EVault™
Endpoint Protection

EVault Endpoint Protection Version 7

Dashboard User Guide

Revision: This manual has been updated for Version 7 (July 2014).

Software Version: 7.0

EVault, A Seagate Company, makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, EVault reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of EVault to notify any person of such revision of changes. All companies, names and data used in examples herein are fictitious unless otherwise noted.

EVault, A Seagate Company
c/o Corporation Trust Center
1209 Orange Street
Wilmington, New Castle
Delaware 19801
www.EVault.com

Acknowledgements: Two encryption methods, DES and TripleDES, include cryptographic software written by Eric Young. The Windows versions of these algorithms also include software written by Tim Hudson. Bruce Schneier designed Blowfish encryption.

The EVault Software Agent, EVault Software CentralControl, and EVault Software Director applications provide encryption options for 128/256-bit AES (Advanced Encryption Standard). Advanced Encryption Standard algorithm (named Rijndael, pronounced “Rain Doll”) was developed by cryptographers Dr. Joan Daemen and Dr. Vincent Rijmen. This algorithm has been chosen by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce to be the Federal Information Processing Standard (FIPS).

The EVault Software Agent and EVault Software Director applications include the security feature of over-the-wire (OTW) encryption.

Contents

1 Introduction

Welcome to the *Dashboard User Guide*. The vault dashboard is where you go for administrative tasks such as creating devices ready to be protected.

The purpose of this document is to provide the information necessary to easily navigate through the various screens of the dashboard. This guide provides step-by-step instructions relative to performing common tasks, such as creating devices, resetting passwords and creating reports.

2 Login

To log in to the dashboard, go to the dashboard URL provided by your administrator. This will normally be either https://*vaultdns* or https://*vaultdns*/Dashboard.

You will need to provide credentials to log in and this is normally your email address and a password. There are other options depending on the configuration of your vault so if your login page doesn't look like this you can see *9.1 Login alternatives* for more details.

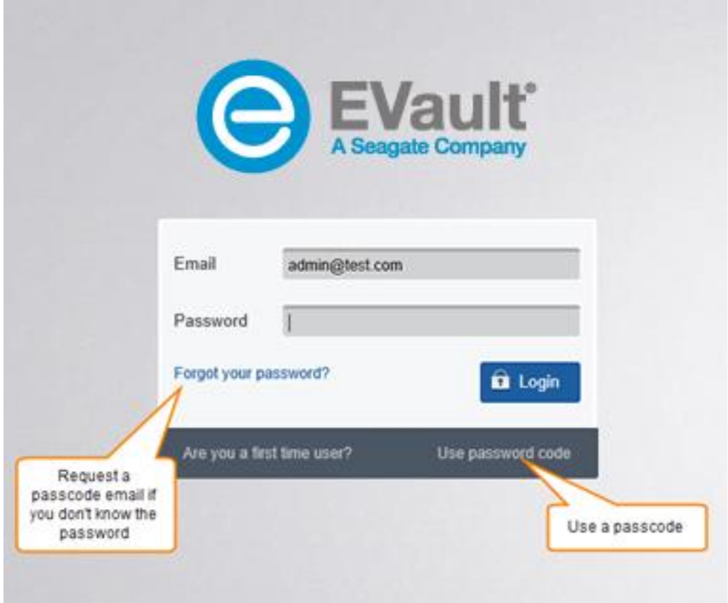


Figure 1 Login page

Login by entering your email address and password and clicking Login.

If you have not set up a password, or you have forgotten it, then you will need to get a passcode. This is a one time use code that will allow you to login and set up your own password. You can request one by clicking the "Forgot your password?" link and confirming your email address. A passcode will be emailed to you.

To use a passcode:

1. Click the link in the passcode email you received.
2. Alternatively enter the details manually from the login page.
    a. Click "Are you a first time user?"
    b. Enter the password code you received via email in the passcode field.
3. Enter or confirm your email address in the email field.
4. Click Login. You will be required to change your password.
5. Enter your new password.
6. To verify your password, enter your new password again.
7. Click Change password

To log out of the Vault Dashboard before closing your browser:

1. Click Logout on the upper right corner of any of the Dashboard screens to sign out.
2. If you want to remove the cookie that allows your email address to be defaulted, click the Forget me button.
3. If you used integrated login, this may still be logged in, so close the browser windows to clear this as well.

3 General navigation

3.1 Home page

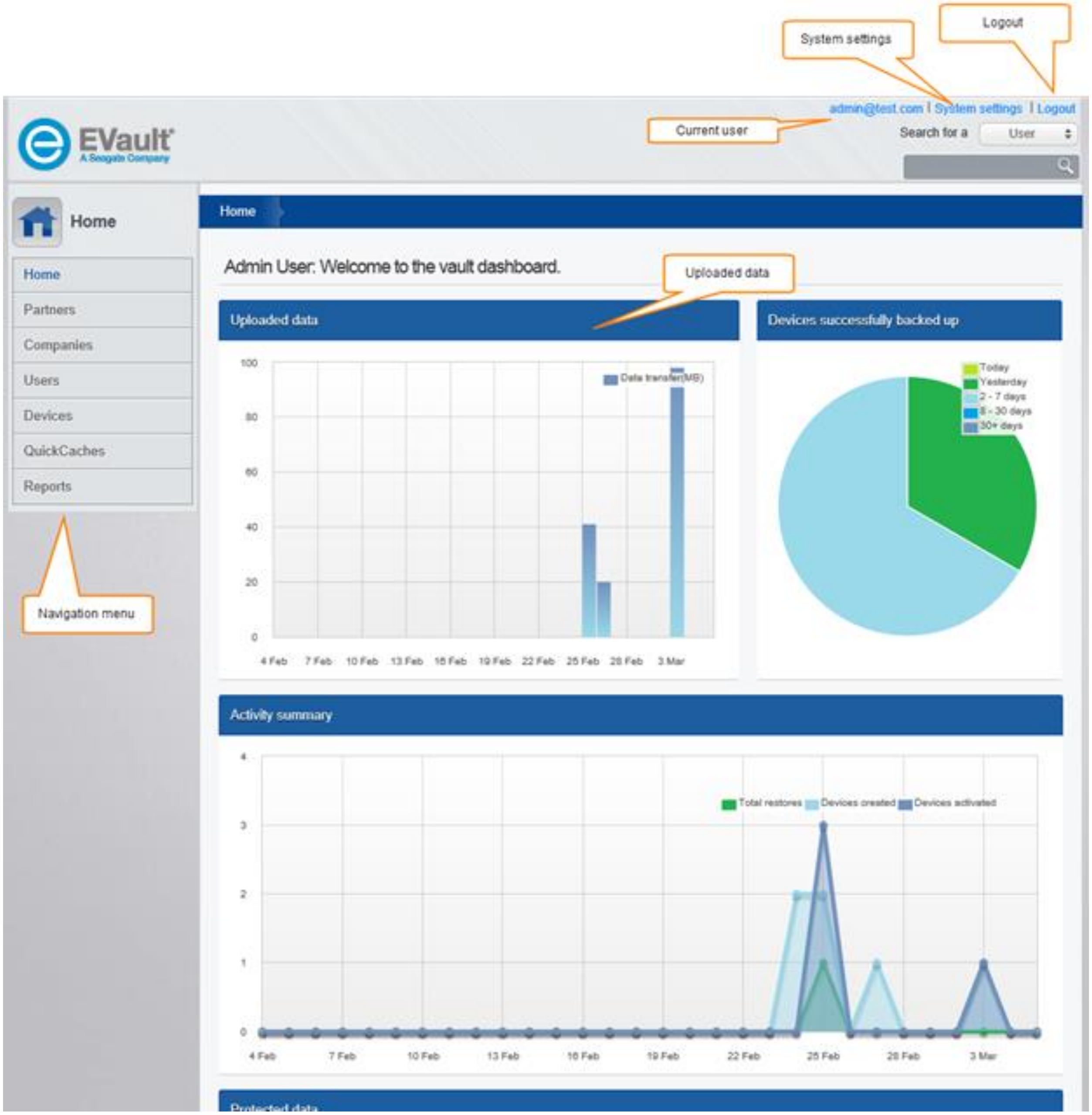
The Dashboard home page is the starting point for all Dashboard actions. Use the navigation menu on the left side of the home page to access list pages for:

- Partners
- Companies
- Users
- Devices
- QuickCaches
- Custom Reports

Note that depending on your level of access, some of these items may not be visible to you.

The home page also provides a high-level view of current activity in the vault. There are four graphical reports on the home page:

- Uploaded data
- Devices successfully backed up
- Activity summary
- Protected data



Admin User: Welcome to the vault dashboard.

Figure 2 Dashboard home page

3.1.1 Uploaded data

The uploaded data chart shows how much data has been uploaded from protected devices each day over the last month. If a number of new devices were activated on a day you will see a spike as those devices do their first backups, otherwise this chart will show the pattern of data change in your organization – this can be fairly constant, or may have a weekly pattern if not much data changes on weekends for example.

3.1.2 Devices successfully backed up

This pie chart shows all active devices, and how recently they were protected. This is organized on a sliding scale – devices which have backed up today, ones that backed up yesterday but not yet today, then ones that backed up earlier this week, in the last month or more than 30 days ago.

If computers are turned on and connecting to the vault they should normally display in the graph as protected either today or yesterday (if nothing has changed yet today). If a device is performing a large backup that is taking more than a day to upload (usually a first backup or if lots of data has been added) then it will show up in an older category until that upload completes.

If you have devices showing up as protected a long time ago, this often indicates that they are not being used any more. The machine could be turned off or the software uninstalled. If the backups from those devices are no longer needed you can cancel them, otherwise you can suspend them to remove them from this pie chart. Use the Device list to find these devices.

3.1.3 Activity summary

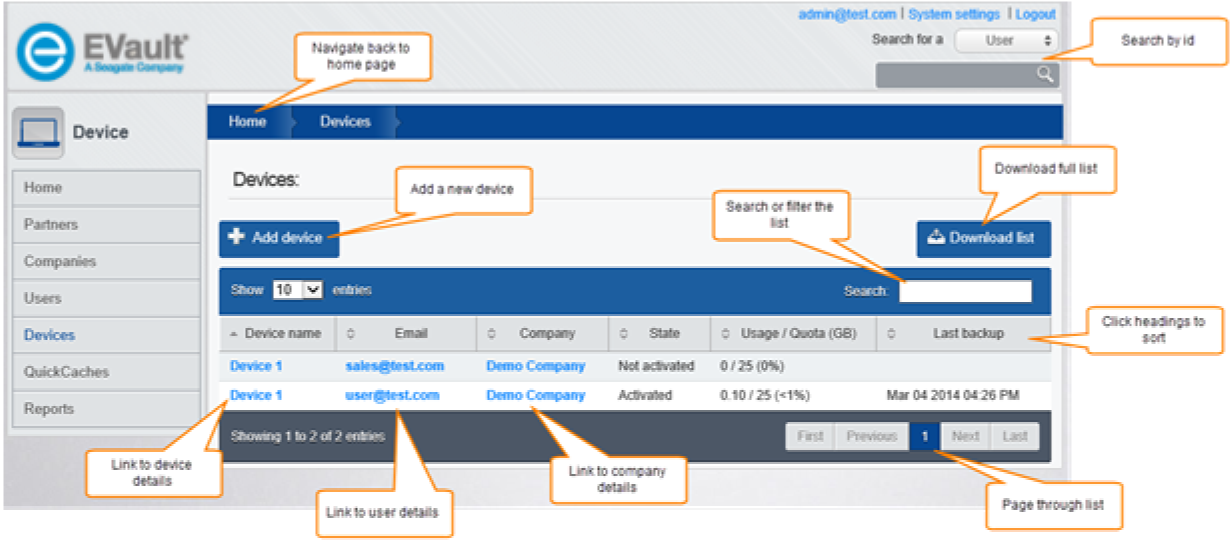
The activity summary shows some of the more variable activity that has happened over the last month. You will see restores and devices being created or activated. When you are getting started there will be lots of activity here as devices are created and then activated, but over time it is common to see less here if you are not adding new devices. You will see restores from time to time, but depending on your users this can be quite rare.

3.1.4 Protected data

This chart shows the number of devices and total amount of protected data. Normally this just grows as new devices are added and existing devices add data but it will go down if you cancel devices.

3.2 Lists

You can use the items on the menu on the left to navigate through the entities in your vault. Clicking on these normally take you to a list, such as a list of devices. Depending on your level of access, sometimes it will take you directly to an item. For example, if you are a company administrator it will take you directly to the company details page for your company.



Device name	Email	Company	State	Usage / Quota (GB)	Last backup
Device 1	sales@test.com	Demo Company	Not activated	0 / 25 (0%)	
Device 1	user@test.com	Demo Company	Activated	0.10 / 25 (<1%)	Mar 04 2014 04:26 PM

Figure 3 Device list

You can page through the list using the controls on the bottom right to move to a specific page, or the next or previous pages.

When you are in a list, you can jump to details pages for an item by clicking hyperlinks in the list. For example, on a device list you will see links for the device, the user and the company that each take you to those details.

