



vaultize

Administration Guide

Version 14.06.04

Copyright © 2014 Vaultize Technologies Pvt. Ltd. All rights reserved.

Vaultize Administration Guide, Version 14.06.04.

If this guide is distributed with software that includes a customer agreement, this guide, as well as the software described in it, is furnished only under license and may be used or copied only in accordance with the terms of such license and such agreement. Except as permitted by any such license and such agreement, no part of this guide may be reproduced, stored, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written permission from Vaultize Technologies Pvt. Ltd.

Please note that the content in this guide is protected under copyright law even when it is not distributed with software that includes a customer agreement.

The content of this guide is furnished for informational use only. The content is subject to change without notice, and should not be construed as a commitment by Vaultize Technologies Pvt. Ltd. No responsibility or liability for any errors or inaccuracies that may appear in the content of this guide is assumed by Vaultize Technologies Pvt. Ltd.

Any references to company names and individuals in examples are for demonstration purposes only and are not intended to refer to any actual organization or person in any manner.

Table of Contents

1 Introducing Vaultize	5
1.1 How it works	5
1.2 My Vault	6
1.3 Data Sharing	6
1.4 Anywhere Access	6
1.5 Data Protection	7
1.6 Restore	7
1.7 Access Control	8
1.8 Data Sync	8
2 Getting Started	9
2.1 First time Logging into My Vaultize	9
2.2 Forgot Password	11
3 Basic Information	13
3.1 Dashboard	13
3.2 Account	14
3.3 Switching to Admin Role	17
3.4 Downloads	20
4 Policies	22
4.1 General Policies	22
4.2 Data Sharing Policy	26
4.3 Data Protection Policy	31
4.4 Access Control	38
4.5 Anywhere Access	42
4.6 Network Policies	46
4.7 Mobility	48
4.8 Applying a Policy	50
4.9 Editing a Policy	58
4.10 Un-applying a Policy	59
4.11 Import/export of a policy	61
5 Settings	63
5.1 SMTP	63
5.2 Authentication	65
5.3 Audit Trail	69
5.4 Cloud Storage Configuration	70
5.4.1 Rackspace	70
5.4.2 Amazon Simple Storage Service (Amazon S3)	71
5.5 SSL Certificate Configuration	71
6 User Management	73
6.1 Create User	74

6.2 Edit User	80
6.3 Password Change.....	82
6.4 View a User.....	82
6.5 Block a User.....	84
6.6 Download Keys	87
6.7 Delete Keys.....	88
6.8 Wipe.....	88
6.9 Purge User Files	89
6.10 Purge User Devices.....	90
7 Groups	92
7.1 Creating New Group	94
7.2 Editing a Group.....	95
8 Data Sources	97
9 Reporting	98
9.1 Scheduling new report.....	98
9.2 Editing report.....	102
9.3 Deleting report	103
10 Installing on a Device	105
10.1 System Requirements.....	105
10.2 Installation.....	105
10.3 Client UI.....	115
10.4 Version History.....	119
10.5 Data Sync	120
10.6 Online Document Viewer.....	121
10.7 Outlook Plugin	122
Annexure A.....	128
Annexure B	129

1 Introducing Vaultize

Welcome to Vaultize - a next-generation cloud-based Secure File Sharing, Data Access and Data Protection Solution!

We at Vaultize Technologies believe that it is not only important where and how you keep your data; it's more important what you do with it. Vaultize provides the users a complete control over unstructured data. It also allows access to data coming from different sources through a single window. It can be accessed from different devices and locations.

Vaultize protects files/folders, emails (Outlook PST), application data on your servers, desktops and laptops (even while they are on the move) continuously to a secure Vaultize cloud, while keeping restores and undelete operations quick and painless. And then comes the fun part - using Vaultize cloud, the users can collaborate on a bunch of files or folders, keep their devices (e.g. office desktop and laptop) in sync, create a Disaster Recovery task for their servers or securely share a file with their clients - everything through a single interface in a few simple steps!

You just need to install Vaultize client software on the devices you want to protect. There is no need for the devices to be on your office LAN or at a single office location—they only need to be connected to internet. That means you can deploy Vaultize across your all office locations—including remote offices where you have intermittent internet connectivity, and that too without requiring any VPN connectivity!

1.1 How it works

Here is how Vaultize works:

1. After your organization subscribes to Vaultize, you get an Administrative account e.g. vzadmin@example.com. This is a special account for your organization using which you would manage settings, account creation for individual users, quota and permissions etc.
2. You define policies for your organization and apply them on groups and users.
3. Vaultize administrator installs Vaultize software on individual user's devices.
4. Once Vaultize client is installed on individual user's machine, it appears in the system tray with icon as - 

They can invoke the Vaultize Graphical User Interface (GUI) by clicking on this icon.

In the following sections we will familiarize you with the features and functionalities of Vaultize.

1.2 My Vault

“My Vault” refers to that data which is available to a user. It contains the data that is shared to the user by others, data from file servers and NAS. It also shows the data that is protected from various devices of the user.

1.3 Data Sharing

Vaultize allows users within your organization to selectively share files/folders with their colleagues in real time—making collaborative effort within your business more efficient. Vaultize provides location transparency, which means a user can share a file/folder with his/her colleagues at different locations, and even when somebody is on the move. Unlike many other collaboration solutions, all this is done securely and without need of a VPN! Recipient can download or sync it to a local folder or just ignore the shared data completely.

With Vaultize it is now super easy and fast to share even large files. The recipient will be able to see the latest files as you modify them—giving you an efficient way to collaborate with your outside parties. Vaultize users see the shared data in their client. Users outside Vaultize, see the shared data using a web link. You can protect the link through a password. You can also set up a time to auto-expire this link or deactivate the link manually to keep the access to these files and folders under your control. Because Vaultize only sends the incremental changes, you save on network bandwidth while sending revisions.

1.4 Anywhere Access

Vaultize allows admin to provide access to a data source in the organization even when the users are outside the corporate network. However, note that only single copy of the data is maintained in this case and no versions are stored.

If the data source is a file server say NAS, which is always online, data is made available to the outside world without keeping a copy of it on the Vaultize server. Storing at Vaultize end is considered unnecessary since the source is always up. Hence, data passes via the Vaultize server but is not stored in it. This option is also called “*Pass Through*” since data just passes

through the Vaultize server.

1.5 Data Protection

Data can be protected via Vaultize in 2 ways:

Protecting data to Vaultize:

After an initial full protection of your data to the cloud, Vaultize continuously monitors your data for any modification and sends only the changes to the cloud. During this process Vaultize maintains all revisions and timestamps them. Vaultize also preserves deleted files so that you can restore them in future. Protection however means that data is backed up onto Vaultize and user cannot view or modify it. Users can choose to do a one-time upload to protect single copy of their data.

The data that is transferred from your device to the cloud is encrypted using strong encryption techniques at the source (i.e. on the device itself). This means nobody other than you can see the contents of your data—while being transmitted over SSL (a secure channel) on the internet, and as well as while it is stored in the cloud. Vaultize uses optimization techniques like de-duplication and compression that significantly reduce your internet bandwidth requirement for transfer of data being protected.

The key feature is that your data on a roaming laptop is continuously being protected while you are on move. You need not be connected to your office network for data protection. In case you are not connected to internet, the changes you make to your data will be accumulated on your device and will be sent to cloud next time you connect to internet—and that too automatically without you even realizing it!

On disk-encryption of data:

This feature is used to secure data while it lies in your local machine itself. Via protection policy, admin can enable encryption of data. This will encrypt and thereby secure data on the local machines of users.

1.6 Restore

The restoring any previous version of a file/folder is very easy. This can be done through Vaultize client using various options by users themselves.

A user just needs to go to "All Data" tab on the client and select the file and version he/she

wants to restore. Now, the user can click “Download” button if he/she wants to download just the latest copy of the file. User can also perform sync by clicking the “Sync” button which ensures that the copy of the file/folder on his/her device is up-to-date.

Also, user can view a file/folder as it appeared at some time in the past. For this, he/she can enter some previous Date and Time in “View data until” option in “All Data” page. This will give the user, a copy of data as it appeared on that given date and time.

User can also select a lost/broken device from “All devices” button and download all the data that was present in that device into his/her current device.

1.7 Access Control

Vaultize allows admin to provide data access to users from their vault. There can be restrictions for data access from certain regions (via geo fencing) and from certain IPs. Also, there are several other options to restrict data access. For example, there can be time based access to data say from 9 AM to 8 PM on Monday and Tuesday and so on.

1.8 Data Sync

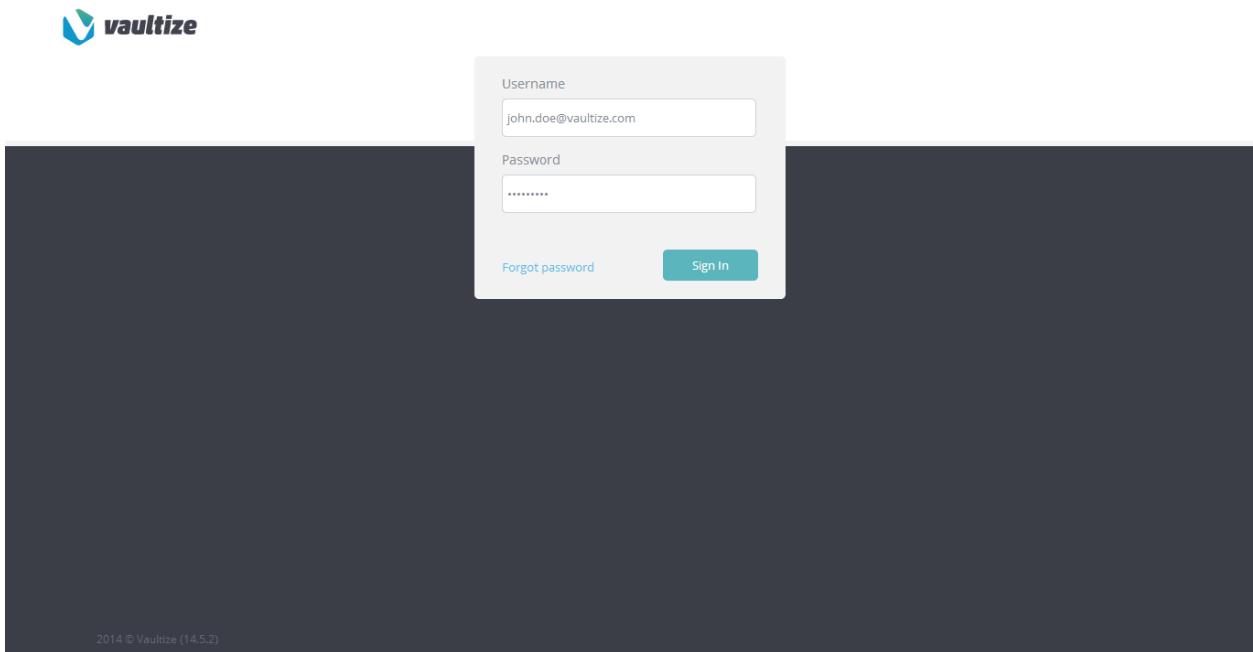
The Data Sync feature is provided via a “Sync” button across each data instance on the client. When a data instance is synced, the local copy of the data is always kept up-to-date with Vaultize server. The user can, at any point in time, decide not to sync the data anymore. Then, he/she can simply click the “Unsync” button to stop syncing the data.

2 Getting Started

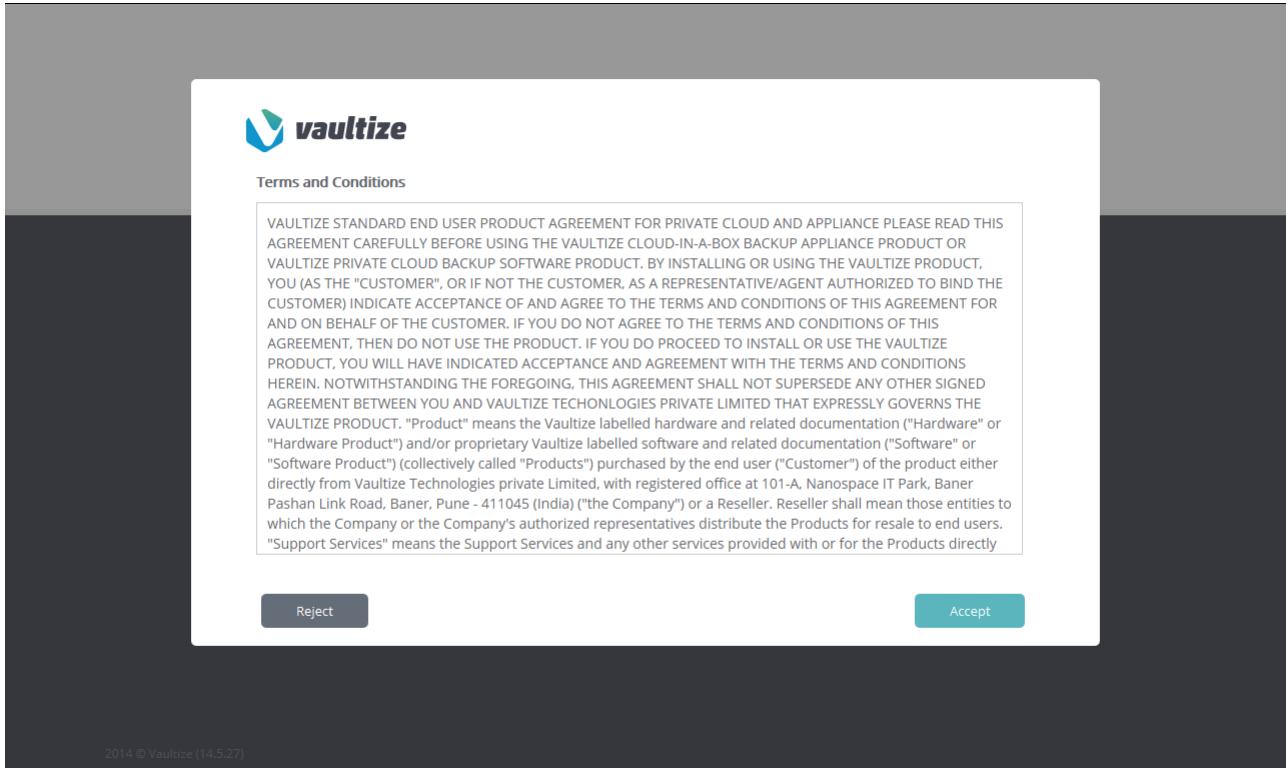
Welcome Vaultize Administrator!

As the Vaultize administrator of your organization, you can monitor and administer your Vaultize setup anytime and anywhere over web at —"My Vaultize"- <https://login.vaultize.com/> (please note the 's' in 'https' – it is a secure SSL connection). You can do things like monitoring your organization's individual Vaultize users' usage, data sharing, data protection, data access, creating new users, changing settings, seeing how quota is being used and so on. The admin console is a powerful tool, please use it with responsibility.

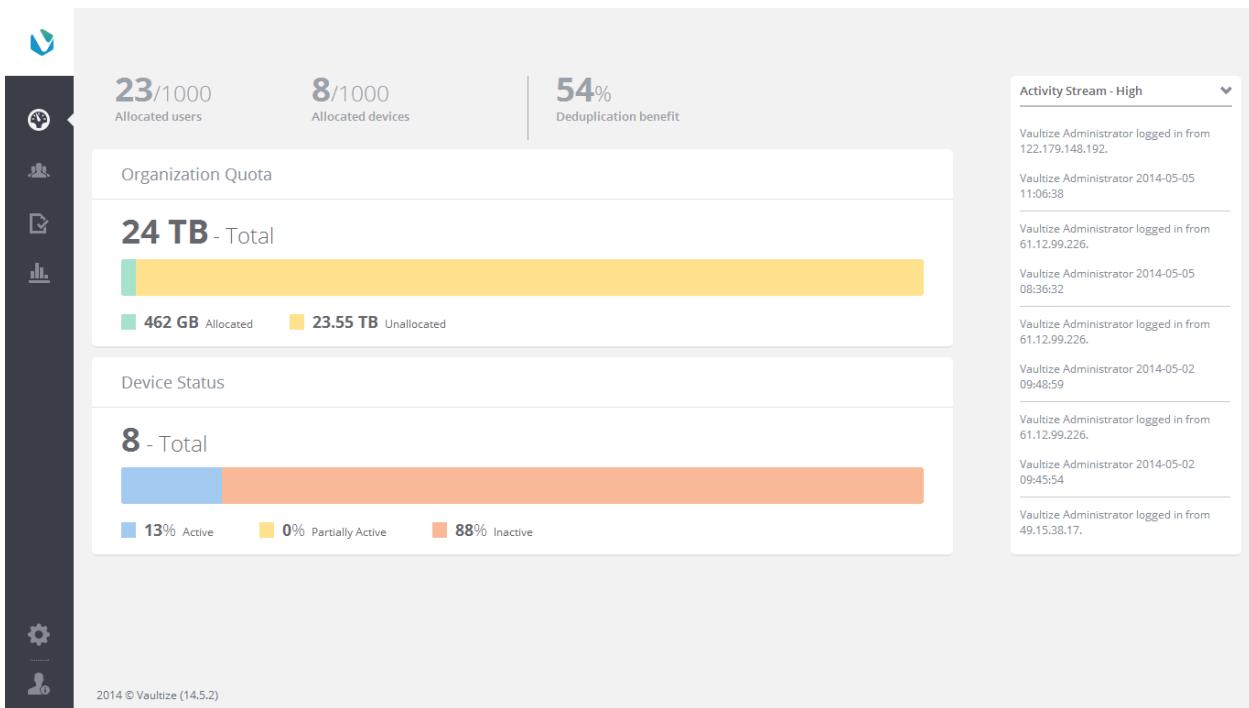
2.1 First time Logging into My Vaultize



After your Administrative account is activated, you would get a separate email that would contain your initial password. You must login to "My Vaultize" using this password first. After logging in, you will also be shown a copy of the Agreement as shown below. Now you are ready to use Vaultize!



After logging in by selecting “Accept”, the dashboard screen appears as shown below-

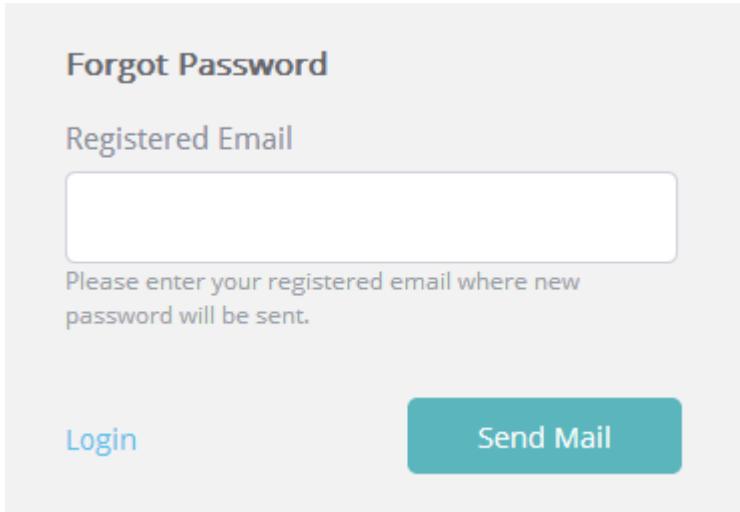


2.2 Forgot Password

When an admin/user forgets his/her password, a new password can be generated. Please note the “Forgot Password” link in the login screen below-

The login screen features two input fields for **Username** and **Password**. Below the password field is a **Forgot password** link. To the right of the password field is a large teal **Sign In** button.

Upon clicking this, the admin/user is taken to below screen-



The image shows a 'Forgot Password' page. At the top, the title 'Forgot Password' is displayed. Below it, the label 'Registered Email' is followed by a text input field. A placeholder text inside the field reads: 'Please enter your registered email where new password will be sent.' At the bottom left is a 'Login' button, and at the bottom right is a teal-colored 'Send Mail' button.

When an admin/user enters the email address here and clicks “Send Mail”, a new system generated password is sent to his/her mail id. He/she can now login to the portal using the newly generated password and then reset it. The “Login” button in the above page takes you to the login page.

3 Basic Information

3.1 Dashboard

When you login to My Vaultize web console as Vaultize administrator, you will see the "Dashboard" page by default. It contains all the generic information such as:

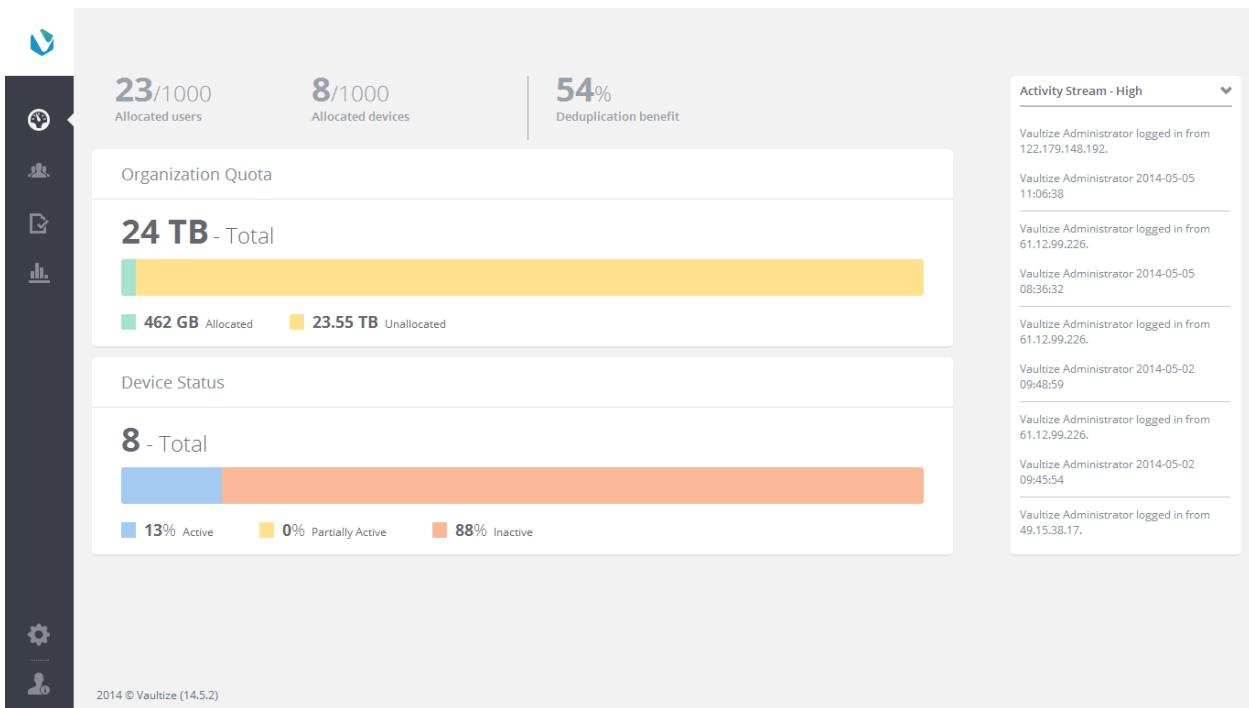
- *organization memory quota status* - the quota mentioned here is soft quota. For example, if 500 GB is the overall organization quota, you can allocate 20 GB each to 50 users. Some users can utilize the 20 GB limit. However, the overall quota must not exceed 500 GB.
- *devices status* - A device can be active, inactive or partially active. A user is considered active if he/she has connected to the server in the last 24 hours. A user is considered partially active if he/she has not connected to the server in the last 24 hours but has connected in the last 7 days. A user is inactive if he/she has not connected to the server in the last 7 days.
- *De-Duplication status* - Deduplication is a data compression technique to eliminate duplicate copies of repeating data.

Deduplication benefit is counted as-

$$\frac{((\text{actual data size on disk}) - (\text{deduplicated data size on Vaultize server})) * 100}{(\text{Actual data size on disk})}$$

For example, if actual data on disk is 500 GB and deduplicated data size on Vaultize server is 100 GB, the Deduplication benefit is 80%
$$\frac{(500-100)*100}{500}=80\%$$

- *Activity Stream* (on the right-side) - indicates various actions taken by users across the organization. This information is categorised into high, medium and low where high indicates high information and low indicates low information.



3.2 Account

Upon clicking “Profile” icon on the left menu, a pop up appears. Profile icon is indicated by .

The screenshot shows the Vaultize Admin Guide interface. On the left, a sidebar menu includes icons for Downloads, Account (which is highlighted with a red box), and Logout. The main content area displays the following statistics:

- Organization Quota:** 24 TB - Total. A progress bar shows 462 GB Allocated (green) and 23.55 TB Unallocated (yellow).
- Device Status:** 8 - Total. A progress bar shows 13% Active (blue), 0% Partially Active (yellow), and 88% Inactive (orange).
- Deduplication benefit:** 54%
- Allocated users:** 23/1000
- Allocated devices:** 8/1000

On the right, an "Activity Stream - High" section lists several log entries:

- Vaultize Administrator logged in from 122.179.148.192.
- Vaultize Administrator 2014-05-05 11:06:38
- Vaultize Administrator logged in from 61.12.99.226.
- Vaultize Administrator 2014-05-05 08:36:32
- Vaultize Administrator logged in from 61.12.99.226.
- Vaultize Administrator 2014-05-02 09:48:59
- Vaultize Administrator logged in from 61.12.99.226.
- Vaultize Administrator 2014-05-02 09:45:54
- Vaultize Administrator logged in from 49.15.38.17.

Please click “Account” to access your account information as shown below. It includes your profile details like your name, email address, password, time zone, last login time, last access IP address etc.

The screenshot shows the 'Account' page of the Vaultize Admin Guide. On the left is a dark sidebar with icons for Home, Organization, Devices, Reports, and Help. The main content area has a light gray header 'Account'. Below it is a 'Plan Details' section with a quota of 24 TB and usage of 1 GB, with a note about deduplication. The 'Maximum Number of Devices' is listed as 1000, and the 'Subscription ends' on April 17 2016. The 'Profile' section is the focus, with an 'Edit' button. It shows the 'Name' as 'Vaultize Administrator', 'Email' as 'it@vaultize.com', 'Password' as a masked string, 'Time Zone' as 'US/Pacific', 'Last Login time' as 'May 05 2014 (01:36 AM)', and 'Last Access IP address' as '61.12.99.226'. At the bottom of the page is a footer with the text '2014 © Vaultize (14.5.2)'.

You can edit your profile by clicking the “Edit” button on the “Profile” screen. Here, you edit your details like name, password etc. Hence, if you want to change your password, it can be done through this screen. The profile edit screen appears as below:

Edit Profile

X

Email

Name

Old Password

>Password Minimum 8 characters required.

Confirm Password

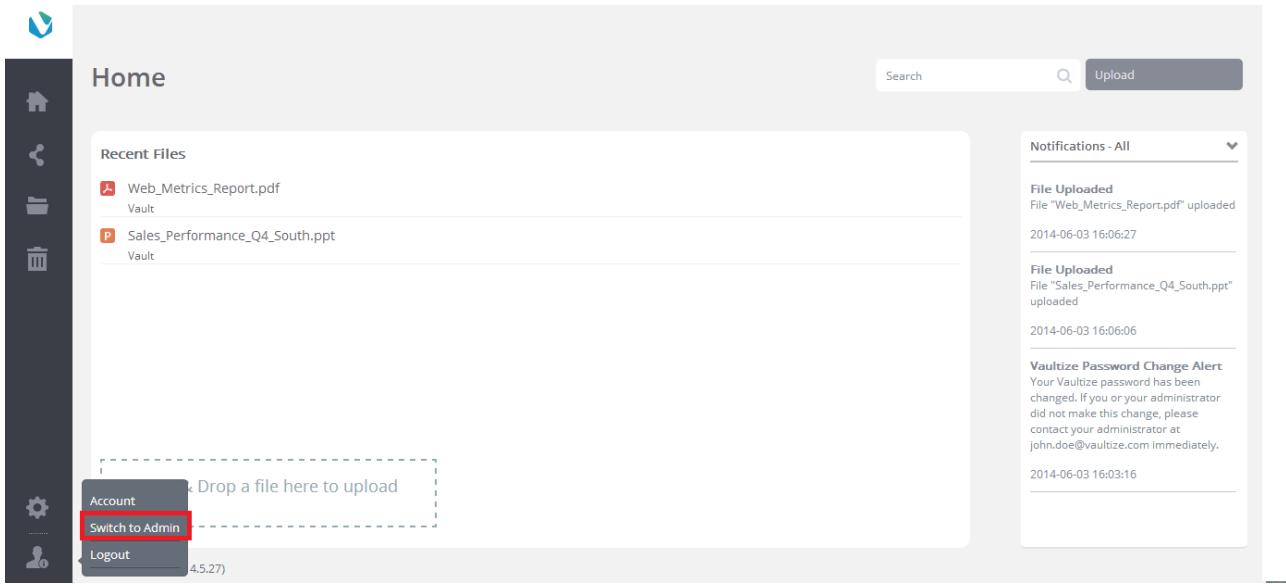
Time Zone

Besides, the “Account” page also displays your plan details like –
Quota – memory quota assigned to user
Usage – Memory being used by the user at present
Usage after deduplication – Memory consumption by user after deduplication has been applied.

It also shows maximum number of devices allowed for all the users together and your Vaultize subscription end date.

3.3 Switching to Admin Role

If a user is given Administrator role, the “Switch to Admin” option appears when Profile button is clicked from his/her client. The same is shown below:



When the user logs in, by default he/she logs in as a user. The user can switch to admin role by clicking the above shown button. The Administrator role can be given to a user by the admin while creating the user itself or by editing an already created user. This can be done by selecting an option from “Administrator Role” drop down as shown below:

Edit User Details

X

1 /2 General

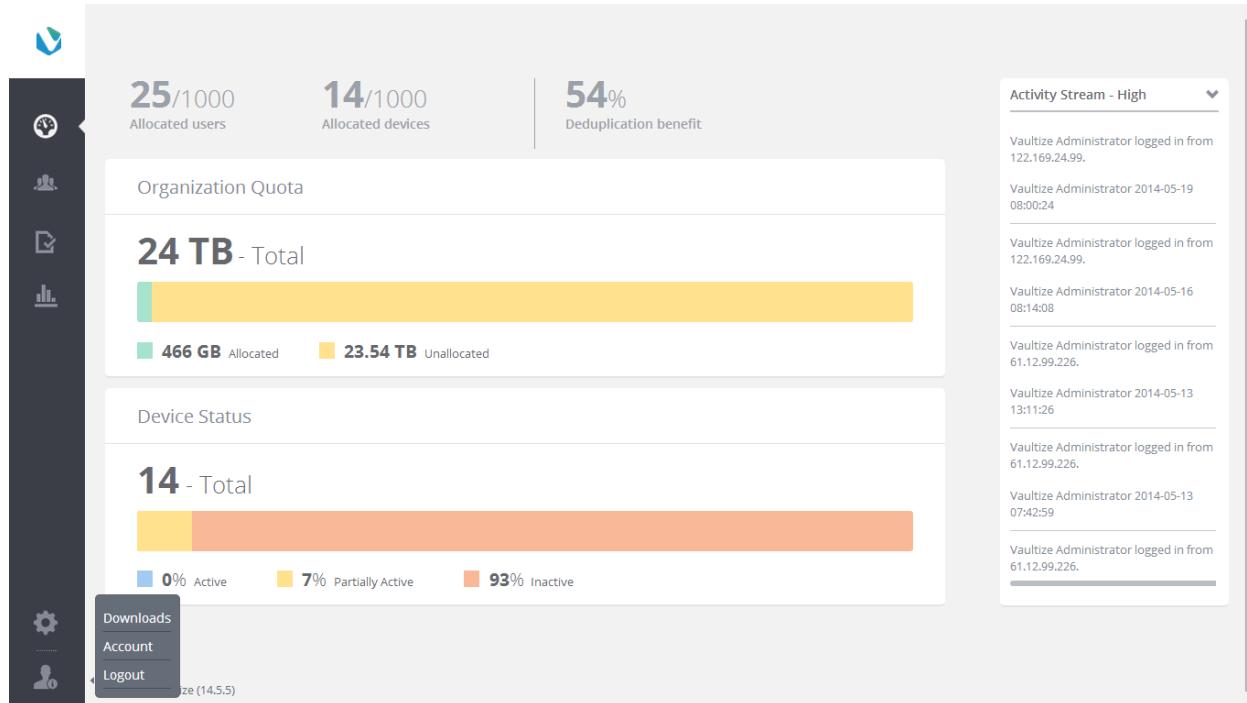
Display Name	Email												
<input type="text" value="Jane Thomas"/>	<input type="text" value="jane.thomas@vaultize.com"/>												
Quota													
<input type="text" value="10 GB"/>	i												
Select Groups to add user in	Groups selected												
<table><tr><td>Search to Add</td><td>Q</td></tr><tr><td>Organization</td><td></td></tr><tr><td>Management Team</td><td></td></tr><tr><td>Sales Team</td><td></td></tr><tr><td>HR Team</td><td></td></tr></table>	Search to Add	Q	Organization		Management Team		Sales Team		HR Team		<table><tr><td>Organization</td></tr><tr><td>Sales Team</td></tr></table>	Organization	Sales Team
Search to Add	Q												
Organization													
Management Team													
Sales Team													
HR Team													
Organization													
Sales Team													
Group's Admin													
<input type="text"/>													
Time Zone													
<input type="text" value="US/Pacific"/>	▼												
Administrator role													
<input type="text" value="None"/>													

Administrator role can be one of the 2 options:

- View Only
- Full Control

3.4 Downloads

Upon clicking the “*Profile*” section, you can see “*Downloads*” option as seen below:



Upon clicking “Downloads”, the below screen appears where Vaultize agents compatible for various operating systems are listed. The one suitable for your organization can be downloaded from here. Also, Support Utilities for each operating system can be found here. Documents such as Admin Guide, User Guide and Data Deletion Guide can also be downloaded for your reference. For IOS client, visit Apple’s Help Store and search for Vaultize. Similarly, get your Android client from Google Play.

The support email address is support@vaultize.com which can be contacted in case of any further queries.



