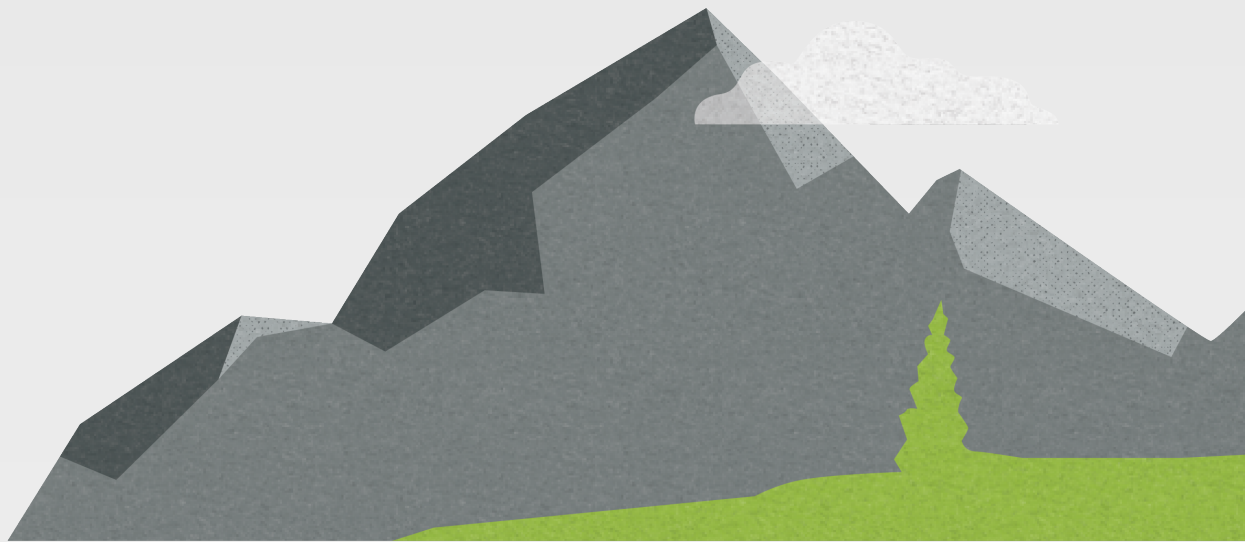


Administrator Guide



Notices

Carbonite Endpoint Administrator Guide, version 10.12, June 2023

© 2023 Open Text. All rights reserved.

One or more patents may cover this product. For more information, please visit <https://www.opentext.com/patents>.

If you need technical assistance, you can contact Customer Support. All basic configurations outlined in the online documentation will be supported through Customer Support. Assistance and support for advanced configurations may be referred to a Pre-Sales Systems Engineer or to Professional Services.

This documentation is subject to the following: (1) Change without notice; (2) Furnished pursuant to a license agreement; (3) Proprietary to the respective owner; (4) Not to be copied or reproduced unless authorized pursuant to the license agreement; (5) Provided without any expressed or implied warranties, (6) Does not entitle Licensee, End User or any other party to the source code or source code documentation of anything within the documentation or otherwise provided that is proprietary to OpenText; and (7) All Open Source and Third-Party Components (“OSTPC”) are provided “AS IS” pursuant to that OSTPC’s license agreement and disclaimers of warranties and liability.

Open Text and/or its affiliates and subsidiaries in the United States and/or other countries own/hold rights to certain trademarks, registered trademarks, and logos. Microsoft and Azure are registered trademarks of the Microsoft group of companies. macOS is a registered trademark of Apple Inc. Okta is a registered trademark of Okta, Inc.. All other trademarks are the property of their respective companies. For a complete list of trademarks registered to other companies, please visit that company’s website.

Contents

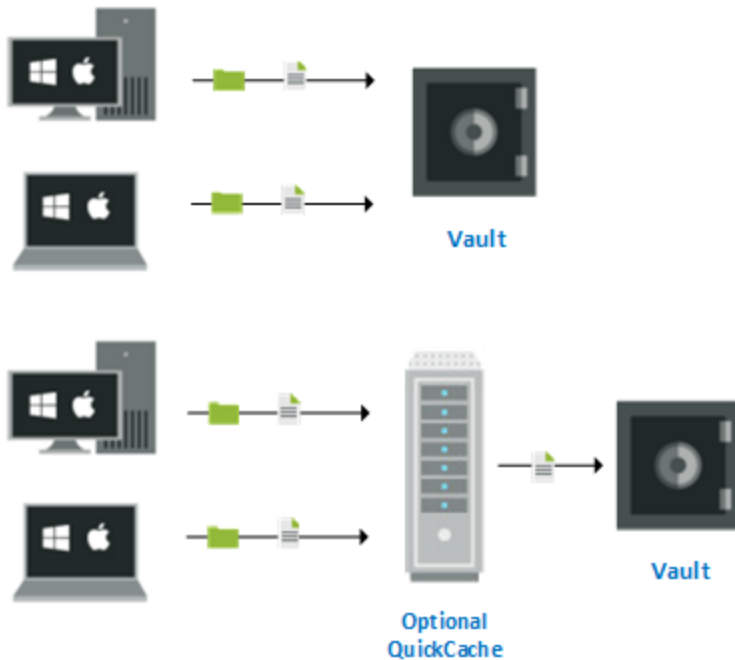
Chapter 1 Overview	6
Chapter 2 Endpoint Administration overview	7
Chapter 3 Get started	9
Log in to the dashboard	9
Log in to the dashboard with a temporary passcode	10
Log in to the dashboard with two-factor authentication	11
Log in to the dashboard with an emailed authentication code:	11
Log in to the dashboard with a code from a mobile authenticator:	12
Set up or remove a mobile authenticator	13
Set up a mobile authenticator:	13
Remove a mobile authenticator:	13
Reset your password	14
Access your user account	14
Navigate to a page	15
View records	15
Switch between vaults	16
Chapter 4 Dashboard	17
Chapter 5 View and manage your company	19
Administrative tasks on the Company details tab	20
Chapter 6 Create and manage policies	22
View available policies	23
Create a policy	23
General policy settings	24
Protected Files policy settings	25
Device Settings	27
Retention and Storage policy settings	30
Bandwidth Management settings	31
Edit an existing policy	33
Delete a policy	34
Manage backup rules for centrally managed policies	35
Default exclusions	38
Policy inheritance	40
Set the policy for a company	40
Set the policy for a group	41
Set the policy for a user	42
Set the policy for a device	43
Chapter 7 Manage deployment	45
Activation codes	46
View available activation codes	46
Add an activation code	48
Edit an activation code	49
Delete an activation code	50
Installation	50
Install on Windows or macOS using the installation wizard	51

Install on Windows using Msiexec	53
Install on Windows using group policy	56
Install on macOS using the installer app	57
Examples for LocalAutoConfig.xml	59
Activate on macOS	60
Chapter 8 Create and manage groups	63
View groups	63
View group details	64
Add a group	65
Add users to a group	66
Edit an existing group	66
Delete a group	67
Chapter 9 Create and manage users	69
View users	69
View user details	71
Administrative tasks on the User details tab	72
Add users	73
Add a single user	73
Import multiple users	76
Edit user settings	78
View devices for a user	79
Manage user permissions	80
Reset a user password	84
Delete a user	85
Enable a disabled user	85
Manage users with SCIM	85
Create an API user and SCIM access token in Carbonite Endpoint	86
Set up SCIM synchronization with Azure AD	87
Create an application in Azure AD	87
Add required attributes and map values to the SCIM application	88
Set up and test user provisioning	91
Set up SCIM synchronization with Okta	93
Add a SCIM application in Okta	93
Specify a time zone value	94
Add required attributes and map values to the SCIM application	94
Assign the SCIM application to users and test the integration	96
Manage users with LDAP	99
LDAP requirements	99
Sample configurations	100
Install the LDAP agent	102
Configure LDAP synchronization	104
Monitor and troubleshoot LDAP synchronization	108
Chapter 10 Create and manage devices	111
View devices	112
Add devices	114
Add a single device	114
Import multiple devices	116

View device details	118
Edit device settings	119
Manage a device	120
Put a device on legal hold	121
Suspend a device	122
Delete data from a device	123
Reset a device	124
Scan the user state of a device	125
Delete a device	126
View device activity	127
View device issues	129
View device events	129
View and/or delete device messages	130
Transfer a device to a different user	131
Restore files from a device	132
Locate a device	136
Chapter 11 Manage alerts	138
Chapter 12 View and manage admin restores	140
Chapter 13 Manage reports	142
View a list of available reports	142
Add a report	143
View a report	144
Delete a report	145
Chapter 14 Create and manage a QuickCache	146
View available QuickCaches	147
Add a QuickCache	148
View QuickCache activity	150
View QuickCache details	150
Edit QuickCache server settings	151
Manage the QuickCache bandwidth schedule	152
Manage a QuickCache	154
Assign a QuickCache to a device	156
Delete a QuickCache	156
Chapter 15 Single sign-on	158
View single sign-on details	158
Enable single sign-on for the first time	159
Edit single sign-on configuration	161
Disable single sign-on for one user	162
Disable single sign-on	163

Chapter 1 Overview

Carbonite Endpoint provides backup protection for desktop and laptop data. Desktops and laptops are known as devices or endpoints. All endpoints are backed up to a single location known as the vault. After the initial backup, subsequent backups are smaller and faster because only changes are backed up. An optional QuickCache can be used for faster backups in local environments. Backed up data can be restored from the vault to any device, any time, anywhere. The backup files are immutable and therefore forensically defensible.