You can sort lists by clicking on the headings, and the column currently used for the search will be indicated by an up or down triangle.

You can search within a list by typing in the search box on the top right. This searches in all the columns you see, and also the custom fields, and will filter the list to only those including the search criteria. You can keep typing to further filter the list.

If there are more results that show on the page, you can use the buttons at the bottom of the page to navigate more entries.

In most lists you can also download the full list by clicking on the Download list button on the right. This will give you the option to download the full list as either an Excel file or .csv. If you use the Excel format the spreadsheet will have links in it so it is similar to the list you see in the dashboard. Click the links to go directly to the appropriate page in the dashboard. When you open the spreadsheet in Excel, you may see a warning because the spreadsheet has been downloaded from an internet site. Click Enable Editing to allow the hyperlinks to be shown. The .csv file can also be opened in Excel or loaded into another application.

Both list formats will include more columns of data, so they can be useful for finding using different criteria. For example, when you download the list of devices you will see the operating system version installed on those machines, as well as the data protection agent version number.

Another way to find an item is using the search field in the upper right. This allows you to quickly find a specific Device, User, Company or Partner, by name or id. This is particularly useful when looking for a specific device id since you can find the device id on the About box in the client.

To search for a device by id:

1. Select Device from the “Search for a” menu.
2. Enter the device id in the edit field.
3. Press Enter or click the search icon. The search is active on every page within the dashboard.

4 Users

In most deployments, devices in the vault are allocated to the user of the device. This allows that user to log in to web retrieve to access files backed up from that device, as well as helping you find the device for management purposes.

4.1 Find existing users

Click Users in the left menu to get a list of users. Use the search box above the list to find the user you are looking for. Click their name or email address to get to the user details.

Other ways to get to user details or list of users:

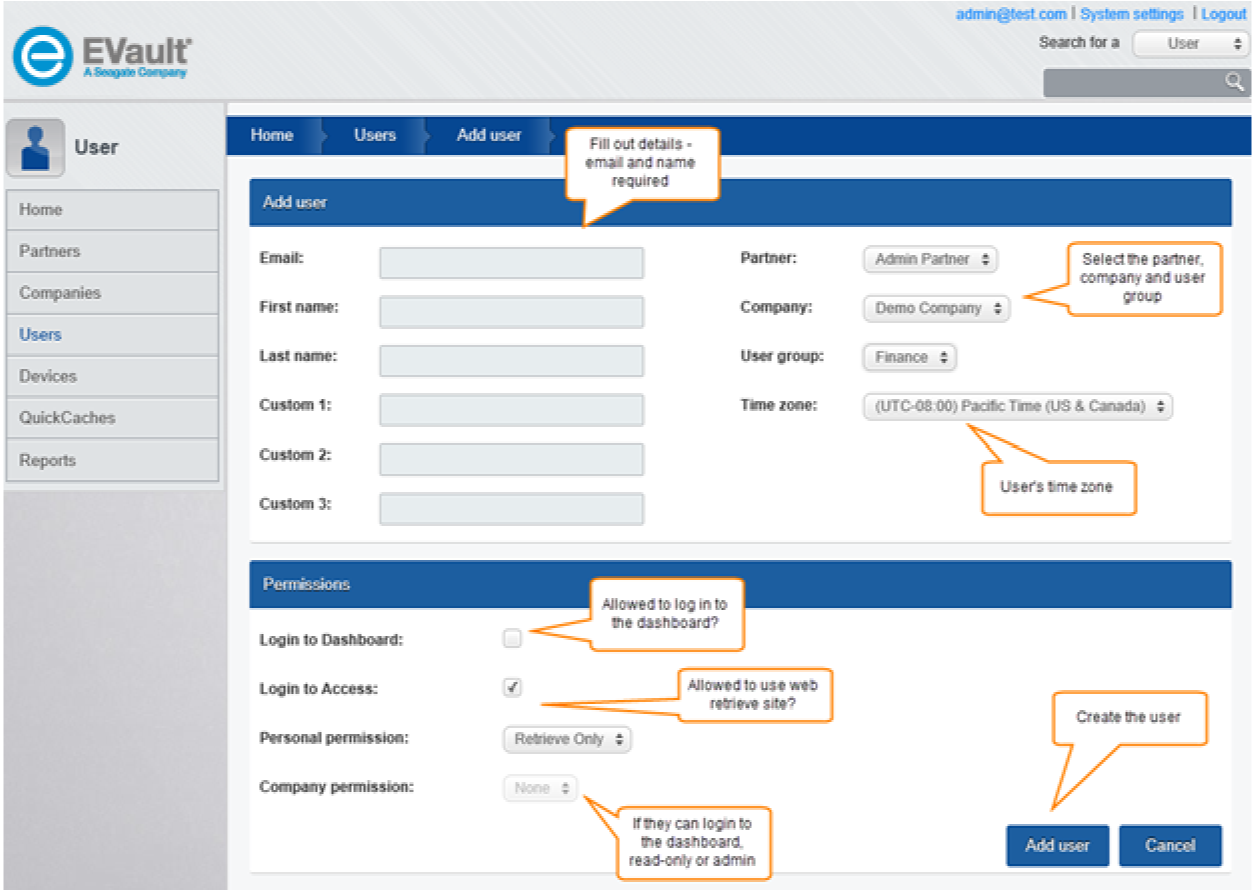
- On the top right you will see a link with your email address. Clicking on this is a fast way to get to your user details page.
- Click on the user email or name shown in other places in the system such as on a device details page.
- On a company details page, click the number of users in the company to get a user list restricted to just that company.

4.2 Create a new user

To create a new user manually:

1. From the home page menu, click on Users to get to the list of users
2. Click the Add user button on top of the list
3. Enter user’s email address in the “Email:” field. This will be their login to the web retrieve site as well as the dashboard if they are an admin, and will also be used to send emails with device activation information if you manually create devices for them.
4. Enter user’s first name in the “First Name:” field.
5. Enter user’s last name in the “Last Name:” field.
6. Enter desired optional information in the next three “Custom 1:,” “Custom 2:,” and “Custom 3:” fields. For example, enter physical address of company or contact name.
7. If needed, select the partner, company and user group for the user from the lists on the right. These may be automatically filled in by the system.
8. If the user is to be an administrator, you can change their time zone if needed. Times in the dashboard will be converted to this time zone for display.
9. Select desired permissions for the user – you can only give the user permissions that you already have:
    a. Check Login to Dashboard if this user is to be an administrator – then select either Read Only or Administrator to give them permission to the company. Other permissions such as administrator to a user group or to the whole system can be set after you create the user.
    b. Check Login to Access to allow the user to retrieve files from their backup from web retrieve

10. Click “Add user” to save the changes
11. If there are any problems with the data entered they will be shown at the top of the page. For example if one of the required fields has not been set.
12. Once the user is created the user details page for that user will be displayed.



Fill out details - email and name required

Email:

First name:

Last name:

Custom 1:

Custom 2:

Custom 3:

Partner: Admin Partner

Company: Demo Company

User group: Finance

Time zone: (UTC-08:00) Pacific Time (US & Canada)

Select the partner, company and user group

User's time zone

Login to Dashboard: ☐

Allowed to log in to the dashboard?

Login to Access: ☑

Allowed to use web retrieve site?

Personal permission: Retrieve Only

Company permission: None

If they can login to the dashboard, read-only or admin

Create the user

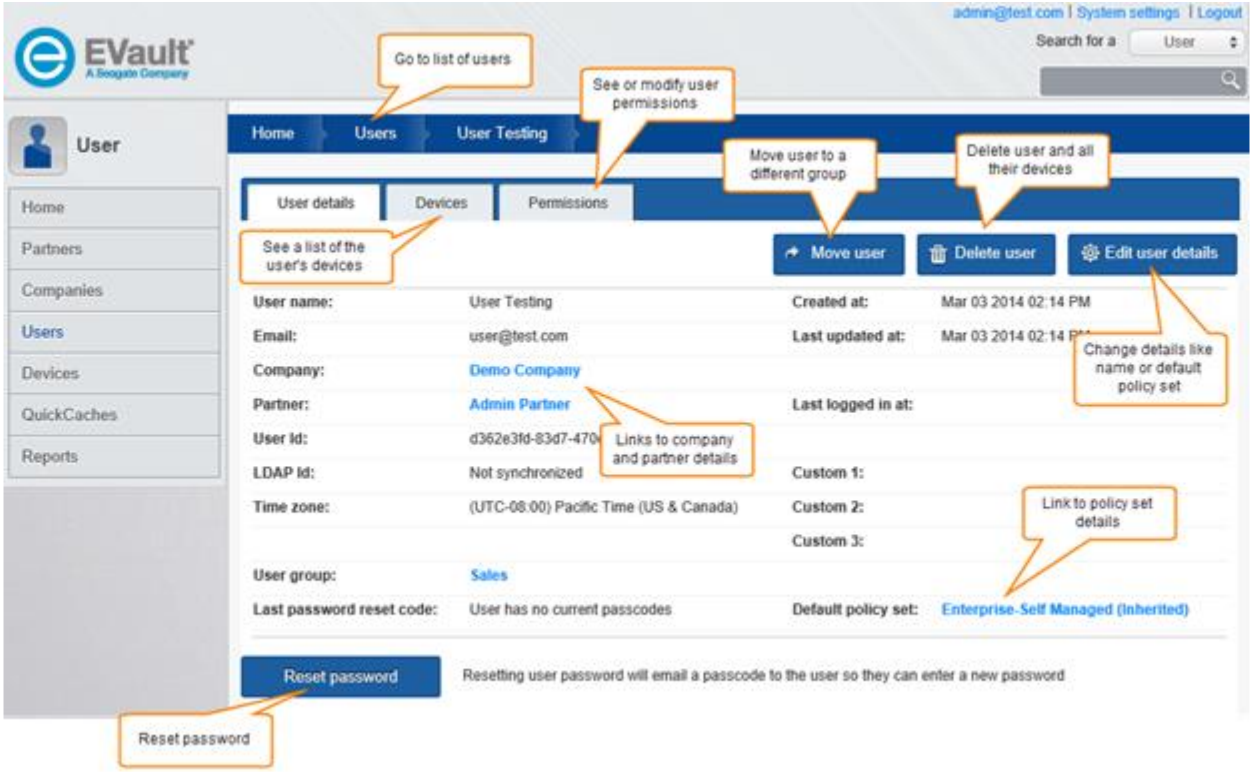
Figure 4 Add user

Users can also be created in other ways:

- From the company details page you can import users from a spreadsheet – see 9.6 Bulk creation of users or devices
- Users can be created automatically when deploying devices – see the document “Automating client deployment”
- LDAP synchronization can be set up for a company to automatically create users based on the corporate directory (such as Active Directory) – see the document “LDAP Synchronization”

4.3 User details

Once you add the user or when a user has been selected another way, you will see the user details page. From here, you can see information about the user or their devices and make changes.



Go to list of users

See or modify user permissions

Move user to a different group

Delete user and all their devices

See a list of the user's devices

Change details like name or default policy set

Links to company and partner details

Link to policy set details

Reset password

User name: User Testing

Email: user@test.com

Company: Demo Company

Partner: Admin Partner

User Id: d362e3fd-83d7-470

LDAP Id: Not synchronized

Time zone: (UTC-08:00) Pacific Time (US & Canada)

User group: Sales

Last password reset code: User has no current passcodes

Created at: Mar 03 2014 02:14 PM

Last updated at: Mar 03 2014 02:14 P

Last logged in at:

Custom 1:

Custom 2:

Custom 3:

Default policy set: Enterprise-Self Managed (Inherited)

Resetting user password will email a passcode to the user so they can enter a new password

Figure 5 User details

4.3.1 Making changes

To edit the details of an existing user:

1. Click the “Edit user details” button.
2. Make the desired changes.
    a. Change the user's email address to change the email address they need to enter to log in to the dashboard or web retrieve site.
    b. Change the user's name, custom information or dashboard time zone as needed.
    c. Change the assigned policy set to change protection settings for any devices using the default policy set. See policy assignment for more information on this.
3. After editing user information, click “Save changes.”

To reset a user’s password for their Dashboard sign on:

1. From the user details page click the Reset password button.
2. A message box will pop up to confirm that you want to reset the user’s password and send the user an email with a new passcode, click Ok to confirm.

If you do this on your own user details page you will instead be presented with a change password screen where you enter your current password and a new one.

4.3.2 Delete a user

Users can be deleted if desired. If you delete a user, that will delete all devices belonging to that user, along with all backups. In most cases you don't want to lose that data so you should first suspend and move their devices – see 9.4 Keeping backup data for old devices for more details

To delete a user once you have determined the devices they have are not needed:

1. From the user details page, click the Delete button.
2. Read the warning message. If you are sure this is the correct user and you want to delete them, along with all the backed up data from their devices, check the confirmation box and then click Ok.
3. Click the close (x) on the box if you do not want to proceed.

