System Administration for Partners

This article describes the system administration functions of STASH that are available for partners operating their own servers or white-label servers.

As a partner admin, you have the ability to provision vaults for your customers, create and administer user accounts for your customers, and assist your customers with groups, folder permissions, company settings, profiles, storage locations, as well as view the plans offered, transactions, and promotion codes for your customers to use when signing up.

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

- Provisioning
- Access Control
- Companies
- E-Commerce
- Billing System
- Additional Information

To access the administration module, login to your server with your partner 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 implemented on your server.

Provisioning
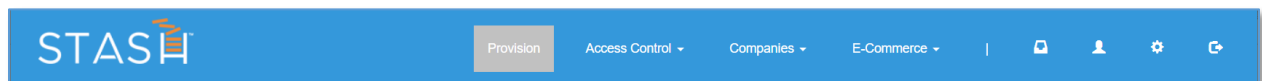
The "Provision" menu item is where you will create Vaults for your customers. To provision an account for a customer, click the "Provision" menu link, and complete the form. The vault will be provisioned

with the selected plan, and the system will send two emails to the email address provided on the form. The first email will contain a link to activate the account, the second email will contain the temporary password for their account.

The STASH system has a built-in billing module powered by Authorize.net. If this module is enabled, a valid credit card will be required to provision accounts. This credit card will be authorized and charged for the plans you provision through the "Provision" menu. This allows you to accept and process customer credit cards directly and have the STASH system handle recurring billing for you. If the billing module is not enabled, then you will be responsible for billing outside the STASH system, and all vaults created through the "Provision" menu do not require a credit card. However, all details, including pricing on the plans, use of promotions codes, and assigned plan options, all stay the same and are tracked by the system regardless of billing method used.

For more information, see Plans, Free Trials, and Promotion Codes in the E-Commerce section of this article.

This method can be automated, and you can create an E-Commerce page for your customers to sign-up. Refer to the Provisioning Guide for Partners for more information on the API.

Example E-Commerce Site with Automated Provisioning via STASH API

Access Control
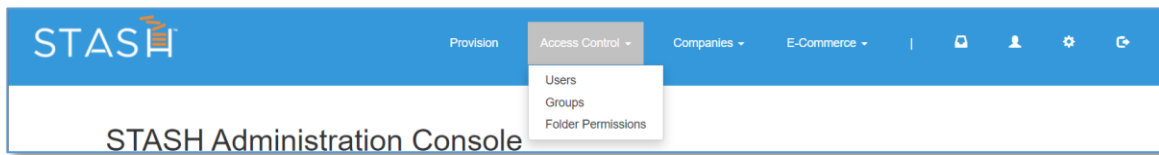
Access Control Menu in the Administration Module

The "Access Control" menu item allows you to create, edit and delete individual accounts, groups, and folder permissions for both the STASH company (your partner accounts are members of this default company) and for your user's companies. *PLEASE SEE IMPORTANT NOTE* about passwords in this section before you change any user passwords.

Users

User accounts are organized by company. The default company on the system is 'stash', and is where your partner account and other system-wide administrator accounts reside. All of these accounts are members of the 'stash' company. Other user accounts for your client's use are created under their own companies.

With the Users administrator module, you can create, edit, and delete other user accounts within the 'stash' company with up to "Partner" account permissions. Server administrator and global administrator accounts are reserved for STASH administrators and have access to additional functions such as creating and editing storage locations. User accounts within the 'stash' company should all be created with the "Account" plan type and a partner, company admin, or company user admin privilege level. This allows the user to access the system administration module and gives them 500MB of storage in a vault they can access. The directory structure is shared with other accounts in the 'stash' company, but users may only access data that they have uploaded.

For more information on Plan types, see Plans in the E-Commerce section.

IMPORTANT NOTE ON PASSWORDS – as the partner administrator account, you SHOULD NOT change passwords directly for users within a company – only the company administrator account should do so. When a company administrator changes a user's password, their access to files already in storage is not affected; but if a partner administrator account changes a user's password directly, that user will lose access to any data in their account. As a last resort, the partner administrator may change the password for a company administrator or other account, but they will lose access to any files in their Vault. The files may appear in the vault, but they can't be decrypted because forcefully resetting a password also resets the key used to encrypt and decrypt files. Again, this should be used only as a last resort, when a company administrator can't get into their account, and with the company administrators full knowledge and acceptance of the fact that they will no longer be able to access data in their account.

