1. InfoVaultz Administration Guide . . . 3
1.1 InfoVaultz Site Setup . . . 3
1.1.1 Logging as Administrator . . . 4
1.1.1.1 Logging In . . . 4
1.1.1.2 Changing Admin Password . . . 4
1.1.2 Basic Server Settings . . . 5
1.1.3 Setting up InfoVaultz Managed Storage . . . 6
1.1.4 Setting up User Access . . . 8
1.1.4.1 InfoVaultz User . . . 8
1.1.4.2 InfoVaultz User Authentication . . . 10
1.1.4.2.1 InfoVaultz Default Authentication . . . 10
1.1.4.2.2 Active Directory Authentication . . . 11
1.1.4.2.3 LDAP Based Authentication . . . 14
1.1.4.3 Enable new account creation requests . . . 16
1.1.4.3.1 Account Approval . . . 19
1.1.4.4 Preload data for new accounts . . . 23
1.1.5 Creating User Groups . . . 24
1.1.6 Setting up Network Shares . . . 27
1.1.7 Setting up InfoVaultz Branding . . . 34
1.1.7.1 Labels and Logos . . . 34
1.1.7.2 UI Messages . . . 36
1.1.7.3 Email Templates . . . 37
1.1.7.4 News Feed . . . 39
1.1.7.5 Terms of Service . . . 41
1.1.7.6 Customize Product URLs . . . 43
1.1.8 Configuring Email Integration . . . 46
1.1.9 Enable Antivirus Scanning . . . 48
1.1.10 Enable WebDAV . . . 50
1.1.11 Setting up Document Preview . . . 51
1.1.11.1 Ubuntu/Debian Instructions . . . 51
1.1.11.2 Redhat/CentOS Instructions . . . 54
1.1.11.3 Windows Instructions . . . 54
1.1.12 Enable File Change Notifications . . . 56
1.2 InfoVaultz Site Maintenance . . . 61
1.2.1 Managing Users . . . 61
1.2.1.1 Create new InfoVaultz user . . . 61
1.2.1.2 Import a InfoVaultz user from AD or LDAP Service . . . 62
1.2.1.3 Bulk creation of InfoVaultz users from CSV File . . . 63
1.2.1.4 Bulk import of InfoVaultz Users from AD Server . . . 65
1.2.1.5 Listing InfoVaultz Users . . . 67
1.2.1.6 Viewing User Properties . . . 67
1.2.1.7 Disabling InfoVaultz User . . . 69
1.2.1.8 Deleting a InfoVaultz User . . . 70
1.2.1.9 Reset User Password . . . 71
1.2.2 Managing Groups . . . 72
1.2.3 Managing User Folders and Files . . . 75
1.2.4 Managing Disk space Usage . . . 79
1.2.5 Managing Client Devices . . . 79
1.2.6 Upgrading InfoVaultz . . . 85
1.2.7 Audit Logs . . . 88
1.2.8 Backing up InfoVaultz Data . . . 92
1.2.8.1 InfoVaultz Backup and Restore - Linux Tool . . . 92
1.2.8.2 InfoVaultz Backup and Restore - Linux Manual . . . 98
1.2.8.3 InfoVaultz Backup and Restore - Windows Manual . . . 102
1.3 InfoVaultz Troubleshooting . . . 104
1.3.1 Known Issues . . . 104
1.3.2 Reporting problems in InfoVaultz . . . 105
1.3.2.1 InfoVaultz Debug Log File Locations . . . 105
1.3.3 Accessing InfoVaultz from an external location fails . . . 106
1.3.4 Active Directory Setup Issues . . . 106
1.3.4.1 Fails to connect to Active Directory Server . . . 106

1.3.4.2 Unable to find an AD User 106
1.3.4.3 Unable to find an AD Group 106
1.4 InfoVaultz Best Practices 106
1.4.1 Security 106
1.4.1.1 Changing default config and log directory for InfoVaultz 107

InfoVaultz Administration Guide

The InfoVaultz Administration Guide provides information for managing InfoVaultz v4.0 and above. Click on the following topics to learn more.

> ⚠ **Do not start this section without completing InfoVaultz installation and ensuring that Basic and Extended checks pass without any errors**

InfoVaultz Site Setup

InfoVaultz Site

Maintenance InfoVaultz

Troubleshooting InfoVaultz

Best Practices

Audience
This guide is intended for InfoVaultz Administrator

InfoVaultz Site Setup

Once InfoVaultz is installed successfully and started, Administrative tasks need to be performed to allow InfoVaultz users to log in and use InfoVaultz efficiently. InfoVaultz ships with most common settings as default.

Administrator should configure and enable each piece of functionality needed for a specific installation.

Refer to the following sections to setup your InfoVaultz site.

- Logging as Administrator
  - Logging In
  - Changing Admin Password
- Basic Server Settings
- Setting up InfoVaultz Managed Storage
- Setting up User Access
  - InfoVaultz User
  - InfoVaultz User Authentication
    - InfoVaultz Default
    - Authentication Active Directory
    - Authentication LDAP Based Authentication
  - Enable new account creation requests
    - Account Approval
  - Preload data for new accounts
- Creating User Groups Setting
- up Network Shares Setting up
- InfoVaultz Branding
  - Labels and Logos
  - UI Messages
  - Email Templates
  - News Feed
  - Terms of Service
  - Customize Product URLs
- Configuring Email Integration
- Enable Antivirus Scanning
- Enable WebDAV
- Setting up Document Preview

    - Ubuntu/Debian Instructions
    - Redhat/CentOS Instructions
    - Windows Instructions
- Enable File Change Notifications

Logging as Administrator

This section describes how an administrator can access InfoVaultz management user interface.

- Logging In
- Changing Admin Password

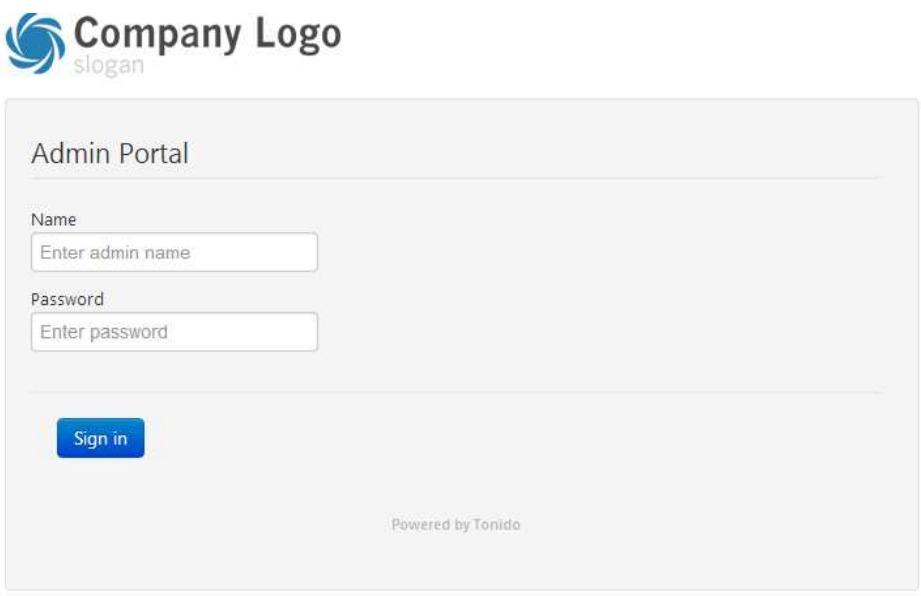
Logging In

After InfoVaultz is installed, you need to log in using your admin account to perform administrative tasks.

Administrator Web UI

In a supported web browser, open the following link depending on whether or not you are using SSL connection.

> **Admin URLs**
> **http://<your InfoVaultz address or IP>/ui/admin/index.html (or)**
> **https://<your InfoVaultz address or IP>/ui/admin/index.html**



Default Credentials

If the credentials were not changed during InfoVaultz install, admins can use the following information to login into admin UI.

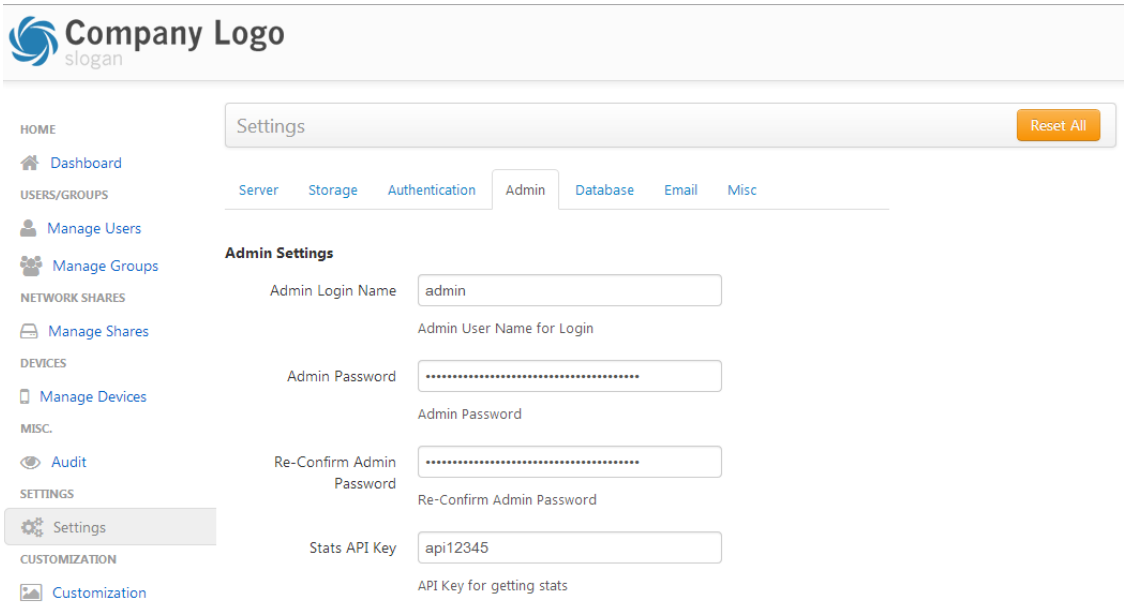
Field	Default
Name	*admin*
Password	*password*

Changing Admin Password

InfoVaultz Admin can change the Admin password using the Administration Portal. The steps are

1. Log into the Administration Panel
2. Select "Settings" in the left hand navigation menu

3. Select "Admin" tab
4. Set the Admin Password.



Basic Server Settings

This section explains the basic settings needed for every InfoVaultz

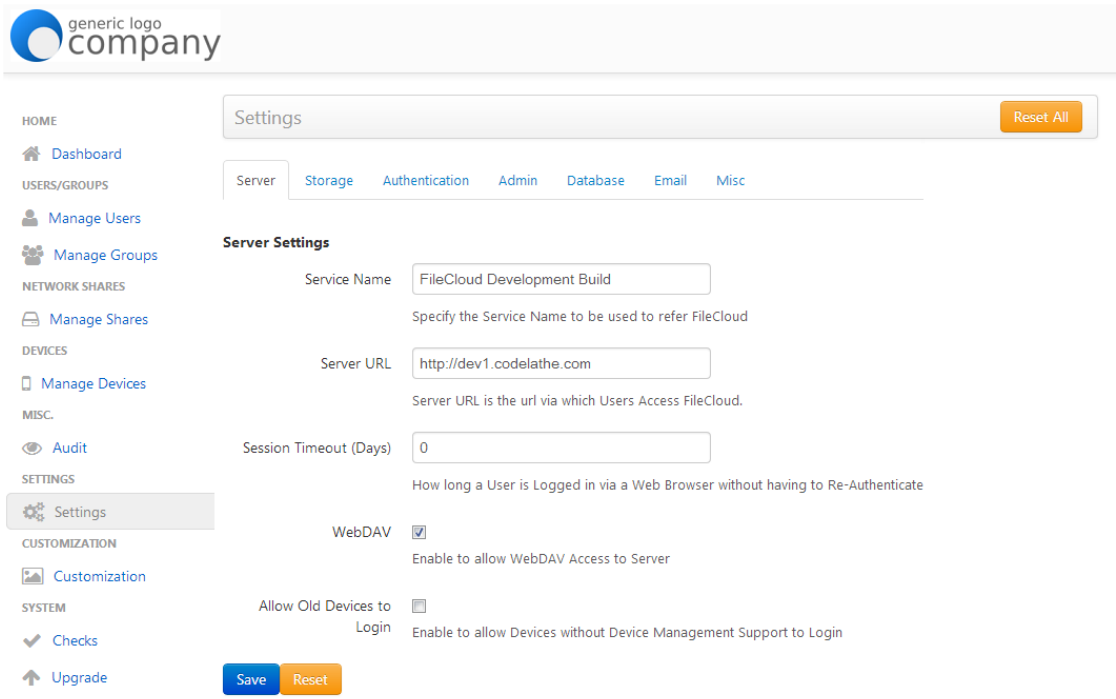
installation. The settings can be accessed by

1. Log into InfoVaultz Administration Portal
2. Click on **Settings** in the left navigation panel
3. Click on **Server** tab (The default view)
4. Change settings as needed
5. Click **Save**.

⚠ It is very important that the "**Server URL**" is a valid externally accessible URL. This URL will be used for creating shares

Settings Name	Description
Service Name	The name to be used when referring to your InfoVaultz service. This will be used in email messages etc
Server URL	This is your DNS entry registered with DNS service. example xyz.company.com . This is the URL by which users will access InfoVaultz service.
Session Timeout	The default value is 0. This means, everytime an user closes the browser and reopens, the login credentials will be needed to log back into the system. Alternatively, you can enter a number indicating the number of days the authentication is valid even if the browser window is restarted.

WebDAV	You can enable WebDAV support for your InfoVaultz installation. If you enable this function, users can mount their InfoVaultz home folders as a windows or mac or linux drives.
Allow Old Devices to Login	InfoVaultz supports Remote Client Management(RCM) of various clients. As of v4.5 onwards, All the InfoVaultz clients are RCM compliant. However, you can allow access using older InfoVaultz (non RCMcompliant) clients by enabling this setting.



Setting up InfoVaultz Managed Storage

InfoVaultz supports storing of user data in different types of storage devices. This type of InfoVaultz storage is called "Managed Storage".

Managed Storage

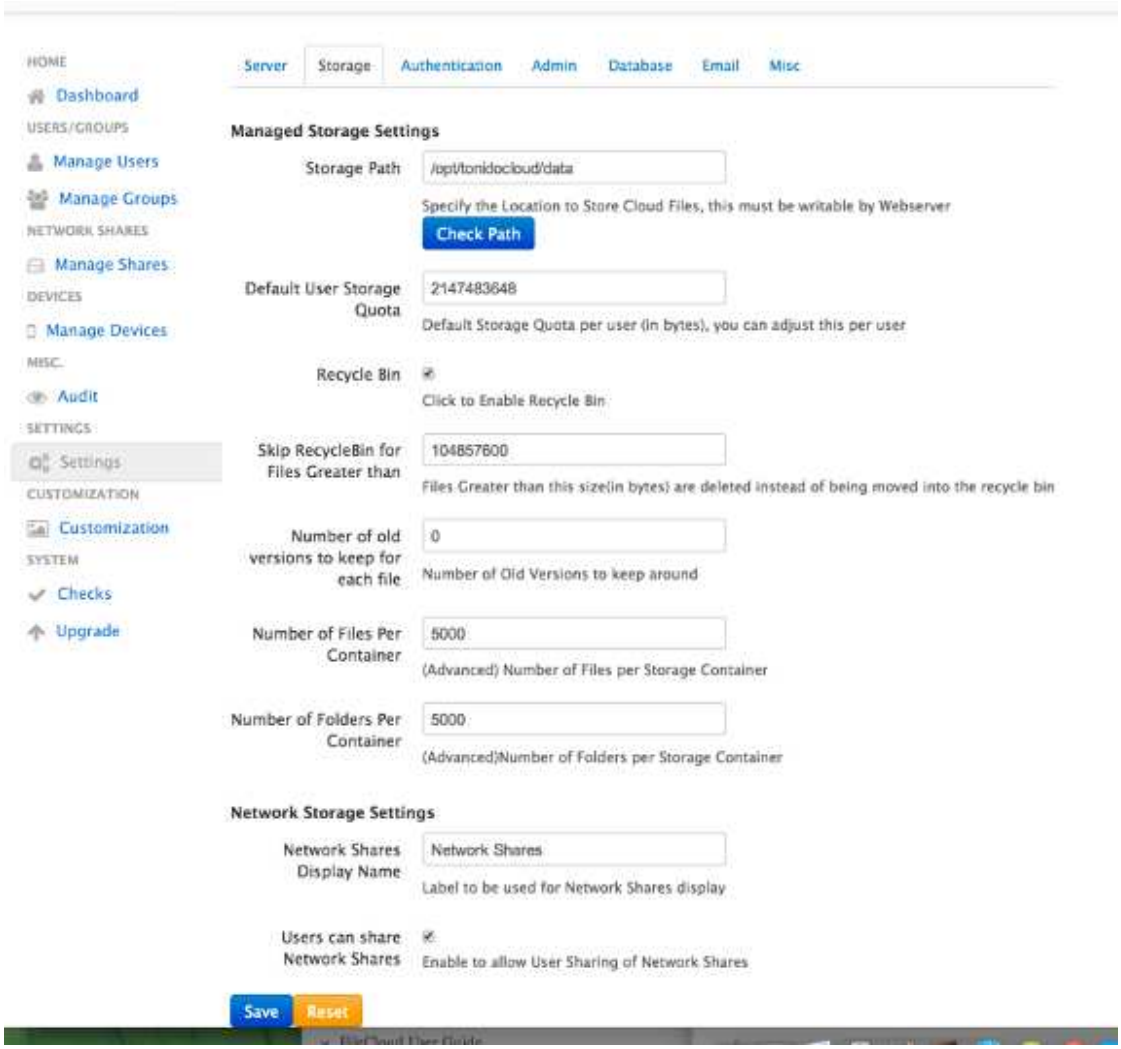
This is the default storage where the user files are stored in a filesystem that can accessed directly by InfoVaultz. The Managed Storage provides InfoVaultz complete control over the management of user content. The storage can be on filesystems on a local harddisk, SAN or NAS

The following steps should be followed to setup the Managed Storage

1. Log into the Administration portal
2. Click on "**Settings**" on the left hand navigation panel
3. Click on "**Storage**" tab and enter the appropriate information
4. Click Save

Setting	Description
Storage Path	This is the location where all the InfoVaultz data is to be stored. Be sure to allow enough options to expand storage in future

Default User Storage Quota	This is the storage quota that will be provided for every user of the InfoVaultz. Note that, this is only a "Quota" and does not require physical storage until the user actually consumes the space.
Recycle Bin	Enable this setting if you wish to provide "Recycle Bin" support to your users. When this option is enabled and user deletes a file/folder, the deleted item gets moved into his/her personal recycle bin. Then the user can restore files from recycle bin or empty recycle bin completely. **Note: Files in recycle bin count towards user's storage quota.**
Skip Recycle Bin for Files Greater than	Set this value in bytes. Any file larger than this setting will be permanently deleted instead of getting moved into recycle bin.
Number of old versions to keep for each file	If a file with the same path and name is uploaded, InfoVaultz versions the file. This setting determines number of recent versions that InfoVaultz should retain. To disable versioning completely, set the number of versions to 0. **NOTE: Versioned files count towards the user's storage quota.**
Number of Files Per Container	Internal setting. Please do not change unless recommended by InfoVaultz Engineers
Number of Folders Per Container	Internal setting. Please do not change unless recommended by InfoVaultz Engineers
Network Share Display Name	The label to be displayed to user when accessing a network share. Read more about Network shares.
Users can share Network Shares	Check this setting if you wish to allow users the ability to share files/folders from these Network shares with other users.



Setting up User Access

InfoVaultz allows users to store and use files. Every user of InfoVaultz needs an user account before he/she can store and/or consume files from InfoVaultz.
This section describes various ways user account(s) can be created and managed under InfoVaultz.

- InfoVaultz User
- InfoVaultz User Authentication
    - InfoVaultz Default
    - Authentication Active Directory
    - Authentication LDAP Based Authentication
- Enable new account creation requests
    - Account Approval
- Preload data for new accounts

InfoVaultz User

Introduction

Files stored in InfoVaultz are access restricted by means of user accounts. Every user who likes to use InfoVaultz storage needs an user account.

Creating User Accounts

A new InfoVaultz user can be :

1. Created using "Default Authentication", where the user credentials are stored and authenticated within InfoVaultz.
2. Imported using "LDAP or AD Authentication", where the user credentials are stored and authenticated from an external LDAP or AD server.

Creating or importing a user will count towards license.

- The default user storage quota for every new user is set in Managed Storage.
- An optional sample set of files can be preloaded for every user on creation.

User Access Levels

Once an user account is created, it can be assigned different access levels. There are three different access levels for an user account.

- **Admin Access**: An account with admin access level has complete control over the InfoVaultz system. This account will be used to manage the InfoVaultz server instance. In the current InfoVaultz version, there can be only one admin user account.
- **Full Access**: An account with full access level has its own private cloud storage space. These user accounts can store files in their own private cloud storage space, view/download files stored in their storage space and view/download files shared with them by other user accounts.
- **Guest Access**: An account with guest access level have restricted access to the InfoVaultz system. These user accounts do not have a private cloud storage. These user accounts can only view/download files shared to them by other user accounts.

Both Full and Guest users accounts are counted towards licensing units.

Comparison

User Access Feature	Guest Access	Full Access
Web UI Access	Permitted Not all functions available	Permitted Fully functional
Mobile App Access	Permitted Not all functions available	Permitted Fully functional
Personal storage in InfoVaultz	**Not Available**	Available
Share files with other users	Permitted	Permitted
View shared files	Permitted	Permitted
View Network Shares	Permitted	Permitted
Access storage using Cloud Drive	Permitted	Permitted
Sync storage using Cloud Sync	Permitted	Permitted

Checking User Access Level

The access level of any user account can be checked by the Administrator using the Administration Portal.

The steps are as follows:

1. Log on to Administration Portal

2. Click on "**Manage Users**" on the left hand navigation menu
3. In the "**Filter Users**", Enter the name or the email of user
4. The Access for the user will be listed in the "**Status**" column.

InfoVaultz User Authentication

InfoVaultz provides multiple ways of authenticating an user account. This is applicable for both full and guest user

accounts. InfoVaultz supports the following Authentication modes

- Default Authentication
- Active Directory based Authentication
- LDAP based Authentication

Passwords for LDAP user can only changed in the LDAP server

	Default Authentication	AD	LDAP
Authentication	Performed by InfoVaultz Server	In AD Server	In LDAP Server
Allowing Users to Create Accounts	Permitted	Not Permitted	Not Permitted
Bulk User creation	using CSV files	Import from AD group	Not Available
Can Admin Change Password	Password change for all users allowed	Passwords for AD user can only changed in the active directory.	Passwords for LDAP user can only be changed in LDAP server.
Can user change/reset password	Yes	Passwords for AD user can only changed in the active directory	Passwords for LDAP user can only be changed in LDAP server

Note

- An user account can have only single type of authentication mechanism.

This section describes these different authenticating methods.

- InfoVaultz Default
- Authentication Active Directory
- Authentication LDAP Based Authentication

InfoVaultz Default Authentication

Introduction

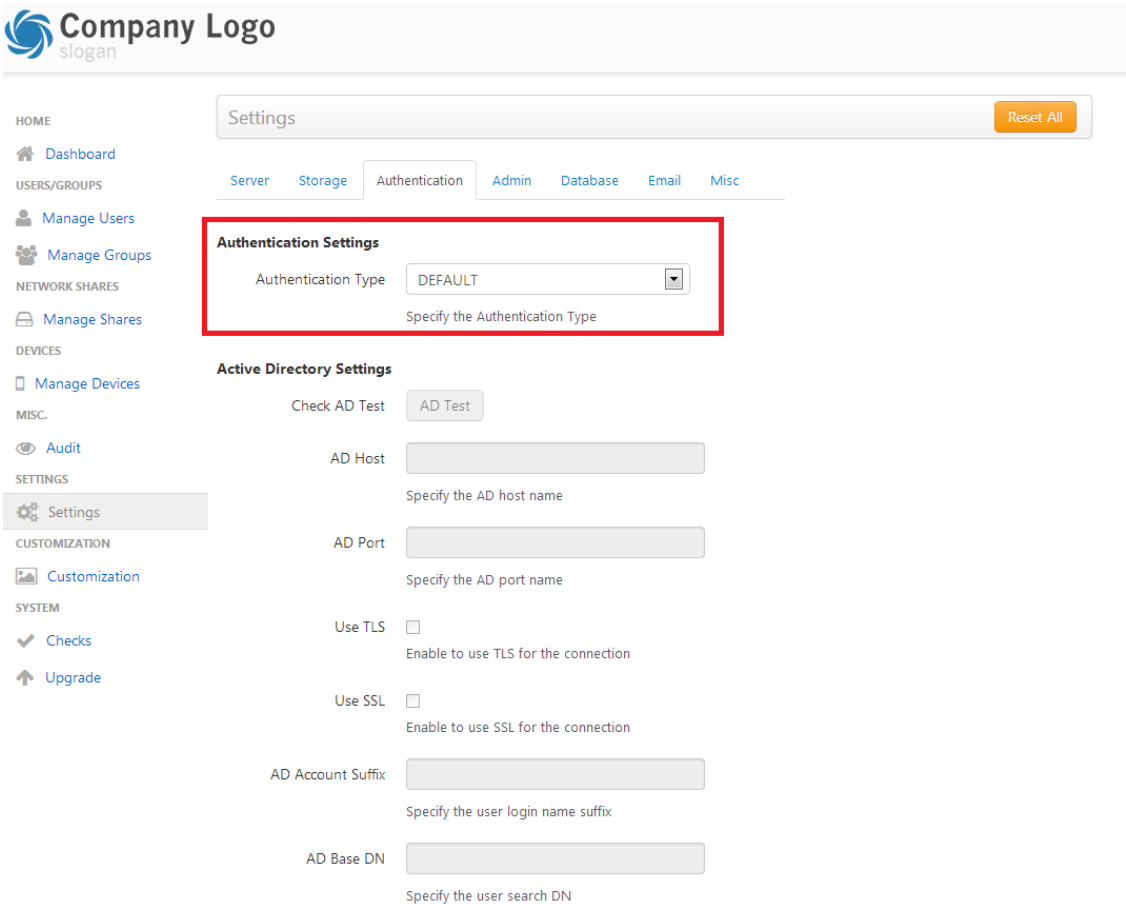
This is the default authentication of InfoVaultz. User accounts created with this authentication type will have their credentials stored and managed within InfoVaultz.
The user accounts with this type of authentication is also known as local users.

Prerequisites

As this authentication mechanism is fully managed by InfoVaultz, there are no prerequisites for this mechanism.

Enabling InfoVaultz Managed Authentication

1. Log into the InfoVaultz Administration Portal
2. Navigate to **Settings** in the left navigation panel
3. Click on **Authentication** tab
4. Under Authentication Settings, change the Authentication Type to "DEFAULT" using the dropdown box.
5. Administrator can either create new user or enable self creation of user accounts



Active Directory Authentication

Introduction

In this type of authentication mechanism, an user account is authenticated against an external Active Directory server. Accounts with this type of authentication are also known as external accounts.

Prerequisites

1. Active Directory service must be accessible from InfoVaultz (IP and Port must be accessible)
2. Active Directory must support Simple Authentication Method (Anonymous or Name/Password Authentication Mechanism of Simple Bind)
3. Active Directory users must have email attribute.
4. InfoVaultz version must be 4.0 or higher.

Note

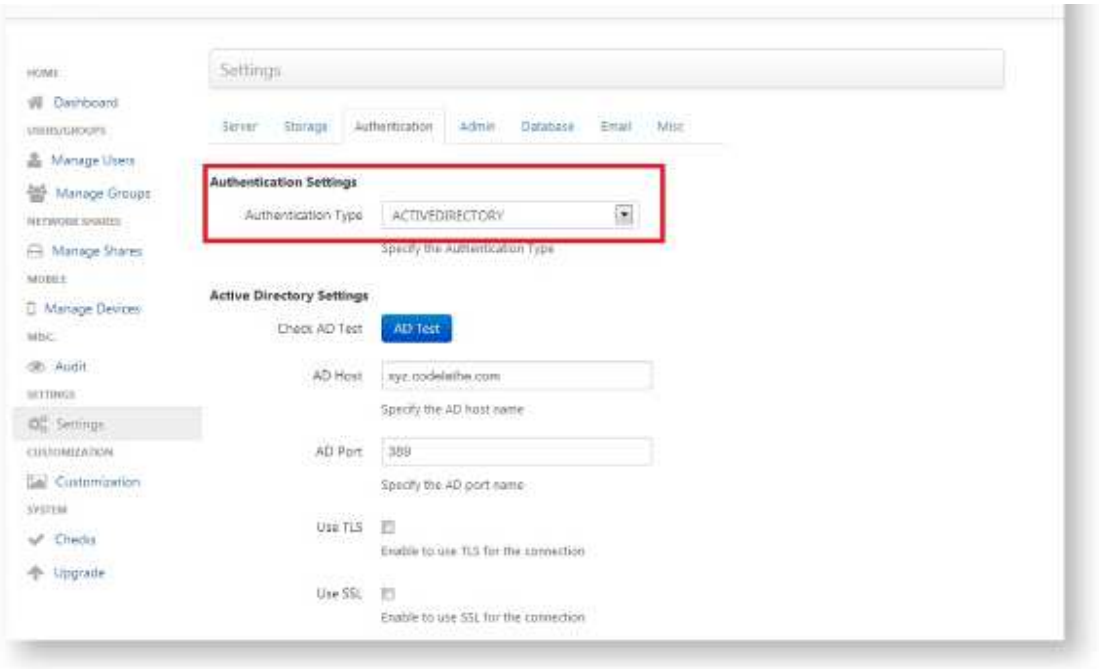
- If AD Authentication is enabled, then Automatic User creation cannot be enabled (i.e, All user creation should be done in AD

server).

- The AD user will count towards InfoVaultz License only after the user account logs into InfoVaultz. or if users of a AD group is explicitly imported by Admin.

Enabling AD Authentication in InfoVaultz

1. Log into the InfoVaultz Administration Portal
2. Click on **Settings** in the left navigation panel
3. Click on **Authentication** tab
4. Under Authentication Settings, change the Authentication Type to "ACTIVEDIRECTORY" using the dropdown box. This will enable the "Active Directory Settings" group.
5. Enter the following information and be sure to hit "Save" once all the settings are entered.



AD Configuration Parameters

Setting	Description
AD Host	This is the IP address or host name of the AD server.
AD Port	This is the port to be used to connect to AD server. The default is 389
Use TLS	Enable this checkbox if your AD server requires clients to use TLS to connect
Use SSL	Enable this checkbox if your AD server requires clients to use SSL to connect
AD Account Suffix	The full account suffix for your domain

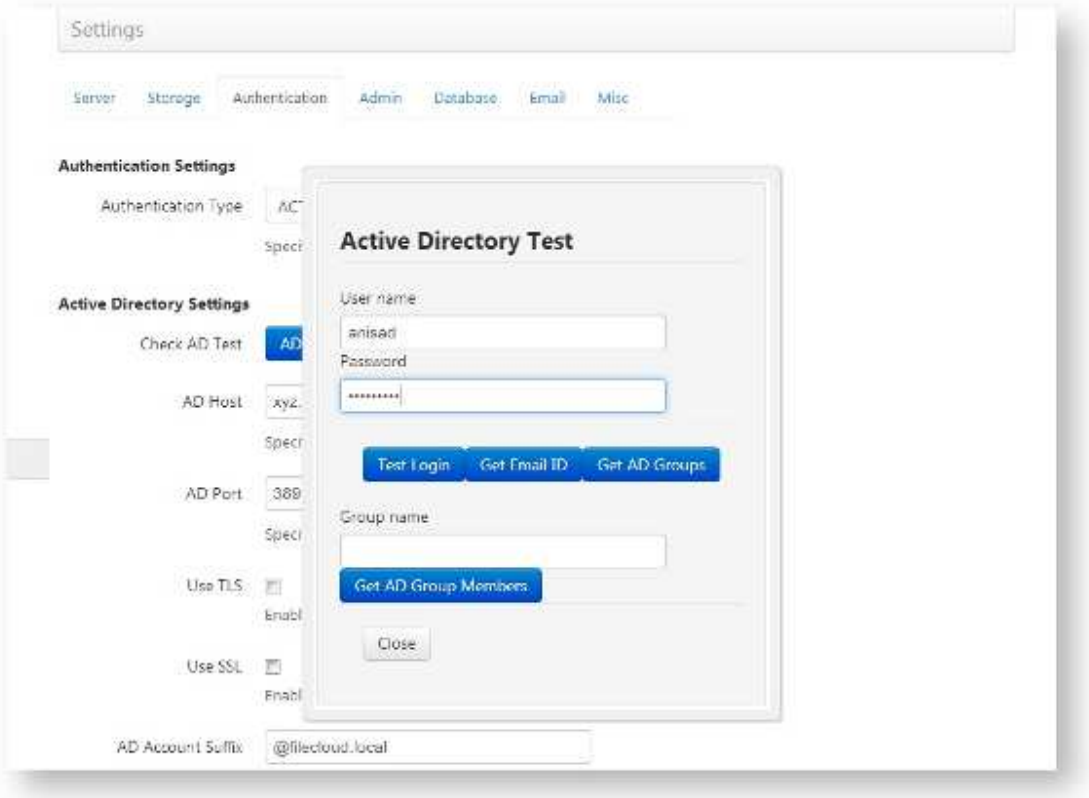
Base DN	The base dn for your domain. This is generally the same as your account suffix, but broken up and prefixed with DC=. Your base dn can be located in the extended attributes in Active Directory Users and Computers MMC. For example if your account suffix is @mydomain.local then your base DN is usually DC=mydomain,DC=local If you can authenticate users ok, but searching doesn't work, it's generally because you have specified an incorrect Base DN.
Mail Attribute	InfoVaultz requires use account to have an associated email id. Typically the name of this attribute in AD is "mail". If a user account has no mail attribute associated, then login will be disallowed
Limit Login to AD **Group**	If you want to limit the login to a specific AD group, specify the group members here (Typically this is left blank)
Use Admin Account **for Binding**	Enable this checkbox if your AD does not allow Anonymous Binding. Enabling this checkbox will enable the "AD Admin Account Name" and "AD Admin Account Password" text boxes
AD Admin Account **Name**	Provide the service account name to be used to bind with the AD server
AD Admin Account **Password**	Service account password to be used to bind with the AD server

Test AD Connectivity

Once all data is entered and saved, the AD settings can be validated using the AD Test button.

The following tests can be done.

1. Test if a specific AD user login/password (This will verify if the user will be able to login into InfoVaultz using the AD login/password)
2. Read email id associated with a specific AD user login
3. Get all groups that can be read by the InfoVaultz server
4. Get group members of a specific AD group
5. Enter a valid AD user name and password and try each of the function to verify AD connectivity.



LDAP Based Authentication

Introduction

In this type of authentication mechanism, an user account is authenticated against an external LDAP server. Accounts with this type of authentication are also known as external accounts.

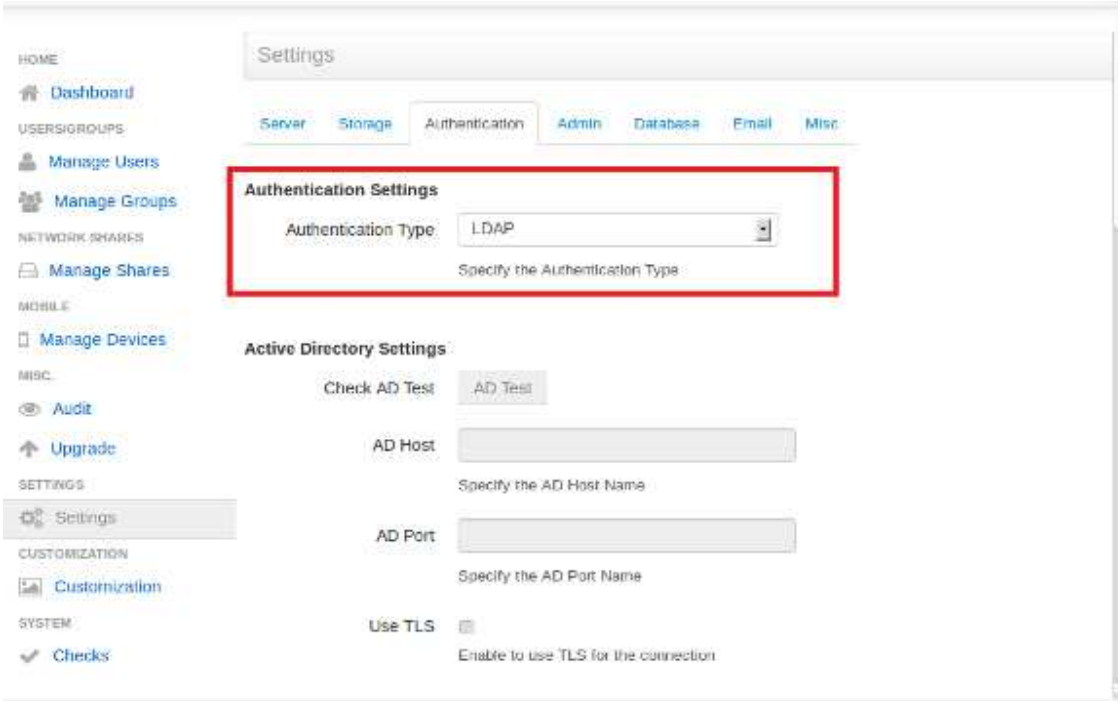
Prerequisites

1. LDAP service must be accessible from InfoVaultz (IP and Port must be accessible)
2. LDAP must support Simple Authentication Method (Anonymous or Name/Password Authentication Mechanism of Simple Bind)
3. LDAP users must have email attribute.
4. InfoVaultz version must be 4.0 or higher.

- If LDAP Authentication is enabled, then Automatic User creation cannot be enabled (i.e, All user creation should be done in LDAP server).
- The LDAP user will count towards InfoVaultz License only after the user account logs into InfoVaultz

Enabling LDAP Authentication in InfoVaultz

1. Log into the InfoVaultz Administration Portal
2. Click on **Settings** in the left navigation panel
3. Click on **Authentication** tab
4. Under Authentication Settings, change the Authentication Type to "LDAP" using the dropdown box. This will enable the "LDAP Settings" group.
5. Enter the required information and be sure to hit "Save" once all the settings are entered.