To configure protection, an administrator or user selects the files to be backed up and how often the files are checked for changes (default every 15 minutes). Once protection is configured, the files are backed up and protected as long as the computer is running. Protection occurs locally if the computer is not connected to the local network or Internet. The changes are sent to the vault (or optional QuickCache) when the computer is back online. You do not need to take any additional action unless you want to change the protection configuration or restore files. If you want to restore files, they are downloaded from the vault to the original location or a new location. In the event your computer crashes or is stolen, you can restore all of your protected files to your replacement computer.

This document is for IT administrators whose responsibilities include configuring Carbonite Endpoint for their company. It includes tasks like configuring Carbonite Endpoint policies and deploying Carbonite Endpoint within your company. This document does not include topics for using the end-user client running on each device or topics for partners managing multiple companies.

Chapter 2 Endpoint Administration overview

As an Carbonite Endpoint administrator, you can create and manage policies, companies and users using the Carbonite Endpoint vault dashboard.

You must also determine how to deploy end-user client software on endpoint devices.

Create and manage policies

A policy configures the behavior of the end-user client, for example a policy determines which content to back up, the backup frequency, bandwidth management, and so on. Carbonite Endpoint supports two main types of policies:

- **Centrally-managed policy**—With a centrally-managed policy, the Carbonite Endpoint administrator configures the policy definitions.
- **Self-managed policy**—With a self-managed policy, end-users configure the policy definitions.

You can implement multiple policy types to meet the needs of different users or groups of users in your organization. A starter policy is included (with common default settings) for you to use or customize as needed.

See *Create and manage policies* on page 22 for more details and tasks available for policies.

Create and manage Carbonite Endpoint users

In order to protect an endpoint device, a user must be associated with the device. You can think of a user as an organizational tool for devices. You must decide which type of organizational user account strategy you want to implement.

- **Multiple user accounts**—With this strategy, you add multiple user accounts, and each account has one or more devices associated with that particular user. Use this strategy when devices are used by only one person.
- **Single user account**—With this strategy, you add a single user account, and many devices are assigned to that account. Use this strategy when devices are shared by many people.

You can implement a combination strategy to meet the needs of individually used devices and shared devices. You have multiple methods for adding user accounts, from manual entry to bulk uploads to automation using LDAP. In some cases, you can add the user when you deploy the end-user software on the devices.

See *Create and manage users* on page 69 for more details and tasks available for manually adding user accounts and bulk uploads to add user accounts. For automated methods, see end-user client deployment below.

End-user client deployment

Deployment is the process of obtaining an activation code and installing the end-user software on the endpoint devices. In some cases, the deployment process also includes adding a user account.

- **Activation codes**—The activation code option you select depends on what you want to happen when the client software is installed.

- **Add devices and add user accounts**—If you want to add both a device and a user in Carbonite Endpoint when the client software is installed and activated, use the **Enable full directory integration** option. (If the user already exists, only the device will be added.) This method requires the user to log in on the device when connected to the corporate network to capture the user information, and it requires a valid email address for the user in LDAP for the mail attribute.
- **Add devices for existing, individual user accounts**—If you want to add a device in Carbonite Endpoint for a user account that already exists, use the **Enable directory user integration** option. This method requires you to add individual user accounts in Carbonite Endpoint before the client software is installed.
- **Add devices for existing, single user account**—If you want to add a device in Carbonite Endpoint for a single user account that already exists, use the **Enable directory device integration** option. This method requires you to add a single user account in Carbonite Endpoint before the client software is installed. All devices will be associated with this single user account.
- **Do not add devices**—If you do not want to add any devices in Carbonite Endpoint when the client software is installed, do not select any option (or use the **Disable automatic creation** option if you selected another option and want to go back to no selection). This method requires you to add individual user accounts and devices in Carbonite Endpoint before the client software is installed.
- **Installation**—You can select the type of installation to perform.
 - **Remote deployment**—With this strategy, you can push the end-user client software to each device.
 - **Local installation**—With this strategy, the software is installed manually on each device.



Regardless of the method you choose, you should initially work with a small subset of devices until you are confident your deployment strategy is working. Once you are sure, you can implement the strategy for larger numbers of devices.

See *Manage deployment* on page 45 for more details and tasks for activation and installation.

Chapter 3 Get started

As an administrator, you can manage Carbonite Endpoint using the vault dashboard.

This section describes how to:

- *Log in to the dashboard* on page 9
- *Log in to the dashboard with a temporary passcode* on page 10
- *Log in to the dashboard with two-factor authentication* on page 11
- *Set up or remove a mobile authenticator* on page 13
- *Reset your password* on page 14
- *Access your user account* on page 14
- *Navigate to a page* on page 15
- *View records* on page 15
- *Switch between vaults* on page 16

Log in to the dashboard

As an administrator, you can manage Carbonite Endpoint using the vault dashboard. You can log in to the vault dashboard from a web browser.

1. Open a web browser and enter the vault dashboard URL in the address bar. The URL is <https://red-regioncode.mysecuredatavault.com>, where *regioncode* depends on your location. The following table shows available URLs.

Location	Region Code	URL
Asia-Pacific	APAC	https://red-apac.mysecuredatavault.com
Australia	AU	https://red-au.mysecuredatavault.com
Canada	CA	https://red-ca.mysecuredatavault.com
Europe, the Middle East, and Africa	EMEA	https://red-emea.mysecuredatavault.com
France	FR	https://red-fr.mysecuredatavault.com
India	IN	https://red-in.mysecuredatavault.com
United Kingdom	UK	https://red-uk.mysecuredatavault.com
United States	US US2	https://red-us.mysecuredatavault.com https://red-us2.mysecuredatavault.com



If users are permitted to log in to the web retrieval site (where they can restore their data without using their device), the URL is: *URL/access*. For example, if you are using <https://red-us.mysecuredatavault.com>, a user can access the web retrieval site by going to <https://red-us.mysecuredatavault.com/access>.

If a cookies preferences banner appears, you must accept or reject optional cookies before you can log in. You can only reject optional cookies; you cannot reject cookies that are necessary for Carbonite Endpoint. Your cookies are saved in the browser for a year, unless you clear your cookies or change your cookie preferences. To change your cookie preferences, click **Cookies Preferences** on the login page or, when logged in, click the arrow in the top, right corner of the page and click **Cookies Preferences** in the list.

2. On the login page, type your email address and password and click **Login**.

If you have forgotten your password, Carbonite Endpoint can send you a temporary passcode in an email message that can be used to access the portal and reset your password. For more information, see *Reset your password* on page 14.

3. If you are prompted for an authentication code, enter an authentication code from your email or third-party authenticator app. For more information, see *Log in to the dashboard with two-factor authentication* on page 11.

Log in to the dashboard with a temporary passcode

This procedure describes how to log in to the vault dashboard for the first time using a temporary passcode.

A temporary passcode is valid for 24 hours. If the passcode expires, open the login page and request a password reset by clicking **Forgot your password?** For more information, see *Reset your password* on page 14.

After you log in with a passcode you must enter a new password. Passwords must :

- Be at least eight characters in length.
- Contain at least one lower case and one upper case letter.
- Contain at least one number or symbol.

1. In your email client, open the email message from Carbonite Endpoint.
2. Copy or note the temporary passcode in the email message and then click the **Set up account** button.

The login page appears, with your email address and temporary passcode pre-populated in the fields.



If a cookies preferences banner appears, you must accept or reject optional cookies before you can log in. You can only reject optional cookies; you cannot reject cookies that are necessary for Carbonite Endpoint. Your cookies are saved in the browser for a year, unless you clear your cookies or change your cookie preferences. To change your



cookie preferences, click **Cookies Preferences** on the login page or, when logged in, click the arrow in the top, right corner of the page and click **Cookies Preferences** in the list.

3. Click **Login**.

The password reset dialog box appears.

4. Type a password in the **Enter new password** box.

5. Retype the password in the **Confirm new password** box.

6. Click **Change password**.

The Dashboard page appears when you are successfully logged in.

Log in to the dashboard with two-factor authentication

If two-factor authentication is enforced, you must enter an authentication code when you log in to the vault dashboard. Two-factor authentication (2FA), also called multi-factor authentication (MFA), provides increased security for your data.

You can receive an authentication code using two methods:

- **Email**—You can receive an authentication code in an email. This is the default 2FA method.
- **Mobile authenticator**—If you set up a mobile authenticator, you can obtain an authentication code from a third-party mobile authentication app, such as LastPass Authenticator, Microsoft Authenticator, or Google Authenticator, on your Android or iOS device. If you obtain codes from a mobile authenticator, you can also request authentication codes by email, if required. For more information, see *Set up or remove a mobile authenticator* on page 13.



Critical users should set up a mobile authenticator in case email is unavailable or inaccessible at some point.

If 2FA is not enforced, you can log in to the dashboard without entering an authentication code. See *Log in to the dashboard* on page 9. If your company uses SSO (single sign-on), 2FA is disabled and you log in using the specified SSO method.

Log in to the dashboard with an emailed authentication code:

1. Open a web browser and enter the vault dashboard URL in the address bar. The URL is `https://red-regioncode.mysecuredatavault.com`, where *regioncode* depends on your location. For a list of possible URLs, see *Log in to the dashboard* on page 9.



If a cookies preferences banner appears, you must accept or reject optional cookies before you can log in. You can only reject optional cookies; you cannot reject cookies that are necessary for Carbonite Endpoint. Your cookies are saved in the browser for a year, unless you clear your cookies or change your cookie preferences. To change your cookie preferences, click **Cookies Preferences** on the login page or, when logged in, click the arrow in the top, right corner of the page and click **Cookies Preferences** in the list.