4.3.3 Change groups

If a company is using user groups, users can be moved between groups within their company. This could be needed if they are initially created in the wrong group or if they have changed roles within the company. As long as the user and their devices are using the default policy set for the current group, they will change to using the policy set for the new group.

To move a user:

1. Click the "Move user" button – this button will only be available if the company has multiple user groups.
2. In the popup, choose the new user group for the user.
3. Click Ok.

4.3.4 User permissions

Most users will just have permission to retrieve files from their devices using the Access site. This is the default setting when you create a new user.

Some users should be able to log in to the dashboard to manage users and devices. If you check Allow login to Dashboard when creating a user it will default to giving the user admin access to the company. This will allow the user to manage groups, users and devices in their company.

Changes to the user's permissions can be made on the Permissions tab. See 9.2 Changing permissions for more information.

5 Devices

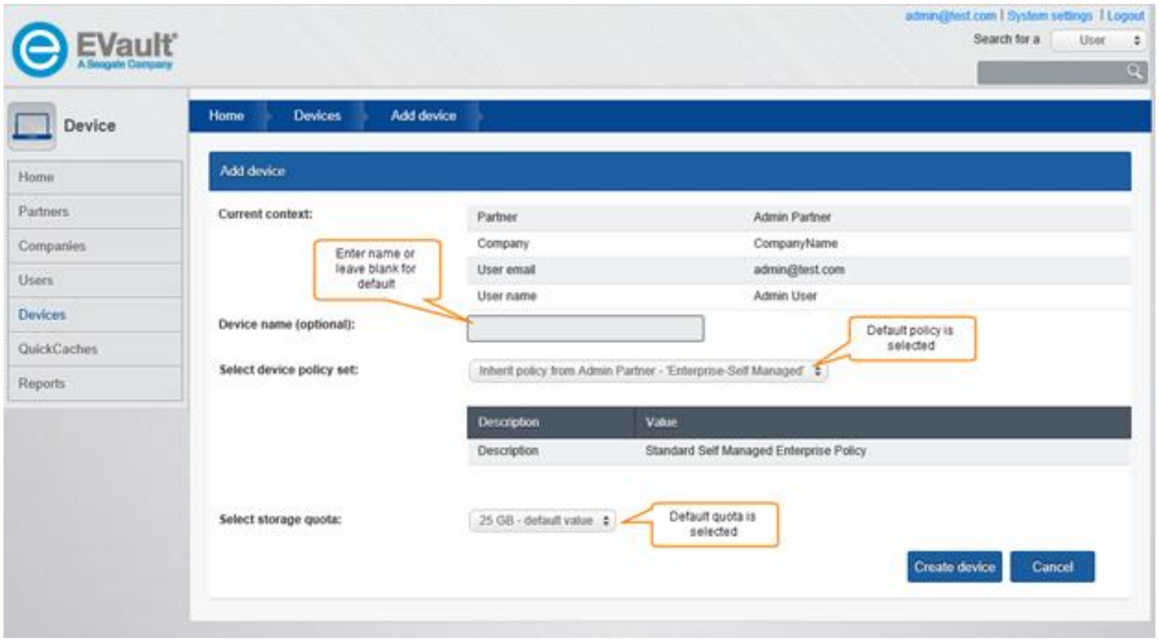
5.1 Create devices

Devices can be created in bulk using Import devices from the company details page – for more information see *9.6 Bulk creation of users or devices*. Devices and users can also be created automatically during deployment and the document “Automating client deployment” has more information on these options.

Devices can also be created manually. Normally devices are created under the user who is the actual user of the machine and the system will send them an email with installation instructions.

To create a new device:

1. Navigate to the user details page for the user.
2. Click Devices to go to the devices list for that user.
3. Click Add device at the top of the list.
4. The user will be automatically selected and only the device details need to be entered.
5. Enter a name if desired to identify the computer. This is optional as a name such as Device 1 will be created automatically.
6. The default policy and quota will be selected which you can change if needed.
7. Click Create device.
8. The device details will be displayed.


admin@test.com | System settings | Logout
Search for a
User
Device
Home
Partners
Companies
Users
Devices
QuickCaches
Reports
Home
Devices
Add device
Enter name or leave blank for default
Default policy is selected
Default quota is selected
Create device
Cancel

Add device

Current context:

Partner	Admin Partner
Company	CompanyName
User email	admin@test.com
User name	Admin User

Device name (optional):

Select device policy set: Inherit policy from Admin Partner - 'Enterprise-Self Managed'

Description	Value
Description	Standard Self Managed Enterprise Policy

Select storage quota: 25 GB - default value

Figure 6 Add Device

You can also create a new device from other starting points.

- On the Company details page, click Add device.

- Click Devices in the menu on the left to get the list of devices then click Add device.
- On the Company details page, click the number of devices to get a device list and click Add device.

In these cases you will need to select the user to own the device before the add device page is shown.

To select a user and create a device:

1. Navigate to Add device from the devices list or company details.
2. If you want to select an existing user for this device, enter some search criteria to help you find them. For example, enter part of their email address. Alternatively, select a different criteria in the list such as user name. Click Search. A user list will be presented which can be sorted and filtered as for other lists. This list will be already restricted to users in the company if you started from the company details page. Find the user and click the radio button on the left to select them, then click Select user.
3. If you need to create a new user for this device you can click Add user to create a new user and select that user for the device.
4. You will now see the Add device page with the details for the user displayed.
5. Enter a device name if you wish.
6. The default policy and quota will be selected which you can change if needed.
7. Click Create device.
8. The device will be created and the device details page displayed.

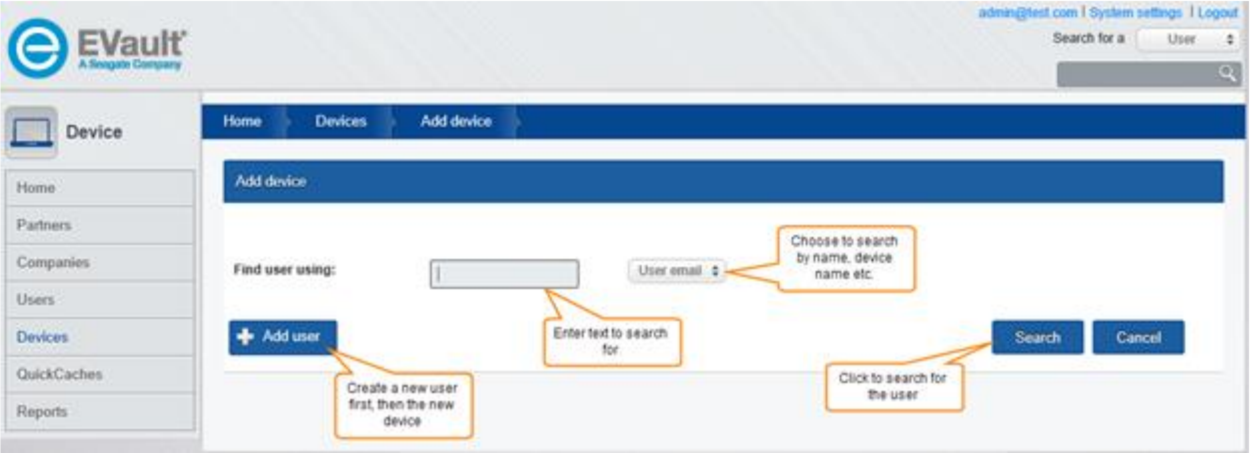
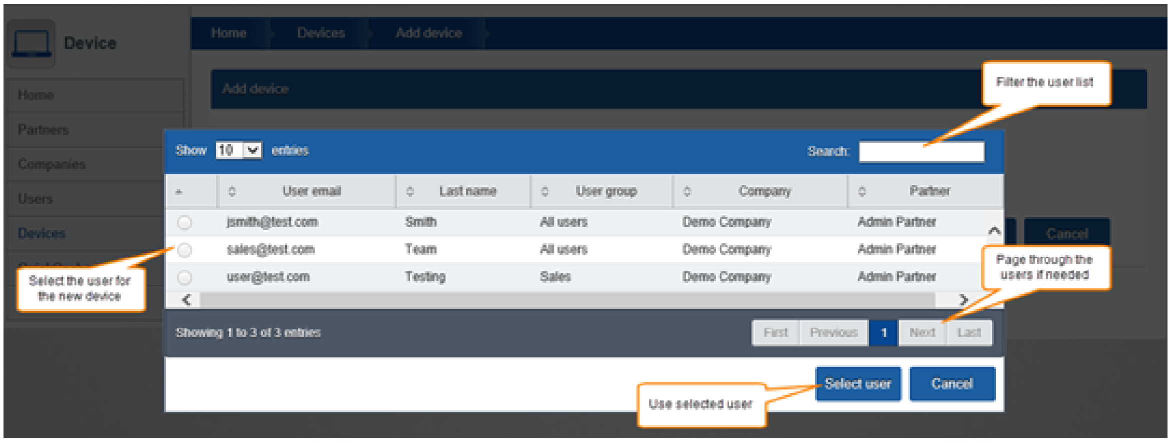


Figure 7 Search for user for new device



	User email	Last name	User group	Company	Partner
○	jsmith@test.com	Smith	All users	Demo Company	Admin Partner
○	sales@test.com	Team	All users	Demo Company	Admin Partner
○	user@test.com	Testing	Sales	Demo Company	Admin Partner

Showing 1 to 3 of 3 entries

Filter the user list

Select the user for the new device

Page through the users if needed

Use selected user

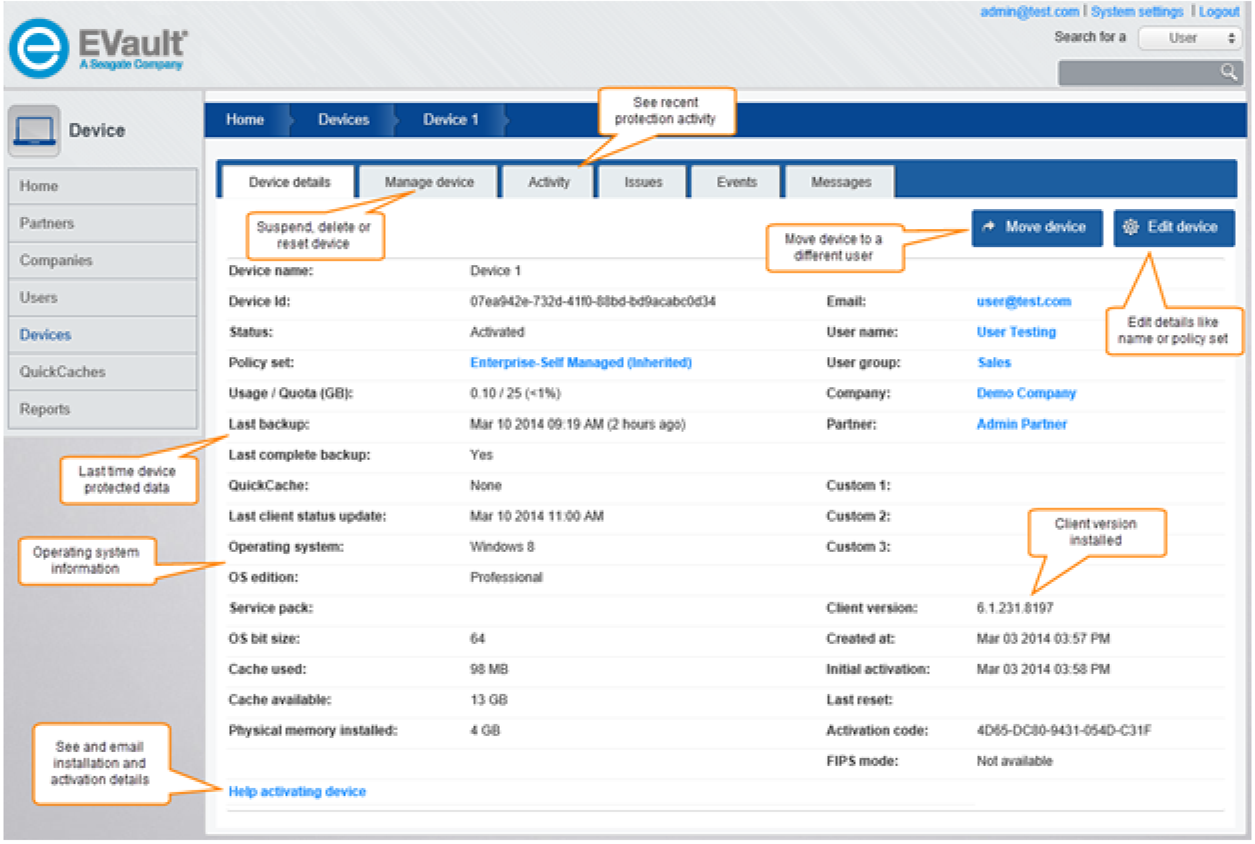
Figure 8 Select user for new device

5.2 Device Details

There are a number of tasks that can be performed on a device and the first step is to find the device in a list and click on the device to get to the device details page.