Downloads

Windows

Windows Installer (EXE)
Windows Silent Installer (EXE)
Windows Installer MSI
Outlook Plugin 32bit (EXE)
Outlook Plugin 64 bit (EXE)

Mac

Mac OS X Installer (64-bit, 10.6+)
Mac OS X App (Compressed, 64-bit, 10.6+)

Linux

Ubuntu deb package (64 bit, 12.04+)
Ubuntu deb package (32 bit, 12.04+)

Support Utilities

Remote Support EXE for Windows

Remote Support app for Mac OS X

Remote Support app for Linux

Manuals

Administrator Guide
User Guide
Data Deletion Guide

Contact

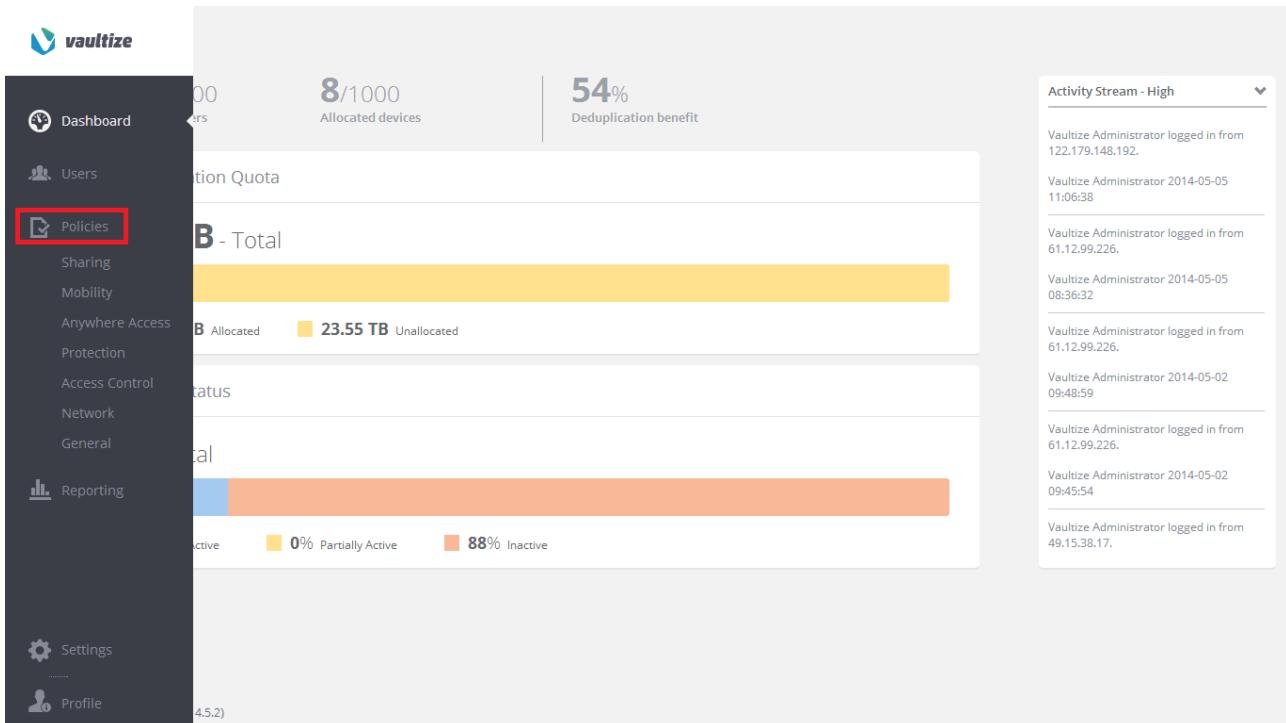
support@vaultize.com

2014 © Vaultize (14.5.5)

4 Policies

You as a Vaultize administrator get complete control over the policies in order to effectively customize data sharing, data access and data protection according to your organization's requirements. Policies could be applied to the whole organization or a group of users or to individual users. In case a user is part of multiple groups, the group priority will decide which policy would be applied.

You can access the Policies section from the menu by clicking .



There are 7 different types of policies available. There are some factory default policies available and applied to the "Organization" group.

4.1 General Policies

Under the "Policies" section, there is a "General" subsection which helps us in setting generic criteria such as quota for new users, startup delay time etc. It also includes mailing criteria such as when a user is created, when user's password is changed etc.

Policy Name	Applied to	Quota	Startup Delay	Actions
Organization default policy	0 groups & 1 users	20 GB	1 Minutes	

2014 © Vaultize (14.5.2)

Creating a general policy:

A general policy can be created by clicking “Create Policy” from “General Policies” page.

Basics:

Create General Policy

X

1 / 2 Basics

Policy Name

Default quota for new users

 ⓘ

Startup delay

 Minutes ⓘ

Upgrade Vaultize automatically

Show icon in system tray of user devices

Show "Quit" option in system tray menu of user devices

Process removable media ⓘ

Process hidden files or folders ⓘ

Cache data on user devices (for quick download/restore)

Allow user to use Vaultize context menu (e.g. right click)

Use background threads on user devices ⓘ

Cancel Continue

Certain general policy settings can be specified which include:

- *Policy Name* – a name for this general policy is given
- *Default quota for new users* – usage quota for new user. All new users would be given this default quota if not explicitly defined during user creation.
- *Startup delay* – it is the time for which Vaultize client remains idle after starting. This gives breathing time to users to finish more important tasks in the beginning. The default value is 1 minute. It is recommended that you keep it as minimum as possible for all

users so that data is always protected.

- *Upgrade Vaultize automatically* – it is recommended that you keep it checked so that all user devices are up to date with the latest version of Vaultize.
- *Show icon in system tray of user devices*– is it recommended that you keep it enabled so that user can access Vaultize client UI through it. Disable it only if you wish to run Vaultize in stealth mode.
- *Show “Quit” option in system tray menu of user devices*– Controls visibility of Quit option in system tray menu.
- *Process removable media*– by default Vaultize does not protect media. Check this option if you want to protect data from removable media too.
- *Process hidden files or folders*– by default Vaultize does not protect hidden files/folders. Check this option if you want to protect data from hidden files/folders too.
- *Cache data on user devices*– data is cached on user devices. It helps in quicker download and restore as data is present in cache
- *Allow user to use Vaultize context menu*– when selected, right click option is enabled on Windows systems through which data protection and sharing can be done.
- *Use background threads on user devices*– This is a Windows only feature. When this option is selected, Vaultize is put into the category of background processes. This option helps in reducing system slowness, if observed. However, the downside is that data protection could be delayed.

Alert Mail:

Create General Policy

X

2 / 2 Alert Mail

When to Alert Users

- When a User is created
- When an User's allowed features are changed
- When User's email address is changed
- When User's quota is changed
- When User's quota is reaching or exceeds
- When User is blocked
- When User is deleted

Previous

Cancel

Create

Lists some of the events upon which the corresponding user receives an email such as when a user is created, when user's email address is changed, when user's quota is changed etc.

NOTE: A user always receives an email when his/her password is changed. This option is not configurable.

4.2 Data Sharing Policy

Data Sharing policy is used to define sharing among users. If the recipient is a Vaultize user, he/she can see the data on Vaultize client. If the user is outsider, a link is sent to him/her via email. Upon clicking this link he/she can view the shared data. Data can be downloaded or viewed depending on the permissions given. If a link is being sent, there is an option of making it password protected and even giving an expiration time for it. Once this expiration time is passed, the link becomes deactivated. You can even control the number of downloads of the shared data.

As an admin, you can set maximum limits for each of these parameters and the user can select a value less than the maximum limit specified here.

Each data share instance in the list consists of the Data Share policy name, count of groups and users to whom it has been applied, whether it is password protected, download link expiration specification and actions that can be taken on this policy.

Any shared data can be synced via “Sync” button which keeps the data up to date on user’s machine.

Policy Name	Applied to	Password Protection	Link expiry	Actions
for_outlook_sharing	0 groups & 1 users	-	After 0 times of download	✅ Sync 🗑
Share office files only	3 groups & 0 users	✓	After 0 times of download	✅ Sync 🗑

Creating a data sharing policy:

Please click “Sharing” under “Policies” to go to the Sharing Policies page. Here, you can create a data sharing policy by clicking “Create Policy” button. By design, the sharing policies are restrictive and therefore, need to be allowed as per the organization’s requirements.

Define Fencing:

Create Sharing Policy

X

1 / 3 Define Fencing

Policy Name

Geo fencing

Include Location

Select Country to Include



Add

IP fencing

Allowed IP's

* for all or IP ranges (comma separated list or CIDR format or hyphen separated). e.g. 192.168.9.1,192.168.9.20 or 192.168.9.29/30 or 192.168.9.90-192.168.9.99



Blocked IP's

Cancel

Continue

Enter a policy name for the new data sharing policy.

Fencing defines the geographic locations and IP addresses from which shared data could be accessed.

When IP/domain fencing is applied, you can specify specific IP addresses or IP range(s) or wild-card expression like *.

Define Time based access:

Create Sharing Policy

X

2 /3 Define Time based access

Days of the week

Mon Tue Wed Thu Fri Sat Sun

Add 24x7 access

Time From

HH MM AM ▾

Time To

HH MM AM ▾

Add ↓

Previous Cancel Continue

You can restrict sharing based on days of the week and time in a day as shown above. Also, you can allow 24X7 access via "Add 24X7 access" button.

Define expiry and password protection:

Create Sharing Policy

X

3 /3 Define expiry and password protection

- Link expiry
- Password Protection required
- Notify the share participants by email
- Allow external users to upload

Previous

Cancel

Create

The share link can be configured to expire after certain number of days or certain number of downloads or certain number of unique accesses.

The link that is send to a user can be chosen to be password protected by checking “*Password Protection Required*”. Also, you can setup the number of incorrect password attempts after which a notification is sent.

If the checkbox “*Notify the share participants by email*” is checked, mails will be sent to the share participants notifying them about the share.

If the checkbox “*Allow external users to upload*” is checked, users who are outside the organization are allowed to upload content to the shared data resource.

NOTE: Mail is sent to external users though “*Notify the share participants by email*” option is kept un-checked.

Pause and Resume:

You can select a data sharing policy and pause it by clicking —“*Pause*” button under “Actions” column. This will pause the share policy application and the data share would now be inaccessible. You can resume the paused data share anytime by clicking “*Resume*” button.

Editing Data Sharing Policy:

You can edit the data sharing policy by clicking edit button under “Actions” column of the policy.

Deleting Data Sharing Policy:

You can delete a data sharing policy by using the “Delete” button under “Actions” column of the policy.

Duplicating Data Sharing Policy:

You can create a new data sharing policy by duplicating an existing policy.

To see how to share data through client UI, please refer to section “*Client UI*”.

NOTE: A maximum limit of 200MB is allowed for web-based downloads and uploads.

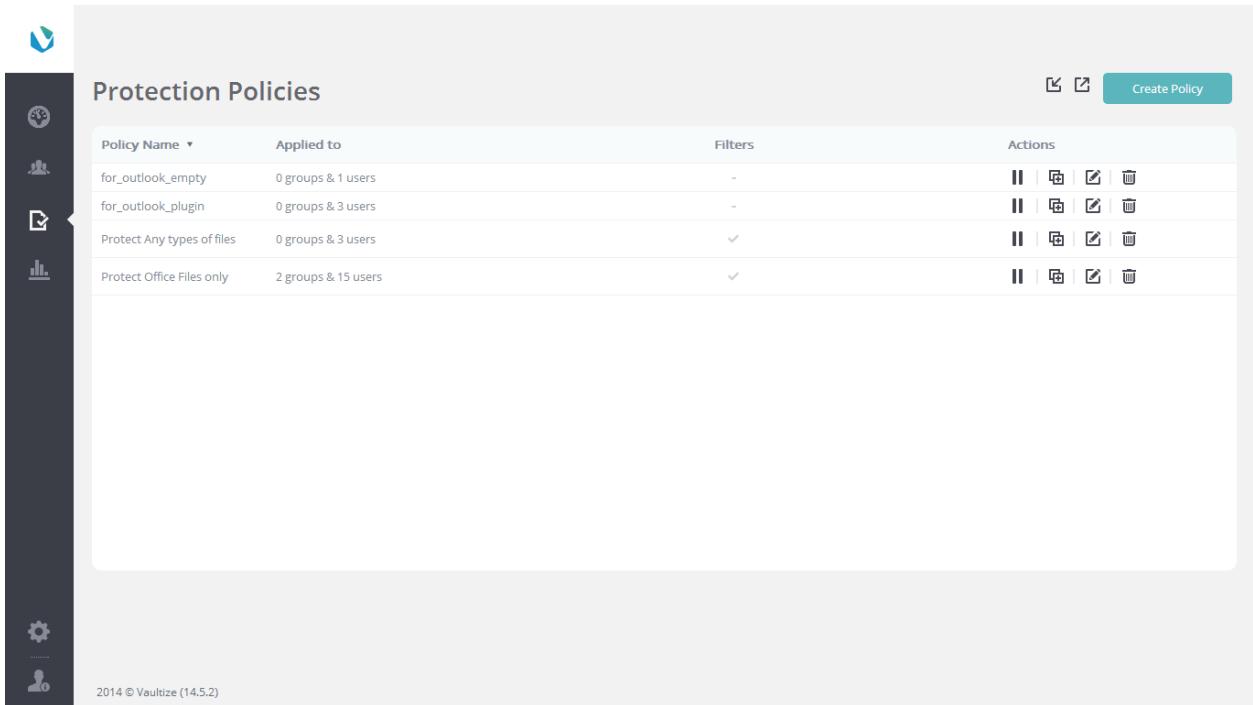
4.3 Data Protection Policy

Data protection policy defines backup, on-disk encryption and wiping policies for the organization. Protection policy has following attributes:

- *Filters* – Filters will shortlist files based on their extension, size, age or location.
- *Schedule* – Schedule will define the periodicity of protection.
- *Target* – It could be pre-defined by admin or selected by users as per their wish.

As an admin, you could define organization wide policy with selection of filters and schedule so that if user selects the target, the data protected is still specific to organization requirements. Default protection policy would allow users to protect all files from any location.

Each policy shows policy name, count of users and groups to which it is applied, type of Protection, whether filter are applied or not, schedule, actions that can be taken on policy like pause/resume, duplicating, editing, deletion etc.



Policy Name	Applied to	Filters	Actions
for_outlook_empty	0 groups & 1 users	-	 ⊕ ☒ ☒ ☒
for_outlook_plugin	0 groups & 3 users	-	 ⊕ ☒ ☒ ☒
Protect Any types of files	0 groups & 3 users	✓	 ⊕ ☒ ☒ ☒
Protect Office Files only	2 groups & 15 users	✓	 ⊕ ☒ ☒ ☒

Creating a data protection policy:

You can go to the Protection Policies page by clicking “*Protection*” under “*Policies*” tab. You can create a data protection policy by clicking “*Create Policy*” button here.

General:

Create Protection Policy

X

1 /4 General

Policy Name

Actions taken when Protection runs on client

- Backup Filtered Files
- Decrypt Encrypted Files (Applicable for Windows targets only)
- Encrypt Filtered Files (Applicable for Windows targets only)
- Wipe Filtered Files

Cancel

Continue

Here, the name of the policy must be specified. Also, one or more actions must be selected which will happen while protection is on the run. These include:

- *Backup filtered files* - Selected files will be protected onto Vaultize.
- *Decrypt encrypted files* - Selected files, if encrypted, will be decrypted. This feature is applicable only for Windows targets.
- *Encrypt filtered files* - Selected files will be encrypted. This feature is applicable only for Windows targets.
- *Wipe files* - Selected files will be wiped (removed) from the user's system. However, their server copy will remain.

Restrict Sources of Data:

Create Protection Policy

X

2 /4 Restrict Sources of Data

Desktop / Laptop

Include Sources	Exclude Sources
<p>* for all OR enter folder paths or IP ranges (comma separated list or CIDR format or hyphen separated). e.g. 192.168.9.1,192.168.9.20 or 192.168.9.29/30 or 192.168.9.90-192.168.9.99</p>	<p>* for all OR enter folder paths or IP ranges (comma separated list or CIDR format or hyphen separated). e.g. 192.168.9.1,192.168.9.20 or 192.168.9.29/30 or 192.168.9.90-192.168.9.99</p>

Previous **Cancel** **Continue**

Data Source can be specified by selecting Desktop/Laptop and then, specifying ip addresses or a range of ip addresses in each of the Include/Exclude sources field. If nothing is specified in Include/Exclude Sources, then any ip addresses would be accepted.

Please refer to [Annexure A](#) for more details on adding data sources.

Define Files/Folders Filter:

Create Protection Policy

X

3 /4 Define Files/Folders Filter

Files/Folders to Include or Exclude

- Office files
- Outlook files
- Email files
- Picture/image files
- Audio/music files
- Video/movie files
- Outlook folder
- Desktop folder

Or type a custom filter

Include Files/Folders

Exclude Files/Folders

Exclude files bigger than KB

Exclude files smaller than KB

Exclude files older than Days

Previous

Cancel

Continue

Vaultize allows you to completely control what data to protect based on following parameters:

- *Include Files/Folders for Data Protection* – you can specify the patterns for file and folder names that you wish to protect. Vaultize provides few pre-defined macros to quickly select specific category of files. For example, Office files macro includes all Microsoft Office extensions, OpenOffice extensions and PDF. Refer [Annexure B](#) for more details of each macro.
- *Exclude Files/Folders for Data Protection* – you can specify the patterns for file and folder names that you do not wish to protect. If nothing is selected in Exclude, all files will be protected whether they are added into Include list or not. In order to protect files listed in Include list only, select “*Everything Else*” in Exclude list.

- *Exclude files bigger than* - you can specify if you do not want to protect files bigger than certain size.
- *Exclude files smaller than* - you can specify if you do not want to protect files smaller than certain size.
- *Exclude files older than* - you can specify if you do not want to protect files older than certain number of days. For example, you may decide to not protect files which are more than a year old.

Schedule and Retention Policies:

Create Protection Policy X

4 / 4 Schedule & Retention Policies

Schedule

Continuous

▼

i

Stop After

Hours i

Minutes i

Retention

Keep file changes for

Days i

Maximum file versions to be

Versions i

Delete files older than

Days i

Previous

Cancel

Create

Vaultize supports four types of scheduling:

- *Continuous* - Vaultize continuously monitors the modification to the data and sends the incremental changes as soon as those are saved to the disk. This provides a complete protection to your data

- *Periodic* – you can specify the periodicity of the data protection (minimum 5 min). The incremental data protection will be performed every ‘N’ minutes or every ‘N’ hours, as specified by you
- *Dates of Month* – you can schedule the incremental data protection at some fixed time on certain dates of the month
- *Days of Week* – you can schedule the incremental data protection at some fixed time on certain days of the week
- *Stop after* – you can pause the data protection after sometime (in hours and minutes). Protection will automatically resume on next schedule date.

Keep file changes for – this value means that Vaultize by default purges the versions (from data protection) older than the specified number of days. You may give a higher value if you wish to retain the versions for longer time. However, the latest version remains always.

Delete files older than – purges the files and all their versions from Vaultize server which are older than the mentioned number of days.

WARNING! This setting removes all the versions from protection, use it with caution.

Maximum file versions to be – indicates maximum number of latest versions protected.

Pause and Resume:

You can select a data protection policy and pause it by clicking —"Pause" button under "Actions" column. The data protection policy active on that folder will be paused.

You can resume the paused data protection policy anytime by clicking "Resume" button. The data protection will resume from then on.

Editing Data Protection Policy:

You can edit the data protection policy by clicking edit button under "Actions" column of the policy.

Deleting Data Protection Policy:

You can delete a data protection policy by using the "Delete" button under "Actions" column in

the data protection policy list. This will not delete any files or folders on the device. All the data protected in the cloud will be archived and will not be wiped.

Duplicating Data Protection Policy:

You can create a new data protection policy by duplicating an existing policy.

4.4 Access Control

Vaultize allows admin to provide data access to users from their vault. There can be restrictions for data access from certain regions (via geo fencing) and from certain IPs. Also, there are several other options to restrict data access. For example, there can be time based access to data say from 9 AM to 8 PM on Monday and Tuesday and so on.

Creating a data access policy:

You can go to the Access Control Policies page by clicking "Access Control" under "Policies" tab. Here, you can create a access control policy by clicking "Create Policy" button.

Define Fencing:

Create Access Control Policy

X

1 / 3 Define Fencing

Policy Name

Geo fencing

Exclude Location

Select Country to Exclude ▾

Add

IP fencing

Allowed IP's

Blocked IP's

Cancel

Continue

Desired name of the access control policy is to be given. Fencing has to be defined. Fencing is a process of restricting data access to a particular region or certain IPs.

Geo Fencing:

This includes restricting data access to certain countries. This can be done by excluding countries.

IP/Domain Fencing:

This includes restricting data access to certain devices. This can be done by giving certain IP addresses to allow/block data access.

Define Time Based Access:

Create Access Control Policy

X

2 / 3 Define time based access

Define time based access

Days of the week

Mon Tue Wed Thu Fri Sat Sun

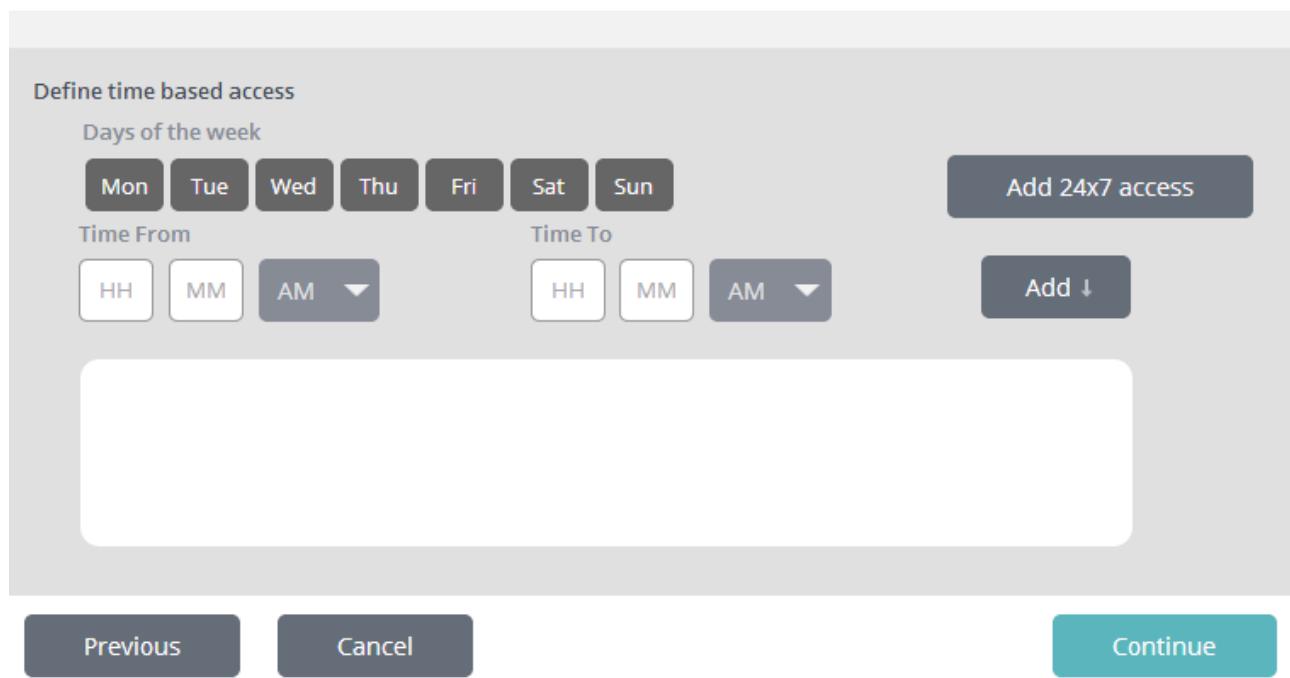
Add 24x7 access

Time From Time To

HH MM AM ▾ HH MM AM ▾

Add ↓

Previous Cancel Continue



Data Access can be restricted based on time such as certain days of the week or in certain period(s) of time in a day. Also, you can add 24X7 data access using the "Add 24X7 access" button.

User Access Settings:

Create Access Control Policy

X

3 / 3 User Access Settings

Access permission within the fence boundary

With App(non-editable)

- Allow web access
- Allow "Upload"
- Allow "Download"

Without App

- Allow web access
- Allow "Upload"
- Allow "Download"

Access permission outside the fence boundary

With App

- Allow web access
- Allow "Upload"
- Allow "Download"

Without App(non-editable)

- Allow web access
- Allow "Upload"
- Allow "Download"

Previous

Cancel

Create

Here, access permissions for users within and outside the defined fence boundary can be defined. Also, permissions for users with Valutize and without Vaultize app in each of these categories are defined.

In fence (With App):

These settings correspond to those users who access Vaultize via app and are currently within the range of the specified fence. These settings are non-editable. All permissions are always enabled.

In fence (Without App):

These settings correspond to those users who access Vaultize via web (without app) and are currently within the range of the specified fence. These settings can be enabled/disabled as per requirement.

Outside fence (With App):

These settings correspond to those users who access Vaultize via app and are currently outside the range of the specified fence. These settings can be enabled/disabled as per requirement.

Outside fence (Without App):

These settings correspond to those users who access Vaultize via web (without app) and are currently outside the range of the specified fence. These settings are non-editable. All permissions are always disabled.

Pause and Resume:

You can select an access control policy and pause it by clicking —"Pause" button under "Actions" column. The access control policy running on that folder will be paused for now. You can resume the paused access control anytime by clicking "Resume" button. The access control will resume from then on.

Editing Access Control Policy:

You can edit the access control policy by clicking edit button under "Actions" column of the policy.

Deleting Access Control Policy:

You can delete an access control policy by using the "Delete" button under "Actions" column of the policy.

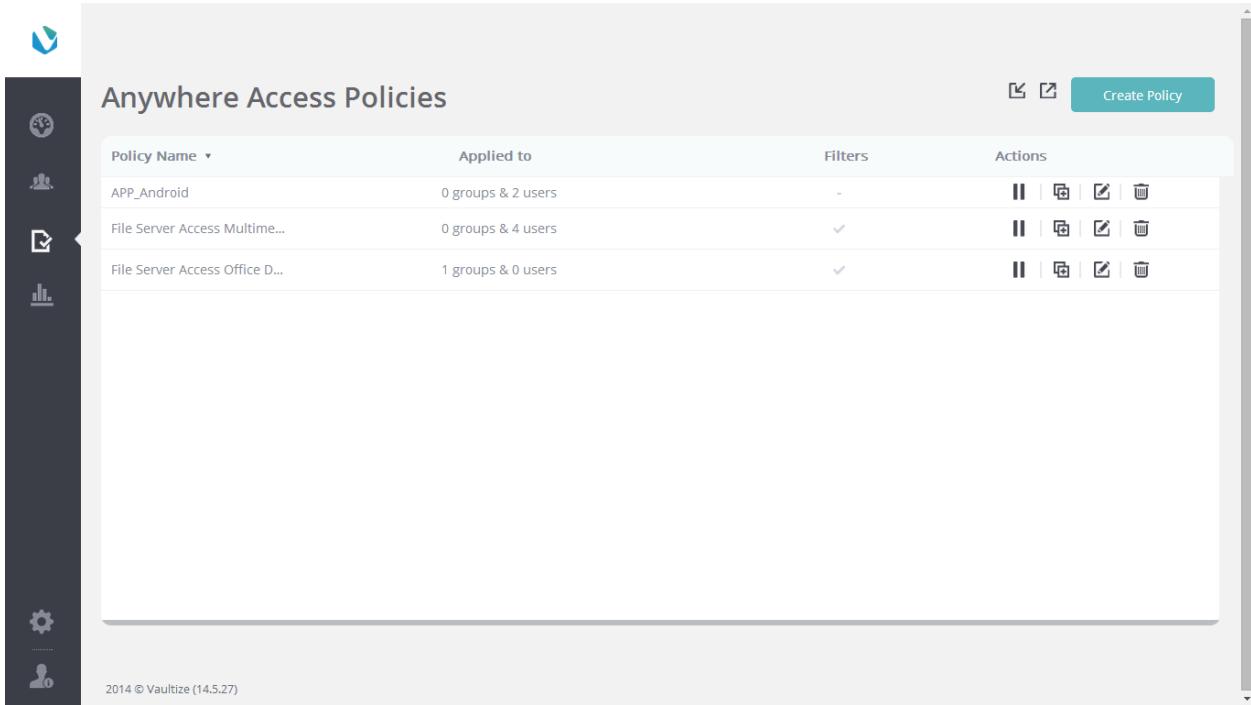
Duplicating Access Control Policy:

You can create a new access control policy by duplicating an existing policy.

4.5 Anywhere Access

Anywhere Access policy is used to allow data access from corporate file servers and NAS to people when they are outside the corporate network beyond firewall. The changes made by user on his/her mobile device is synced back to file server to ensure consistency. On other devices, users can download/upload the files.

Each policy in the list shows policy name, count of the users and groups to whom policy is applied, whether filter are applied or not, schedule of the policy and actions that can be taken on the policy.



Policy Name	Applied to	Filters	Actions
APP_Android	0 groups & 2 users	-	More Edit Delete
File Server Access Multime...	0 groups & 4 users	✓	More Edit Delete
File Server Access Office D...	1 groups & 0 users	✓	More Edit Delete

2014 © Vaultize (14.5.27)

Creating an access anywhere policy:

Please click on “Anywhere Access” under “Policies” tab to go to the Anywhere Access Policies page. Here, you can create an access anywhere policy by clicking “Create Policy” button.

Define Source Filter:

Create Anywhere Access Policy

X

1 / 2 Define Source Filter

Policy Name

Select Data Filters

Desktop / Laptop

File Server

Include Sources i

Exclude Sources i

Cancel Continue

Data Source can be specified by selecting from a list of devices such as –

- Desktop/Laptop
- File Server

You can further specify list of ip addresses or a range of ip addresses in each of these in Include/Exclude sources field. If nothing is specified in Include/Exclude Sources, the any ip addresses would be accepted.

NOTE: If data source is NAS, local copy of data is not kept on Vaultize server. If data source is Desktop/Laptop, latest copy of data is kept on Vaultize server.

Define Files/Folders Filter:

Create Anywhere Access Policy

X

2 / 2 Define Files/Folders Filter

Files/Folders to Include or Exclude

- Office files
- Outlook files
- Email files
- Picture/image files
- Audio/music files
- Video/movie files
- Outlook folder
- Desktop folder

Include Files/Folders

Exclude Files/Folders

Previous Cancel Create

Every organization thinks differently when it comes to what data to access. Using the following parameters you can manage the data that you wish to access:

- Include Files/Folders for Anywhere Access – you can specify the patterns for file and folder names that are to be accessed. In the text box below the file/folder patterns, you can specify custom file types such as *.dwg.
- Exclude Files/Folders for Anywhere Access – you can specify the patterns of file and folder names that should not to be accessed

Pause and Resume:

You can select an access anywhere policy and pause it by clicking —"Pause" button under "Actions" column. The policy running on that folder will be paused for now. You can resume the paused policy anytime by clicking "Resume" button. The access anywhere policy will resume from then on.

Editing Anywhere Access Policy:

You can edit an access anywhere policy by clicking edit button under “Actions” column of the access anywhere policy.

Deleting Anywhere Access Policy:

You can delete an access anywhere policy by using the “Delete” button under “Actions” column in the policy list.

Duplicating Anywhere Access Policy:

You can create a new access anywhere policy by duplicating an existing anywhere access policy.

4.6 Network Policies

You can set up a network policy for your organization. Network Policies control the network bandwidth and proxy.

Creating a network policy:

Please click on “Network” under “Policies” tab to go to the Network Policies page. Here, click on “Create Policy” button to create a new Network Policy for your organization.

Basic:

Create Network Policy

X

1 /2 Basics

Policy Name

Proxy Details

Host

Port

Username

Password

Bandwidth Details

Bandwidth limit for Upload

Kb/s

Bandwidth limit for download

Kb/s

Cancel

Continue

Proxy Details:

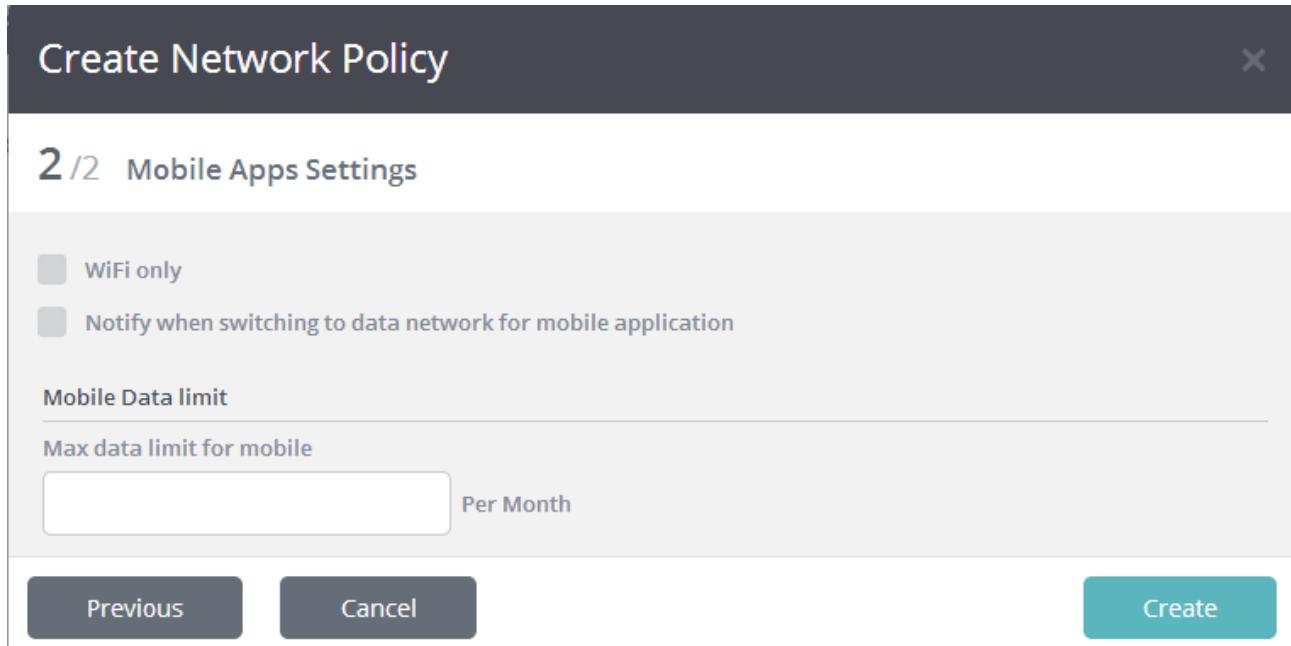
If you have common proxy set up in your organization, you can update the proxy settings like host, port, username, password etc., so that Vaultize can connect to the cloud.

Bandwidth Details:

Vaultize uses optimizations like differential change extraction, de-duplication and compression, utilizing your network bandwidth optimally. Vaultize also uses various algorithms to monitor the activity on individual devices and network and works silently so as to avoid interfering with users' normal activities.

This way bandwidth usage is automatically controlled. But if you wish to control the use of network bandwidth, you can change the bandwidth settings.