2. On the login page, enter your email address and password and click **Login**.

A message prompts you for an authentication code from your email.

3. Check your email for a message with an authentication code.

Make sure that Carbonite Endpoint emails are not blocked by spam filters or any other email blocking technology.

Emailed authentication codes are valid for 5 minutes. If you do not enter the code within that time frame, you must request a new code.

4. Enter the authentication code, and click **Validate**.

A message asks if you want to set up a third-party authenticator. If you want to set up a mobile authenticator, click the link to open the **Security Settings** dialog box. For more information, see *Set up or remove a mobile authenticator* on page 13. If you do not want to set up a mobile authenticator, click the link to go to the home page.

Log in to the dashboard with a code from a mobile authenticator:

1. Open a web browser and enter the vault dashboard URL in the address bar. The URL is <https://red-regioncode.mysecuredatavault.com>, where *regioncode* depends on your location. For a list of possible URLs, see *Log in to the dashboard* on page 9.



If a cookies preferences banner appears, you must accept or reject optional cookies before you can log in. You can only reject optional cookies; you cannot reject cookies that are necessary for Carbonite Endpoint. Your cookies are saved in the browser for a year, unless you clear your cookies or change your cookie preferences. To change your cookie preferences, click **Cookies Preferences** on the login page or, when logged in, click the arrow in the top, right corner of the page and click **Cookies Preferences** in the list.

2. On the login page, enter your email address and password and click **Login**.

A message prompts you for an authentication code from your mobile authenticator app.

3. Check the authenticator app for an authentication code. Enter the authentication code, and click **Validate**.

If you cannot obtain an authentication code from the authenticator app, click **Send new authentication code by email** to log in using an emailed authentication code.

Set up or remove a mobile authenticator

When two-factor authentication (2FA) is enforced, you must enter an authentication code when you log in to the vault dashboard. See *Log in to the dashboard with two-factor authentication* on page 11.

By default, users receive authentication codes by email. If you set up a mobile authenticator, you can also obtain authentication codes from a third-party mobile authentication app on your Android or iOS device. You can set up a mobile authenticator if:

- 2FA is enforced for your company and enabled for your user.
- You have a mobile authentication app, such as LastPass Authenticator, Microsoft Authenticator, or Google Authenticator, installed on your Android or iOS device.



Critical users should set up a mobile authenticator in case email is unavailable or inaccessible at some point.

You can also remove a mobile authenticator from your account. If you remove a mobile authenticator, you must receive an authentication code by email when you next log in. System administrators can also remove users' mobile authenticators. For more information, see *View user details* on page 71.

Set up a mobile authenticator:

1. Do one of the following:
 - When logged in to the dashboard, click the arrow at the top right corner of the page, and click **Security Settings** in the menu.
 - Log in using an emailed authentication code. See *Log in to the dashboard with two-factor authentication* on page 11. A message asks whether you would like to configure a third-party authenticator on your account. Click **Yes, take me to my security settings**.
2. Using a mobile authentication app on your Android or iOS device, scan the QR code shown on the page.

If you cannot to scan the code, click the **Can't scan the QR code?** link to display the key and enter the key manually.
3. Check the authenticator app for an authentication code. Enter the code and click **Save**.

A message indicates that an authenticator was successfully registered to your account.
4. Click **Close**.

Remove a mobile authenticator:

1. When logged in to the dashboard, click the arrow at the top right of the page and click **Security Settings** in the menu.
2. Click **Remove authenticator**.
3. Check your email for a message with an authentication code.

Emailed authentication codes are valid for 5 minutes. If you do not enter the code within that time frame, you must request a new code.

4. Enter the authentication code in the Security Settings dialog box, and click **Remove**.

The mobile authenticator is removed. You must enter an emailed authentication code when you next log in to the dashboard.

5. Click **Close**.

Reset your password

If you have forgotten your password, Carbonite Endpoint can send you a temporary passcode in an email message that can be used to access the portal and reset your password.

Passwords must:

- Be at least eight characters in length.
 - Contain at least one lower case and one upper case letter.
 - Contain at least one number or symbol.
1. On the login page, click the **Forgot your password?** link. Type your email address that you use to log into the portal and click **Get a passcode**.
 2. Open the email sent by Carbonite. In the email message, copy the passcode or click the link to open the Login dialog box.
 3. Enter your email address and/or passcode and click **Login**.
The Change password dialog box appears.
 4. Type a new password in the **Enter new password** box.
 5. Retype the new password in the **Confirm new password** box.
 6. Click **Change password**.

The Carbonite Endpoint dashboard page appears.



Users with Administrator privileges can also change a user's password. For more information, see *Reset a user password* on page 84.

Access your user account

Use this procedure to access your user account. Your account contains your user details, devices associated with your account, and your permissions.

1. At the top of the portal page, click the "down" arrow and select the email address you used to log into the portal.

Your User page appears.

2. Do any of the following:

- To view your details, click the **User details** tab.
- To view devices associated with your user profile, click the **Devices** tab.
- To view your user permissions and role details, click the **Permissions** tab.

Navigate to a page

Use this procedure to navigate to a page in the vault dashboard.

1. Click the page name tab on the navigation bar on the left of the screen.
2. The name and icon of the page that you are viewing is highlighted. You can click the toggle switch to reduce the navigation bar so that it displays only the icons.

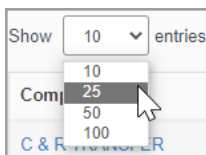
Breadcrumbs for the pages you are viewing also appear at the top of the screen.

View records

To make viewing information in the portal easier, Carbonite Endpoint displays records in a table format. Depending on the page, the table can also display hyperlinks that allow you to quickly navigate to a relevant page. For example, on the Company page under the Policies tab, policy names display as hyperlinks that open the Edit policy details page.

You can perform the following tasks in the records table:

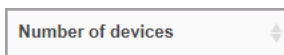
- Set the number of entries to display in the table - On a page with many records, click the **Show <number of> entries** list at the top of the table and click a number in the list. The table displays the selected number of entries.



- Search for an entry - Type text in the **Search** box and click the Search icon. The table displays only rows that contain the specified text. The search checks the entire table, not just the visible rows.



- Sort the table entries - Click any table column heading to display results in ascending or descending order (numerical or alphabetical).



- Use the table paging buttons - Click the paging buttons to scroll through the pages of the table or immediately move to the first, previous, next, or last page of the records.

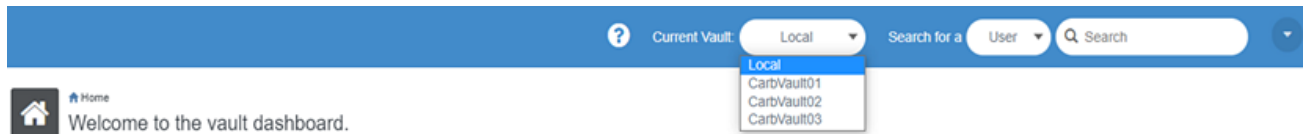


Switch between vaults

If you are an administrator with access to multiple vaults, and Carbonite has configured multi-vault access, you can switch between vaults in the dashboard without logging into each vault separately.

If you can switch between vaults, the **Current Vault** name appears at the top of the vault dashboard.

To switch to a different vault, click the **Current Vault** drop-down arrow and select a vault from the list. Information for the selected vault then appears in the dashboard. If you were viewing the company list, user list, device list, QuickCache list or report list in the first vault, you will be directed to the same information in the new vault. If you were viewing another page, you will be directed to the home page of the new vault.

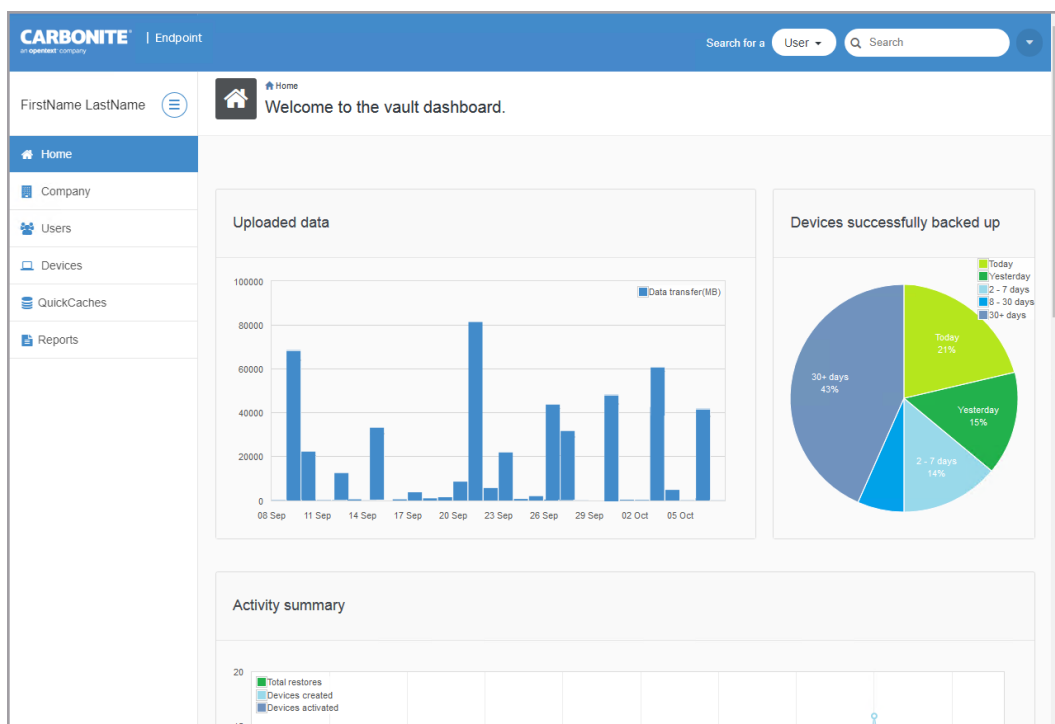


Chapter 4 Dashboard

The Carbonite Endpoint administration console is called the vault dashboard. The dashboard appears when you log in.