Listing users

From the admin module, click Access Control, then click Users. A list of the users registered on the system 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 as 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.
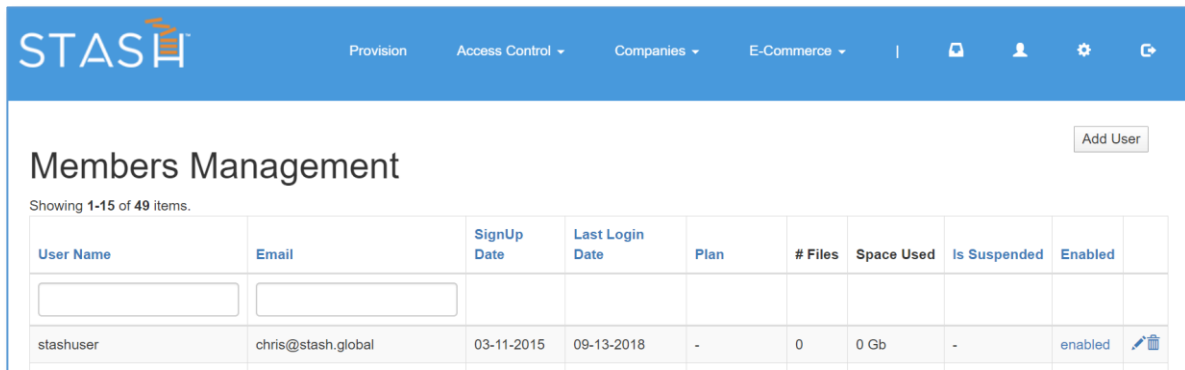
User List – Available from Access Control -> Users in the Administration Module

Creating a new user

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 provisioning or company 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 Partner accounts, select "Account". For User accounts that are part of a company, select "Vault Account". For standalone accounts, select the Plan they should be given. See Plans in E-Commerce section for more information.
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
Global Admin	Reserved for STASH administrator only
System Admin	Reserved for STASH administration only
Partner Admin	White-Label server administrators; access user, company, and e-commerce functions relevant to white-label server deployments
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.

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. If the account is a stand-alone account, all their files will be deleted. If the account is one that belongs to a company and shared vault, the files WILL NOT be affected, unless you are deleting the last user in the company, in which case, all the files will be deleted with the user account. This action is NOT reversible, and once the files and the last company account are deleted, they cannot be recovered.
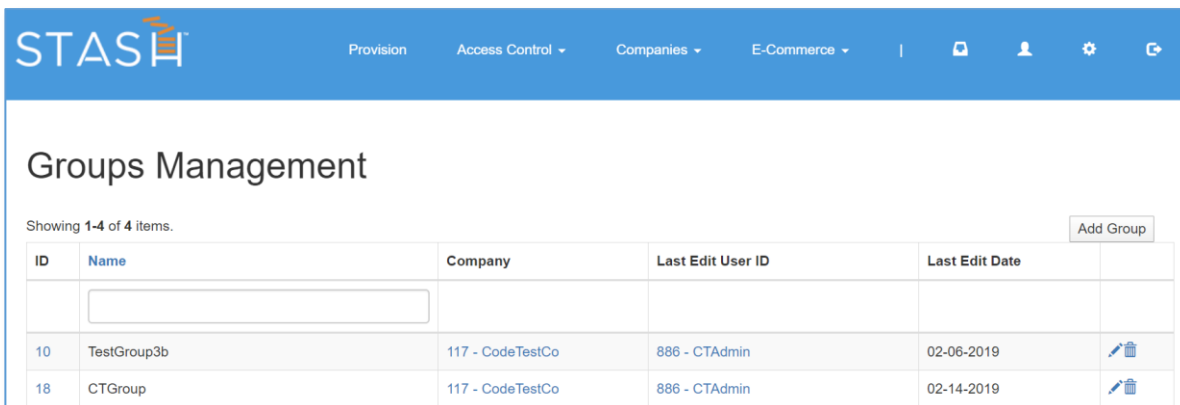

Actions for Editing and Deleting User Accounts

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. As a partner admin, groups that you define and those that your clients define within their companies, will be listed here. You can see basic summary of the groups including the name, company they belong to, 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
Company ID	Select the company the group belongs to
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 account 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.

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.

Actions for Editing and Deleting Groups

Folder Permissions

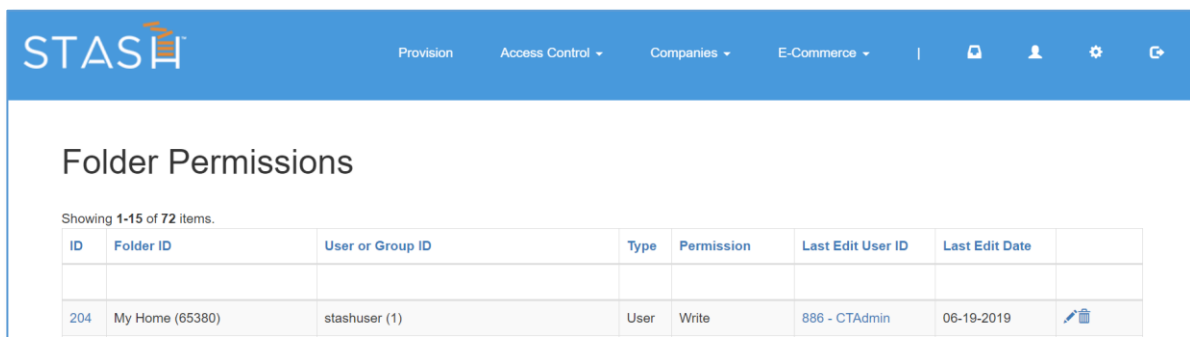Folder permissions control who can view or edit files in folders in a company. A folder permission consists of a user or group, the folder to apply the permission to, and the permission level. Folder permissions are normally set through the Vault interface, but can be viewed, added, edited, or deleted 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 on the system. As a partner admin, you can view, create, edit, and delete folder permissions for your client companies. 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.