To find the device in a list do one of the following:

- Search by selecting "Search for a" device and entering the device name, id or name of the user the device belongs.
- Click Devices to get a list of all devices and find the device in the list.
- From a user details page, click the Devices tab to see a list of that user's devices.
- From a company details page click the link for the number of devices in the company to get a list of devices in that company.



See recent protection activity

Suspend, delete or reset device

Move device to a different user

Edit details like name or policy set

Last time device protected data

Operating system information

Client version installed

See and email installation and activation details

Device name:	Device 1		
Device Id:	07ea942e-732d-41f0-88bd-bd9acabc0d34	Email:	user@test.com
Status:	Activated	User name:	User Testing
Policy set:	Enterprise-Self Managed (Inherited)	User group:	Sales
Usage / Quota (GB):	0.10 / 25 (<1%)	Company:	Demo Company
Last backup:	Mar 10 2014 09:19 AM (2 hours ago)	Partner:	Admin Partner
Last complete backup:	Yes		
QuickCache:	None	Custom 1:	
Last client status update:	Mar 10 2014 11:00 AM	Custom 2:	
Operating system:	Windows 8	Custom 3:	
OS edition:	Professional		
Service pack:		Client version:	6.1.231.8197
OS bit size:	64	Created at:	Mar 03 2014 03:57 PM
Cache used:	98 MB	Initial activation:	Mar 03 2014 03:58 PM
Cache available:	13 GB	Last reset:	
Physical memory installed:	4 GB	Activation code:	4D65-DC80-9431-054D-C31F
		FIPS mode:	Not available

Figure 9 Device details

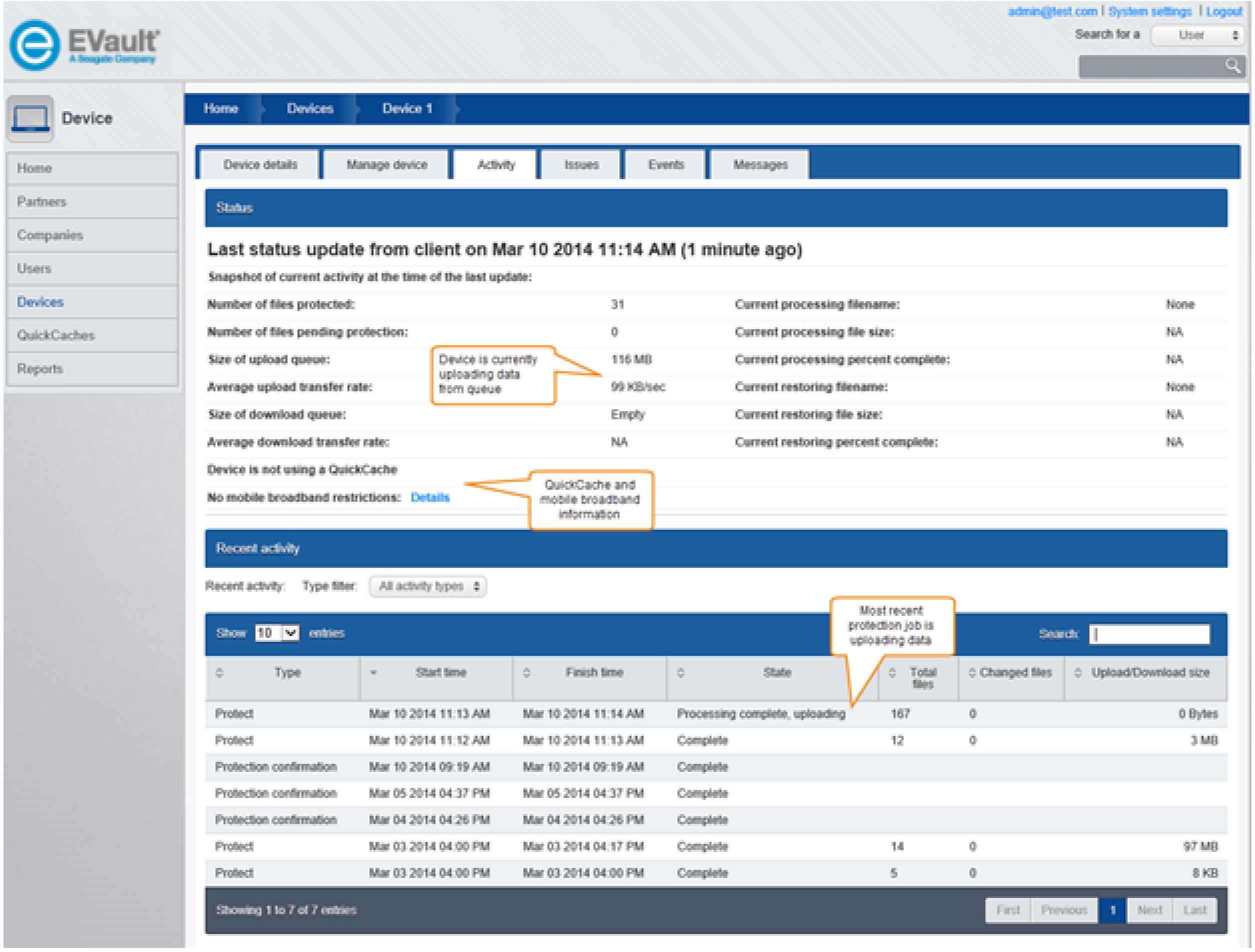
On the device details page you can see all the information the system has about a device and the computer it is installed on. For example, you can see the version of the client installed as well as the operating system type and version, and when it last completed a backup.

5.2.1 Activity

To see more detail about what has been happening on a device, you use the Activity tab on the device details. The top section shows most of the information that the user can see in the home page of the client application on the machine. Below that is the list of what has happened on the device, which is also available in the client by clicking “Show recent activity” in the client. This allows you to look at the current state of backups without having to go to the computer itself.

In the top section you can also see whether the device has been connecting through a QuickCache or through a mobile network.

On the Issues, Messages and Events tabs you will see information about other things that have happened on the device.



Last status update from client on Mar 10 2014 11:14 AM (1 minute ago)

Snapshot of current activity at the time of the last update:

Number of files protected:	31	Current processing filename:	None
Number of files pending protection:	0	Current processing file size:	NA
Size of upload queue:	116 MB	Current processing percent complete:	NA
Average upload transfer rate:	99 KB/sec	Current restoring filename:	None
Size of download queue:	Empty	Current restoring file size:	NA
Average download transfer rate:	NA	Current restoring percent complete:	NA

Device is not using a QuickCache

No mobile broadband restrictions: Details

Recent activity: Type filter: All activity types

Show 10 entries Search:

Type	Start time	Finish time	State	Total files	Changed files	Upload/Download size
Protect	Mar 10 2014 11:13 AM	Mar 10 2014 11:14 AM	Processing complete, uploading	167	0	0 Bytes
Protect	Mar 10 2014 11:12 AM	Mar 10 2014 11:13 AM	Complete	12	0	3 MB
Protection confirmation	Mar 10 2014 09:19 AM	Mar 10 2014 09:19 AM	Complete			
Protection confirmation	Mar 05 2014 04:37 PM	Mar 05 2014 04:37 PM	Complete			
Protection confirmation	Mar 04 2014 04:26 PM	Mar 04 2014 04:26 PM	Complete			
Protect	Mar 03 2014 04:00 PM	Mar 03 2014 04:17 PM	Complete	14	0	97 MB
Protect	Mar 03 2014 04:00 PM	Mar 03 2014 04:00 PM	Complete	5	0	8 KB

Showing 1 to 7 of 7 entries

Figure 10 Device activity

5.2.2 Change Quota, Policy Set or other details for a device

Policy sets are used to manage storage quotas, define files / directories to be backed up, history retention, and data deletion / trace and encryption settings.

To edit the device details:

1. From the device details page click the “Edit device” button on the top right.
2. Make the desired changes such as:
    a. Select the desired storage quota from “Select quota storage” menu.
    b. Select the desired policy set from the “Select device policy set” menu. Choose the first option “Inherit policy from …” to select the default policy set rather than set it explicitly. See 5.3 Policy assignment for more information.
    a. Change the device name.
    b. Select the QuickCache the device should use – see 6 QuickCaches for more information.
3. Click “Save changes”.

5.2.3 Find activation information for a device

When you create a device you are creating an entry for it in the vault. Activation is the process of installing the client agent and connecting it to the device entry in the vault to get protection policy information. This is often managed by the automated deployment process or by the end user with the information that was emailed to them when the device was created. However sometimes you may need to retrieve this information again, for example if the user can't find the email, or if the device needs to be reactivated on a new machine.

On the device page there is a link "Help activating device". Click this link to see a popup window with the information needed to activate the device. You will see links to the client software to be installed – click one of these if you are currently using the machine where you want the device installed.

As long as the device is in a state ready to be activated (either newly created or reset) you will also see the information needed to activate – the Activation URL for the vault and the activation code. If you are installing on the machine you are using you can copy and paste these into the agent activation page during installation. If you need to send these details to the user of the device you have 2 options – click the Send link to have the vault send the email directly to the user, or click the Open link to open an email in your email client with the activation details ready for you to add a note to and then send. You can use the Open link to send the email to a different email address if you need to.

5.2.4 Manage device

The Manage device tab has buttons for a number of different actions you can take on the device. Some options may not be available depending on your permissions.

Put on legal hold to prevent any data backed up from the device from being deleted. This will prevent the device from being deleted, stop any instances being removed according to the normal retention policy and prevent the user from removing files using Vault Erase.

To put a device on legal hold:

1. From the device details page, click the Manage device tab
2. Click the Put on legal hold button
3. A dialog will appear so you can enter a comment and confirm.
4. Enter a comment to identify the case or other reason why the device is on legal hold.
5. Click "Put on legal hold" to complete the change.

Remove from legal hold will be available for any device currently on legal hold. Removing a device from legal hold will enable vault erase from the device, reapply the retention settings from policy as well as allow the device to be deleted.

To remove a device from legal hold:

1. From the device details page, click the Manage device tab
2. Click the Remove from legal hold button

3. A confirmation dialog will appear. Read the details to ensure this is what you want to do, including that data backed up from this device will again be able to be deleted, and check the checkbox if you are ready to proceed.
4. Click “Ok” to proceed or click the close icon at the top right if you change your mind

Suspend the device to stop it doing further protection activity, and to prevent data from being restored. One reason you may want to do this is if the user has left the company and their computer has be wiped and reallocated but the data previously backed up is still important. Suspending lets the vault know that device isn’t expected to be online and working so it will be removed from health alerts.

Delete data from the device to instruct a computer to delete all the protected data. This will delete all the data on the computer that is protected and stop the client from working on that machine until reinstalled. It will not delete any backups from the vault, so the data will be available to restore later. You would do this if a device has been reported lost or stolen for example.

To delete data from a device:

1. From the device details page, click the Manage device tab
2. Click the Delete data from device button
3. A confirmation dialog will appear. Read the details to ensure this is what you want to do, and check the checkbox if you are ready to proceed.
4. Click “Ok” to send the command or click the close icon at the top right if you change your mind

Delete device to delete all of the backups for that device and the device information. The backups will not be able to be recovered. Be careful not to confuse “Delete device” with “Delete data from device”. “Delete device” will remove all information about the device and will remove the backups that have been done for that device. “Delete data from device” retains all the backups and only sends a command to the computer to delete the protected files from the machine.

To delete a device:

1. From the device details page, click the “Manage device” tab.
2. Click “Delete device”.
3. Read the warning message. If you are sure this is the correct device and you want to delete it, check the confirmation box and then click Ok.
4. Click the close (x) on the box if you do not want to proceed.

Reset device makes the device available for reinstallation. If the software needs to be installed on a new machine (or reinstalled) the first step is to reset the device. This creates an activation code that can be used on the new machine and also prepares the vault so that after the installation the user will be able to restore their data.

To reset a device:

1. From the device details page, click the Manage device tab.
2. Click “Reset device” and confirmation dialog will appear.
3. You may need to enter your email address and password to confirm that you wish to reset this device, this depends on your vault installation.
4. A passphrase is usually needed. This will be entered by the user when they install the software to confirm that they are the right person to get access to the data backed up to that device. Select a passphrase and enter it into both fields.
5. Click “Reset device” to complete the process.
6. Give the passphrase to the user who will be doing the installation. You will also need to give them the installation location and activation code. It is best to give them the passphrase and activation code in different ways to ensure that only the appropriate user will get access to the data. For example, have the vault send them an email with the activation information, and tell them the passphrase over the phone.

5.2.5 Move users and devices

Devices can be moved between users in the same company. If the device is using the default policy set for the user then it will switch to the correct policy set for the new user it is assigned to.

To move a device:

1. Navigate to the device details page
2. Click the “Move device” button
3. If needed, use the search box to filter users to find the right new user
4. Select the new user by clicking the option button on the row
5. Click “Select user”
6. Confirm the device and user information is correct then click Yes to complete the move

If the option to Move the device doesn’t appear it is either because you don’t have sufficient permission or because there is no other user to be selected.