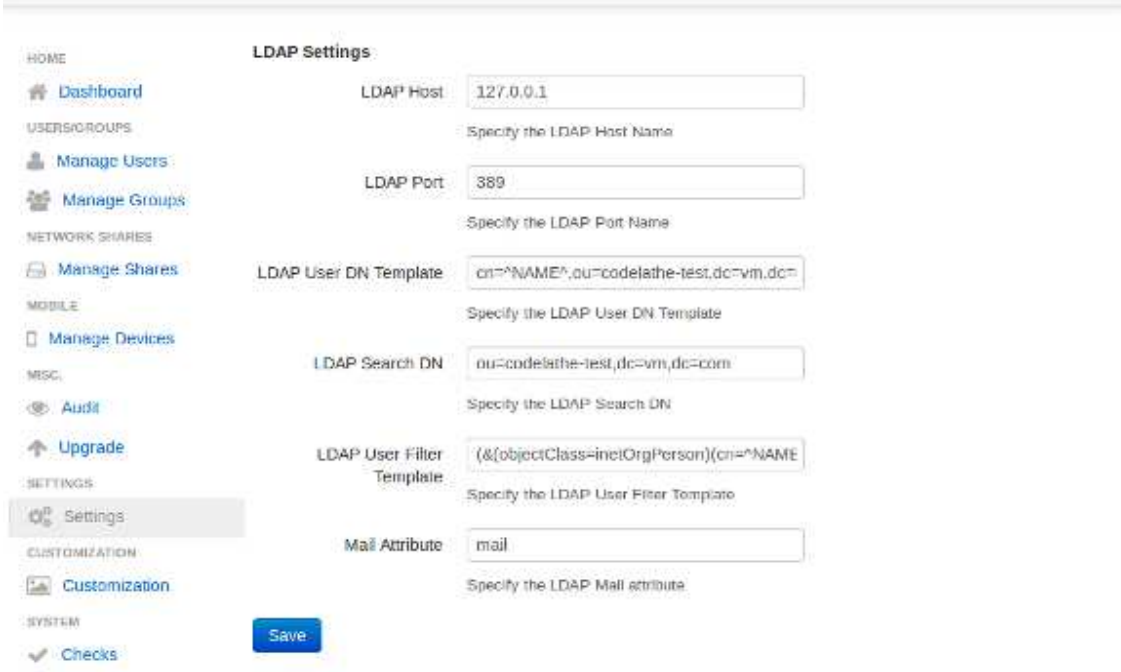
LDAP Settings

Setting	Description
LDAP Host	The hostname or IP address where the LDAP server is running
LDAP Port	The port to be used to connect to LDAP server (typically 389)

LDAP User DN Template	The LDAP Distinguished Name(DN) template. Every entry in the directory has a DN that uniquely identifies an entry in the directory.
	This is usually a combination of CN, OU , DC. Refer to your specific LDAP settings to uniquely identify an user.
	`Use the token ^USER^ in place of user name`
	`Example : cn=^USER^,ou=someorg,dc=company,dc=com`

LDAP Search DN	Enter the search DN (Specifies the set of resources to search for an user). If there is a ou encompassing all users, then the search DN would be pointing to that DN. For example, if all users are under "employees" ou, then the search DN would be ou=employees,dc=company,dc=com

LDAP User Filter Template	Entery the filter to be used to identify a user entry record from results. For example, if the object class is inetOrgPerson, then you would enter `(&(objectClass=inetOrgPerson)(cn=^NAME^))`
Mail Attribute	In InfoVaultz environment, Every user requires a email id . Enter the attribute name used in the LDAP's user record to refer to the email id.



Enable new account creation requests

Introduction

User accounts with InfoVaultz managed authentication mechanism can also created by user themselves.

> User created InfoVaultz access accounts are available only for DEFAULT Authentication mechanism. User cannot create accounts when the authentication mechanism is set to "ACTIVEDIRECTORY" or "LDAP".

Steps

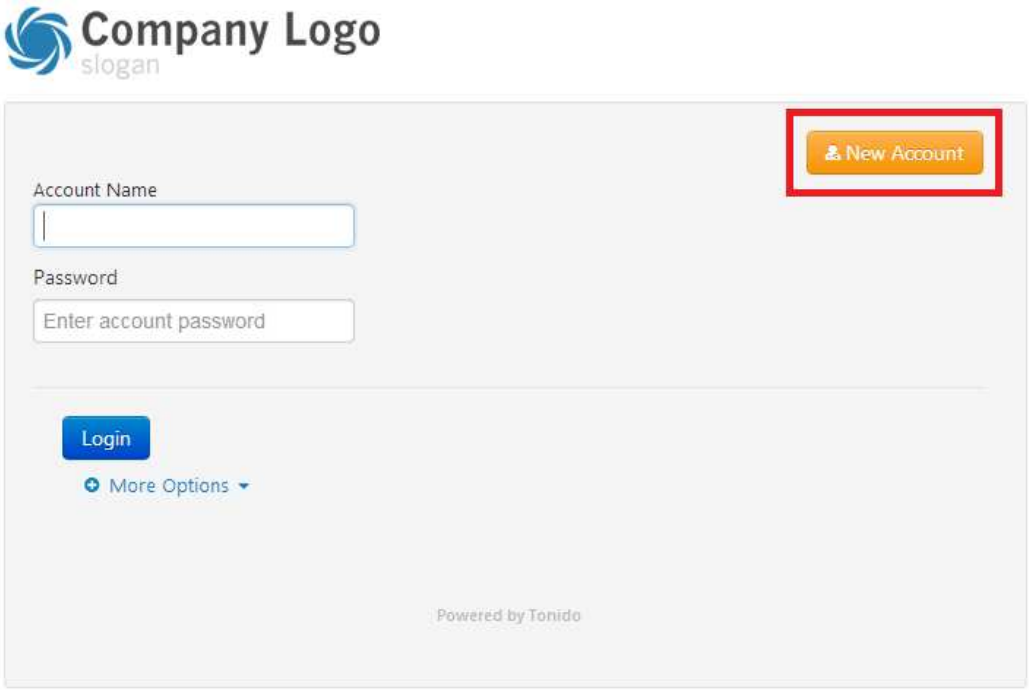
Here are the steps to create a new account by user:

1. User clicks on "New Account" button in user portal.
2. User enters details in the account creation fields.
3. If "Automatic Account Approval" setting is disabled,
    a. Admin will be notified of new account creation request.
    b. Admin will approve the account and will set the user account type to "Full User" or "Guest User".
4. User will receive account creation email to the mail id provided during account creation.
5. User is required to verify the email account to complete the account creation process

Administrator can control various aspects of this account creation process. These control points are discussed further.

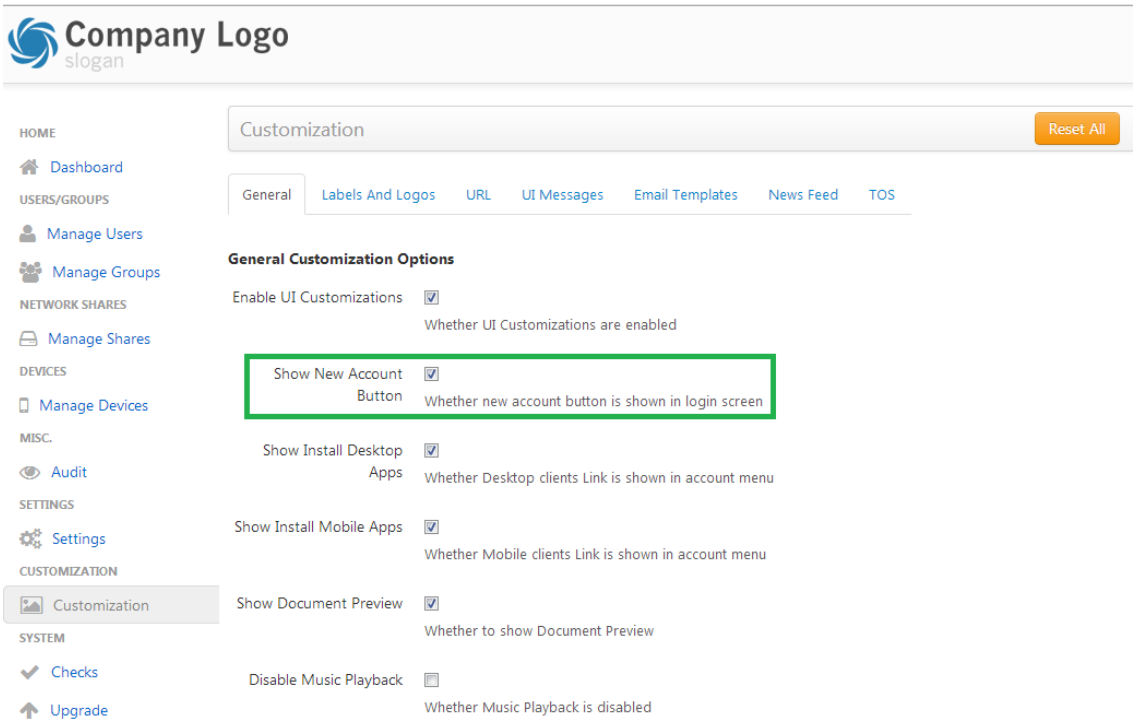
Controlling Step 1: Show/Hide "New Account" Button In User Portal

Administrator can choose to show or hide "New Account" button in user portal.



To do that, use the following steps:

1. Log into the Administration Portal
2. Navigate to "**Customization**" in the left navigation menu panel
3. In the "**General**" Tab, Check "**Show New Account Button**" to allow the "**New Account**" button to be displayed to the user login page.
4. Once the New account Creation is enabled, InfoVaultz server will display "New Account" button in user portal.



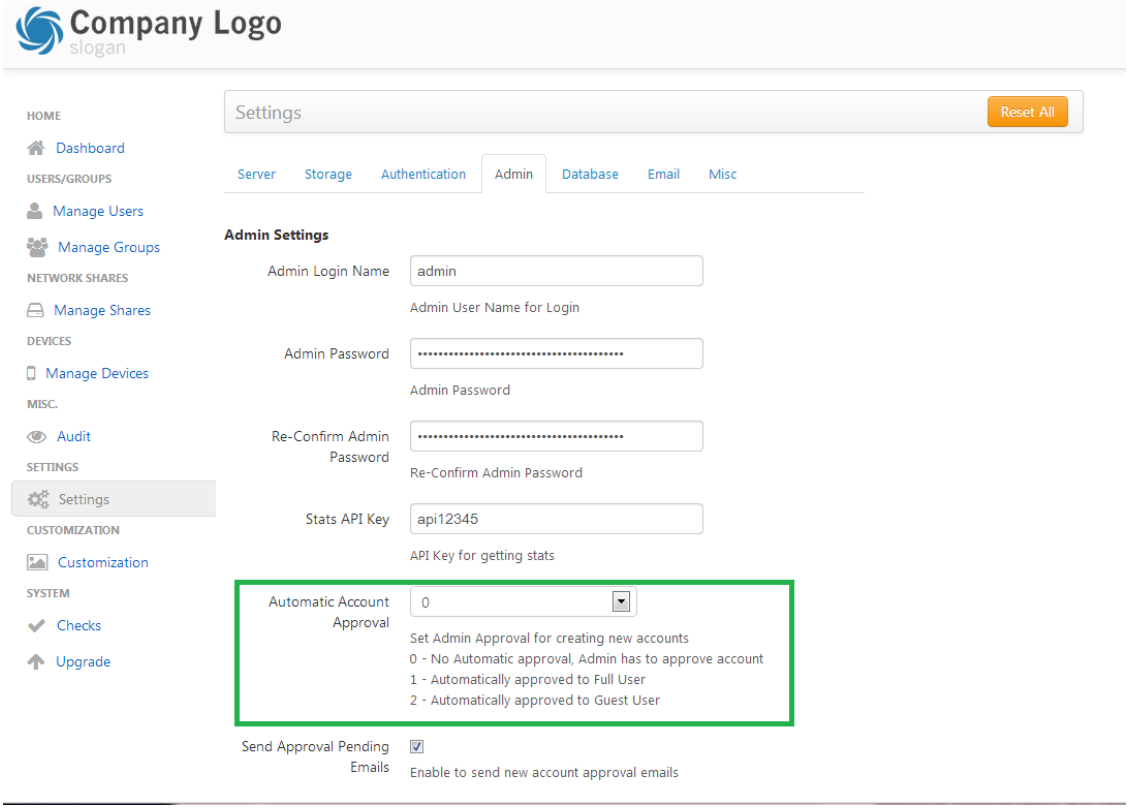
Controlling Step 3: Enable/Disable Automatic Account Approval

When an user account is created by the user, by default, the created account has to be approved by the administrator. For large organizations, this might not be optimal as admin intervention is needed for every account created.
One option is to enable automatic account approval.

Approval Code	Description
0 (default)	In this mode the account created will be DISABLED by default. It requires Admin approval to assign FULL or GUEST access to the account.
1	This mode allows the user to create account and automatically approve it to FULL access.
2	This mode allows the user to create account and automatically approve it to GUEST access. The access level can be changed to FULL at any later point in time.

Use the following steps to set the automatic approval mode:

1. Log into the Administration Portal
2. Navigate to Settings in the left navigation menu panel
3. Open the "Admin" Tab
4. Select the appropriate account approval mode in the "Automatic Account Approval" dropdown box.



Account Approval

Account Approval

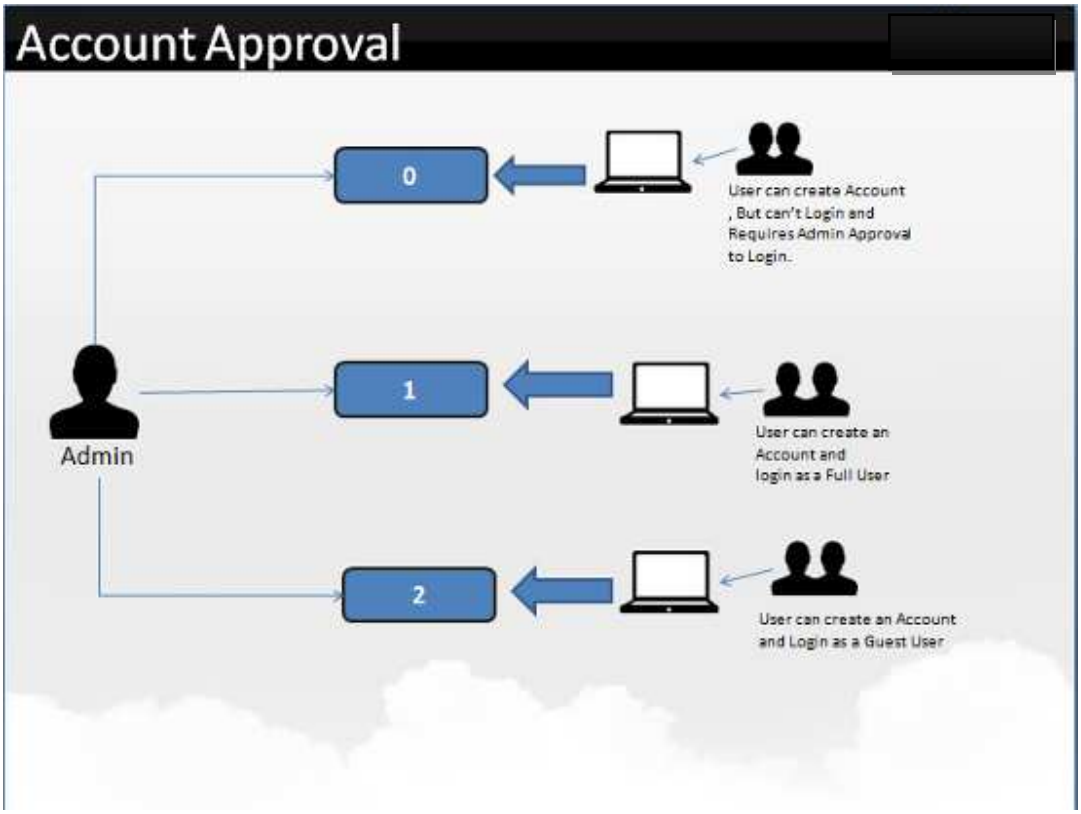
This feature is used to allow Automatic Account Creation by user on clicking the "New Account" button in user UI page.

The Admin can set this mode in the following 3 ways:

0 - In this mode the account can be created by the user but cannot Login . It requires Admin approval for the user to access the account.

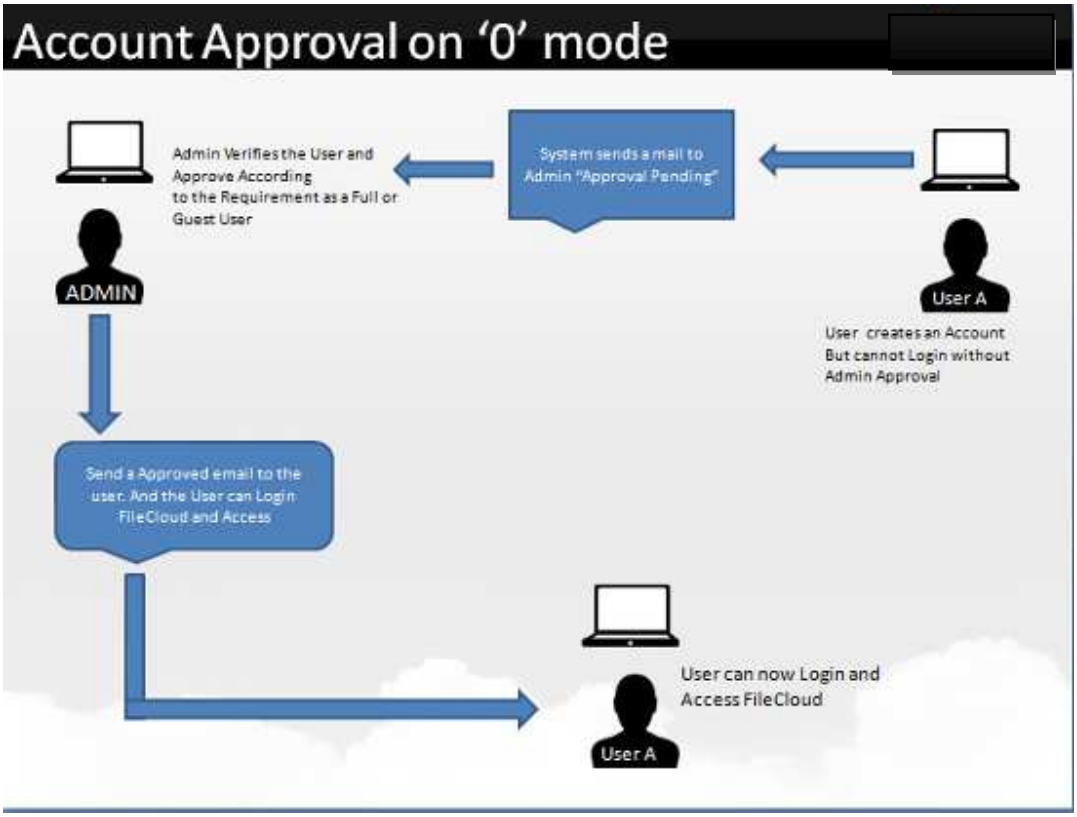
1 - This mode allows the user to Create Account and access InfoVaultz without waiting for Admin 's approval. This mode lets user create account in FULL USER Permission.

2 - This mode also allows the user to Create Account and access InfoVaultz without waiting for Admin 's approval. This mode lets user create account in GUEST USER Permission only. Later If the Admin wants the user to have Full User Permission It can be managed by the Admin.



Account Approval on mode '0'

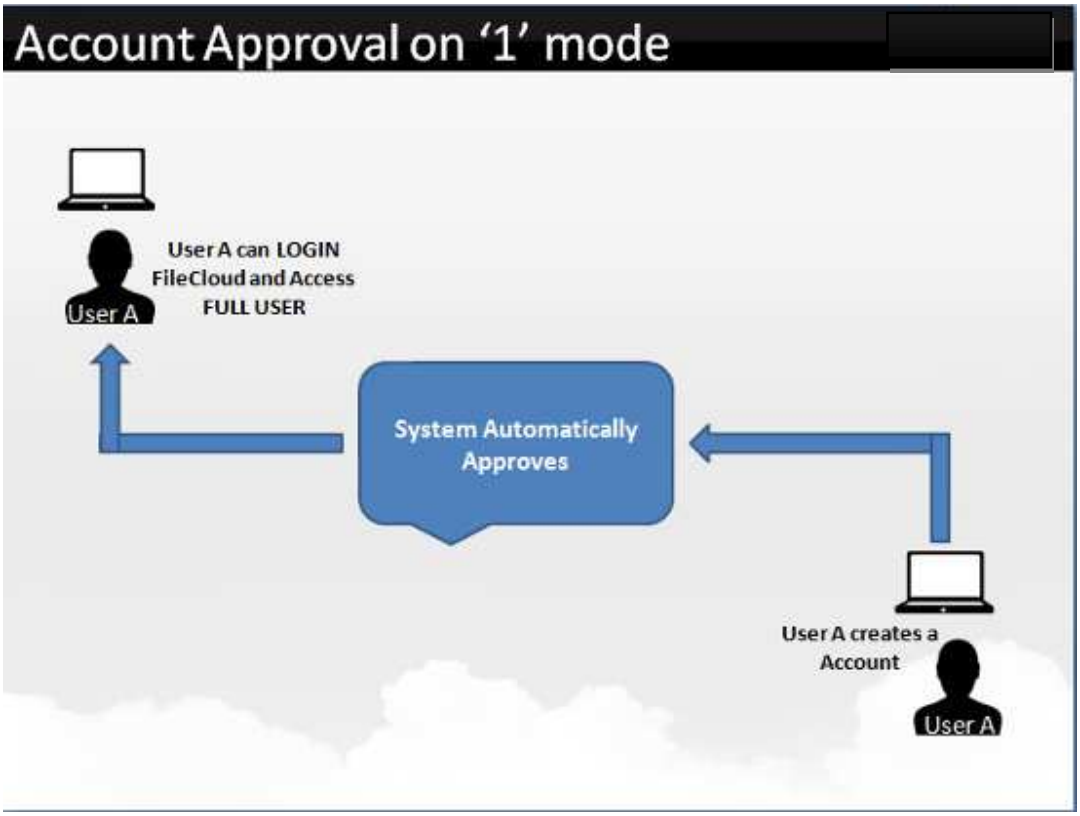
In this mode the user can Create an Account to access InfoVaultz but cannot Login . To Login it requires Admin's approval, so the system sends a Approval Pending Email to the Admin. Once Admin approves the user and sets the required Permission like Full User or Guest User. The user receives a email of Approval , and can Login and access InfoVaultz.



Account Approval on mode '1'

In this mode, user can Create Account and can access InfoVaultz. User does not need to wait for approval. The system automatically approves and allows Login.

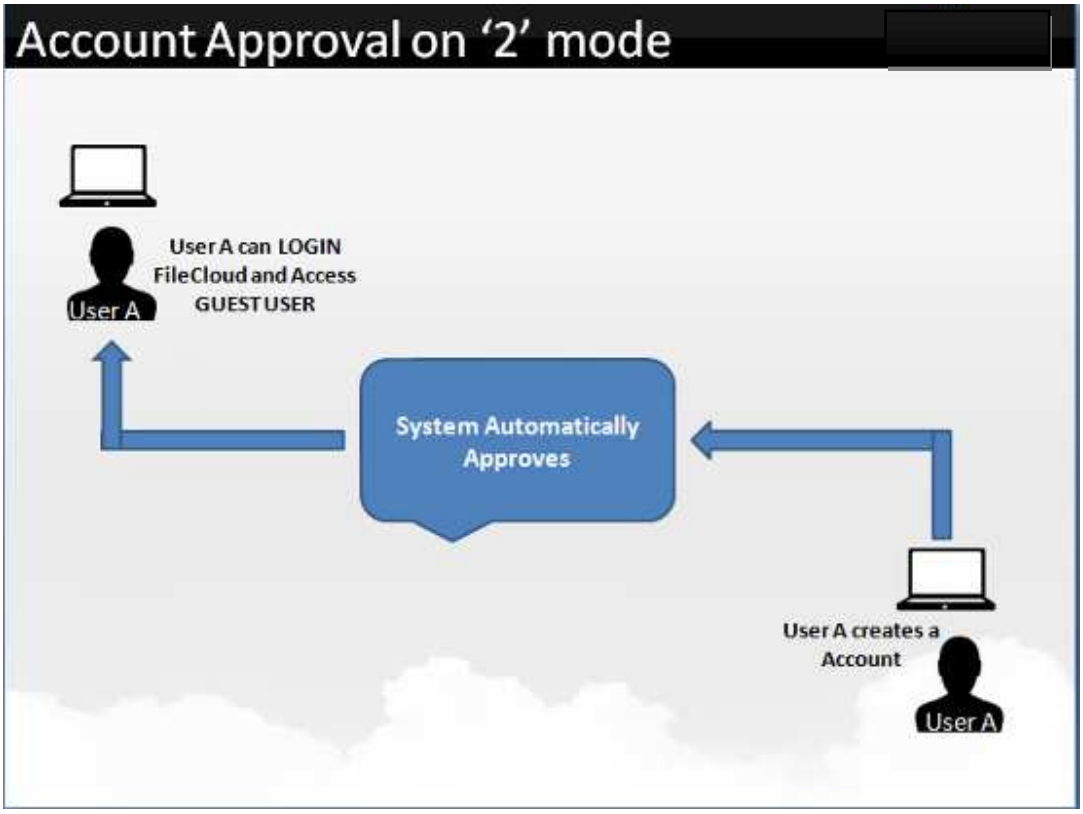
User is logged in the System as FULL USER in this mode.



Account Approval on mode '2'

In this mode, user can Create Account and can access InfoVaultz. User does not need to wait for approval. The system automatically approves and allows Login.

User is logged in the system as GUEST USER in this mode. To know more about Guest User check **User Access** page.



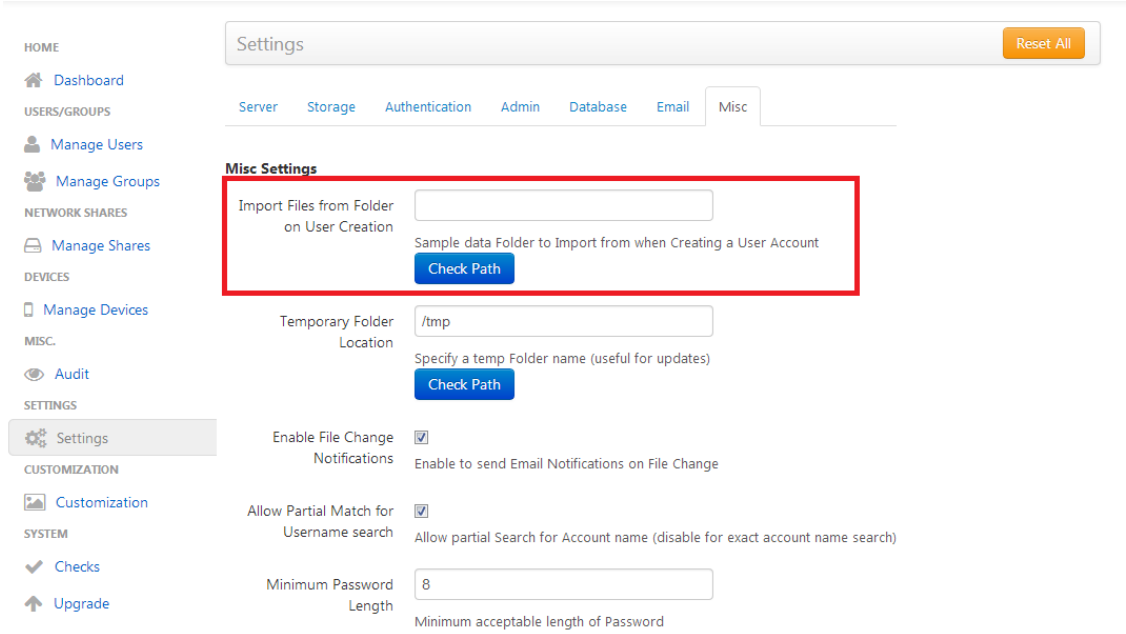
Preload data for new accounts

It is possible to preload user account with a set of sample data folder

Setup sample data folder when creating user account

This can be done using the following steps

1. Log on to Administration Portal
2. Click on "**Settings**" in the left navigation panel
3. Click on "**Misc**" tab
4. User "Misc" Settings, Enter the path containing the folder to preload in "**Import Files from Folder on User Creation**"
5. Click **Save**



Creating User Groups

InfoVaultz allows you to create groups of users. Creating groups allows setting network shares access and sharing of files and folders

> ⚠ An automatic group called "EVERYONE" is created by default for every InfoVaultz installation. This is a special group that contains all active users in the InfoVaultz system.
>
> Be sure to set a valid email address for the group in the group details OR delete the group if "EVERYONE" is not needed)

Group attributes

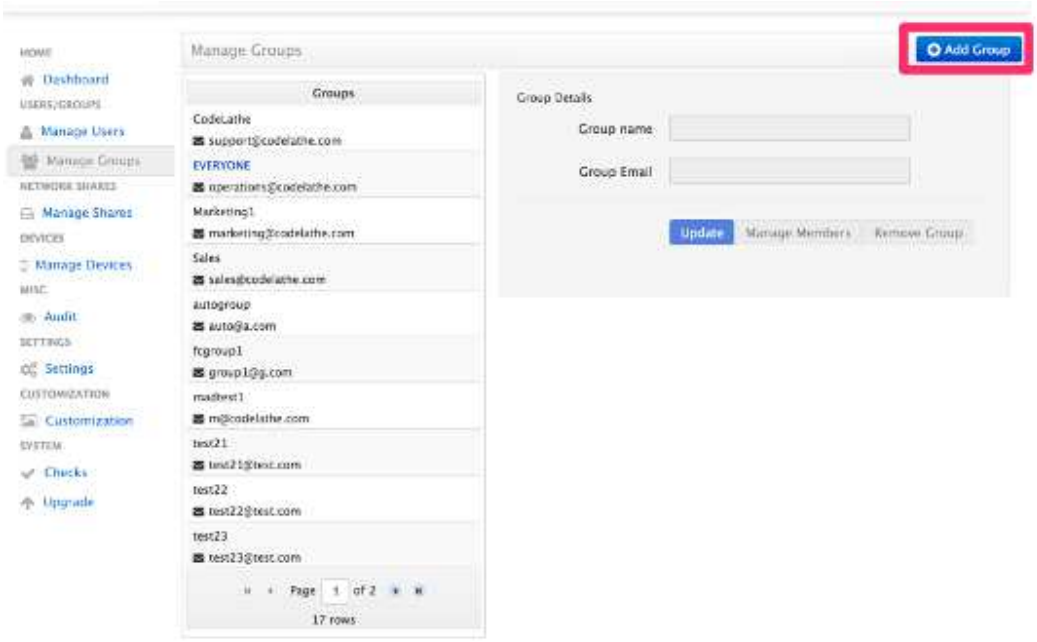
Every group contains the following attributes

1. **Group Name** - Name assigned by the Administrator
2. **Group Members** - List of users that are part of the group
3. **Group Email** - Email address associated with the group

Creating new group

A InfoVaultz group can be created using the following steps

1. Log on the Administration Panel
2. Click on "**Manage Groups**" on the left hand control Panel
3. Click on "**Add Group**" tab
4. Enter the name of the group and a unique email associated with the group



Adding users to group

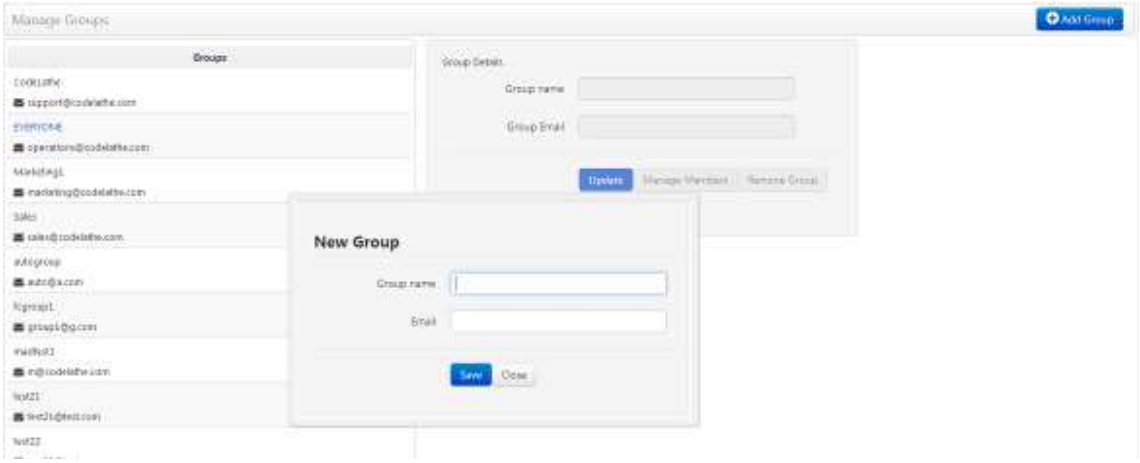
Once a group is created, they can be populated with users using one of the two methods

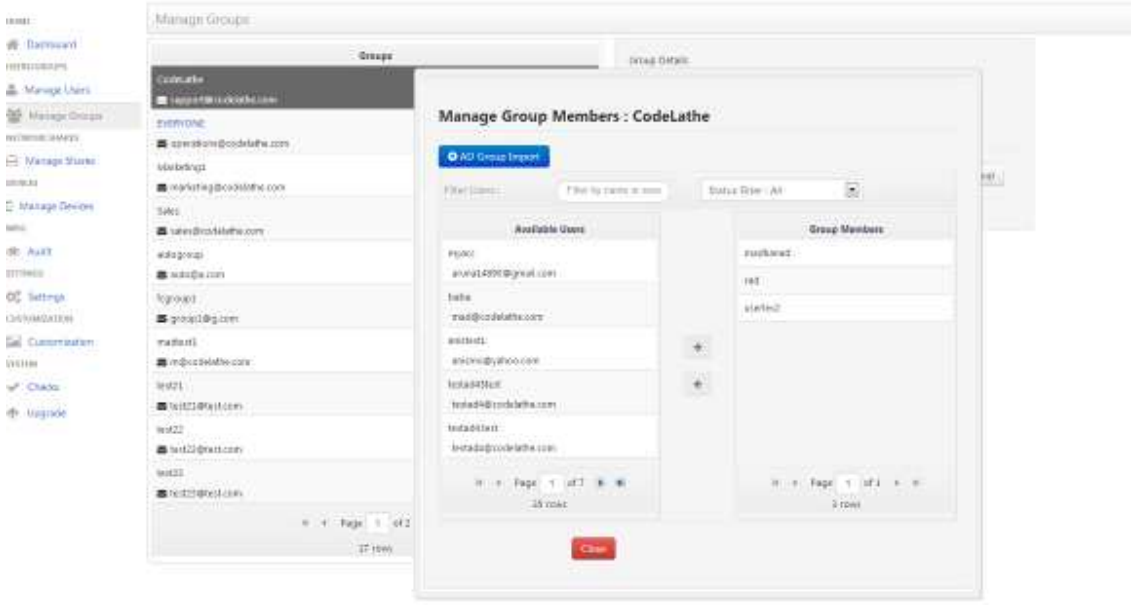
1. Manually adding users that are already in the InfoVaultz system.
2. Importing members of a group from an external AD server.

Adding users already in local InfoVaultz system

Admin can add existing InfoVaultz users into a InfoVaultz group using the following steps:

1. In the Administration Panel, select "**Manage Groups**" in the left navigation panel
2. Select the group to add users
3. Click on "**Manage Members**"
4. Select the users to add from "**Available Users**" and move it to the "**Group members**" view.

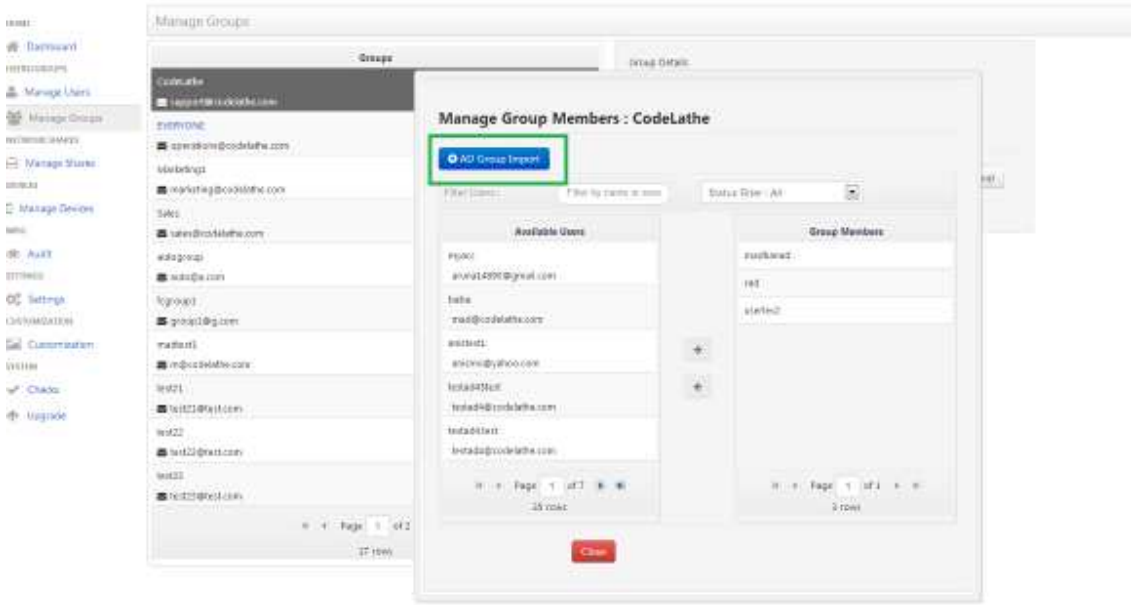


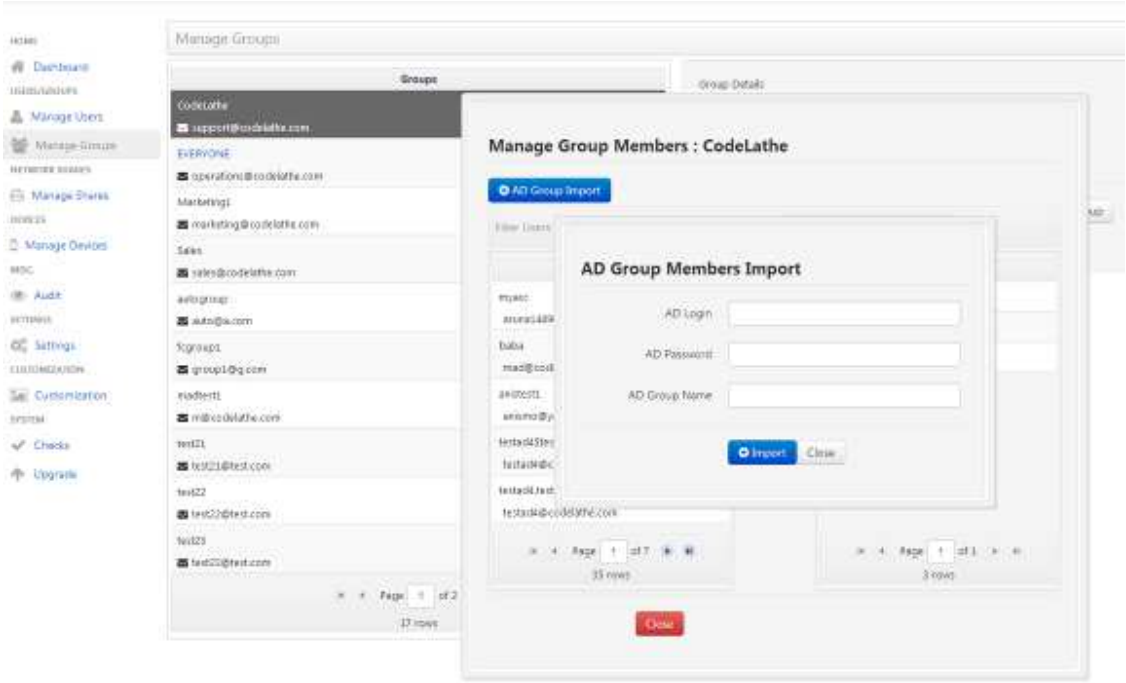


Importing members from external Active Directory server

Admin can also import users from an Active Directory into a InfoVaultz group using the following steps:

1. Setup and Verify Active Directory Settings
2. Select "**Manage Groups**" in the left navigation panel
3. Select the group to import members
4. Click on "**Manage Members**"
5. Click on "**AD Group Import**"
6. Enter "**AD Login**", "**AD Password**", "**AD Group Name**" information
7. Click "**Import**" to import the members of the AD Group.