The Carbonite Endpoint dashboard is divided into three main sections.

- **Header**—A search tool and a link to your user account is displayed at the top of the window. You can limit your search term by device, user, or company. If you select your name under the down arrow in the far right corner, you will automatically go to your user account. This down arrow is also where you log out of the dashboard.
- **Navigation tabs on the left**—The navigation tabs on the left side take you to the main areas of the dashboard. You can click the toggle above the tabs to expand to the full tab names or collapse to the tab icon only.
 - **Home**—This page provides the highest level view of protected data and devices, and displays data and device usage information.



- **Uploaded data**—This chart displays the amount of data that was backed up each day.
- **Devices successfully backed up**—This chart displays the percentage of your devices that were backed up during the specified time period.
- **Activity summary**—This chart displays the devices that were added and activated as well as the total number of restores for each day.
- **Protected data**—This chart displays the total number of devices being protected and the total amount of data being protected.

- **Company**—This page allows you to perform administrative tasks for your company. See *View and manage your company* on page 19 for details.
- **Users**—This page provides a list of users and allows you to manage your users. See *Create and manage users* on page 69 for details.
- **Devices**—This page provides a list of devices and allows you to manage your devices. See *Create and manage devices* on page 111 for details.
- **QuickCache**—This page provides a list of QuickCaches and allows you to manage your QuickCaches. See *Create and manage a QuickCache* on page 146 for links where you can find details about installing and using a QuickCache.
- **Reports**—This page provides a list of reports and allows you to manage your reports. See *Manage reports* on page 142 for details.
- **Pages on the right**—The remaining part of the dashboard display is the various pages you interact with. These pages may have additional tabs within them, at the top of the page.

Some of the right side pages in the dashboard display different lists of data depending on how you navigated to the page. For example, if you click on the **Devices** tab on the left, the **Devices** page opens and displays all devices. However, if you click on the hyperlink in the **Number of devices** column on the **Users** page, the **Devices** page opens and displays only the devices assigned to the user you were viewing.

In addition to this dashboard, there is also the backup client software including an end-user interface, installed on each device, which may or may not be hidden to end-users. The end-user interface is not covered in this document.

Chapter 5 View and manage your company

On the Company page, you can view detailed information and perform administrative tasks for your company.

The Company page shows information on the following tabs:

- **Company details**—This tab shows information for a company, including the company name, ID and policy. The tab also shows the following settings for the company:
 - **Authentication.** This setting indicates how users log in to the vault dashboard or web retrieval site. The Authentication value can be:
 - **Default**—Indicates that users log in with an email address and password.
 - **SSO**—Indicates that users log in using single sign-on.
 - **2FA**—Indicates that users log in using a two-factor authentication method, either email authentication or a mobile authenticator app.
 - **Auto sync device/computer names.** This setting indicates whether the company's device names in Carbonite Endpoint are automatically synchronized with computer names on endpoint devices. When this feature is enabled, if the computer name of an endpoint device changes, the device name is automatically updated in Carbonite Endpoint. If the user already has a device with the new name, a space and number are added to the new device name in Carbonite Endpoint (e.g., *deviceName 2*).

On the Company details tab, you can access other administrative functions for the company. See *Administrative tasks on the Company details tab* on page 20.

- **Policies**—A policy configures the behavior of the end-user client, for example determining what content is backed up, backup frequency, bandwidth management, and so on. For more information, see *Create and manage policies* on page 22.
- **Groups**—Groups provide a way to associate multiple users. This provides the ability to perform tasks for the users in a group. For example, you can define a policy for a group and all users in the group will use that policy. See *Create and manage groups* on page 63 for details.
- **Deployment (AD/LDAP)**—Deployment is the process of getting an activation code and installing the end-user software on the devices. In some cases, the deployment process also includes adding a user account. See *Manage deployment* on page 45 for details on activation codes and installation.
- **LDAP synchronization**—If you are using Lightweight Directory Access Protocol (LDAP), you can manage Carbonite Endpoint users by synchronizing Carbonite Endpoint and LDAP. This will add and disable users based on their status in your LDAP company directory. See *Manage users with LDAP* on page 99 for details.
- **SCIM synchronization**—System for Cross-domain Identity Management (SCIM), you can manage Carbonite Endpoint users by synchronizing Carbonite Endpoint and SCIM. This will add and disable users based on their status in your SCIM company directory. See *Manage users with SCIM* on page 85 for details.
- **Alerts**—You can enable daily alerts (email notifications) to notify you when specific device and QuickCache criteria have been met. See *Manage alerts* on page 138 for details.

- **Single sign-on**—This tab is available only if you have worked with Carbonite Professional Services to configure it. See *Single sign-on* on page 158 for details.
- **Admin restores**—You can view the restores performed by an administrator. See *View and manage admin restores* on page 140 for details.

The screenshot shows the 'Company details' tab of a management interface. At the top, there is a navigation bar with tabs for 'Company details', 'Policies', 'Groups', 'Deployment', 'User synchronization', 'Alerts', and 'Admin restores'. Below the navigation bar, there are two buttons: 'Manage keys' and 'Edit company'. The main content area is divided into several sections:

- Company name:** CompanyName
- Company Id:** 1b2b345e-6789-0123-4f5e-67a890a1cc23
- Total storage quota:** 413540 GB
- User groups:** Company uses user groups
- Passcode rule:** Allow passcodes to be emailed to users
- Default policy set:** Base Policy
- Authentication:** 2FA
- Created at:** Nov 01 2018 10:57 AM
- Last updated at:** Jan 06 2021 10:33 AM
- Expiration Date:**
- Expiration State:** Active
- Custom 1:**
- Custom 2:**
- Custom 3:**

At the bottom, there are three rows of user-related data and actions:

- Users:** 80. Actions: + Add user, Export users, Import users.
- Devices:** 77 (15 activated). Actions: + Add device, Export devices, Import devices.
- QuickCaches:** 3 (0 activated). Actions: + Add QuickCache, Export QuickCaches.

Administrative tasks on the Company details tab

On the Company details tab, you can click the following buttons and hyperlinks to perform administrative tasks for the company you are viewing:

- **Manage keys**—A key server, or reset server, is an advanced function that allows you to store and control access to keys for device resets. You will only use this button if you are using your own key server and need to manage your keys.
- **Edit company**—Click this button to modify your company settings.
- **Default policy set**—Click this hyperlink to edit the policy details. See *Edit an existing policy* on page 33 for details.
- User-related buttons and hyperlinks:
 - **Users hyperlink or number**—Click the hyperlink or the number to go to the **Users** page. See *View users* on page 69 for details.
 - **Add user**—Click this button to add a new user. See *Add a single user* on page 73 for details.
 - **Export users**—Click this button to export a complete user list to your local computer. You can download a Microsoft Excel (.xlsx) file or a comma-delimited file (.csv). If you

download the Excel format, you must enable editing for any hyperlinks to the portal to be active.

- **Import users**—Click this button to import multiple users. See *Import multiple users* on page 76 for details.
- Device-related buttons and hyperlinks:
 - **Devices hyperlink or number**—Click the hyperlink or the number to go to the **Devices** page. See *View devices* on page 112 for details.
 - **Add device**—Click this button to add a new device. See *Add a single device* on page 114 for details.
 - **Export devices**—Click this button to export a complete device list to your local computer. You can download a Microsoft Excel (.xlsx) file or a comma-delimited file (.csv). If you download the Excel format, you must enable editing for any hyperlinks to the portal to be active.
 - **Import devices**—Click this button to import multiple devices. See *Import multiple devices* on page 116 for details.
- QuickCache-related buttons and hyperlinks:
 - **QuickCaches hyperlink or number**—Click the hyperlink or the number to go to the **QuickCaches** page. For more information, see *Create and manage a QuickCache* on page 146.
 - **Add QuickCache**—Click this button to add a new QuickCache. For more information, see *Add a QuickCache* on page 148.
 - **Export QuickCache**—Click this button to export a complete QuickCache list to your local computer. You can download a Microsoft Excel (.xlsx) file or a comma-delimited file (.csv). If you download the Excel format, you must enable editing for any hyperlinks to the portal to be active.

Chapter 6 Create and manage policies

A policy configures the behavior of the end-user client, for example a policy determines which content to back up, the backup frequency, bandwidth management, and so on. Carbonite Endpoint supports two main types of policies:

- **Centrally-managed policy**—With a centrally-managed policy, the Carbonite Endpoint administrator configures the policy definitions.
- **Self-managed policy**—With a self-managed policy, end-users configure the policy definitions.

You can implement multiple policy types to meet the needs of different users or groups of users in your organization. A starter policy is included (with common default settings) for you to use or customize as needed.

Think about the following key questions and situations when determining what type of policy to use.