5.3 Policy assignment

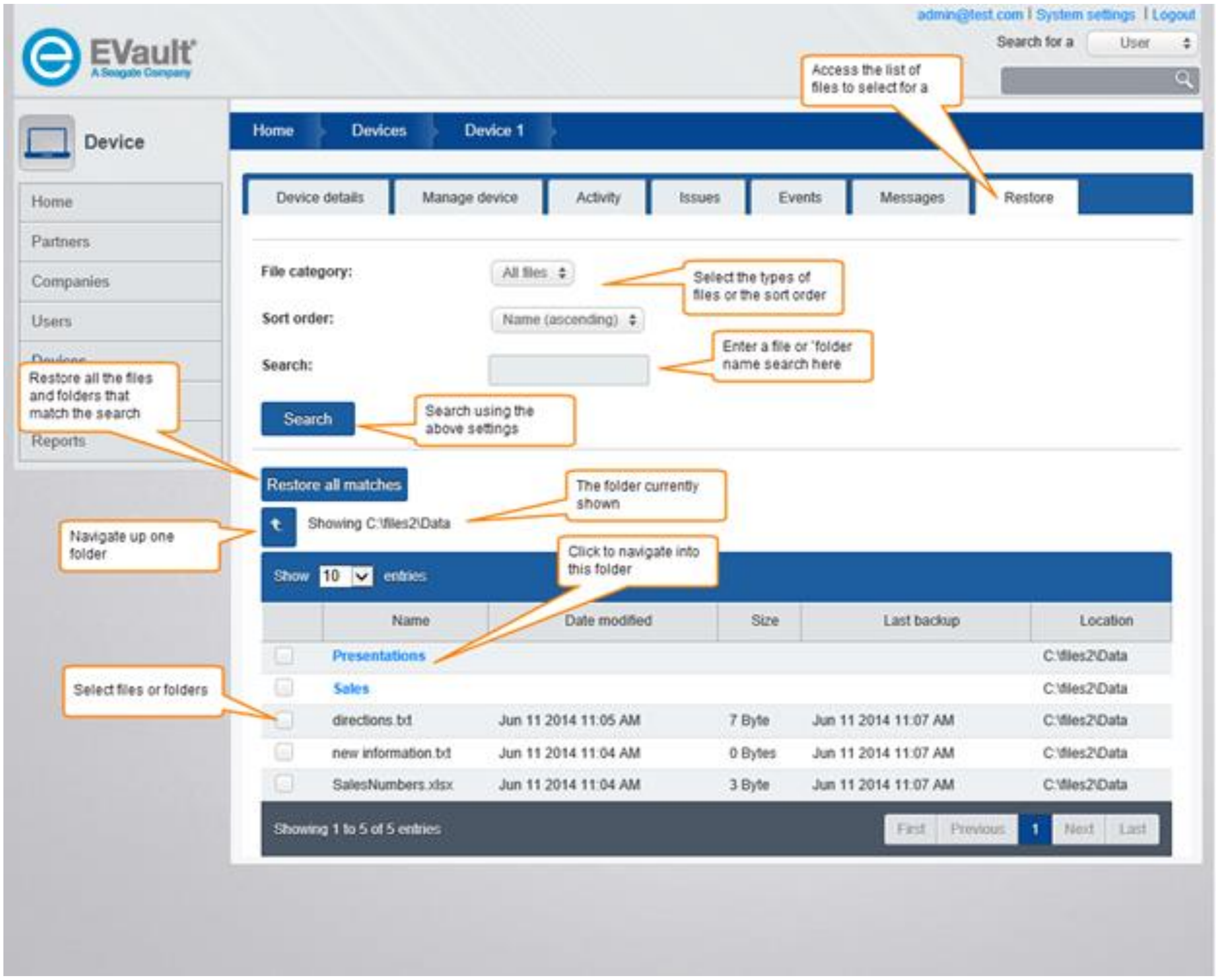
The policy set on a device controls how protection is configured for that device. Each device can have the policy specified directly, but normally you will want to have devices pick up the policy automatically based on the user or group they are under.

To set the device to get the policy automatically, select the top entry in the policy set list when you create or edit the device. This entry will start with “Inherit policy from” and will then list the entity that actually defines the default policy, as well as the name of the policy which is currently the default. For example, it could say “Inherit policy from Admin Company – ‘Enterprise Self Managed’”. In this case, the device has the default policy from the company. To change the default for a company, user group or user, edit the entity and change the Default policy set. In each of these cases you can choose either a specific policy set, or choose the top “inherit policy” option to set back to the default.

If you have sufficient permissions, you can click on the policy on the details page for the device, user, user group or company to see the definition of the policy and edit it. Any changes made will apply to all device using the policy so be careful when making changes. Details of the policy items and available values are in *Policy Management Guide*. Policies can be set on either partners or companies and there is a tab on the details page for each of these where the available policies can be found.

5.4 Administrative restore

A company administrator can restore data from a device using the Restore tab on the device page. You may want to do this to assist a user who is unfamiliar with performing restores using the client application or who doesn’t have access to their machine at this time.



Access the list of files to select for a

File category: All files

Select the types of files or the sort order

Sort order: Name (ascending)

Search:

Enter a file or 'folder name search here

Search using the above settings

Restore all the files and folders that match the search

The folder currently shown

Showing C:\files2\Data

Navigate up one folder

Click to navigate into this folder

Show 10 entries

Select files or folders

	Name	Date modified	Size	Last backup	Location
□	Presentations				C:\files2\Data
□	Sales				C:\files2\Data
□	directions.txt	Jun 11 2014 11:05 AM	7 Byte	Jun 11 2014 11:07 AM	C:\files2\Data
□	new information.txt	Jun 11 2014 11:04 AM	0 Bytes	Jun 11 2014 11:07 AM	C:\files2\Data
□	SalesNumbers.xlsx	Jun 11 2014 11:04 AM	3 Byte	Jun 11 2014 11:07 AM	C:\files2\Data

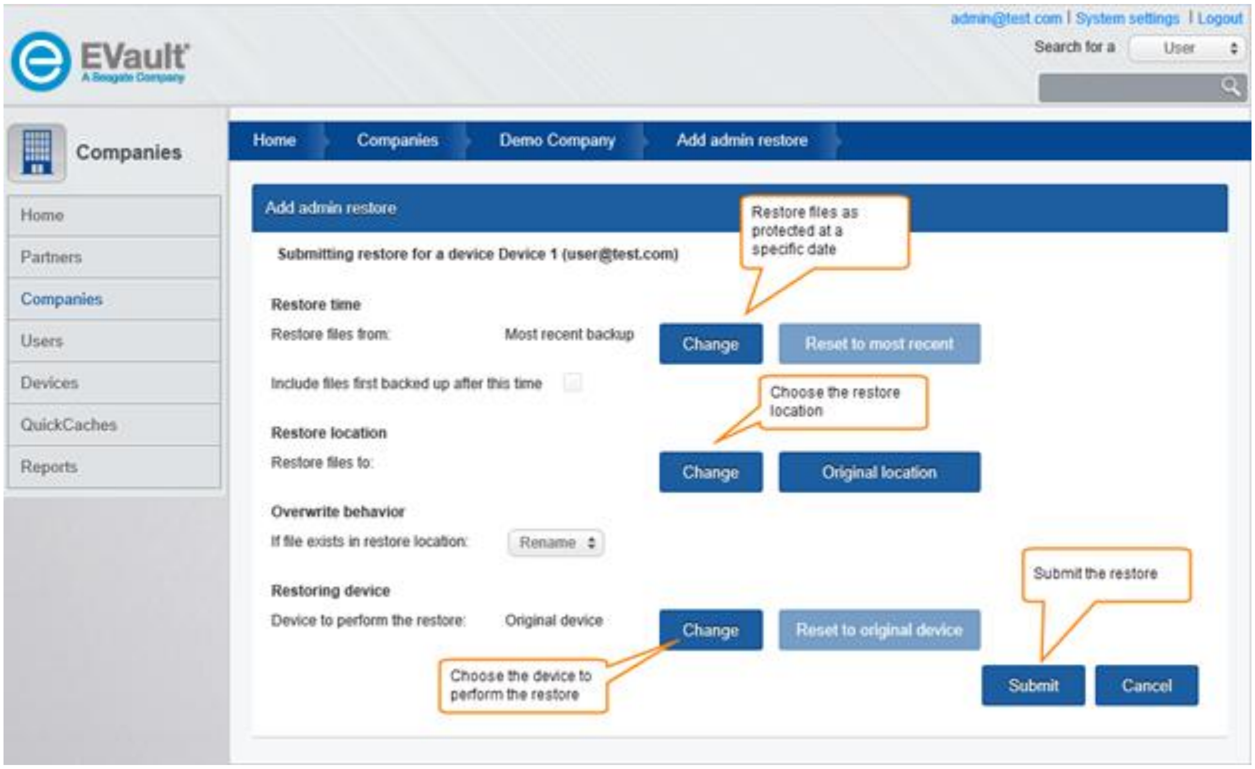
Showing 1 to 5 of 5 entries

Figure 11 Administrative Restore

To select files to be restored:

1. Navigate to the device details page
2. Click the Restore tab
3. If you know where the files to be restored are located, you can click the drive or folder locations in the list to find them.
4. If you know part of the name of the files you can enter it in the Search text box and click Search. You can also restrict to some file types using the File category list, or change the sort order.
5. The list will show up to 100 matches.
6. If you found a few specific items you want to restore you can check the checkbox on some files or folders and then click Restore selection.
7. If you don't want to select anything specific then you can click "Restore all matches" to restore all files or folders that match your current search and location. Use this option if there are more than 100 items found and you don't have more specific criteria to select.

After selecting the files to be restored you will be on the Add admin restore page, with the default settings of restoring the most recent files back to the original device. To start the restore you need to at least select the location for the files to be restored to.



Add admin restore

Submitting restore for a device Device 1 (user@test.com)

Restore time

Restore files from: Most recent backup

Include files first backed up after this time □

Restore location

Restore files to:

Overwrite behavior

If file exists in restore location: Rename

Restoring device

Device to perform the restore: Original device

Restore files as protected at a specific date

Choose the restore location

Choose the device to perform the restore

Submit the restore

Figure 12 Add admin restore

To restore files back to the location where they were protected from:

1. In the Restore location area, click the Original location button
2. By default the restored files will be renamed if a file of the same name already exists. Use the list in the Overwrite behavior area to change this to either Overwrite the existing file, or to Skip restoring that file if a file with the same name exists.

To select a different restore location:

1. In the Restore location area, click the Change button
2. A popup dialog will be shown for Change restore location
3. Enter a path for the files such as C:\Restore. This is on the machine which will do the restore, so for a Mac you would use a location such as /Volumes/Macintosh HD/Data.
4. Clicking the buttons for tokens will place a token in the path that will be automatically during the restore, such as {DeviceName} for the name of the device being restored, or {DateTime} for the time the restore is started.
5. Click Save changes when you have the path that you want to use.
6. By default the restored files will be renamed if a file of the same name already exists in the restore location. Use the list in the Overwrite behavior area to change this to either Overwrite the existing file, or to Skip restoring that file if a file with the same name exists.

By default, the restore will be performed by the same device that backed up the data. This may be a different computer if the device has been reactivated, such as if the user replaced their computer. Click Submit to accept this default.

If you are performing the restore for a user who doesn’t have access to their computer, perhaps because it has been lost or stolen, you will need to choose a different device to perform the restore. You may want to use your own computer. If you do this, the files will be restored to your machine and you can then get them to the user via email (if they are small enough) or another way such as placing them on a network share.

To select a different restore device:

1. In the Restoring device area, click the Change button.
2. A popup dialog will be shown for Change restoring device.
3. Search for the device you wish to use by typing in the Search box.
4. Note that all devices in your company will be available, including ones that are not yet activated. This allows you to select a device that has been created for a user’s new computer before they have installed, and the restore will start once the device is activated.
5. Select the radio button at the start of the line for the device you wish to use and click Select device to proceed.

If you change your mind, click “Reset to original device” to send the restore to the device that protected the data.

After clicking Submit, you will see the Admin restores tab on the company with a list of the restores and links to the device the data came from (device name) and the device doing the restore (restoring device). Click the Restoring device link, if present, to see the activity page for that device to check the restore status. Click the Cancel link to cancel a restore either before it starts or while it is restoring. Note that it can take some time for the device to start the restore, or to cancel after it has started, so the restore may actually complete even if you click cancel.

6 QuickCaches

A QuickCache can be installed within company network to provide faster protection for devices while allowing the bandwidth used for protection to be managed. Devices can be configured to look for a QuickCache and send their backup data to that location rather than directly to the vault, if they can connect to the QuickCache. Uploading to a QuickCache will be faster since it is on the local network rather than the internet. The QuickCache will then upload the data from all devices to the vault. The bandwidth used by the QuickCache is configured with peak and off-peak limits so it uploads most of the data overnight or on weekends. Devices will also use data from the QuickCache to restore which can speed up restores as much of the data will be already available locally.

To configure a device to use a QuickCache:

1. Go to the device details page.
2. Click Edit device details.
3. Choose the appropriate QuickCache from the list “QuickCache this device can use:”.
4. Click Save changes.