Setting up Network Shares

Network Shares in InfoVaultz are special entities that allows the InfoVaultz users to access pre-existing (Legacy) files on your corporate windows, linux servers.

It can be viewed as a pointer to an existing folder in the system that runs InfoVaultz.

Network share location should have write permissions for the userid used by InfoVaultz server

The Network shares have special restrictions

Operation	Allowed (Y/N)
Sync	N
Share	Y
Mount as Drive	Y
Copy from/to Managed Storage	N
Move from/to Managed Storage	N

When a Network share is given user access permission, it will show up in the "Network Shares" folder when the user logs into the InfoVaultz server.

The label "**Network Shares**" can be customized by the administrator in Managed Storage Configuration panel.

Administrator can also control if a network shared folder can be shared by InfoVaultz user in Managed Storage Configuration panel.

Setting up a Network Share

This refers the action of configuring a existing folder in the filesystem of InfoVaultz server and adding user permission for access. The steps are

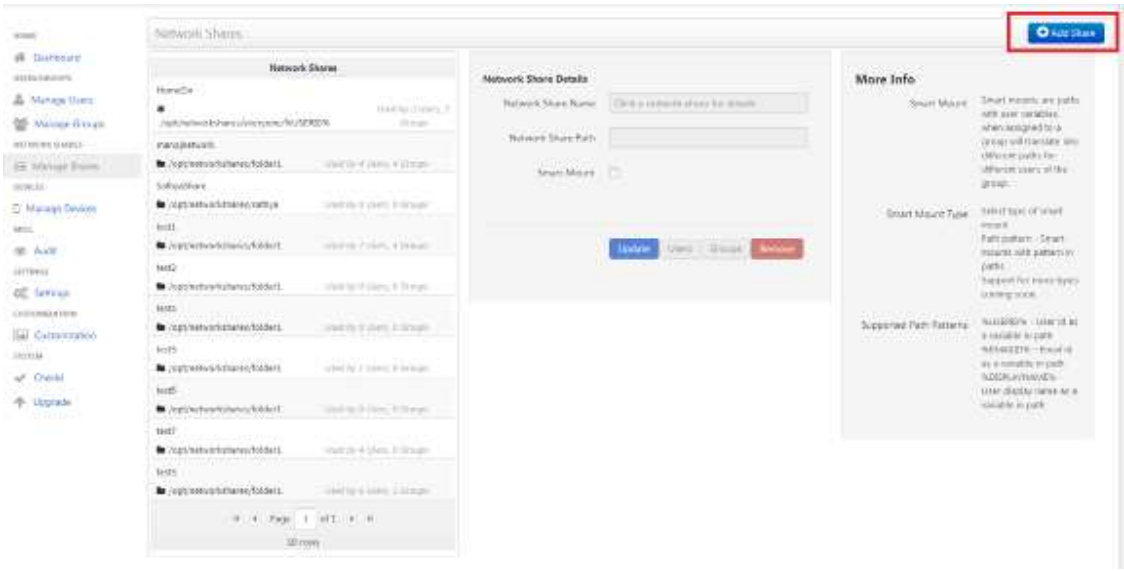
1. Creating a network share
2. Granting access to a network share

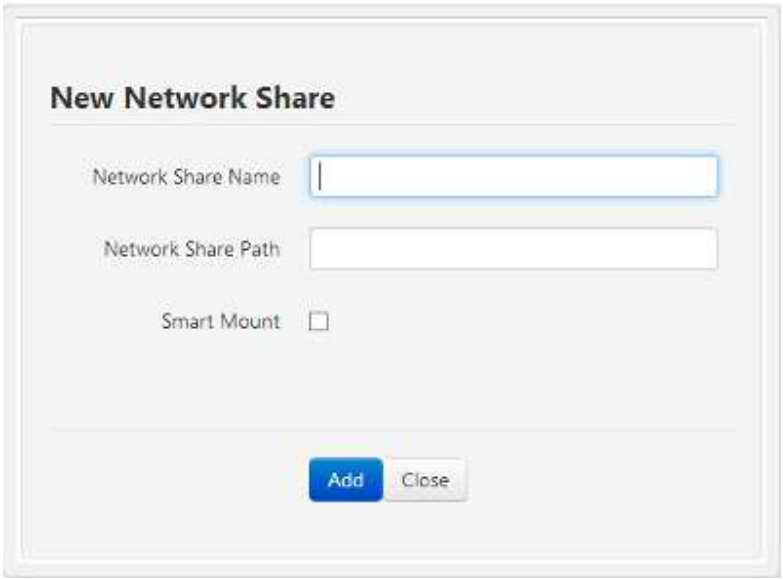
Creating a Network Share

To create a network share, the steps are

1. Login to the Administration Portal
2. Navigate to "**Manage Shares**" in left navigation panel
3. Click on "**Add Share**" Button to launch the "New Network Share" dialog box
4. Enter the required information
5. Click on "**Add**" Button

Field	Description
Network Share Name	This will be the name shown to the user to access this network share resource. For example, "TrainingMaterial". This can have only alpha numeric characters (no spaces etc)
Network Share Path	This is the actual path in the filesystem to mount
Smart Mount	Read more .





Granting access to a Network Share (non Smart Mount)

Once the share is created, the next step is to add access to the share.

For setting up permissions for "Smart Mount" Network Share, please read this section.

The network share access can be granted to

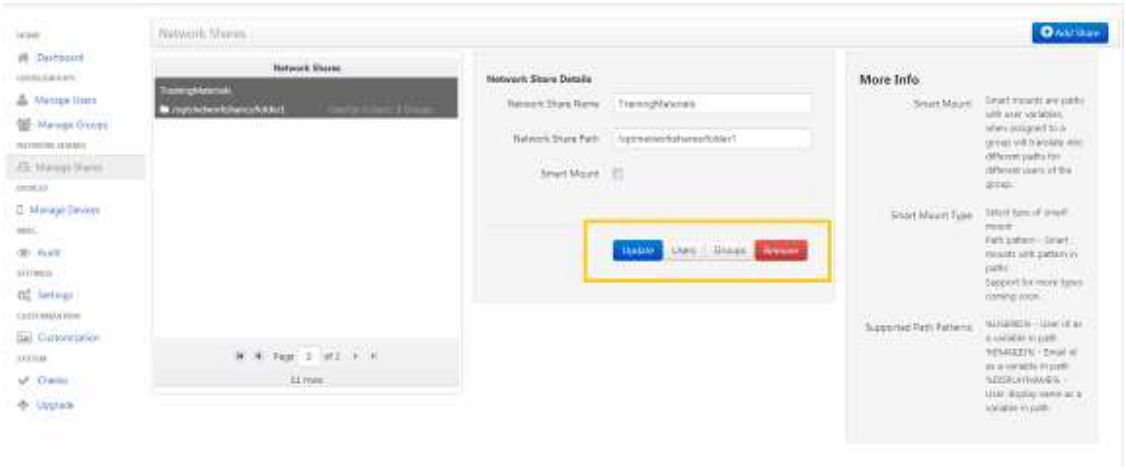
1. Guest User
2. Full Access User
3. User Group

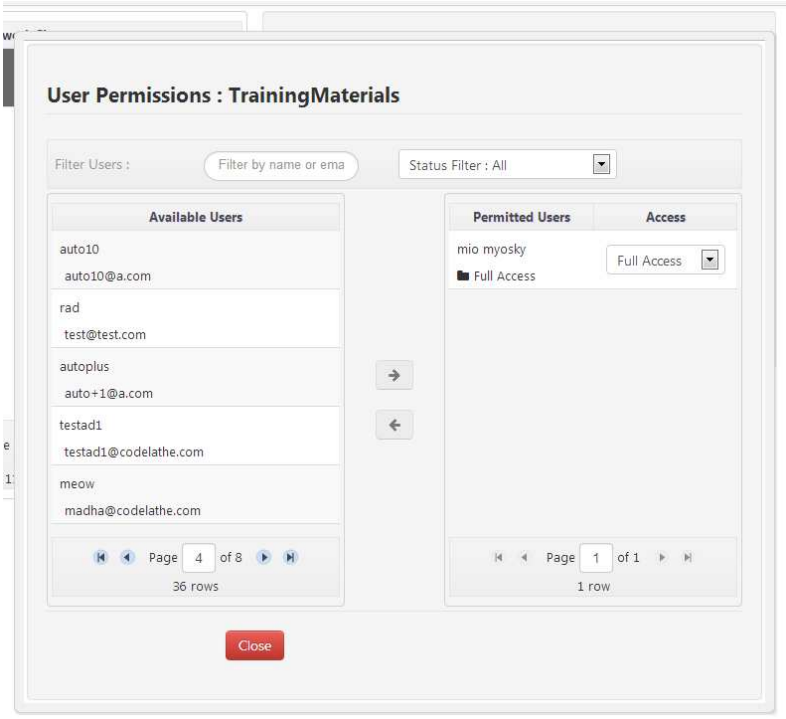
To grant access to a share, the following steps should be performed

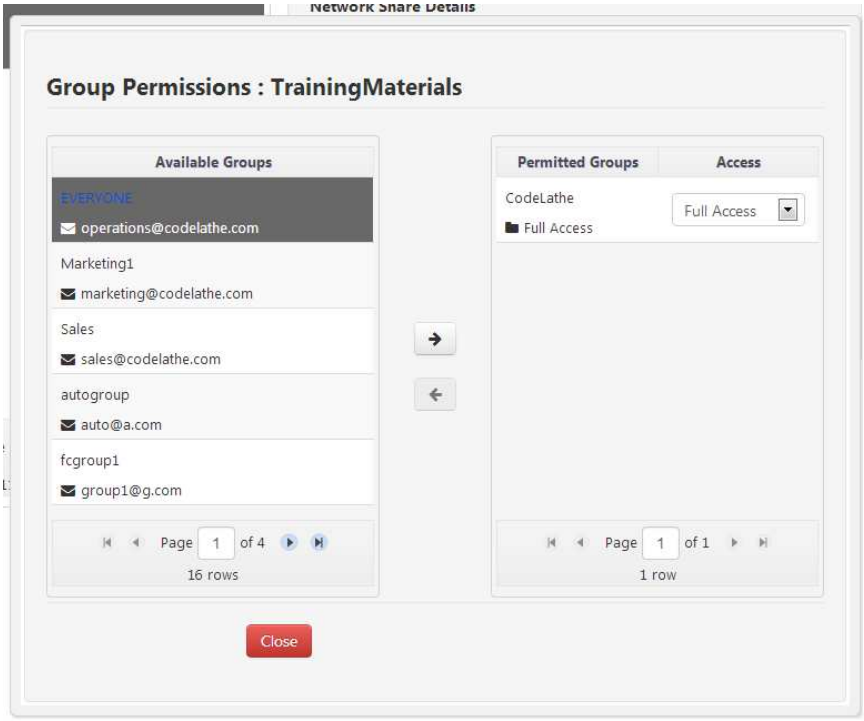
1. Click on "Manage Share" in the left navigation menu to display the list of available network shares
2. Select the network share entry to add the user or group access
3. Click on "Users" or "Groups" in the Network Share Details panel
4. Set the appropriate Access level

The Access level for a user or group can be

Access	Description
Full Access	This allows the user to read, write and share the contents of the share
Read Access	The user can only read (no write and share) the Network share contents.



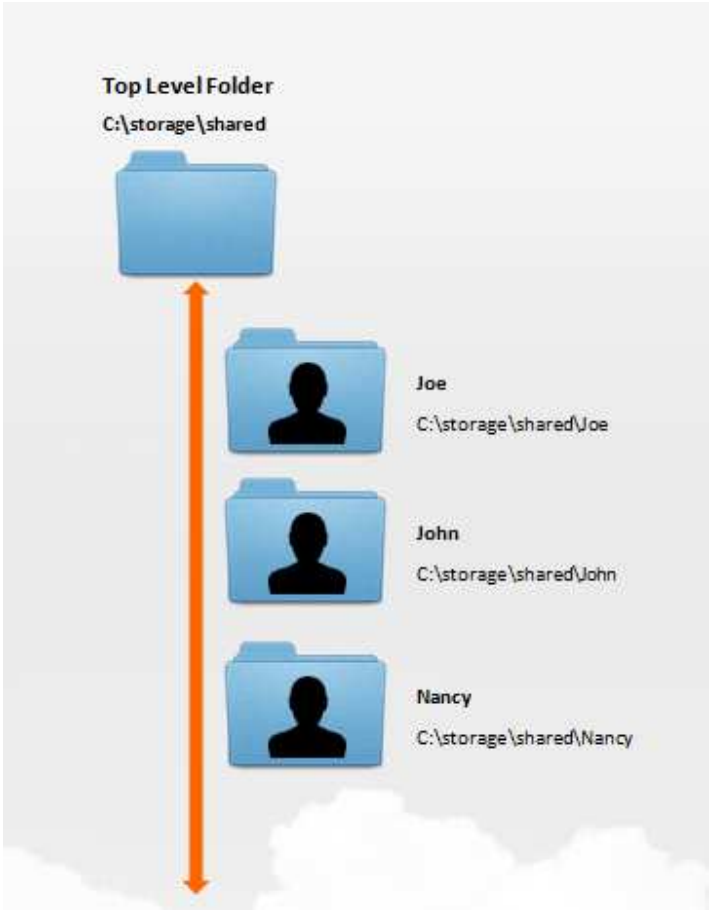




Smart Mounts

Smart mounts are special type of Network share whose file system paths contain variables. The variables will be translated to get to the actual filesystem path. This will greatly simplify setting access to a network share as long as certain criteria is met.

For example, take a look at the following image showing a folder structure in the filesystem



In the folder structure shown in the image above, the Administrator can setup the Network share in such a way that when user "joe" logs in, he will be able to see c:\storate\share\Joe folder and no other folder and when user Nancy logs into InfoVaultz, she will only be able to see and access C:\storage\shared\Nancy folder.

So the "Smart" mount path will look something like C:\storage\shares\%USERID% . The system will automatically replace the "%USERID% variable with the actual user name and mount it to the Network Share for the user to access.

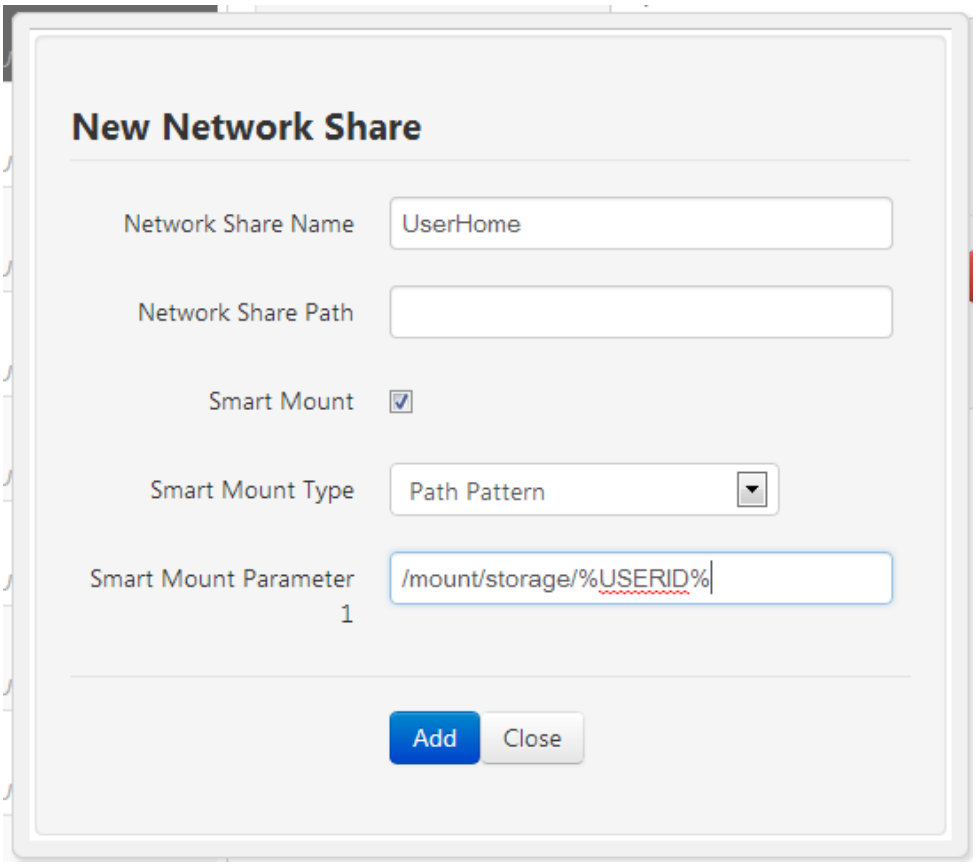
The following special tokens can be inserted in the smart mount parameter

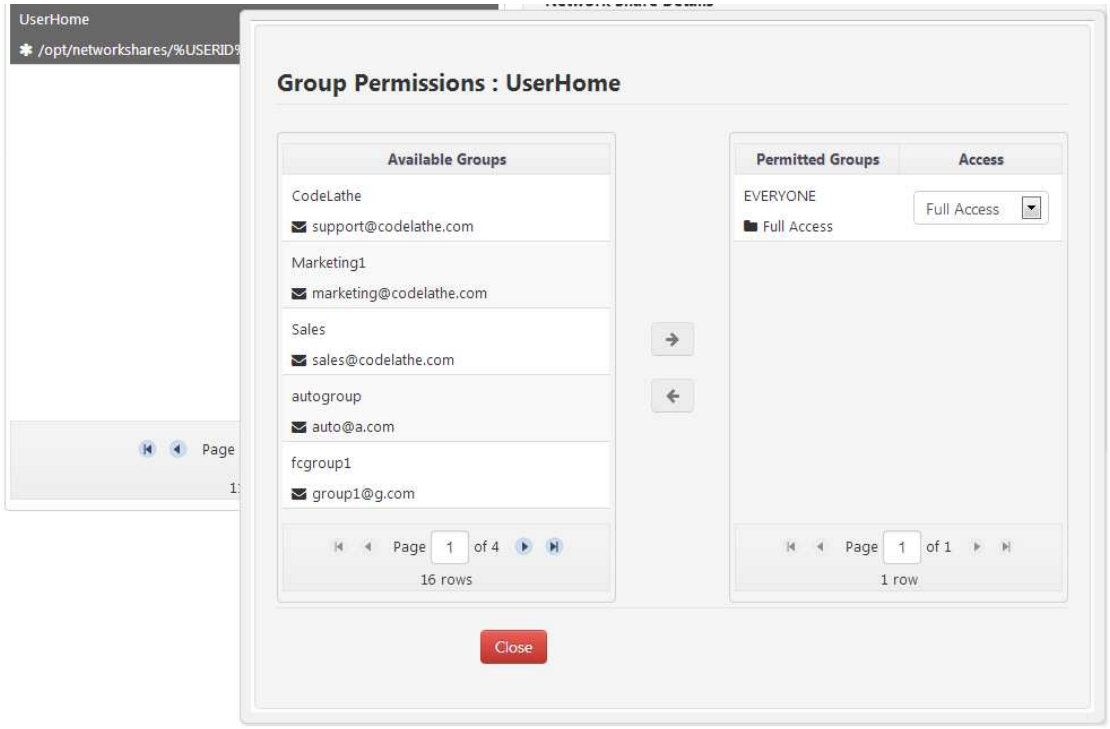
PATH PATTERN SPECIAL VARIABLES	NOTES
%USERID%	User id as a variable in path
%EMAILID%	Email id as a variable in path
%DISPLAYNAME%	User display name as a variable in path

To create a smart mount network share, the steps are

1. Navigate to "**Manage Shares**" in the Administration panel and Click on the "**Add Share**" button
2. In the "**New Network Share**" dialog, enter the Network Share Name and select the "**Smart Mount**" checkbox. IGNORE THE "**Network Share Path**" textbox
3. Set the "**Smart Mount Type**" to "Path Pattern" using the dropdown box
4. Enter the "Smart Mount" path in the "**Smart Mount Parameter**" text box
5. Click "**Add**" to create the smart mount
6. Select the newly created smart mount entry and assign access by clicking "Users" or "Groups" in the Network Share Details

> If you want to assign this to all users in the system, simply assign it to the EVERYONE group. The EVERYONE group is a special group which has all the members in the InfoVaultz system





Setting up InfoVaultz Branding

InfoVaultz provides facilities to customize the branding of InfoVaultz service. The following items can be customized in InfoVaultz using the Admin Portal

- Labels and Logos
- UI Messages
- Email Templates
- News Feed
- Terms of Service
- Customize Product URLs

Labels and Logos

InfoVaultz supports customization of company logo.

The following Labels and Logos can be customized	
Type	**Description**

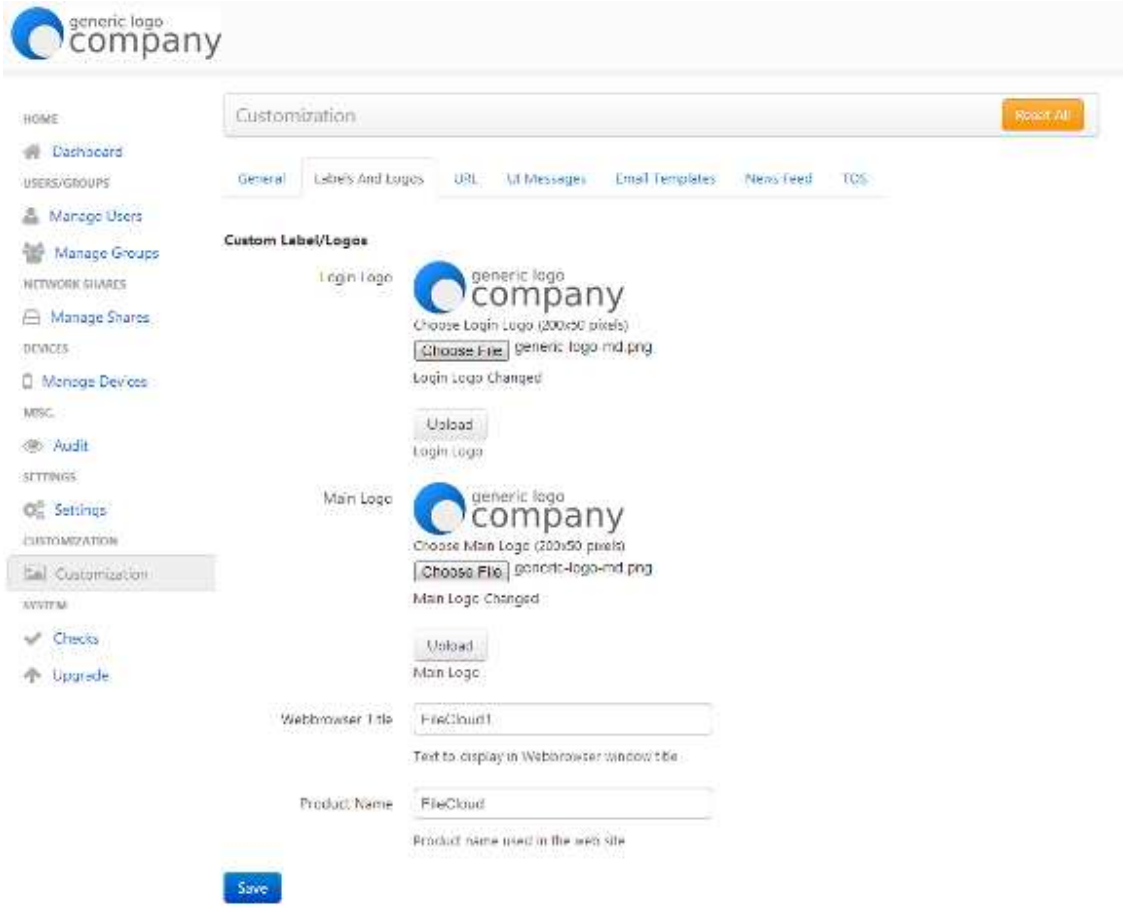
Login Logo	This is the image that will be displayed to all users in the login page. Image must be of png format and must be less than or equal to 200x50
Main Logo	This is the image that will be displayed on top left of every page when logged in. This is also the log that will be displayed in Mobile Apps when connecting to the InfoVaultz server Image must be of png format and must be less than or equal to 200x50
WebBrowser Title	TBD
Product Name	This is the name that will be sent as a part of email subjects and other notifications. Enter your custom service name here.

Setting the logo files will change the logo displayed in the login page and the logo displayed on the top left of every page. Mobile apps will also use this logo when connecting to the InfoVaultz server.

To change the logo, follow steps

1. Login to Administration portal
2. Click on **Customization** on the left navigation menu panel
3. Click on **Label And Logos** Tab
4. Select the the Login Logo and/or Main Logo and upload your company logo.

The logo must be 200x50 or smaller. If the size is not correct, UI will have problems with layout.



UI Messages

InfoVaultz generates a number of messages for user actions. InfoVaultz comes with default messages and these can be customized.

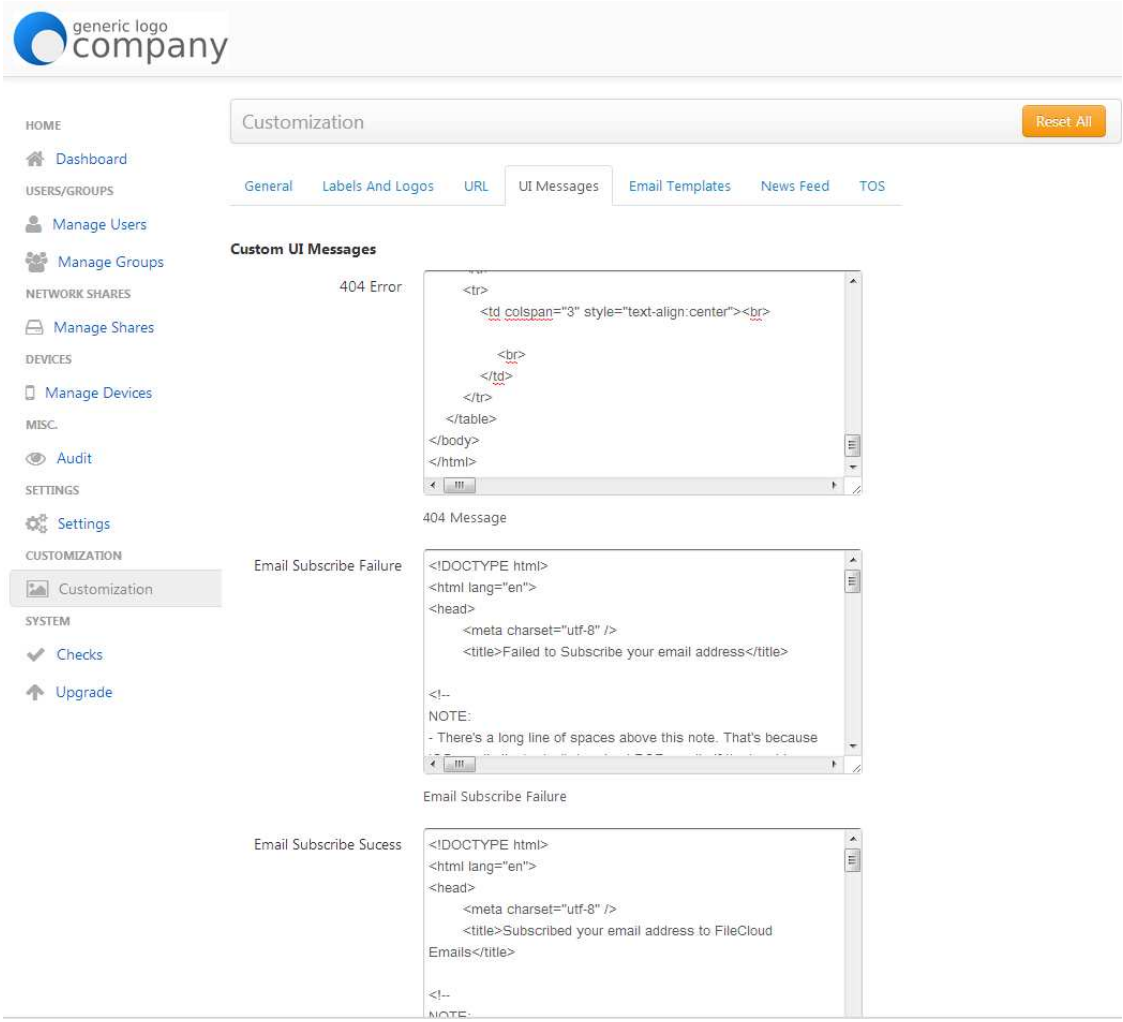
> As of InfoVaultz v4.0, the UI Messages should be entered as HTML. Incorrect HTML will cause rendering issues.

The following messages can be changed

Message Type	Description
404 Error	This is the HTML response shown to user in browser when URL requesting invalid received by InfoVaultz
Email Subscribe Failure	This is the error if a user email could not be subscribed for notifications
Email Subscribe Success	This is the message that will be displayed when user email is subscribed successfully
Email Unsubscribe Failure	This is the error displayed when user email unsubscribe fails.
Account Verification Failure	This is the error shown when a user email verification fails

Account Verification Success	This is the message shown when a user email verification succeeds

1. Log into Administration Portal
2. Click on "**Customization**" on the left navigation panel
3. Click on "**UI Messages**" tab
4. Change the entries as needed.
5. Click on **save** button



Email Templates

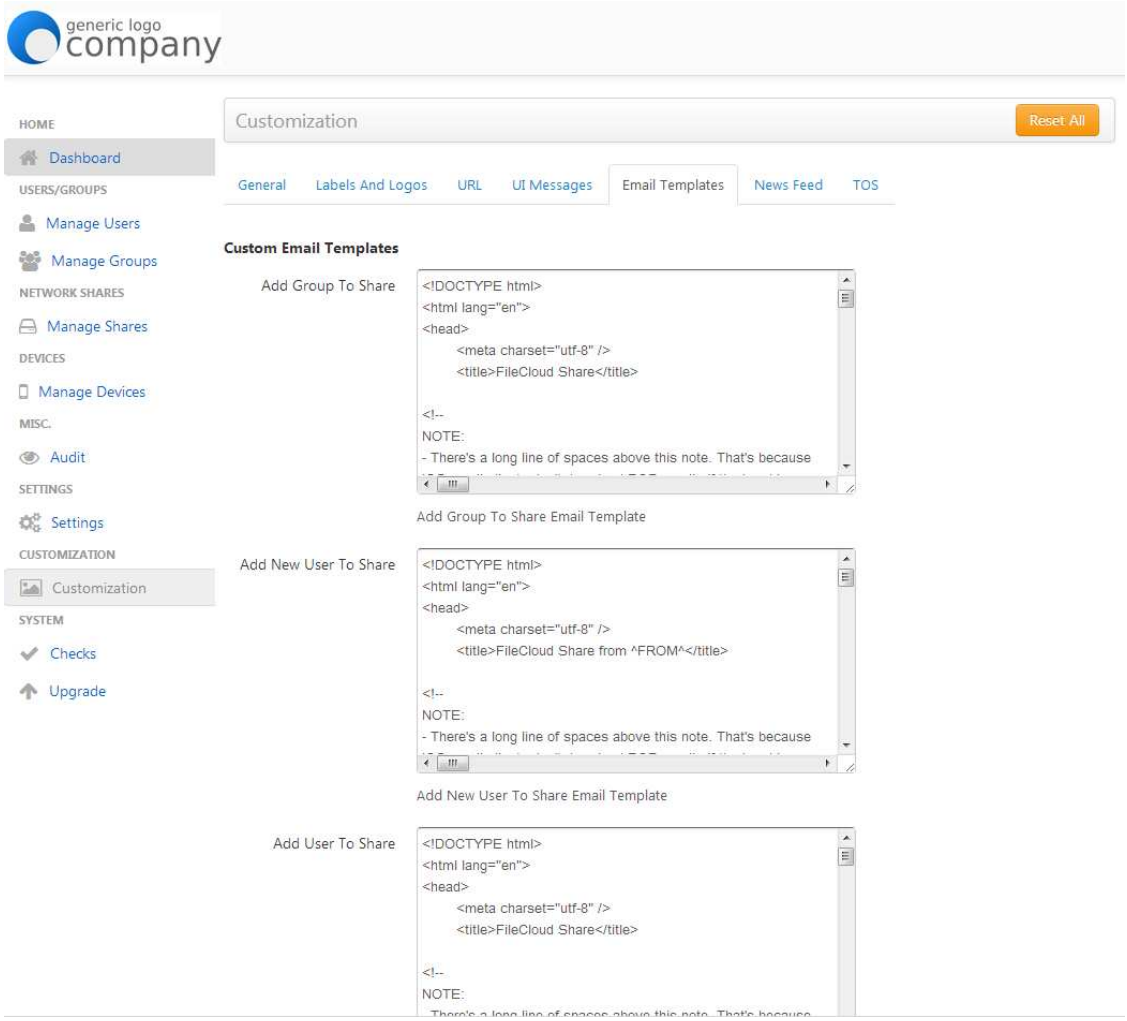
InfoVaultz has various messages to send to user on different user actions. These messages can be customized (overridden from the default messages that come with InfoVaultz)

As of InfoVaultz v4.0, the Email templates should be entered as HTML. Incorrect HTML will cause rendering issues.

Message Template	Description
Add Group To Share	When a share is created for a Group, This is the message that will be sent to all users of that group.

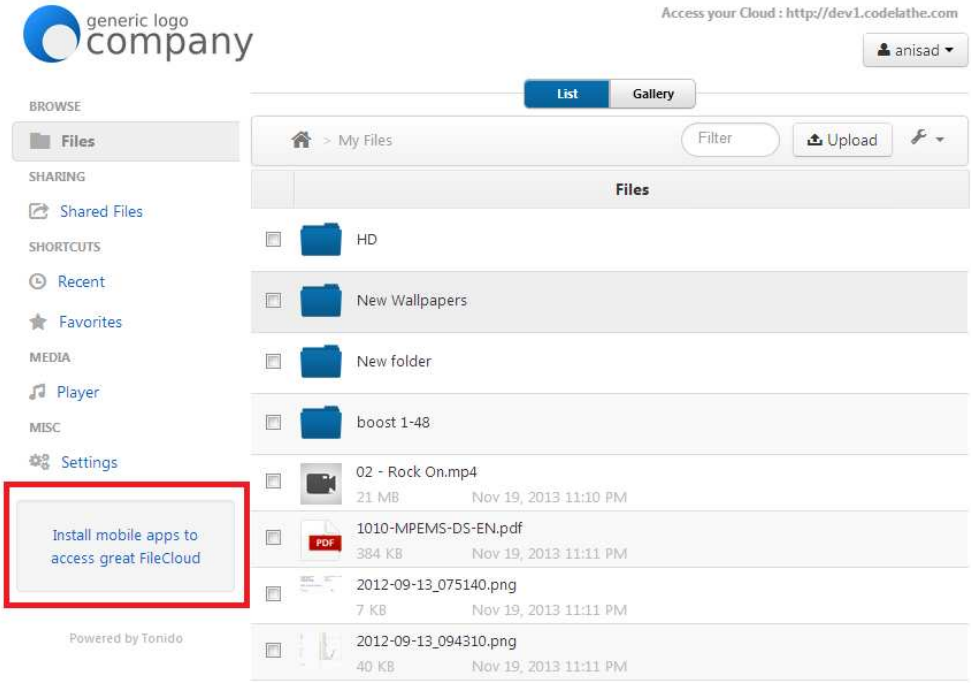
Add New User To Share	When a new share is created this is the message to be sent to a user who is currently NOT a InfoVaultz user. This will contain instructions for the non-InfoVaultz user to first create an account before attempting to access the shared resource
Add User To Share	When a new share is created this is the message to be sent to a user who is already a InfoVaultz user.
File/Folder Share	When a public share is created by a user, the user can send that shared link using email. This message will be used for reporting that share link.
Account Approval	This is the email message to the user that will be sent when Admin approves a user account .
Forgot Password	This is the email message sent when user does password reset
Waiting For Approval	This is the email message that will be sent when a user registers for a new Account in InfoVaultz (and if automatic account approval is not turned on).
Welcome	This is the email message that will be sent when a new user account is approved into InfoVaultz system.
FileChange Notification	This is the email message that will be sent if a share is modified.

1. Log into Administration Portal
2. Click on "**Customization**" on the left navigation panel
3. Click on "**Email Templates**" tab
4. Change the required entries
5. Click on **save** button.



News Feed

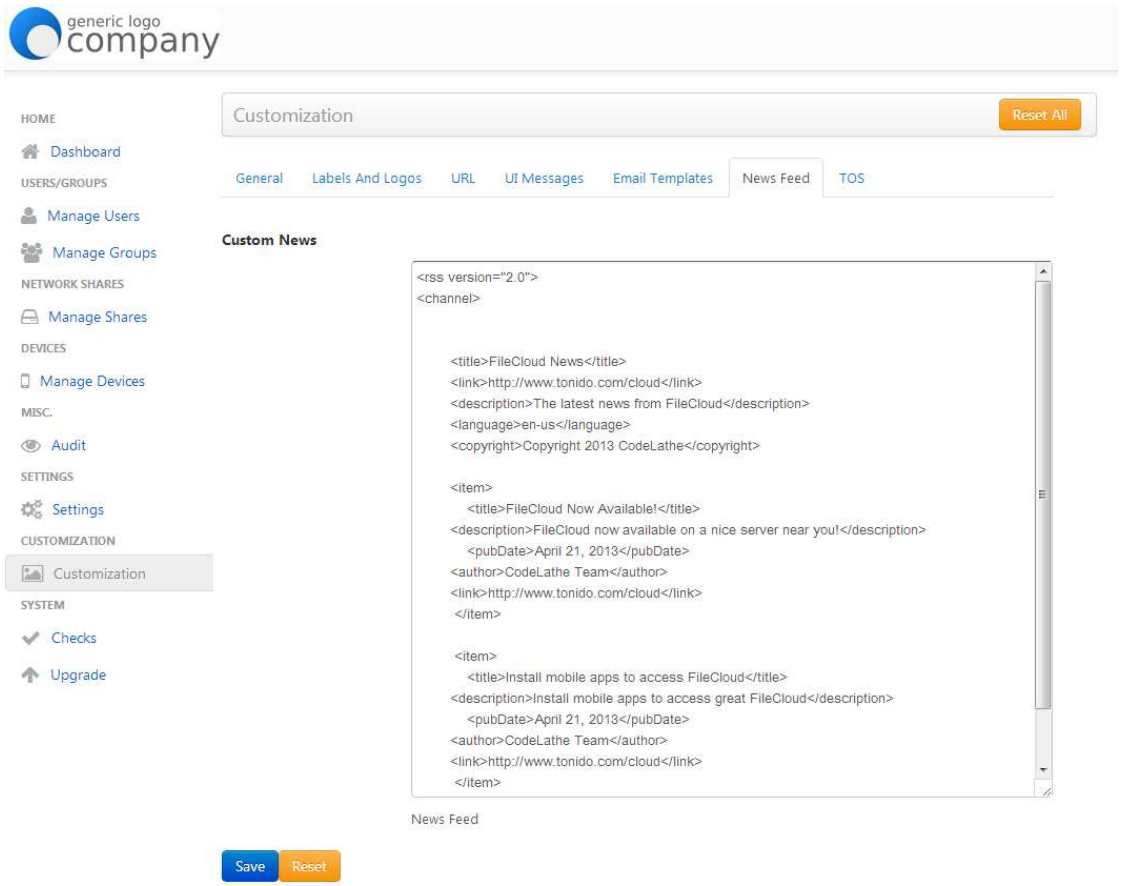
InfoVaultz supports RSS feed to be displayed in the front page of user web UI when the user logs into the InfoVaultz server. This feed can be modified by Administrator.