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.
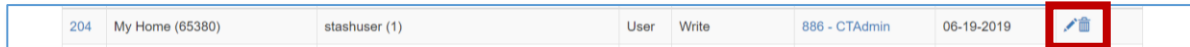
Actions for Editing and Deleting Folder Permissions

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.
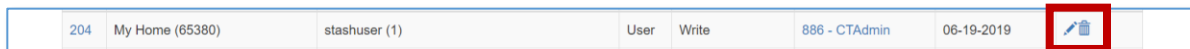
Actions for Editing and Deleting Folder Permissions

Companies
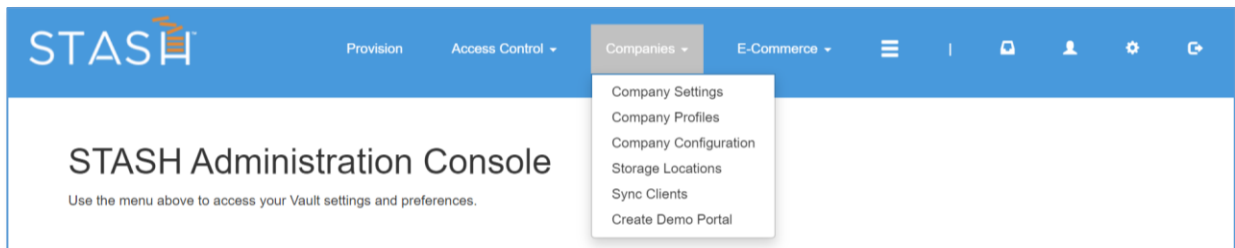
Companies Menu in the Administration Module

A Company is the organizational unit of users in STASH. All users are assigned to a company. The default company 'stash' holds the administration accounts and any other individual accounts. Other companies and their default user are created through the provisioning process. Company administrators can then create additional users which are assigned to the company. All company users except those in the 'stash' company have shared access to their company vault – meaning, users can see and interact with the same data unless folder permissions are used to further restrict the list.

The "Companies" menu item allows you to create, edit and delete companies, their profiles, and adjust their settings. As a general rule, you should create companies through the provisioning or demo portal process, but you can manually create companies using this module.

Click "Company" -> Company Settings to list the companies on the system. As a partner admin, you can view, create, edit, and delete companies. You will see a basic summary of the company including the name, website, email address for the vault administrator, the profile ID, and the number of users in the company. You can sort the list by clicking any of the headings that appear as links.
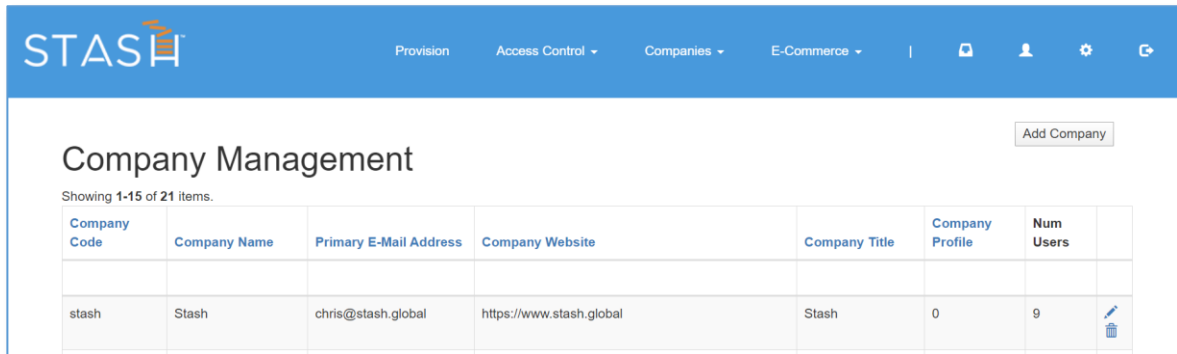
Company List – Available from Companies -> Company Settings in the Administration Module

Creating a new company

To create a new company manually, click the "Add Company" button on the company management / company list page, fill out the form, and click, "CREATE".

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 Company Profile 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 Company Profile 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 Company Profile 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.

Editing a company

To edit a company, click on the pencil icon to the right of its entry in the company list. See creating a new company section for an explanation of the fields available. Some fields displayed, such as ID or Portal Link are not editable and displayed for informational purposes only.