Mobile App Settings:



The screenshot shows a 'Create Network Policy' dialog box. At the top, it says 'Create Network Policy' and has a close button. Below that, it says '2 / 2 Mobile Apps Settings'. There are two checkboxes: 'WiFi only' and 'Notify when switching to data network for mobile application'. Under 'Mobile Data limit', there is a text input field 'Max data limit for mobile' with 'Per Month' next to it. At the bottom are 'Previous', 'Cancel', and 'Create' buttons.

- *Wifi only*- Enable this setting if you want Vaultize to work only on Wifi and not consume your mobile data.
- *Notify when switching to data network for mobile application*- Enable this setting if you want to be notified when data network is being switched.
- *Mobile data limit* - Vaultize allows you to limit the data usage for mobile on per month basis.

4.7 Mobility

Mobility policy defines mobile related settings.

These settings can be selected as per your organization's requirement. Please click on "Mobility" under "Policies" tab to go to the Mobility Policies page. Here, click on "Create Policy" to create a new Mobility Policy.

Create Mobility Policy

X

1 /1 Basics and settings

Policy Name

User interaction in Vaultize mobile application:

- Allow users to access mobile app
- Remember user's "password"
- Allow users to upload from Camera

Containerization:

- Allow users to open files using third party mobile applications
- Allow users to open third party mobile application files

Content rights:

- Allow users to "Edit" data using builtin editor
- Allow user to share files using Bluetooth/Airdrop
- Allow user to share files using Airplay
- Allow copy and paste
- Allow user to print files
- Allow user to email files
- Allow screenshots

Cancel

Create

User interaction in Vaultize mobile application:

- *Allow users to access mobile app*- This option allows users in your organization to use Vaultize application from mobile as well.
- *Remember user's "password"*- This option remembers user's Vaultize password on the

mobile.

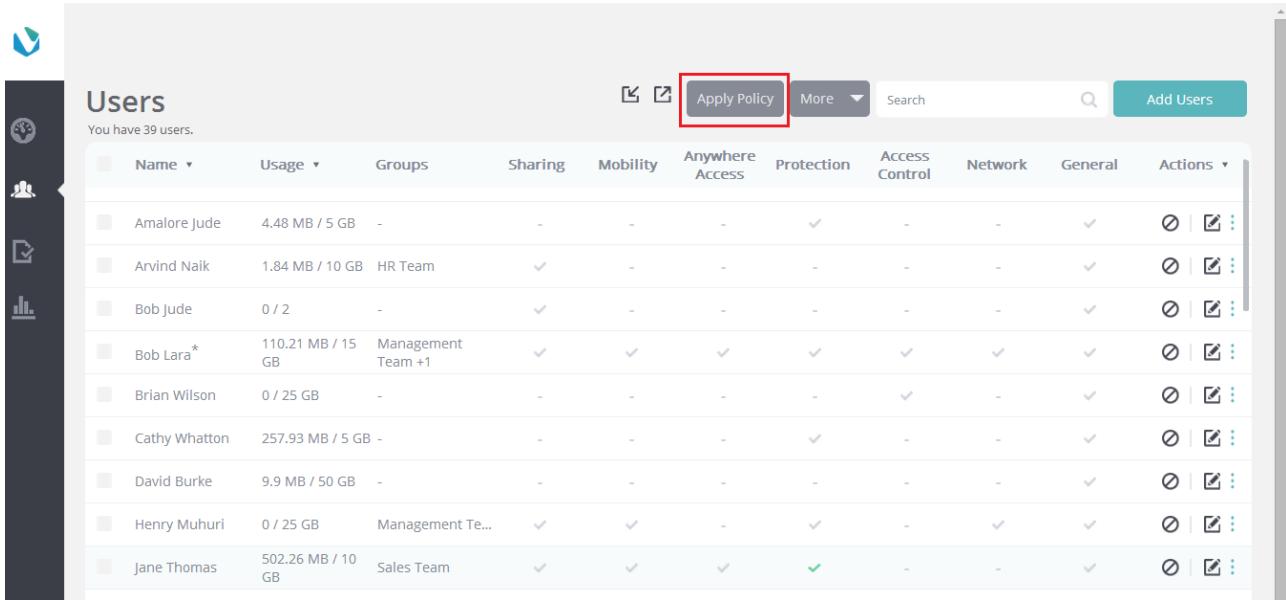
- *Allow users to upload from Camera*- This option allows users to upload content saved via mobile Camera to Vault.
- *Allow users to open files using third party mobile applications*- This option allows users to open Vaultize files from some third party application on the mobile.
- *Allow users to open third party mobile application files*- This option allows users to open third party applications related files on his/her mobile.
- *Allow users to "Edit" data using built in editor*- This option allows users to edit files via built-in editor in mobile.

Content rights:

- *Allow user to share files using Bluetooth/Airdrop*- Allows users to share Vaultize files via Bluetooth/Airdrop.
- *Allow user to share files using Airplay*- Allows users to share Vaultize files via Airplay.
- *Allow copy and paste*- Allows user to copy and paste Vaultize files.
- *Allow user to print files*- Allows users to print Vaultize files.
- *Allow user to email files*- Allows users to send Vaultize files via email.
- *Allow screenshots*- Allows users to take screenshots of Vaultize files.

4.8 Applying a Policy

A policy can be applied to users or groups by clicking the “*Apply Policies*” button in the Users page.



The screenshot shows the 'Users' section of the Vaultize Admin Guide. At the top, there are several icons: a blue 'V' logo, a tree, a person, a document, and a bar chart. The main title is 'Users' with a sub-count 'You have 39 users.' Below the title is a table with the following columns: Name, Usage, Groups, Sharing, Mobility, Anywhere Access, Protection, Access Control, Network, General, and Actions. The table lists nine users with their respective details and policy status. The 'Apply Policy' button is located at the top right of the table area, just below the 'More' and 'Search' buttons, and is highlighted with a red box.

Name	Usage	Groups	Sharing	Mobility	Anywhere Access	Protection	Access Control	Network	General	Actions
Amalore Jude	4.48 MB / 5 GB	-	-	-	-	✓	-	-	✓	∅ <input checked="" type="checkbox"/> ⋮
Arvind Naik	1.84 MB / 10 GB	HR Team	✓	-	-	-	-	-	✓	∅ <input checked="" type="checkbox"/> ⋮
Bob Jude	0 / 2	-	✓	-	-	-	-	-	✓	∅ <input checked="" type="checkbox"/> ⋮
Bob Lara*	110.21 MB / 15 GB	Management Team +1	✓	✓	✓	✓	✓	✓	✓	∅ <input checked="" type="checkbox"/> ⋮
Brian Wilson	0 / 25 GB	-	-	-	-	-	✓	-	✓	∅ <input checked="" type="checkbox"/> ⋮
Cathy Whatton	257.93 MB / 5 GB	-	-	-	-	✓	-	-	✓	∅ <input checked="" type="checkbox"/> ⋮
David Burke	9.9 MB / 50 GB	-	-	-	-	-	-	-	✓	∅ <input checked="" type="checkbox"/> ⋮
Henry Muhuri	0 / 25 GB	Management Te...	✓	✓	-	✓	-	✓	✓	∅ <input checked="" type="checkbox"/> ⋮
Jane Thomas	502.26 MB / 10 GB	Sales Team	✓	✓	✓	✓	-	-	✓	∅ <input checked="" type="checkbox"/> ⋮

Once this button is clicked, a pop up appears. This pop up helps in applying a policy to desired users.

Select Groups/Users:

Here, users or groups to whom the policy is intended is selected.

Apply Policy

X

1 /4 Select Groups/Users

Select Group/User

Search to Add 

Organization
Management Team
Sales Team
HR Team

amalore.jude@vaultize.com
arvind.naik@vaultize.com
bobjude@vaultize.com
bob.lara@vaultize.com
brian.wilson@vaultize.com

Selected Groups/Users

Cancel 

Continue 

Select Policy to be Applied:

Apply Policy

X

2 /4 Select Policy to be Applied

Policies

- Sharing Policies
 - SP_Android 
 - Share office files only
 - outlook_sharing
- Mobility Policies
- Anywhere Access Policies
- Protection Policies
- Access Control Policies
- Network Policies
- General Policies

Policy Details - SP_Android

Time Base Access	mon,tue,wed,thu,fri,sat,sun(12:0 AM - 11:59 PM)
Fencing	
Allowed IP	All
Included Locations	All
Expiry and Password Protection	
Link Expiry	22Days, 2Hr, 0Min
Require Password	Yes
Notification by mail	Allowed
External Upload	Allowed

Add ↓

Policy to be Applied (only one)

Previous **Cancel** **Continue**

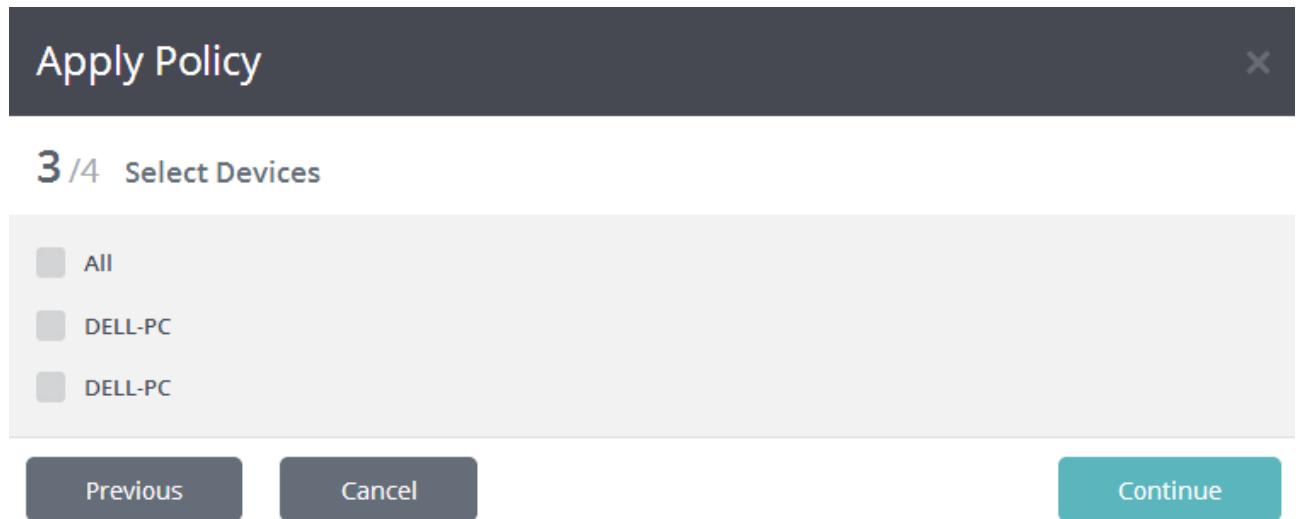
Here, the list of existing policies appear in the “Policies” list. You can select desired policies and click “Add” button to add the policy to the users. When a policy is selected, the details corresponding to the policy appear in the “Policy Details” section.

Flow varies from here depending upon the policy selected. For Sharing, Mobility, Access Control, Network and General Policies, the flow ends here. However, for Protection and Anywhere Access Policies, there are more screens as you can see below.

Select Devices:

If a single user is selected, the below screen with user's devices appears. You can select

one/more devices here.



If more than one user is selected, the below screen appears. Here, you can select one/more device types and operating system types.

Apply Policy

X

3 /4 Select Devices

All types of devices



Previous

Cancel

Continue

Define Target Location:

Here, the target location for data can be specified. It can be a Desktop/Laptop or Google Apps. If Desktop/Laptop is selected, certain suggested locations appear such as Desktop, Outlook folder, My Documents etc.

If Google Apps is selected, you will find options such as All Google Apps, Google Apps Drive, Google Apps Mail.

Target location can be blank in some cases. In this case, the policy can be used by a user on any folder.

Apply Policy

X

4 /4 Define Target Location

Target Type

Desktop/Laptop



Select target location

Desktop

My Documents

Outlook folder

User Profile/Home

Outlook Attachments

Leave blank to let user select the target for protection



Previous

Cancel

Apply

Now that a policy has been applied to a user/group, it can be verified by clicking on the 'tick' mark in the column of each policy type on the user/group page as shown below:

Users

Name	Usage	Groups	Sharing	Mobility	Anywhere Access	Protection	Access Control	Network	General	Actions
Amalore Jude	4.48 MB / 5 GB	-	-	-	-	✓	-	-	✓	∅ ☑ ⋮
Arvind Naik	1.84 MB / 10 GB	HR Team	✓	-	-	-	-	-	✓	∅ ☑ ⋮
Bob Jude	0 / 2	-	-	-	-	-	-	-	✓	∅ ☑ ⋮
Bob Lara*	110.21 MB / 15 GB	Management Team +1	✓	✓	-	✓	✓	✓	✓	∅ ☑ ⋮
Brian Wilson	0 / 25 GB	-	-	-	-	-	-	-	✓	∅ ☑ ⋮
Cathy Whatton	257.93 MB / 5 GB	-	-	-	-	-	-	-	✓	∅ ☑ ⋮
David Burke	9.9 MB / 50 GB	-	-	-	-	-	-	-	✓	∅ ☑ ⋮
Henry Muhuri	0 / 25 GB	Management Te...	✓	✓	-	-	-	-	✓	∅ ☑ ⋮
Jane Thomas	502.26 MB / 10 GB	Sales Team	✓	-	-	-	-	-	✓	∅ ☑ ⋮
Joe Lewis	32.46 MB / 20 GB	Sales Team	✓	-	-	✓	-	-	✓	∅ ☑ ⋮
John Doe	1.66 MB / 50 GB	Management Te...	✓	✓	-	✓	-	✓	✓	∅ ☑ ⋮

2014 © Vaultize (14.5.2)

Similarly, policies applied to groups can also be seen as below:

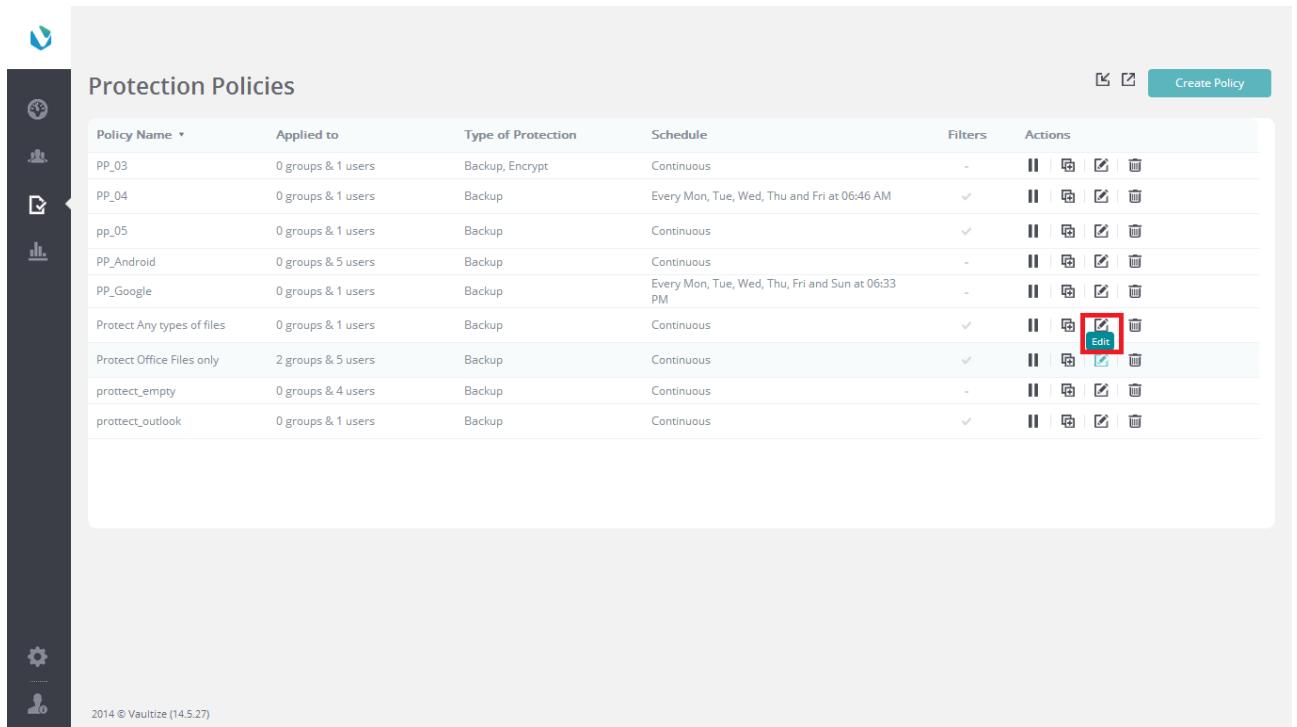
Groups

Name	Users	Admins	Priority	Sharing	Mobility	Anywhere Access	Protection	Access Control	Network	General	Actions
Management Te...	6	-	80	✓	✓	-	✓	-	✓	✓	∅ ☑ ⋮
Sales Team	5	-	50	✓	-	-	✓	-	✓	∅ ☑ ⋮	
HR Team	3	-	25	✓	-	-	-	-	✓	∅ ☑ ⋮	
Organization	23	-	0	-	-	-	-	-	✓	∅	

2014 © Vaultize (14.5.2)

4.9 Editing a Policy

Policies applied to a user/group can be edited from the respective Edit functionality(by clicking the edit icon across the policy- ) as shown below:



The screenshot shows the 'Protection Policies' page in the Vaultize interface. On the left is a vertical sidebar with icons for Home, Policies, Groups, and Users. The main area is titled 'Protection Policies' and contains a table with the following data:

Policy Name	Applied to	Type of Protection	Schedule	Filters	Actions
PP_03	0 groups & 1 users	Backup, Encrypt	Continuous	-	   
PP_04	0 groups & 1 users	Backup	Every Mon, Tue, Wed, Thu and Fri at 06:46 AM	✓	   
pp_05	0 groups & 1 users	Backup	Continuous	✓	   
PP_Android	0 groups & 5 users	Backup	Continuous	-	   
PP_Google	0 groups & 1 users	Backup	Every Mon, Tue, Wed, Thu, Fri and Sun at 06:33 PM	-	   
Protect Any types of files	0 groups & 1 users	Backup	Continuous	✓	   
Protect Office Files only	2 groups & 5 users	Backup	Continuous	✓	   
protect_empty	0 groups & 4 users	Backup	Continuous	-	   
protect_outlook	0 groups & 1 users	Backup	Continuous	✓	   

At the bottom left of the table, there is a red box highlighting the 'Edit' icon (a pencil icon) for the policy 'Protect Any types of files'. The bottom right of the page shows the text '2014 © Vaultize (14.5.27)'.

Any details of the policy can be edited as per your requirement. The screens are same as that of create policy but are prefilled with data.

Edit Protection Policy

X

1 /4 General

Policy Name

Protect Office Files only

Applied to

Groups 2

Users 15

Actions taken when Protection runs on client

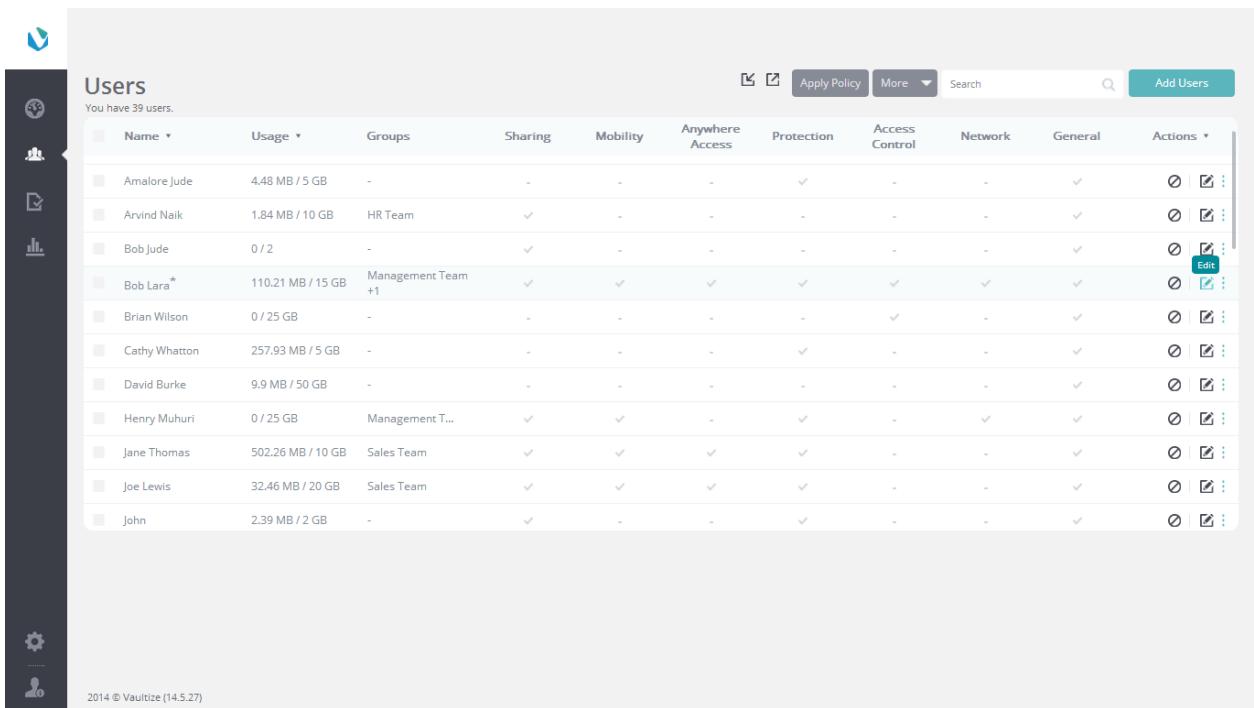
- Backup Filtered Files
- Decrypt Encrypted Files (Applicable for Windows targets only)
- Encrypt Filtered Files (Applicable for Windows targets only)
- Wipe Filtered Files

Cancel

Continue

4.10 Un-applying a Policy

A policy which is applied to a user/group can be unapplied at any point in time. This can be done by clicking on the edit button of the user/group on which the policy is to be unapplied.



Users
You have 39 users.

Name	Usage	Groups	Sharing	Mobility	Anywhere Access	Protection	Access Control	Network	General	Actions
Amalore Jude	4.48 MB / 5 GB	-	-	-	-	✓	-	-	✓	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="button" value="Edit"/>
Arvind Naik	1.84 MB / 10 GB	HR Team	✓	-	-	-	-	-	✓	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="button" value="Edit"/>
Bob Jude	0 / 2	-	✓	-	-	-	-	-	✓	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="button" value="Edit"/>
Bob Lara*	110.21 MB / 15 GB	Management Team +1	✓	✓	✓	✓	✓	✓	✓	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="button" value="Edit"/>
Brian Wilson	0 / 25 GB	-	-	-	-	-	✓	-	✓	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="button" value="Edit"/>
Cathy Whatton	257.93 MB / 5 GB	-	-	-	-	✓	-	-	✓	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="button" value="Edit"/>
David Burke	9.9 MB / 50 GB	-	-	-	-	-	-	-	✓	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="button" value="Edit"/>
Henry Muhuri	0 / 25 GB	Management T...	✓	✓	-	✓	-	✓	✓	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="button" value="Edit"/>
Jane Thomas	502.26 MB / 10 GB	Sales Team	✓	✓	✓	✓	-	-	✓	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="button" value="Edit"/>
Joe Lewis	32.46 MB / 20 GB	Sales Team	✓	✓	✓	✓	-	-	✓	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="button" value="Edit"/>
John	2.39 MB / 2 GB	-	✓	-	-	✓	-	-	✓	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="button" value="Edit"/>

2014 © Vaultize (14.5.27)

The Edit user page comes up.

Edit User Details

X

2 / 2 Edit Applied Policies

Policies

- Sharing Policies
- Share office files only
- Mobility Policies
- Anywhere Access Policies
- Protection Policies
- Access Control Policies
- Network Policies
- General Policies

Policy Details - Share office files only

Time Base Access	mon,tue,wed,thu,fri,sat,sun(12:0 AM - 11:59 PM)
Fencing	
Allowed IP	All
Included Locations	All
Expiry and Password Protection	
Link Expiry	21 Days, 0Hr, 0Min
Require Password	Yes
Notification by mail	Allowed
External Upload	Allowed

Add ↓

Policies to be Unapplied

- Share office files only

Previous Cancel Save

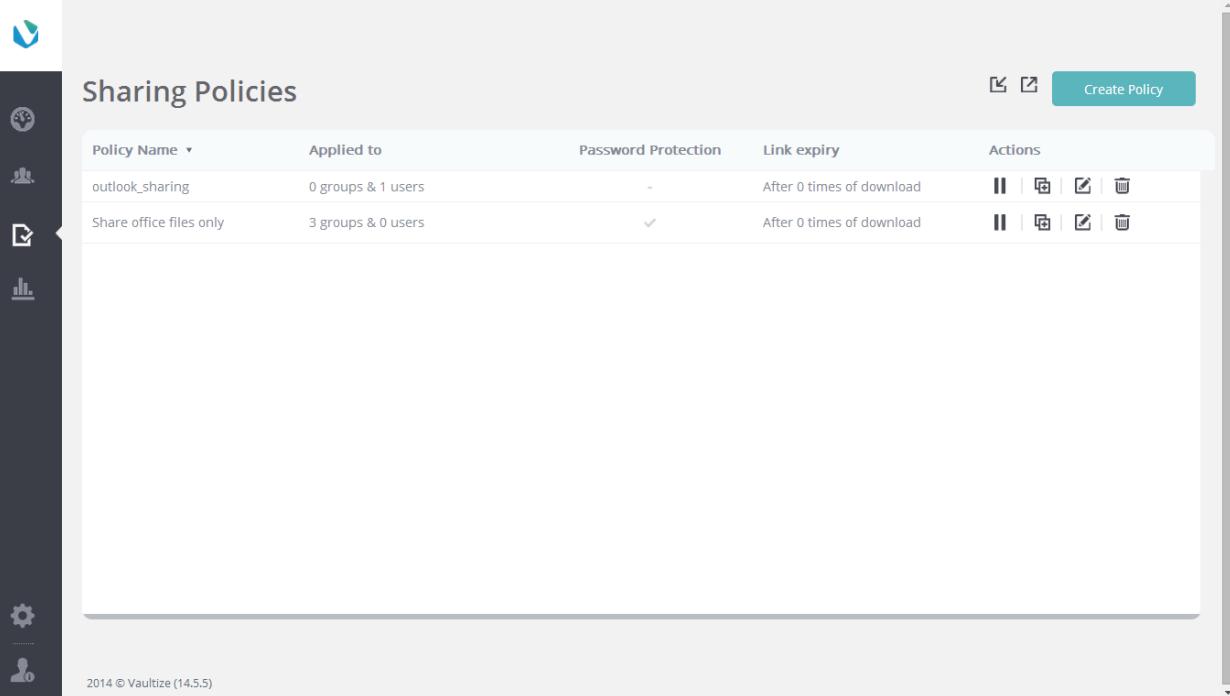
Click “Continue” to go to the “Edit User Details” page. Here, the policies that have been applied to the user/group are shown under “Policies” section. Select the policy that you want to unapply and click on the “Add” button. Now, the selected policy appears in the “Policies to be Unapplied” section. Click on the “Save” button. This will unapply the policy to the selected user/group. This can be verified from user/groups page by clicking the tick under corresponding policy column and checking if its removed.

4.11 Import/export of a policy

In every policy page, there are icons -   on the top. These are for import and export of policies.

Whenever there is a need to back up the policies into the local system, say when there is an upgrade happening, the export functionality can be used.

Similarly, whenever the policies need to be put back into the Vaultize app, say once the upgrade is done, the import functionality can be used.



The screenshot shows the 'Sharing Policies' page in the Vaultize app. The interface includes a sidebar with icons for users, groups, reports, settings, and help. The main area displays a table with two rows of policy information:

Policy Name	Applied to	Password Protection	Link expiry	Actions
outlook_sharing	0 groups & 1 users	-	After 0 times of download	Edit Delete
Share office files only	3 groups & 0 users	✓	After 0 times of download	Edit Delete

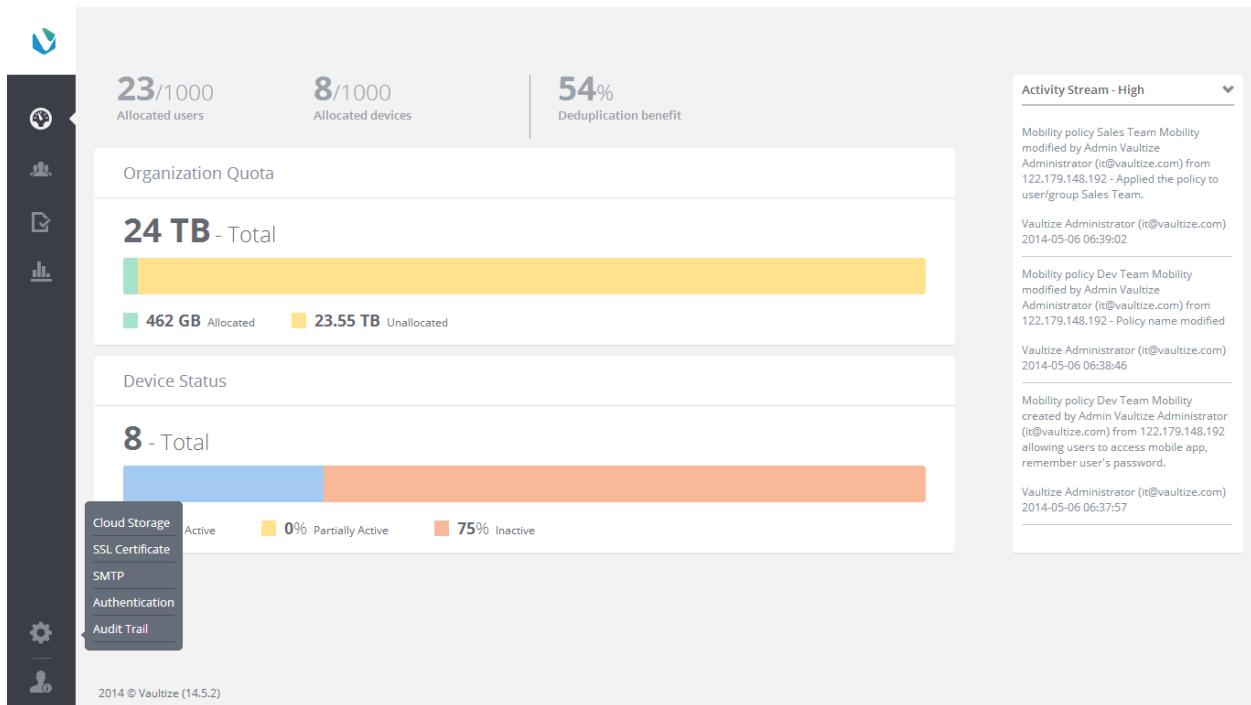
At the top right, there are 'Create Policy' and 'Import' buttons. The bottom of the page shows the footer text '2014 © Vaultize (14.5.5)'.

5 Settings

Vaultize allows you to configure SMTP server, AD/LDAP, Google Apps, Audit Trail, Cloud Storage and SSL Certificate. Each of these is available under Settings tab on the left pane.

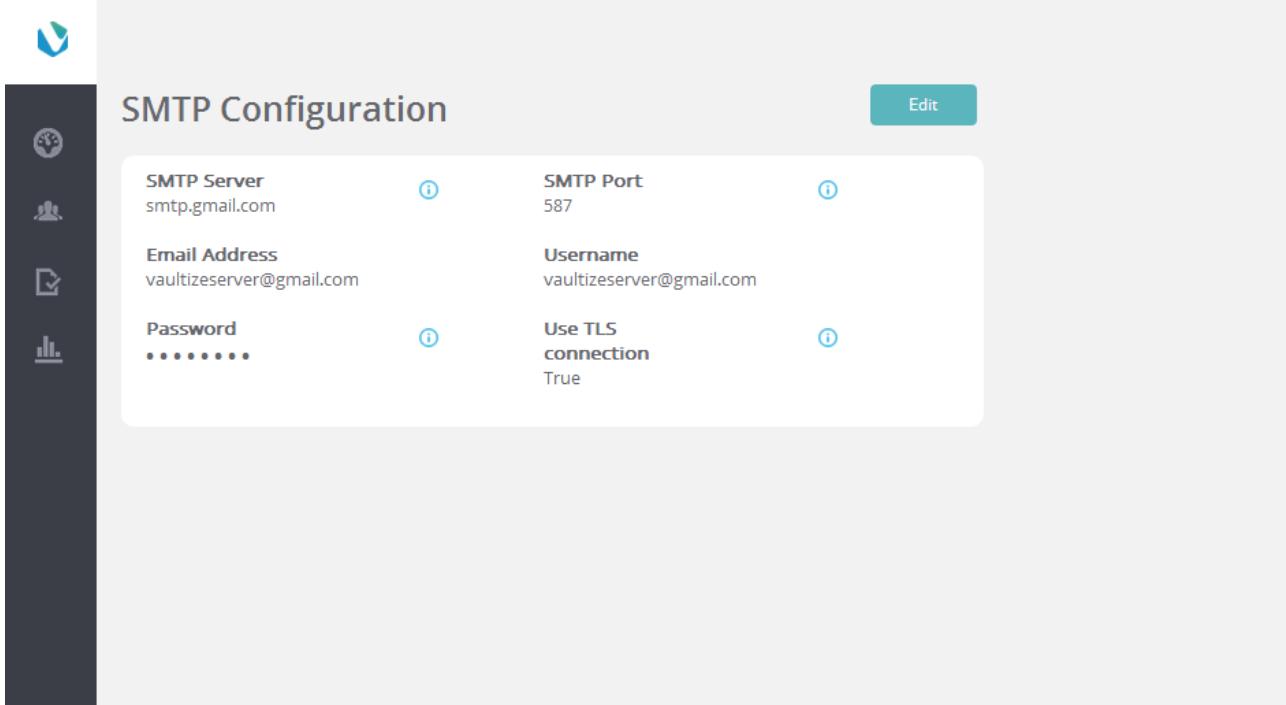
The Settings tab is denoted by - 

Please read corresponding sections to understand the configuration of each of them.



5.1 SMTP

You can access SMTP settings by clicking Settings tab on the left pane and then clicking "SMTP". This page is used to setup the SMTP (Simple Mail Transfer Protocol) server. You need to give the SMTP server IP, Port, Email Address from which mails will be sent on behalf of server, Username and Password with which you login to the server. The option "*Use TLS Connection*" can be selected if your SMTP server is TLS enabled. TLS is used for secure emails.



SMTP Configuration

Edit

SMTP Server	smtp.gmail.com	SMTP Port	587
Email Address	vaultizeserver@gmail.com	Username	vaultizeserver@gmail.com
Password	*****	Use TLS connection	True

The SMTP configuration settings can be changed by clicking the “Edit” button. Here, you can also send a test mail to the specified mail id by clicking “Send Test Mail” button.