The RSS feed must follow RSS XML format version 2. Otherwise user UI parsing will fail

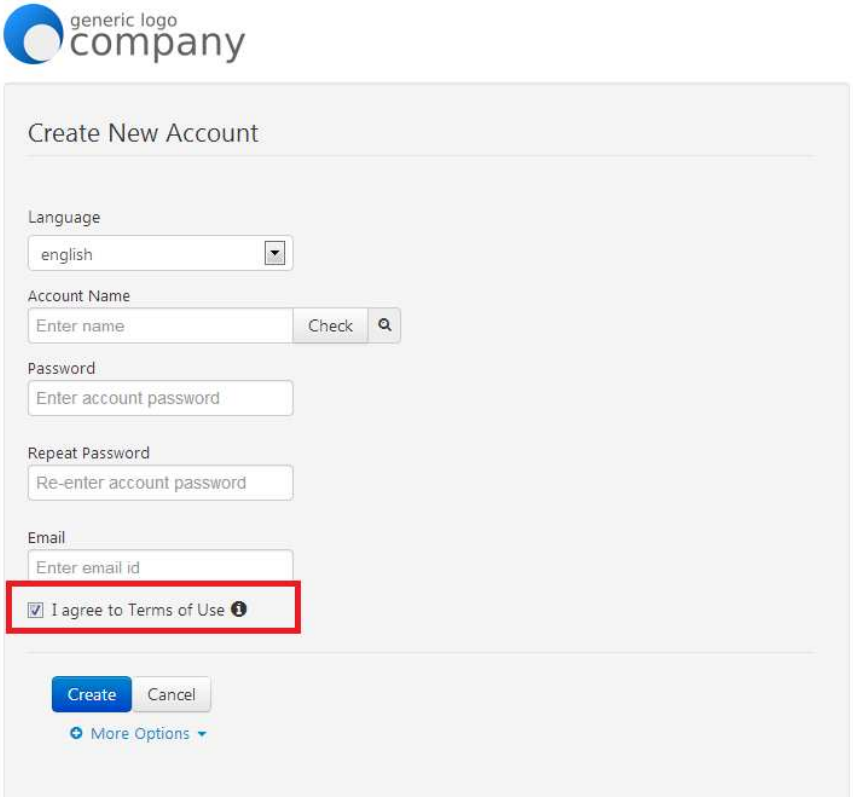
To change the RSS feed ,

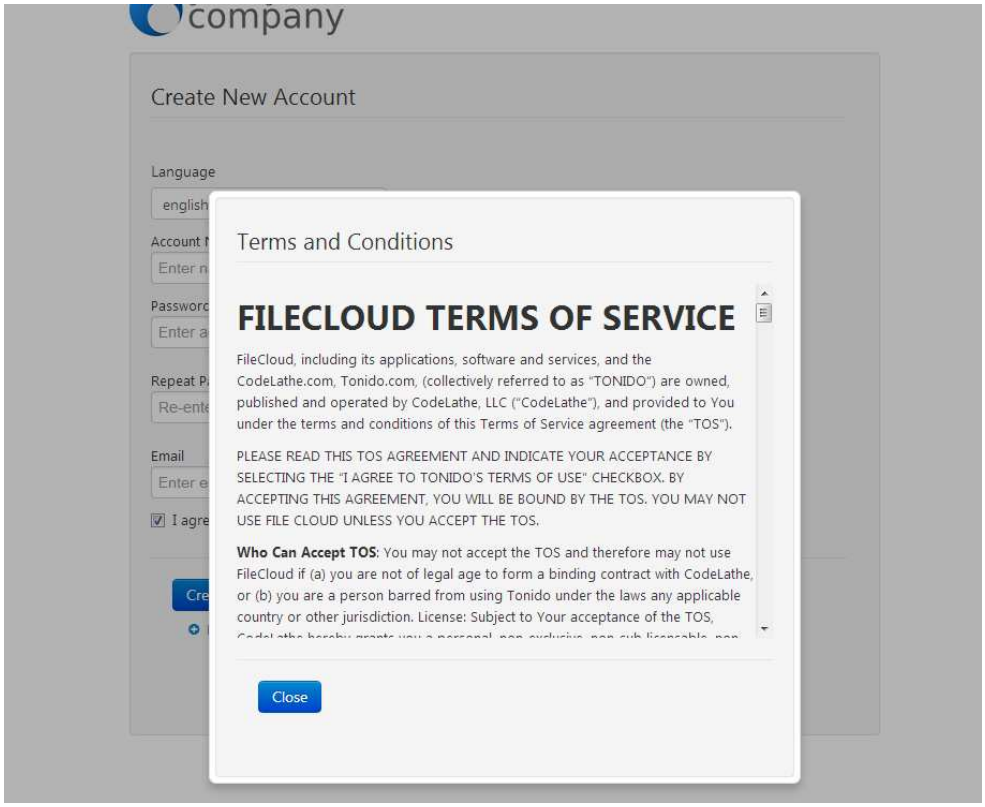
1. Log into Administration Portal
2. Click on "**Customization**"
3. Click on "**News Feed**"
4. Change the feed
5. Click on **save** button.



Terms of Service

Creating an account in InfoVaultz requires the user to accept to the Terms of Service. This can be modified by the InfoVaultz Administrator.

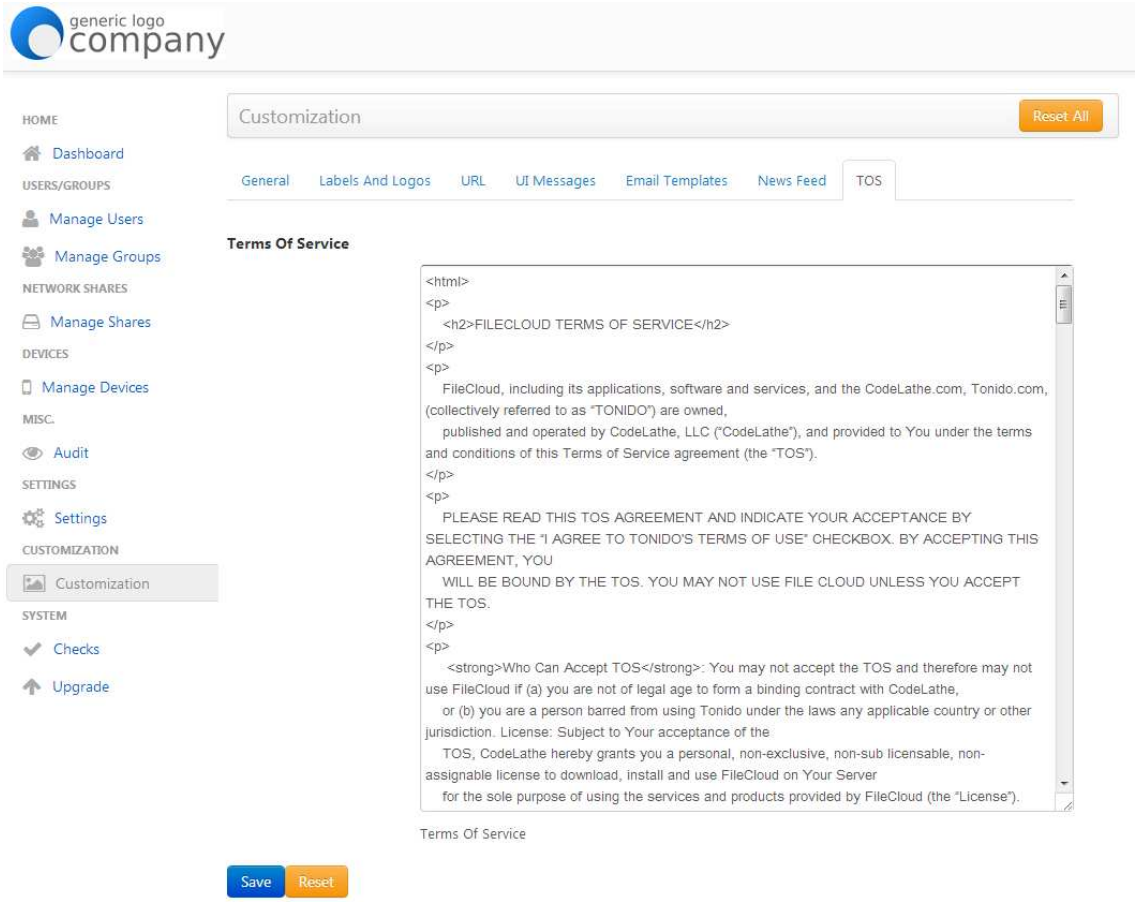




To change the Terms of service,

1. Log into the InfoVaultz Administration portal
2. Click on "**Customization**" in the left navigation panel
3. Click on "**TOS**" tab
4. Change the terms of service

5. Click "**Save**" button



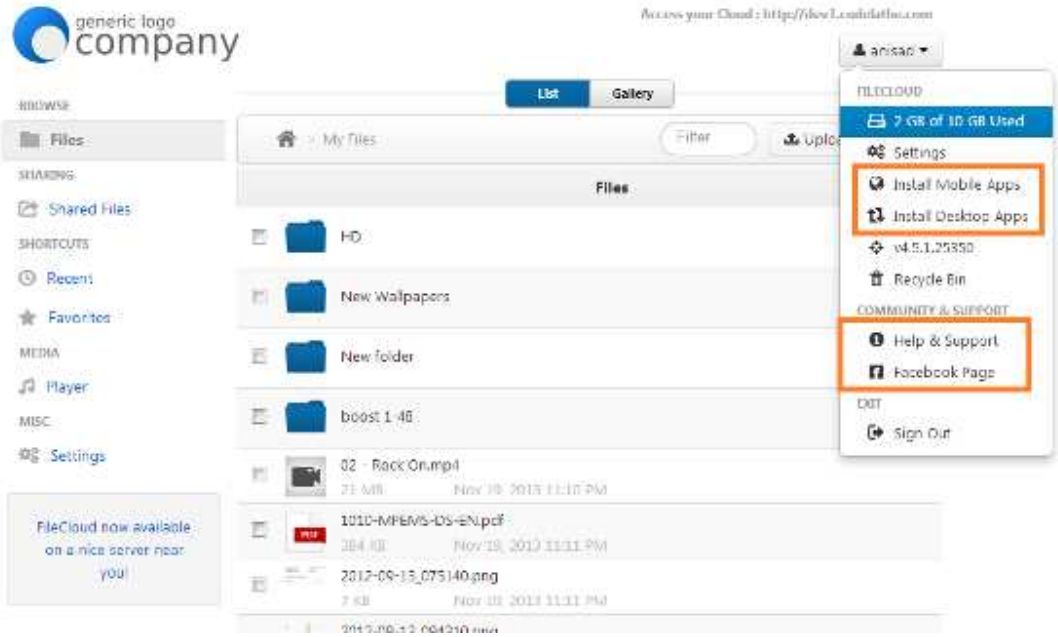
Customize Product URLs

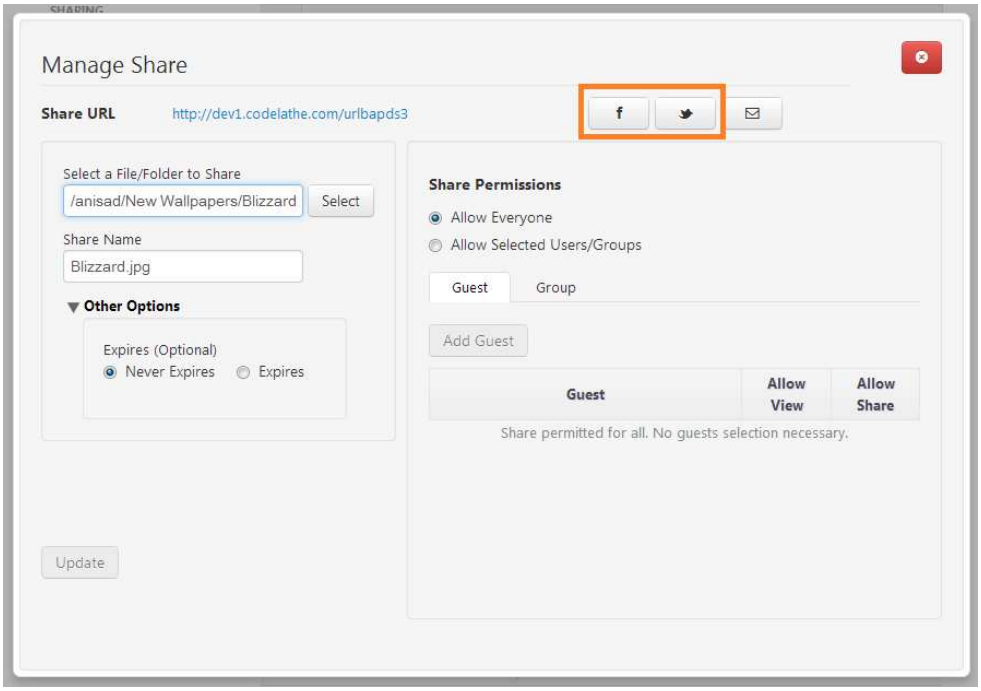
InfoVaultz allows changes to a number of URLs used in the system to customize your user experience.

The following URLs can be customized.

URL	Description
Install Desktop Apps URL	This is the URL that will be opened when user clicks on "Install Desktop Apps" in the dropdown menu (See attached picture). The desktop apps refer to Cloud Sync, Cloud Drive, WebDAV client etc that the user can install in their computer to connect with InfoVaultz. If you are using InfoVaultz's default apps, then no changes is necessary

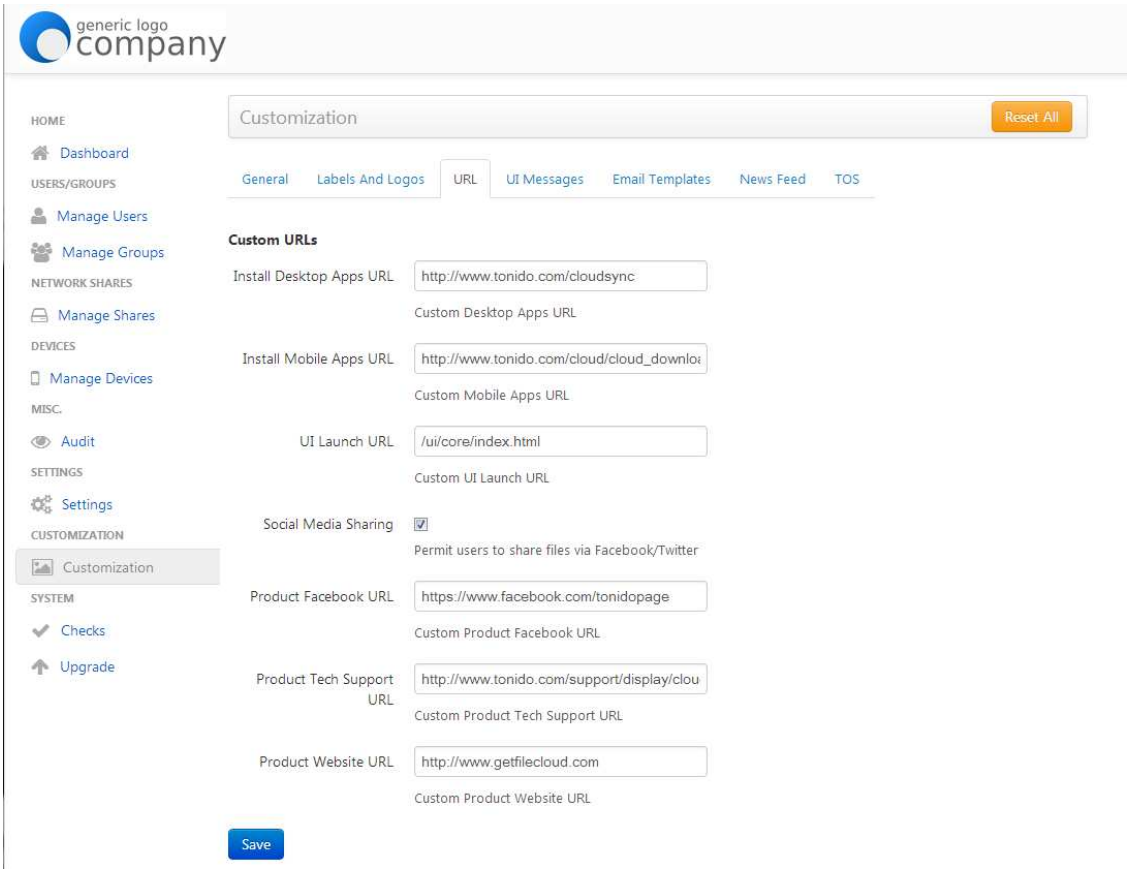
Install Mobile Apps URL	This is the URL that will be opened when user clicks on "Install Mobile Apps" in the dropdown menu (See attached picture). The Mobile apps refer to iOS, Android, Windows Store App, BB10 apps. If you are using InfoVaultz's default apps, then no changes is necessary
UI Launch URL	This is an advanced option and requires redirection to be setup in webbrowser's htaccess file. If there is a redirect setup in htaccess (some url --> /ui/core/index.html), then the "some url" can be entered here to allow browsers to connect. Do not change this if you are not sure. Incorrect setting will cause failure in connecting to InfoVaultz instance.
Social Media Sharing	When a resource is shared by user, the shared resource can be posted to social media (Facebook and Twitter). This can be turned off by unchecking this setting. See attached picture
Product Facebook URL	If this is set, the user UI will contain a link to open this URL in the account dropdown menu.
Product Tech Support URL	This is the url that will be opened when user clicks on "Help & Support" in the drop down menu.
Product Website URL	This is the url that will be opened when a user clicks on "Powered by" url.





To perform customizations, follow the following steps

1. log into the Administration portal
2. Click on "**Customizations**" on the left navigation panel
3. Click on "**URL**" tab
4. Do the changes for the appropriate customization item
5. Click on "**Save**" button



Configuring Email Integration

InfoVaultz sends messages to its users via email. The messages range from share notifications, File change notification to error notifications. In order for the email system to work, the InfoVaultz administrator must setup the mail configuration.

Setting	Description
Email From Address	This is the address from which the email messages will be sent to users.
Email From Name	This is the display name used when sending the email message
Email Reply to Address	This is the address that the recipient will use when they click "Reply" to a message sent from InfoVaultz system.
Email Reply to Name	This is the display name used when recipient replies to a email sent from InfoVaultz system
Email Type	Specify the email facility to be used . The type can be "SMTP", "Mail" or "SendMail". Note that "Mail" and "SendMail" use underlying OS's function (Available only for Debian/Ubuntu installation). The recommended setting is to use SMTP .

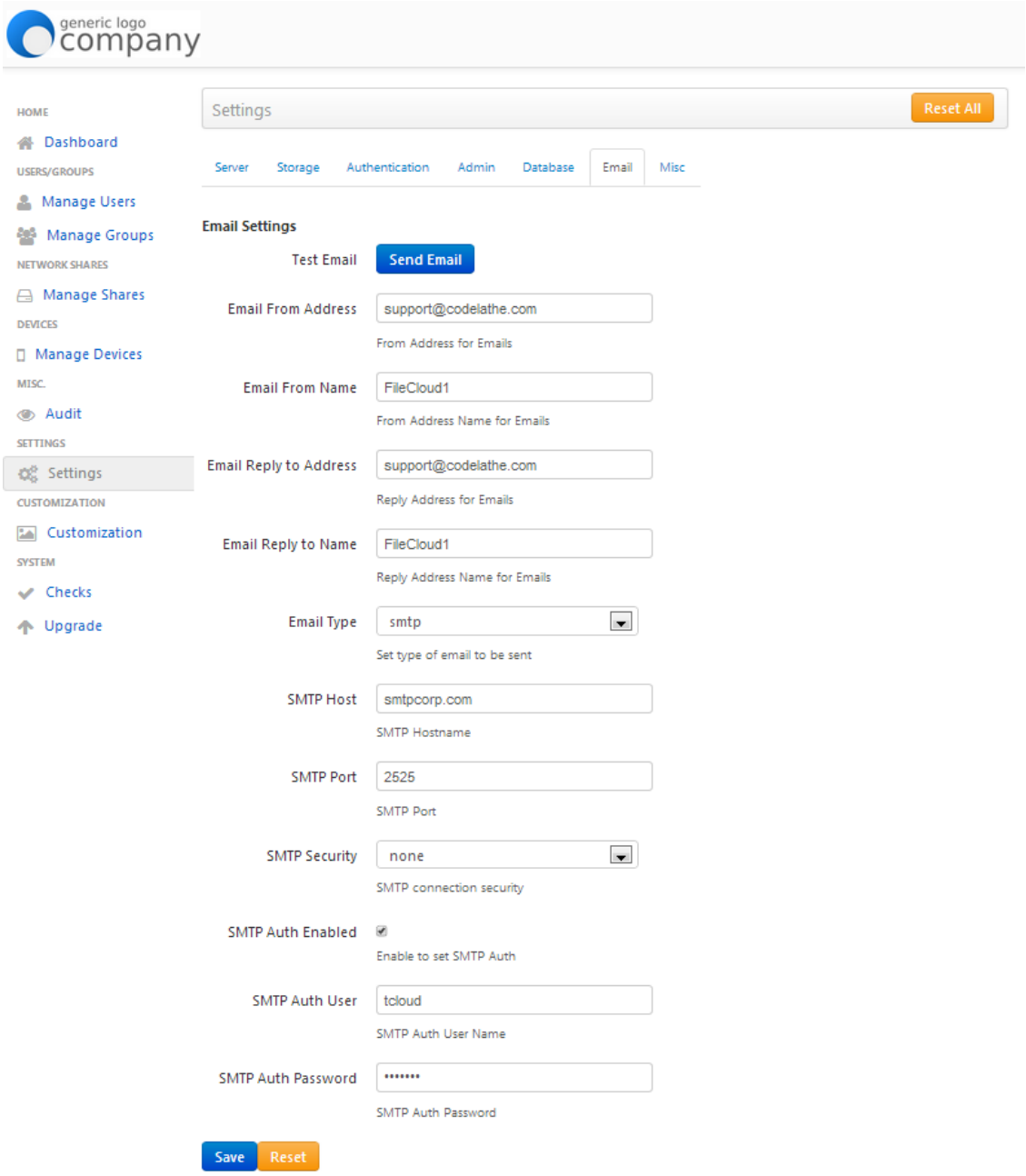
SMTP Configuration

You need an SMTP account to setup email using SMTP type.

SMTP Setting	Description
SMTP Host	SMTP Server to use for sending email
SMTP Port	The SMTP port to use to connect to SMTP Host (This will be given by your SMTP Provider
SMTP Security	If your SMTP provider uses SSL or TLS security then select as appropriapriate
SMTP Auth Enabled	If SMTP requires authentication using username/password, then enable this to enter the user/password
SMTP Auth User	If SMTP Auth is enabled, then enter the authentication username
SMTP Auth Password	If SMTP Auth is enabled, then enter the password for SMTP Auth User.

To Setup the Email,

1. Log into the administration portal
2. Click on "Settings" on the left navigation panel
3. Click on "Email" tab
4. Enter the required information
5. Click Save
6. Click on "Test Email->Send Email" to try the setting (The email will send to the admin's email)



Enable Antivirus Scanning

InfoVaultz supports scanning of uploaded files using ClamAV (an opensource antivirus software).

Antivirus Scanning of Uploaded Files

It is possible to use the OpenSource Free ClamAV Antivirus to scan uploaded files automatically.

ClamAV is available for Windows and Linux.

> *The instructions are for Ubuntu Linux only, but can be used for other Linux systems using equivalent commands*

Note: Currently, Antivirus scanner can only be setup on a Linux server. This Antivirus scanner can be used by a Windows install of InfoVaultz as well, by setting the HOST to the remote Linux server.

Installing ClamAV in Ubuntu

1. **Install the ClamAV package**

   ```
   sudo apt-get install clamav-daemon
   ```

2. **You might need to run 'freshclam' to update the antivirus database files**

   ```
   sudo freshclam
   ```

3. **Update the ClamAV-Daemon mode to use TCP, by running the sudo dpkg-reconfigure clamav-base**

   ```
   sudo dpkg-reconfigure clamav-base
   ```

4. **In the reconfigure wizard, choose Socket Type TCP and Interface as localhost to listen to.**

5. **After reconfigure finishes, verify the clamd.conf file is setup correctly (/etc/clamav/clamd.conf)**

   ```
   TCPSocket 3310
   TCPAddr localhost
   StreamMaxLength 100M
   ```

6. **Start ClamAV-Daemon**

```
sudo /etc/init.d/clamav-daemon start  \
```

Integrating ClamAV with InfoVaultz

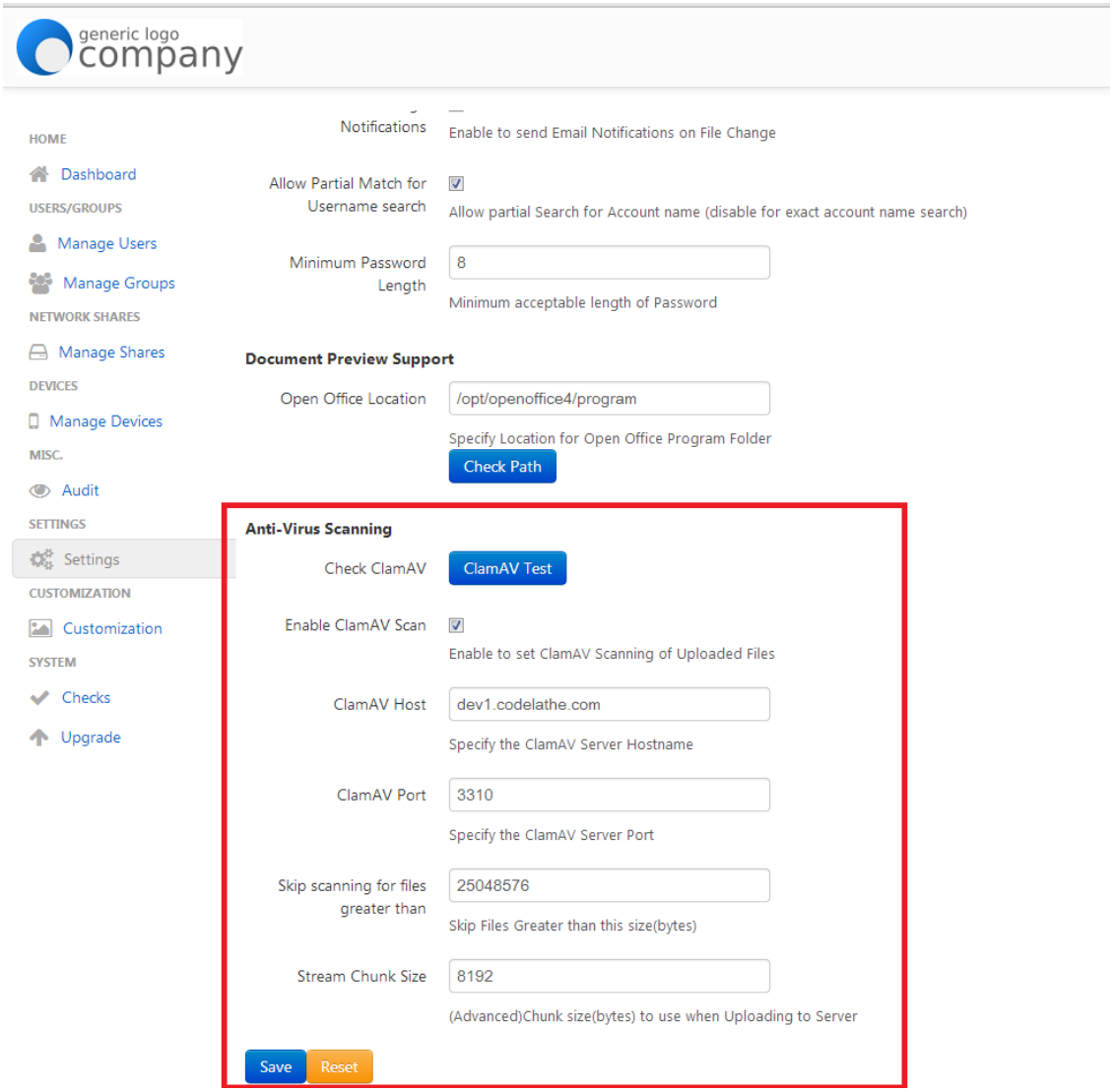
Once the ClamAV is setup and started, The next step is to add details of the ClamAV service to InfoVaultz server

1. Log into InfoVaultz Administration Portal
2. Click on **Settings** in the left navigation panel
3. Click on **Misc** tab
4. Locate the group of settings under **Anti-Virus Scanning**
5. Enter the following information
6. Click the **save** button
7. Click on **ClamAV Test** button to verify connectivity

Once AV configuration is setup , every file uploaded to InfoVaultz will be scanned before being added to InfoVaultz storage. If a file fails AV check (a virus detected) then the file will be deleted and an entry will be added to the Audit log with the details of the file

Setting	Description
Enable ClamAV Scan	Check this setting to enable AV scanning

ClamAV Host	Enter the URL or IP of the system where Clam AV is running. This can be local or remote system. In the case of Windows version of InfoVaultz, the AV will be running on a different linux system and in the Windows InfoVaultz setting, enter the linux system's IP
ClamAV Port	The port used by ClamAV (This is set when ClamAV is installed in the previous section)
Skip scanning for files greater than	This is the file limit in bytes that will be scanned. For example, very large files can be excluded from scanning. default value 25MB
Stream Chunk Size	This is a advanced setting used to stream the file content to AV server for scanning. Default is 8k.



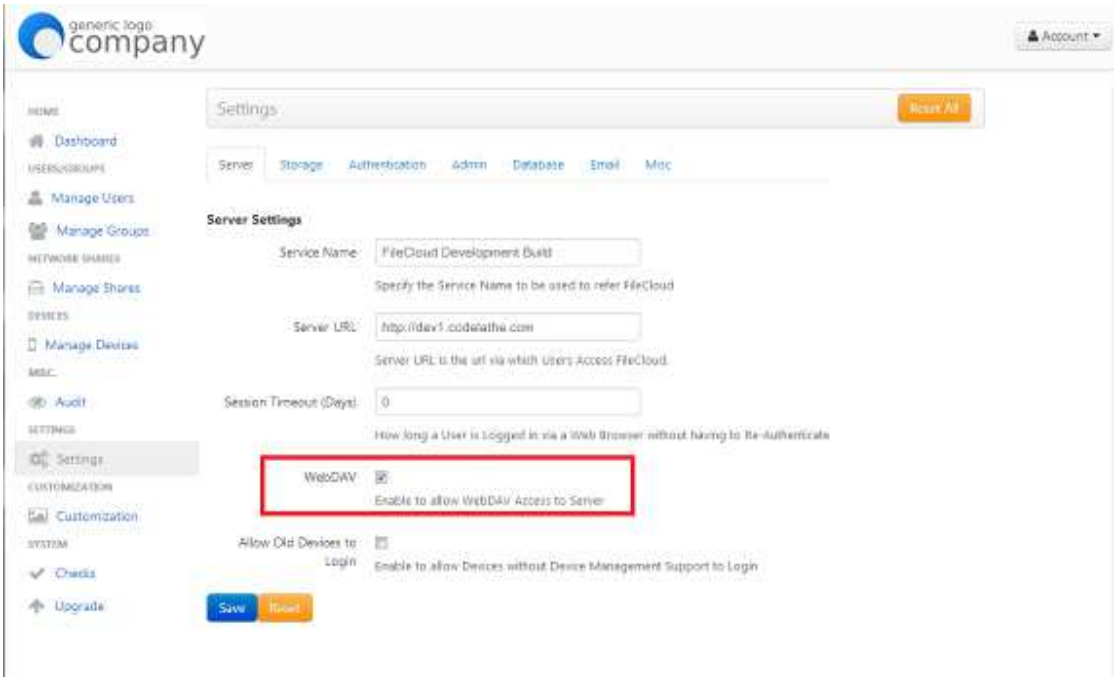
Enable WebDAV

InfoVaultz has support to allow InfoVaultz users to access their storage using WebDAV clients.

Enable WebDAV

To enable WebDAV,

1. Log on to Administration Portal
2. Click on "**Settings**" on the left navigation panel
3. Click on "**Server**" Tab
4. Check the "**WebDAV**" checkbox
5. Click Save



Accessing storage using WebDAV

Read about it here.

Setting up Document Preview

This section explains the process to setup document preview to allow the user to view pdf, doc, docx, ppt, pptx, xls,xlsx documents directly in the webbrowser.

InfoVaultz supports the capability to preview documents starting from Version 4.0.
This feature allows to preview document types such as word, excel, text, power point.

InfoVaultz uses OpenOffice as a converter to convert these different document into PDF and presents them in a viewable format in the browser.
O penOffice is the main component in the document preview support and it should be run in server mode for converting the documents on the fly.
This article describes how to run openoffice in server mode.

- Ubuntu/Debian Instructions
- Redhat/CentOS Instructions
- Windows Instructions

Ubuntu/Debian Instructions

1) Download OpenOffice

Download the latest version of OpenOffice from here applicable for your platform.

2) Setup OpenOffice On Ubuntu/Debian

1. Install necessary prerequisites for OpenOffice.
   Install OpenOffice Prereqs

```
# sudo apt-get install libxt6
# sudo apt-get install libxrender1
# sudo apt-get install openjdk-6-jre-headless
```

2. Install OpenOffice
   Install OpenOffice

```
# sudo tar zxvf Apache_OpenOffice_4.0.0_Linux_x86-64_install-deb_en-US.tar.gz   //name of the file mi
# sudo cd en-US/DEBS
# sudo dpkg -i *.deb
```

3. Setup permissions for OpenOffice
   Running OpenOffice Server In Linux

```
# sudo chown www-data:www-data /var/www
# sudo su - www-data -c 'mkdir .openoffice'
```

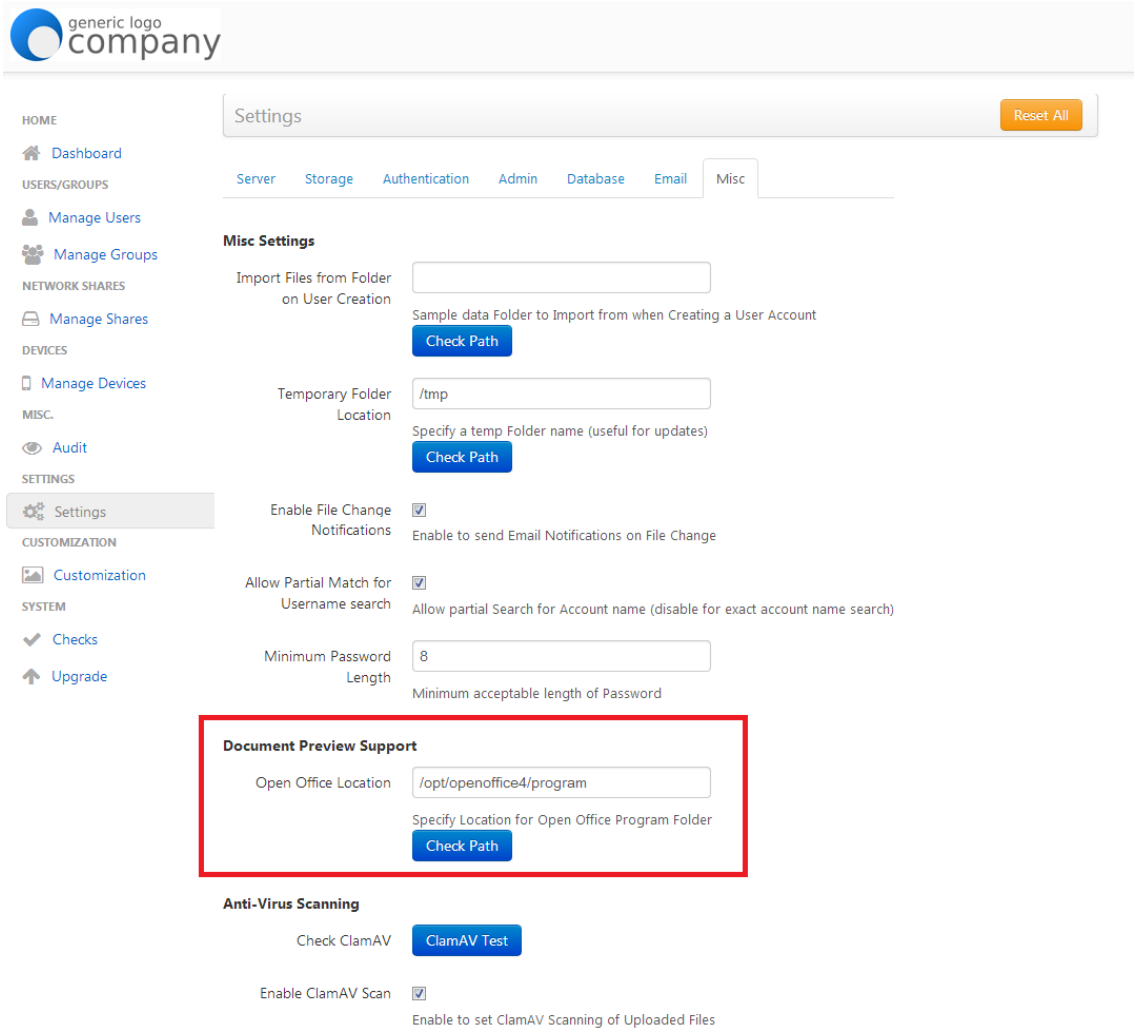
4. Start OpenOffice in server mode using same user id that runs apache server.
   Running OpenOffice Server In Linux

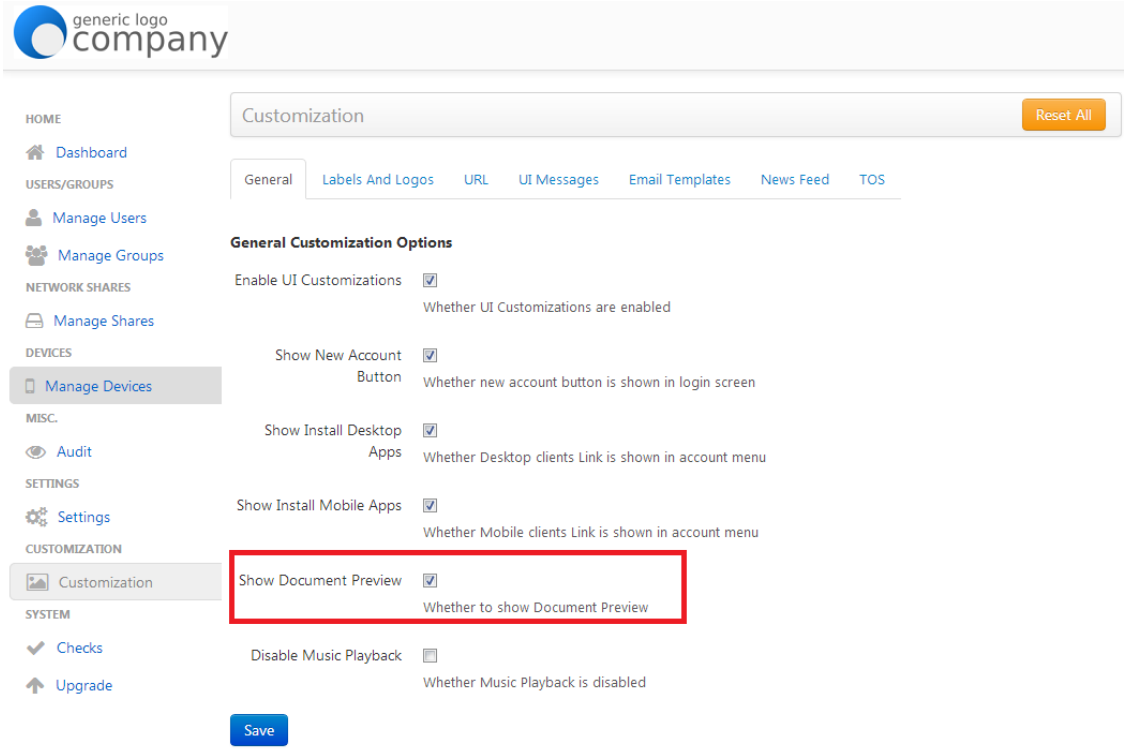
```
# sudo cd /var/www
# sudo su - www-data -c '/opt/openoffice4/program/soffice -headless -accept="socket,host=127.0.0.1,po
```

3) Configure InfoVaultz

There are two steps to enable Preview.