- What is the size of your user-base? If you have a smaller number of end-users, you may want to use self-managed policies. If you have many end-users, you may be better off using centrally-managed policies.
- Where are your users located? If your users are geographically dispersed, each with their own bandwidth, you may not have bandwidth concerns for backing up files. If your users are all in the same location, you may need to have bandwidth policies in place to protect the available bandwidth.
- Who needs to define what should be backed up? If you are comfortable with users deciding what files to back up, you can use self-managed policies. If you must retain control over the files that are backed up, you will need to use centrally-managed policies.
- Does it matter if users know the software is there? If you want to hide the software, you must use centrally-managed policies (and remote deployment).
- Do you have separate groups that have different backup needs? For example, if one office location or department needs to have different protected files than another office location or department, you may want to have different centrally-managed policies for the groups or a combination of centrally-managed and self-managed policies. You should also consider if you have different groups of employees, such as executives, that have different legal needs. In that case, you may need different centrally-managed policies or a combination of centrally-managed and self-managed policies.
- Do you have a dedicated IT staff to administer the centrally-managed policies? If not, you may want to use self-managed policies.

For more information about working with policies, see:

- *View available policies* on page 23
- *Create a policy* on page 23
- *Edit an existing policy* on page 33
- *Delete a policy* on page 34

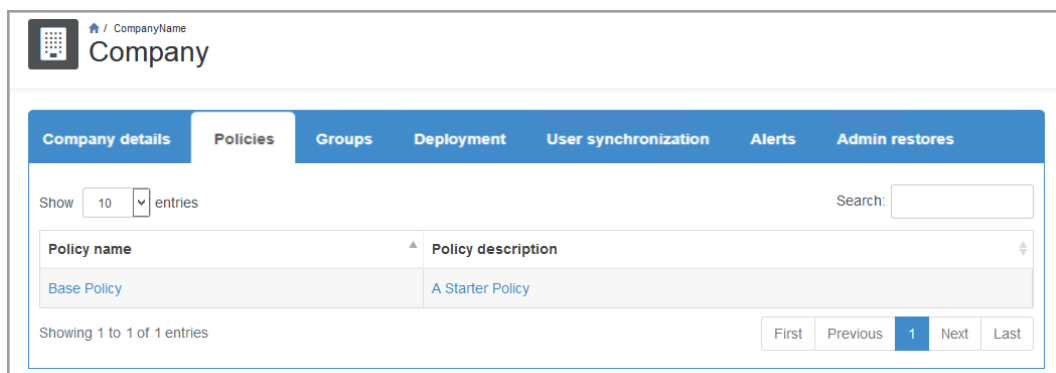
For more information about:

- Policy settings, see *General policy settings* on page 24, *Protected Files policy settings* on page 25, *Device Settings* on page 27, *Retention and Storage policy settings* on page 30 and *Bandwidth Management settings* on page 31.
- Files, folders, and files without an extension that are excluded from the backup, see *Default exclusions* on page 38.
- How policies are assigned and inherited, see *Policy inheritance* on page 40.

View available policies

Use this procedure to view your available policies.

- Go to the **Company** page and click the **Policies** tab. All companies start with the Base Policy which is a starter policy that you can use to add your own customized policies.



The following controls are available on the **Policies** tab.

- **Show Entries**—Specify the number of rows to be shown in the table on each page. Additional rows over the number you select are shown on additional pages and can be viewed by using the paging buttons at the bottom of the table.
- **Search**—Text entered in the box narrows the list displayed to only the rows that contain the search text. The search checks the entire table, not just the visible rows.
- **Sort**—You can sort the table by clicking on any column heading.
- **Table hyperlinks**—Click a policy name or the policy description to manage that policy. See *Edit an existing policy* on page 33 for details.
- **Table paging buttons**—The paging buttons at the bottom of the table allow you to move more quickly between pages. Each button jumps to that respective page of the table.

Create a policy

Use this procedure to create a policy.

To create a new policy, you start by making a copy of an existing policy.

1. Go to the **Company** page and click the **Policies** tab.
2. Locate in the table an existing policy you want to copy. See *View available policies* on page 23 for details on searching the table.

3. Click the policy name.
4. In the Edit policy details page, edit the following policy settings as required:
 - *General policy settings* on page 24
 - *Protected Files policy settings* on page 25
 - *Device Settings* on page 27
 - *Retention and Storage policy settings* on page 30
 - *Bandwidth Management settings* on page 31
5. When you are satisfied with the policy settings, select one of following options:
 - **Done**—Click this button if you have not made any changes to the policy settings. No new policy will be added.
 - **Save as**—Click this button if you have specified a different, unique policy name. One new policy will be added using the name you specified. If you have not changed the policy name, one new policy will be added by appending a number to the existing policy name.
 - **Save policy**—You will not be able to click this button unless you have made a policy setting change. If you have specified a different, unique policy name, one new policy will be added using the name you specified. If you have not changed the policy name, one new policy will be added by appending a number to the existing policy name.

If you selected either save option, click **Done** to return to the **Policies** tab, or click **Continue editing** to remain on the **Edit policy details** page.

General policy settings

When you create or edit a policy, you can specify the general policy settings. The general settings include the policy name and description, and the option to enable or disable the policy.



You may not have access to all of these settings if Carbonite has restricted your access.

In the Edit policy details page, specify the following general settings:

- **General**

The screenshot shows a form titled "General" with three sections:

- Policy name:** A text input field containing "Base Policy". Below the field is a small blue link that says "Show policy ID".
- Policy description:** A text input field containing "A Starter Policy".
- Policy status:** A toggle switch that is currently turned on, with the word "Enabled" displayed to its right.

- **Policy name**—Provide a name for the policy. If the name already exists and you select **Save as**, Carbonite appends a number to the policy name. The name cannot contain any of the following reserved characters.
 - less than <
 - greater than >
 - colon :
 - quotation marks or double quote "
 - forward slash /
 - backslash \
 - vertical bar or pipe |
 - question mark ?
 - asterisk *
- **Policy description**—Provide a description of the policy. The description cannot contain any of the reserved characters identified under policy name.
- **Policy status**—Specify whether you want to enable or disable this policy.

Protected Files policy settings

When you create or edit a policy, you can specify the type of file selection management to be used and configure the backup frequency and schedule.



The lock icon that displays to the right of some settings is a toggle you can turn on and off. The icon indicates whether end users can modify the policy setting in the client interface. When the icon displays as locked, end users cannot modify the setting. When the icon displays as unlocked, end users can modify the setting.

- **Protected Files**

Protected Files

File Selection Management ?

Backup frequency

Only back up during Backup Schedule

Backup schedule

Self managed by end users
 Centrally Managed by administrator

every 🔒

Disabled 🔒

Start time

↑

:

↓

End time

↑

:

↓

🔒

- **File Selection Management**—This setting identifies who defines the files that will be backed up.
 - **Self managed by end users**—Users define the backup rules.
 - **Centrally managed by administrator**—Administrators define the backup rules. When this option is selected, you must define the rules the policy will use to identify which files to include or exclude in the backup. See *Manage backup rules for centrally managed policies* on page 35 for details.
 - **End user can also add file selection rules**—Select this option if you want to give users the ability to add their own personal rules, in addition to the centrally-managed administrator defined rules.



Regardless of whether a policy is self-managed or centrally-managed, some files and folders (including files without an extension) are excluded, by default, from backups. See *Default exclusions* on page 38 for details.

If you are using a centrally-managed policy with or without allowing users to add file selection rules, you should have at least one rule defined.

- **Backup frequency**—Specify the amount of time between backups. Carbonite Endpoint scans for changes on this interval and backs up any changes, additions, or deletions. The lock icon is a toggle you can turn on and off. The icon indicates whether end users can modify the policy setting in the client interface. When the icon displays as locked, end

users cannot modify the setting. When the icon displays as unlocked, end users can modify the setting.

- **Only back up during Backup Schedule**—When enabled, a defined backup schedule controls when files are backed up, and files are backed up only within the defined schedule. When disabled, files are backed up at any time.

The lock icon is a toggle you can turn on and off. The icon indicates whether end users can modify the policy setting in the client interface. When the icon displays as locked, end users cannot modify the setting. When the icon displays as unlocked, end users can modify the setting.

- **Backup schedule**—When **Only back up during Backup Schedule** is enabled, you can configure the schedule when you want files to be backed up. This option is not used when **Only back up during Backup Schedule** is disabled. The toggle circle will be on the right and blue when enabled and on the left and gray when disabled.
 - **Start time**—Specify when you want the backup schedule to start. Files will be backed up between this time and the **End time**.
 - **End time**—Specify when you want the backup schedule to end. Files will be backed up between the **Start time** and this time.

The time is configured using your local machine time.

Device Settings

When you create or edit a policy, you can specify the device settings to be used. The device settings include optional advanced settings.

- **Device Settings**

The screenshot shows a 'Device Settings' panel with the following configuration:

Setting	Value
Track device location	Enabled
Remote Wipe	Quick Delete
Timed Remote Wipe	Disabled
End user self restore	Enabled

A link for 'Show advanced settings' is located at the bottom right of the panel.

- **Track device location**—When enabled, Carbonite Endpoint tracks the physical location of a device, and the location can be viewed on a map. When disabled, the location of the device is not tracked. This setting can be useful for locating lost or stolen devices. The toggle circle will be on the right and blue when enabled and on the left and gray when

disabled.