Edit SMTP Configuration

X

All fields are mandatory.

SMTP Server

SMTP Port

Email

Username

Password

Confirm Password

Use TLS Connection

Send Test Mail 

Cancel **Done**

5.2 Authentication

This page can be accessed by clicking on “*Settings*” button on the left pane and clicking on “*Authentication*”. This page has AD/LDAP and Google Apps tabs. Each of these can be configured by going to the respective tabs.

Active Directory and LDAP Config:

Vaultize provides an option of enabling LDAP authentication. This is available with either *Private Cloud* or *Cloud in a Box* and not with *Public Cloud*. Once you click on “*Set it up*”, a series of fields appear as shown below.

You need to enter the IP and port of your organization's LDAP server. Base DN (Distinguished Name) is base directory structure where the LDAP search starts. If multiple base DNs are being

given, they have to be separated by semicolon. For example, ou=sales,dc=vaultize,dc=com;ou=qa,dc=vaultize,dc=com where dc denoted Domain Component.

LDAP Manager DN would typically look like cn=John Doe,ou=sales,dc=vaultize,dc=com. Enter the Manager DN and Password in the fields indicated.

Username attribute denotes username with which the LDAP user logs into Vaultize. It can be sAMAccountName/Email/UID etc. Version denotes the version of your LDAP server.

Mapping Attribute denotes the attribute to map to LDAP which can be sAMAccountName/UID/entryUUID. By setting this attribute, changes that happen on LDAP such as a user moving from one group to other, user being added etc. can be tracked based on this unique id. *“Frequency to sync”* indicated the frequency with which we sync LDAP and Vaultize so as to keep the changes like add/delete/move updated.

“Auto import AD/LDAP groups as Vaultize groups” imports AD/LDAP groups into Vaultize server as Vaultize groups. This in turn will automatically add LDAP users to Vaultize.

There is a “*Test Connection*” button which can be used to test if connection is properly established.

Configure AD/LDAP

X

All fields are mandatory.

LDAP server IP	Port
<input type="text" value="192.168.9.29"/>	<input type="text" value="389"/>
Base DN	Username Attribute
<input type="text" value="DC=myorg;DC=com"/>	<input type="text" value="cn"/>
LDAP Manager DN	LDAP Manager Password
<input type="text" value="cn=Administrator;cnUsers;DC=myorg;DC=com"/>	<input type="text" value="*****"/>
Version	
<input type="button" value="LDAP protocol V2"/>	
<input type="button" value="Test Connection"/>	

Configure AD/LDAP

X

2 / 2 Sync Schedule

Auto import AD/LDAP groups as Vaultize groups i

Enable sync i

Mapping attribute i

sAMAccounName

Frequency to sync with AD/LDAP server (in hours)

8

Previous

Cancel

Done

Google Apps:

Create Google Apps configuration

X

OAuth Consumer key

OAuth Consumer Secret

Cancel

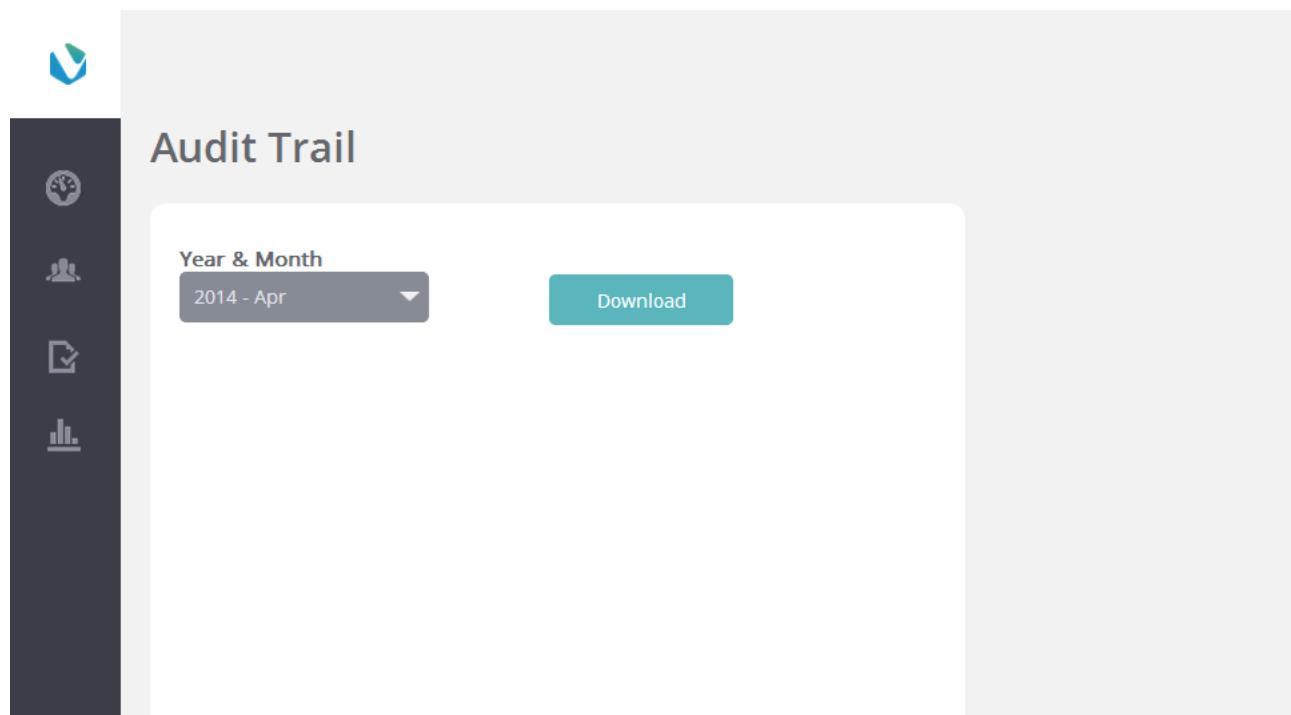
Done

Google Apps can be used to protect user data in google apps like gmail, gdrive etc. For this, you need an *OAuth Consumer Key* and an *OAuth Consumer Secret*. These can be obtained from Google Apps Management console (*Manage this domain* option in Settings). Then please go to

the *Advanced Tools* tab and click on *Manage OAuth domain key*. This page displays your domain's OAuth key and secret. The Key is usually the domain name like myorganization.com. Please select *Enable this consumer key* option to enable OAuth on your domain. Also select the *Allow access to all APIs* option (near the bottom of the page) and click on *Save changes*.

Now, you can auto-register your Google Apps users so that their data can be protected. The registration can be done from Google Apps admin console. To do this, you first need to enable read-only user provisioning in your Google Apps domain. Please login to your Google Apps administration console, go to the *Advanced tools* tab and click on *Manage third party OAuth Client access*. Add a new entry - your domain in *Client Name* field (e.g. myorg.com) and <https://apps-apis.google.com/a/feeds/user/#readonly> (without the quotes) in *One or More API Scopes*. Click on the *Authorize* button. Then, you can create a backup with `$$GOOGLE$$/USERS` as the path, to auto-register your users and keep them in sync. This feature gives the luxury of having a copy of the google apps content on Vaultize which can be obtained onto your local system as well say, when the account is deleted.

5.3 Audit Trail



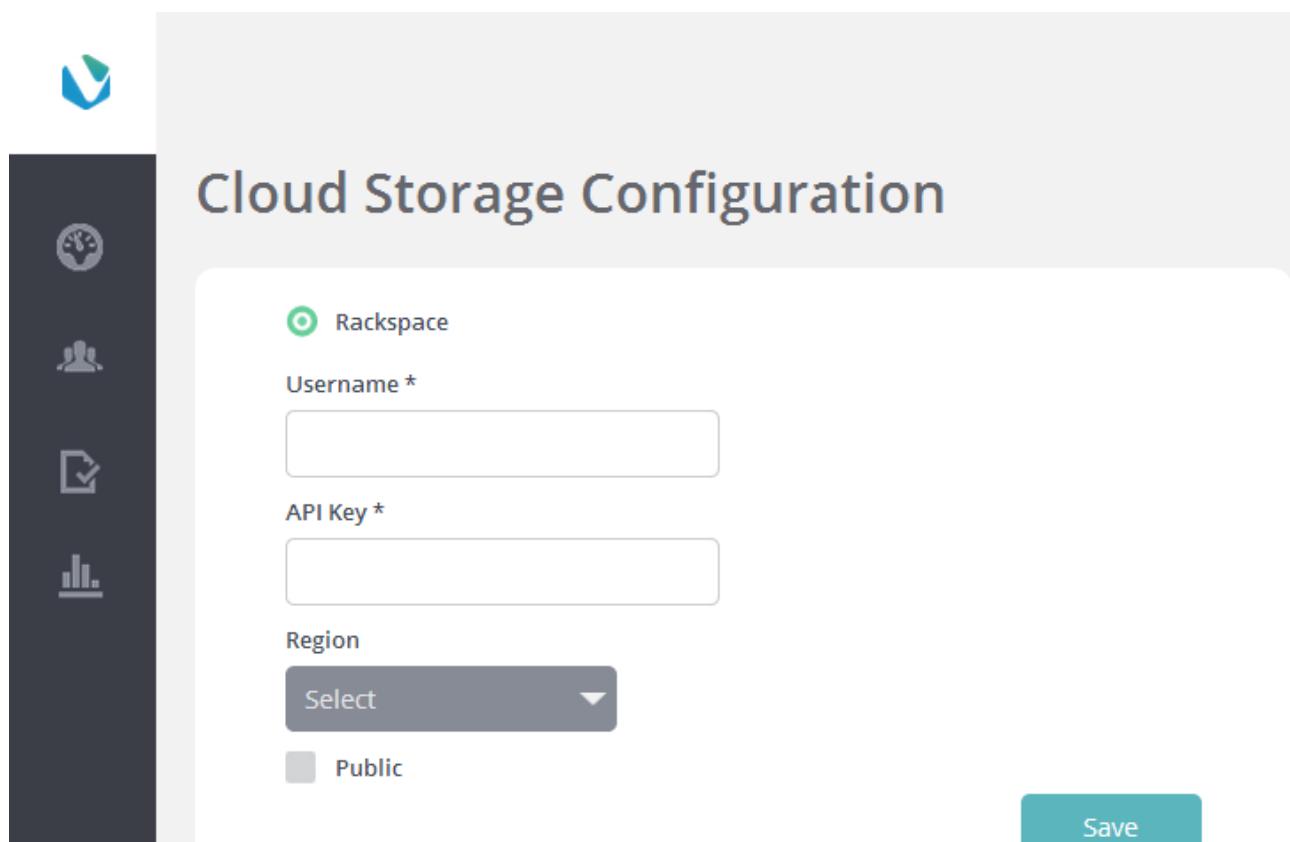
Audit trail can be either enabled or disabled. Once enabled, the audit details corresponding to a particular month and year can be downloaded.

5.4 Cloud Storage Configuration

Vaultize provides 2 options for Cloud Storage- Rackspace and Amazon S3. Organization which has already subscribed to Rackspace/AmazonS3 can utilize that storage along with Vaultize to ensure that data is still stored on the cloud. However, the keys are in control of the organization. So, certain laws that allow agencies to obtain organization data without due notification can be avoided. It also helps in knowing if someone breaks into storage space and steals the data.

Vaultize in this case, can have its installation on premise and utilize cloud storage for encrypted content storage.

5.4.1 Rackspace



The screenshot shows the 'Cloud Storage Configuration' page for Rackspace. The interface includes the following fields:

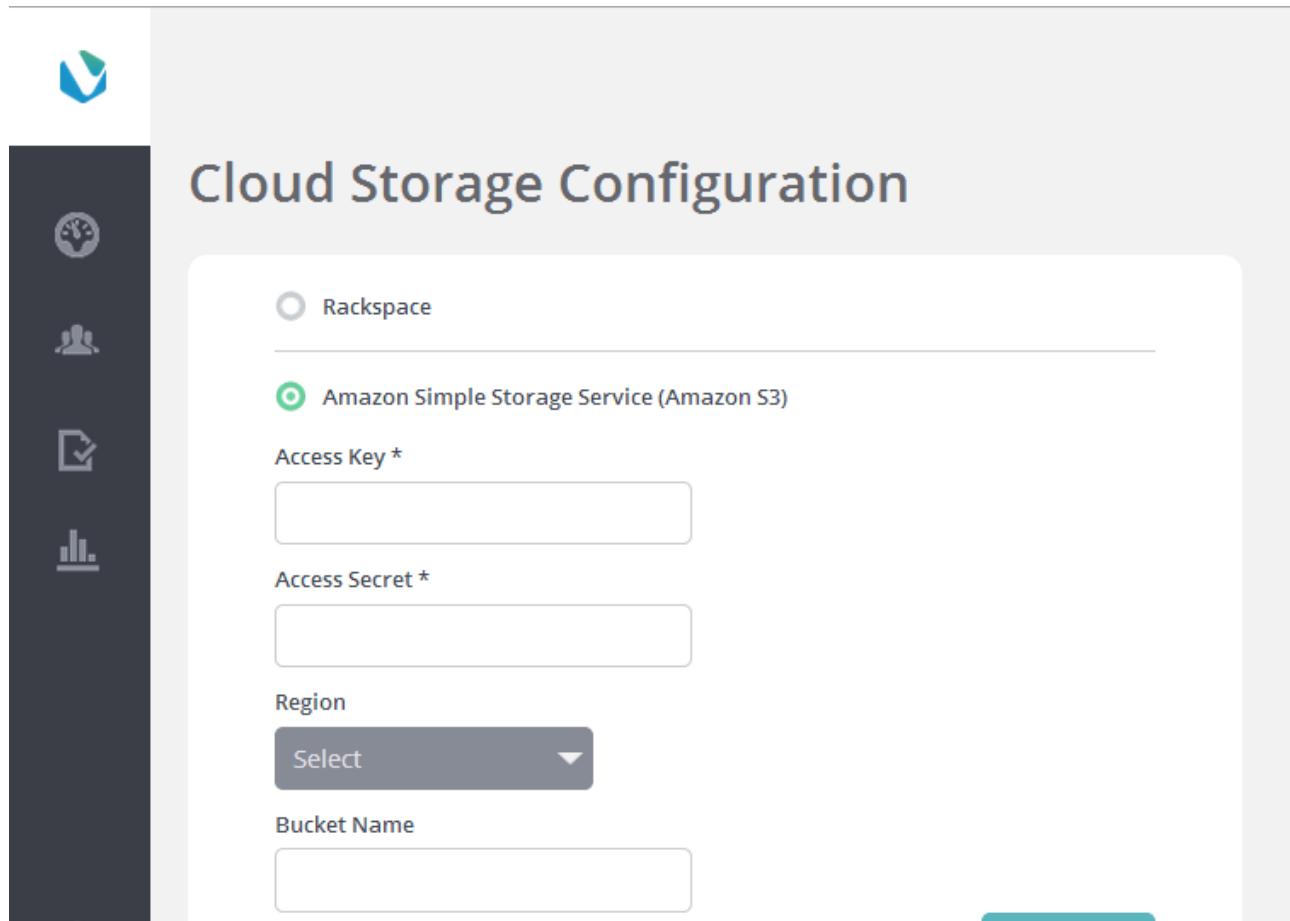
- Username ***: An input field for entering the Rackspace username.
- API Key ***: An input field for entering the Rackspace API key.
- Region**: A dropdown menu with the current selection set to 'Select'.
- Public**: A checkbox labeled 'Public'.

A 'Save' button is located at the bottom right of the form. The sidebar on the left contains icons for users, groups, and metrics.

For private cloud or appliance to act in such a mode as mentioned above, admin can configure cloud storage by providing username, key. Region specifies the data centre of Rackspace. In case admin is not clear about region, he/she can leave it blank. Public checkbox has to be

selected if it is public cloud or else it is treated as private cloud. Enter provided API key in the documentation of Rackspace.

5.4.2 Amazon Simple Storage Service (Amazon S3)



Cloud Storage Configuration

Rackspace

Amazon Simple Storage Service (Amazon S3)

Access Key *

Access Secret *

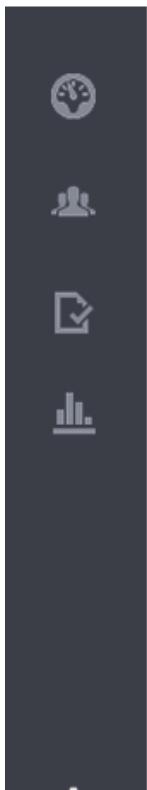
Region

Select

Bucket Name

Enter provided Access Key, Access Secret and Bucket Name in the documentation of Amazon S3. Region specifies the data centre of Amazon S3. In case admin is not clear about region, he/she can leave it blank.

5.5 SSL Certificate Configuration



SSL Certificate Configuration

Private Key *

(PEM encoded)

Public Key Certificate*

(PEM encoded)

Certificate chain

Save

By default Vaultize private cloud or appliance carry a self-signed certificate. Since the certificate is not trusted, anyone accessing this server would receive a certificate warning message in browser. Organizations therefore need to buy a valid certificate for their installation.

Organizations may also use their existing wild card certificate, if they have one. To install a valid certificate on Vaultize server, login as admin, go to SSL Certificate Configuration page (shown below) and provide following in base 64 encoded format-

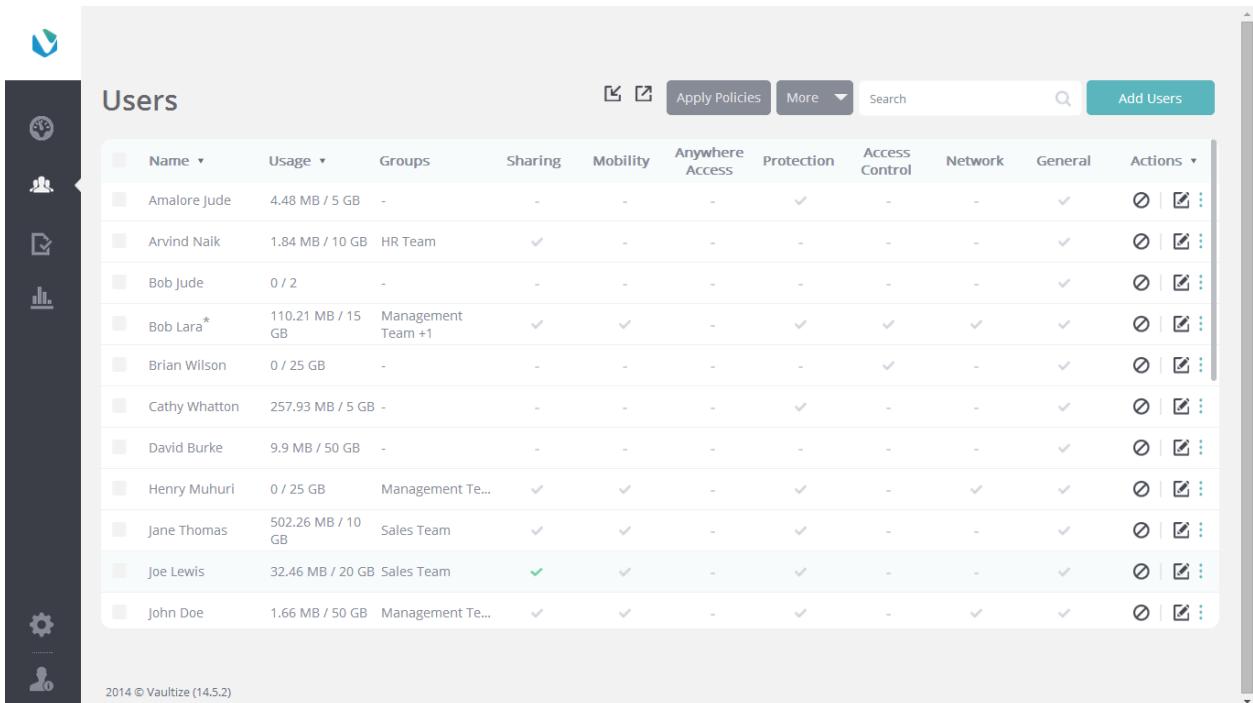
- Private key
- Public key certificate
- Certificate chain – this would contain root CA and subordinate CA.

Please note that the private key must not be in encrypted format.

Once it's saved, close your browser and start a new instance as the communication would break as a result of web server restart.

6 User Management

You can see the user details after you click “Users” menu on the left pane of the screen. For each user, there is a username, memory usage, groups to which he/she belongs, policies applied to the user and actions that can be taken on the user. The list can be sorted on any column.



Name	Usage	Groups	Sharing	Mobility	Anywhere Access	Protection	Access Control	Network	General	Actions
Amalore Jude	4.48 MB / 5 GB	-	-	-	✓	-	-	✓	✓	Block Edit Details
Arvind Naik	1.84 MB / 10 GB	HR Team	✓	-	-	-	-	-	✓	Block Edit Details
Bob Jude	0 / 2	-	-	-	-	-	-	-	✓	Block Edit Details
Bob Lara*	110.21 MB / 15 GB	Management Team +1	✓	✓	-	✓	✓	✓	✓	Block Edit Details
Brian Wilson	0 / 25 GB	-	-	-	-	-	✓	-	✓	Block Edit Details
Cathy Whatton	257.93 MB / 5 GB	-	-	-	✓	-	-	✓	✓	Block Edit Details
David Burke	9.9 MB / 50 GB	-	-	-	-	-	-	-	✓	Block Edit Details
Henry Muhuri	0 / 25 GB	Management Te...	✓	✓	-	✓	-	✓	✓	Block Edit Details
Jane Thomas	502.26 MB / 10 GB	Sales Team	✓	✓	-	✓	-	-	✓	Block Edit Details
Joe Lewis	32.46 MB / 20 GB	Sales Team	✓	✓	-	✓	-	-	✓	Block Edit Details
John Doe	1.66 MB / 50 GB	Management Te...	✓	✓	-	✓	-	✓	✓	Block Edit Details

A new user can be added by clicking “Add Users” and an existing user can be searched using the search box provided on the top of the screen.

Besides, the “Actions” column allows admin to perform various actions on the user profile like block/unblock, edit and delete.

One or more users can be selected and any policy can be applied to them using “Apply Policies” button above the Users list.

If user name or access policies are hovered, additional details about these appear in a popup.

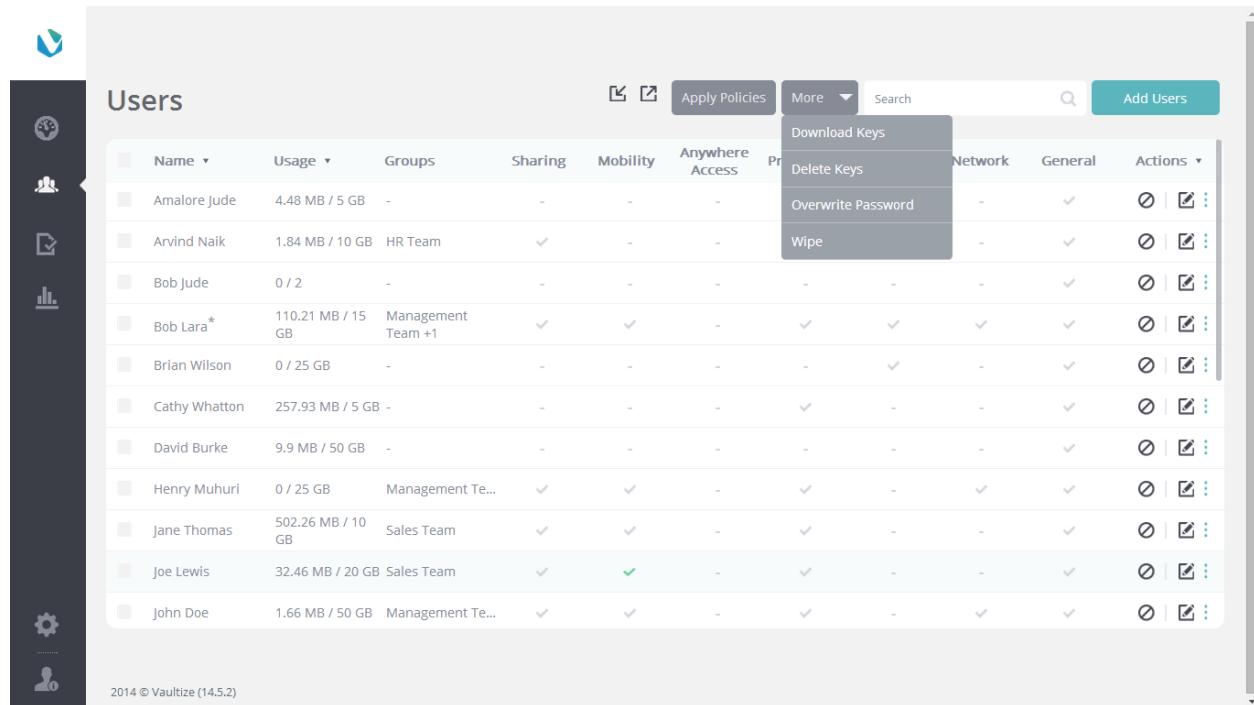
On the top, you see a “More” dropdown. It contains below functionality:

If Data Privacy Option is being implemented and you want to safeguard the user keys, you can do so by clicking —“Download Keys”

You can delete keys from server side using this option. It's used while implementing Data Privacy Option —"Delete Keys"

You can delete user data from all devices by clicking —"Wipe Devices"

You can change the password of user by clicking —"Overwrite Password"



Name	Usage	Groups	Sharing	Mobility	Anywhere Access	Pr	Network	General	Actions
Amalore Jude	4.48 MB / 5 GB	-	-	-	-		-	✓	∅ ☰
Arvind Naik	1.84 MB / 10 GB	HR Team	✓	-	-		-	✓	∅ ☰
Bob Jude	0 / 2	-	-	-	-		-	✓	∅ ☰
Bob Lara*	110.21 MB / 15 GB	Management Team +1	✓	✓	-	✓	✓	✓	∅ ☰
Brian Wilson	0 / 25 GB	-	-	-	-	-	✓	-	∅ ☰
Cathy Whatton	257.93 MB / 5 GB	-	-	-	-	✓	-	✓	∅ ☰
David Burke	9.9 MB / 50 GB	-	-	-	-	-	-	✓	∅ ☰
Henry Muhuri	0 / 25 GB	Management Te...	✓	✓	-	✓	-	✓	∅ ☰
Jane Thomas	502.26 MB / 10 GB	Sales Team	✓	✓	-	✓	-	✓	∅ ☰
Joe Lewis	32.46 MB / 20 GB	Sales Team	✓	✓	-	✓	-	✓	∅ ☰
John Doe	1.66 MB / 50 GB	Management Te...	✓	✓	-	✓	-	✓	∅ ☰

6.1 Create User

You can create a new user by clicking "Add Users" on Users page.

You can create a single user or multiple users at a time.

1. Single User-

Select Type:

When you wish to create a single user, select "Add Individual User".

Add Users

X

1 /2 Select Type

Add Individual User

Add Multiple User

Sync via Active Directory/LDAP

Sync via Google Apps

i

Import users from csv file

Cancel

Continue

Add User:

Add Users



2 / 2 Add Details

Display Name

Email

Quota

Add to groups

Time Zone

Assign Administrator role?

Back

Cancel

Add

Enter the display name, user email, usage quota, groups in which user is to be included, time zone of the user. If the user is an ldap user, you can provide the ldap username in "Display name" field. Also, the user can be provided with admin role while creation itself via the "Assign Administrator role?" drop down.

2. Multiple Users-

Select Type:

You can create multiple users by selecting "Add Multiple Users". There are various options to add multiple users.

- Import Users – This can be done by uploading a .csv file containing users' details. Please make sure to create the .csv file such that each line has each user's email, name and quota separated by commas. Once .csv file is uploaded and you hit "Submit", the pop up disappears and all the users in the file are added.

Add Users

1 /2 Select Type

Add Individual User
 Add Multiple User

Sync via Active Directory/LDAP
 Sync via Google Apps

Import users from csv file (i)

- Sync via Active Directory/LDAP – Users can be synced from Active Directory of the organization by applying search filters. Filters have to be compliant with AD server specifications.

Add Users

X

1 /2 Select Type

Add Individual User

Add Multiple User

Sync via Active Directory/LDAP

Sync via Google Apps

i

Import users from csv file

Cancel

Continue

- Sync via Google Apps – Users can be synced from a google account. Desired users can be selected and added.

Add Users

X

1 /2 Select Type

Add Individual User

Add Multiple User

Sync via Active Directory/LDAP

Sync via Google Apps

Login credentials would be used based upon settings.



Import users from csv file

Cancel

Continue

Select Users:

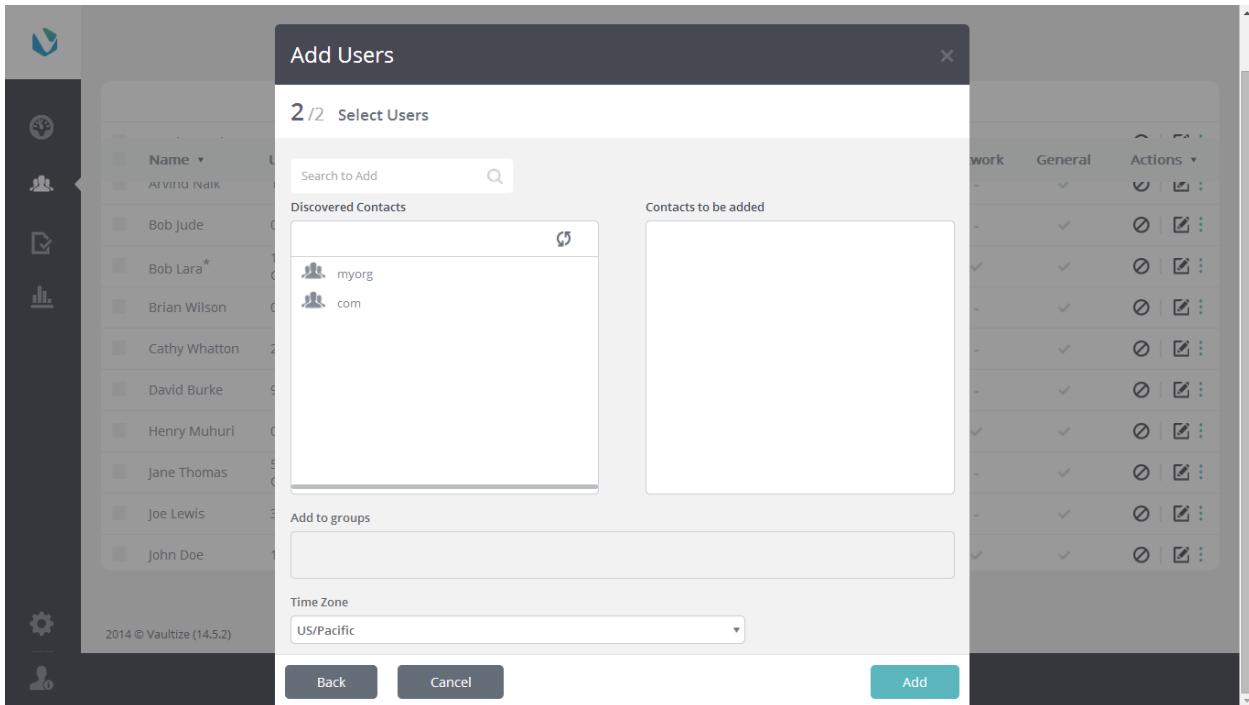
If “AD/LDAP” is configured in “Settings”, the option of “Sync via Active Directory” can be used.

In this case, search criteria can be provided in the search box. For example, ‘cn’ pattern or username can be given there. Filtered results appear and desired users can be selected and added.

If “Google Apps” is configured in “Settings”, the option of “Sync via Google Account” can be used.

In this case, all the google contacts corresponding to the organization which is configured appear in the “Discovered Contacts” list. Desired contacts can be selected and added.

Also, in each case, group(s) in which the users need to be included can be mentioned in Groups field. Also, the time zone of the users can be mentioned.



6.2 Edit User

To edit user information and/or user policies, just select the checkbox across user and click “Edit” under “Actions”. The fields are pre-populated with the current user information and user policies. As shown in the screenshots below, you can change the Email, Name, Quota, Groups, Time zone and Administrative rights of a user.

1 /2 General

Display Name: Arvind Naik

Email: arvind.naik@vaultize.com

Quota: 10 GB

Select Groups to add user in:

- Search to Add
- Organization
- Management Team
- Sales Team
- HR Team

Groups selected:

- Organization
- HR Team

Group's Admin:

Time Zone: US/Pacific

Administrator role: None

Cancel Continue

Also, applied policies to the user can be altered.

2 /2 Edit Applied Policies

Policies:

- Sharing Policies
 - Share office files only
- Mobility Policies
- Anywhere Access Policies
- Protection Policies
- Access Control Policies
- Network Policies
- General Policies

Policy Details - Share office files only

Time Base Access: mon.tue.wed.thu.fri.sat.sun(12:0 AM - 11:59 PM)

Fencing: Allowed IP: All, Included Locations: All

Expiry and Password Protection:

- Link Expiry: 21Days, 0Hr, 0Min
- Require Password: Yes
- Notification by mail: Allowed
- External Upload: Allowed

Add ↓

Policies to be Unapplied:

Previous Cancel Save

6.3 Password Change

You can change password of a user through the “More” dropdown menu on the top right corner of the User list. Select “Overwrite Password” option and enter new password details. Note that change password is irreversible and is effective immediately, so use it with care.

Overwrite Password

All fields are mandatory.

New Password

Minimum 8 characters required.