1. Log into Administration Portal
2. Click on "Settings" on the left navigation panel
3. Click on "Misc" Tab
4. Enter the path to the open office program folder
5. Click on "Customization" on the left navigation panel
6. Click on "General Tab
7. Check the "Show Document Preview" checkbox


generic logo
company
HOME
Dashboard
USERS/GROUPS
Manage Users
Manage Groups
NETWORK SHARES
Manage Shares
DEVICES
Manage Devices
MISC.
Audit
SETTINGS
Settings
CUSTOMIZATION
Customization
SYSTEM
Checks
Upgrade
Settings
Reset All
Server
Storage
Authentication
Admin
Database
Email
Misc
Misc Settings
Import Files from Folder on User Creation
Sample data Folder to Import from when Creating a User Account
Check Path
Temporary Folder Location
/tmp
Specify a temp Folder name (useful for updates)
Check Path
Enable File Change Notifications
Enable to send Email Notifications on File Change
Allow Partial Match for Username search
Allow partial Search for Account name (disable for exact account name search)
Minimum Password Length
8
Minimum acceptable length of Password
Document Preview Support
Open Office Location
/opt/openoffice4/program
Specify Location for Open Office Program Folder
Check Path
Anti-Virus Scanning
Check ClamAV
ClamAV Test
Enable ClamAV Scan
Enable to set ClamAV Scanning of Uploaded Files



Redhat/CentOS Instructions

Windows Instructions

1) Download OpenOffice

Download the latest version of OpenOffice from here applicable for your platform.

2) Setup OpenOffice for Windows

1. Install OpenOffice for windows.
2. Open OpenOffice once and finish the registration.(Skip step 2 if already Registered)
3. Start Open Office service. Open Command Prompt in Windows and run the following Command.
4. To verify successful installation check if soffice is running in Task Manager.

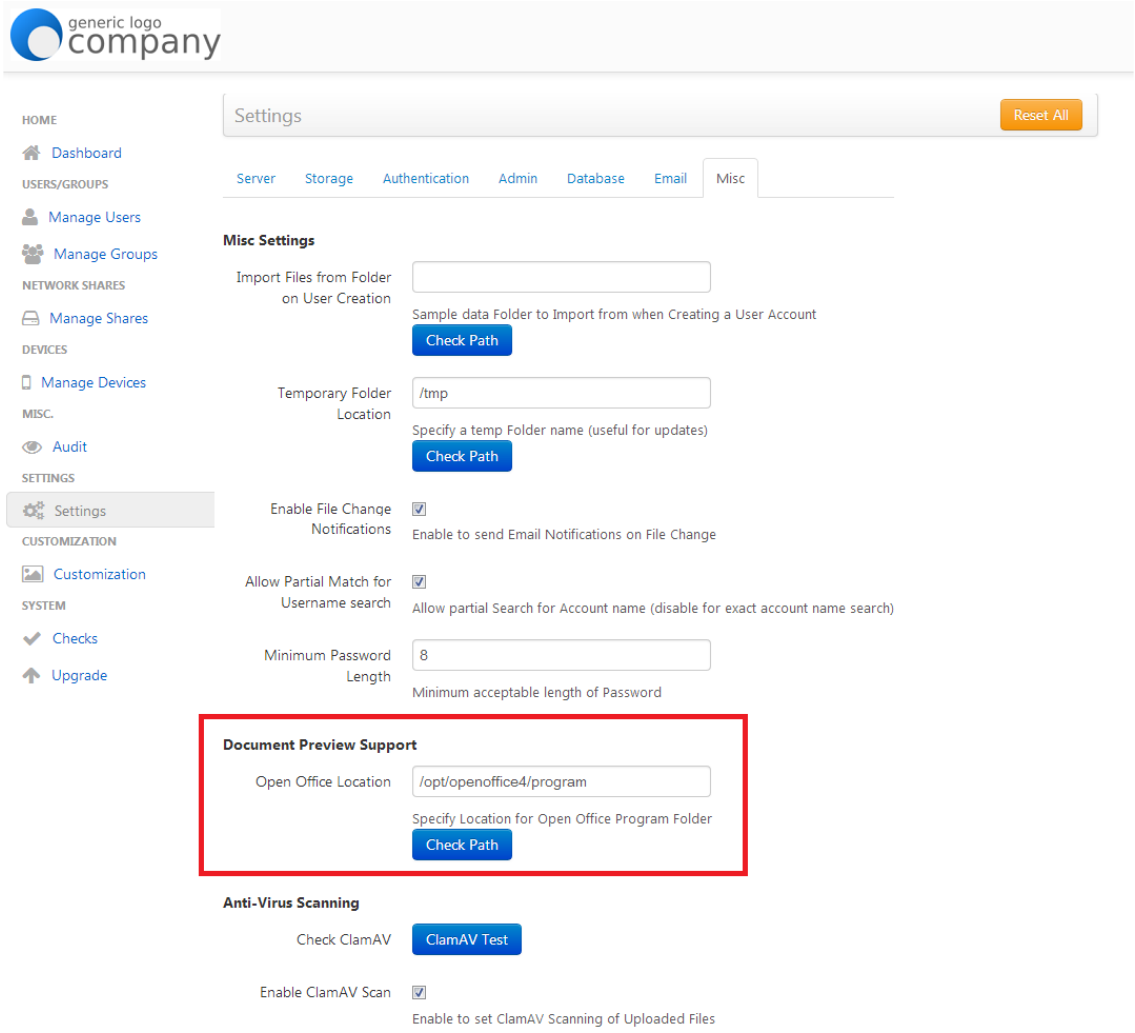
Start OpenOffice Server In Windows (Assuming Open office is installed in C:\Program Files (x86)

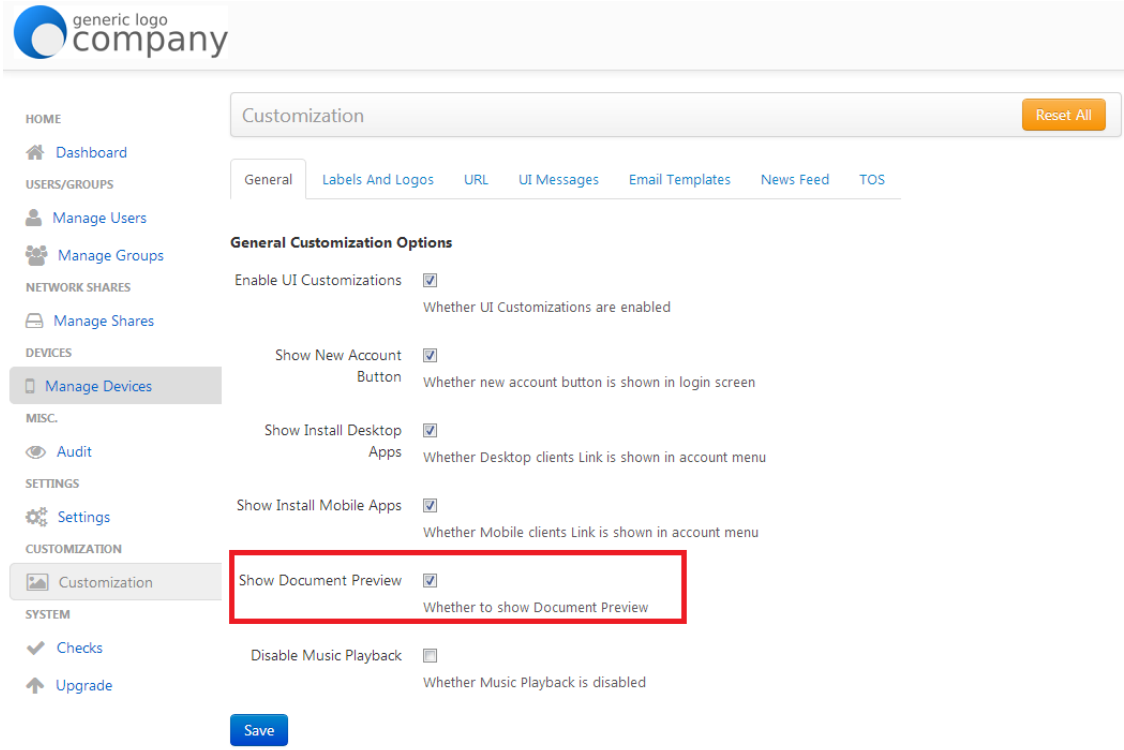
```
C:\>"C:\Program Files (x86)\OpenOffice 4\program\soffice.exe" -headless -accept="socket,host=127.0.0.1,port=
```

3) Configure InfoVaultz

There are two steps to enable Preview.

1. Log into Administration Portal
2. Click on "Settings" on the left navigation panel
3. Click on "Misc" Tab
4. Enter the path to the open office program folder
5. Click on "Customization" on the left navigation panel
6. Click on "General Tab
7. Check the "Show Document Preview" checkbox


generic logo
company
HOME
Dashboard
USERS/GROUPS
Manage Users
Manage Groups
NETWORK SHARES
Manage Shares
DEVICES
Manage Devices
MISC.
Audit
SETTINGS
Settings
CUSTOMIZATION
Customization
SYSTEM
Checks
Upgrade
Settings
Reset All
Server
Storage
Authentication
Admin
Database
Email
Misc
Misc Settings
Import Files from Folder on User Creation
Sample data Folder to Import from when Creating a User Account
Check Path
Temporary Folder Location
/tmp
Specify a temp Folder name (useful for updates)
Check Path
Enable File Change Notifications
Enable to send Email Notifications on File Change
Allow Partial Match for Username search
Allow partial Search for Account name (disable for exact account name search)
Minimum Password Length
8
Minimum acceptable length of Password
Document Preview Support
Open Office Location
/opt/openoffice4/program
Specify Location for Open Office Program Folder
Check Path
Anti-Virus Scanning
Check ClamAV
ClamAV Test
Enable ClamAV Scan
Enable to set ClamAV Scanning of Uploaded Files



Enable File Change Notifications

Users can automatically receive notifications through email when files are added, updated or deleted.

In order for users to get notifications through email, InfoVaultz administrators must enable File Change Notification emails to be sent whenever files have been changed.

Additionally, Users can disable notification emails on a specific folder.

Email configuration must be done for this feature to work

How does File Change Notifications Work?

When multiple users have access to the same files and folders any change made by a user to the file or folder will trigger email notifications to all users that have access to that file or folder. In InfoVaultz, multiple users can have access to the same file or folder when:-

- Files from network storage are shared with different users.
- Files from network storage are shared with different groups.
- Folders from managed storage or network storage has been shared with other users.
- Folders from managed storage or network storage has been shared with other groups.

It must be noted that the users will receive email notifications even when a subfolder within a shared folder has file changes.

All file change notifications are consolidated and emails are are sent by InfoVaultz at regular notification frequency (15 minutes, 1 hour, 1 day etc) as set by your InfoVaultz administrator.

Set up File Change Notification Cron in Linux

Prerequisite

To run from a cron job, mongodb extension should be enabled in PHP CLI mode. To enable mongodb, the following line should be added to the end of PHP ini file.

Enabling mongodb

```
extension=mongo.so
```

In Linux, PHP ini file should be under /etc/php5/cli/php.ini

How to set up Cron for File Change Notifications in Linux:

1. Open the crontab

   ```
   crontab -e
   ```

2. At the end of the crontab file add the following line to schedule Notifications every 60 minutes.

   ```
   */60 * * * * php /var/www/core/framework/cron.php
   ```

   The above command assumes your InfoVaultz installation is under /var/www/ folder.

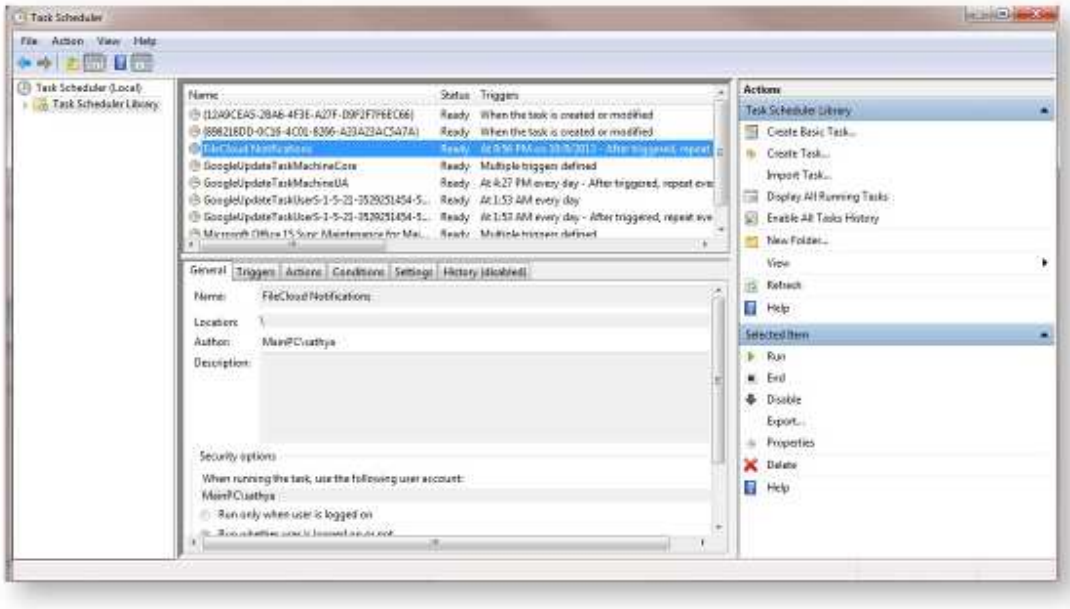
3. Save and Exit

Set up File Change Notification Scheduled Task in Windows

Use Notepad or similar program to create a new file named "fccron.vbs" in a location like c:\xampp\htdocs\resources\backup folder.
On "fccron.vbs" enter the contents from the code block below and save the file. Additionally, in the code block below ensure that paths to php.e and cron.php files are correct.

```
CreateObject("Wscript.Shell").Run "C:\xampp\php\php.exe -f ""c:\xampp\htdocs\core\framework\cron.php"" ", 0,
```

1. Click Start
2. Type "Task Scheduler" in the search programs and files text box.

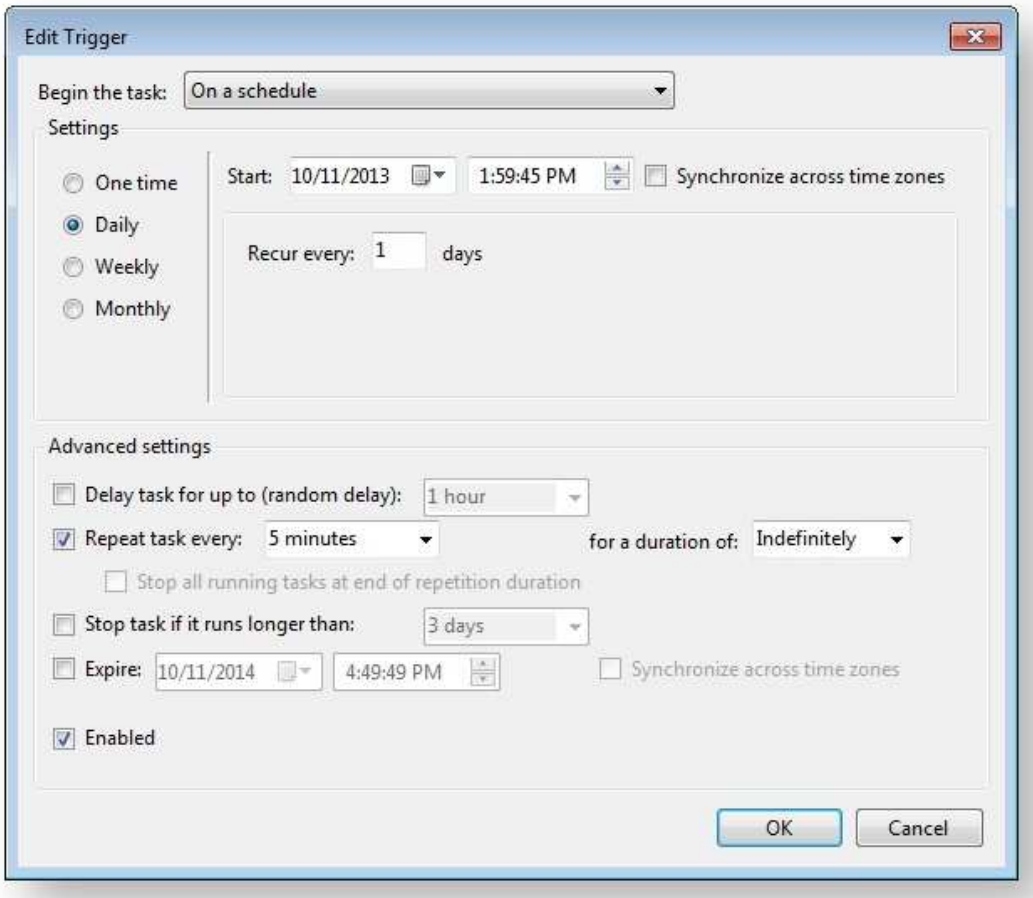


3. Click Create Task in the right menu under Actions

General Tab

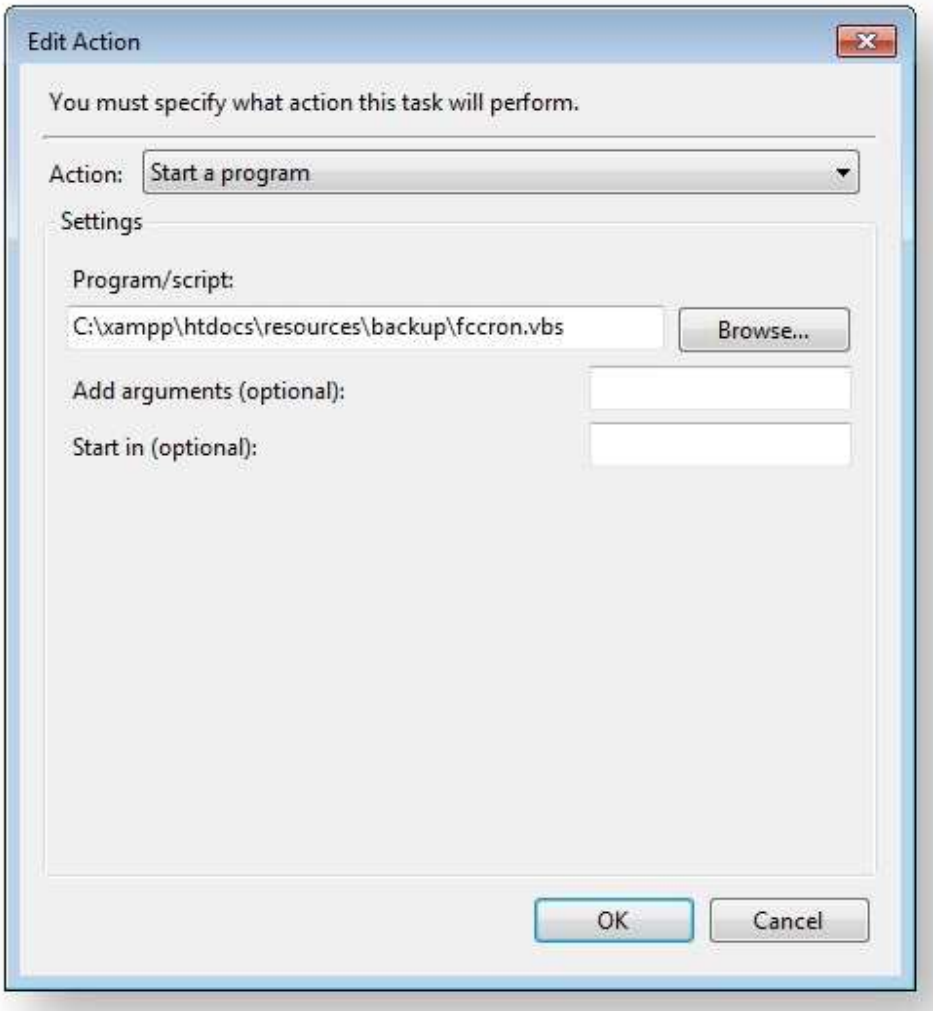
```
Set the Name "InfoVaultz Notifications"
Under Security options, select run whether user is logged on or not.
```

Triggers Tab




```
Click New Trigger
Select "On a Schedule"from Begin the task drop down
In Settings->Select "Daily"and select a time and then select "Recur every 1 days"
Under Advanced Settings - Check Repeat Task every 5minutes (you can adjust ifyou want more frequent n
Select "indefinitely"forthe duration of dropdown.
Check Enabled.
Click OK
```

Actions Tab



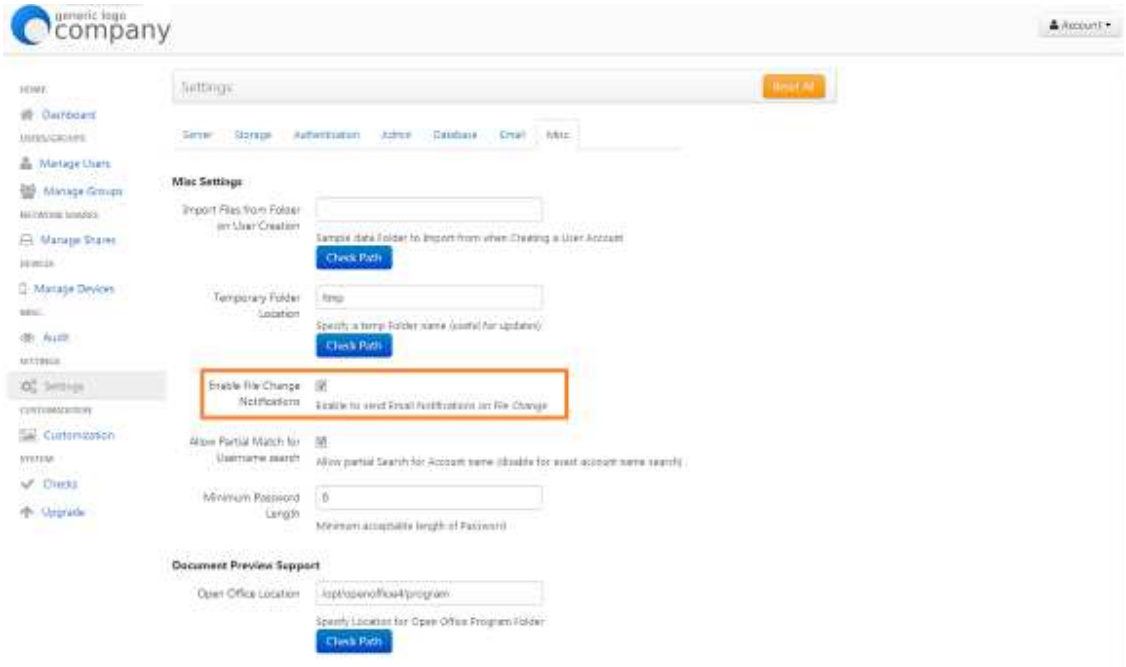

```
Click New Action
From the Action drop down, select "start a program"
Enter the path to fccron.vbs file in the Program/Script text box. (e.g. c:\xampp\htdocs\resources\bac
Click OK
```

All other settings can be default, unless you need to change them for a different reason.

Enabling File Change Notification

Once the cron jobs are properly setup as described in the previous sections, enable the file change notifications setting using the following steps

1. Log on to InfoVaultz Administration Portal
2. Click on **Settings** on left navigation panel
3. Click on "**Misc**"
4. Check "**Enable File Change Notifications**" checkbox



InfoVaultz Site Maintenance

- Managing Users
- Managing Groups
- Managing User Folders and Files
- Managing Disk space Usage
- Managing Client Devices
- Upgrading InfoVaultz
- Audit Logs
- Backing up InfoVaultz Data

Managing Users

This section provides information on managing InfoVaultz users. Click on the appropriate title to learn more.

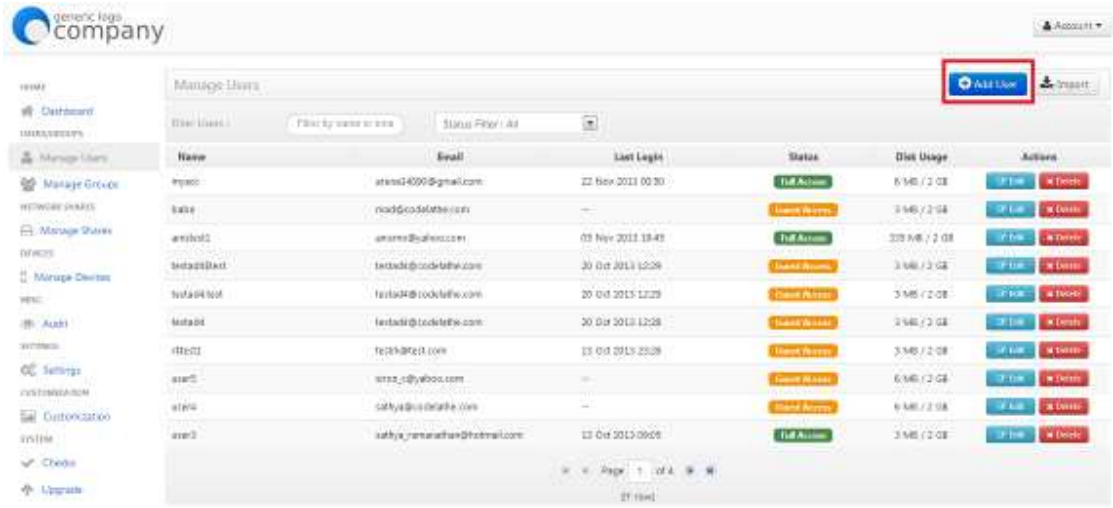
- Create new InfoVaultz user
- Import a InfoVaultz user from AD or LDAP
- Service Bulk creation of InfoVaultz users from
- CSV File Bulk import of InfoVaultz Users from AD
- Server Listing InfoVaultz Users
- Viewing User Properties
- Disabling InfoVaultz User
- Deleting a InfoVaultz
- User Reset User Password

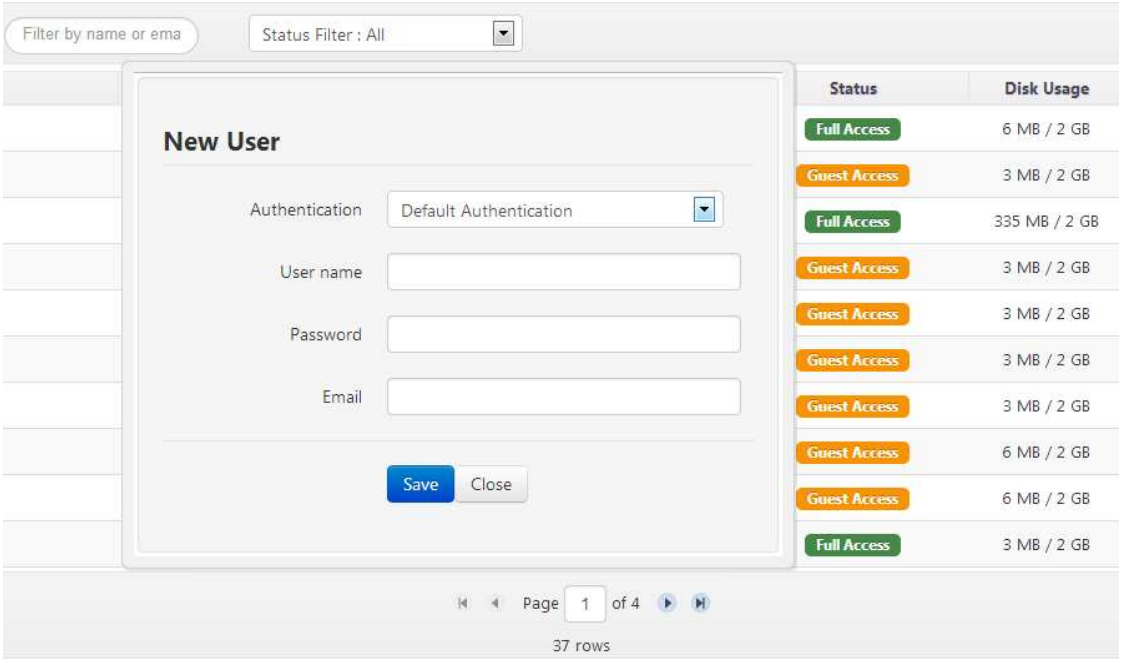
Create new InfoVaultz user

Create InfoVaultz user with Default Authentication

1. Log on to Administration Portal
2. Click on "**Manage Users**" on the left navigation panel
3. Click on "**Add User**" button
4. Set the required account information as shown and click save

Settings	Description
Authentication	Set to **"Default Authentication"**
User name	Name to be used to log into the system (ASCII alphanumeric)
Password	Password for the user (Should adhere to Password length and strength requirements for your organization)
Email	The email id should be unique in the InfoVaultz system



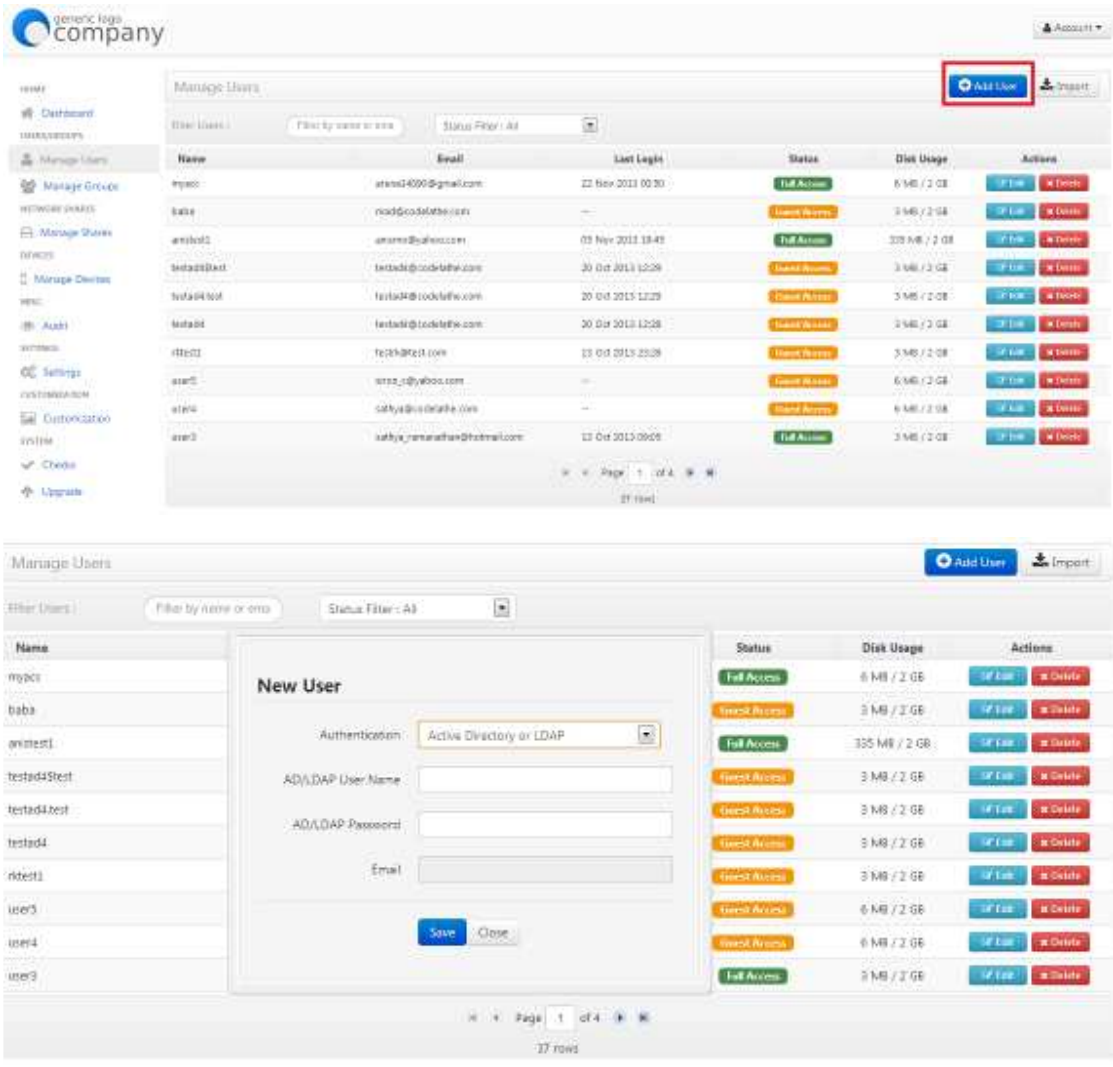


Import a InfoVaultz user from AD or LDAP Service

Import a InfoVaultz user from AD or LDAP Service

1. Log on to Administration Portal
2. Setup AD configuration or LDAP configuration depending on your requirements.
3. Click on "**Manage Users**" on the left navigation panel
4. Click on "**Add User**" button
5. Set the required account information as shown and click save

Settings	Description
Authentication	Set to **"Active Directory or LDAP"**
AD/LDAP User name	AD/LDAP User name to import
AD/LDAP Password	AD/LDAP User name's Password
Email	Disabled: This will be imported from AD/LDAP service



Bulk creation of InfoVaultz users from CSV File

InfoVaultz allows bulk creation of InfoVaultz users using Comma Seperated Files (CSV)

The users created by method will have

1. Default Authentication
2. Will be created as "Guest Access" user. The Administrator can change this access once the user account is created.
3. Will be marked as "Email Verified" (i.e, the account can be immediately used with the correct password

Format of CSV file for creating user

The CSV file must have the following structure

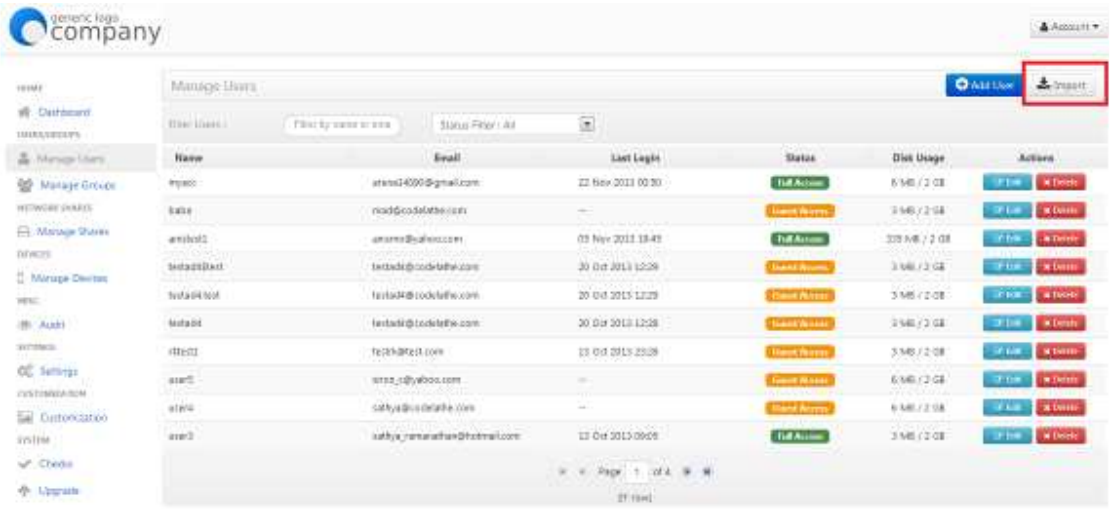
```
userid,emailid,password
```

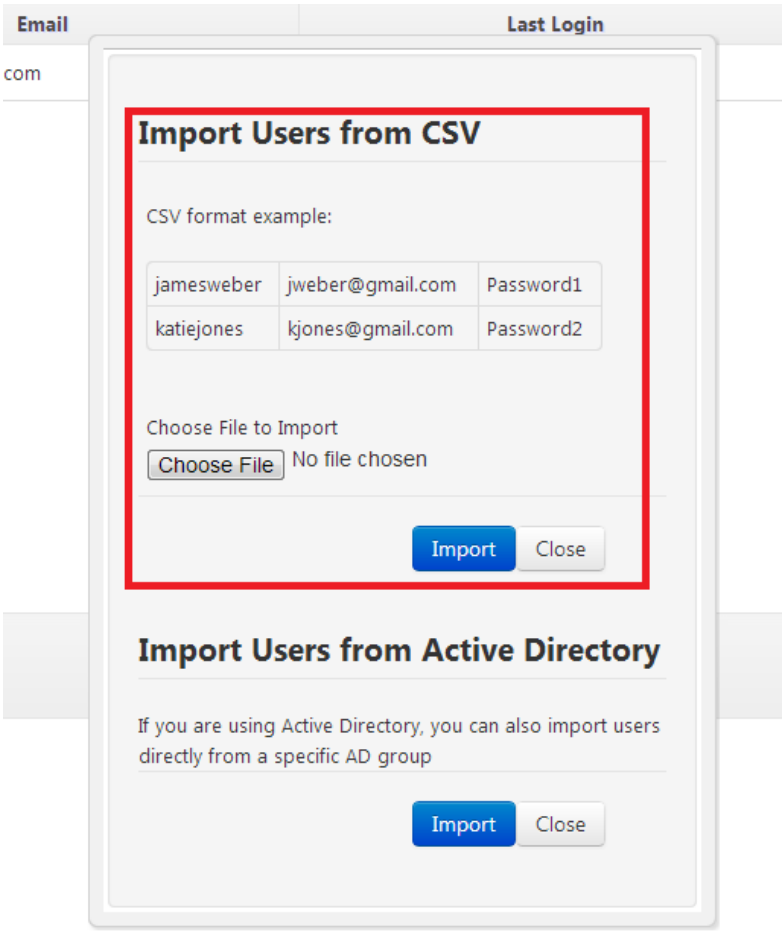
Field	Description
Userid	This is the user id to be created in the system
emailid	This must be a unique email id to be associated with the user
password	Password for the user. Must follow password requirement (like minimum length etc)

Importing CSV File

To import a CSV File, follow the steps listed

1. Log on to the Administration Portal
2. Click on "**Manage Users**" in the left navigation panel
3. Click on "**Import**" button on top right corner to launch the import dialog window
4. Select the CSV file containing the entries of users to be created and click "Import"
5. Once the process is complete, a report will be generated indicating the status of each user account creation



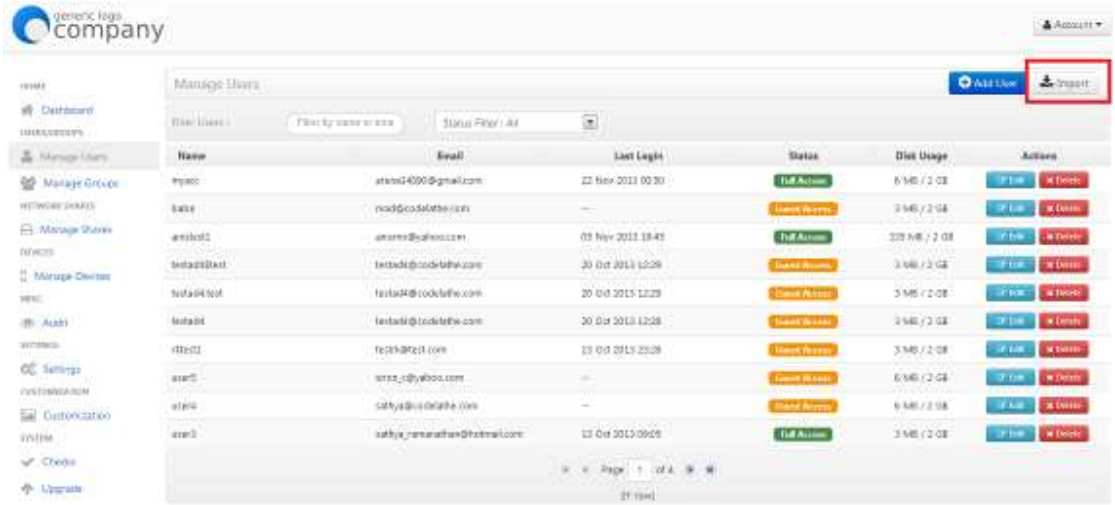


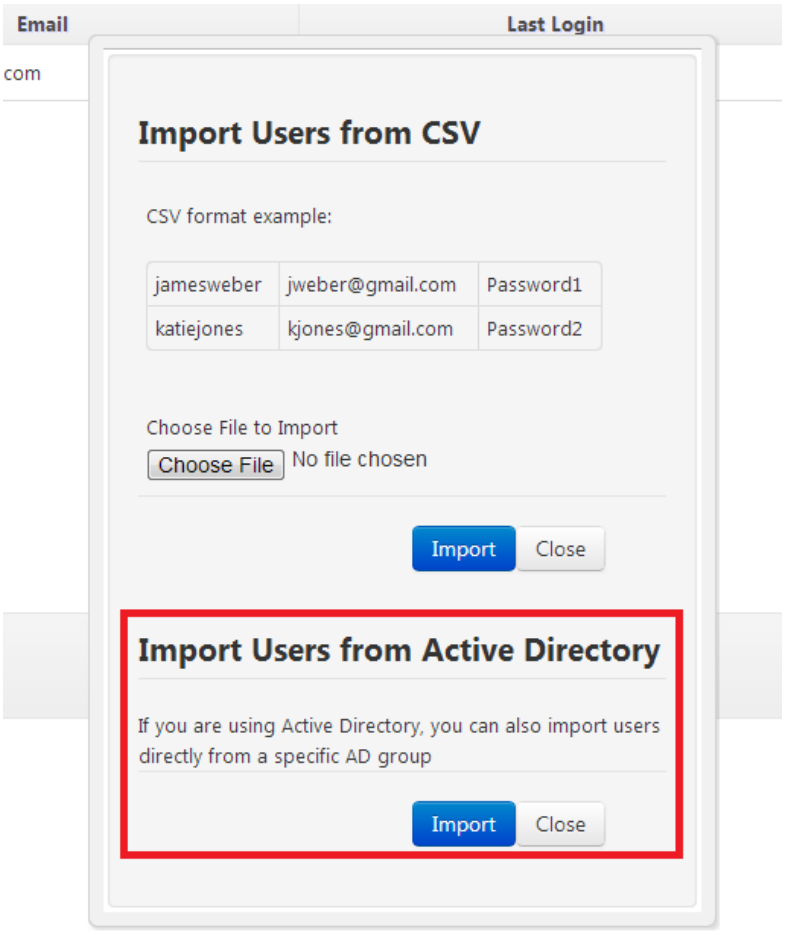
Bulk import of InfoVaultz Users from AD Server

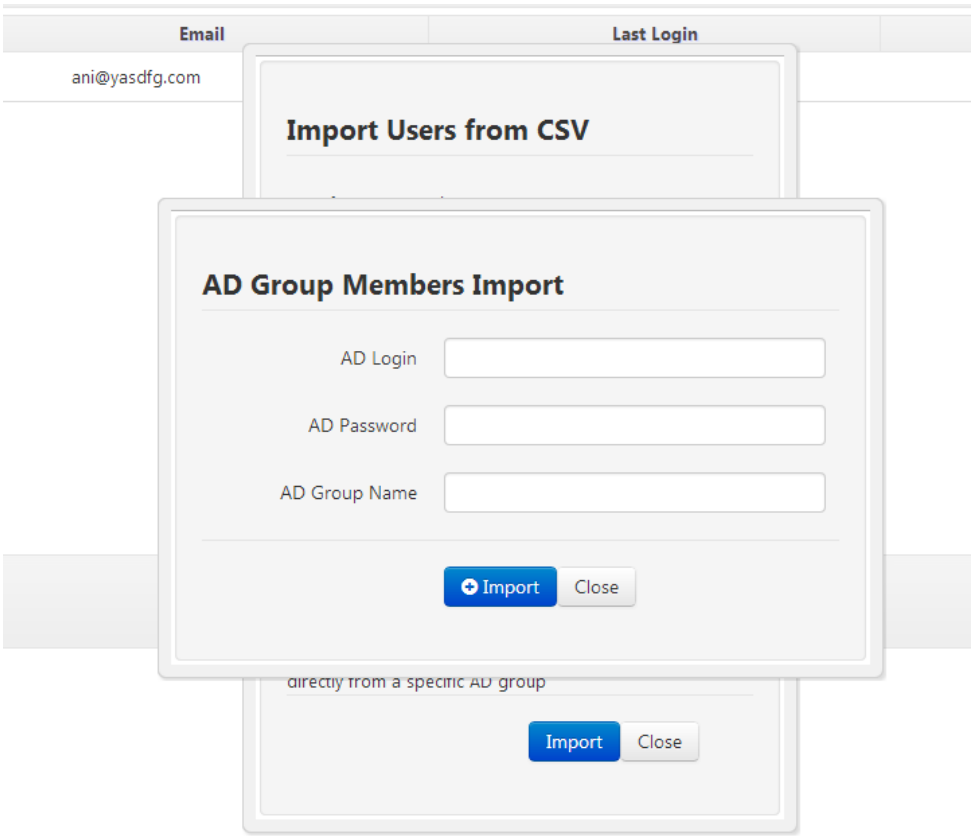
InfoVaultz allows creation of user accounts by importing existing accounts of a AD group from your AD server.

