH service; this service may not be available on all deployments, and may be disabled by the STASH administrators, in which case, this setting is ignored.
Allow User to View Data Map	If checked, allows the user to view the location of their data on a global map; this service may not be available on all deployments, and may be disabled by the STASH administrators, in which case, this setting is ignored.
Num Failed Logins	READ ONLY, indicates the number of failed logins the user account has. All accounts are locked after 6 failed login attempts and must be unlocked by an administrator.
Plan ID	Select the Plan this account should use. For User accounts that are part of a company, select "Vault Account". For external users, select "External Account", and for WebErase accounts select "WebErase Account".
Vault ID	Leave blank; the system will automatically assign a Vault ID based on the plan type
Permissions	Select one or more permissions to assign to the account; see Permissions Table below
Last Failed Login Date	Lists the date/time the last login occurred for this account or blank if none have occurred


The following table summarizes the account permission types and when it's appropriate to use one level or another. Multiple permissions may be defined for a given account – for example, the initial account created for each company has Company Admin, Company User Admin, Company User Vault Master, and User privileges assigned to it.

Permission Level	Purpose
Company Admin	Company administrator; access user and company functions

Company User Admin	Administrator for company users; access user function only
Company User Vault Master	The master account for a company; this account is used to store the master file structure and defines encryption/decryption keys.
Company DLP Admin	Reserved for future use
Company DLP Approver	Reserved for future use
User	Standard user access
No Access	Overrides any other privilege level and will not be able to log on

### Editing a user


To edit a user, click the pencil icon to the right of their entry in the user list. See creating a user section for an explanation of the fields available. Some fields, such as username, are not editable once the account is created.

stashuser	chris@stash.global	03-11-2015	09-13-2018	-	0	0 Gb	-	enabled	
-----------	--------------------	------------	------------	---	---	------	---	---------	---

*Actions for Editing and Deleting User Accounts*

### Deleting a user

To delete a user, click the trash icon to the right of their entry in the user list. A confirmation box will appear to make sure you want to delete this user. Once the account is deleted, they will not be able to login to the Vault or use any other STASH services. Files in the vault WILL NOT be affected by deleting a user.

stashuser	chris@stash.global	03-11-2015	09-13-2018	-	0	0 Gb	-	enabled	
-----------	--------------------	------------	------------	---	---	------	---	---------	---

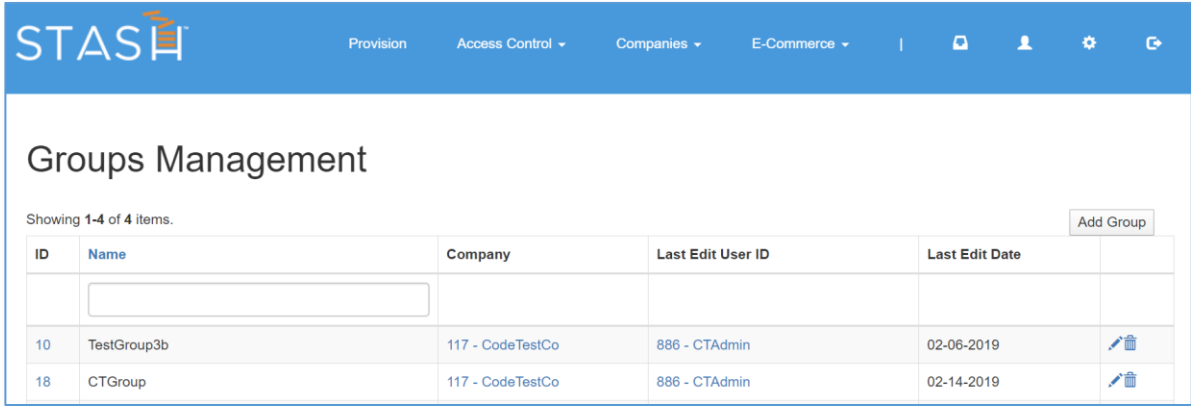
*Actions for Editing and Deleting User Accounts*

## Groups

Groups are a mechanism for organizing users in a company to simplify administration. A group may contain one or more users, and can be used to define permissions elsewhere in the system (e.g. Folder Permissions).