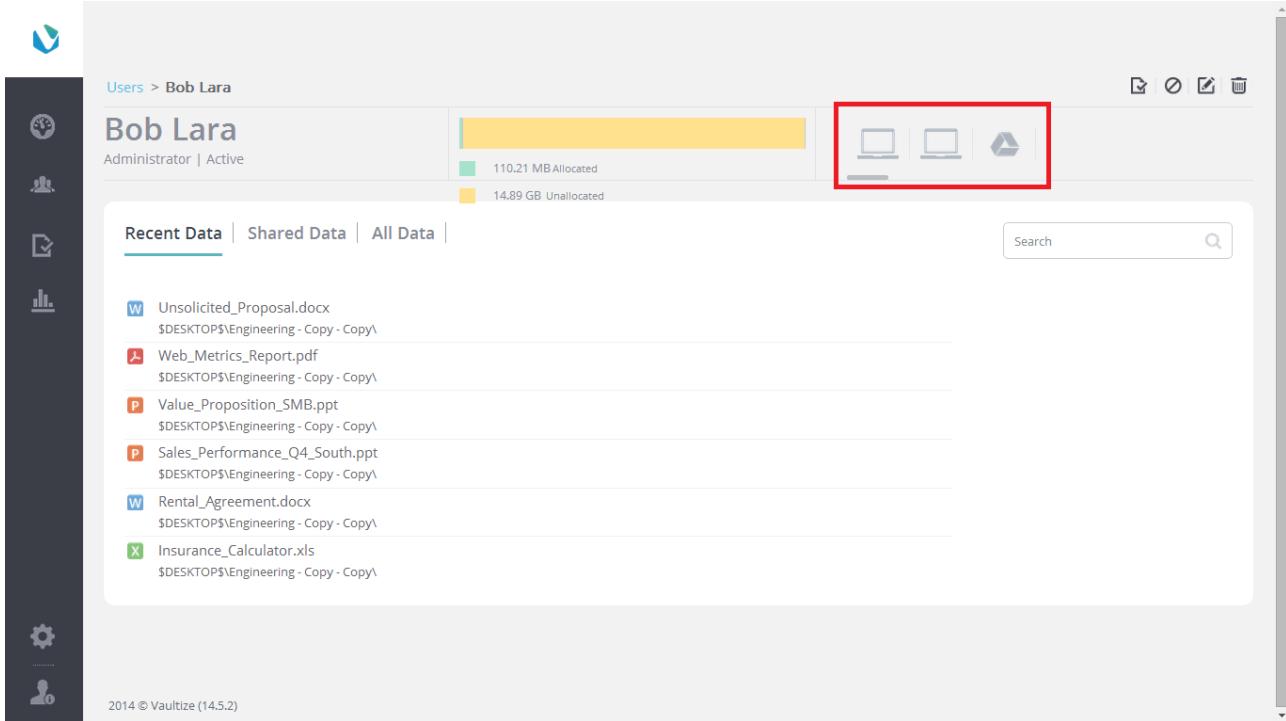
Confirm Password

Cancel **Save**

NOTE: To restrict the user from the using Vaultize, use Block feature. Changing the password will not restrict a user from using Vaultize.

6.4 View a User

When we click on a user from the list, the user details page appears. Here, user details such as user's display name, usage quota details, if user is admin/user, if user is blocked/unblocked etc., are shown.



Users > Bob Lara

Bob Lara
Administrator | Active

110.21 MB Allocated
14.89 GB Unallocated

Recent Data | Shared Data | All Data |

Search

Recent Data:

- W Unsolicited_Proposal.docx
\$DESKTOP\$\\Engineering - Copy - Copy\\
- A Web_Metrics_Report.pdf
\$DESKTOP\$\\Engineering - Copy - Copy\\
- P Value_Proposition_SMB.ppt
\$DESKTOP\$\\Engineering - Copy - Copy\\
- P Sales_Performance_Q4_South.ppt
\$DESKTOP\$\\Engineering - Copy - Copy\\
- W Rental_Agreement.docx
\$DESKTOP\$\\Engineering - Copy - Copy\\
- X Insurance_Calculator.xls
\$DESKTOP\$\\Engineering - Copy - Copy\\

2014 © Vaultize (14.5.2)

Also, various actions that can be taken on user like edit, block, delete are also available.

There are 3 tabs in the page. The first one shows recent data that was protected by the user or shared to the user. In other words, it's the recent activity in a user's Vault. The second tab shows data that was shared to/by the user. The third tab shows all data corresponding to the user's Vault.

All the devices associated with the user are shown in graphical format. They are highlighted in red in the above screenshot. When each of these devices is clicked, a pop up appears where you can see details like name, status, ip, device type, last synced date and time etc.,. A sample pop up is shown below.

DELL-PC

X

Name : Bob Lara's Laptop

Status : Inactive

Last IP : -

Device Type : Laptop

Vaultize Version : 14.04.08

OS Version : Windows 7

Last Synced : -

Last Access : 2014-04-15 17:40:41

Device Name : DELL-PC

Block

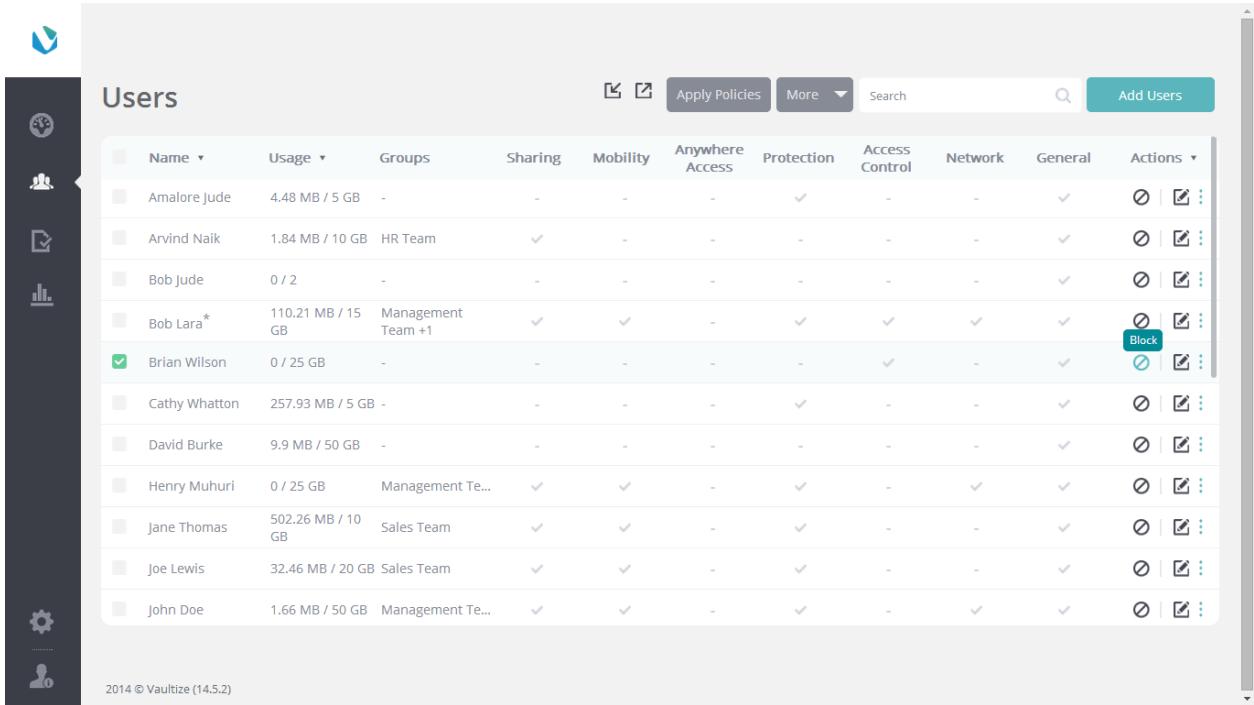
Wipe

Purge

Dismiss

6.5 Block a User

You can block a user through the “*Block*” option in “*Actions*” column on Users screen.



Name	Usage	Groups	Sharing	Mobility	Anywhere Access	Protection	Access Control	Network	General	Actions
Amalore Jude	4.48 MB / 5 GB	-	-	-	-	✓	-	-	✓	Block Edit More
Arvind Naik	1.84 MB / 10 GB	HR Team	✓	-	-	-	-	-	✓	Block Edit More
Bob Jude	0 / 2	-	-	-	-	-	-	-	✓	Block Edit More
Bob Lara*	110.21 MB / 15 GB	Management Team +1	✓	✓	-	✓	✓	✓	✓	Block Edit More
<input checked="" type="checkbox"/> Brian Wilson	0 / 25 GB	-	-	-	-	✓	-	-	✓	Block Edit More
Cathy Whatton	257.93 MB / 5 GB	-	-	-	✓	-	-	-	✓	Block Edit More
David Burke	9.9 MB / 50 GB	-	-	-	-	-	-	-	✓	Block Edit More
Henry Muhuri	0 / 25 GB	Management Te...	✓	✓	-	✓	-	✓	✓	Block Edit More
Jane Thomas	502.26 MB / 10 GB	Sales Team	✓	✓	-	✓	-	-	✓	Block Edit More
Joe Lewis	32.46 MB / 20 GB	Sales Team	✓	✓	-	✓	-	-	✓	Block Edit More
John Doe	1.66 MB / 50 GB	Management Te...	✓	✓	-	✓	-	✓	✓	Block Edit More

After you block a user, the Vaultize software of that user's device will not be able to perform any operation or send any data to the cloud. This will also invalidate the user's password denying all access including his/her My Vaultize account. This operation takes effect within a few minutes. You can use this operation when somebody leaves your organization.

You will not be able to edit the user details or change permissions for a blocked user. The following screenshot shows a blocked user. Once a user is blocked, "Unblock" sign appears across the user in the place of "Block" sign as shown below.

Name	Usage	Groups	Sharing	Mobility	Anywhere Access	Protection	Access Control	Network	General	Actions
Amalore Jude	4.48 MB / 5 GB	-	-	-	-	✓	-	-	✓	Block Unblock Edit More
Arvind Naik	1.84 MB / 10 GB	HR Team	✓	-	-	-	-	-	✓	Block Unblock Edit More
Bob Jude	0 / 2	-	-	-	-	-	-	-	✓	Block Unblock Edit More
Bob Lara*	110.21 MB / 15 GB	Management Team +1	✓	✓	-	✓	✓	✓	✓	Block Unblock Edit More
Brian Wilson	0 / 25 GB	-	-	-	-	✓	-	-	✓	Block Unblock Edit More
Cathy Whatton	257.93 MB / 5 GB	-	-	-	-	✓	-	-	✓	Block Unblock Edit More
David Burke	9.9 MB / 50 GB	-	-	-	-	-	-	-	✓	Block Unblock Edit More
Henry Muhuri	0 / 25 GB	Management Te...	✓	✓	-	✓	-	✓	✓	Block Unblock Edit More
Jane Thomas	502.26 MB / 10 GB	Sales Team	✓	✓	-	✓	-	-	✓	Block Unblock Edit More
Joe Lewis	32.46 MB / 20 GB	Sales Team	✓	✓	-	✓	-	-	✓	Block Unblock Edit More
John Doe	1.66 MB / 50 GB	Management Te...	✓	✓	-	✓	-	✓	✓	Block Unblock Edit More

2014 © Vaultize (14.5.2)

You can unblock a user by clicking the “Unblock” icon and toggling the action from block to unblock. When this is done, a pop up appears asking for password change.

Overwrite Password

All fields are mandatory.

New Password

Password strength : Strong

Confirm Password

Cancel
Save

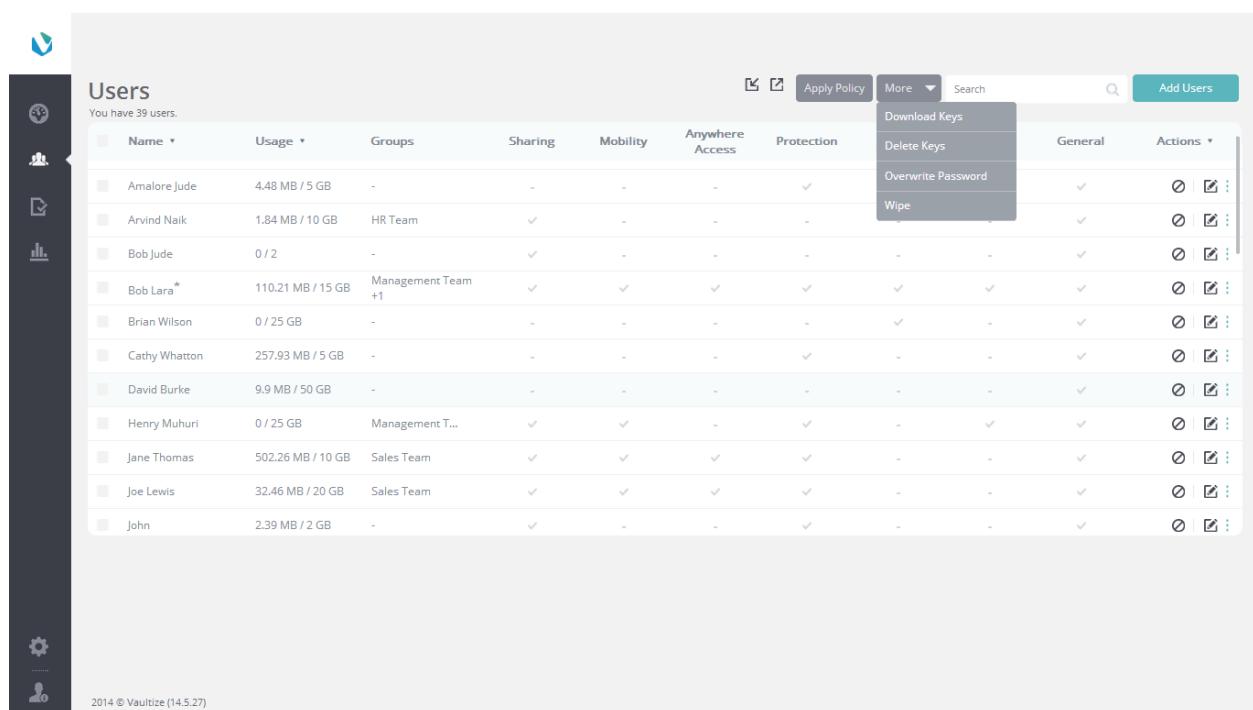
Please enter a new password and share it with the user. The user can now login with this new

password. This will re-activate the user. Once logged in, the user can change his/her password.

NOTE: When an AD/LDAP user is unblocked, password change option does not appear. He/she can resume his/her activities as before.

6.6 Download Keys

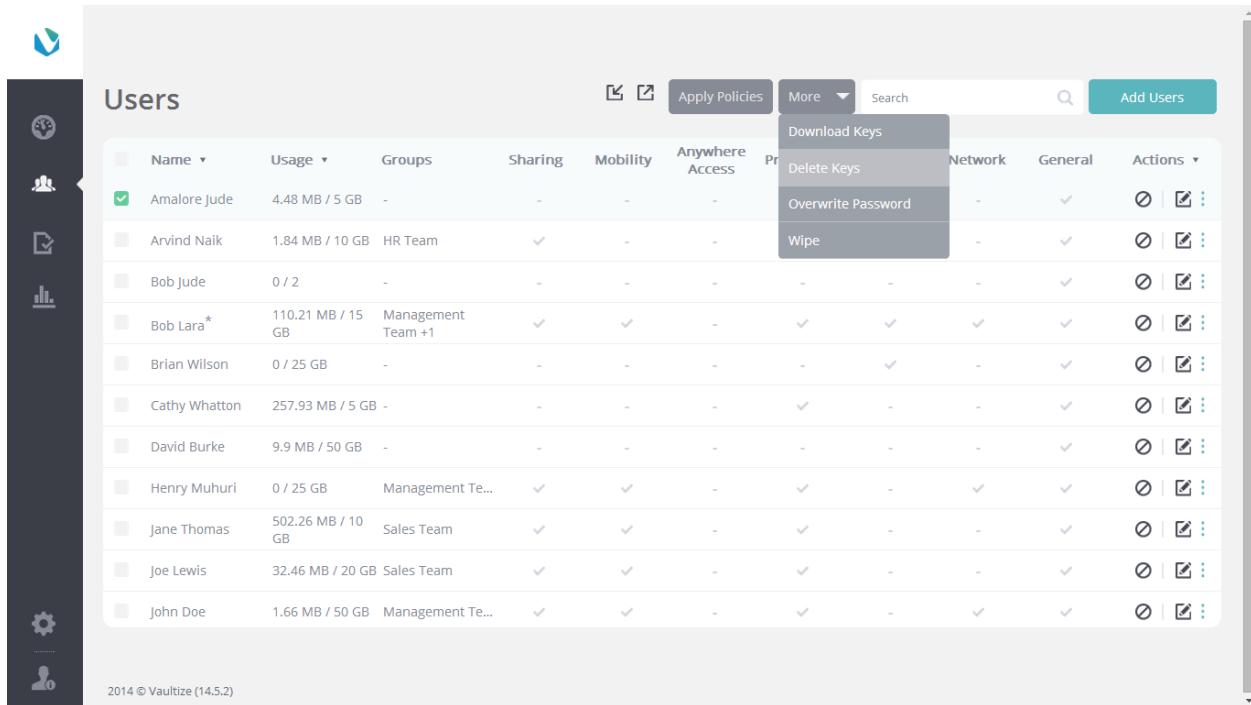
Every user has a unique key generated for him/her. The key is generated at the client and a copy of it is kept at the server as well. This unique key is used to encrypt data of the corresponding user. Every organization must keep these keys private and secure (prevent loss). Some organizations may prefer to implement **DPO (Data Privacy Option)**. This is a great way to ensure further security as it ensures that customers retain full control over encryption keys. If this option is implemented, all user keys should first be downloaded by the admin and then deleted at the server side. This can be done by clicking the “Download Keys” option in “More” dropdown. These downloaded keys must be stored safely for any future use. Then, “Delete Keys” button must be clicked to delete the keys from server-side.



The screenshot shows the 'Users' page of the Vaultize Admin Guide. On the left is a sidebar with icons for users, groups, and settings. The main area shows a table of users with columns for Name, Usage, Groups, Sharing, Mobility, Anywhere Access, and Protection. A 'More' dropdown menu is open, showing options: Download Keys (selected), Delete Keys, Overwrite Password, and Wipe. The 'Download Keys' option is highlighted with a red box. The 'Actions' column contains checkboxes for each user. At the bottom left of the main area, it says '2014 © Vaultize (14.5.27)'.

6.7 Delete Keys

If you select one or more users and click on “Delete Keys” under “More” dropdown, web access, mobile access, and sharing over web for those users will be disabled irreversibly. Please use the feature with caution. Also, it is strongly advised to download the keys before performing this operation.



The screenshot shows the 'Users' page in the Vaultize Admin interface. A context menu is open over a selected user, with 'Delete Keys' highlighted. The menu also includes 'Download Keys', 'Overwrite Password', and 'Wipe'. The table lists various users with their names, usage, groups, and access permissions. The 'Actions' column for each user includes icons for edit, delete, and more.

Name	Usage	Groups	Sharing	Mobility	Anywhere Access	Actions
Amalope Jude	4.48 MB / 5 GB	-	-	-	-	  
Arvind Naik	1.84 MB / 10 GB	HR Team		-	-	  
Bob Jude	0 / 2	-	-	-	-	  
Bob Lara*	110.21 MB / 15 GB	Management Team +1			-	  
Brian Wilson	0 / 25 GB	-	-	-	-	  
Cathy Whatton	257.93 MB / 5 GB	-	-	-	-	  
David Burke	9.9 MB / 50 GB	-	-	-	-	  
Henry Muhuri	0 / 25 GB	Management Te...			-	  
Jane Thomas	502.26 MB / 10 GB	Sales Team			-	  
Joe Lewis	32.46 MB / 20 GB	Sales Team			-	  
John Doe	1.66 MB / 50 GB	Management Te...			-	  

6.8 Wipe

You can select one or more users and click on “Wipe Devices” under “More” dropdown. This will permanently wipe off all data under Vaultize from all the devices of the selected users. Also, the users will be blocked.

Name	Usage	Groups	Sharing	Mobility	Anywhere Access	Pr	Network	General	Actions
Amalore Jude	4.48 MB / 5 GB	-	-	-	-	Download Keys	-	✓	∅ 🗑
Arvind Naik	1.84 MB / 10 GB	HR Team	✓	-	-	Delete Keys	-	✓	∅ 🗑
Bob Jude	0 / 2	-	-	-	-	Overwrite Password	-	✓	∅ 🗑
Bob Lara*	110.21 MB / 15 GB	Management Team +1	✓	✓	-	Wipe	-	✓	∅ 🗑
Brian Wilson	0 / 25 GB	-	-	-	-		-	✓	∅ 🗑
Cathy Whatton	257.93 MB / 5 GB	-	-	-	-		-	✓	∅ 🗑
David Burke	9.9 MB / 50 GB	-	-	-	-		-	✓	∅ 🗑
Henry Muhuri	0 / 25 GB	Management Te...	✓	✓	-		-	✓	∅ 🗑
Jane Thomas	502.26 MB / 10 GB	Sales Team	✓	✓	-		-	✓	∅ 🗑
Joe Lewis	32.46 MB / 20 GB	Sales Team	✓	✓	-		-	✓	∅ 🗑
John Doe	1.66 MB / 50 GB	Management Te...	✓	✓	-		-	✓	∅ 🗑

2014 © Vaultize (14.5.2)

6.9 Purge User Files

Admin can delete user files using his/her Admin account. Upon doing this, the file(s) are deleted from the server. However, this action(of deletion of files of a user) has to be approved by the registered ‘approvers’. While creation of an admin account, data deletion approvers’ email ids are to be given. Now, these approvers are sent mails regarding the data deletion action taken by the admin. The approvers can either Accept/Reject the data deletion. If all the approvers Accept the deletion, file is deleted. Even if 1 approver doesn’t Accept the deletion, the file is not deleted.

The below screen shows the “Purge” option that an admin has over the files of the users:

The screenshot shows the Vaultize Admin Guide interface. On the left is a sidebar with icons for users, devices, reports, and settings. The main area is titled 'Users > Bob Lara' and shows 'Bob Lara' as an 'Administrator | Active' user. A progress bar indicates '110.21 MB Used' (green) and '14.89 GB Unused' (yellow). Below the progress bar are icons for a desktop and a laptop. The 'All Data' tab is selected, showing a list of data items: 'Engineering - Copy' (DELL-PC), 'Engineering' (DELL-PC), 'GetData' (DELL-PC), 'HR-Data' (DELL-PC), 'Sales-data' (DELL-PC), and 'Vaultize-Client' (DELL-PC). A 'Purge' button is located to the right of the data list. A search bar is at the top right, and a 'Search' button is to its right. The bottom left of the main area shows the text '2014 © Vaultize (14.5.27)'.

6.10 Purge User Devices

Admin can purge user devices. This means, admin can select a user device as shown below and click on "Purge" button. This will unregister the user device from Vaultize server. This feature is helpful when a user decides to no longer use the device.

DELL-PC

X

Name : Bob Lara's Laptop

Status : Inactive

Last IP : -

Device Type : Laptop

Vaultize Version : 14.04.08

OS Version : Windows 7

Last Synced : -

Last Access : 2014-04-15 17:40:41

Device Name :

Block

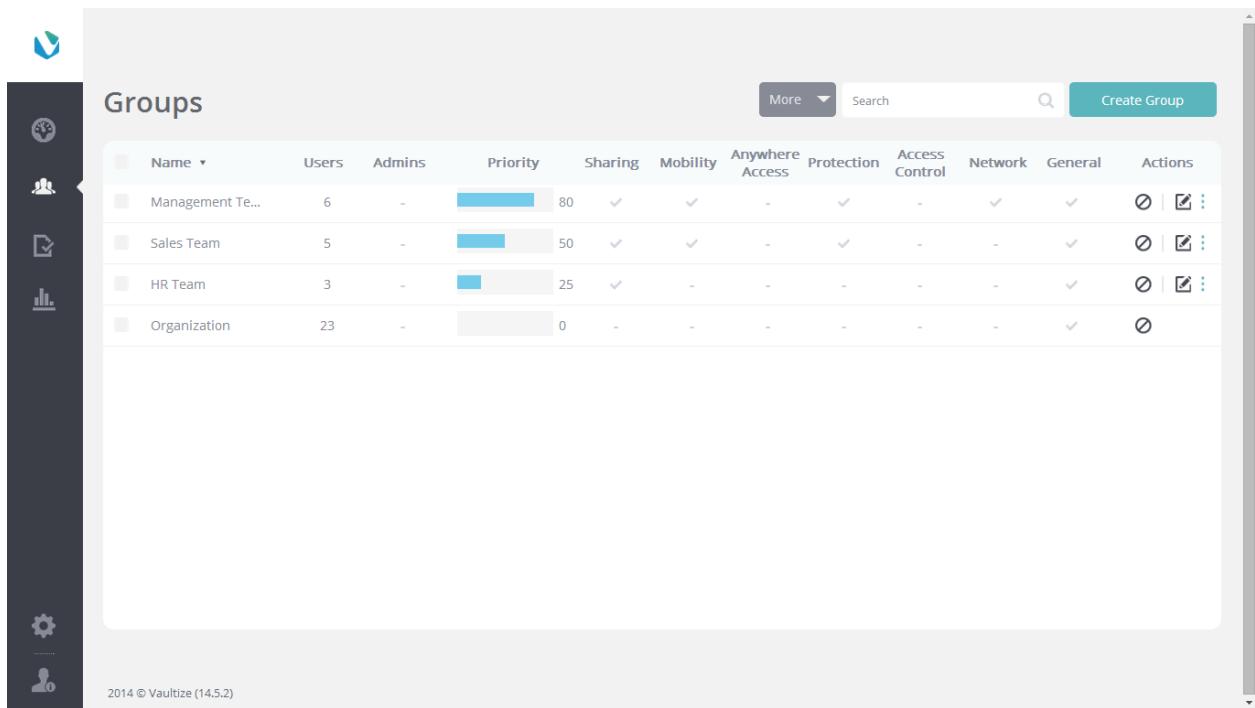
Wipe

Purge

Done

7 Groups

Groups are created for a logical grouping of users under your organization. Each group is given a name, priority, admin, policies and list of users. Groups are displayed on decreasing priority in the list. Each user can be part of multiple groups. As a result if there is any conflict, it is resolved based on the priority. Higher the priority number, higher the priority given to the group. For example, if group 1 has priority 50 and group 2 has priority 45, group1 has a higher priority. Each organization will have a default group called the “Organization”. This group includes all the users of the organization.



The screenshot shows a table titled "Groups" with the following data:

Name	Users	Admins	Priority	Sharing	Mobility	Anywhere Access	Protection	Access Control	Network	General	Actions
Management Te...	6	-	80	✓	✓	-	✓	-	✓	✓	∅ 
Sales Team	5	-	50	✓	✓	-	✓	-	-	✓	∅ 
HR Team	3	-	25	✓	-	-	-	-	-	✓	∅ 
Organization	23	-	0	-	-	-	-	-	-	✓	∅

2014 © Vaultize (14.5.2)

The “More” drop down enables us to take various actions like Overwrite Password /Delete Keys/ Wipe Devices /Download keys. The effect of these actions would be the same as explained in the corresponding sections for users. When these actions are applied to a group, they are applied to all the users of the group.

A user can be part of one/more groups or can be part of none of the groups. Find the below screen as an illustration:

Name	Usage	Groups	Sharing	Mobility	Anywhere Access	Protection	Access Control	Network	General	Actions
Amalore Jude	4.48 MB / 5 GB	-	-	-	-	✓	-	-	✓	
Arvind Naik	1.84 MB / 10 GB	HR Team	✓	-	-	-	-	-	✓	
Bob Jude	0 / 2	-	-	-	-	-	-	-	✓	
Bob Lara*	110.21 MB / 15 GB	Management Team +1	✓	✓	-	✓	✓	✓	✓	
Brian Wilson	0 / 25 GB	-	-	-	-	✓	-	-	✓	
Cathy Whatton	257.93 MB / 5 GB	-	-	-	✓	-	-	-	✓	
David Burke	9.9 MB / 50 GB	-	-	-	-	-	-	-	✓	
Henry Muhuri	0 / 25 GB	Management Te...	✓	✓	-	✓	-	✓	✓	
Jane Thomas	502.26 MB / 10 GB	Sales Team	✓	✓	-	✓	-	-	✓	
Joe Lewis	32.46 MB / 20 GB	Sales Team	✓	✓	-	✓	-	-	✓	
John Doe	1.66 MB / 50 GB	Management Te...	✓	✓	-	✓	-	✓	✓	

2014 © Vaultize (14.5.2)

When you click on a group, the Group Details page appears as below. It contains details like the users in the group along with their usage quota, policies etc.

Also, there is an "Actions" column that allows us to block/unblock the user, pause/resume the user, edit a user and delete a user.

In AD based deployments, the AD groups would be directly synced with Vaultize. Hence, it will be very easy to manage and apply policies based on AD groups. For configuring AD, refer to section 5.2 "Authentication".

To view the group member list, just click on Group Name.

Name	Usage	Groups	Sharing	Mobility	Anywhere Access	Protection	Access Control	Network	General	Actions
Bob Lara*	110.21 MB / 15 GB	Management Team +1	✓	✓	-	✓	✓	✓	✓	⋮
Henry Muhuri	0 / 25 GB	Management Te...	✓	✓	-	✓	-	✓	✓	⋮
John Doe	1.66 MB / 50 GB	Management Te...	✓	✓	-	✓	-	✓	✓	⋮
John Lennon	2.66 MB / 15 GB	Management Te...	✓	✓	-	✓	-	✓	✓	⋮
Maria Miller	0 / 20 GB	Management Te...	✓	✓	-	✓	-	✓	✓	⋮
Tu Le	0 / 25 GB	Management Te...	✓	✓	-	✓	-	✓	✓	⋮

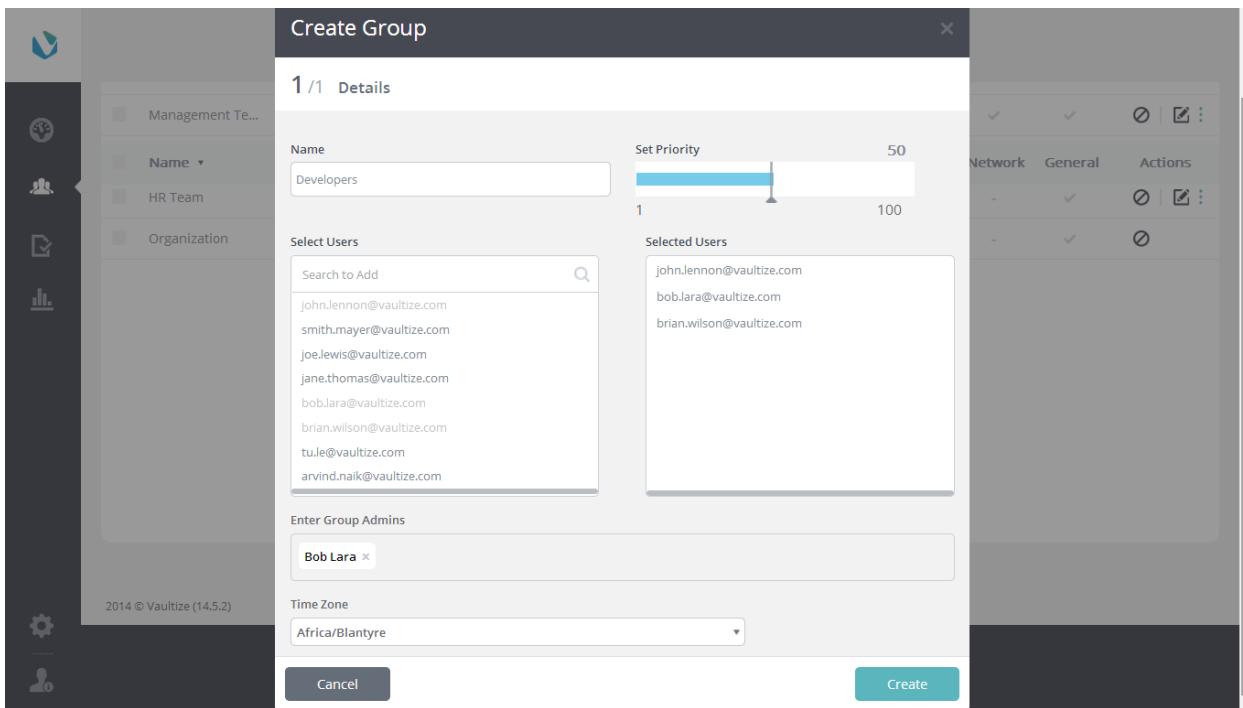
2014 © Vaultize (14.5.2)

7.1 Creating New Group

General:

From the Groups list page click “Create Group” button. Enter a group name and set the group priority in the range of 0-100. Select users to be part of the group. You can assign a group admin and select a time zone for the group.

For each group, you could define one or more users as its admin. The group admins may or may not be a member of the group. A user with group admin privilege would see option to switch to admin’s role from the Profile tab.



7.2 Editing a Group

The pages for editing a group are same as that of creating a group but the fields are prepopulated with details which can be edited. For example, the users in a group can be modified and so can the applied policies be.

Edit Group

1 / 2 Edit Details

Name HR Team **Set Priority** 25

Select Users

Search to Add

john.lennon@vaultize.com
smith.mayer@vaultize.com
joe.lewis@vaultize.com
jane.thomas@vaultize.com
bob.lara@vaultize.com
brian.wilson@vaultize.com
tule@vaultize.com
arvind.naik@vaultize.com

Selected Users

arvind.naik@vaultize.com
julia.bucket@vaultize.com
nigel.clegg@vaultize.com

Enter Group Admins

Time Zone UTC

Cancel **Continue**

Edit Group

2 / 2 Remove Applied Policies

Policies

- Sharing Policies
 - Share office files only
- Mobility Policies
- Anywhere Access Policies
- Protection Policies
- Access Control Policies
- Network Policies
- General Policies

Policy Details - Share office files only

Time Base Access
mon,tue,wed,thu,fri,sat,sun(12:0 AM - 11:59 PM)

Fencing
Allowed IP All
Included Locations All

Expiry and Password Protection
Link Expiry 21Days, 0Hr, 0Min
Require Password Yes
Notification by mail Allowed
External Upload Allowed

Add ↓

Policies to be Unapplied

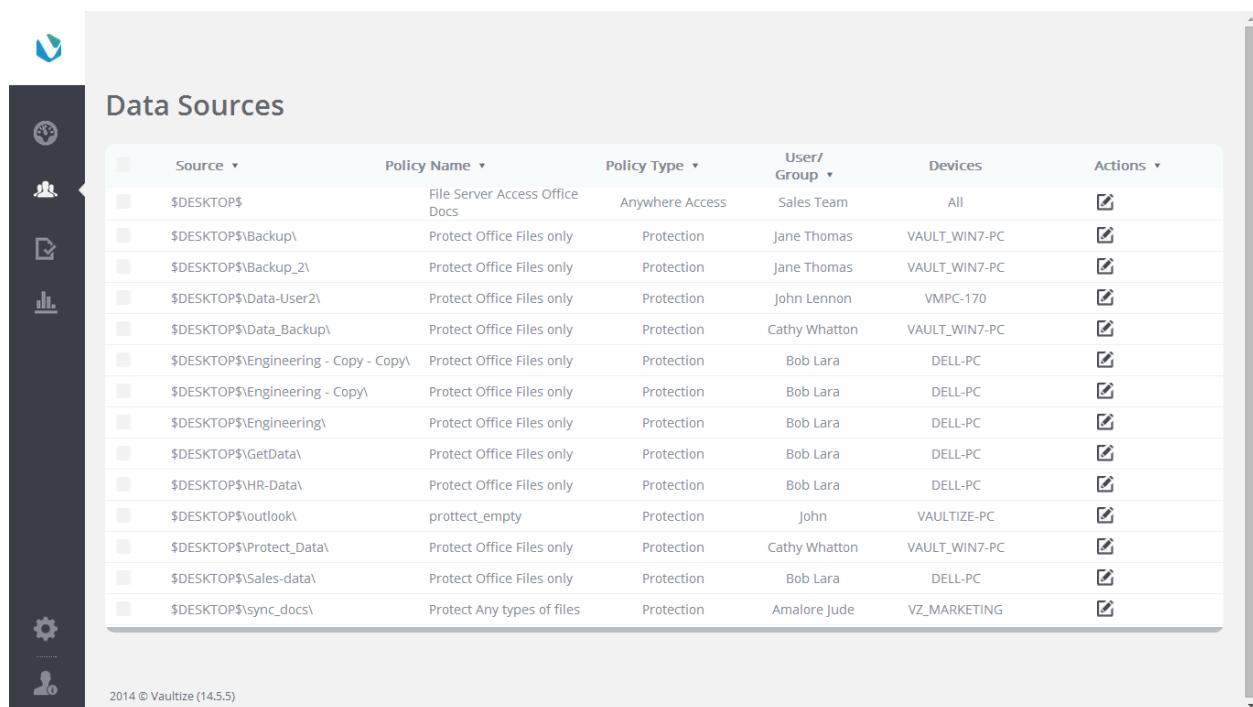
Previous **Cancel** **Save**

8 Data Sources

Data Sources page lists all the sources of data for data protection, sync, sharing etc. It is a list which displays the source of data say, Outlook folder along with other details like policy applied on the data source, policy type, users to whom the policy is applied and devices that are included.