- **Remote Wipe**—Select which files can be deleted from the device (but not the backup) by the administrator.
 - **None**—No files can be deleted from the device.
 - **Quick Delete**—Files configured for backup can be deleted from the device. Files are not retained in the trash or recycle bin.
 - **Delete and Overwrite**—Files configured for backup can be deleted from the device. After they are deleted, the file location is overwritten multiple times. This option is more secure and makes recovery of the original files more difficult, however, the deletion process takes longer.
 - **Quick Delete with remove EFS keys**—For Windows devices, files configured for backup are deleted from the device. Also, the folder on the device containing the EFS encryption keys is deleted. After the encryption keys are deleted, all files encrypted with EFS will be inaccessible, even those that were not backed up with Carbonite Endpoint.
 - **Delete and Overwrite with remove EFS keys**—For Windows devices, files configured for backup are deleted from the device. After they are deleted, the file location is overwritten multiple times and the folder on the device containing the EFS encryption keys is also deleted. This option has the same benefits and caveats as above, in addition to making EFS files inaccessible.
- **Timed Remote Wipe**—The toggle circle will be on the right and blue when enabled and on the left and gray when disabled. When disabled, files will never be automatically deleted from a device. When enabled, files will be automatically deleted from a device (but not the backup) when the device has failed to connect to the vault or QuickCache within the time period specified. If you enable this option, you must confirm that you want to use this setting because it can lead to unintended data loss. Select **Devices will be wiped based on time configuration**, click **Enable Remote Wipe**, and specify the number of days. For example, if you set this option to 30 days, at the beginning of the 31st day, data on the device will be deleted as configured in **Remote Wipe**. Each time the device connects, the countdown will be reset for the time remote wipe.
- **End user self restore**—When enabled, users can perform file restores from the vault or QuickCache. When disabled, only administrators can restore files. The toggle circle will be on the right and blue when enabled and on the left and gray when disabled.
- **Advanced settings**—Click the link to show or hide advanced settings.
 - **Advanced File Deletion**
 - **End users can erase their data from vault**—When enabled, users can erase (delete) their backed up files from the vault and QuickCache. When disabled, users cannot erase their backed up files and the backed up files are maintained until a retention or storage policy overwrites the file or the device is deleted from the vault. The toggle circle will be on the right and blue when enabled and on the left and gray when disabled.
 - **User State Migration Tool**—Carbonite Endpoint uses Microsoft User State Migration Tool (USMT) to provide a process for replacing or refreshing Windows computers. The utility captures operating system settings, application settings, user accounts, and user files and migrates them to a new Windows installation. You must be familiar with using and configuring USMT. See <https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-topics> for

details on this utility.

- **Scheduled user scan backup**—When enabled, Carbonite Endpoint scans a Windows device for the latest settings, accounts, and files. The frequency of the scan is defined by the number of days specified. When disabled, scans must be run manually. The toggle circle will be on the right and blue when enabled and on the left and gray when disabled.



You can also perform manual scans as needed. See *Manage a device* on page 120 for details.

- **Location of the 32-bit USMT executable**—Specify the location of the 32-bit version of the utility. This file will be used on 32-bit Windows computers. The location must be accessible by the Windows devices. You do not need to specify the file name, just the location.
- **Location of the 64-bit USMT executable**—Specify the location of the 64-bit version of the utility. This file will be used on 64-bit Windows computers. The location must be accessible by the Windows devices. You do not need to specify the file name, just the location.
- **Parameters for ScanState executable**—Specify the options you want to use with ScanState. Generally, this is /config:filename.xml, however you should review <https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-scanstate-syntax> for details on the command syntax.
- **Abort ScanState execution**—Specify the length of time you want ScanState to run before it is automatically terminated. The minimum duration is one minute.
- **Location for custom configuration files**—Specify the location of your XML files for custom configurations. See <https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-include-files-and-settings> and <https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-exclude-files-and-settings> for details on custom files to include and how to exclude files and settings. You do not need to specify the file names, just the location.
- **After a restart, start USMT ScanState**—Specify the length of time to wait after a Windows computer has been restarted to initiate a scan. The minimum duration is one minute.
- **Parameters for LoadState executable**—Specify the options you want to use with LoadState. See <https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-loadstate-syntax> for details on the command syntax.
- **Abort LoadState execution**—Specify the length of time LoadState should run before it is automatically terminated. The minimum duration is one minute.

Retention and Storage policy settings

When you create or edit a policy, you can configure the retention and storage settings for files. The Retention and Storage settings include optional advanced settings.

- **Retention & Storage**

Retention & Storage

Versions
Minimum number of file versions to maintain

Unlimited
 Specified number of versions

at least versions

Keep older versions
Number of days of version history to be retained for individual files

Forever
 Specified length of time

at least days

Retain deleted files ?

Forever
 Specified length of time

for days

[Show advanced settings](#)

- **Versions**—Select the number of versions of an individual file to keep. Different file versions do not count against your total billable storage.
 - **Unlimited**—Select this option to keep all file versions. If you have specified a length of time for **Keep older versions**, that time will be disregarded because all versions are being kept.
 - **Specified number of versions**—Select this option to keep at least the number of versions specified. Versions outside of this minimum number will be deleted at the specified length of time for **Keep older versions**.
- **Keep older versions**—Select the number of days of version history to retain.
 - **Forever**—Select this option to keep all days of version history. If you have specified a number of versions for **Versions**, that number will be disregarded because all days of version history are being retained.
 - **Specified length of time**—Select this option to keep at least the number of days of version history specified. Versions outside of this minimum date will be removed at the specified number of versions for **Versions**.

- **Retain deleted files**—Select the number of days to keep files that have been deleted from a device or files that were once backed up but are no longer being backed up because of a change to file selection rules. Deleted files that are retained count against your total billable storage.
 - **Forever**—Select this option to keep all deleted files within the backup even if they are deleted from the device or are no longer included in the backup policy.



Keep in mind your consumed capacity will always grow and will not be subject to any retain policy, even if you delete users and their devices.

- **Specified length of time**—Specify the number of days to keep all deleted (or no longer backed up) files. After the specified number of days, the files will be deleted. The maximum number of days is 180. If you need more than that, you must select **Forever**.



The default value for retaining deleted files changed in Carbonite Endpoint version 10.6. If you were using the default value previously (forever or 180 days depending on your version), your new default value will be 90 days. Files beyond the 90 day value will be deleted from the backup. If you customized the value, your setting will be retained.

- **Advanced settings**—Click the link to show or hide the following advanced settings.
 - **Unlimited storage quota**—When enabled, there is no size limit to how much data can be backed up. When disabled, the size specified will be used as a quota. The toggle circle will be on the right and blue when enabled and on the left and gray when disabled. The minimum storage quota is 5 GB. You can use the quota for reporting and to monitor usage to avoid overage fees.
 - **Prevent backups when storage quota is reached**—When enabled, backups will stop when the specified quota limit has been reached. When disabled, devices can exceed the specified quota limit.
 - **Largest file size to include in backups**—Specify the maximum file size, up to 70 GB, that will be backed up. Files larger than the size you specify will not be backed up.

Bandwidth Management settings

When you create or edit a policy, you can configure the bandwidth usage for devices. You can configure devices to use reduced bandwidth, or all available bandwidth. You can also configure the upload and download rates and specify proxy settings. The Bandwidth Management settings include optional advanced settings.



The lock icon that displays to the right of some settings is a toggle you can turn on and off. The icon indicates whether end users can modify the policy setting in the client interface. When the icon displays as locked, end users cannot modify the setting. When the icon displays as unlocked, end users can modify the setting.

- **Bandwidth Management**

Bandwidth Management

Device bandwidth configuration ? Reduced Bandwidth Use all available bandwidth 🔒

Maximum upload rate when reduced ? KB / second

Maximum download rate KB / second

Proxy settings Specify proxy settings

[Show advanced settings](#)

- **Device bandwidth configuration**—Select the amount of bandwidth a device will use to back up files. This setting applies to upload speeds only. Select one of the following options:
 - **Reduced Bandwidth**—This option limits the amount of bandwidth used for backing up files to the amount specified in the **Maximum upload rate when reduced** setting.
 - **Use all available bandwidth**—This option allows Carbonite Endpoint to use unlimited bandwidth for backing up files.
- **Maximum upload rate when reduced**—Specify the amount of bandwidth a device will use to back up files when the **Device bandwidth configuration** setting is set to **Reduced Bandwidth**.
- **Maximum download rate**—Specify the bandwidth limit a device will use when downloading during restores and when using the User State Migration Tool.
- **Specify Proxy settings**—Select one of the following options to specify proxy server settings.
 - **No Proxy**—Select this option if you want remove an existing proxy server or prevent users from using a proxy server.
 - **Automatically detect settings**—Select this option to have the system automatically detect the proxy server.
 - **Specify the server and port**—Select this option to specify the proxy server to use. You need to specify credentials, the server, and the port number.

- **Use automatic configuration script**—Select this option to use a configuration script on your proxy server to automatically configure the device. You need to specify credentials and the IP address of the proxy server.
- **Advanced settings**—Click the link to show or hide the following advanced settings.
 - **Do not upload when device is attached to a mobile broadband network**—When enabled, Windows devices attached to a mobile network will not back up files. When disabled, Windows devices attached to a mobile network will back up files. The toggle circle will be on the right and blue when enabled and on the left and gray when disabled.
 - **Mobile Network Names**—This setting allows you to identify specific WiFi networks as a mobile network, which can be used to identify tethering or hotspot scenarios. WiFi networks identified as mobile networks will be limited by the **Do not upload when device is attached to a mobile broadband network** setting. Enter each network name on a separate line.

Edit an existing policy

Use this procedure to edit an existing policy.