Actions for Editing and Deleting Companies

Deleting a company

To delete a company, click the trash icon to the right of its entry in the company list. A confirmation box will appear to make sure you want to delete this company. Once the company is deleted, it can't be recovered. CAUTION: A company should not be deleted unless all its user accounts are deleted first.

Actions for Editing and Deleting Companies

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 client companies.

This module is also available to company administrators, but will only allow them to adjust their own company profile.

A default company profile is created when a new company is created – either manually or through the provisioning or demo portal process. Should you need to create new profile, you can click the "New Profile" button on the profile list.

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, will allow company administrators and company user administrators to create new users within their company. This box is read-only for company administrators.
Is Dash Enabled	If checked, will allow company users to access the DASH service; this box is read-only for company administrators and may not be available on all servers.
Is DLP Enabled	If checked, enables the DLP service to process files and generate alerts or blocks. This box is read-only for company administrators and may not be available on all servers.
Company	Select the company this profile should be applied to
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.
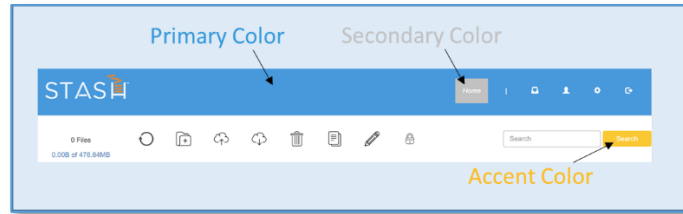
Main, Secondary, and Accent Colors and Location in the Vault

To edit a company profile, click on the pencil icon to the right of its entry in the profile list. See above for an explanation of the fields available.

To delete a company profile, click the trash icon to the right of its entry in the profile list. A confirmation box will appear to make sure you want to delete this company profile. Once the company profile is deleted, it can't be recovered, and the company will revert to the default STASH colors for their profile.

| Default Profile | CodeTestCo | CodeTestCo-45-Default_Profile-logo-1589212629.png | YES | 🖉🗑 |
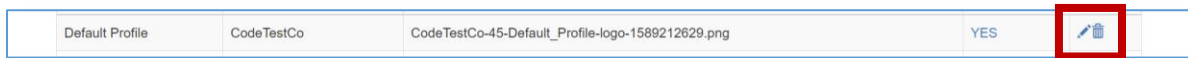
Edit and Delete Actions for Company Profiles

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 client companies. This page is available to company administrators.

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

To set or change a company configuration, select the company name from the drop down box, complete each section on the page, then click "Save".

For MFA settings, you can set a company's MFA provider to one of available options, or you can disable MFA for all users in a company. MFA can be enabled for a 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 a company's IAM provider 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 – see the provisioning services document for more information. 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 the 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 backed 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".

For logging, if a company wants to log their company-specific 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 wish the company users to be able to create their own API keys, check this box. If you want to allow 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 the default 'stash' company only. 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 storage locations listed on this page. These are locations that the global administrator has configured for use on this server. Some of these locations may be unavailable for use – check the data location map to confirm which locations have been used by your company.

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 the vault with the name _#_cfsl_#_.txt and is hidden by default.

Attribute	Description
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.

Company administrators have access to these functions and may define company specific locations for their use too.

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.
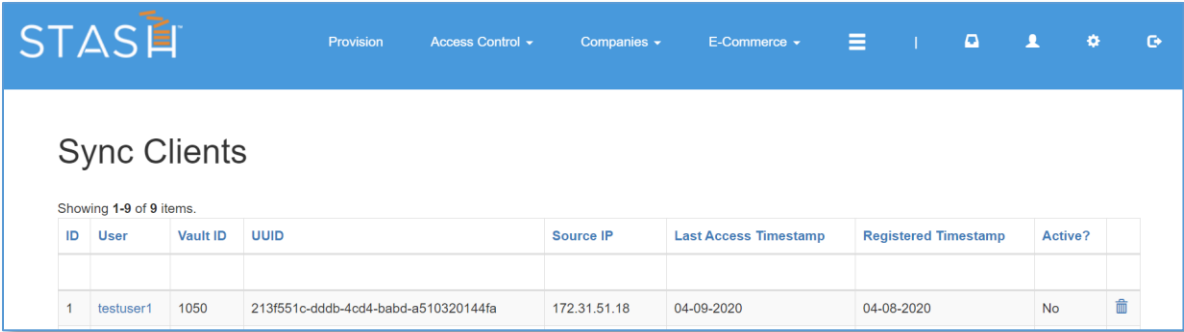
List of Registered Sync Clients

Create Demo Portal

You can create a fully configured and operational company portal for demonstration purposes with this module. These demo portals are valid for 3 months and should only be used for evaluation purposes. They cannot be converted to regular or paid accounts.

To create a demo portal, click "Create Demo Portal", fill out the form and click "Create".