To check if a device is using the QuickCache:

1. Go to the device details page.
2. Click the Activity tab.
3. Look at the bottom of the status section.
4. The QuickCache message could be:
    a. Device is not using a QuickCache – for devices that either don’t have a QuickCache assigned or have not been able to connect to that QuickCache.
    b. Using QuickCache *name* – this indicates that the last time the device uploaded status it was connected to the QuickCache. The name will be linked to the QuickCache details page.
    c. Last QuickCache used was *name* at *time* – indicating that the device is not currently connected to the QuickCache but was at the given time. The device may have roamed to a different location, or may no longer be assigned to the QuickCache.

To see which devices are assigned to a QuickCache, download the list of devices as either Excel or csv. The assigned QuickCache will be included in the list.

To view the QuickCache status:

1. Navigate to the QuickCache details page – use the list from the QuickCaches menu or click on the QuickCache name from the device details or activity page.
2. The QuickCache activity page will be shown (as long as the QuickCache has been activated).
3. Current activity shows current rates of upload and download of data as well as the current free space on the QuickCache.

4. Queue state shows information about the data that is on the QuickCache and waiting to be uploaded to the vault.
5. For any of the data shown, click on the Graph button to see historical information about that data in the graph below. The data can be shown hourly for the last 7 days or daily for the last 30 days or one year. Because the graph shows hourly or daily averages, it may not show the same numbers as seen for the current values above the graph.

Expected behavior for the QuickCache is different during device deployment and afterwards.

During initial deployment of protection to devices to the site the QuickCache will normally build up a queue that will take a day or two or longer to upload to the vault. The Pending upload graph will show this – normally the pending data will increase during the day as devices upload and the QuickCache is only uploading slowly, then decrease overnight as the QuickCache uploads at the faster off-peak rate. As most devices complete uploading the QuickCache will show a decreasing queue until it empties. This may take a few days or longer depending on the amount of data and bandwidth availability.

After devices have been first protected the amount of data needing to be uploaded is generally small so the QuickCache will not be very active. If a lot of data is generated or changed at the location then the queue may build up during the day but should normally empty overnight. If it is not getting to empty overnight or at least by the weekend, it is possible that the allowed bandwidth usage from the location is too low. Consider allowing additional bandwidth usage so that devices will be fully protected in the vault in a timely manner to minimize impact if the QuickCache fails.

7 Reports

The Reports list provides users the ability to create and view detailed and customized reports.

To view an existing report:

1. From the home page menu, click Reports. The list of available reports appears.
2. If there are no reports, see the steps below to create a report.
3. Click the report name in the list.
4. If this is a time based report, the report will show the totals for the given day or days, with the date shown on the left.
5. If this is an organizational report, the report will show totals for each partner or company, depending on your level of access, and the report definition. The first column will be a link enabling you to drill down into the organization.
6. Click the link next to Alternative view to switch between date based and organization based.
7. Some of the data may be shown as links which will take you to a list of the data behind the number. For example, the count of Total backups for a day will take you to a list of backups for that day.
8. To export the report data as either Excel or csv format, click Download list then choose the desired format.
9. To modify the report, click Edit report definition.

To create a custom report:

1. From the home page menu, click “Reports”. The list of Reports appears.
2. Click the Add new report button at the top of the list.
3. Enter the report name in the “Report Name:” field.
4. If desired, select “Stretch report to full width of screen” next to the “Report Layout:” box.
5. Select who can view the report from the “Report Visibility:” menu.
   The options for this menu are:
   a) Personal report (default – the report will only be available to you)
   b) Shared report (only available for system administrators, makes the report visible to everyone, though each person will only see data they have access to)
6. Select the report type option from the “Report Type” menu.
   The options for this menu are:
   a) Time based report (default report type – shows the report by date)
   b) Organizational breakdown report – shows the report by partner/company/group
   c) Device details report – lists all devices
   d) User details report – lists all users
7. When selecting a time-based report, select the report date option from the “Report Dates:” menu.
   The options for this menu are:
   a) Last day (default report date)

b) Last 3 days
c) Last 7 days
d) Last 30 days
e) Last month
f) Scaling summary (Refers to displaying report information within date ranges, such as: Today, Yesterday, 2-7 days, 7-30 days, 30+ days, and so on.)

8. Select the desired Organization option from the “Organization:” menu.
   Normally the default of Depends on user’s roles is appropriate as it will include all the data the user is allowed to see, but you can also choose a specific organization.
9. Select “Policy Sets To Include:” to include all policy sets. The default for this is already selected. Deselect this box if only certain policy sets are desired.
10. Select the desired data points from the “Available Data Points:” menu.
    The options for this menu are:
    a) Last backup job – counts the devices which last backed up on a given day, similar to the pie chart on the home page
    b) Last restore job – counts the devices which last restored data on a given day
    c) Last vault erase job – counts the devices which last erased data on a given day
    d) All backup jobs – shows count or transferred data for all backup jobs
    e) All restore jobs – shows count or transferred data for all restore jobs
    f) All vault erase jobs – shows count for all vault erase jobs
    g) All jobs – shows count or transferred data for all jobs
    h) Devices created – number of devices created during the report time period
    i) Devices activated – number of devices activated during the report time period
    j) Devices reset – number of devices reset during the report time period
    k) Devices data deleted – number of devices told to delete data during the report time period
    l) Devices suspended – number of devices suspended during the report time period
    m) Total device state changes – number of devices that changed state (activated, were reset, reactivated etc.) during the report time period
    n) Active devices – devices activate at the given time
    o) Created devices (not activated) – devices that have been created but not yet activated at the given time
    p) Subscribed devices – devices able to be protected at the given time
    q) Suspended devices – devices that were suspended at the given time
    r) Reset devices – device that were in the reset state at the given time
    s) Unsubscribed Devices – devices unable to be protected at the given time
    t) Devices – all devices
    u) Users – all users
    v) User Groups – all user groups
    w) Companies – all companies
    x) Partners – all partners

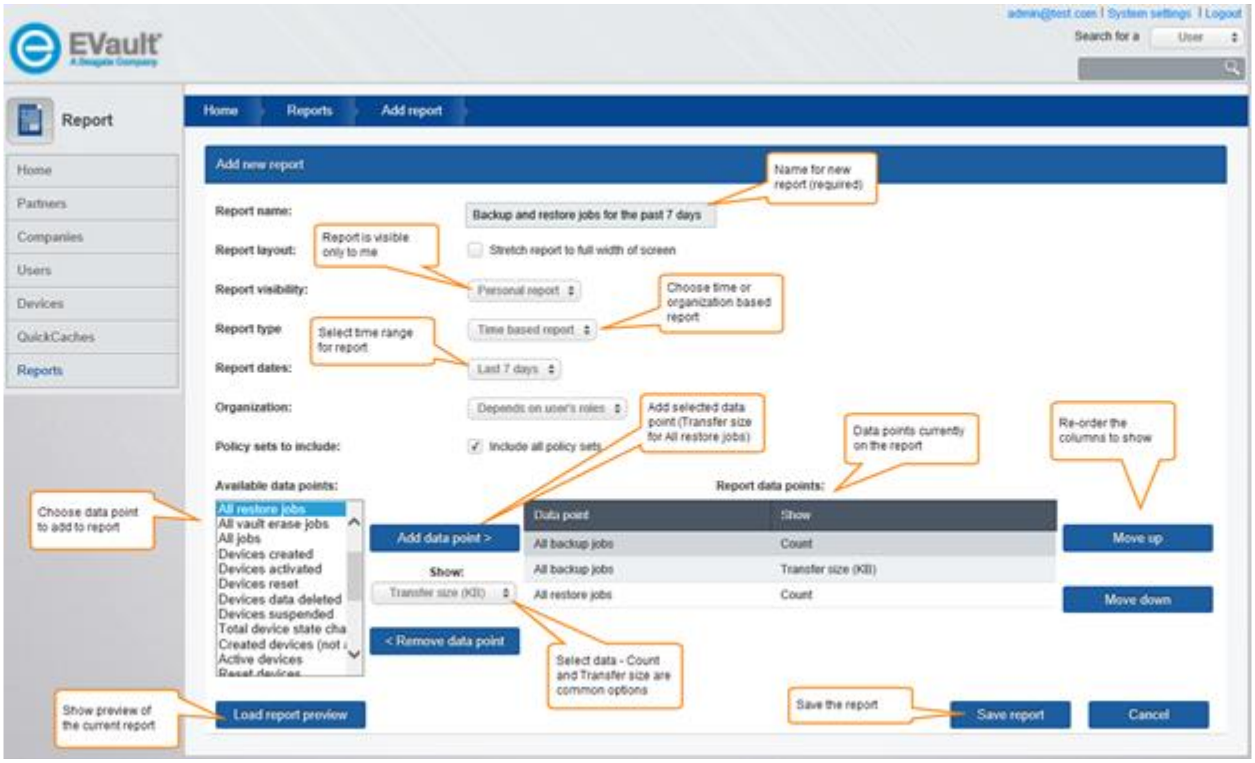
11. Select the type of data desired from the “Show:” menu. The default data is Count for the number of items, and the other options in this menu will vary depending on the data point selected. For example, for All backup jobs you can select transfer size, for Active devices you can include the usage or quota totals as well
12. Click “Add data point >” to add the selected data point to the report.
13. Click “Move up” or “Move down” to reorder the selected data points.
14. Click “Load report preview” to view the report prior to saving.
15. Click “Save report” to save the report.

7.1 An example custom report

This section describes the step-by-step instructions to create a report of total backups and restores for 7 days showing the number and transfer size. This is an example of one report that you can create by clicking the Reports link from the home page.

To add the sample report:

1. From the home page menu, click “Reports”. The Reports list appears.
2. Click the Add new report button at the top of the list
3. Enter “Backup and restore jobs for the past 7 days” in the “Report name:” field.
4. Select “Time based report” from the from the “Report Type” menu.
5. Select “Last 7 days” from the “Report Dates:” menu.
6. Select “All backup jobs” from the “Available data points:” menu.
7. Select “Count” from the “Show:” menu.
8. Click “Add data point >” to add this selection to the report.
9. Select “Transfer size” from the “Show:” menu.
10. Click “Add data point >” to add this selection to the report.
11. Select “All restore jobs” from the “Available data points:” menu.
12. Select “Count” from the “Show:” menu.
13. Click “Add data point >” to add this selection to the report.
14. Select “Transfer size” from the “Show:” menu.
15. Click “Add data point >” to add this selection to the report.
16. Click “Save report”



Add new report

Report name: Backup and restore jobs for the past 7 days

Report layout: □ Stretch report to full width of screen

Report visibility: Personal report

Report type: Time based report

Report dates: Last 7 days

Organization: Depends on user's roles

Policy sets to include: ☑ Include all policy sets

Available data points:

- All restore jobs
- All vault erase jobs
- All jobs
- Devices created
- Devices activated
- Devices reset
- Devices data deleted
- Devices suspended
- Total device state cha
- Created devices (not a
- Active devices
- Reset devices

Show: Transfer size (KB)

Report data points:

Data point	Show
All backup jobs	Count
All backup jobs	Transfer size (KB)
All restore jobs	Count

Name for new report (required)

Report is visible only to me

Choose time or organization based report

Select time range for report

Add selected data point (Transfer size for All restore jobs)

Data points currently on the report

Re-order the columns to show

Choose data point to add to report

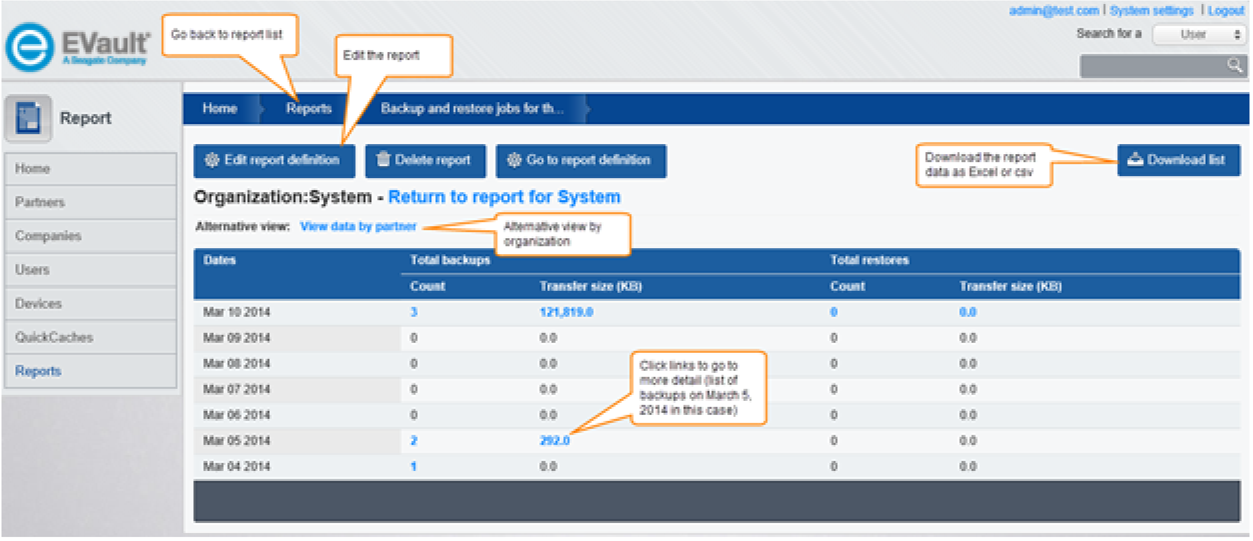
Select data - Count and Transfer size are common options

Show preview of the current report

Save the report

Figure 13 Adding report of all backup and restore jobs in the past 7 days

17. The report appears in the Reports list.
18. Click the “Backup and restore jobs for the past 7 days” report in the list of available reports.