1. Go to the **Company** page and click the **Policies** tab.
2. On the **Policies** tab, locate in the table the policy you want to edit. See *View available policies* on page 23 for details on searching the table.
3. Once you have located the policy you want to edit, click on the policy's name.
4. On the **Edit policy details** page, modify any of the following policy settings:
 - *General policy settings* on page 24
 - *Protected Files policy settings* on page 25
 - *Device Settings* on page 27
 - *Retention and Storage policy settings* on page 30
 - *Bandwidth Management settings* on page 31

The screenshot shows the 'Edit policy details' interface. At the top, there's a breadcrumb 'Company / Base Policy' and a 'Company' logo. Below that is a blue header 'Edit policy details'. Action buttons include 'Delete policy', 'Cancel changes', 'Save as', and 'Save policy'. The 'General' section contains:

- Policy name:** 'Base Policy' with a 'Show policy ID' link below it.
- Policy description:** 'A Starter Policy'.
- Policy status:** A toggle switch set to 'Enabled'.

 The 'Protected Files' section has a 'File Selection Management' link and two radio buttons: 'Self managed by end users' (selected) and 'Centrally Managed by administrator'.

5. If you have changed the policy name to a unique name, you can click **Save as** or **Save policy**. If you have not changed the policy name, **Save as** will create a new policy by appending a number to the existing policy name, and **Save policy** replaces the existing policy reusing the existing policy name.



You cannot change the policy name to a name that already exists.

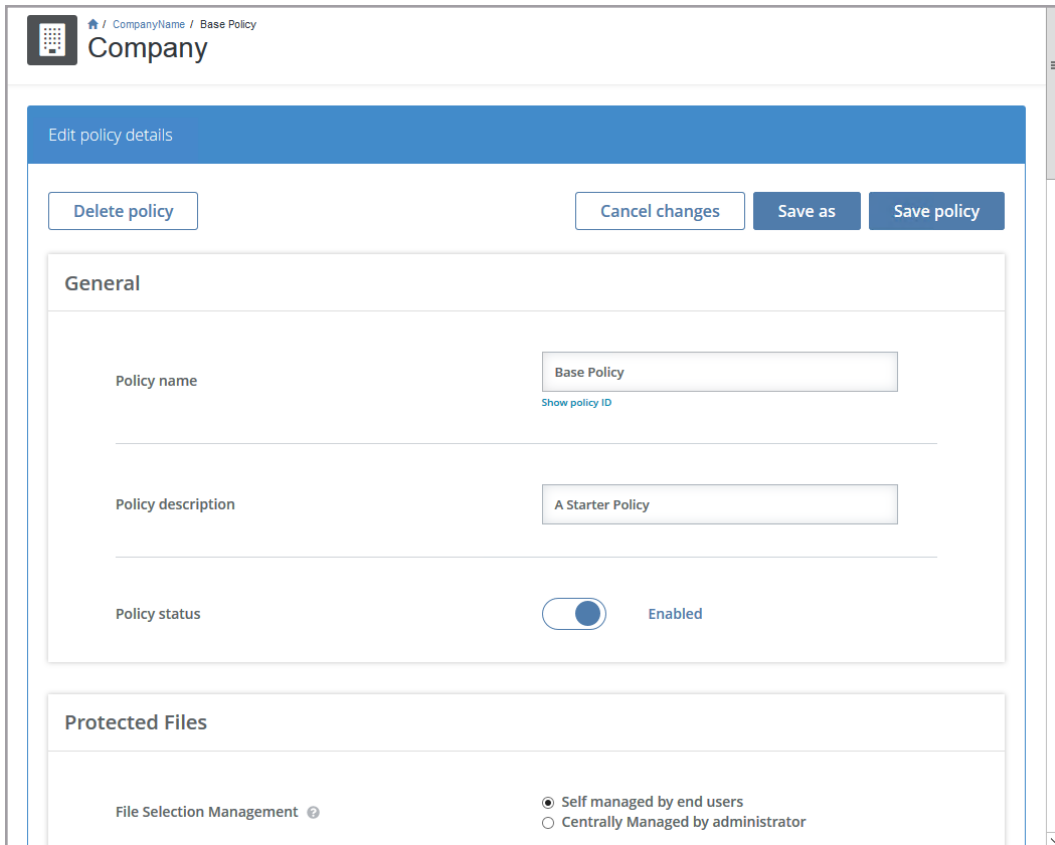
Changes to policies will be applied to devices using the policy as soon as the changes are saved and the device is connected.

6. Click **Done** to return to the **Policies** tab, or click **Continue editing** to remain on the **Edit policy details** page.

Delete a policy

If you no longer need a policy, you can delete it.

1. Go to the **Company** page and click the **Policies** tab.
2. On the **Policies** tab, locate in the table the policy you want to delete. See *View available policies* on page 23 for details on searching the table.
3. Once you have located the policy you want to delete, click on the policy's name.
4. On the **Edit policy details** page, click **Delete policy**.



5. Click **Delete policy** on the confirmation box.

Manage backup rules for centrally managed policies

If you want administrator control over which files do and do not get backed up (a centrally-managed policy), you must define rules in the policy to identify the files to include or exclude in the backup.

- Rules can be specified for volumes, folders, files, and file types.
- Wildcards can be used.
- All rules are recursive, meaning the rule is automatically applied to the subfolders of the specified path.
- A rule for a file takes precedence over a rule for All Files.
- In the case of multiple rules, files use the rule that is closest in the folder structure to them. In the following example, all files and folders under C:\Users will be backed up (the first rule). However, video files will be excluded from C:\Users and its subfolders (the second rule), except the videos located in C:\Users*\marketing and its subfolders will be included (the third rule).

RULE TYPE	FILE TYPE CATEGORY	LOCATION [▲]
Backup	All Files	C:\Users
Do not backup	Videos	C:\Users
Backup	Videos	C:\Users*\marketing

- Some files and folders (including files without an extension) are excluded, by default, from backups. See *Default exclusions* on page 38 for details.
- Do not specify the same rule in different ways. For example, do not create a rule for C:\Users*\MyDocuments and %MyDocuments%.

The following toolbar and table controls are available for the **File selection rules** section on the **Edit policy details** page.

Use the following procedure to view and/or edit the **File selection rules**.

1. Go to the **Company** page and click the **Policies** tab.
2. Locate the policy that contains the backup rules you want to view or modify. See *View available policies* on page 23 for details on searching the table.
3. Click on the policy's name.
4. Make sure **File Selection Management** is set to **Centrally Managed by administrator** to display the **File selection rules** section.

The screenshot shows the 'File Selection Management' section of a web interface. At the top, there are radio buttons for 'Self managed by end users' (unselected) and 'Centrally Managed by administrator' (selected). Below this is a checkbox for 'End user can also add file selection rules' which is unchecked. The main section is titled 'File selection rules' and contains a search filter box with the text 'Filter by... example: doc'. To the right of the filter are two buttons: 'Manage custom file types' and 'Add rule'. Below these is a table with the following columns: 'RULE TYPE', 'FILE TYPE CATEGORY', and 'LOCATION'. Each row in the table has a vertical ellipsis menu icon on the right side.

RULE TYPE [▲]	FILE TYPE CATEGORY [▲]	LOCATION
Backup	Email	%AllDrives%
Backup	All Files	%AllDrives%
Backup	Documents	%AllDrives%
Backup	All Files	/users/*/Library/Mail
Do not backup	Images	%AllDrives%
Do not backup	Audio	%AllDrives%
Do not backup	Videos	%AllDrives%

5. Edit the following settings as required.

- **Filter by**— Enter text to narrow the list to only rows that contain the filter text.
- **Manage custom file types**—Click this button to display a list of custom file types. These are specific files you want to include or exclude from the backup.
 - **Add custom file type**—Click this button to add a new custom file type.
 - **File type name**—Specify a name to identify this type of file.
 - **Copy from**—Select an existing file type to pre-populate the **File type extensions** field (optional).
 - **File type extensions**—Specify the file extensions for the files you want to include or exclude from the backup. Separate multiple extensions with a space.

Click **Save** once you have defined the new custom file type.

- **Edit**—Click this button to edit the file type definition. Use the same guidelines as outlined above when adding a custom file type. Click **Save** to save the changes.
- **Table row overflow menu**—Click **Delete** in the overflow menu of a table row to delete the file type definition. Confirm the deletion by clicking **Delete**.
- **Close**—Click this button to close the **Manage custom file type** dialog box.
- **Add rule**—Click this button to add a new file selection rule.
 - **Define type of rule**—Select the type of rule you want to add.
 - **Backup**—Select this option if you want the file types defined by this rule to be backed up.
 - **Do not backup**—Select this option if you do not want the file types defined by this rule to be backed up.
 - **Select a file type**—Select the type of file to be included in the rule.
 - **Pre-defined file type**—Click on one of the pre-defined tiles to select that specific file type.
 - **Custom file type**—If you have added custom file types, select a custom file type definition from the drop-down list. If you only have one custom file type, it is a single tile, not a drop-down list. Click **Edit** to modify the selected custom file type, or click **Create custom file type** to add a new custom file type.
 - **Define the file location**—Select where to look for files that should be backed up
 - **Commonly used file locations**—If desired, select a common location on the devices to look for files that should be backed up. You can select all drives for both Windows and macOS devices, or for Windows devices only, you can select the system drive, desktop, documents folders, or user folders.

If you do not select anything, then the specified **File location** will be used.
 - **File location**—If you selected a commonly used location, this field is automatically populated. You can specify a folder, file, or wildcard that

exists under the common location if desired. For example, if you selected the %Users% common Windows location, you could modify that to %Users%*\Documents. However, do not modify the syntax of the common location (%AllDrives%, %SystemDrive%, %Desktop%, %Documents%, or %Users%) or enter any other shortcuts or macros. Only the pre-defined shortcuts or macros listed in **Commonly used file locations** can be used. Any other shortcut or macro will not work.

If you did not select a commonly used location, enter the file location on the devices to look for files that should be backed up. Make sure you use the proper syntax for the operating system. For example, use C:\folder\subfolder for Windows and /folder/subfolder for macOS. Each device will use the rules formatted for its operating system syntax.