See the provisioning section for details on the required fields – but note that no credit card is required for a demo portal. The plan, which defines the amount of storage for the demo portals, can be edited. See Plans in E-Commerce section for more information.
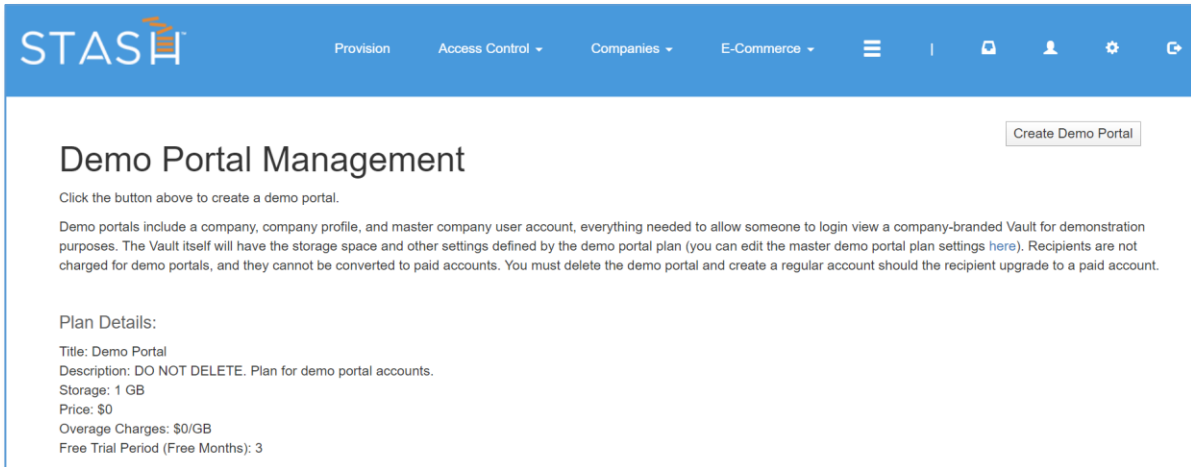
Demo Portal – Available from Companies -> Create Demo Portal in the Administration Module

When a demo portal is no longer needed, you must manually delete the user created for the demo portal, and then manually delete the company.

E-Commerce

The E-Commerce admin module allows you to view the plans available to your customers, view transactions from the billing system, view and edit the sales tax rates used by the server, and create / edit / delete promotion codes that your clients can use for discounts on service.
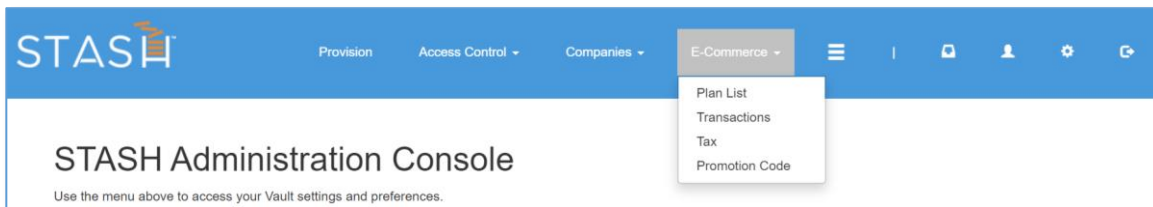
E-Commerce Admin Module Functions

Plan List

The Plan module allows you to view plans that your clients can sign up for on this server. A plan defines the amount of secure data storage a user has, along with any optional services, and the cost. The plans are created for you by the STASH administrator based on your requirements. You can see the result of these plans listed on this page. You can sort the list by clicking on the column headers. If any plans need to be modified, contact your STASH administrator.

Some plans are system level plans and cannot be deleted.
- Account – used for global and partner administrator accounts
- Vault Account – used for company user accounts, these accounts share a single Vault
- External Account – used for external sharing; this service may not be available on your server
- WebErase Account – used with WebErase; this service may not be available on your server
- Demo Portal – this plan defines the attributes of the portal created with the Demo Portal function – see Demo Portal in the Company section. This plan can be modified if you wish to offer a different configuration through the demo portal function.

To view the details of any plan, click the eye icon to the right of the plan entry in the list. The following attributes will be displayed for the plan:

Attribute	Description
ID	The unique identifier for this plan, assigned by the system
Title	The title of the plan; this is displayed on the change plan list in account settings
Description	The description of the plan; this is displayed on the change plan list in account settings
Price ($/mo)	The base price of the plan in $ per month not including taxes or options
1yr Subscription Price	The base price of the plan if purchased for 1 year in advance
2yr Subscription Price	The base price of the plan if purchased for 2 years in advance
3yr Subscription Price	The base price of the plan if purchased for 3 years in advance
Max Storage (GB)	The maximum amount of secure data all users may consume
Overage Type	The type of overage charge (1 = fixed overage, 2 = tiered cost) – see overage charges in billing section
Overage Charges ($/GB)	If overage charge type is 1, the amount charged per GB per month of overage
Overage Charges SKU	If overage charge type is 1, the SKU to represent fixed overage; this will appear on the credit card receipt
Overage Tiers	If overage charge type is 2, this is a JSON encoded string containing the tiers and cost of GB per month at each tier.
Is Enabled	If enabled (1), this plan will be available for provisioning and for users to upgrade / downgrade their plans.
Products	If optional services are included with this plan, they will be listed here in a JSON encoded string
Free Months	The number of months included in a free trial; requires free trials be enabled for this server
Free Trial Days	The number of days included in a free trial; requires free trials be enabled for this server
Min Size / Max Size	These parameters are deprecated and will be removed in a future version of STASH
Is Add By User	If 1, this plan can be added to a new user created by company admins; a global or partner admin can add this plan to any new user they created.
First Account Permissions	These permissions are given to a user when they activate their plan

1ˢᵗ Login Wizard Type	The type of login wizard displayed when the user first logs in with this plan. Available options are 'None' (no wizard is displayed), 'Simple' (a wizard with just MFA and Company Profile options is displayed, or 'Enterprise' where all options are displayed.
Eligible Upgrade/Downgrade Plan	Lists the plans that a user can change their current plan to. This allows the user to change their plan through self-service.

Transactions

The transactions module allows you to view credit card transactions processed by the billing system and the response from the credit card processor. You can short items in the list by clicking the column header, though not all columns support sorting. The list will show you the user ID that generated the transaction (clicking on the User ID will take to you to the user information page), the Plan ID, the price in USD, the type of transaction, Yes/No if the transaction was successful or not, the date of the a transaction and link for more details about the transaction including the response from the credit card processor. If the User and Plan are set to -1, this indicates an authorization transaction, which are used to validate the payment method only and not an actual charge against the card. If the billing system is not enabled, for example, your server is set for 3rd party billing, this list will be empty.

Transaction List – Available from E-Commerce -> Transactions in the Administration Module

Note: No credit card data (numbers, expiration, CVV, or track) are stored on the system. When billing is enabled, this information is set straight to Authorize.net and a unique customer and payment profile token is returned; these tokens are used to reference the customer in Authorize.net, process recurring billing charges, and update credit card information.
For additional information on credit card processor responses, see Authorize.net.

Tax

The internal billing system will collect sales tax on all plans sold; this tax is added to the amount of the plan and options and charged to the credit card on file when the plan is initially purchased and during each recurring billing. You can filter the list of displayed rates by entering a partial ID, country name, state name, or tax rate in the boxes at the top of the list. You can sort the list of displayed rates by clicking the column header.

Tax List – Available from E-Commerce -> Tax in the Administration Module

Tax rates are assigned on a country and state/region basis. The tax rate displayed is a percentage, e.g. 4% for Alabama, United States as show in the graphic above. The tax rate selected is based on the billing address of the credit card used to purchase the plan. You can add a tax rate by clicking the "Add Tax" button in the upper right of the page. You can edit a tax rate by clicking the pencil icon to the right of entry in the tax list. You can delete a tax rate by clicking the trash can icon to the right of the entry in the tax list.

The default tax rates for states in the United States are provided and are based on the assumption that your company has a presence in the United States and is mandated to collect sales tax on digital purchase. Consult your company's finance department or an advisor for the tax rates to use based on where you are operating the server.

Promotion Codes

Promotion codes can be used to offer discounts to your customers on plans. To sort the list of promotion codes displayed, click the column header.

Promotion Codes – Available from E-Commerce -> Promotion Code in the Administration Module

Promotion codes can be used to offer a percentage off or set discount on the established plan cost. They can also be used to offer a set number of free months or days before or after a plan is charged. Promotion codes can't be combined with a free trial offer if you have the plan and server configured to offer free trials (see E-Commerce, Plans for more information). A promotion code is not required if the multi-month/year discounts are used in the plans (see E-Commerce, Plans for more information). An implicit promotion code "FREETRIAL" is automatically applied to plans that are configured for free trial. This "FREETRIAL" code does not need to be created, nor will it be listed in the promotion code list because it is always enabled, always on and applied automatically.

Discount on the monthly rate promotion codes:
To create a discount code that provides a discount on the plan rate, either as a percentage, or a set amount, select "A discount on the monthly rate" for the promotion type. These codes can be used, for example, to offer a 50% discount off the monthly rate, or $5 off the monthly rate of a plan.

A Specified number of months/days free codes:
To create a discount code that provides a set number of months or days free with a plan purchase, select "A specified number of months/days free" for the promotion type. This type of code can be used, for example, to offer "buy 12 months get 3 free at the end of the subscription" or "buy 6 months, get 1 free month now" discounts.

To add a new promotion code, click the "New Code" button in the upper right of the promotion code list display. Complete the form and click "Save".