The primary use of this feature is that the administrator can modify the details like say, a mistyped folder name. Hence, each entry has an option to be edited.

A typical data sources page looks as below:



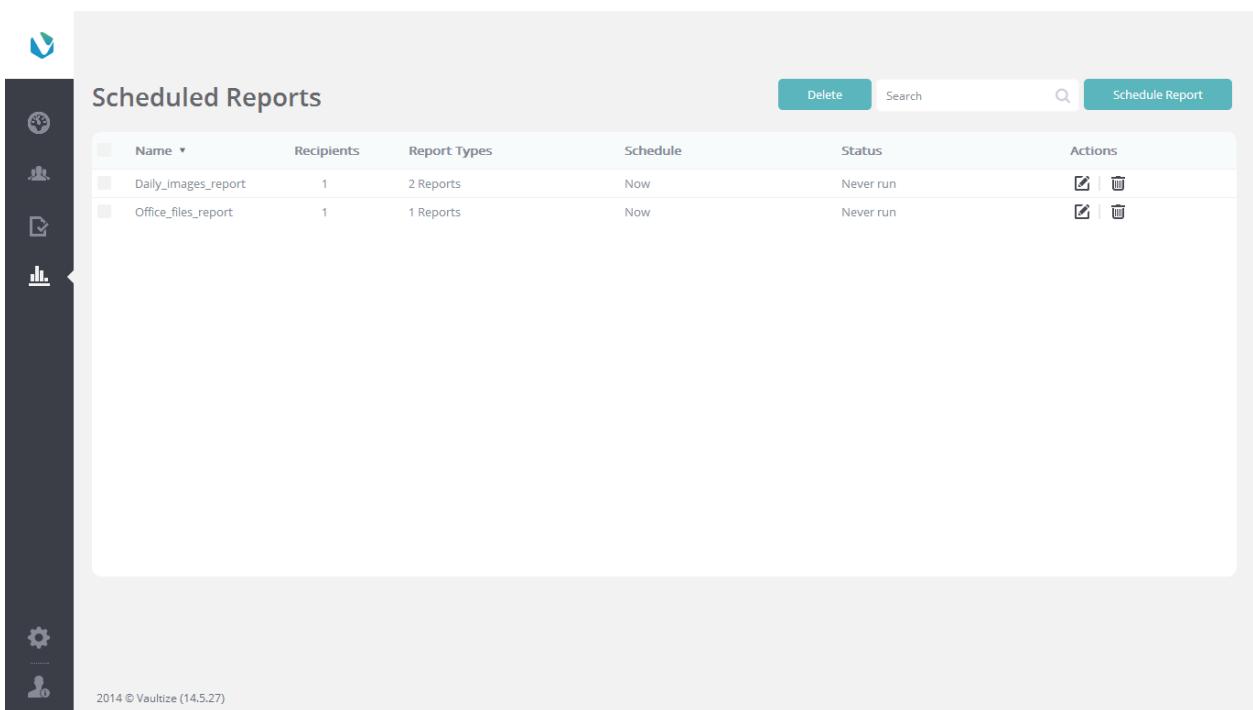
Source	Policy Name	Policy Type	User/Group	Devices	Actions
\$DESKTOP\$	File Server Access Office Docs	Anywhere Access	Sales Team	All	
\$DESKTOP\$\Backup\	Protect Office Files only	Protection	Jane Thomas	VAULT_WIN7-PC	
\$DESKTOP\$\Backup_2\	Protect Office Files only	Protection	Jane Thomas	VAULT_WIN7-PC	
\$DESKTOP\$\Data-User2\	Protect Office Files only	Protection	John Lennon	VMPC-170	
\$DESKTOP\$\Data_Backup\	Protect Office Files only	Protection	Cathy Whatton	VAULT_WIN7-PC	
\$DESKTOP\$\Engineering - Copy - Copy\	Protect Office Files only	Protection	Bob Lara	DELL-PC	
\$DESKTOP\$\Engineering - Copy\	Protect Office Files only	Protection	Bob Lara	DELL-PC	
\$DESKTOP\$\Engineering\	Protect Office Files only	Protection	Bob Lara	DELL-PC	
\$DESKTOP\$\GetData\	Protect Office Files only	Protection	Bob Lara	DELL-PC	
\$DESKTOP\$\HR-Data\	Protect Office Files only	Protection	Bob Lara	DELL-PC	
\$DESKTOP\$\outlook\	protect_empty	Protection	John	VAULTIZE-PC	
\$DESKTOP\$\Protect_Data\	Protect Office Files only	Protection	Cathy Whatton	VAULT_WIN7-PC	
\$DESKTOP\$\Sales-data\	Protect Office Files only	Protection	Bob Lara	DELL-PC	
\$DESKTOP\$\sync_docs\	Protect Any types of files	Protection	Amalore Jude	VZ_MARKETING	

2014 © Vaultize (14.5.5)

9 Reporting

This feature can be used to schedule reports regarding devices, usage, users, backed up files, geo tracking etc., periodically. Hence, this feature helps by keeping users informed on various statistics.

Each scheduled report includes information like name of the report, the recipients, report types, schedule of the report, report status and actions that can be taken on the report.



Name	Recipients	Report Types	Schedule	Status	Actions
Daily_Images_report	1	2 Reports	Now	Never run	<input type="checkbox"/> trash
Office_files_report	1	1 Reports	Now	Never run	<input type="checkbox"/> trash

9.1 Scheduling new report



From the left pane, click the “Reports” button which is indicated by - . The reports list page appears. Here, you can schedule a report by clicking —“Schedule Report” button. You have to specify the following while scheduling a report:

General:

Schedule Reports

X

1/3 General

Name

Recipients i

Example: user@domain.com, admin@domain.com

Report Format

XLS PDF

Cancel Continue

- *Name*- Name of the reporting job
- *Recipients*- Email addresses of users who will receive the report. You need to mention only registered email addresses here. If this field is left blank, the report will be sent to admin.
- *Report Format*- Format of the report required which is either PDF or XLS.

Schedule:

Schedule Reports

X

2/3 Schedule

Schedule

Now ▾

Report Type

All users information

All devices information

Active and Inactive users information

More than days of inactivity would be called as Inactive Users

[Previous](#) [Cancel](#) [Continue](#)

Here, you can mention the frequency with which the report is to be sent. The frequency can be:

- Now
- Certain dates of each month
- Certain days of each week.

Also, report type has to be selected. This indicates the information to be included in the report such as:

- All users information
- All devices information
- Active and Inactive users information

Also, you can mention the number of days of inactivity after which a user is called 'Inactive'.

If you scroll down, there are more report type options such as:

- Backed up files information
- Usage information
- Geo Tracking information.

Schedule Reports

X

2/3 Schedule

Schedule

Now



Report Type

More than days of inactivity would be called as Inactive Users

- Backed up files information
- Usage information
- Geo Tracking information

Previous

Cancel

Continue

Select Groups whose reports to be generated:

Schedule Reports

X

3/3 Select Groups whose reports to be generate

Select Groups

Search to Add

Organization

Management Team

Sales Team

HR Team

Groups selected

Previous

Cancel

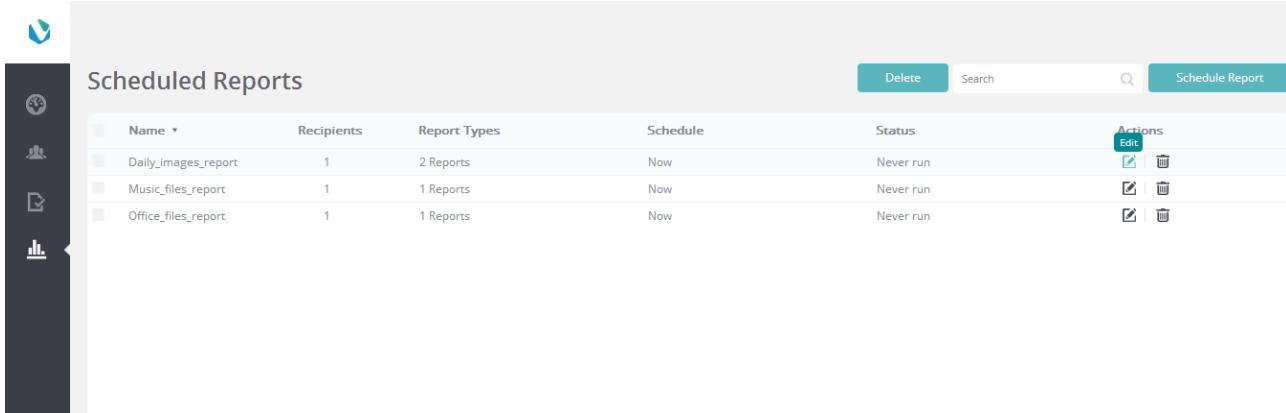
Schedule

Here, you can include Groups to whom the report is to be sent.

Now that the report is created, as per the schedule mentioned, mails will be sent to the intended recipients.

9.2 Editing report

A reporting job can be edited at any point in time by selecting it from the list of scheduled reports and clicking “Edit” button from “Actions” column.

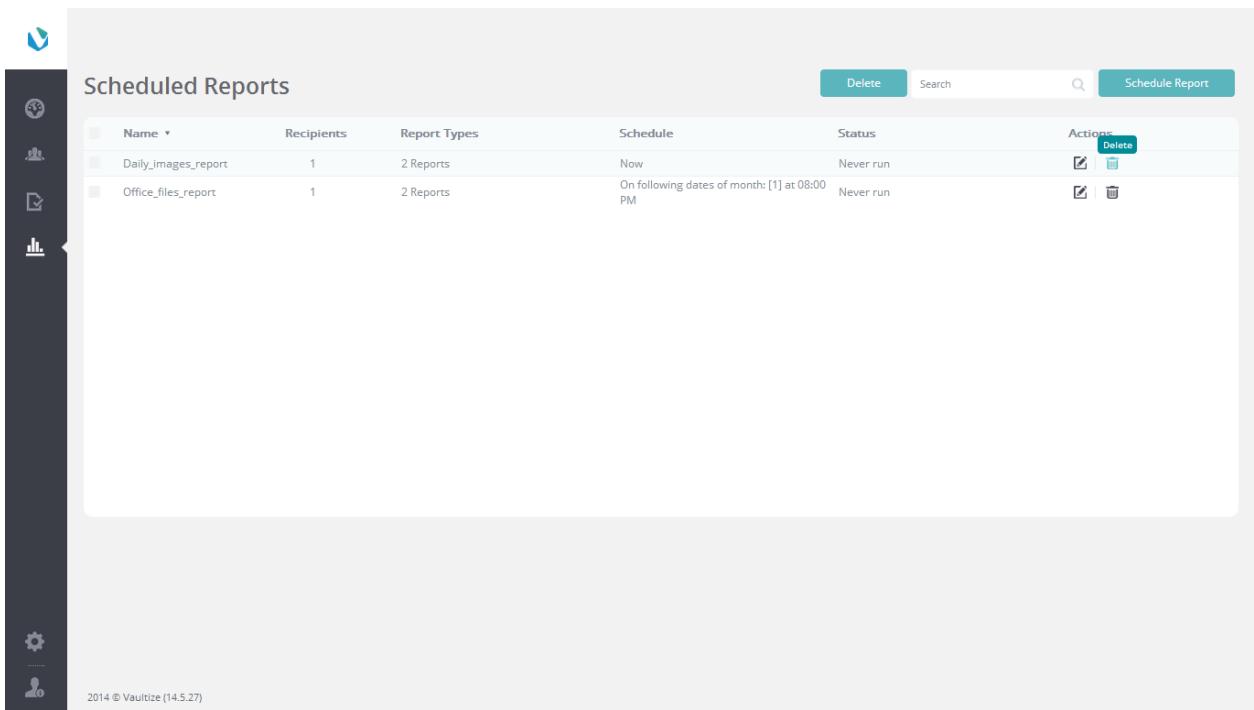


Scheduled Reports					
Name	Recipients	Report Types	Schedule	Status	Actions
Daily_images_report	1	2 Reports	Now	Never run	 
Music_files_report	1	1 Reports	Now	Never run	 
Office_files_report	1	1 Reports	Now	Never run	 

The report details appear in a pop up and can be edited as required. The pages are same as that of report creation but the details would be prefilled. You can change the details as required and save them.

9.3 Deleting report

A reporting job can be deleted at any point in time by selecting it from the list of scheduled reports and clicking “Delete” button from “Actions” column.



The screenshot shows the 'Scheduled Reports' page within the Vaultize Admin Guide. The page has a header with a search bar and a 'Schedule Report' button. On the left, there is a sidebar with various icons: a gear for settings, a person for users, a bar chart for reports, a document for documents, a gear for scheduled reports, and a gear for system status. The main content area is titled 'Scheduled Reports' and contains a table with two rows of data. The table columns are: Name, Recipients, Report Types, Schedule, Status, and Actions. The first row has a 'Name' of 'Daily_images_report', 'Recipients' of 1, 'Report Types' of '2 Reports', 'Schedule' of 'Now', and 'Status' of 'Never run'. The second row has a 'Name' of 'Office_files_report', 'Recipients' of 1, 'Report Types' of '2 Reports', 'Schedule' of 'On following dates of month: [1] at 08:00 PM', and 'Status' of 'Never run'. The 'Actions' column for each row contains a 'Edit' icon and a 'Delete' icon.

Name	Recipients	Report Types	Schedule	Status	Actions
Daily_images_report	1	2 Reports	Now	Never run	 
Office_files_report	1	2 Reports	On following dates of month: [1] at 08:00 PM	Never run	 

10 Installing on a Device

10.1 System Requirements

Vaultize requires:

- **Operating System:** Windows XP Professional SP3 onwards, Windows Server, Mac OS 32-bit (SnowLeopard onwards) and 64-bit (Lion onwards), iOS 4 onwards and Android 2.3 onwards
 - **RAM:** Minimum 512 MB for Windows and Mac
 - **Disk Space:** 40 MB on Windows and Mac
 - **Internet Browser:** Chrome, Mozilla Firefox 8 and above, Safari, Internet Explorer 8 and above
-

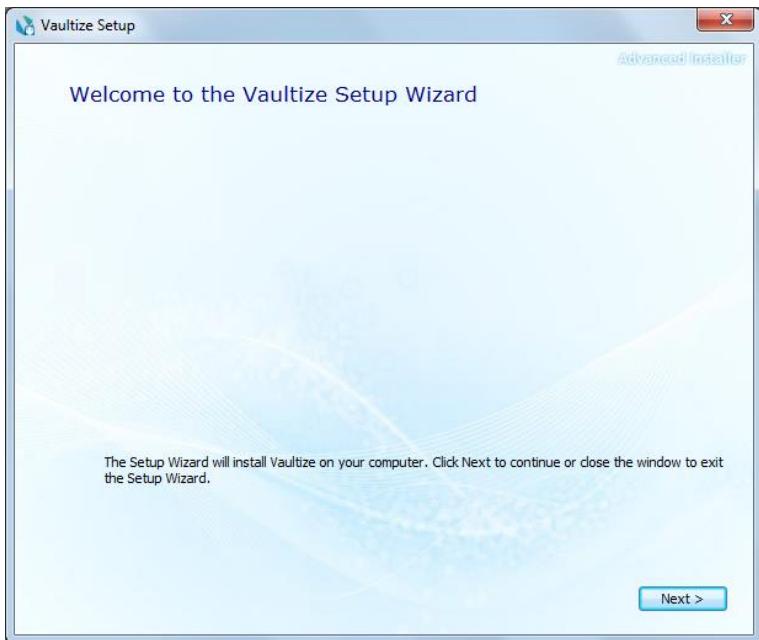
10.2 Installation

If you want to deploy Vaultize in bulk, please refer to our “**Client Installation Guide**” or contact Vaultize customer support. For single user installation, continue reading this section.

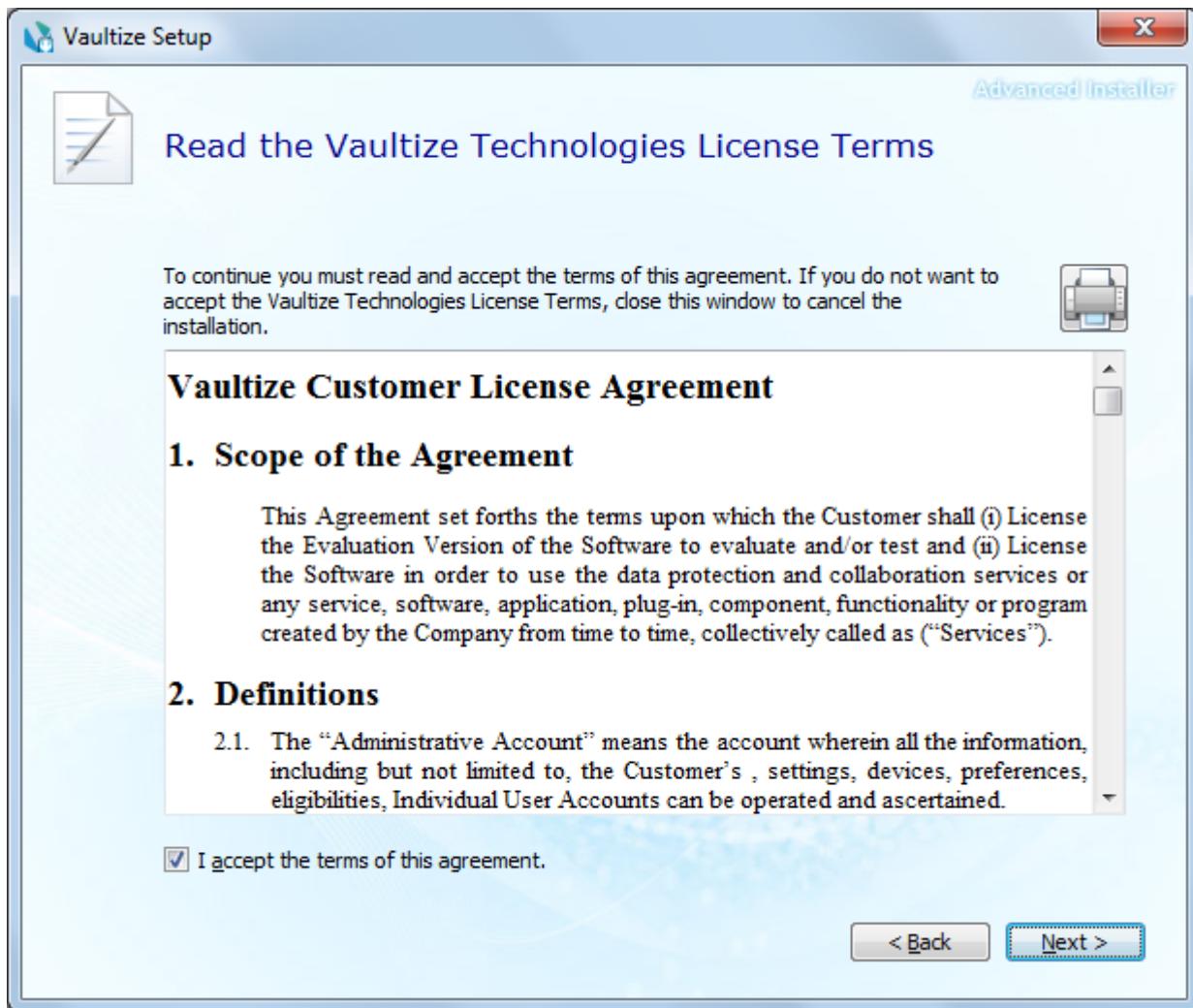
NOTE: If you are using private cloud or appliance server, place “server.url” file in the same location as your Vaultize installer. The file should contain address of your Vaultize API server.

Start the Vaultize installer provided to you by double-clicking on it. Make sure that you run it under administrative privileges. Some operating systems may explicitly prompt you for permission to install the software.

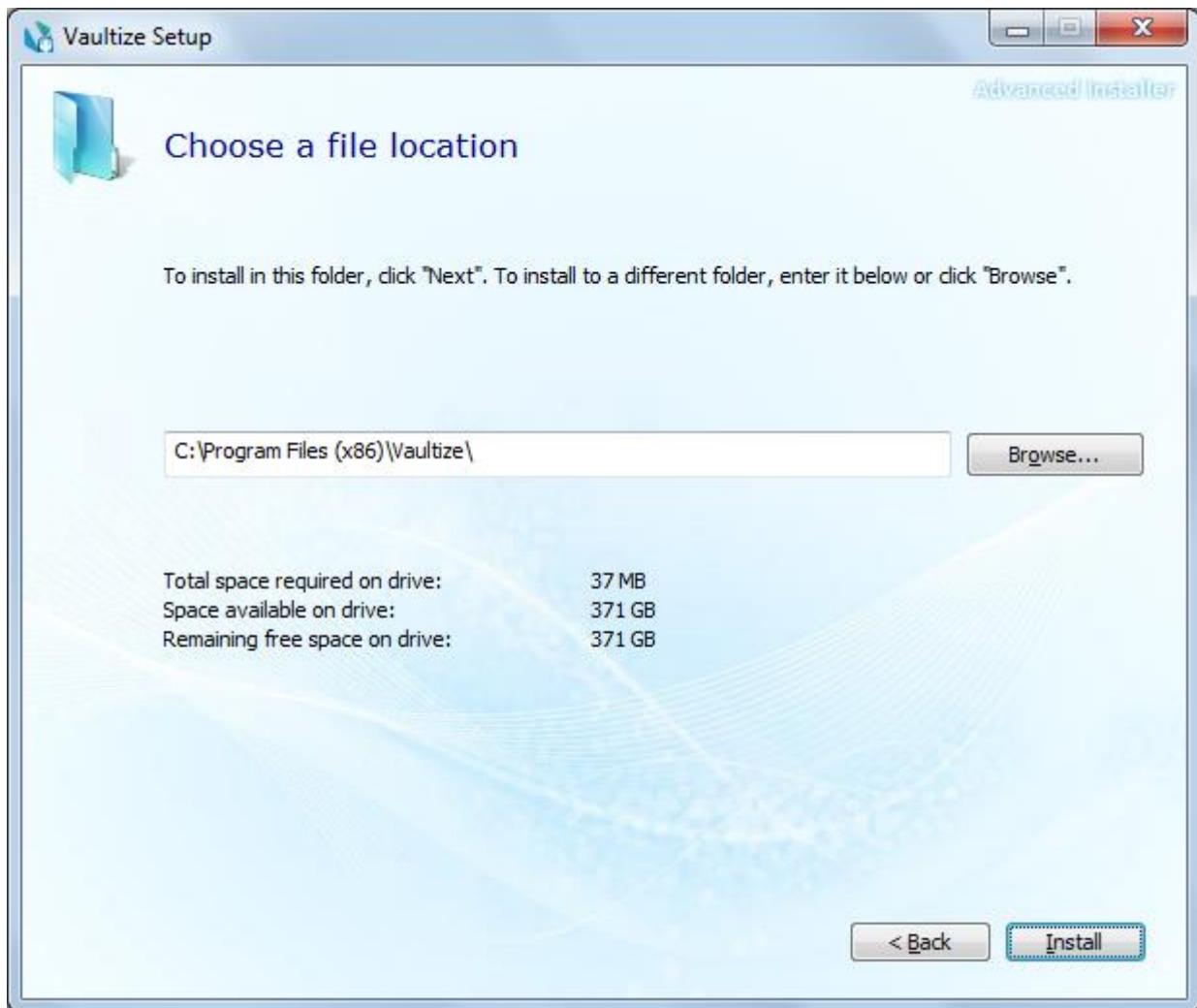
NOTE: In the cases of private cloud and cloud in a box, please include a file named “server.url” in the folder where Vaultize is installed. Please make sure that the content of this file is - <https://myserver.myorg.com:8443> where **myserver.myorg.com** is to be replaced by IP/FQDN of Vaultize server. If server.url file exists and server cannot be connected, proxy page is shown. If server.url is missing, the client tries to connect to Vaultize public cloud.



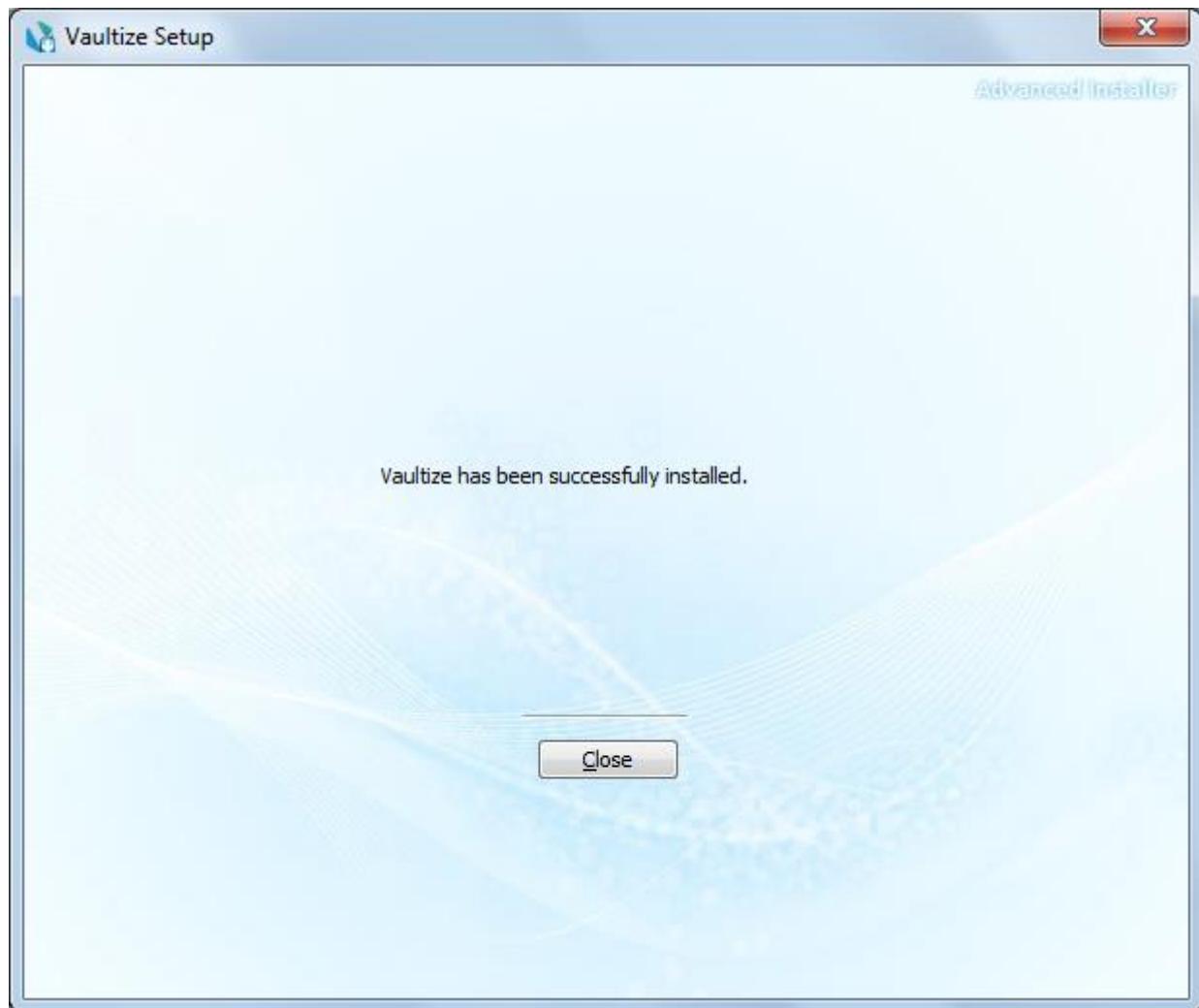
It is recommended that you close all applications before clicking —"Next". This will ensure that Vaultize is installed cleanly. After you click —"Next", the installer will show you the —"Customer License Agreement". You are required to read each and every term carefully before accepting them. If you don't agree to any of the terms, don't install the software. You can stop the installation of software by closing the window. If you accept the terms, select —"I accept the terms of this agreement" and proceed with the installation by clicking "Next"



You will have to provide the install location – default being C:\Program Files (x86)\Vaultize. Vaultize requires 40MB of space.

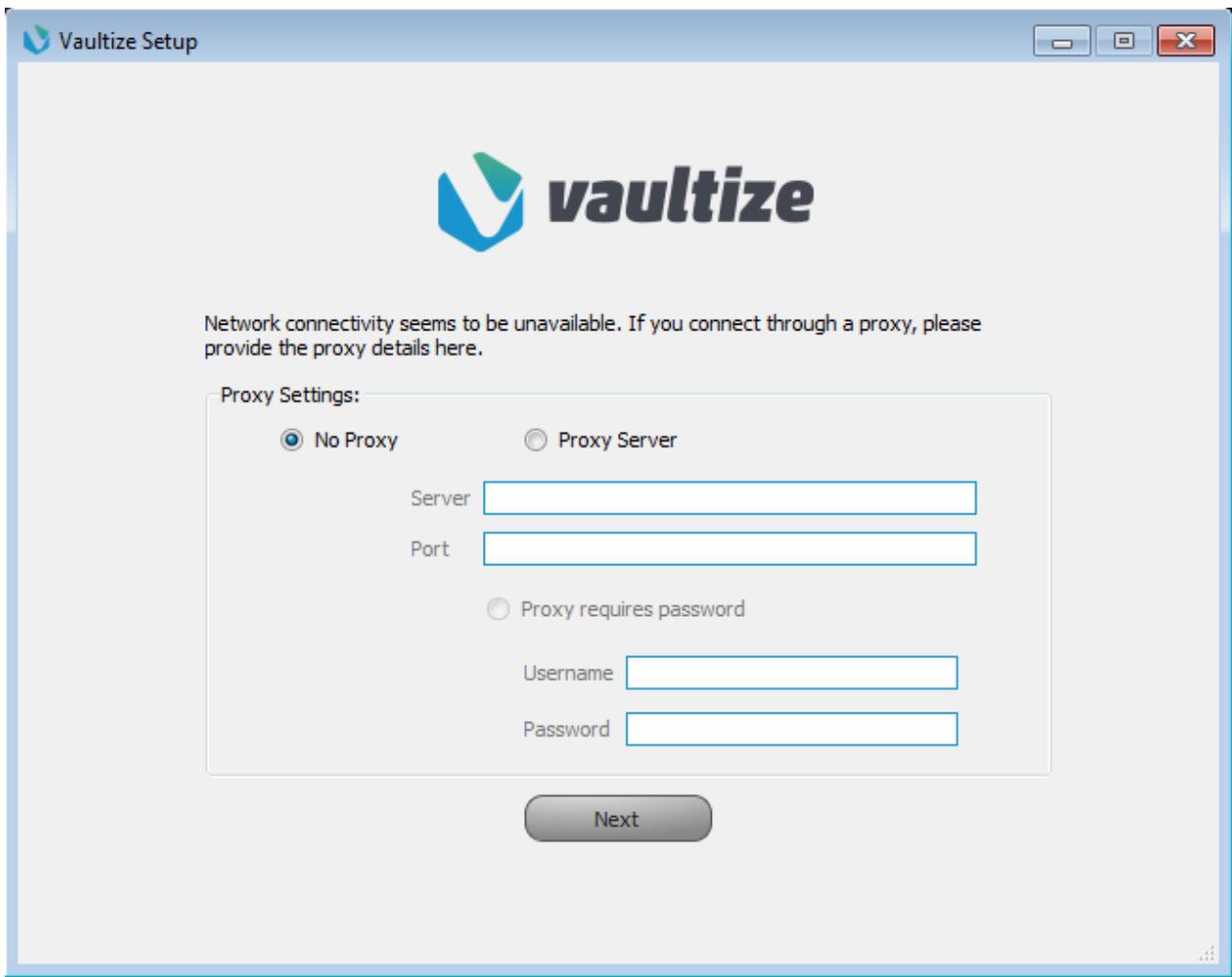


Once the installation is done, the following screen appears.