Go back to report list

Edit the report

Download the report data as Excel or csv

Organization:System - Return to report for System

Alternative view: View data by partner

Alternative view by organization

Dates	Total backups		Total restores	
	Count	Transfer size (KB)	Count	Transfer size (KB)
Mar 10 2014	3	121,819.0	0	0.0
Mar 09 2014	0	0.0	0	0.0
Mar 08 2014	0	0.0	0	0.0
Mar 07 2014	0	0.0	0	0.0
Mar 06 2014	0	0.0	0	0.0
Mar 05 2014	2	292.0	0	0.0
Mar 04 2014	1	0.0	0	0.0

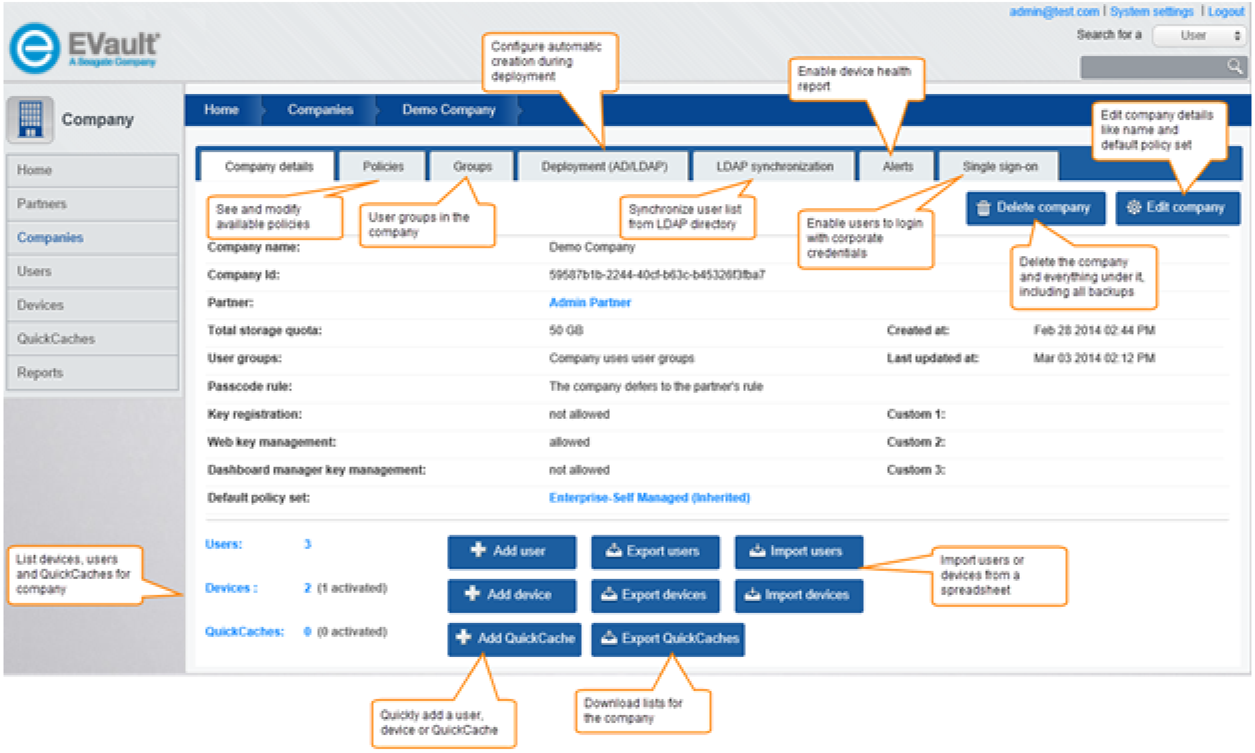
Click links to go to more detail (list of backups on March 5, 2014 in this case)

Figure 14 Sample custom report

19. Click “View data by partner” next to “Alternative view:” to provide a view of the report with a list of data with the totals for the week by Partner. Click on the partner name to drill in to see the totals for each company in that partner.
20. Click “Download list” to download the report into either an Excel spreadsheet or .csv file.

8 Company

The company page enables you to manage the company, including how devices within the company are deployed and protected.



Company name: Demo Company

Company Id: 59587b1b-2244-40cf-b63c-b45326f3fba7

Partner: Admin Partner

Total storage quota: 50 GB

User groups: Company uses user groups

Passcode rule: The company defers to the partner's rule

Key registration: not allowed

Web key management: allowed

Dashboard manager key management: not allowed

Default policy set: Enterprise-Self Managed (Inherited)

Created at: Feb 28 2014 02:44 PM

Last updated at: Mar 03 2014 02:12 PM

Custom 1:

Custom 2:

Custom 3:

Users: 3

Devices : 2 (1 activated)

QuickCaches: 0 (0 activated)

Configure automatic creation during deployment

Enable device health report

Edit company details like name and default policy set

See and modify available policies

User groups in the company

Synchronize user list from LDAP directory

Enable users to login with corporate credentials

Delete the company and everything under it, including all backups

List devices, users and QuickCaches for company

Import users or devices from a spreadsheet

Quickly add a user, device or QuickCache

Download lists for the company

Figure 15 Company details

On the company details page you can see the total number of users, devices and QuickCaches within the company. Click the number to see the list of these items.

The Add buttons here for user, device and Quickcache are here for convenience and will take you to the same Add page as the Add button on the top of any of these lists. The company will be autoamtically filled in. Similarly the Export buttons are the same as the Download list buttons on the lists, automatically restricted to this company.

The other tabs on the Company page are mostly used during intitial deployment of protection within your company and not used regularly.

- Policies – here the set of policies used to configure protection for devices can be seen and modified. See the *Policy Management Guide* for more information.
- Deployment (AD/LDAP) provides access to company activation codes which can be used in conjunction with automated deployment of the client application to endpoints. See the document Automating client deployment for details.

- LDAP synchronization can be used to keep the list of users in the vault aligned with the list of users in a company Active Directory. This can be useful to apply different policies to different groups based on groups or properties in Active Directory. See the document LDAP Synchronization.
- Alerts – enables the device health report alert to be turned on for this company and to specify the email addresses to receive the alerts, see 8.1 Alerts.
- Single sign-on allows users to log on to the web retreive site (as well as the dashboard) using their corporate credentials rather than needing a separate user name and password for the vault. See the document Single Sign-On Configuration.

8.1 Alerts

The vault can be configured to send email alerts with details of devices that are not properly protected. Devices show up on this report for a variety of reasons. Most common is that they haven't completed a backup in the last week. The alert can be configured to be sent for all devices in the vault, or for a partner or company.

To configure the alert:

1. Navigate to the company, partner or the system settings page.
2. Click the Alerts tab.
3. If alerts have already been configured, click "Edit alert settings" to make changes, or click "Enable alert".
4. In the popup enter the email addresses for the people to receive the alert. You can enter multiple addresses by separating with ;
5. Select the approximate time to send the report, and on which days. You can choose a day of the week or every day.

9 Advanced topics

These topics may be applicable depending on your deployment.

9.1 Login alternatives

The Login section above covers the basic case of using a user email address and password to log in to the system. There are some other options, particularly when the vault has been set up to enable single sign on with corporate directories. The document Single Sign-On Configuration has more information on setting this up.

The first page you see may ask for just the email address.

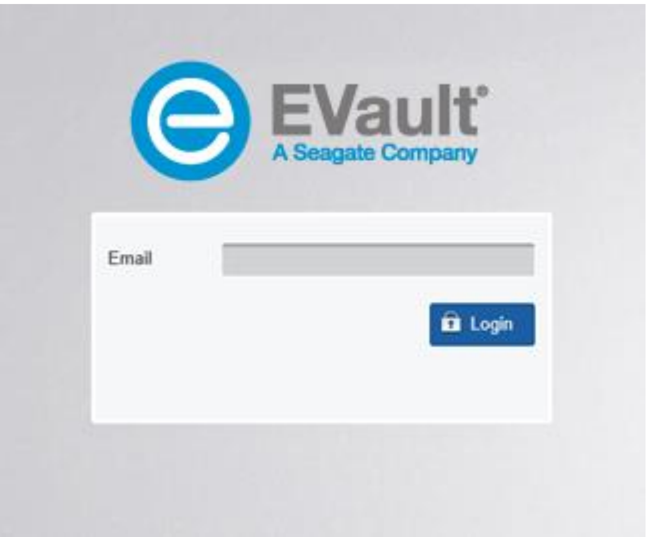
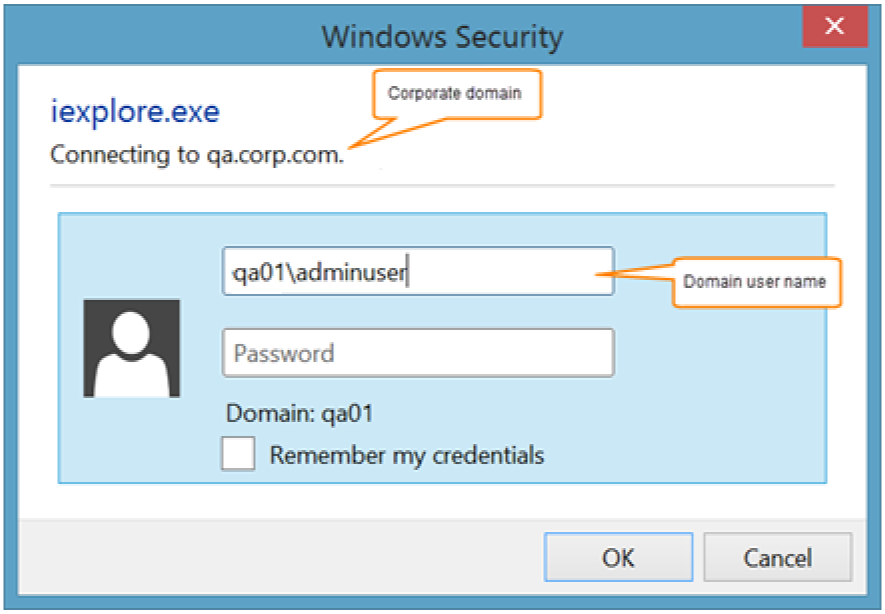


Figure 16 Login email address

If you see this page, the vault needs to know more about who you are before it can ask you for your credentials. Enter your email address and click Login. This will identify you to the system. If you log in using this same computer in the future it should already know who you are using a cookie and you won't need to enter this unless you delete the cookie. If the page displays an Invalid email error, then you have not entered an email address for a user in the vault.

After you enter your email address and click login, if your user account has a password associated with it, you will see the Email and Password login screen covering in Login.

If your company and user have been set up to use single sign on from your corporate directory, you will instead see a popup asking you to log in to your domain, similar to one of these. Note that this displays your corporate domain.



Connecting to qa.corp.com.

Corporate domain

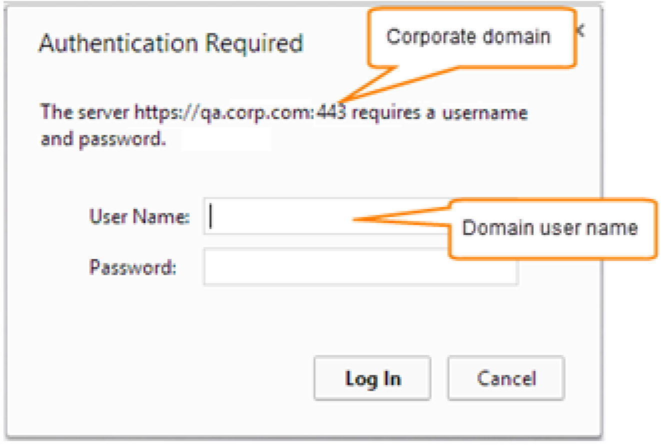
qa01\adminuser

Domain user name

Domain: qa01

□ Remember my credentials

Figure 17 Corporate domain credentials dialog



Corporate domain

The server https://qa.corp.com:443 requires a username and password.