The steps to import users from AD server is

1. Log on to Administration Portal
2. Setup AD configuration or LDAP configuration depending on your requirements.
3. Click on "**Manage Users**" on the left navigation panel
4. Click on "**Import**" button to launch the Import dialog window
5. Under "**Import Users from Active Directory**", click "**Import**"
6. Enter the required credentials and AD group name and Click "**Import**" button


company
Manage Users
Add User
Import
Name
Email
Last Login
Status
Disk Usage
Actions

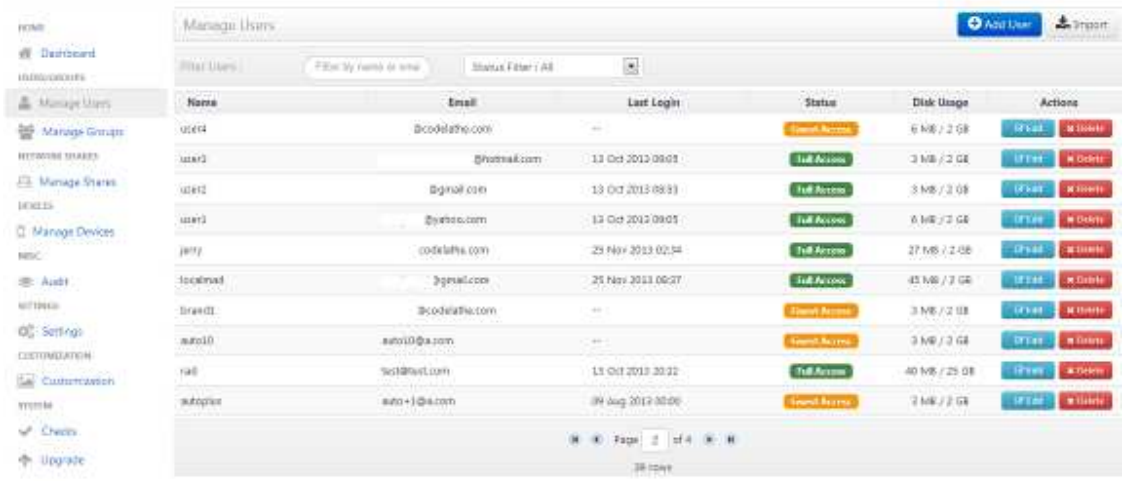

Email
Last Login
com
Import Users from CSV
CSV format example:
jamesweber
jweber@gmail.com
Password1
katiejones
kjones@gmail.com
Password2
Choose File to Import
Choose File
No file chosen
Import
Close
Import Users from Active Directory
If you are using Active Directory, you can also import users directly from a specific AD group
Import
Close



Listing InfoVaultz Users

To list all users in InfoVaultz system,

1. Log on to Administration Portal
2. Click on **Manage User** on the left navigation Panel to list all user
3. For finding a specific user(s), use the Filter box

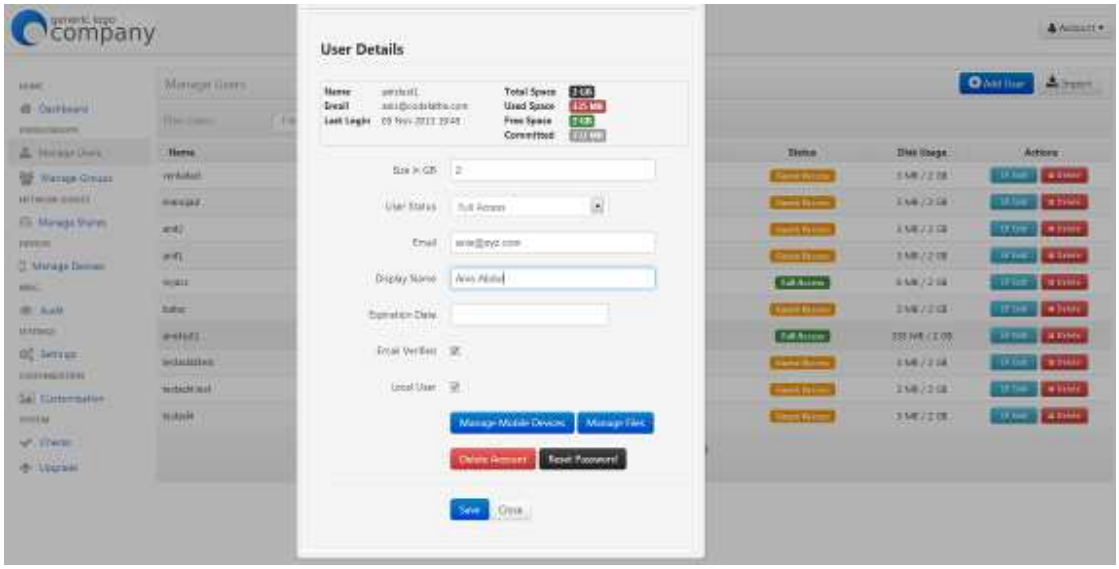


Viewing User Properties

InfoVaultz administrator can see user properties and change as needed.

To see a property of a user, the steps are

1. Log on to Administration Portal
2. Click on "**Manage Users**" in the navigation panel
3. Locate the user in the users list
4. Click on "**Edit**" to display the properties of the user



Property Name	Description
Name	The user id
Email	Email id associated with the account (This can be changted using the "**Email**" text box
Last Login	Last login attempted on this account
Total Space	Quota allocated for this account (This can be changed using "**Size in GB**" text box
Used Space	This is the size of data this user has access to. For example, Guest access users have this value calculated from the amount of data shared to that account
Free Space	Space available
Committed	Space taken by all this user content. This includes space used for **multiple file versions**, **files in Recycle bin** contents, **Partial files in progress** and **Shared files**.
User Status	This is the access level set for this user. This can be changed between "**Full Access**" and "**Guest Access**" as well as "**Disabled State**"
Display Name	This can be set to a user readable name that will be used in various places such as email notifications etc
Expiration Date	If this is date is set, then once the date is past, the account will be disabled automatically.

Email Verified	Indicates if the entered email has been verified. If email is not verified, then account cannot be logged in until the verification is completed.
Local User	Indicates if the user authentication is using "Default Authentication" or "AD/LDAP Authentication"
Manage Mobile Devices	Launch Device Management Portal. Read more here.
Manage Files	Launch user file management portal. Read more here.
Delete Account	Delete this user account. Read more here
Reset Password	Reset the user's password. Read more here

Disabling InfoVaultz User

Disabled User Status

A user account can be disabled by Administrator.

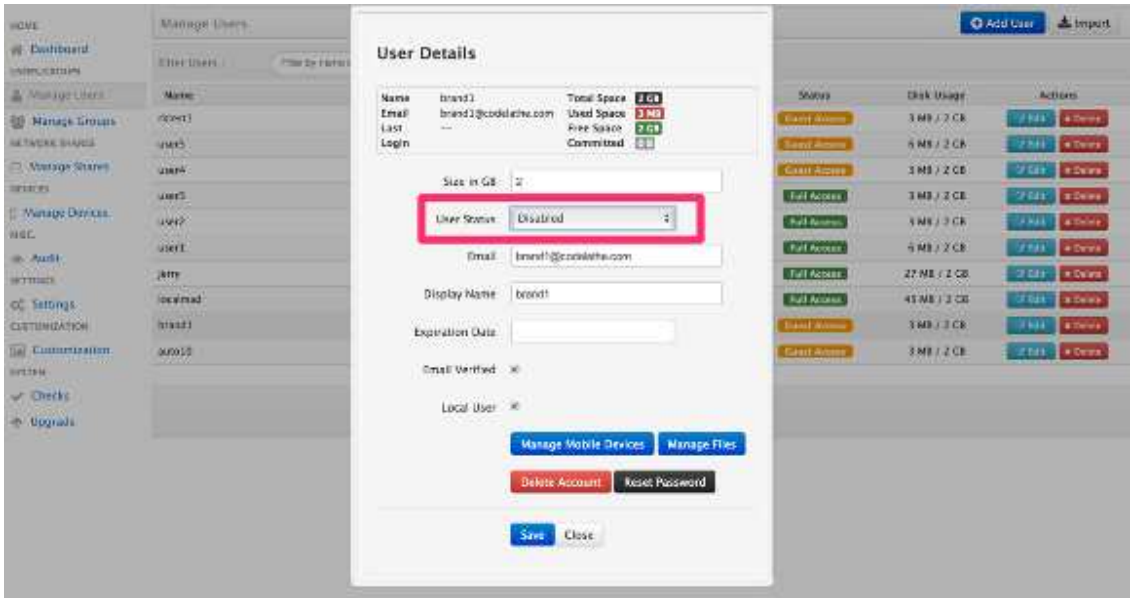
If a user account is disabled, then the following rules apply

	Description
Login using user id from Browser or other clients	Disallowed. User will see explicit message when attempting to log in
User files	Not deleted.
License count	Disabled users count towards consumed license count

Disabling a User

A user can be disabled by Administrator by following the steps listed below

1. Log on to Administration Portal
2. Click on "**Manage Users**" on the left navigation panel
3. Locate the user using Filter box or by browsing the Users list
4. Click on "**Edit**" button in the user row
5. Using the drop down box of **User Status,** change the status to "**Disabled**"
6. Click **Save**.



Deleting a InfoVaultz User

Administrator can delete a InfoVaultz user account.

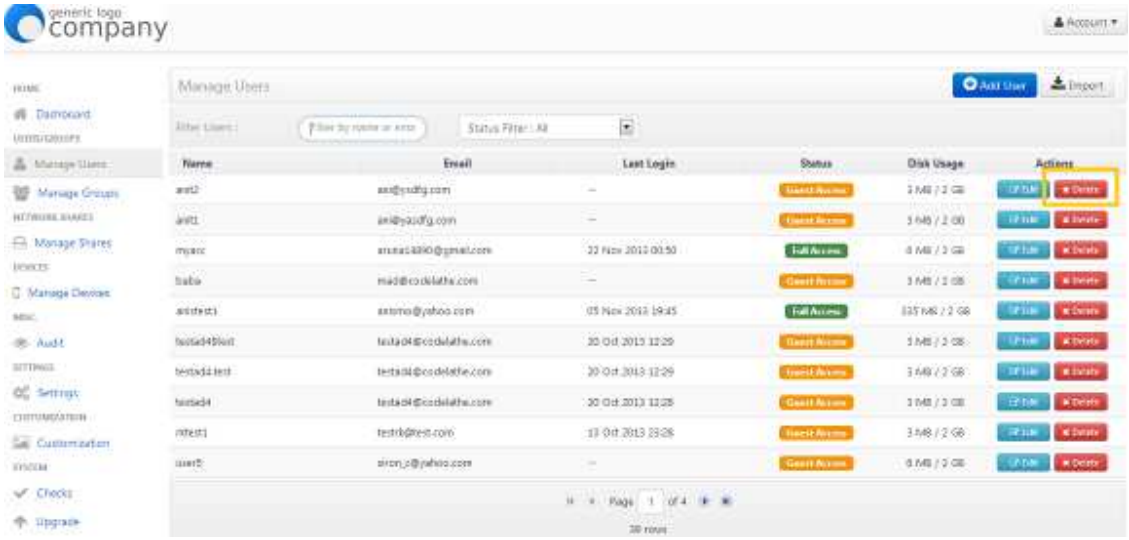
> ⚠ When a user account is deleted
>
> - **All data stored by that user is deleted**
> - **User can no longer log in via browser or connect using sync client or drive client**
> - **License account consumed by the account is released to "Available License" count**
> - **All data shared to that user will no longer be shared**
> - **All data shared by the user will no longer be available**

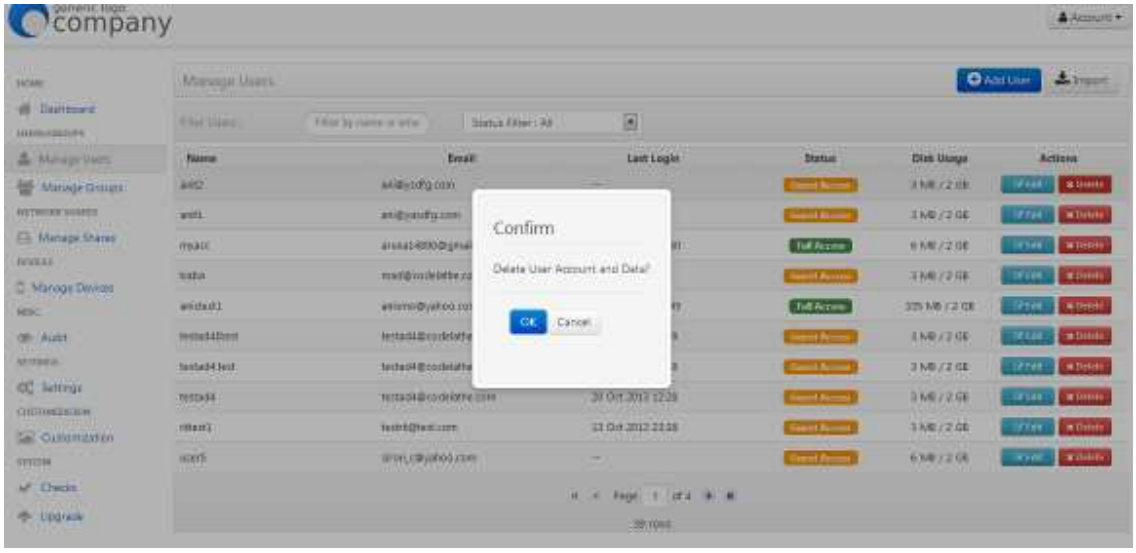
Account Type	Effect
User with "Default Authentication" (Local User)	Local user account is deleted.
User with "AD or LDAP Authentication"	Only the InfoVaultz account will be deleted. No change will be done to the user in the AD or LDAP server.

To delete a user, follow these steps

1. Log on to Administration Portal
2. Click on "**Manage Users**" on the left navigation panel
3. Locate the user to be deleted (using Filter or by paging)
4. Click on "**Delete**" under "Actions" column
5. Click "**OK**" in confirmation dialog

It is also possible to delete an account using the account properties panel.





Reset User Password

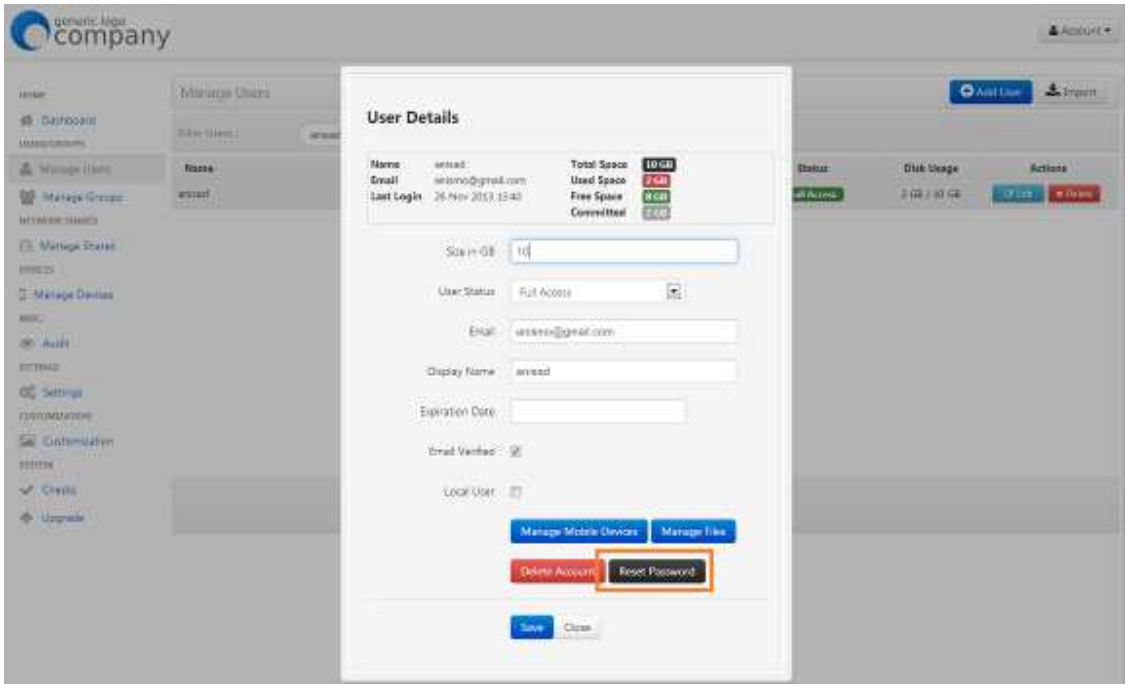
InfoVaultz Administrator can reset password for accounts with Authentication Type set to "Default"

> ⚠ For user accounts with "Authentication Type" set to "AD or LDAP", the password management must be done in AD or LDAP admin portal.

To reset password for user account using "Default" Authentication Type,

1. Log on to Administration Portal
2. Click on "**Manage Users**" on left navigation panel
3. Locate the user to reset the password using "**Filter Users**" or from the user list
4. Click on "**Edit**" for the user row under the "Actions" column to launch the Account Properties

5. Click on "**Reset Password**" Button
6. Click on "**Ok**" for the confirmation dialog
7. A new password will be generated and displayed for that user.



Managing Groups

InfoVaultz Administrator can manage User Groups

Once a user group is created,

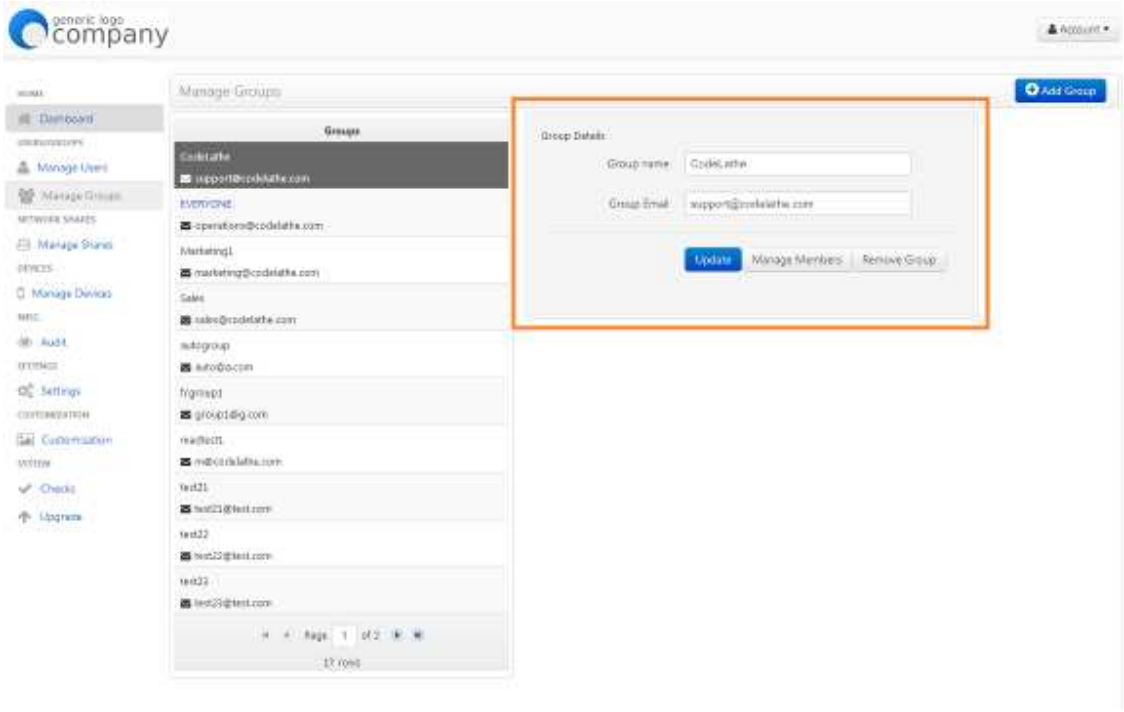
The following operations can be performed

1. Change group details
2. Delete a group
3. View and Change Group members

Change User Group Details

InfoVaultz Administrator can change a group's detail using the following steps

1. Log on to Administration Portal
2. Click on "**Manage Groups**"
3. Click on the desired user group from the list of groups
4. In The Group details panel, you can
    a. Change group name
    b. Change group email
5. Click "**Update**" once the change is complete

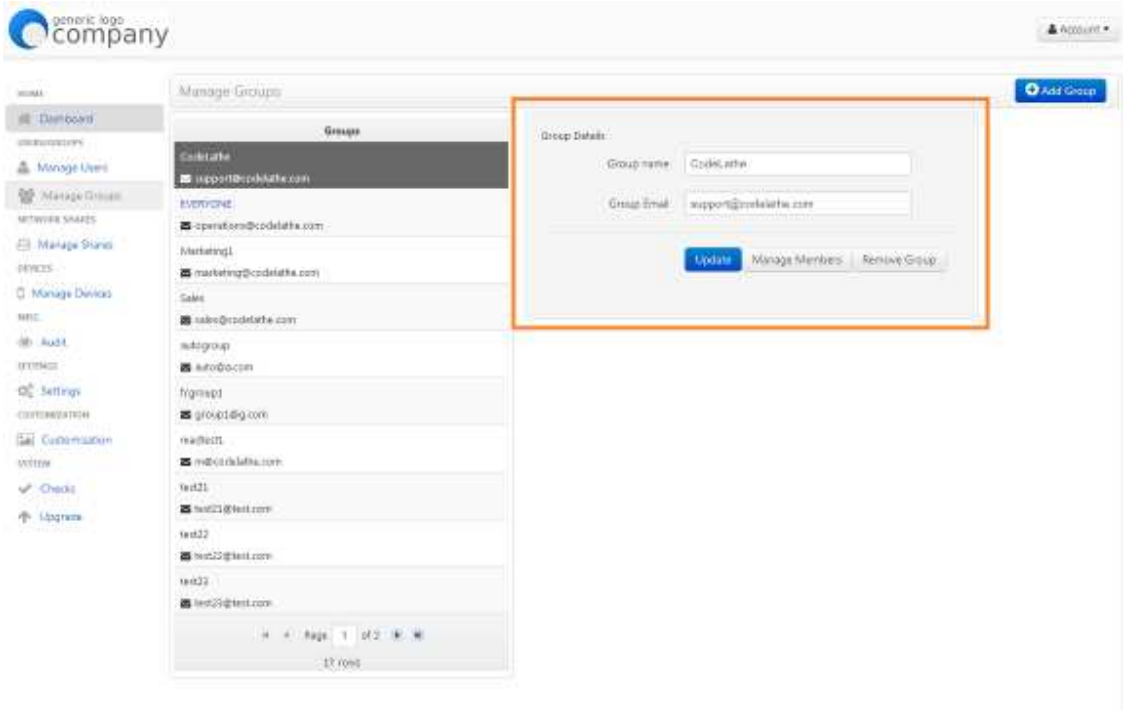


Delete User Group

InfoVaultz Administrator can change a group's detail using the following steps

1. Log on to Administration Portal
2. Click on "**Manage Groups**"
3. Click on the desired user group from the list of groups
4. In The Group details panel, Click "**Remove Group**"
5. Click "**OK**" in the confirmation dialog to complete the operation.

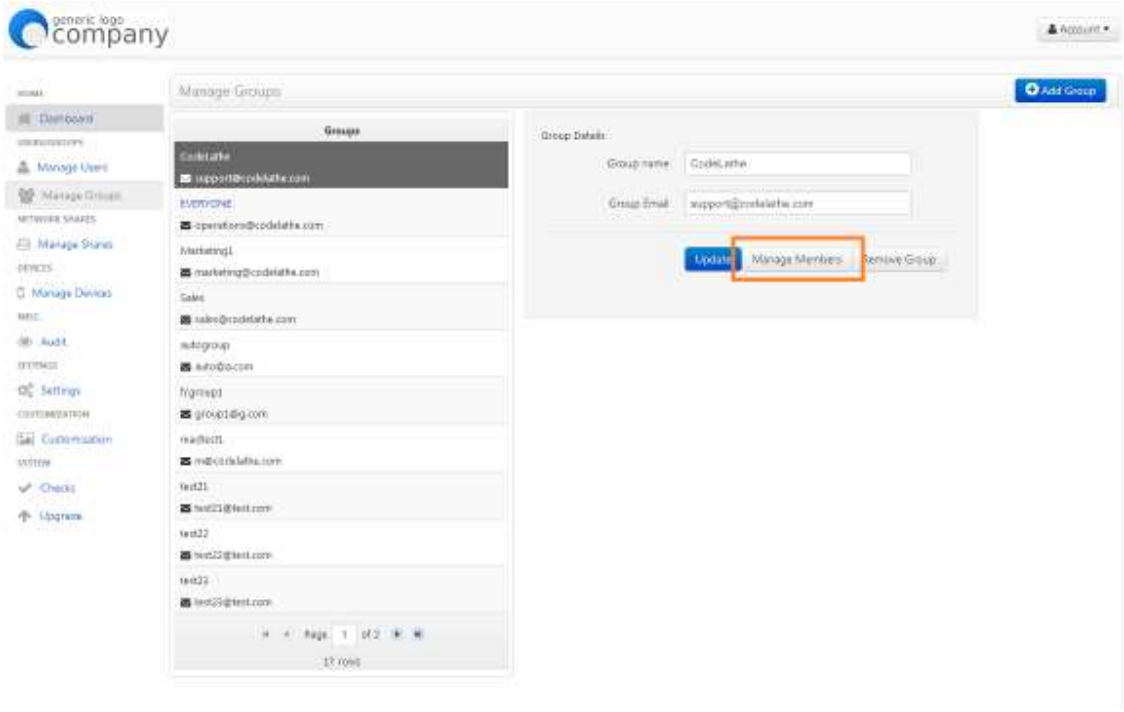
⚠ Once a group is removed, network shares shared with that removed group will no longer be available to the former members of the group

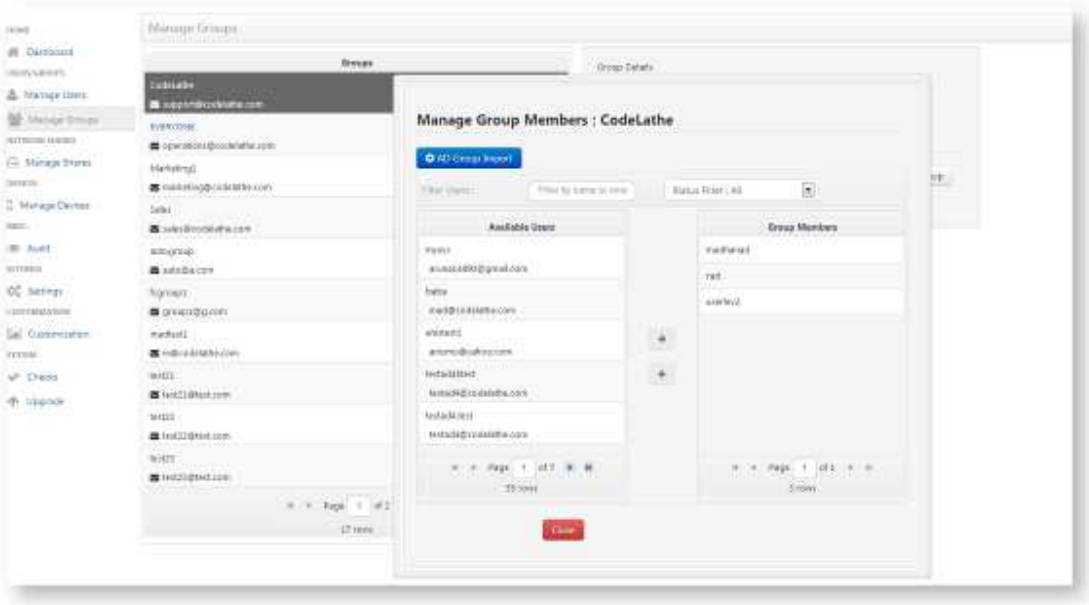


View and Change Group Members

InfoVaultz Administrator can change a group's detail using the following steps

1. Log on to Administration Portal
2. Click on "**Manage Groups**"
3. Click on the desired user group from the list of groups
4. Click on "Manage Members" to launch the members list dialog
5. You can view, add or remove members using the dialog





Managing User Folders and Files

Admin user has complete control on any user file/folder in the InfoVaultz

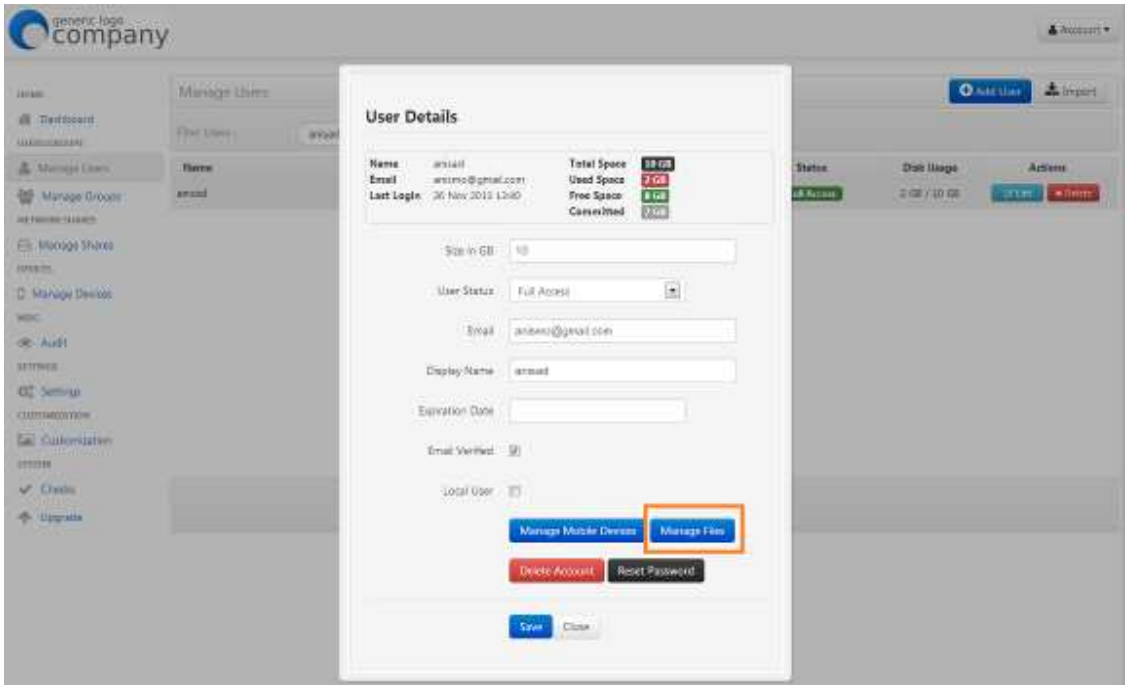
system. The Admin user can View, Download, Copy, Delete, Paste any of the

user files.

The Admin user can also perform copy, move of files and folders between two InfoVaultz users as well.

To manage user folder and files,

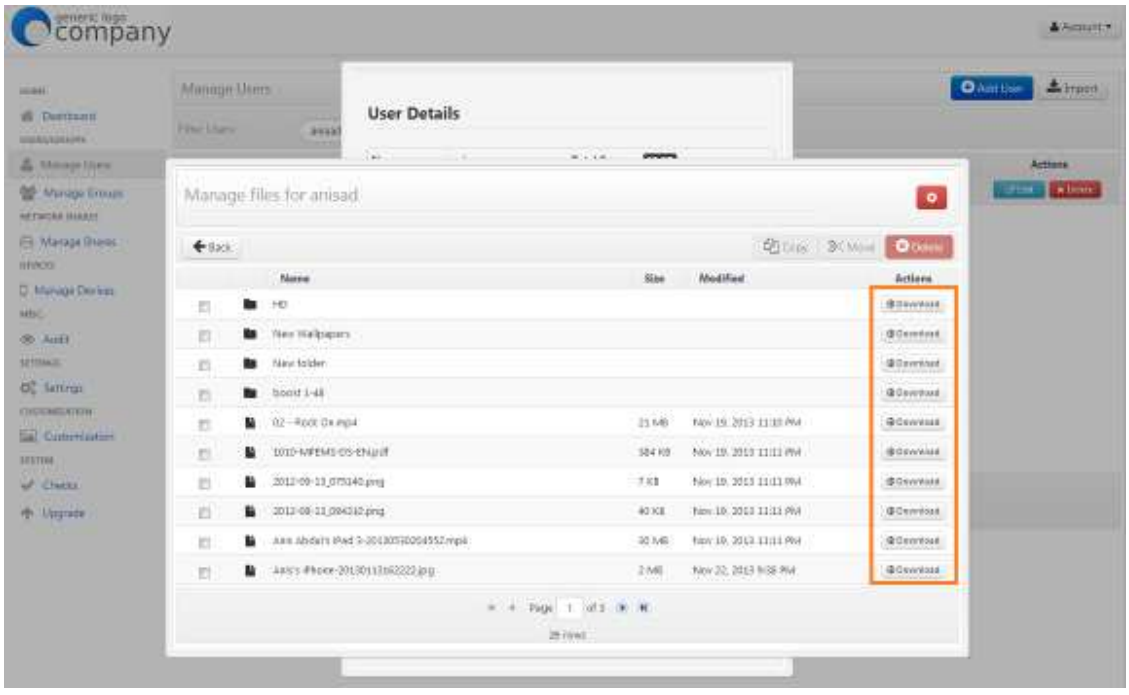
1. Open the user's properties panel
2. Click on "Manage Files" to launch the files management portal for that user



Downloading user files and folders

In the files management portal, click on the "Download" button of the file or folder to download it.

> ⚠ Folders will be zipped first and then downloaded.