Attribute	Description
Code	Enter up to 10 letters or numbers for the code; this is the code you will give to your customers to get the discount.
Description	A description of what the code is intended to do
Starting Date	A code can be set to start immediately or sometime in the future – select the date the code will be valid.
Expiration Type	Code can be set to expire after a set number of hours or days from the point they are created; this is useful if you want to allow a promotion code to be used only for a set period of time. Valid options are "Hours", "Days" or "No Expiration". If "No Expiration" is selected, the code must be manually marked as inactive or manually deleted.
Expiration	Enter the number of hours or days the code is valid for; requires Expiration Type be set to "Hours" or "Days" accordingly.
Is Active	Check the box to allow the code to be used. You can temporarily disable a promotion code by unchecking this box.
Max Usage	Specify the maximum number of times a code may be used. If you are unsure of the interest or level of response, you can set a value here to limit the number of times a code can be used, and reduce the financial risk of open-ended promotion codes.
Company ID	Select the company this promotion code applies to, if desired, or select "any" to allow any user from any company to use the code.
Min Requirements	Set the number of months that must be purchased in order to qualify for this promotion code; or 0 if none. This is useful if you want a promotion code to apply only if the user purchases the minimum number of months specified, for example, this code is only valid if purchasing a plan for 12 months or more.
Promotion Type	Sect the type of promotion discount – see above for the difference between "discount on monthly rate" versus "free months/days".
Discount Type	If the promotion type is discount on monthly rate, select the discount (either % or Amount), and enter the discount in the Discount box.
Discount	If the promotion type is discount on the monthly rate, enter the discount amount here. For example, if offering 50% off a plan, you would select "Discount on the

	monthly rate" for promotion type, "%" for discount type" and enter "50" for the discount.
Free Month Type	If the promotion type is a set number of free months or days, select when the months/days should apply – either ATB or ATE. ATB applies the free months/days at the beginning of the plan, before the user is charged for their plan. ATE applies the free months/days at the end of a plan period. For example, if a user is to get 3 months free up front, you would select "ATB" and the user would be billed for their plan at the end of the 3 month period. If you want the user to pay for the plan first, and then get the free period, you would select "ATE", the user would be billed for their plan immediately, and wouldn't be charged again for their plan until after their subscription period plus their free months/days was up.
Free Months	If the promotion type is a specified number of months/days free, enter the number of free months or 0 if no free months are allowed.
Free Days	If the promotion type is a specified number of months/days free, enter the number of free days or 0 if no free days are allowed.
Eligible Plans	Check the plans which a user can use this plan with. This allows you to restrict promotion codes to certain plans only.

To view the details of a promotion code, click on the eye icon to the right of its entry in the promotion code list.

To edit a promotion code, click on the pencil icon to the right of its entry in the promotion code list. See the table above for an explanation of the fields available.

To delete a promotion code, click the trash can icon to the right of its entry in the company list. A confirmation box will appear to make sure you want to delete this promotion code. Once the code is deleted, it can't be recovered.
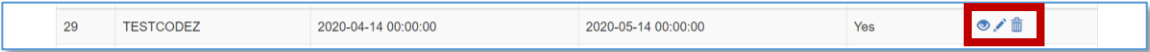
Actions for Viewing, Editing and Deleting Promotion Codes

Billing System

The STASH system has a built-in billing system which works with Authorize.net. The internal billing system can be turned off by a STASH administrator if you use your own billing methods. If the billing system is turned off, you can still provision accounts, and a credit card is not required. Initial payments and recurring payments will not be processed if the internal billing system is turned off, however, all plan costs will remain the same to make it easy for you to determine how much to bill your customers.

In order to use the built-in billing system, you must obtain an Authorize.net merchant account and API access credentials. A STASH administrator will configure your server to use your Authorize.net account.

The billing system will process all initial plan payments if the plan, free trial, and promotion settings result in an upfront cost of the plan. The billing system will also automatically process recurring payments for monthly, yearly and 3 year plans on the anniversary of their service date. For example, if a user signs up on May 10 for a plan that costs $100 per month, and is given a 1 month free trial, the billing system will authorize, not charge, the provided credit card to make sure it's a valid card, and

activate their account on May 10. After the 1 month free trial is over, on June 10, the system will automatically charge the first month of service ($100). The system will then charge the same amount each month, on the anniversary of the signup date, in this example, the 10ᵗʰ of the month.

Initial billing for plans is processed by the provisioning process. Recurring billing is handled by a scheduled job on the server and is not accessible or configurable through the admin module. In all cases, the credit card details provided with the provisioning request are sent immediately to Authorize.net and not stored or logged on the STASH system. Authorize.net provides a customer profile ID and a payment profile ID, which are saved with the user's account data on the STASH system. These profile IDs are used by the recurring billing process to charge the user's card – and no credit card information is sent, stored, or processed by the billing system for these recurring payments. If a user needs to update their card, they can do so through the Accounts Settings page, and the card details will be immediately transmitted to Authorize.net, which will provided updated profile IDs to the STASH system. The billing system will use these new profile IDs for the user's next billing activity.