### Listing Groups

Click "Access Control" -> Groups to list the groups defined on the system. You can see basic summary of the groups including the name, who created the group and when. You can filter the list of groups by entering a partial name in the box at the top of the "Name" column. You can sort the list by clicking any of the headings that appear as links; not all columns support sorting.



*Group List – Available from Access Control -> Groups in the Administration Module*

### Creating a new group

To create a new group, click Access Control in the admin module, then select Groups, and click “Add Group” button at the top of the group list. Once you create a new empty group, you can edit the members of the group – see below.

Attribute	Description
ID	Assigned by the system to uniquely identify this group.
Name	The name of the group; must be unique for a company
Last Edit TS	The date/time, in Unix epoch format, this group was last modified
Last Edit User ID	The ID of the user which last modified this group

### Editing a group

To edit a group, click on the pencil icon to the right of its entry in the group list. See creating a new group section for an explanation of the fields available. Some fields displayed, such as ID or Last Edit TS are not editable once the group is created and displayed for informational purposes only.






*Actions for Editing and Deleting Groups*

You can delete any members in the group by clicking the trashcan icon to the right of the group membership entry. You can add a member to the group by selecting the user or group from the dropdown and click the “Add Entry” link.

## Update Group: CTGroup

Group Memberships  
Showing 1-3 of 3 items.

Object Name	Group name	Last Edit User ID	Last Edit Date	
CTAdmin (886, User)	CTGroup	886 - CTAdmin	07-06-2020	
tokenusera (1101, User)	CTGroup	886 - CTAdmin	07-06-2020	
TestGroup (26, Group)	CTGroup	886 - CTAdmin	07-06-2020	

User - CTAdmin (886)

[Add Entry](#)

*Updating the Members in a Group*

### Deleting a group

To delete a group, click the trash icon to the right of its entry in the group list. A confirmation box will appear to make sure you want to delete this group. Once the group is deleted, it can't be recovered, and any permissions defined using this group will be updated accordingly.

10	TestGroup3b	117 - CodeTestCo	886 - CTAdmin	02-06-2019	
----	-------------	------------------	---------------	------------	---

*Actions for Editing and Deleting Groups*

### Folder Permissions

Folder permissions control who can view or edit files in folders in a company. A folder permission consists of a user or group, the folder to apply the permission to, and the permission level. Folder permissions are normally set through the Vault interface, but can be viewed, added, edited, or deleted from the admin interface.

Folder Permission Level	Description
None	The user has no permission on the folder and cannot view or edit files in the folder
Read	The user can view and open the files in the folder
Write	The user can view, open, edit, overwrite, and delete files in the folder
Full	The user has Write permission and can adjust permissions on the folder for other users

A folder will inherit permissions from its parent folder unless permissions are defined on the folder itself, in which case, these take precedent. When user and group permissions are in conflict, the most restrictive permission applies.

### Listing Folder Permissions

Click "Access Control" -> Folder Permissions to list the folder permissions defined for your company. You will see a basic summary of the folder permissions, the folder they apply to, and the user or group and permission level along with who edited or created the permission and the last time it was modified. You can sort the list by clicking any of the headings that appear as links.

ID	Folder ID	User or Group ID	Type	Permission	Last Edit User ID	Last Edit Date
204	My Home (65380)	stashuser (1)	User	Write	886 - CTAdmin	06-19-2019

*Folder Permission List – Available from Access Control -> Folder Permissions in the Administration Module*

### Creating a Folder Permission

To create a new folder permission, use the boxes in the last row of the folder permissions display table. Select the folder, the user or group the permission applies to, and the permission level, then click “Add Entry”.

*Creating a new Folder Permission*

Attribute	Description
ID	Assigned by the system to uniquely identify this permission
Folder ID	The ID of the folder the permission applies to
User or Group ID	The user or group ID the permission applied to
Type	If 'User', indicates the user or group ID is a user ID; if 'Group', indicates the user or group ID is a group ID
Permission	The permission level – see table above for description
Last Edit User ID	The ID of the user who created or last edited the folder permission
Last Edit Date	The date the folder permission was created or last edited

### Editing a Folder Permission

To edit a folder permission, click on the pencil icon to the right of its entry in the folder permission list. See [creating a new folder permission](#) section for an explanation of the fields available. Some fields displayed, such as ID or Last Edit TS are not editable and displayed for informational purposes only.