Copying, Moving User files

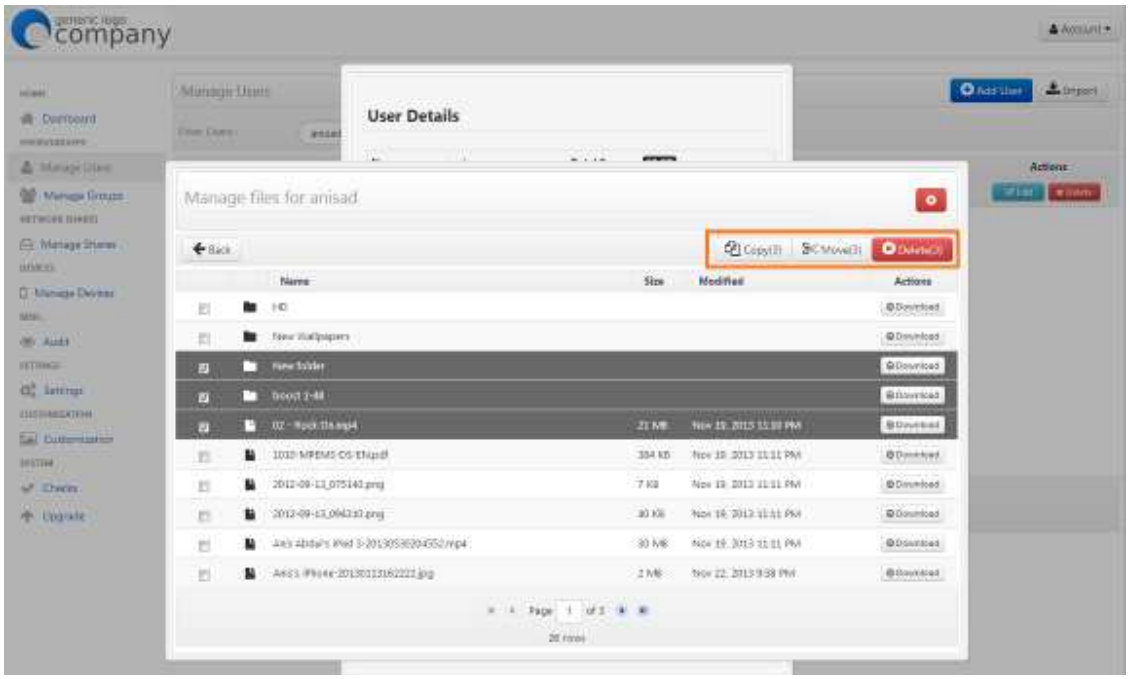
The Administrator can copy or move files between

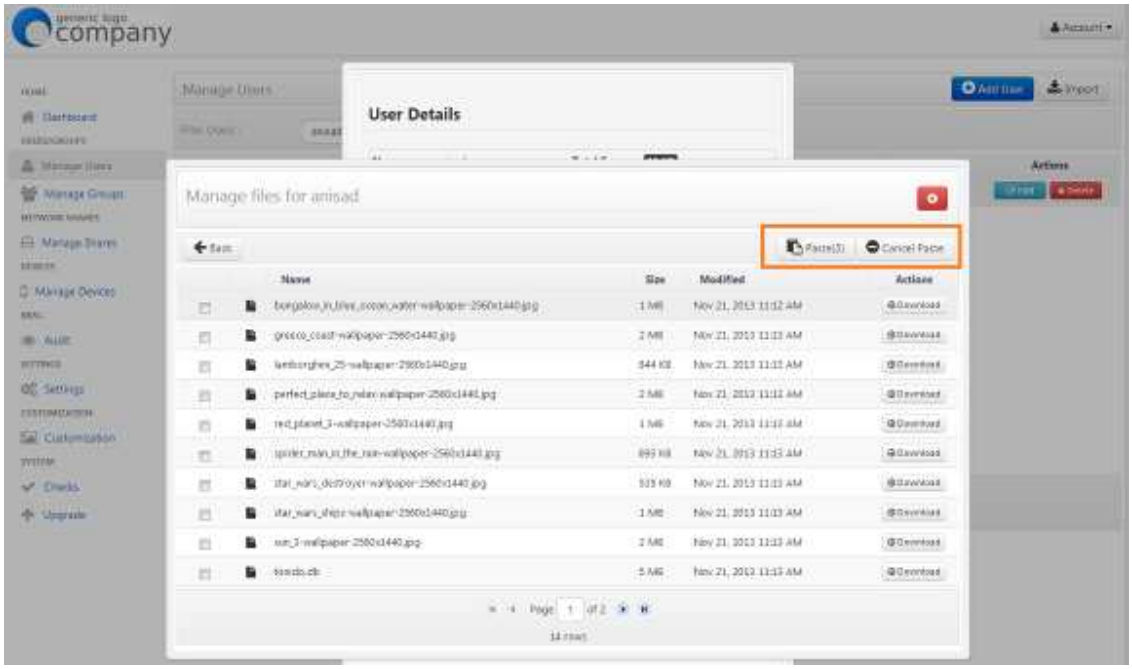
1. Two folder locations of the same user account or
2. Two folder locations of two different user account

The steps to copy or move files are

- In the user files management portal, select the desired files and folders and hit "Copy" or "Move" button, The buttons will then change to "Paste" and "Cancel Paste".
- Navigate to target folder to paste using one of the two ways
  - Navigate to the target folder to paste either in the same user's storage space (or)
  - open the user files management portal of a different user and navigate to the target folder to paste
- Click on "Paste" button to paste the previously selected files

⚠ This action will be logged in Audit log as "Action performed by ADMIN"





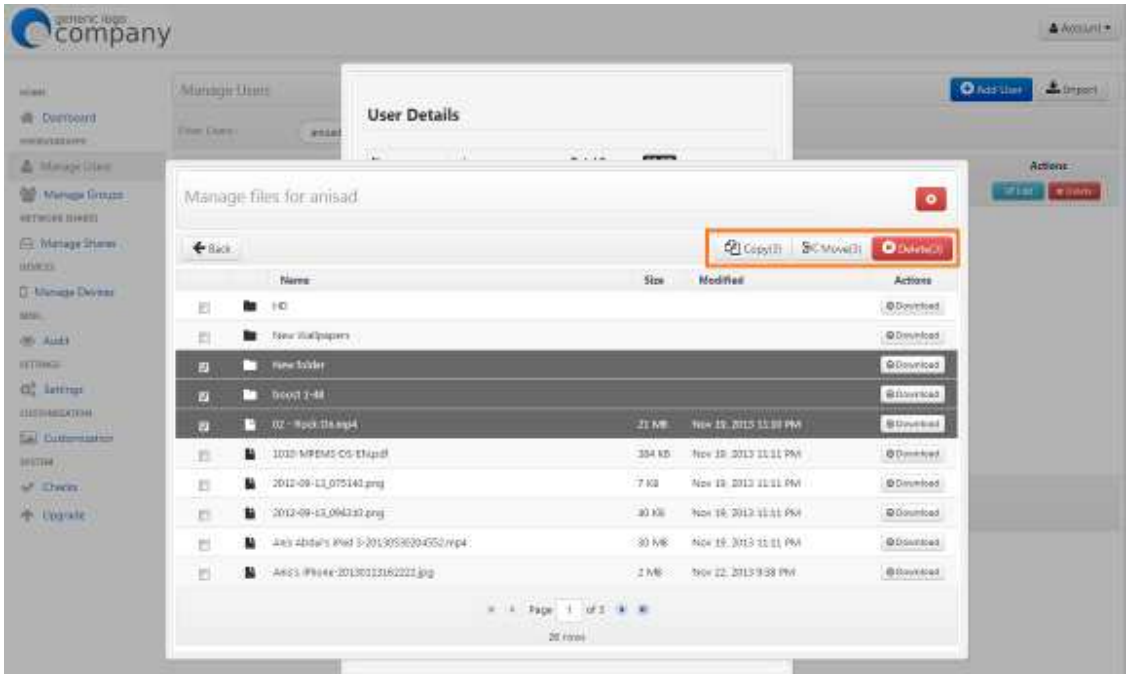
Deleting user files

InfoVaultz Administrator can delete any user's file

To delete a user's file(s) and/or folder(s)

1. Launch the user's file management portal
2. Select the file(s) and/or folder(s)
3. Click "Delete"
4. Click "YES" on confirmation dialog to complete the operation.

⚠ This action will be logged in Audit log as "Operation performed by ADMIN"



Managing Disk space Usage

Administrator can manage the space usage of any InfoVaultz user in the system

The following actions are available

1. View space usage of any user
2. Change space usage quota of any user

Managing Client Devices

InfoVaultz supports administrator management of various clients connecting to the InfoVaultz instance. This feature is called Remote Client Management (RCM)

The following devices can be managed from the Admin Panel

- **InfoVaultz iOS App InfoVaultz**
- **Android App InfoVaultz**
- **Windows Store App**
- **InfoVaultz Sync**
- **InfoVaultz Drive**

> By Default InfoVaultz will not allow non RCM Compliant clients to connect into InfoVaultz service. You can change this behavior in Basic Server Settings page.

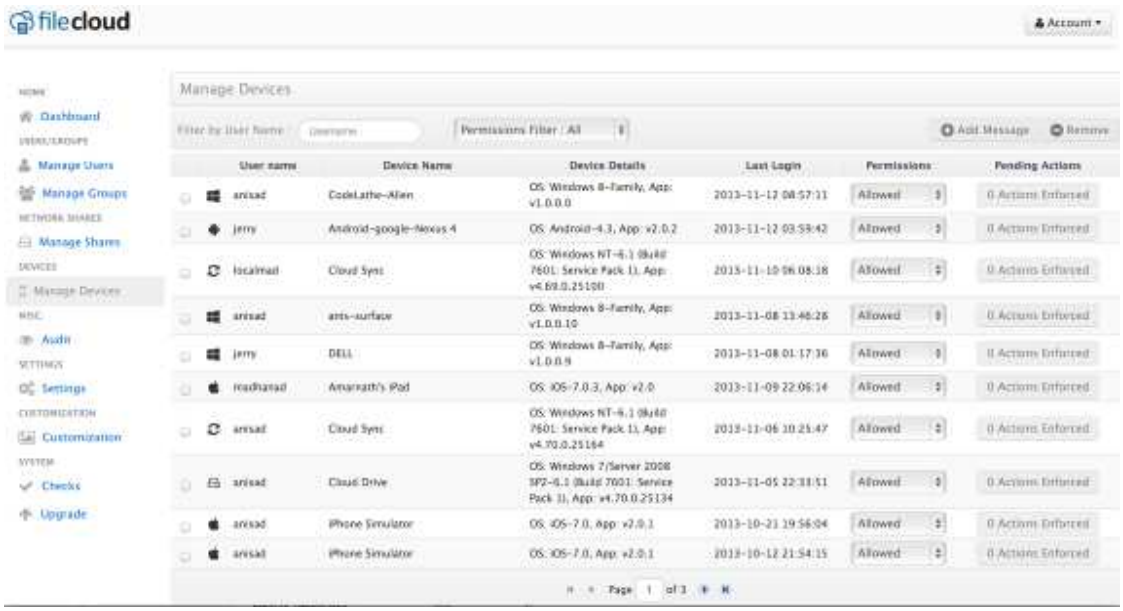
Admin user will be able to see all devices that connected to a InfoVaultz server using the Admin Control Panel.

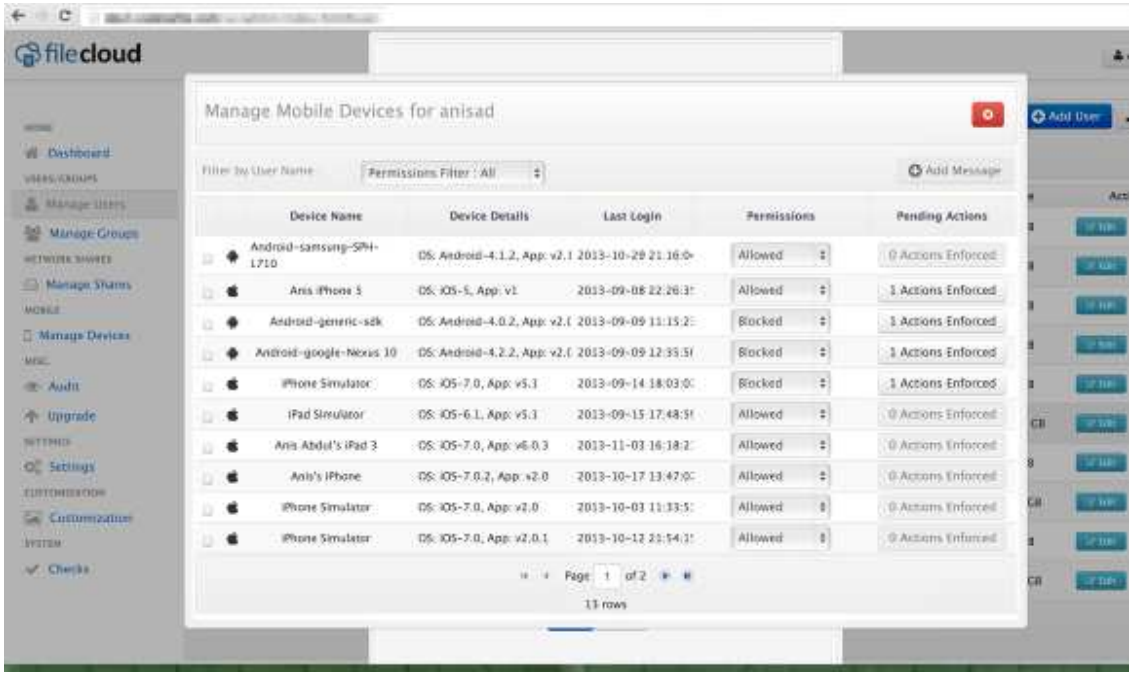
The number of devices are shown in the Summary and the actual list of devices can be seen from the "Manage Devices" menu.

Listing Devices using Admin Control Panel

Admin can open the list of devices to manage using one of the two ways.

1. Log on to Administration Panel
2. Click "**Manage Devices**" on the Admin left control panel (or) Click on "**Manage Mobile Devices**" on a User Properties Panel.





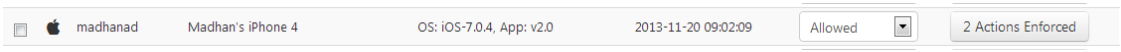
Supported Device Operations

The following operations are available from the Device Management panel.

- **View details of a client device**
- **View and manage actions queued for a client device**
- **Add a message to display in the client device**
- **Remove a previously queued message**
- **Block a device from logging in**
- **Block a device and force wipe of application data**
- **Remove client record from the InfoVaultz system**

View Details of a client device

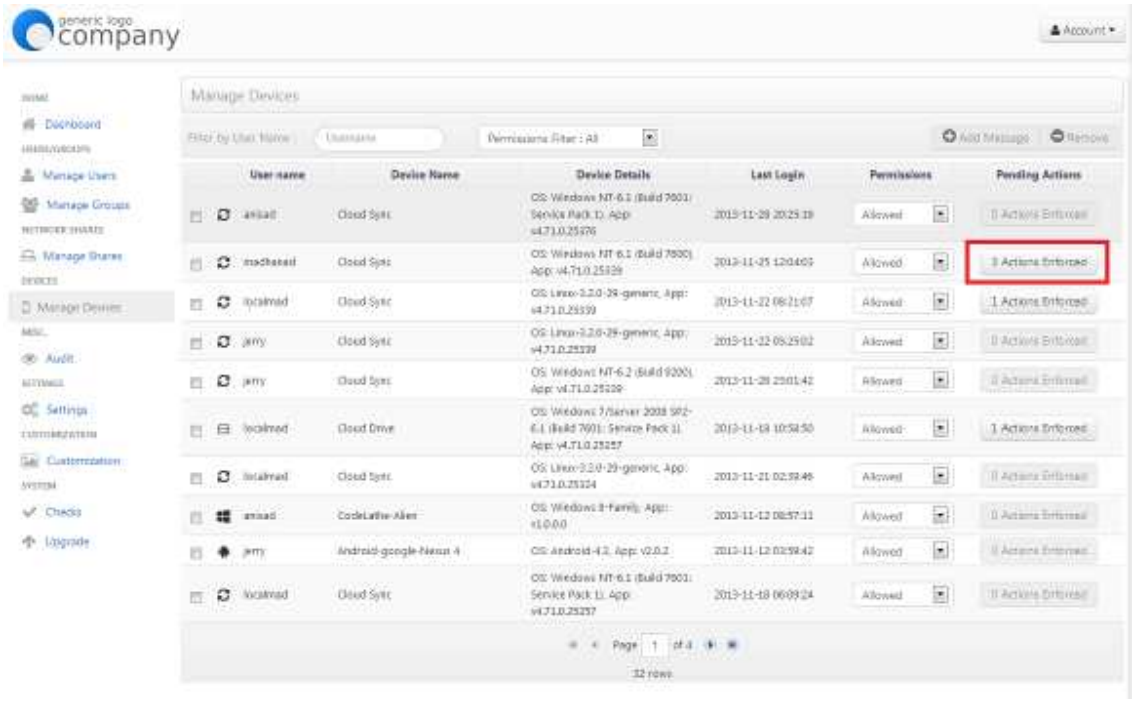
Column	Details
Column 0	Checkbox to check the client device record to add message or remove the client
Column 1	Client device icon
User name	The user id used by the client device to connect
Device name	The device name setup by the client device. This can be generic like "Cloud Sync" or "Client Drive" or specific like "Anis' iPhone 5"
Device Details	This field provides OS type, OS version and the Client App's version.
Last Login	The last time this device connected to the InfoVaultz server
Permissions	The current enforced login permission. This can be changed to block or block and remote wipe
Pending Actions	The list of queued actions for that client device (A number of messages etc)

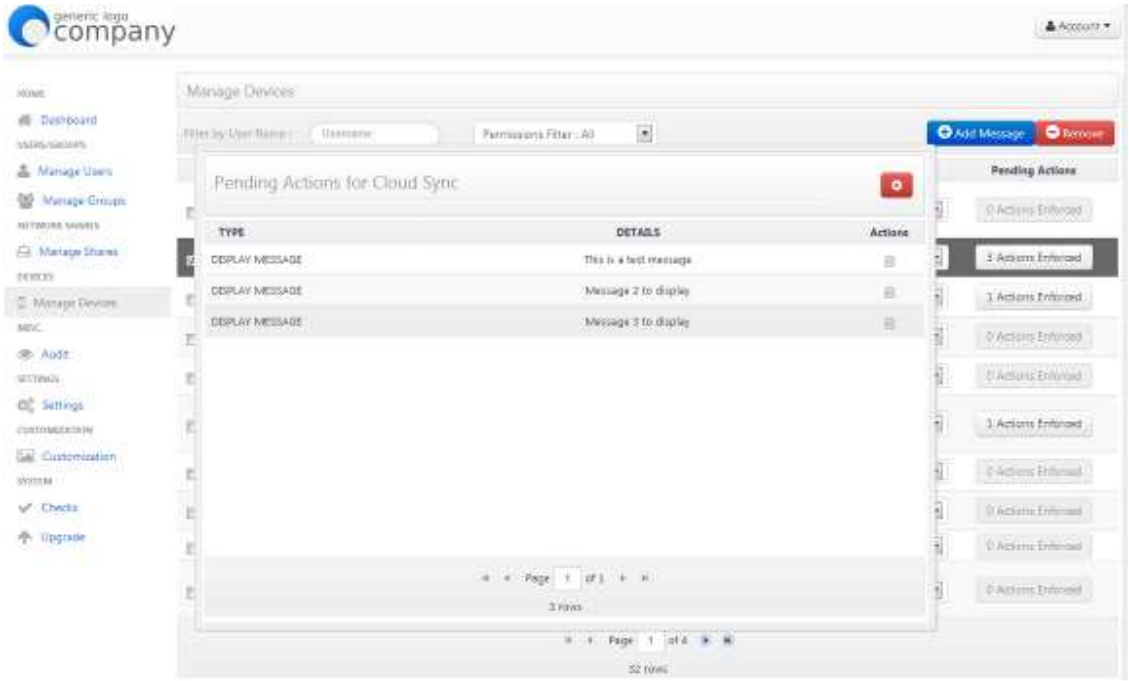


View and Manage Actions queued for a client device

If a message is queued to a device, it is possible to view them using the Admin panel

1. Log on to Administration Panel
2. Click on the "**Manage Devices**" on the left navigation panel
3. Locate the record to view the queued action
4. Click on the button in "**Pending Actions**" column
5. This will display the list of pending actions for that device
6. Any queued action can be deleted from the pending actions list by clicking the "trash can" icon under **Actions** column in that list





Add message to display in the client device

Admin can display a short message on the remote client using the "Add message" feature.

The entered message(s) will be displayed when the remote client is connected to the InfoVaultz instance. If more than one message is queued to a device, they will be

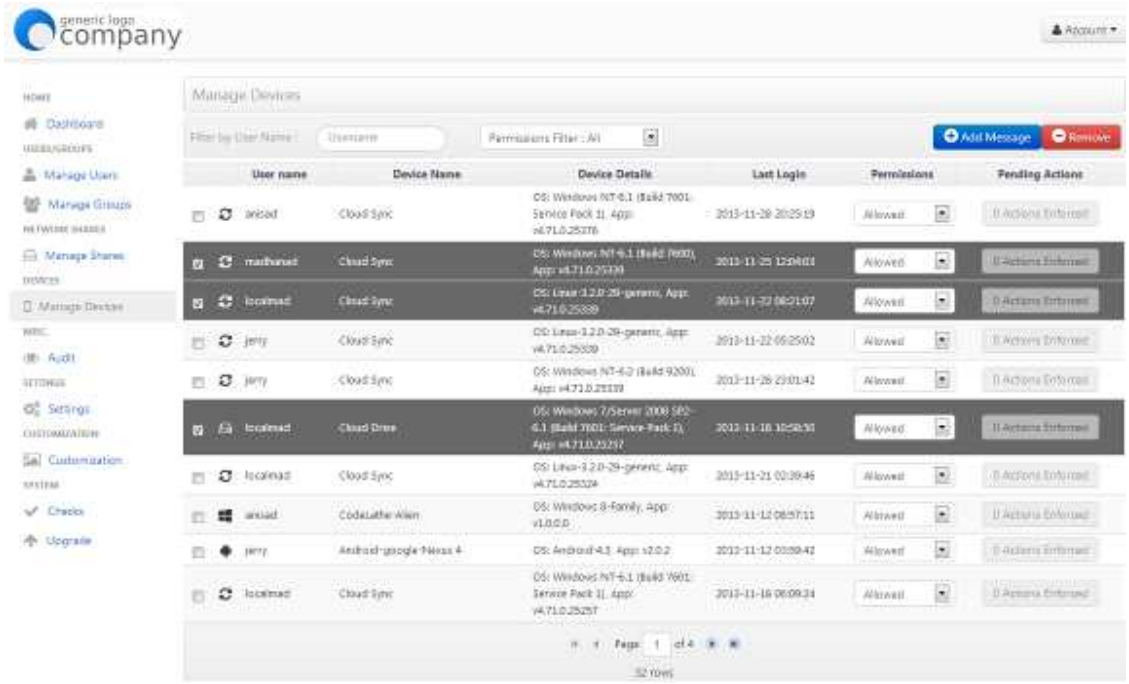
displayed in the order it was entered. The messages will be shown only once per client and during

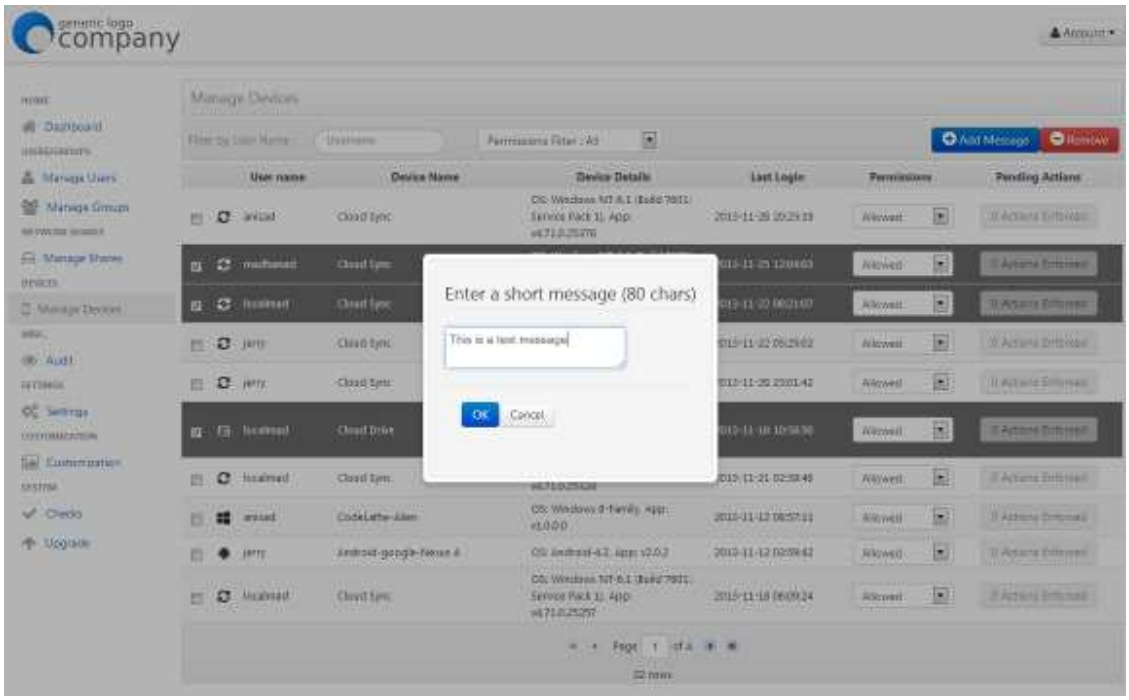
> Message will be shown

- When the client connects to the InfoVaultz server (as a part of login operation)
- If the client is already connected, then it will retrieve the message periodically and display it to the user

Steps to add message

1. Log on Administration Panel
2. Select one or more device using the checkbox on the left most column of a device record
3. Click on "**Add Message**" button





Blocking and Remote Wiping Client Device

InfoVaultz's RCM function allows the Administrator to selectively block a specific client device from logging into the InfoVaultz server. In addition to Blocking a Client Device from logging in, Administrator can also wipe InfoVaultz folders in the remote device.

When a client device is blocked (or blocked with remote wipe action), it will be executed one of the following two ways

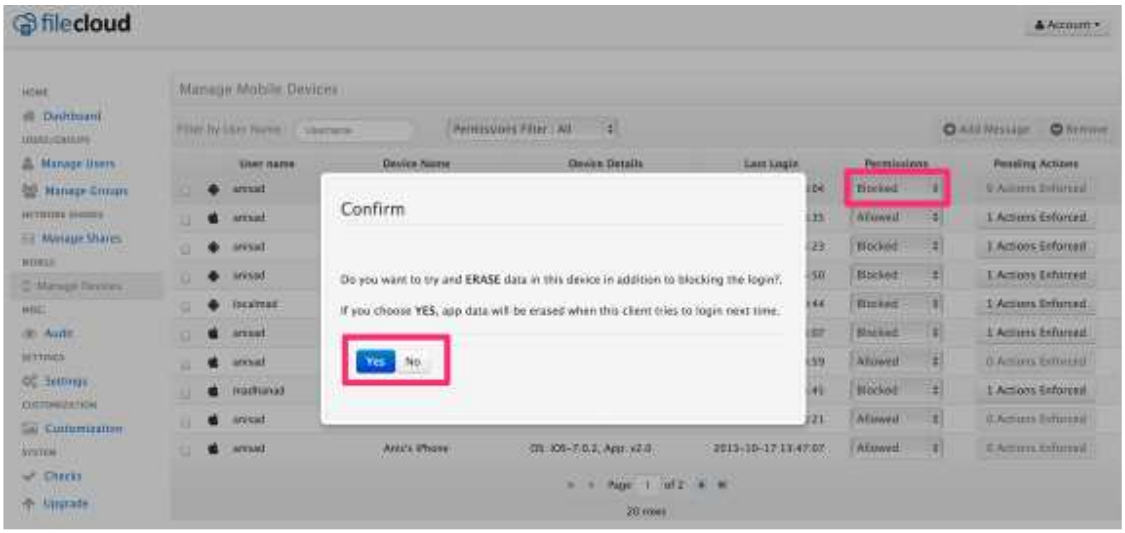
1. If the client is not connected, the block (and remote wipe) will happen when it tries to log into the server
2. If the client is connected, the block and remotw wipe will occur and the client will automatically exit out.

Steps to block (but no wipe remote data) in a client device

1. Log on to Administration Portal
2. Click on "**Manage Devices**" on the left navigation panel
3. Locate the client device to be blocked and under the "**Permissions**" column, Change the value to "**Blocked**"
4. In the "**Confirm**" dialog, select "**NO**" to just block but not remote wipe the client device

Steps to block and wipe remote data in a client device

1. Log on to Administration Portal
2. Click on "**Manage Devices**" on the left navigation panel
3. Locate the client device to be blocked and under the "**Permissions**" column, Change the value to "**Blocked**"
4. In the "**Confirm**" dialog, select "**YES**" to just block but not remote wipe the client device



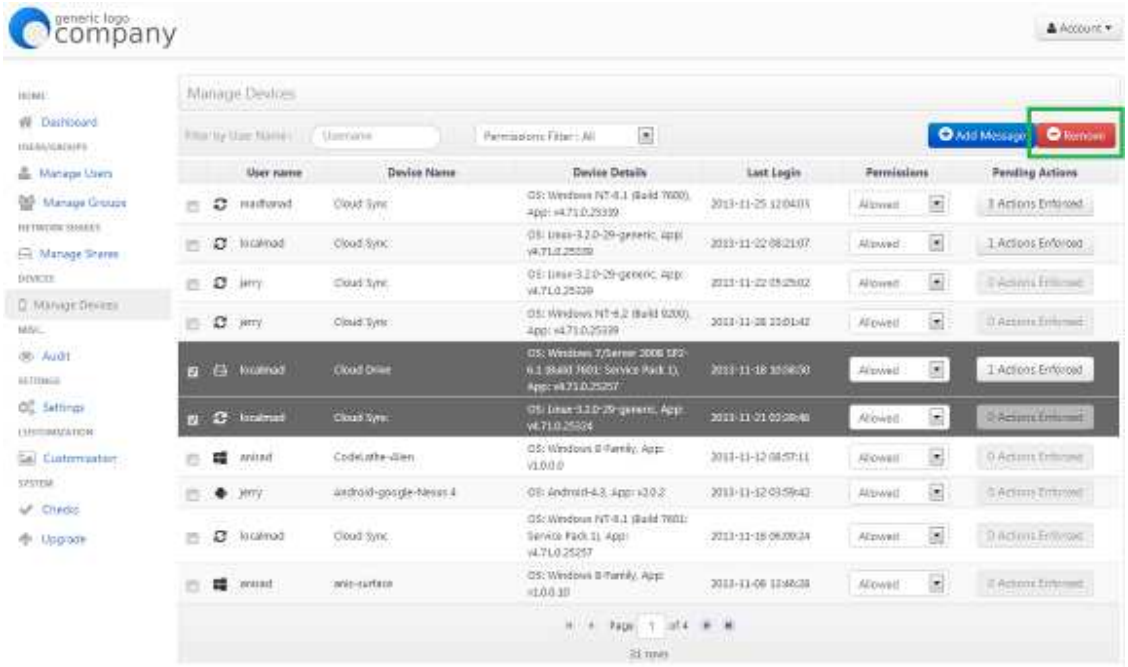
Remove Client Device Record from the system

It is possible to remove a client record from the InfoVaultz system.

This can be due a a number of reasons such as the userid is no longer valid and the associated client record is no longer needed to be manage etc

1. Log on to Administration Portal

2. Click on the "**Manage Devices**"
3. Locate the device record(s) to remove and select them
4. Click on the "**Remove**" button on top right.



Upgrading InfoVaultz

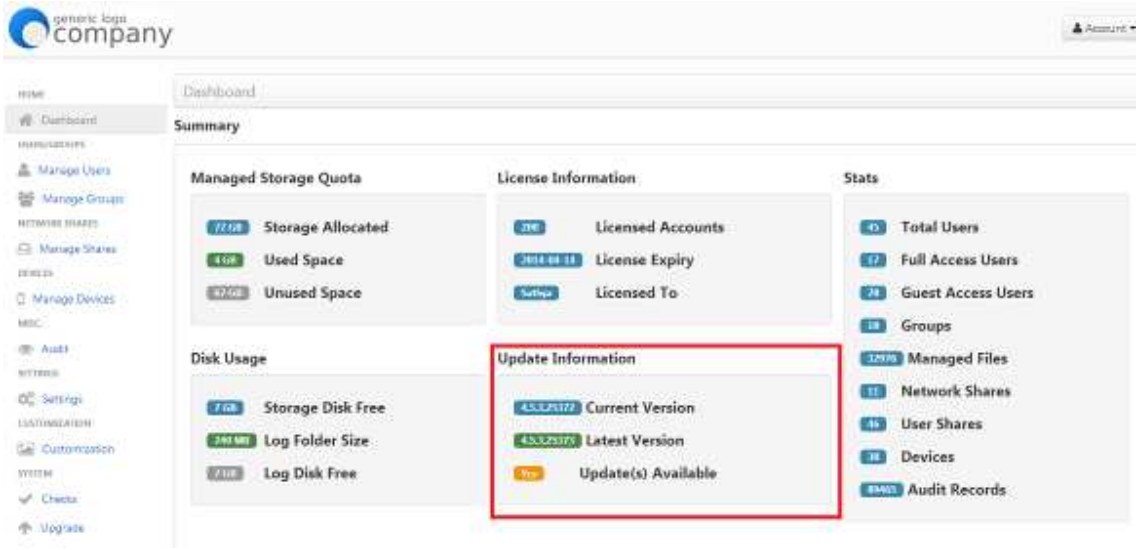
Introduction

Updates to InfoVaultz containing bug fixes, security patches and new features are released as necessary. These updates can be applied to an existing installation from within the administrator UI.

Getting notified of new InfoVaultz releases

Generally, new InfoVaultz release availability will be notified in two ways:

1. By subscribing to the InfoVaultz Mailing List
2. By seeing the version update available in the InfoVaultz Admin Dashboard



Step 1: Backup

> ⚠ Before any updating current InfoVaultz installation, it is important to backup your data

Based on the installation environment, choose one of the following links to perform backup:

InfoVaultz installation environment	Backup steps
Linux OS and installation with backup tool	Linux tool backup
Linux OS and installation without backup tool	Linux manual backup
Windows OS and installation without backup tool	Windows manual backup

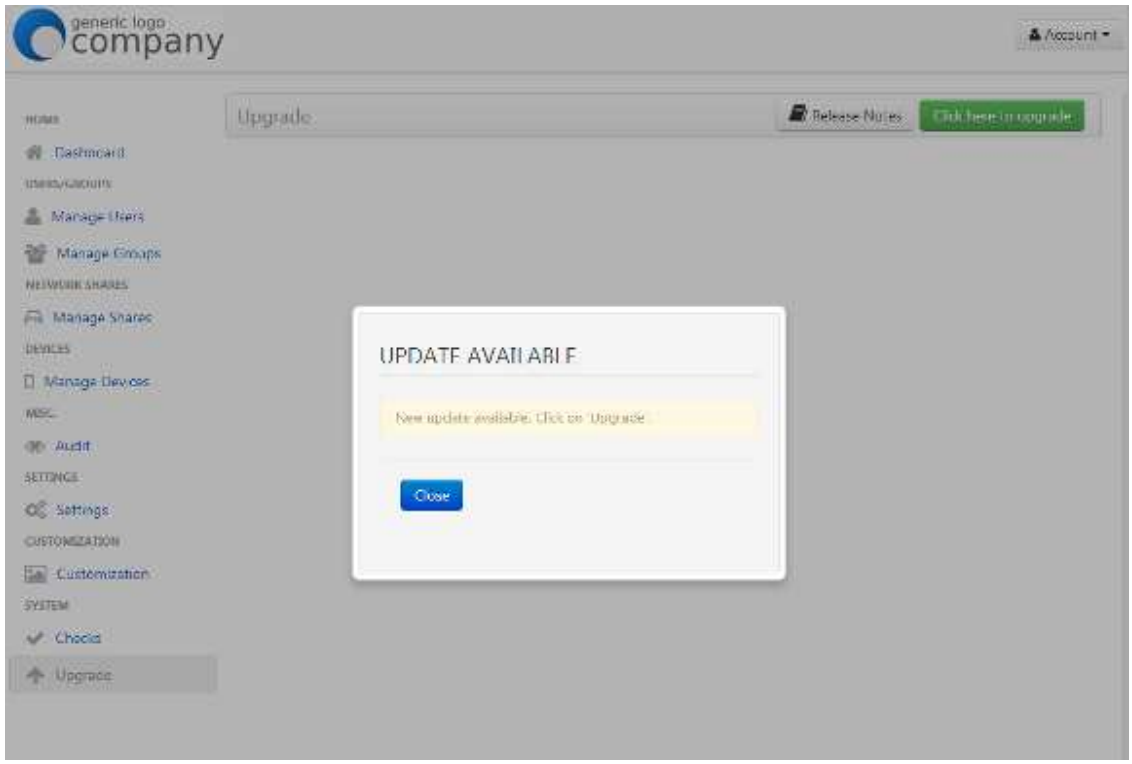
Step 3: Performing update

1. Login into the admin UI. Select "Upgrade" from the left-side navigation panel.

2. In the upgrade screen, click on "Click here to upgrade" button.

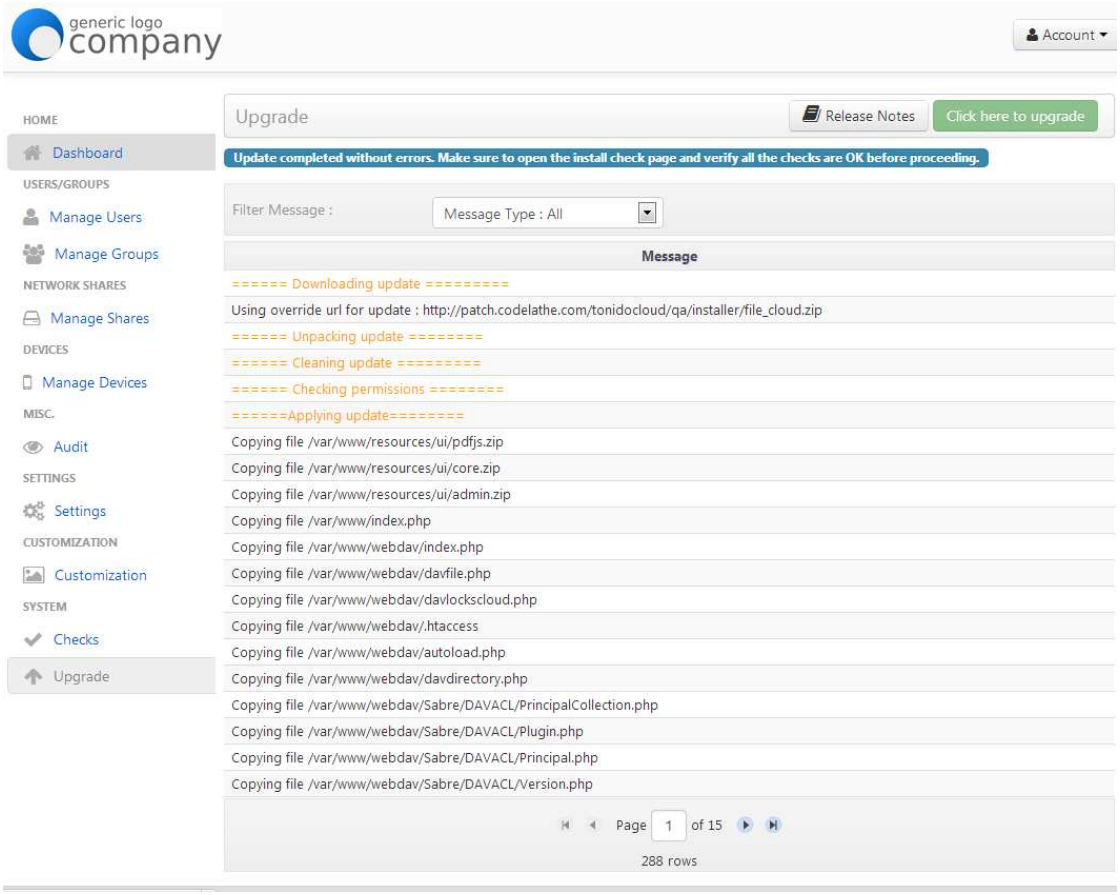
3. If there are no new updates available, no additional actions required.