If the billing system detects a charge cannot be made, the account will be deactivated and the user will only able to access their account settings page to update their credit card information. If the user does not do this, their account will be locked and then closed within 7 days. The user will send notices of this activity to the email address on file for the master account owner.

If the internal billing system is disabled, you will be responsible for performing initial and recurring billing. Further, the self-service options to change their plan or cancel their account will not be available to the user

Additional Information

Billing Receipts
If the internal billing system is enabled, every time a charge is processed, the user will receive a notification of charges from the STASH system and if configured, will receive a receipt for the charge from Authorize.net. The STASH administrator can enable or disable credit card receipts as you need. Credit card receipts and charge notifications are not sent if the internal billing system is disabled.
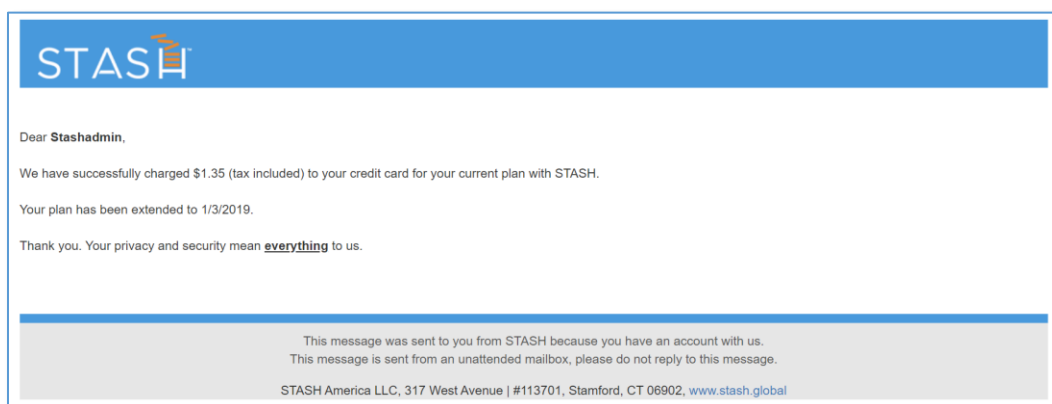
Example Charge Notification from STASH Billing System

Order Information

Description: Goods or Services
Customer ID 1050

Billing Information   **Shipping Information**
John Smith
123 Main St
San Antonio, TX 78231
United States
john@example.com

Item	Name	Description	Qty	Taxable	Unit Price	Item Total
761	STASH 10TB	STASH, 10TB of secure data	1	Y	$4350.00 (USD)	$4350.00 (USD)
1	Option	STASH Dash - Secure File Sharing	1	Y	$0.00 (USD)	$0.00 (USD)
19	Option	STASH Add Users	1	Y	$0.00 (USD)	$0.00 (USD)
37	Option	STASH FLEX - Flexible Storage Locations	1	Y	$0.00 (USD)	$0.00 (USD)
46	Option	STASH Data Map	1	Y	$0.00 (USD)	$0.00 (USD)
N/A	Tax	Sales Tax	1	N	$0.00 (USD)	$0.00 (USD)

Total: $4350.00 (USD)

Payment Information

Date/Time: 7-May-2020 17:05:03 PDT
Transaction ID: 40048566553
Payment Method: Visa xxxx1111
Transaction Type: Purchase
Auth Code: 2CRSTD

Merchant Contact Information

Stash America
Las Vegas, NV 78110
US
billing@stash.global

Example Credit Card Receipt from Authorize.net

Overage Charges

Plans can be configured to charge a user for overage or storage used above their plan limit. There are two types of overages, 1) Fixed, and 2) Tiered. If the internal billing system is used, charges for any overage a user has during the month is billed and charged separately from their recurring subscription charge.

For fixed overages, a set cost per Gigabyte per month is charged. The actual overage usage is calculated on an hourly average. For example, if a user uses 1 extra gigabyte over their plan limit, and the overage cost is $2.00 per gigabyte, for the last half of their billing cycle, they would be charged $1.00 as the average overage was 1 gigabyte for half the month, resulting in 50% overage usage.

For tiered overages, a sliding scale is used to determine the cost per gigabyte. The more overage, the less per gigabyte charge, for example. The tiers are fixed at 0-250 GB, 251–500GB, 501-1000GB, 1-4.99TB, 5-25TB, and 25TB+. When creating your plans, you can assign a cost per gigabyte to each of these tiers, and the user will be charge the rate according to their usage. For example, if they were to use 575GB overage in a given period, they would be charged the 501-1000GB tier rate per gigabyte.

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 user 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 enabled with the 'use3rdPartyBill' parameter.
- Change Plan – a user 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 enabled with the 'use3rdPartyBill' parameter.
- Cancel Plan – a user 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 enabled with the 'use3rdPartyBill' parameter. When a user / 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 (set by the 'suspended_files_life_days' parameter). During the suspension period, company admins will receive email reminders, and 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.