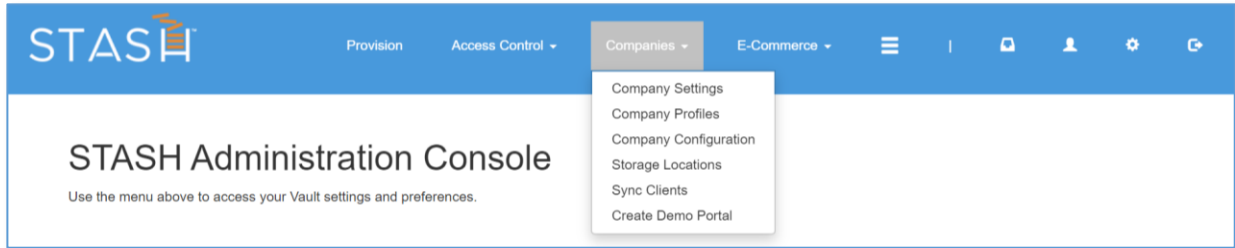
*Actions for Editing and Deleting Folder Permissions*

### Deleting a Folder Permission

To delete a folder permission, click the trash icon to the right of its entry in the folder permission list. A confirmation box will appear to make sure you want to delete this permission. Once the permission is deleted, it can't be recovered, and access to this folder will be updated accordingly.

*Actions for Editing and Deleting Folder Permissions*

Companies



*Companies Menu in the Administration Module*

The “Companies” menu item allows you to edit your company settings, profile information, configuration, create or edit storage locations, and view a list of SyncClients in use within your company.

*Editing your company settings*

Click “Company Settings” to view and change your company settings.

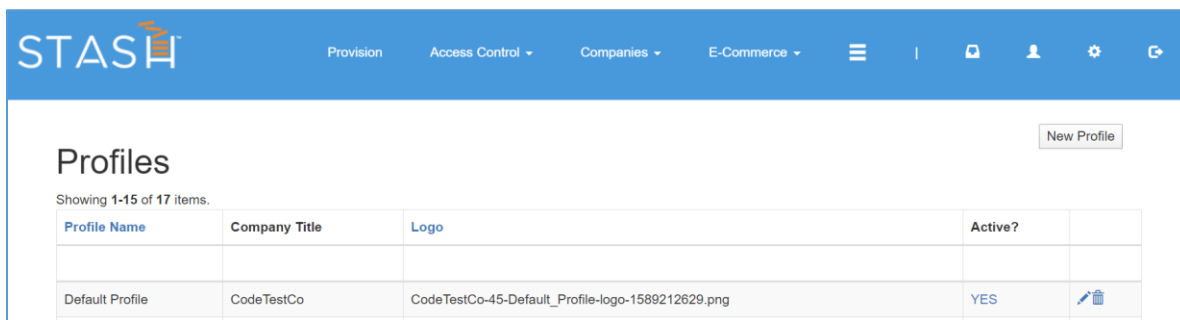
Attribute	Description
ID	Assigned by the system to uniquely identify this company
Company Name	The full company name; this will be displayed on the company portal landing page.
Company Code	A 6-32 character word or phrase which identifies the company; this will be used as part of the company portal link. This cannot be changed once the company is created.
Portal Link	Read-Only. The full URL for the company to access their portal through a branded landing page. This cannot be changed once the company is created.
Primary E-Mail Address	The email address to send customer inquiries to from the contact us page on the portal landing page. This contact page can be hidden – see the <a href="#">Company Profile</a> section.
Company Description	A long description of the company. This may be displayed on the portal landing page.
Short Description	A short description of the company. This may be displayed on the portal landing page or navigation footer – see the <a href="#">Company Profile</a> section.
Company Website	The URL for the company; this value is overlaid on the company logo in the upper left of all pages – see the <a href="#">Company Profile</a> section.
Company Title	The company name; this shortened version is displayed on the portal landing page.
Company Email Subject	Used as the subject for auto responder emails sent when a user sends a message through the Contact Us page.
Contact Email Body	Used as the body for auto responder emails sent when a user sends a message through the Contact Us page.