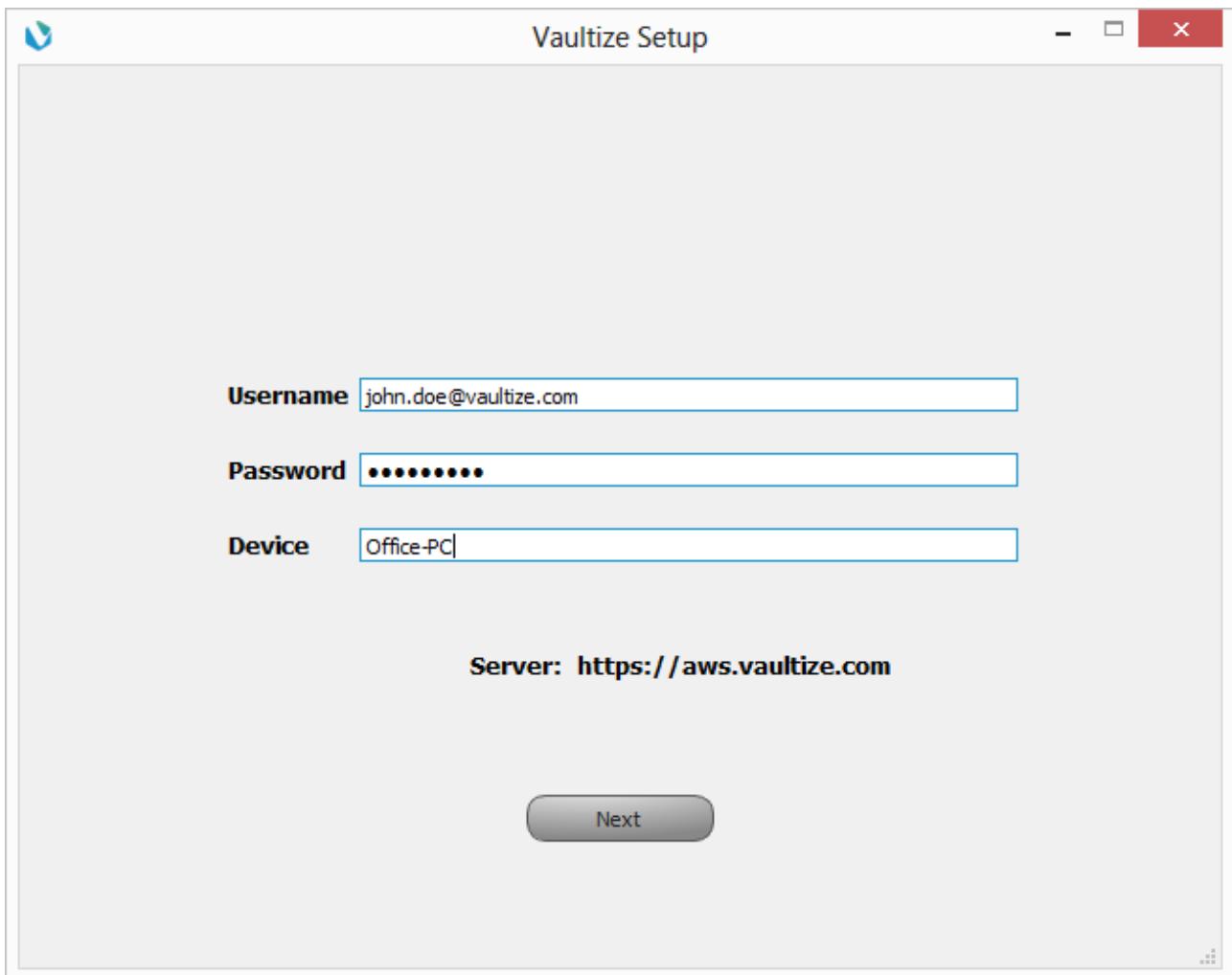
If you are doing bulk install, Vaultize customer support would have given you the key files for your individual users. You need to upload a key file for the user. You can locate the key file through —"Browse". After selecting the correct key file just press —"Install". You will get install completion message. Just press —"Finish" and Vaultize will start running. You can see the Vaultize icon in the system tray. You can invoke the Vaultize GUI by double-clicking the icon. If you are not doing bulk install, continue the installation by pressing —"Install". You will get install completion message. Just press —"Finish".

After installation is done, you get the below screen. If there is a proxy, please enter it here in order to communicate with the server and click "Next".

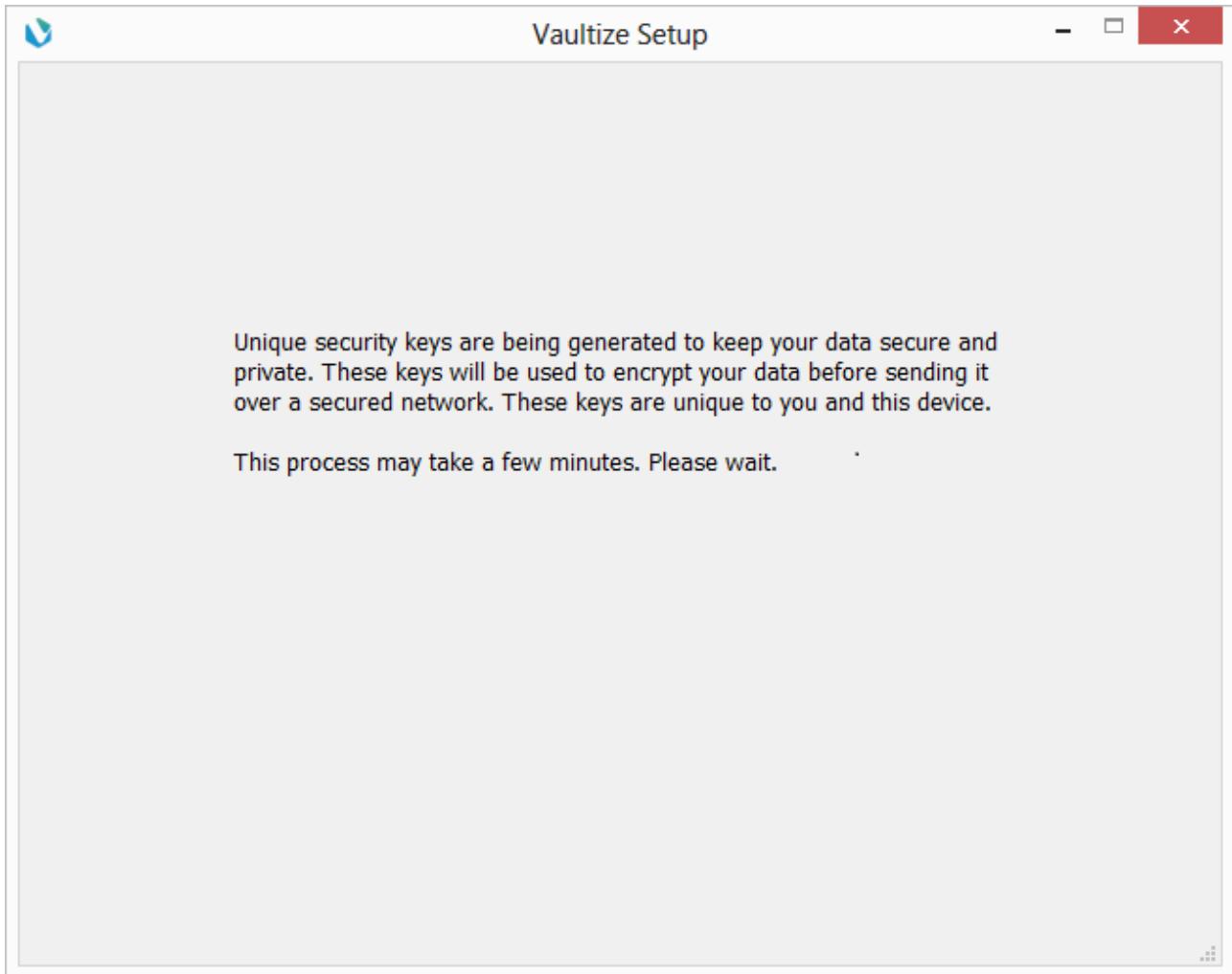


Upon clicking "Next" the below screen appears.

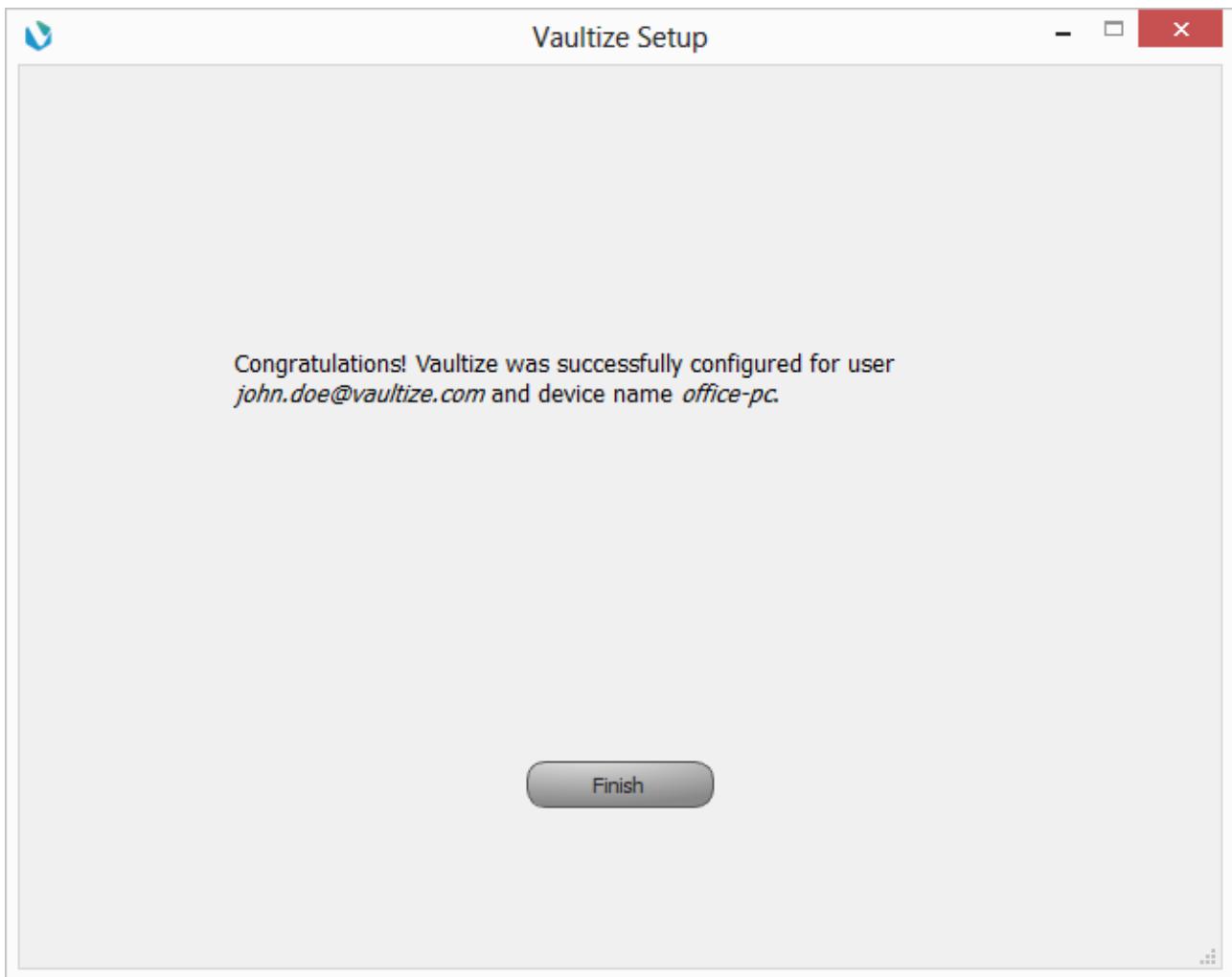
Also, if there is no proxy, the below screen is shown. Here, enter the login credentials to access the Vaultize client.



Once "Next" is clicked, the below screen appears. Unique security keys are generated during this time. These keys keep the user's data safe and are used during encryption of data.

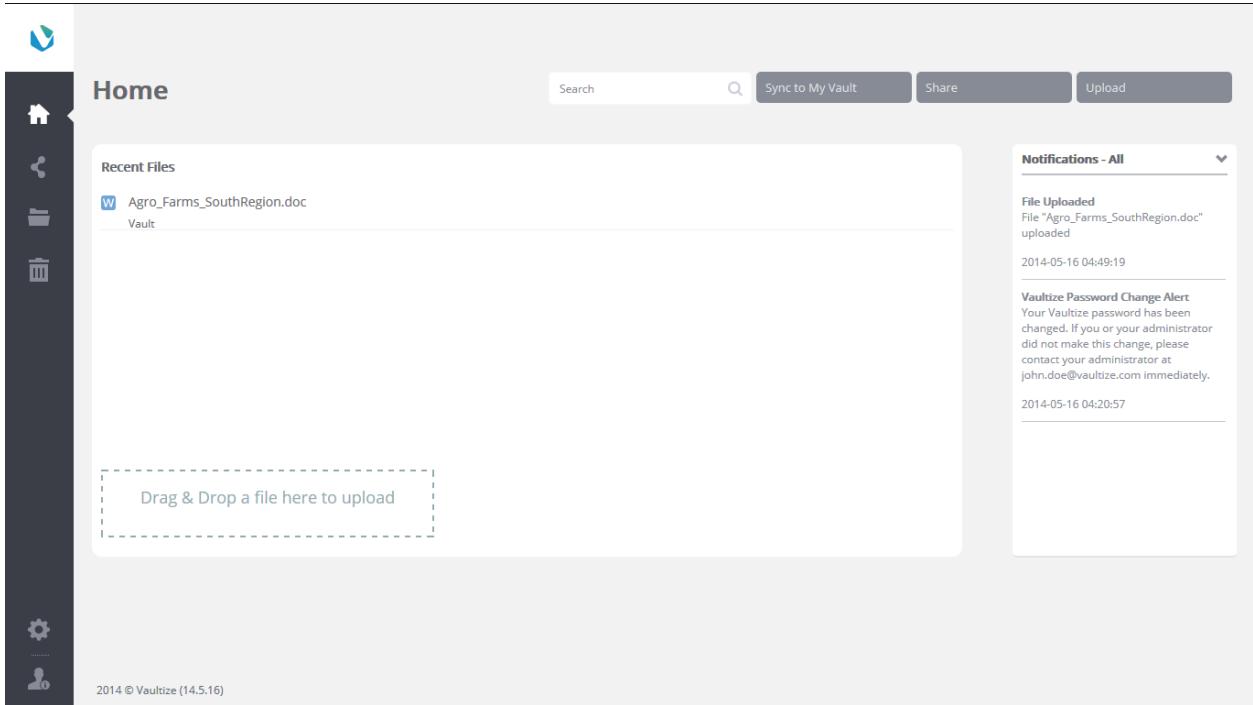


Once keys are generated, the final screen appears wherein it notifies that Vaultize was successfully configured on the system.

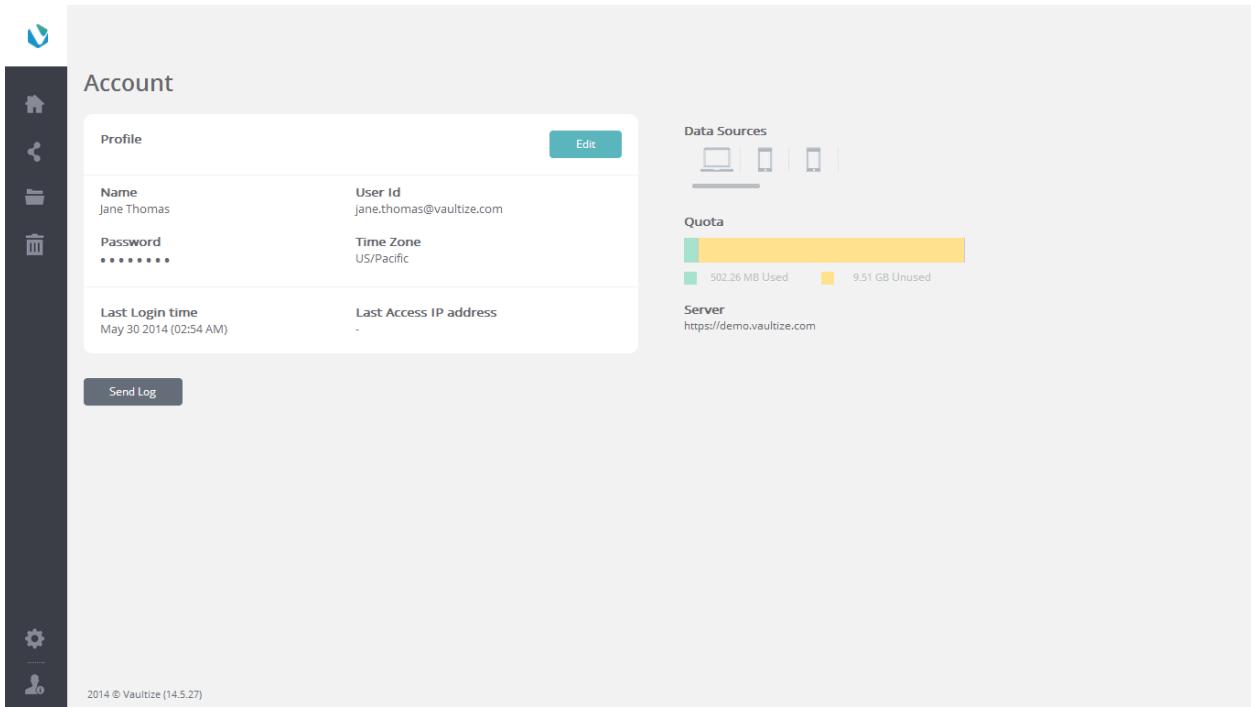


Now that Vaultize is successfully configured for the specified user name and device correspondingly, you can access Vaultize from system tray by just right-clicking it and selecting "My Vault".

The GUI of Vaultize client typically appears as below:-



Please note the button “Send Log” on the “Account” page. If a user has any issues with the client, he/she can hit this button to send the logs to the admin for debugging.



10.3 Client UI

When a user logs into the Vaultize client through his device, he/she can see some tabs on the left pane of the screen. These include:

- **Recent Data**- This includes the recent data that was protected by or shared to the user. Each of these files has an option to be viewed/shared/downloaded via the buttons across each file depending on the permissions. Each file record includes filename, updated time, user who updated it and path of the file.
You can select the desired files and click the Sync button. This will keep the contents at user device up to date.
Upload button helps in one-time upload of data to Vaultize.

The screenshot shows the Vaultize Home interface. On the left is a vertical sidebar with icons for Home, Recent, Shared, Sync, and Help. The main area is titled 'Home' and contains a 'Recent Files' section with a list of documents: 'Unsolicited_Proposal.docx', 'Web_Metrics_Report.pdf', 'Value_Proposition_SMB.ppt', 'Sales_Performance_Q4_South.ppt', 'Insurance_Calculator.xls', and 'Rental_Agreement.docx'. Below this is a dashed box for file uploads with the text 'Drag & Drop a file here to upload'. On the right, there is a 'Notifications - All' section with a 'Vaultize Error' message about quota exceeded, a 'File Uploaded' message for a .doc file, and a 'Vaultize Password Change Alert' message. The bottom left of the main area shows the text '2014 © Vaultize (14.5.16)'.

- **Shared Data-** This includes the data that was shared to/shared by the user. Each of these files/folders has an option to be viewed/synced/unsynced/rejected/edited using the buttons across each file.

View button helps in viewing the files/folders.

Sync/Unsync helps in syncing or unsyncing the files/folders. Sync is done to keep the local copy of data up to date. Whenever the user no longer needs to keep the copy updated, unsync can be used.

Reject button helps in rejecting a data share sent by someone to current user.

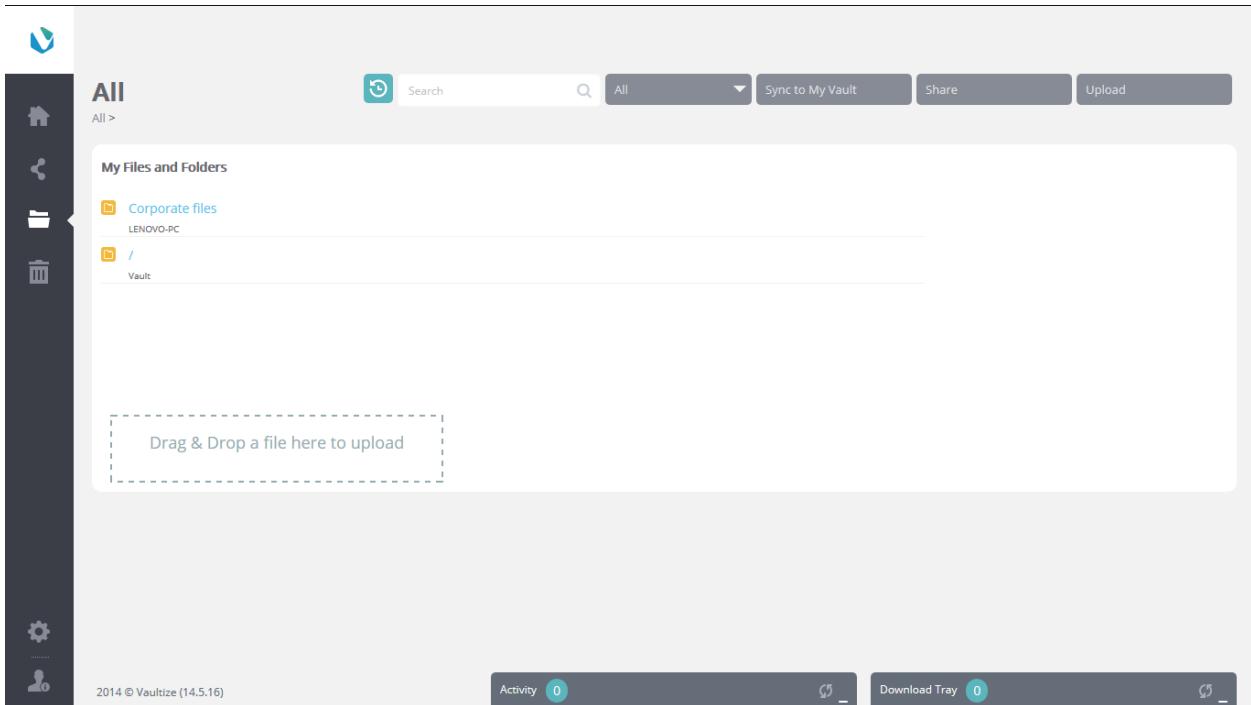
Edit Share helps in editing a data share that is done to one/more users by current user.

You can select the desired files and click the Share button. This will open a pop up where in you can share the file to desired recipients. For further details please refer to section 4.2.

Upload button helps in uploading data for protection. You can upload content to a file/folder if you have the permissions to do so.

The screenshot shows the 'Shared Data' section of the Vaultize interface. On the left is a sidebar with icons for Home, Shared, Folders, Recycle Bin, Settings, and Help. The main area has a header with 'Shared Data', a search bar, and buttons for 'Sync to My Vault', 'Share', and 'Upload'. The left panel is titled 'Shared by me' and lists 'Corporate_Profile_Executive.ppt' (PowerPoint) and 'Web_Metrics_Report.pdf' (PDF). The right panel is titled 'Shared with me' and is currently empty. At the bottom left is the text '2014 © Vaultize (14.5.16)'.

- **All Data**- This includes all the data that is present in a user's vault. Each of these files/folders can be synced. Also, upload of files/folders can be done based on due permissions. There is an option to drag-drop files/folders to be uploaded.



NOTE: When a device is lost or disk crashes, click on “All devices” button in “All Data” tab, select the lost/broken device and download entire or partial data as needed into the current device. This is an easy and effective way to recover from any data loss.

- **Trash**- This includes all the data that has been deleted by the user.

Once a data sharing policy is applied, a user can share data by clicking the “Share” button across the file/folder.

The below pop up appears wherein the following details are given:

- users/email addresses/group names to whom the data is shared
- permissions for each user can be given as edit/view/admin if the user is a Vaultize user. The permissions for a non-Vaultize user can be view/download. He/she also gets an upload option if the shared data is a folder.
- share link can be made view only wherein the user cannot download the data and can just view it on his browser. This option is also called “**Web View**”
- password restriction can be enforced
- expiry date for the link can be provided. This value overrides the one given during policy creation. However, this value should not exceed the one given during policy creation.

Sharing "Corporate_Profile_Executive.ppt"

X

Add users/mail addresses

<input type="text"/>	Select Permissions	Add ↓
----------------------	--------------------	-------

For outside organization contacts enter email id

Shared to	Permissions	Link
Bob Lara	View Edit Admin	- 
bob.jude@gmail.com	View Download	- 

Link for sharing



<https://61.12.99.226:1443/share>

/k-1-cEA1DPQSVZ3vBw7B18xbwoEq1Asm

[View](#) [Download](#)

This link could be shared outside the organization following the sharing policies.

Password

Expiry

06/30/2014



[Unshare](#)

[Cancel](#)

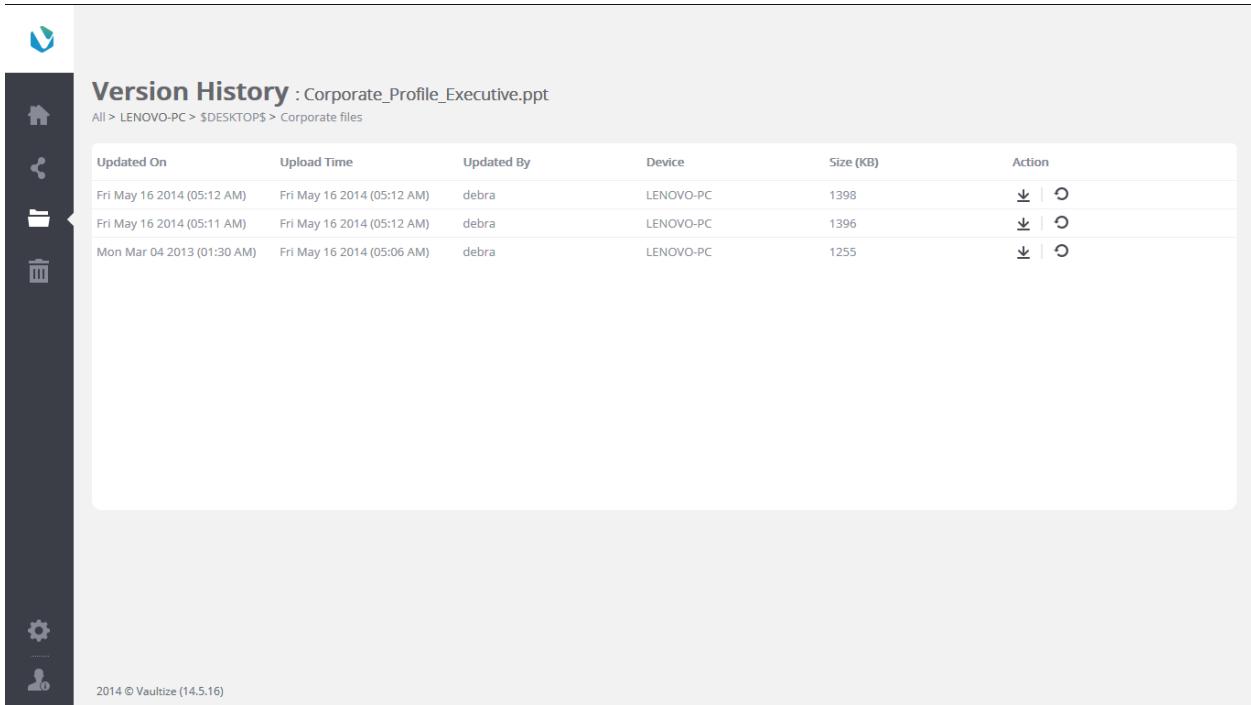
[Done](#)

10.4 Version History

When you access any file and click on it, you see all the versions of the file as shown below. This is called the version history. It comes handy when, for example, we need to check the difference between current and a previous version. Depending on settings and mode of data protection, there can be only the latest version available on Vaultize.

Each record of file version includes the version number, updated date and time, user who

updated it, device from which it was updated and size of the file.



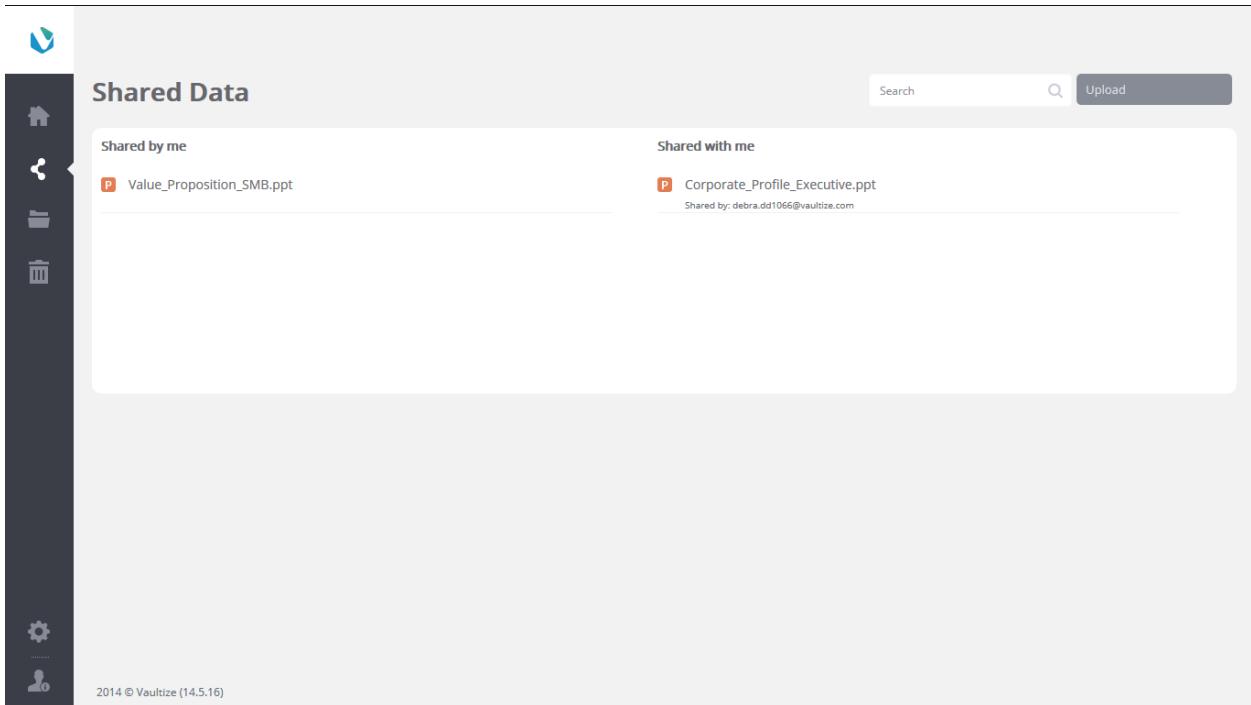
Updated On	Upload Time	Updated By	Device	Size (KB)	Action
Fri May 16 2014 (05:12 AM)	Fri May 16 2014 (05:12 AM)	debra	LENOVO-PC	1398	
Fri May 16 2014 (05:11 AM)	Fri May 16 2014 (05:12 AM)	debra	LENOVO-PC	1396	
Mon Mar 04 2013 (01:30 AM)	Fri May 16 2014 (05:06 AM)	debra	LENOVO-PC	1255	

2014 © Vaultize (14.5.16)

10.5 Data Sync

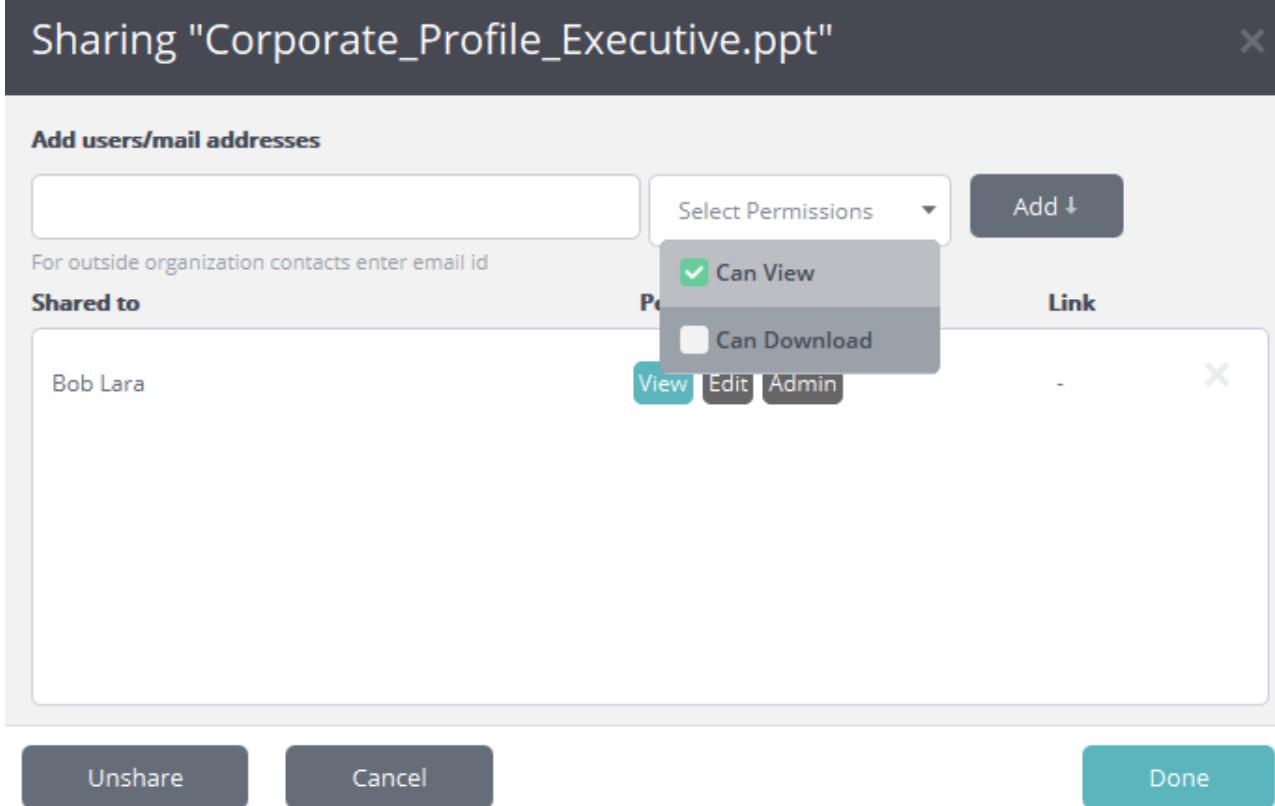
Data Sync feature can be used in order to keep a local copy of a file in sync with Vaultize server. When a file is shared to a user and he/she wants to keep the file synced, "Sync" button across the corresponding data instance has to be selected. The user can, at any point in time, decide not to sync the data anymore. Then, he/she can simply click the "Unsync" button to stop syncing the data.

Also, when data is uploaded using one device of a user, it can be synced onto other devices of the same user.