User Name:

Domain user name

Password:

Figure 18 Corporate domain credentials dialog

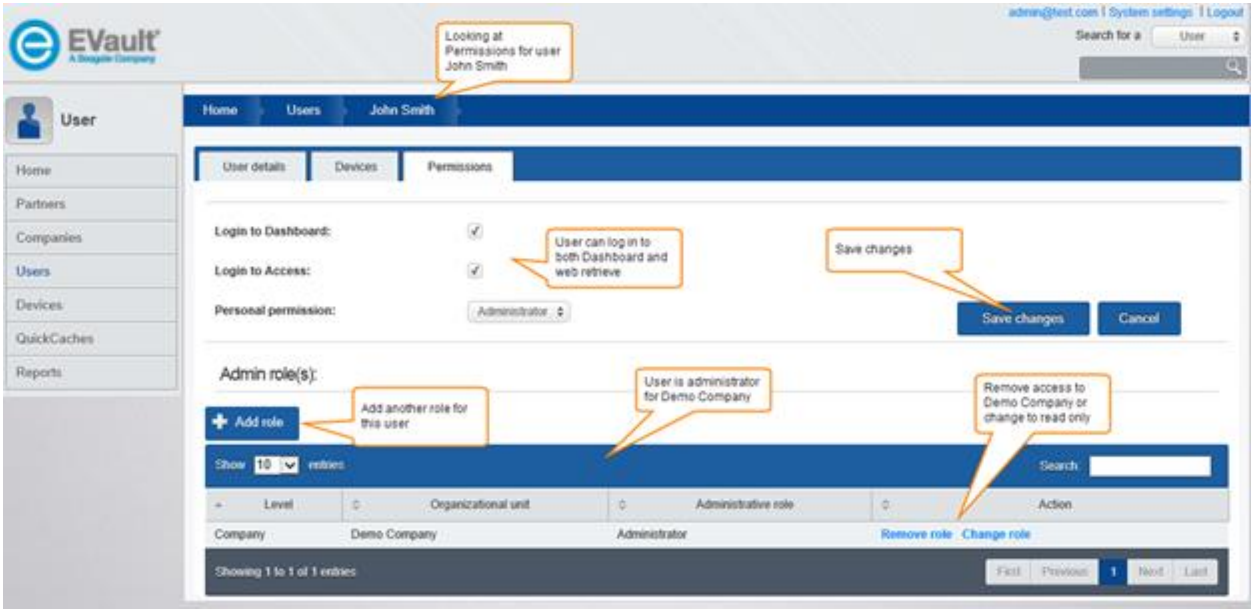
These are asking for your organization credentials. This type of login means that you use the same user name and password as you usually use for logging on to your corporate network. Your user name in this case may be different to the email address you entered into the vault dashboard page. Depending on your corporate directory you may need to use an email address, or a domain user name such as qa01\adminuser. Contact your administrator if you are not sure what to use.

9.2 Changing permissions

When you create a user you can give them read only or admin access to their company, or permission to use web retrieve to get files from their backups. To make changes to this after the user is created use the Permissions tab on the user details page. You will only be able to give users permissions which you already have, so you may not see all the options described below such as system access.

To change a user's permissions:

1. From the user details page click the Permissions tab.
2. To allow a user to log in to the Access site to retrieve files from their device backups, check the Login to Access box.
3. To allow a user to log in to the Dashboard to administer devices, check the Login to Dashboard box.
4. To change what a user can do with their own devices, change the Personal permission setting. If they can only login to the Access site, Retrieve only will be the only available option as other options require them to log in to the dashboard.
5. If the user can log in to the dashboard, then the Admin role(s) section allows you to change what they can do in the dashboard. If you have only just checked the box to allow dashboard login, you need to click the Save changes button so that it will show the Admin role(s) section.



Login to Dashboard: ✓

Login to Access: ✓

Personal permission: Administrator

Admin role(s):

Level	Organizational unit	Administrative role	Action
Company	Demo Company	Administrator	Remove role Change role

Showing 1 to 1 of 1 entries

Looking at Permissions for user John Smith

User can log in to both Dashboard and web retrieve

Save changes

Add another role for this user

User is administrator for Demo Company

Remove access to Demo Company or change to read only

Figure 19 Change a user's permissions

To manage administrative roles:

1. To add a role, click the Add role button.
2. A dialog will appear that allows you to give the user either admin or read-only access to their user group, company, partner or the whole system. Read permission allows them to see the information, admin permission will let them make changes.
3. Click OK to save the role
4. To remove a role, click "Remove role" and confirm.

5. To change their permission on an entity from read only to admin or back, click “Change role” and select the new role then OK to save.
6. If you want to give a user permission to a different entity – a different user group or company for example
    a. Click the Advanced button.
    b. Select the type of entity in the list (Partner, Company, User group)
    c. Enter some or all of the name in the box and click search
    d. Select the appropriate entity in the list – use the search box on the top right of the popup to refine the list as needed
    e. Click the Select button at the bottom once you have selected the item you wanted.
    f. Select the role and click the Add role button to save.

9.3 Deleting

Partners, companies, groups, users and devices can all be deleted. Once deleted they cannot be recovered. Everything under the item you delete will also be deleted. For example, deleting a partner will delete all companies, groups, users and devices under that partner.

If a device is deleted, then all of the backups for that device will be deleted as well. They will not be able to be recovered. Be careful not to confuse “Delete device” with “Delete data from device”. “Delete device” will remove all information about the device and will remove the backups that have been done for that device. “Delete data from device” retains all the backups and only sends a command down to the computer to delete the protected files from the machine.

Be very careful when deleting partners, companies, groups or users as all devices they have will be deleted as well. This will mean that the backups from any of those devices will not be able to be restored any more. Do this delete only after you are sure none of the backed up data needs to be kept. For example, if a user is leaving the company, in most cases you don’t want to lose that data so you should first suspend and move their devices – see 9.4 Keeping backup data for old devices for more details

To delete a partner, company, group or user:

1. Navigate to the appropriate details page
2. Click the Delete button
3. Read the warning message. If you are sure you want to proceed with the delete, check the confirmation box and then click Ok.
4. Click the close (x) on the box if you do not want to proceed.

You can’t delete the currently logged in user, so you will see a message if your user is in the selected partner, company or group.

9.4 Keeping backup data for old devices

If you delete a device then you will lose all the backups associated with that device. This may not be desired, even though the user who had the computer has left the company and the hardware has been wiped and reassigned.

You should consider suspending the device rather than deleting. By suspending the device you will remove this device from health reports as well as prevent backups and restored (if the client software hasn’t already been uninstalled anyway).

You may also want to move the device to a different user. This will allow you to delete the original user for the device, as well as preventing them from using web retrieve to access files from the backups. You could move the device to your own user if you are now responsible for the data, or you could create a user for your operations or support team email address and move the device to that user.

9.5 Create a User Group

Not all companies are set up to have user groups. This can be enabled by editing the company details.

To create a user group:

1. Find the company either by searching or navigating from the Companies list.
2. Open the company details page by clicking on the company name.
3. Display the current list of groups for the company by clicking the Groups tab.
4. Click Add group to create a new group.
5. Enter the user group name.
6. Enter custom values as desired.
7. Click Add group.
8. You will be returned to the company details page showing the new group in the list.

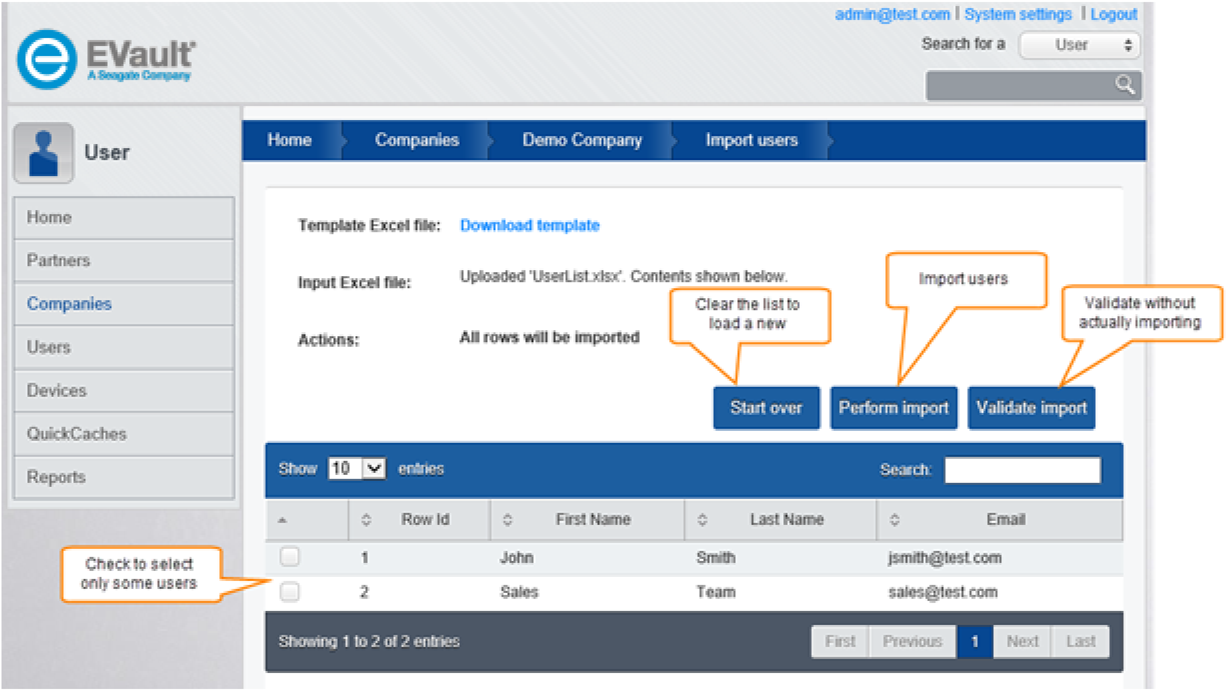
9.6 Bulk creation of users or devices

You can create users or devices in bulk by importing a spreadsheet into the dashboard. There are other options for automatically creating users and devices during deployment by pushing the installation out to computers. See the document Automating client deployment for more details on these options.

To import users using a spreadsheet:

1. Navigate to the company detail page.
2. Click the Import users button.
3. Click the Download template link to download a spreadsheet set up ready to be filled for importing.
4. In Excel, fill in the spreadsheet, focusing on the columns with shaded headings.
   a. You may need to click the Enable Editing button in Excel to allow editing.

   b. The first column is prefilled with a row number, leave that as it is.
   c. Fill in the first and last name for each user.
   d. Fill in the email address – this will be used as their login to the system, and for sending device activation emails if you create devices manually.
5. Save the spreadsheet.
6. Click the Choose File button on the Import users page, select the spreadsheet and click Open.
7. The spreadsheet will be loaded and the first rows shown.
8. If this was the wrong list, click Start over to return to the page ready to select a file.
9. If you want to import just a selection of users, check the appropriate checkboxes in the first column, otherwise all users will be imported.
10. You can click Validate import to check the entries first.
11. Click Perform import to create the users.
12. The result of either validation or importing will be shown at the top of the page, along with a link to download the results spreadsheet. This spreadsheet will be in the same format as the import spreadsheet, but the additional columns filled in. Look here for the details of any errors.



Template Excel file: Download template

Input Excel file: Uploaded 'UserList.xlsx'. Contents shown below.

Actions: All rows will be imported

	Row Id	First Name	Last Name	Email
□	1	John	Smith	jsmith@test.com
□	2	Sales	Team	sales@test.com

Showing 1 to 2 of 2 entries

Figure 20 Import users

To import devices using a spreadsheet:

1. Navigate to the company detail page.
2. Click the Import devices button.
3. Click the Download template link to download a spreadsheet set up ready to be filled for importing.

4. In Excel, fill in the spreadsheet, focusing on the columns with shaded headings.
    a. You may need to click the Enable Editing button in Excel to allow editing.
    b. The first column is prefilled with a row number, leave that as it is.
    c. Fill in the first, last name and email for each user. The user will be automatically created if they don't already exist. If the email address is already used then the name must match the existing name.
    d. If desired, fill in additional information. If not filled in they will defaulted in the same way as they would if you created the device manually.
5. Proceed as for user importing.
6. The results spreadsheet will include additional information such as the device id and the activation code.

9.7 Partner email templates

On the Partner details page the templates used for the automatic emails sent by the system can be edited. Click the Edit link next to the template to bring up the editing page.

The email will be seen by the user as coming from the address and name in the fields "Email from address" and "Email from display name". Select the default values for the vault by clearing the Override checkbox, or check it to supply the details here.

Enter the body of the email into the Template content field. This can be plain text or can be formatted using HTML if desired. If HTML is used, check the "Email content is HTML" checkbox to ensure it is sent properly.

Click "Send test email" to see a preview of the email. Enter your email address and click "Send email" to have the system send you a test copy of this mail.

Each mail template has some values that can be filled in by the system before sending. For example, the Passcode email uses @@Passcode@@ which will be replaced by the passcode generated for a user when the email is sent.

9.8 System settings

Next to the user link on the top right of the page you may see a System settings link (only if you have system administration rights to the whole vault).

Click this to see overall information about the vault license, including the Vault Id. Please include this information if you ever need to call Support. If needed, proxy and email settings can be changed from here as well.