Is Flex Enabled	If checked, the company can created and manage their own storage locations using FLEX.
Company Profile	Read-Only. The ID of the active company profile.

### Company Profiles

Each company can define its own color scheme, logo, and landing page panels and menu items. The first time login configuration wizard shows a core subset of the profile; the admin module allows you to customize all the profile settings for your company.

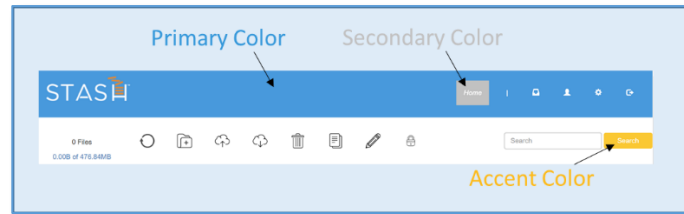


*Company Profile List – Available from Companies -> Company Profiles in the Administration Module*

A default company profile is created when your company account was created.

Attribute	Description
ID	Assigned by the system to uniquely identify this profile
Profile Name	A name for this profile, defaults to “Default Profile”
Is Active	Check the box if this profile is active; a company may have multiple profiles defined, but only one may be active at a time.
Main Color	The HTML color code for the primary color used in the Vault, see graphic below
Secondary Color	The HTML color code for the secondary color used in the Vault, see graphic below
Accent Color	The HTML color code for the accent color used in the Vault, see graphic below
Custom CSS	CSS added to each page to customize the look of the page
Text Overlay	The text to display over a media file when using DASH
Page Elements Enabled	Select the panels to display on the company portal landing page
Title Menu Elements Enabled	Select the menu items to display at the top of the company portal landing page
Allow Adding Users	If checked, your plan supports creating new users and the “Add User” button will be visible in the Users list. This box is read-only.
Is Dash Enabled	If checked, will allow company users to access the DASH service; this box is read-only and may not be available based on your plan.
Is DLP Enabled	If checked, enables the DLP service to process files and generate alerts or blocks. This box is read-only and may not be available based on your plan.

Logo	Select a file to use as the logo which will be displayed in the upper left of the vault and portal landing page.
Texture	This option is being removed in future versions – do not use.
Acceptable Use Policy	Company specific acceptable use policy to display on the acceptable use page; if blank, the default STASH acceptable use policy will be displayed.
Privacy Policy	Company specific privacy policy to display on the company privacy policy page; if blank, the default STASH privacy policy will be displayed.
Terms of Service	Company specific terms of service to display on the terms of service page; if blank, the default STASH terms of service will be displayed.



Main, Secondary, and Accent Colors and Location in the Vault

To edit your company profile, click “Company Profiles” from the Company menu

### *Company Configuration*

The company configuration module allows you to configure the Multi-factor Authentication, Identify and Access Management, Digital Risk Management, Encryption, Logging and Service options for your company.

A subset of these configuration options are available in the first time login wizard.

For MFA settings, you can set which MFA provider your company uses to one of available options, or you can disable MFA for all users in your company. MFA can be enabled for your company, and disabled for specific users within the company – see [editing user accounts](#). However, if MFA is disabled for a company, then the user MFA settings is ignored.

For IAM settings, you can set which IAM provider your company uses to one of the available options, or it defaults to STASH. If selecting Active Directory as the IAM provider, you must complete the active directory options – this may be configured for you when your account is created. If the default IAM provider, STASH, is selected, the STASH server will maintain all user information and serve as the authentication point for all users logging into the system.

For DRM settings, you can turn DRM on or off for your company. If enabled, you must select the DRM provider and set the DRM server options. Additional configuration of the integration component may be required in the backend to fully enable DRM. If the box is checked to log and geolocate access attempts, users may view the DRM map and access attempt list from their Account Settings page. You can also configure the DRM permissions to STASH permissions mappings here. For the given STASH permission, select the granular DRM permissions you want to apply. For example, if a user has “READ” stash permissions and you want them to be able to view, but not print DRM protected files, you would select the View and Light View DRM permissions to the right of the STASH “READ” permission.

For encryption, the option cannot be changed and is for display and informational purposes only. For accounts configured with Active Directory and DRM, this option must display “Passthrough”.