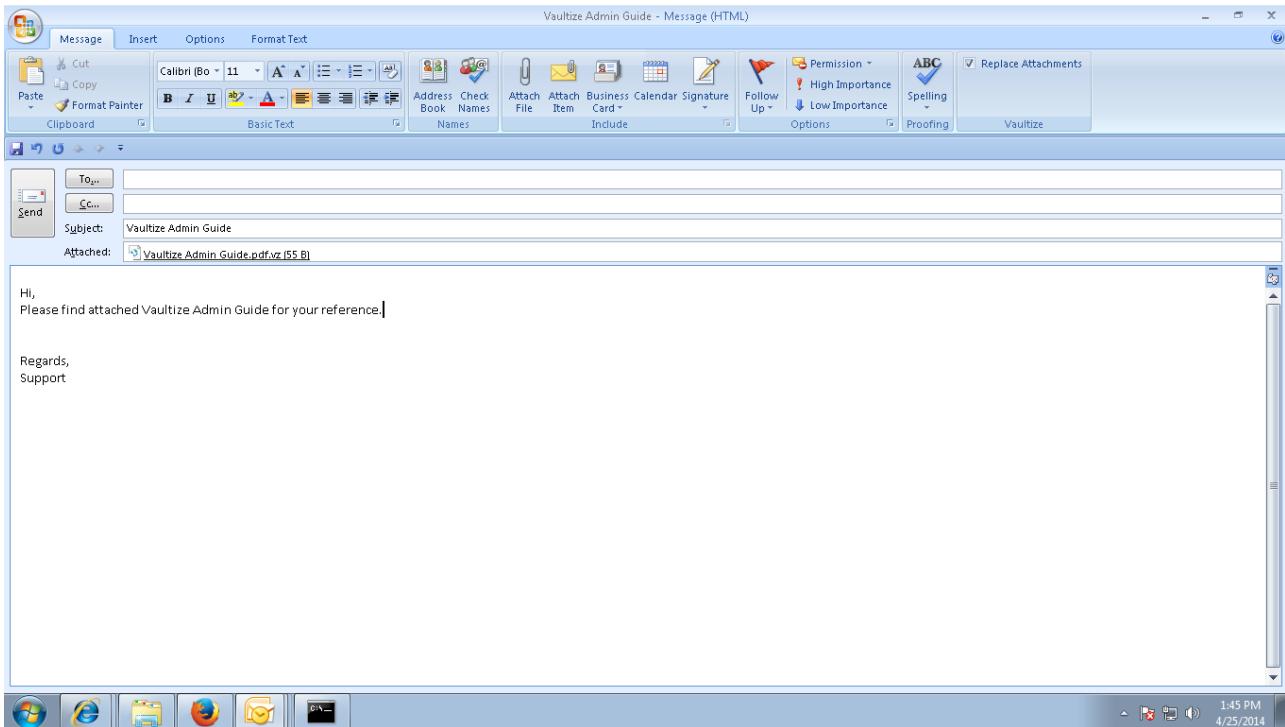
10.6 Online Document Viewer

When data is being shared, it can be made view-only to the recipients. This can be achieved by selecting “Can View” checkbox while creating a share. When this option is selected and data is being shared within the organization, download and reject options appear across the file. When the data is shared outside the organization, a link is sent. When this button/link is clicked, a new tab is opened and the file is displayed in the browser itself. The primary advantage of this feature is that you can share files with people inside/outside of your organization and allow them to only view the files and not download/print them. This is an important stride towards ensuring further security of your data.

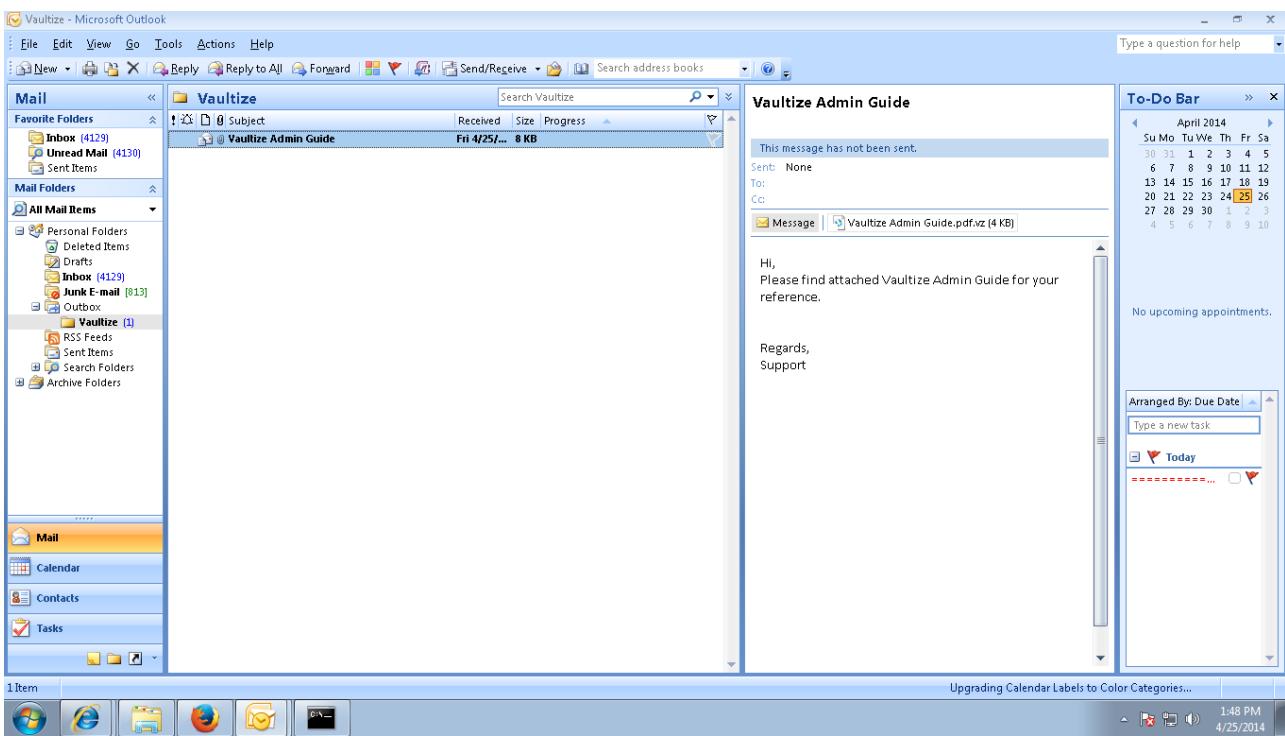


10.7 Outlook Plugin

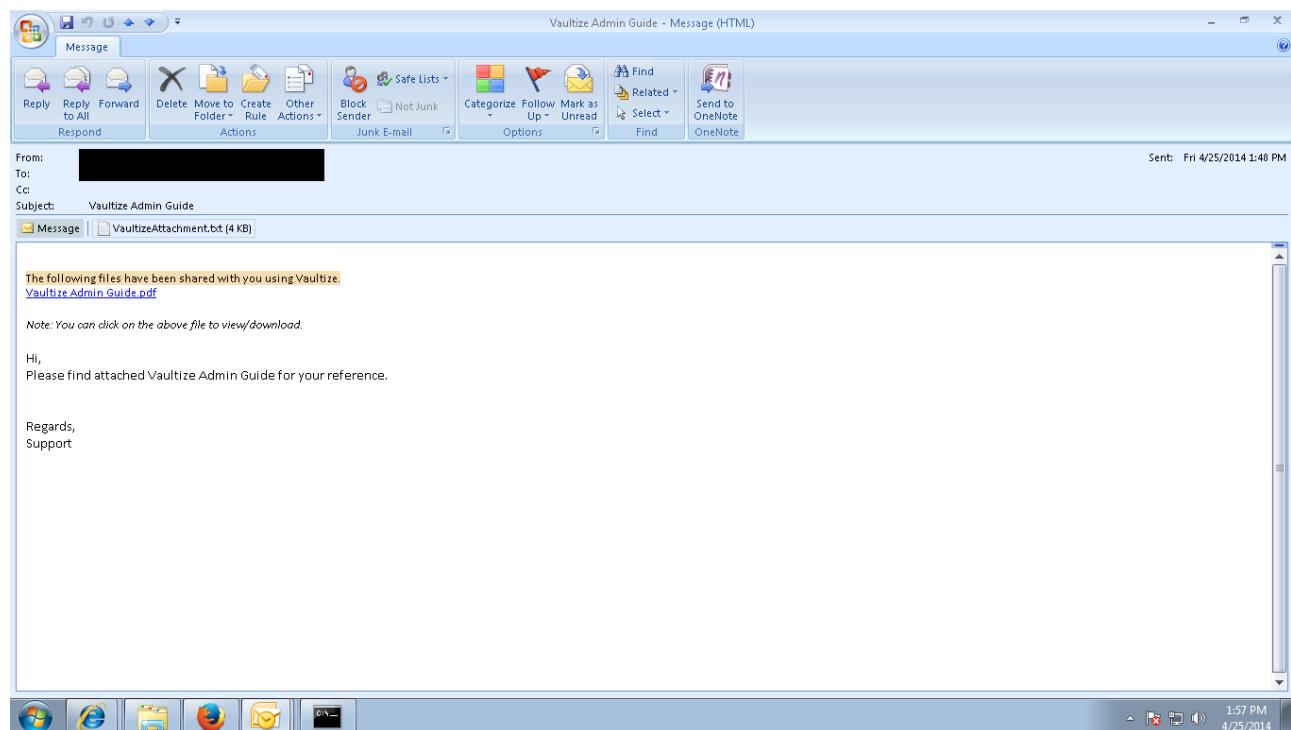
Vaultize Outlook plugin replaces Outlook attachments with Vaultize share links. These links will help in reducing the Exchange and PST storage. This will also help in tracking the data when shared outside the organization. Also large files can be attached easily. Below screenshot shows a large email being attached.



The mail is now sent to "Vaultize" folder under Outbox folder of Outlook.



The email is sent to the recipients and the attachment now appears as a Vaultize link in the body of the email as shown below:



To replace email attachments with links, you first need to create a data protection policy.

During the policy application, please make sure that the "*Target Location*" is "*Outlook Attachments*". Refer to below screen:

Apply Policy

X

4 /4 Define Target Location

Target Type

Desktop/Laptop ▾

Select target location

Desktop My Documents

Outlook folder User Profile/Home

Outlook Attachments

\$OUTLOOK_ATTACHMENT\$ i

Previous Cancel Continue

Once this is chosen, click “*Continue*” to configure other options shown below:

Apply Policy

X

5 /5 Define outlook attachment settings

Replace Attachments :

Bigger than

 kb i

Smaller than

 kb i

Replace attachments only if all recipients belongs to following domain/s:

 comma seperated domain's i

- Skip replacing attachment if vaultize is not running
- Allow user to skip replacing attachments
- Show vaultize message to user

Previous

Cancel

Apply

- *bigger than* - if an outlook attachment is bigger than the size mentioned here, it will be replaced by a link
- *smaller than* - if an outlook attachment is smaller than the size mentioned here, it will be replaced by a link
- *replace attachments only if all recipients belong to following domain/s*- you can specify domains here. If an email recipient belongs to any of the domains mentioned here, only then the attachments would be replaced by links.
- *Skip replacing attachment if vaultize is not running*- if this option is checked, Outlook attachments would be replaced by links only if Vaultize is running on the user's system.
- *Allow user to skip replacing attachments* - if this option is checked, user can either enable or disable the feature replacing attachments with links. User can either enable or disable this feature by checking or unchecking a checkbox in Outlook that reads "Replace Attachments". You can find this checkbox on the top right-hand corner of a new message window in Outlook.
- *Show vaultize message to user* - if this checkbox is enable, Vaultize related messages would be shown to user.

Annexure A

- I. How to protect Office data in your entire system?
 - Create a protection policy with 'Office files' as the filter and schedule as 'Continuous'.
 - Apply the policy on non-system drives (while applying the policy, mention paths in 'Define Target Location' screen).
 - Clone the above protection policy to create a new policy.
 - Schedule the cloned policy for few hours in a day (say 3 hours).
 - Also, include Program Files, Windows system folder in the 'Exclude Files/Folders' list while defining Files/Folders filter .
- II. How to protect Office data in user-defined folders?
 - Create a protection policy with 'Office files' as the filter.
 - Leave the target blank while applying the policy. This will allow users to specify their folders as required.
- III. How to allow users to protect data from a specific drive say D?
 - While protection policy is created, in "*Restrict Sources of Data*" page, mention the required drive. For example, if you want to mention D drive, enter D:/*.
 - Leave the target blank while applying the policy. This will allow users to specify their own folders in the mentioned drive.

Annexure B

This appendix indicates a table where various macros are listed. File extensions included under each of these macros are also shown. These macros are listed in Files/Folders Filter page of various policies.

Macro	File Extensions
Outlook files	"pst", "ost", "pbx", "dbx"
Email files	"pst", "msg", "eml", "emlx", "mbox", "mbx", "mbs", "pbx", "dbx", "nsf"
Office files	"accda", "accdb", "accdc", "accde", "accdp", "accdr", "accdt", "accdu", "acl", "ade", "adp", "cnv", "doc", "docm", "docx", "dot", "dotm", "dotx", "grv", "laccdb", "maf", "mam", "maq", "mar", "mat", "mda", "mdb", "mde", "mdt", "mdw", "mpd", "mpp", "mpt", "one", "onepkg", "ops", "pa", "pip", "pot", "potm", "potx", "ppa", "ppam", "pps", "ppsm", "ppsx", "ppt", "pptm", "pptx", "pub", "puz", "rpmsg", "sldm", "sldx", "snp", "svd", "thmx", "vdx", "vsd", "vss", "vst", "vsx", "vtx", "w1", "xl", "xla", "xlam", "xlb", "xlc", "xll", "xlm", "xls", "xlsb", "xism", "xlsx", "xlt", "xltm", "xltx", "xlw", "xsf", "xsn", "psw", "uot", "hwp", "odm", "sxn", "sxc", "sdc", "123", "wb2", "uof", "dbf", "odf", "sxn", "mnl", "vor", "dotx", "ots", "vor", "xltm", "xltx", "xlm", "sti", "vor", "met", "emf", "sxi", "sxd", "uof", "pct", "sgf", "sgv", "odt", "sxn", "sdw", "pdb", "uof", "wpd", "stw", "oth", "sgl", "ods", "dif", "xlc", "wk1", "wks", "pxl", "uos", "odb", "smf", "ott", "stw", "dotm", "stc", "xlw", "otp", "pot", "potm", "potx", "svm", "odp", "sda", "sdd", "sdd", "uop", "odg", "rtf", "pdf", "fdf", "xfdf", "ps"
Binary files	"paf", "u3p", "fpbf", "vlx", "mpx", "jsx", "reg", "xrm-ms", "its", "gmmp", "mio", "pat", "otm", "diagpkg", "xys", "jse", "pif", "clb", "pid", "prefpane", "hsh", "nb0", "key", "cof", "aos", "ls", "qpx", "cgz", "dat", "chg", "com", "icl", "icm", "panic", "es", "evtx", "mum", "cnt", "cgi", "ppm", "vexe", "mydocs", "mam", "lo", "prf",

	<p>"pwc", "thm", "admx", "fky", "tha", "out", "ds", "grl", "deskthemepack", "iim", "lpd", "grp", "paf", "exe", "air", "jpn", "qvm", "386", "vbe", "wpm", "pol", "frs", "wer", "mbr", "dyc", "z19", "blf", "msstyles", "upx", "ipod", "ko", "vga", "diagcab", "kor", "vgd", "ahk", "cht", "bk2", "chs", "vdo", "pck", "etl", "dlx", "m3g", "rco", "8xu", "dld", "desklink", "nt", "drv", "ebs2", "dll", "elf", "sca", "fid", "ws", "vbs", "actm", "mdmp", "rc1", "cpr", "cab", "prc", "bash_history", "cpl", "prg", "workflow", "cpi", "sbn", "script", "jar", "msc", "ffl", "pyo", "ksh", "htt", "searchconnector-ms", "ion", "pyc", "sbs", "swp", "hta", "rbx", "ipf", "ipa", "sqm", "scpt", "hms", "mapimail", "fxp", "widget", "xap", "fas", "ms", "scf", "bk1", "savedsearch", "str", "efi", "kbd", "regtrans-ms", "mxe", "wgz", "rmt", "bio", "cyw", "cur", "vb", "edj", "log2", "xlm", "nls", "fpi", "ani", "ann", "evt", "plsc", "seed", "spl", "pdr", "pk2", "hhc", "schemas", "scr", "asec", "rpj", "hhk", "sct", "wsf", "pex", "ac", "kix", "msp", "scb", "rxe", "xbap", "spr", "help", "kext", "wsh", "diagcfg", "wdf", "udf", "dss", "tms", "dek", "arscript", "ppd", "webpnp", "ps1", "ps2", "ffo", "ffa", "mobileconfig", "bat", "bin", "ecf", "dev", "ezs", "ezt", "phar", "hlp", "wpk", "xqt", "0", "shb", "group", "dmp", "acr", "0xe", "esh", "mui", "wiz", "vpm", "hdmp", "so", "0", "dmc", "celx", "plx", "cat", "qit", "sfccache", "nfo", "metadata_never_index", "vx_", "sys", "asb", "scar", "adm", "rfw", "gs", "csh", "mem", "crash", "icns", "tcp", "a6p", "mel", "exopc", "theme", "lnk", "pvd", "smm", "rox", "sdb", "mrc", "itemdata-ms", "shd", "ex_", "cdmp", "rc2", "ci", "rgs", "ins", "isu", "bmk", "bashrc", "applescript", "shsh", "lst", "ffx", "bom", "dxl", "action", "apk", "pnf", "command", "mcr", "wpx", "run", "printerexport", "manifest", "gadget", "exe", "osx", "ruf", "js", "app", "cel", "profile", "log1", "ftg", "mi4", "hjp", "job", "pwl", "wcm", "hpf", "wph", "sbf", "pfx", "hiv", "dvd", "spd", "ico", "ham", "fts", "dit", "mlc", "saver", "icd", "vbscript", "cmd", "ebs", "vxd", "ex4",</p>
--	--

	"000", "emerald", "prt", "adml", "wdgt", "gpu", "idx", "library-ms", "msstyle", "ebm", "bash_profile", "gpe", "so", "vol", "msi", "msm", "msp", "mst", "idt", "cub", "pcp", "partial", "crdownload", "part", "download", "pyd", "sfcache"
Audio/music files	"sou", "w64", "npl", "afc", "mid", "band", "nks", "ub", "nkx", "sds", "aob", "nkb", "sdt", "sdx", "nkm", "uw", "nki", "tfmx", "cdr", "bun", "sdii", "xwb", "adg", "sd2", "frg", "cda", "uax", "svx", "r1m", "lvp", "ds2", "svd", "mgv", "jam", "f2r", "wfp", "dts", "dtm", "prg", "wfd", "adt", "wfb", "vrf", "dsm", "peak", "dsf", "dsp", "dss", "wow", "wave", "at3", "tak", "sd2f", "kpl", "tta", "d01", "d00", "txw", "m1a", "ssnd", "acd-zip", "ym", "far", "wpk", "tsp", "sc2", "rx2", "mus", "sppack", "ase", "asd", "pkf", "copy", "jo-7z", "sfap0", "gm", "wyz", "aa3", "pvc", "wus", "xfs", "toc", "rol", "bdd", "cfxr", "miniusf", "rvx", "box", "df2", "mlp", "aax", "aac", "w01", "ntn", "vyf", "ra", "dfc", "sprg", "f64", "amxd", "pac", "mtm", "vdj", "pat", "wwu", "atrac", "ncw", "ktp", "u", "fsm", "vmf", "vgz", "phy", "vox", "ds", "fzb", "voc", "pho", "dm", "sseq", "kt2", "kt3", "fzv", "awb", "mzp", "emx", "sid", "orc", "koz", "dls", "sib", "esps", "8svx", "m4r", "mmp", "cpt", "cpr", "odm", "vgm", "m4a", "m4b", "uni", "zpl", "snd", "sng", "m4p", "mo3", "pcast", "vb", "pek", "au", "mti", "mte", "mtf", "ay", "669", "ab", "aa", "al", "ntp", "mts", "pla", "wrk", "f32", "kar", "pls", "kfn", "mscz", "mscx", "mt9", "musa", "lwv", "mt2", "usflib", "ove", "f3r", "psy", "wav", "psm", "rcy", "psf", "h0", "gbs", "nrt", "smf", "mka", "okt", "8cm", "nra", "sbg", "sd", "sf", "sbi", "gp5", "midi", "ais", "sw", "ksc", "ksf", "wtpt", "ics", "wtpl", "cmf", "bwf", "gpx", "gpbank", "vap", "val", "gpk", "vag", "fls", "flp", "mpu", "dct", "stx", "sty", "mpa", "mpc", "rex", "stm", "ulw", "sbk", "gbproj", "mp_", "la", "ppc", "avr", "mp1", "mp2", "mp3", "wax", "wma", "thx", "dtshd", "Iso", "mbr", "a2m", "cdda", "oga", "ogg", "sap", "fff", "sam", "aiff", "ins", "saf", "m3u", "aifc", "sfk", "sfl", "wv", "caf", "ams", "amr", "igp", "igr", "dcm", "amf", "sfs",

	"DCF", "MXML", "EMP", "PBF", "WVE", "HMA", "WVC", "MPGA", "DEWF", "MWS", "EMD", "ARIAX", "SYN", "FLAC", "EFK", "XA", "EFE", "EFA", "HDP", "XSPF", "EFV", "CFA", "SF2", "EFS", "EFQ", "KIN", "ALAW", "AC3", "RAW", "RAX", "TD0", "ALAC", "QCP", "CIDB", "KIT", "K26", "RAM", "PTS", "BAP", "PTM", "MED", "DVF", "PTF", "ACT", "ACP", "SHN", "8MED", "VPM", "DMF", "ACD", "ACM", "G723", "G721", "G726", "NVF", "PK", "B4S", "CSH", "RSN", "RSO", "ADV", "DDT", "SDAT", "GSM", "WUT", "Krz", "SMP", "C01", "XRNS", "CEL", "FZF", "WPROJ", "RFL", "FTM", "ZVR", "ZVD", "VTX", "MSV", "XMZ", "S3M", "XMI", "ULAW", "IT", "XMF", "KMP", "S3I", "4MP", "F4A", "DRG", "OTS", "DRA", "AIF", "S3Z", "HSB", "SB", "RTS", "VOI", "OMX", "OMG", "OMF", "OMA", "M3U8", "RTI", "CWP", "RTM", "GROOVE", "NST", "BIDULE", "AGM", "MA1", "NSF", "DIG", "NSA", "SEG", "AHX", "TG", "SEQ", "SES", "PCM", "NAP", "PCG", "PCA", "ACD-BAK", "K25", "OVW", "UWF", "RBS", "VMD", "SWA", "RMF", "MXL", "ADTS", "AUP", "RMM", "RMI", "RMJ", "AUD", "RMX", "R", "MMM", "VQF", "EXPRESSIONMAP", "MMF", "ABC", "ABM", "I", "NWC", "VC3", "GIG", "PPCX", "SPX", "MOD", "AKP", "OFR", "IMP", "IMF", "ULT", "SESX", "SYW", "IFF", "A52", "XSB", "XT", "ALS", "XP", "SYX", "XM", "ALL", "XI", "ALC", "SYH", "ARIA", "API", "DMSE", "JO", "DMSA", "APE", "APF", "EAR", "PNA", "6CM", "DWD", "ITS", "RNS", "ITI", "USF", "RNG", "IQT", "MDL", "RIP"
Video/movie files	"MJ2", "STR", "CLPI", "TPR", "CAMPROJ", "MPV", "PIV", "DDAT", "STX", "CVC", "PRTL", "SMV", "VP3", "REC", "SFVIDCAP", "ANIM", "TIX", "PAR", "MPE", "MPF", "F4P", "QTZ", "PJV", "MPL", "PDS", "STL", "W32", "RTS", "SMI", "AVI", "DAV", "CMPROJ", "DAT", "DZP", "AVB", "AVD", "DMMSM3D", "EVO", "DCK", "WP3", "TP0", "AVS", "AVP", "MOVIE", "MYS", "RMD", "R3D", "3GP", "HKM", "MJP", "MP4", "DIR", "PPJ", "CPI", "RSX", "DV", "QTM", "VDR", "MPEG", "VID", "WMX", "FCP", "VOB", "WMV", "DIF", "VGZ", "MPSSUB", "SEC", "DXR", "F4V", "PNS", "IZZ", "RV", "PRPROJ", "SEQ", "MVB", "787", "TP", "DMSS", "TS", "CAMREC", "TPD", "SVI", "MPG2", "MVE", "K3G", "MVC", "OGM", "RDB", "MOD", "GRASP", "MPG", "DLX", "IFO", "OGV", "SCREENFLOW", "OGX", "RMP",

	"mvp", "vsp", "dv4", "gfp", "mtv", "mvy", "mp21", "mgv", "m2ts", "prel", "sbk", "amx", "amv", "veg", "sfd", "zm1", "zm2", "zm3", "dvdmedia", "aet", "aep", "h264", "pro", "dce", "bs4", "vlab", "bix", "modd", "60d", "rcproject", "m4e", "vro", "swt", "hdmov", "tda3mt", "vem", "viv", "dsy", "vs4", "dzt", "wvx", "swi", "wmmp", "m4u", "m4v", "pssd", "wot", "lrec", "imovieproject", "tivo", "viewlet", "gts", "aepx", "vivo", "zmv", "vdo", "bsf", "mxif", "3g2", "vf", "rum", "dzm", "mjpg", "mpeg4", "rms", "dvr- ms", "qtch", "mpv2", "mpls", "mnv", "m1v", "spl", "izzy", "pva", "cmrec", "cmmtpl", "qtl", "mvd", "dnc", "wm", "vse", "vp7", "scn", "scm", "swf", "scc", "moi", "3gp2", "m21", "3p2", "mmv", "mts", "arf", "dvx", "moov", "vc1", "wtv", "dvr", "dmsd3d", "bik", "bin", "vcpf", "ivr", "ivs", "m15", "tdx", "wpl", "tsp", "vft", "moff", "m2a", "vp6", "ncor", "iva", "dmb", "sqz", "3gpp", "wlmp", "m2p", "fcproject", "m2v", "byu", "m2t", "mp2v", "vcv", "264", "nvc", "ASF", "vcr", "divx", "video", "ale", "msdvd", "m1pg", "gvp", "gl", "cst", "playlist", "mp4v", "psh", "gvi", "edl", "yuv", "bmk", "trp", "asx", "dpa", "meta", "smk", "sml", "dpg", "mkv", "tod", "axm", "roq", "xfl", "pvr", "fbr", "tvs", "mpgindex", "bdm", "fbz", "dmsd", "mov", "smil", "nsv", "dmsm", "rp", "vfw", "3gpp2", "sbt", "lsx", "d3v", "box", "vpj", "qt", "dv-avi", "lsf", "webm", "nuv", "osp", "srt", "msh", "pgi", "3mm", "cmmmp", "ssm", "xvid", "dream", "m75", "imovieproj", "vfz", "aaf", "wcp", "jts", "d2v", "aetx", "jtv", "mswmm", "bdmv", "pmf", "fli", "flh", "rmvb", "m4v", "flc", "rm", "eye", "photoshow", "wmd", "flx", "ivf", "flv", "bnp", "ajp"
Picture/image files	"cvi", "afx", "yaodl", "mix", "mip", "cvx", "u3d", "afm", "cvs", "mic", "sdb", "p21", "sda", "suit", "z3d", "cd5", "sdr", "dae", "txf", "eot", "obz", "af2", "af3", "grn", "gro", "xpm", "obj", "iges", "taac", "gry", "cvg", "cv5", "cdr", "mdl", "cdt", "p2z", "cdx", "xwd", "cdc", "cdg", "cdd", "ddd", "frm", "vue", "ilm", "std", "xbm", "mesh", "jfi", "iwi", "sva", "fh11", "pk", "svf", "svg", "qmg",

	"prw", "ffil", "mgs", "t3d", "dtw", "jpx", "sto", "prc", "xaf", "mgf", "pz2", "jas", "atm", "prm", "dsi", "tjp", "fxg", "dsf", "jxr", "pictclipping", "riff", "dt2", "djv", "ldm", "vml", "3fr", "kpg", "erf", "qti", "scp", "scv", "ttc", "sct", "pz3", "sci", "ydl", "cil", "scg", "3d2", "jpd", "vmd", "fon", "bvh", "sxd", "ccx", "fot", "md5camera", "oct", "pdn", "pdd", "ppm", "nff", "sketch", "pkg", "vp", "gf", "drawit", "asw", "asy", "bdf", "wbc", "wbd", "urt", "mrml", "xft", "wbm", "xfn", "dpr", "pvr", "suniff", "dpx", "wbz", "3dxml", "mb", "mcs", "gem", "info", "cimg", "geo", "prefab", "mcf", "spiff", "wmf", "jtf", "pi3", "wb1", "mcz", "cut", "tfm", "ljp", "s2mv", "acfm", "mc5", "dff", "mc6", "anm", "tps", "pac", "vda", "ac6", "ncd", "lt2", "crf", "pat", "par", "pap", "tpi", "nct", "ncr", "tpl", "fhd", "brk", "u", "bro", "egg", "cpy", "brg", "p3l", "p3m", "cgm", "jb2", "p3d", "pict", "brt", "fsh", "sup", "fh9", "fh8", "phy", "xof", "3dc", "v3o", "vox", "fh7", "jbmp", "rds", "obp", "vob", "md5mesh", "agif", "jbf", "awd", "awg", "jbr", "pop", "br3", "br5", "br4", "pov", "br6", "sid", "sig", "sim", "fry", "jp2", "gfb", "pzz", "vst", "vss", "2bp", "ota", "mot", "rdl", "pzp", "mos", "ddrw", "sprite", "cp", "3ds", "cpt", "cps", "ai", "cp", "cpd", "cpc", "fal", "cit", "odi", "odg", "design", "jps", "3dl", "fac", "fax", "a8s", "jpg", "jpf", "jpe", "cin", "jpc", "3dx", "vs", "sgi", "fp3", "db", "mrxs", "cnv", "tb0", "mtl", "sc4model", "spj", "mgmt", "mgmx", "spe", "pef", "spc", "mtx", "mtz", "mgmf", "spu", "spr", "spp", "otg", "egl", "ecw", "wrl", "hf", "itc2", "arw", "art", "arr", "plt", "ply", "hr", "ivr", "lwo", "tlc", "xpr", "ft11", "ft10", "sh3f", "xcf", "ive", "kfx", "blkrt", "pe4", "lws", "vv", "psp", "pl1", "pl0", "pl2", "ovp", "ovr", "psk", "psd", "pse", "psf", "psa", "psb", "gbr", "cdmm", "fbm", "nrw", "pjg", "ic1", "smd", "ic3", "ic2", "cdmz", "dfont", "picnc", "rcs", "pspbrush", "cdmt", "qif", "exp", "exr", "fh10", "si", "aic", "gp4", "hpg", "ntr", "ais", "gks", "sr", "dcx", "cmz", "lfn", "360", "tub", "icn", "dpp", "hip", "ica", "3dmf", "icb", "3don", "off", "zt", "flt", "cag", "gpd", "vac", "graffle", "stp", "dcs", "pix", "pjg", "anim",
--	--

	"mpf", "ste", "hr2", "pic", "mpo", "rw2", "wdp", "ppz", "tg4", "svgz", "ppf", "3d4", "woff", "epsf", "8pbs", "pal", "igt", "zgm", "thm", "ifc", "pi6", "pi4", "pi5", "pi2", "hrf", "pi1", "pwp", "hrz", "pws", "albm", "wmz", "dicom", "wmp", "rle", "pp5", "pp4", "3da", "3df", "tga", "pp2", "step", "x mmap", "orf", "3dm", "blz", "3dv", "mbm", "fc2", "rwl", "ink", "chr", "thumb", "e57", "mnm", "m3d", "sar", "drw", "ithmb", "cha", "int", "cam", "cal", "fif", "can", "vbr", "fil", "dcr", "sfc", "sfd", "sff", "hd2", "dcm", "vrl", "wi", "igx", "nif", "pxr", "mgcb", "cas", "sfw", "wvl", "fig", "c4d", "veg", "emz", "pbm", "ufo", "emf", "yuv", "xrf", "bsk", "gtemplate", "jbig", "3d", "dc2", "fp", "hdp", "hdr", "fpg", "fpf", "fpe", "hdz", "a2c", "ac5", "tmd", "ras", "raw", "ray", "ysp", "kic", "session", "rad", "p3r", "raf", "ips", "ptx", "viff", "met", "fits", "icpr", "psid", "meb", "cdmtz", "mef", "dvl", "ptg", "shg", "glox", "cm2", "acr", "mng", "wic", "shp", "usertile- ms", "smf", "mnr", "br7", "amfm", "pd", "vna", "csy", "adc", "rsr", "pm", "tn1", "blend", "ddb", "csm", "ps", "rsb", "ddt", "px", "csf", "dds", "gsd", "vnf", "v3d", "ft7", "lif", "smp", "epp", "eps", "ft9", "ft8", "bto", "mrw", "pm3", "caf", "gmt", "xsf", "fmv", "vff", "wrp", "msk", "pfr", "md5anim", "ftn", "wrz", "rft", "pdf", "pfb", "pfa", "vic", "msp", "pfm", "gstencil", "ts1", "pl", "001", "pmg", "pmd", "apd", "xmm", "iv", "cfg", "xmf", "xv0", "pxm", "411", "mac", "drf", "tif", "asat", "kmc", "mat", "gdr", "b3d", "oti", "otf", "trif", "sh3d", "otb", "kodak", "max", "x3d", "compositefont", "x3f", "cmod", "bmp", "fcz", "bmf", "omf", "bmc", "sun", "jpeg", "kmcobj", "ttf", "qtif", "yal", "agp", "lbn", "sld", "vtx", "scu", "dib", "dia", "dif", "t2b", "bm2", "jng", "nap", "cmx", "pcd", "pcf", "8xi", "j2c", "pcx", "tri", "cals", "j2k", "mmat", "m3", "fg", "zif", "prv", "ogf", "fs", "fp", "face", "fx", "truck", "ltz", "fxa", "ipx", "jia", "apng", "jif", "xar", "pc1", "pc2", "pc3", "mxi", "hpgl", "mp", "m xm", "avatar", "mxf", "kdk", "ma", "kdi", "mf", "kdc", "mxs", "ms3d", "s", "rpf", "jwl", "v", "tex", "xsi", "tme", "artwork", "y", "x", "vsd", "skm", "skl",
--	--

	"abf", "crw", "dng", "abc", "j", "abm", "crz", "sumo", "qc", "gif", "bip", "gih", "ded", "gim", "icon", "tiff", "maxc", "skp", "grob", "cmf", "des", "pntg", "fbx", "i3d", "Ind", "img", "sk2", "sk1", "vsh", "cr2", "skitch", "jiff", "imj", "fpos", "wbmp", "fnc", "gmbck", "mgtx", "ilbm", "gcdn", "fnt", "tddd", "srw", "rgb", "act", "mrb", "ct", "d3d", "tn3", "tn2", "srf", "jfif", "pgf", "neo", "ce", "pgm", "nef", "webp", "apm", "pnm", "pni", "png", "dxb", "djvu", "apx", "pnt", "pns", "aps", "hpl", "dwf", "hpi", "sr2", "hipnc", "c4", "pspimage", "wpg", "tny", "gfe", "mdx", "lxf", "ric", "rif", "rig", "rix", "an8"
--	---