4. If there are any new updates available, a popup will be shown with new update information.



5. Click on the "Click here to Upgrade" button to start the upgrade process.

6. The upgrade process will check for perform the upgrade and a report will be generated after the update process is completed



7. Once the upgrade is completed, you will be redirected to the install verification page at http://site/install
8. Once it is verified that the checks are complete, refresh the browser UI (Ctrl + F5) to get the latest updated User Interface.

Audit Logs

InfoVaultz has extensive Auditing support and every operation in InfoVaultz is logged into the Audit logs

The following actions are logged in Audit Logs

Actions
New Account creation
Client Login operation
Folder browse
Search actions
Upload file
Download file/folder
File/Folder Creation
File/Folder Share

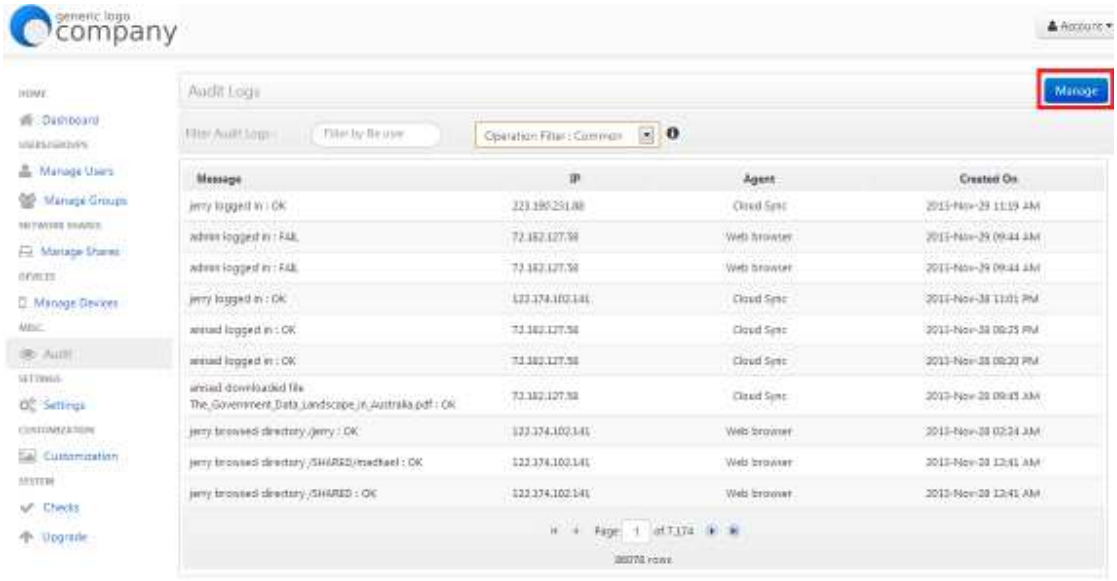
File/Folder Copy
File/Folder Move
File/Folder Delete
All other APIs (Such as thumbnail reads, Setting Favorites, Listing Shares)

Viewing Audit Logs

To view the audit log, the steps are

1. Log into Administration portal
2. Click on "**Audit Logs**" on the left navigation panel

> ⚠ The Operation Filter can be changed from "Common" to "All" to see more fine grained list of all audit logs. The "Common" filter option will list common operations such as "new account creation, account login, file/folder create, upload/download file or folder "



Audit Record Details

Every audit record will have the following information

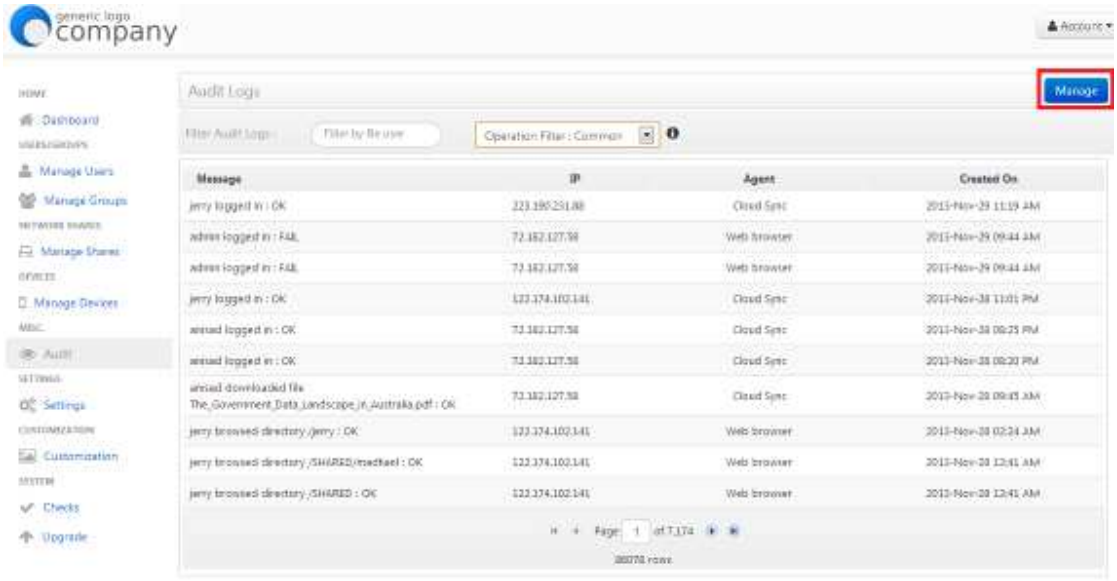
Value	Description
Message	The descriptive message for the audit record
IP	The IP from which the call was performed
Agent	Indicates wether it was from a Webbrowser, or iOS app etc
Created On	The timestamp when the call was performed

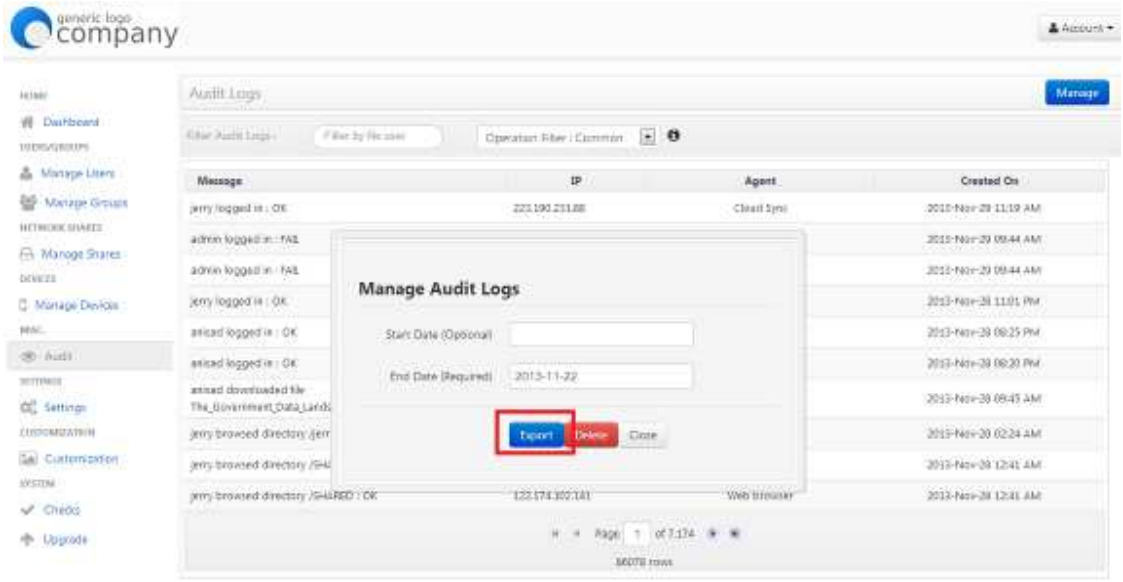
Message	IP	Agent	Created On
jerry browsed directory /SHARED : OK	122.174.102.141	Web browser	2013-Nov-28 12:41 AM
anisad logged in : OK	72.182.127.58	Cloud Sync	2013-Nov-28 08:25 PM

Exporting Audit Logs

The audit logs can be exported as CSV files. To export the audit logs

1. Log on to Administrator portal
2. Click on "**Audit**" in the left navigation portal
3. Click on "Manage" button to launch the audit logs management dialog
4. Enter the Start and end date and click "**Export**"button

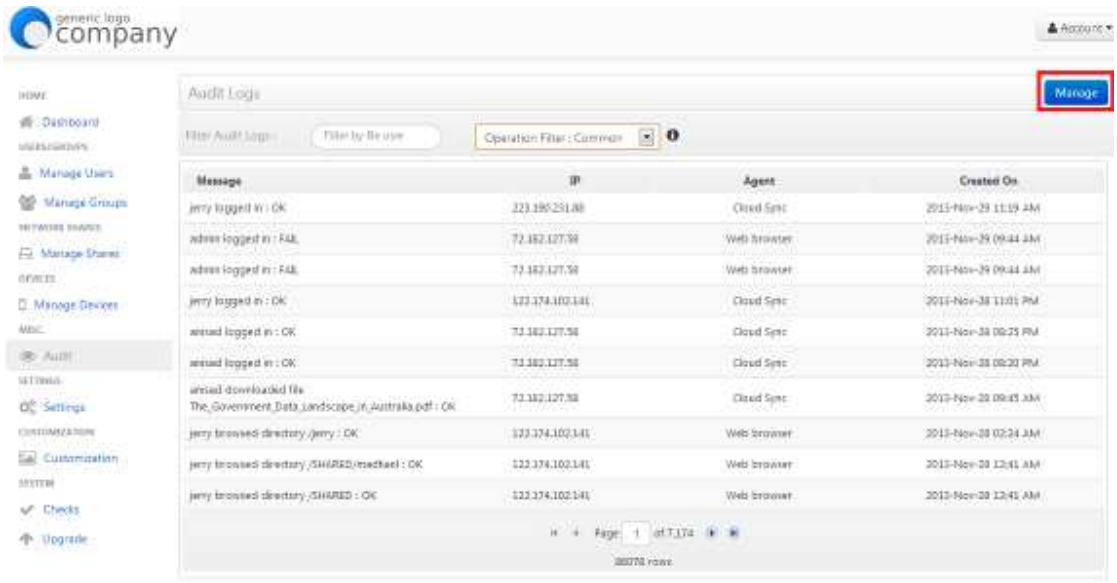


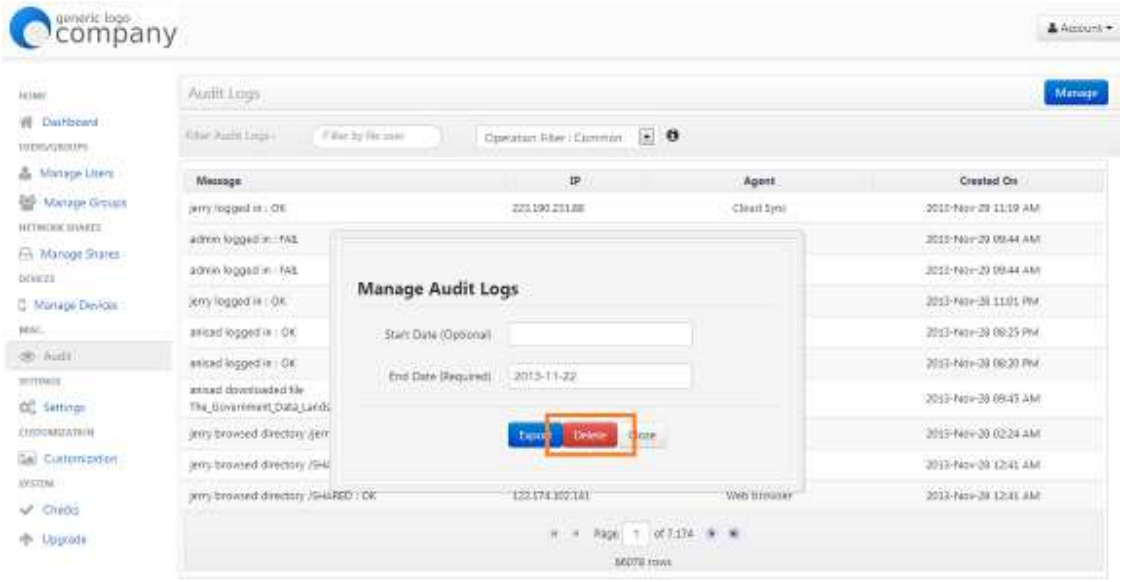


Trimming Audit Logs

The audit logs can be trimmed (Typically after exporting it to CSV) to reduce size taken up in the database. To trim the audit logs

1. Log on to Administrator portal
2. Click on "**Audit**" in the left navigation portal
3. Click on "Manage" button to launch the audit logs management dialog
4. Enter the Start and end date and click "**Delete**"button to trim the logs





Backing up InfoVaultz Data

InfoVaultz Backup and Restore - Linux Tool

InfoVaultz is bundled with necessary tool to perform full backups of your cloud installation ie., both files and

database. Some of the features of these backup scripts:

- can be run at anytime manually from command line
- can be part of an automated system like cron job.
- can be run on a live cloud installation (though its safer to do backup of cloud in maintenance mode).
- can backup to local or remote linux targets.

In this section you can learn some basic tasks such as

1. Initializing backup system
2. Adding a new host to the backup system
3. Removing a target
4. Creating new backups
5. Removing existing backups
6. Listing existing backups
7. Restoring a backup

Terminologies

Here are some basic terminologies used to explain the backup tool.

Backup Target: Host where the backups are stored.

Backup Directory: Directory under which the backups are stored.

Initializing Backup Tool

Backup tool has to be initialized before it can be used to backup your cloud installation. This initialization needs to be done only once and tool will automatically initialize itself upon first use. During this initialization process, the tool performs an important routine that the user needs to be aware of.

SSH Key Generation : The tool generates a RSA ssh key pair during initialization. This key pair will be used to communicate between the tool and backup targets. This enables tool to communicate with the backup target without prompting for password every time. These are encrypted keys and are safer than entering passwords everytime for communication. Also the tool exchanges the key with the localhost and will be used to run even commands on the local host.

When the backup tool is run without any options, it initializes the tool on first run and then displays help. Further runs only displays help. Following section shows a session initializing the backup tool.

Initializing backup tool

```
madhan@li111-150:~$ cd /var/www/resources/backup
madhan@li111-150:/var/www/resources/backup$ sudo chmod +x backup.sh
madhan@li111-150:/var/www/resources/backup$ sudo ./backup.sh
Feb 18 01:26:05 : Initializing backup system
Feb 18 01:26:05 : Generating ssh encryption keys
Generating public/private rsa key pair.
Your identification has been saved in ./keys/id_rsa.
Your public key has been saved in ./keys/id_rsa.pub.
The key fingerprint is:
f4:cd:e8:ff:1e:db:e6:b4:7f:f7:da:d4:02:16:dd:ba root@li111-150
The key's randomart image is:
+--[ RSA 2048]----+
| |
| . . |
| . . . .|
| . . + . . |
| S o = . |
| . . . ..|
| . E +|
| . O=|
| .o==@|
+-----------------+
Feb 18 01:26:06 : Please enter local user to store backups :
madhan
Feb 18 01:26:22 : Exchanging ssh keys with host 127.0.0.1
madhan@127.0.0.1's password:
Feb 18 01:26:30 : Successfully initialized localhost to store backups
Script to backup infovaultz data
Usage :
 sudo /path/backup.sh <command>
 where <command> could be on of the following:
  addtgt <user> <host> <tgtdir>  - Adds the <tgtdir> in machine <user>@<host> as a
valid backup directory
 rmtgt <index>    - Removes the backup target at specified index.
        If index parameter is missing, a list of available targets will be shown to
choose one from.
  lstgts     - Lists available backup directories
 crtbkup <index>   - Create a new backup of infovaultz at specified backup target
index.
        If index parameter is missing, a list of available targets will be shown to
choose one from.
 lstbkups <index>   - List all backups under the specified target index.
       If index parameter is missing, a list of available targets will be shown to
choose one from.
 rmbkup <index1> <index2>  - Removes index2 directory from index1 backup target.
          If index parameters is missing, a lists of available targets and directories
will be shown to choose one from.
 resbkup <index1> <index2>  - Restores index2 directory from index1 backup target.
        If index parameters is missing, a lists of available targets and directories
will be shown to choose one from.
```

Add Backup Target

The backup tool has to have atleast one backup target before it can create and store backups. Even if you plan to store the backups on the local

system, you still need to the local host as a backup target. When multiple backup target directories are added to the tool, the ssh keys are exchanged only the first time.

To add a backup target you need

- a user
- ip address of the remote host.
- a directory to store backups (and the above user should have write permissions)

Use the option addtgt to add a new backup target to the tool. The following snippet shows commands to add 2 backup targets.

Local host (madhan, 127.0.0.1, /backup)

Adding a localhost target

```
madhan@li111-150:/var/www/resources/backup$ sudo ./backup.sh addtgt madhan 127.0.0.1
/cloudbackup/
Feb 18 02:20:23 : Adding backup target : madhan@127.0.0.1:/cloudbackup/
Feb 18 02:20:25 : Added backup target : madhan@127.0.0.1:/cloudbackup
```

Remote host (cloud, 192.168.1.148, /backup)

Adding a remote host target

```
madhan@li111-150:/var/www/resources/backup$ sudo ./backup.sh addtgt cloud
192.168.1.148 /cloudbackup/
Feb 17 18:31:47 : Adding backup target : cloud@192.168.1.148:/cloudbackup/
Feb 17 18:31:47 : Exchanging ssh keys with host 192.168.1.148
cloud@192.168.1.148's password:
Feb 17 18:31:51 : Added backup target : cloud@192.168.1.148:/cloudbackup
```

Remove Backup Target

To remove a backup target use the option rmtgt. This option lists the available backup targets and prompts for the target to be deleted. Upon entering the target number, the tool deletes the target. When a target is deleted, the tool just removes pointer to the target from its internal list. The physical directory is not deleted. This allows admins to add the same target at later point of time with all the backups intact.

Note: The target number can also be specified from the command line

Removing a target

```
madhan@li111-150:/var/www/resources/backup$  sudo ./backup.sh rmtgt
 No Targets
------------------------------------------------------------
 0) madhan@127.0.0.1:/cloudbackup
 1) cloud@192.168.1.148:/cloudbackup
------------------------------------------------------------
Feb 17 18:41:20 : Select a backup target to remove from the above list :
1
Feb 17 18:41:37 : Selected backup target cloud@192.168.1.148:/cloudbackup
Feb 17 18:41:37 : Backup target removed : cloud@192.168.1.148:/cloudbackup
```

List Backup Targets

To list the available backup targets in the tool use the option lstgts.

Listing targets

```
madhan@li111-150:/var/www/resources/backup$  sudo ./backup.sh lstgts
 No Targets
------------------------------------------------------------
 0) madhan@127.0.0.1:/cloudbackup
------------------------------------------------------------
```

Create New Backup

To create a new backup use the option crtbkup.

Create Backup

```
madhan@li111-150:/var/www/resources/backup$ sudo ./backup.sh crtbkup
Feb 18 03:22:19 : Creating backup
 No Targets
------------------------------------------------------------
 0) madhan@127.0.0.1:/cloudbackup
------------------------------------------------------------
Select a backup target from the above list : 0
Feb 18 03:22:21 : Selected backup target madhan@127.0.0.1:/cloudbackup
sending incremental file list
5108a8b6bff4d/
5108a8b6bff4d/5108a8b6c26d2/
5108a8b6bff4d/5108a8b6c26d2/510d2ecb07217.dat
 42.55K 100% 9.33MB/s 0:00:00 (xfer#1, to-check=54/57)
5108a8b6bff4d/5108a8b6c26d2/510d2ecb08d48.dat

.....

5108a8b6bff4d/5108a8b6c26d2/51132eeb6a45a.dat
 174.84K 100% 241.84kB/s 0:00:00 (xfer#55, to-check=0/57)

sent 60.89M bytes received 1.06K bytes 24.36M bytes/sec
total size is 60.88M speedup is 1.00
tonidobak.log 100% 20KB 19.8KB/s 00:00
```

Note: The target number can also be specified from the command line.

List Backups

To list backups available on a particular backup target directory use the option lstbkups .

Listing Backups

```
madhan@li111-150:/var/www/resources/backup$ sudo ./backup.sh lstbkups
 No Targets
------------------------------------------------------------
 0) madhan@127.0.0.1:/cloudbackup
------------------------------------------------------------
Feb 18 03:26:39 : Select a target from above to list available backups :
0
Feb 18 03:27:03 : Selected backup target madhan@127.0.0.1:/cloudbackup
  No         Date                          Files         Size              Status
Path
--------------------------------------------------------------------------------------------
-------------------------
  0)         03:22:21 2013-02-18          59M          44               COMPLETE
/cloudbackup/1361157741
--------------------------------------------------------------------------------------------
-------------------------
```

Note: The target number can also be specified from the command line.

Delete Backup

To delete a backup target directory use the option rmbkup.

Deleting Backups

```
madhan@li111-150:/var/www/resources/backup$ sudo ./backup.sh rmbkup
 No Targets
------------------------------------------------------------
 0) madhan@127.0.0.1:/cloudbackup
------------------------------------------------------------
Feb 18 03:31:25 : Select a target from above to list available backups
0
Feb 18 03:31:28 : Selected backup target madhan@127.0.0.1:/cloudbackup
  No         Date                          Files         Size              Status
Path
--------------------------------------------------------------------------------------------
-------------------------
  0)         03:22:21 2013-02-18          59M          44               COMPLETE
/cloudbackup/1361157741
--------------------------------------------------------------------------------------------
-------------------------
Feb 18 03:31:30 : Select a backup directory
0
Feb 18 03:31:34 : Selected backup path /cloudbackup/1361157741
madhan@li111-150:/var/www/resources/backup$ sudo ./backup.sh lstbkups 0
Feb 18 03:32:01 : Selected backup target madhan@127.0.0.1:/cloudbackup
  No         Date                          Files         Size              Status
Path
--------------------------------------------------------------------------------------------
-------------------------
--------------------------------------------------------------------------------------------
-------------------------
```

Note: The backup target number and backup target directory number can also be specified from the command line.

Restore Backup

To restore a backup from a particular backup target directory use the option resbkup.

Note: When a backup is restored, the cloud service will be stopped to restore the backup. Upon restoring the snapshot the service will be started again.

> **Restoring Backups**

```
madhan@li111-150:/var/www/resources/backup$ sudo ./backup.sh resbkup
  No         Targets
------------------------------------------------------------
  0)         madhan@127.0.0.1:/cloudbackup
------------------------------------------------------------
Feb 18 03:42:00 : Select a target from above to list available backups
0
Feb 18 03:42:05 : Selected backup target madhan@127.0.0.1:/cloudbackup
  No         Date                          Files         Size              Status
Path
-------------------------------------------------------------------------------------------
-------------------------
  0)         03:40:16 2013-02-18          59M          44               COMPLETE
/cloudbackup/1361158816
-------------------------------------------------------------------------------------------
-------------------------
Feb 18 03:42:07 : Select a backup directory
0
Feb 18 03:42:15 : Selected backup path /cloudbackup/1361158816
Rather than invoking init scripts through /etc/init.d, use the service(8)
utility, e.g. service mongodb stop

Since the script you are attempting to invoke has been converted to an
Upstart job, you may also use the stop(8) utility, e.g. stop mongodb
mongodb stop/waiting
Rather than invoking init scripts through /etc/init.d, use the service(8)
utility, e.g. service mongodb start

Since the script you are attempting to invoke has been converted to an
Upstart job, you may also use the start(8) utility, e.g. start mongodb
mongodb start/running, process 17363
```

Note: The backup target number and backup target directory number can also be specified from the command line.

InfoVaultz Backup and Restore - Linux Manual

InfoVaultz can be backed up and restored on Linux following these manual steps.

While performing the backup/restore, these are the important file categories that should be backed up/restored:

- cloud cloud files.
- cloud database.
- cloud user files.

Backup

High level steps to backup InfoVaultz in windows:

1. Stop webserver

2. Backup configuration files
3. Backup database.
4. Backup user files.
5. Start webserver

Stop Webserver and MongoDB

Before backup is performed, stop the apache webserver and mongodb. This prevents any client from adding/removing files while the backup is in progress.

> **Stopping services**

```
# sudo /etc/init.d/apache2 stop
# sudo /etc/init.d/mongodb stop
```

Please use equivalent commands applicable for your OS distro.

Backup InfoVaultz installation

Once the apache server is stopped, make a copy of entire cloud installation. The cloud installation is typically under /var/www/ directory.

> **Backing up InfoVaultz installation**

```
# mkdir -p /InfoVaultzbackup/www
# sudo cp -dprv /var/www/* /InfoVaultzbackup/www
```

If your installation uses a different directory, update the above commands accordingly.

Backup database

Once the mongodb is stopped, backup the database files.

> **Backing up InfoVaultz database.**

```
# mkdir -p /InfoVaultzbackup/db
# sudo cp -dprv /var/lib/mongodb/* /InfoVaultzbackup/db
```

Check your mongodb installation to make sure /var/lib/mongodb is the correct database path.

Backup user files

To backup user files, make a copy of the entire directory specified for the property 'TONIDO_LOCALSTORAGE_TOPLEVELFOLDER' in /var/www/config/localstorageconfig.php.

Note: In the following case, the entire "/opt/InfoVaultz/data" directory has to be backed up.

Sample localstorage config file

```
<?php

/*********************************************************************************
 Copyright(c) 2013 CodeLathe LLC. All rights Reserved.
  This file is part of Infovaultz http://www.tonido.com
 *********************************************************************************/

define("TONIDO_LOCALSTORAGE_TOPLEVELFOLDER", "/opt/InfoVaultz/data");

define("TONIDO_LOCALSTORAGE_DBSERVER", "mongodb://localhost:27017");
define("TONIDO_LOCALSTORAGE_DBNAME", "tonidostoragedb");

define("TONIDO_LOCALSTORAGE_FILESPERCONTAINER", 5000 );
define("TONIDO_LOCALSTORAGE_FOLDERSPERCONTAINER", 5000 );
define("TONIDO_LOCALSTORAGE_NOOFVERSIONS", 3 );

?>
```

Use the following commands, to backup user files.

Backing up user data files

```
# mkdir -p /InfoVaultzbackup/userdata
# sudo cp -dprv /opt/InfoVaultz/data/* /InfoVaultzbackup/userdata
```

Start Webserver and MongoDB

After the above backup steps are performed, start the apache webserver and mongo db processes.

Starting services

```
# sudo /etc/init.d/mongodb start
# sudo /etc/init.d/apache2 start
```

Please use equivalent commands applicable for your OS distro.

Restore

High level steps to restore InfoVaultz in windows:

1. Stop webserver
2. Restore configuration files
3. Restore database.
4. Restore user files.
5. Start webserver

Stop Webserver and MongoDB

Before restore is performed, stop the apache webserver and mongodb. This prevents any client from adding/removing files while the backup is in progress.

Stopping services

```
# sudo /etc/init.d/apache2 stop
# sudo /etc/init.d/mongodb stop
```

Please use equivalent commands applicable for your OS distro.

Restore InfoVaultz installation

Restore the InfoVaultz installation files using the following command.

Note: Check your apache installation to ensure /var/www/ is the document root directory.

Restoring InfoVaultz installation

```
# sudo cp -dprv /InfoVaultzbackup/www/* /var/www/
```

Restore database

Restore the database using the following command.

Note: Check your mongodb installation to ensure /var/lib/mongodb is the database path.

Restoring InfoVaultz installation

```
# sudo cp -dprv /InfoVaultzbackup/db/* /var/lib/mongodb/
```

Restore user files

To restore user files, restore the user files to the directory specified in the property 'TONIDO_LOCALSTORAGE_TOPLEVELFOLDER' in in /var/www/config/localstorageconfig.php.

Note: In the following case, the entire "/opt/InfoVaultz/data" directory has to be restored.

Listing targets

```
<?php

/*********************************************************************************
 Copyright(c) 2013 CodeLathe LLC. All rights Reserved.
  This file is part of Infovaultz http://www.tonido.com
 *********************************************************************************/

define("TONIDO_LOCALSTORAGE_TOPLEVELFOLDER", "/opt/InfoVaultz/data");

define("TONIDO_LOCALSTORAGE_DBSERVER", "mongodb://localhost:27017");
define("TONIDO_LOCALSTORAGE_DBNAME", "tonidostoragedb");

define("TONIDO_LOCALSTORAGE_FILESPERCONTAINER", 5000 );
define("TONIDO_LOCALSTORAGE_FOLDERSPERCONTAINER", 5000 );
define("TONIDO_LOCALSTORAGE_NOOFVERSIONS", 3 );
```

Use the following commands, to restore user files.

Backing up user data files

```
# sudo cp -dprv /InfoVaultzbackup/userdata/* /opt/InfoVaultz/data
```

Check your mongodb installation to make sure /var/lib/mongodb is the correct database path.

Start Webserver and MongoDB

After the above restore steps are performed, start the apache webserver and mongodb process.

Starting services

```
# sudo /etc/init.d/mongodb start
# sudo /etc/init.d/apache2 start
```

Please use equivalent commands applicable for your OS distro.

InfoVaultz Backup and Restore - Windows Manual

InfoVaultz can be backed up and restored on windows following these manual steps.

While performing the backup/restore, these are the important file categories that should be backed up/restored:

- cloud cloud files.
- cloud database.
- cloud user files.

Backup

High level steps to backup InfoVaultz in windows:

1. Stop webserver
2. Backup configuration files

3. Backup database.
4. Backup user files.
5. Start webserver

Stop Webserver and MongoDB

Before backup is performed, stop the apache webserver and mongodb. This prevents any client from adding/removing files while the backup is in progress. To stop the apache webserver, open the Tonido InfoVaultz control panel and hit stop for Apache. Also stop the Mongo DB process.

Backup cloud files

Once the apache server is stopped, make a copy of entire cloud installation. The cloud installation can be found under the installation directory under htdocs. (e.g. c:\xampp\htdocs)

Backup database

To backup the database, copy the mongodb database files under c:\xampp\mongodb\bin\data

Backup user files

To backup user files, make a copy of the entire directory specified for the property 'TONIDO_LOCALSTORAGE_TOPLEVELFOLDER' in <cloud_install_dir>\config\localstorageconfig.php.

Note: In the following case, the entire "c:\infovaultz\userdata\" directory has to be backed up..

> **Sample config file**

```
<?php

/*****************************************************************************
 Copyright(c) 2013 CodeLathe LLC. All rights Reserved.
 This file is part of Infovaultz http://www.tonido.com
 *****************************************************************************/

define("TONIDO_LOCALSTORAGE_TOPLEVELFOLDER", "c:\infovaultz\userdata");

define("TONIDO_LOCALSTORAGE_DBSERVER", "mongodb://localhost:27017");
define("TONIDO_LOCALSTORAGE_DBNAME", "tonidostoragedb");

define("TONIDO_LOCALSTORAGE_FILESPERCONTAINER", 5000 );
define("TONIDO_LOCALSTORAGE_FOLDERSPERCONTAINER", 5000 );
define("TONIDO_LOCALSTORAGE_NOOFVERSIONS", 3 );
```

Start Webserver and MongoDB

After the above backup steps are performed, start the apache webserver and mongo db processes.

Restore

High level steps to restore InfoVaultz in windows:

1. Stop webserver
2. Restore configuration files
3. Restore database.
4. Restore user files.
5. Start webserver

Stop Webserver and MongoDB

Before restore is performed, stop the apache webserver and mongodb. This prevents any client from adding/removing files while the restore is in progress.

Restore cloud files

Once the apache server is stopped, restore copy of entire cloud installation files to <cloud_install_dir>. (c:\xampp\htdocs)

Restore database

To restore the database, copy the mongodb files into the mongodb data directory. (c:\xampp\mongodb\data)

Restore user files

To restore user files, restore the user files to the directory specified in the property 'TONIDO_LOCALSTORAGE_TOPLEVELFOLDER' in <cloud_install_dir>\config\localstorageconfig.php.

Note: In the following case, the user files had to be copied to "c:\infovaultz\userdata\".

Listing targets

```
<?php

/*******************************************************************************
 Copyright(c) 2013 CodeLathe LLC. All rights Reserved.
  This file is part of Infovaultz http://www.tonido.com
 *******************************************************************************/

define("TONIDO_LOCALSTORAGE_TOPLEVELFOLDER", "c:\infovaultz\userdata");

define("TONIDO_LOCALSTORAGE_DBSERVER", "mongodb://localhost:27017");
define("TONIDO_LOCALSTORAGE_DBNAME", "tonidostoragedb");

define("TONIDO_LOCALSTORAGE_FILESPERCONTAINER", 5000 );
define("TONIDO_LOCALSTORAGE_FOLDERSPERCONTAINER", 5000 );
define("TONIDO_LOCALSTORAGE_NOOFVERSIONS", 3 );
```

Start Webserver and MongoDB

After the above restore steps are performed, start the apache webserver and mongodb process.

InfoVaultz Troubleshooting

- Known Issues
- Reporting problems in InfoVaultz
- Accessing InfoVaultz from an external location fails
- Active Directory Setup Issues

Known Issues

InfoVaultz Known Issues List

- Folders downloaded as ZIP do not open properly on Mac OSX
- File names with left bracket or right bracket do not upload via the Web browser

Folders downloaded as ZIP do not open properly on Mac OSX

Problem

- The compression method (NO COMPRESSION) isn't recognized by Mac OSX, therefore it keeps trying to create compressed archive again (.cpgz).

Workaround(s)

- Install a different zip utility rather than the built-in zip utility to extract zip files. ie Unarchiver Mac OSX application
- Unzip using the command prompt (unzip filename.zip)
- Zip files downloaed via Safari are extracted correctly

File names with left bracket or right bracket do not upload via the Web browser

Problem

- This is a known issue with PHP.

Workaround: Rename the file and upload or upload via the Sync Client

Reporting problems in InfoVaultz

Introduction

When administrators run into issues with the InfoVaultz installation, they will be requested to collect the debug logs when the problem occurs. This document discusses how to capture the logs and send them to InfoVaultz development team.

Enable Debug Logging

By default Tonido InfoVaultz installation operates in "PROD" mode. This is the production mode, in which the amount of logging generated is very little. So admins have to enable debug mode to increase the logging information. To enable debug mode, edit the configuration file WEBROOT/config/cloudconfig.php and change the following property.

> **Enable debug mode**
> **Change from:** Current define("INFOVAULTZ_OP_MODE", "PROD"); // < VALID values are DEV | PROD
>
> **To:** Current define("INFOVAULTZ_OP_MODE", "DEV"); // < VALID values are DEV | PROD

After this property change, there is no need to restart any services. The change should be picked up automatically.

(Optional): Recreate Issue

If the issue on hand is re-creatable, perform the steps to recreate the issue. If the issue is not reproducible, then keep running InfoVaultz in "DEV" mode.

Collect Logs

Once the problem to report occurs again, collect the following logs and send to support@codelathe.com with a short description of the problem.

1. InfoVaultz Logs:
   Windows and Linux: WEBROOT/scratch/logs/log_<timestamp>.txt. Collect the file with the latest <timestam
2. Apache Logs:
   Windows: <XAMPPROOT>/apache/logs/error.log
   Linux: /var/log/apache2/access.log and /var/log/apache2/error.log

InfoVaultz Debug Log File Locations

Debug Log File Locations

- Debug Log File Locations

- InfoVaultz Log
- PHP Error Log
- InfoVaultz Sync Client Log:
- InfoVaultz Drive Client Log: (Windows Only)

InfoVaultz Log

Windows: <DriveLetter>\xampp\htdocs\scratch\logs\log_YYYY-MM-DD.txt

Example: c:\xampp\htdocs\scratch\logs\log_2013-08-27.txt (Select the latest date)

Linux: /var/www/scratch/logs/log_YYYY-MM-DD.txt

PHP Error Log

Windows: <DriveLetter>\xampp\php\logs\logs\php_error.log

Linux: Only if PHP Error logging is enabled

InfoVaultz Sync Client Log:

Windows:

%APPDATA%\InfoVaultzSyncData\client\syncclient.log **Linux**:

~/InfoVaultzSyncData/client/syncclient.log

Mac:~/InfoVaultzSyncData/client/syncclient.log

InfoVaultz Drive Client Log: (Windows Only)

Windows: %APPDATA%\TonidoDrive\data\TonidoDrive.log

Accessing InfoVaultz from an external location fails

Active Directory Setup Issues

- Fails to connect to Active Directory Server
- Unable to find an AD User
- Unable to find an AD Group

Fails to connect to Active Directory Server

Unable to find an AD User

Unable to find an AD Group

InfoVaultz Best Practices

- Security
  - Changing default config and log directory for InfoVaultz

Security

Security

InfoVaultz can be secured using multiple methods:

- The InfoVaultz install can be made to run under SSL (HTTPS). This ensures all data transmitted on transit is secure.

    - The Apache webserver needs to have SSL enabled and additionally a SSL certificate valid for the domain needs to be installed.
    - The port that will be used will be 443 instead of 80
    - The clients will need to use https://domain instead of the normal http://domain
- Make user passwords stronger by changing the required strength using the TONIDO_MIN_PASSWORD_STRENGTH parameter in the config.php file
- Make default login cookie session length shorter using the INFOVAULTZ_SESSION_TIMEOUT_IN_DAYS config.php file parameter
- Passwords are never stored in plain text by client apps and stored encoded
- **Coming soon:** Support for Server side file encryption
- **Coming soon:** Remote Data Wipe

Changing default config and log directory for InfoVaultz

Introduction

Out of the box, InfoVaultz has the configuration and log directories under the WEBROOT. This is not a secure practice for production installation. This document discusses how to move these directories to different location.

Changing Config Directory

By default configuration files for InfoVaultz installation will be under WEBROOT/config. To change this directory, move the WEBROOT/config directory to the new location and then update the WEBROOT/localconfig.php file to notify this change to InfoVaultz.

> **Enable debug mode**
> **Change from:** define("INFOVAULTZ_CONFIG_PATH", TONIDO_CLOUD_ROOT_DIR.DIRECTORY_SEPARATOR."config"); // < VALID config directory path, needs to be read/write by www-data
>
> **To:** define("INFOVAULTZ_CONFIG_PATH", "/home/infovaultz/config"); // < VALID config directory path, needs to be read/write by www-data

Note: As the comment says, the new path should have read/write permissions for the user account that is used to run apache. For instance, www-data in Linux.

Changing Log Directory

By default InfoVaultz log files will be placed under WEBROOT/scratch. To change this directory, update the WEBROOT/localconfig.php file to notify the new log path to InfoVaultz.

> **Enable debug mode**
> **Change from:** define("INFOVAULTZ_SCRATCH_PATH", TONIDO_CLOUD_ROOT_DIR.DIRECTORY_SEPARATOR."scratch"); // < VALID scratch directory path, needs to be writable by www-data
>
> **To:** define("INFOVAULTZ_CONFIG_PATH", "/home/infovaultz/config"); // < VALID config directory path, needs to be readable by www-data

Note: As the comment says, the new path should have write permissions for the user account that is used to run apache. For instance, www-data in Linux.