If you want to log vault activity, check the “Enable System Logging” box and provide a syslog compatible log receiver IP address and port. All file accesses, successful or failed logins, and administration functions are logged and can be sent to the syslog compatible server specified in real-time.

For options, if you want your users to be able to create their own API keys, check this box. If you want to allow your users to share files externally, check this box.

### *Storage Locations*

By default, STASH keeps 3 copies of all files protected by the system. The Storage Location page allows you to configure storage locations for use by your company. If you want your files to be stored in different location – select the location from the dropdown and click “Save”. New files uploaded to the system from this point forward, will use these locations. Changing these locations will not move or relocate data from the previous locations to the new locations.

You can see the STASH managed storage locations listed on this page. You can also define company specific storage locations here too. These must be Amazon S3 object storage compatible locations. The following table describes the attributes which must be defined for the new storage location. The storage location data is stored as a protected file in your Vault with the name `##_cfsl_##_txt` and is hidden by default.

<b>Attribute</b>	<b>Description</b>
Description	A descriptive name for the location; displayed in the storage location selection boxes
Is Available for Storage	If checked, this location will be available for company administrators to select as a location.
Storage Bucket-Folder Name	If using a S3 compatible location, enter the bucket name. If using a local storage location, enter the full directory path.
Storage Region Name	If using a s3 compatible location, enter the region name (e.g. us-west-1)
Location API Endpoint	If using a storage location that is accessible via API, enter the destination URL here
API ID	Enter the API ID or username used to access the storage location
API PW	Enter the API PW or password or secret used to access the storage location
Location Physical Address	Enter the physical address of the data center; this is not required or may be generic like a city name only and is displayed on the data storage location map.
Latlong	Enter the latitude and longitude (e.g. 79.2332,-117.2353) of the data center for this location; this will be used to plot the storage location on the data storage location map.
Map Marker Hover Title	Enter the text to be displayed when a user hovers over the map marker for this location on the map.
Map Marker Click Text	Enter the text to be displayed when a user click the map marker for this location on the map.

Map Marker Image	Enter the path to the image to be displayed when a user clicks the map marker for this location on the map.
------------------	---

### Sync Clients

The Sync Clients module displays all registered SyncClients and who they are registered to. Unless there are issues with SyncClient performance or users are having trouble sync'ing their files, these entries should not be deleted. Entries may be removed from the database by clicking trash can icon to the right of the entry in the list. The list may be sorted by clicking the column headers.

The screenshot shows the STASH application interface. At the top is a blue navigation bar with the STASH logo and several menu items: Provision, Access Control, Companies, and E-Commerce. Below the navigation bar is a white header area with the title "Sync Clients" and a sub-header "Showing 1-9 of 9 items." Below this is a table with the following data:

ID	User	Vault ID	UUID	Source IP	Last Access Timestamp	Registered Timestamp	Active?	
1	testuser1	1050	213f551c-dddb-4cd4-babd-a510320144fa	172.31.51.18	04-09-2020	04-08-2020	No	

*List of Registered Sync Clients*

### Additional Information

#### Account Self-Service

Users can accomplish certain tasks with their accounts without needing to contact support.

- Change Password – a user can change their password when they are logged in to their account by clicking “Change Password” on the Account Settings page.
- API Keys – a user can create a set of API keys for their account by clicking on the Generate Keys button on the Account Settings page. This option may not be visible unless the option to allow users to generate keys is enabled by a company admin in the [Company Configuration](#) screen.
- Payment Card - a company administrator can update the payment card used to pay for their services through the Plan Information screen in Account Settings. This option is not available for servers configured to use third-party billing.
- Change Plan – a company administrator can change their plan (upgrade or downgrade) through the Plan Information screen in Account Settings. This option is not available for servers configured to use third-party billing, and may not be available for all plans.
- Cancel Plan – a company administrator may cancel their plan through the Plan Information screen in Account Settings. This option is not available for servers configured to use third-party billing. When a company admin cancels their plan, their service will remain active for the remainder of their billing cycle, and then suspend. Once suspended, all user accounts belonging to that organization are suspended for a certain number of days, during which, company admins will receive email reminders that their account has been suspended. Company admins can login and reactivate their plan if they want. At the end of the suspension period, if the service hasn't been reactivated, all user accounts and files will get deleted.