- **Define rule enforcement**—If you are allowing users to add their own personal rules, you need to select if you want to allow the user rules to be able to override administrator rules. If you did not allow users to add their own personal rules, this option is not used.
 - **User rules cannot override administrator rules**—The administrator rule will be enforced, regardless of user rules.
 - **User rules can override administrator rules**—If a user rule conflicts with an administrator rule, the user rule will be enforced.
- **Save & add another**—Click this button to save the rule and refresh the **Add a rule** dialog box so that you can add another rule.
- **Save**—Click this button to save the rule and close the dialog box.
- **Sort**—You can sort the table by clicking on any column heading.
- **Table row overflow menu**—In the overflow menu on the right of a table row, you can select the following actions.
 - **Edit rule**—Click this option to edit the rule. Use the same guidelines as outlined above when adding a rule. Click **Save** to save the changes.
 - **Delete rule**—Click this option to delete the rule. Confirm the deletion by clicking **Delete rule**.

Default exclusions

Some files and folders (including files without an extension) are excluded, by default, from backups.

- **Windows**—The following apply to all Windows devices.
 - Any file or folder with the system, device, temporary, or offline attribute applied to it are excluded.
 - Any file or folder that starts with ~ and has the hidden attribute is excluded. Both criteria must be met to be excluded. If only one criteria is met, the file or folder will be included if it meets a backup rule.
 - Any folder with the reparse point attribute is excluded.
- **macOS**—For all macOS devices, any file or folder with the following DirectoryEntry (as determined by the readdir_r system method) is excluded.

- DT_BLK—block device
- DT_CHR—character device
- DT_FIFO—named pipe (FIFO)
- DT_LNK—symbolic link
- DT SOCK—UNIX domain socket
- DT_UNKNOWN—unknown file type



If you are using a newer version of a OneDrive client on macOS (Version 22.002.0103.0004 and later), files that appear as cloud only are not backed up by Carbonite Endpoint.

OneDrive files that are stored locally are backed up for all macOS OneDrive versions.

- **File extensions**—The following file extensions are excluded.
 - DT_Store
 - gfs
 - hiberfil*.sys
 - log
 - log*
 - ost
 - pagefile*.sys
 - thumbs*.db
 - tmp
 - db-wal
 - db-shm
 - db-journal
 - sqlite-wal
 - sqlite-shm
 - sqlitedb-wal
 - sqlitedb-shm
 - sqlite3-wal
 - sqlite3-shm
- **Files without an extension**—Files without an extension are excluded unless they are in a folder included in an **All Files** backup rule. Other categories are looking at specific file extensions, so files without an extension will be excluded from those rules.
- **Temp, cache, and runtime data folders**—Folders that contain temp or cache files or runtime data are excluded. This list depends on the applications you are running. For example, on Windows, this might include folders located in %Users%*\AppData\Local, such as folders under %Users%*\AppData\Local\Google\Chrome\User Data\Default or %Users%*\AppData\Local\Mozilla\Firefox\Profiles. On macOS, this might include folders located in /users/*/Library, such as folders under /users/*/Library/Application Support/Google/Chrome/Default or /users/*/Library/Application Support/Slack.

If you need to back up a folder in one of these locations, for example for browser bookmarks, you need to create an include rule for the specific folder.

- **Files and folders using reserved characters**—Files and folders containing reserved operating system characters may appear to be protected, but they cannot be restored. Do not use any of the following reserved operating system characters in any files or folders.
 - less than <
 - greater than >
 - colon :
 - quotation marks or double quote "
 - forward slash /
 - backslash \
 - vertical bar or pipe |
 - question mark ?
 - asterisk *

Policy inheritance

By default, a policy is set at the company level and users, groups, and devices in that company inherit the policy assigned to the company. However, you can set a policy at the user, group, or device level as well. Policies set at those lower levels override the inheritance from higher levels.

After policies are defined, you can set them at a specific level.

- *Set the policy for a company* on page 40—Setting a policy for a company establishes inheritance. All groups, users, and devices assigned to the company use the company policy by default.
- *Set the policy for a group* on page 41—By default, a group's policy is set to inherit from the company the group is assigned to. However, you can override the inheritance and set a policy so that all users and devices assigned to the group use the policy assigned to the group.
- *Set the policy for a user* on page 42—By default, a user's policy is set to inherit from the company the user is assigned to. However, you can override the inheritance and set a policy so that all devices assigned to that user use the policy assigned to the user.
- *Set the policy for a device* on page 43—By default, a device inherits its policy from the company to which it is assigned. However, you can override the inheritance and set a policy so that the device uses its own policy.

Set the policy for a company

Use this procedure to set a policy for a company.

Setting a policy for a company establishes inheritance. All groups, users, and devices assigned to the company use the company policy by default.

1. Go to the **Company** page and click the **Company details** tab.
2. Click **Edit company**.
3. Click the policy you want to use for the company in the **Default policy set** list.

Companies / Company1 / Edit company

Company

Edit company

Partner: Partner Company uses user groups: Yes ▾

Company name: Company1 Allow passcodes to be emailed to users: Yes ▾

Custom 1: Auto sync device/computer names:

Custom 2: Default policy set: Base Policy ▾

Custom 3:

Save changes Cancel

4. Click **Save changes**.

Set the policy for a group

Use this procedure to set a policy for a group.

By default, a group's policy is set to inherit from the company the group is assigned to. However, you can override the inheritance and set a policy so that all users and devices assigned to the group use the policy assigned to the group.

1. Go to the **Company** page and click the **Groups** tab.
2. Locate the group you want to set the policy for. See *Create and manage groups* on page 63 for details on searching the table.
3. Click the name of the group.
4. In the Group properties page, click **Edit group**.
5. Click the policy you want to use for the group in the **Default policy set** list. If you want to revert to an inherited policy, select **Inherit policy from**.

Company

Company / All users / Edit group

Edit group

User group: All users

Default policy set: Inherit policy from CompanyName - Base Policy

Custom 1:

Custom 2:

Custom 3:

Save changes Cancel

6. Click **Save changes**.

Set the policy for a user

Use this procedure to set the policy for a user.

By default, a user's policy is set to inherit from the company the user is assigned to. However, you can override the inheritance and set a policy so that all devices assigned to that user use the policy assigned to the user.

1. On the **Users** page, locate the user for which you want to set the policy. See *View users* on page 69 for details on searching the table.
2. Click on the user name.
3. On the **User** page, click the **User details** tab, and then click **Edit user details**.
4. Click the policy you want to use for the user in the **Default policy set** list. If you want to revert to an inherited policy, select **Inherit policy from**.

Users / FirstName01 LastName01 / Edit user

User

Edit user details

Email: Company:

First name: User group:

Last name: Password managed locally:

Custom 1: Time zone:

Custom 2: Default policy set:

Custom 3: 2FA: Enforced Disabled

5. Click **Save changes**.

Set the policy for a device

Use this procedure to set the policy for a device.

By default, a device inherits its policy from the company to which it is assigned. However, you can override the inheritance and set a policy so that the device uses its own policy.

1. On the **Devices** page, locate the device for which you want to set the policy. See *Create and manage devices* on page 111 for details on searching the table.
2. Click on the device name.
3. On the **Device** page, click the **Device details** tab, and then click **Edit device**.
4. Click the policy you want to use for the device in the **Select device policy set** list. If you want to revert to an inherited policy, select **Inherit policy from**.

🏠 / Devices / DeviceName / Edit device

Device

Edit device

Device name is synchronized with computer name. Device name changes may be reversed during the next synchronization.

Device name (defaults to device id if no name is provided):

Do not sync device/computer name:

Custom 1:

Custom 2:

Custom 3:

Select device policy set:

Policy set description:
A Starter Policy

Select storage quota: (Current client usage is 0.00 GB)
 Unlimited
 Custom GB

QuickCache this device can use:

5. Click **Save changes**.

Chapter 7 Manage deployment

Deployment is the process of obtaining an activation code and installing the end-user software on the endpoint devices. In some cases, the deployment process also includes adding a user account.

- **Activation codes**—The activation code option you select depends on what you want to happen when the client software is installed.
 - **Add devices and add user accounts**—If you want to add both a device and a user in Carbonite Endpoint when the client software is installed and activated, use the **Enable full directory integration** option. (If the user already exists, only the device will be added.) This method requires the user to log in on the device when connected to the corporate network to capture the user information, and it requires a valid email address for the user in LDAP for the mail attribute.
 - **Add devices for existing, individual user accounts**—If you want to add a device in Carbonite Endpoint for a user account that already exists, use the **Enable directory user integration** option. This method requires you to add individual user accounts in Carbonite Endpoint before the client software is installed.
 - **Add devices for existing, single user account**—If you want to add a device in Carbonite Endpoint for a single user account that already exists, use the **Enable directory device integration** option. This method requires you to add a single user account in Carbonite Endpoint before the client software is installed. All devices will be associated with this single user account.
 - **Do not add devices**—If you do not want to add any devices in Carbonite Endpoint when the client software is installed, do not select any option (or use the **Disable automatic creation** option if you selected another option and want to go back to no selection). This method requires you to add individual user accounts and devices in Carbonite Endpoint before the client software is installed.
- **Installation**—You can select the type of installation to perform.
 - **Remote deployment**—With this strategy, you can push the end-user client software to each device.
 - **Local installation**—With this strategy, the software is installed manually on each device.



Regardless of the method you choose, you should initially work with a small subset of devices until you are confident your deployment strategy is working. Once you are sure, you can implement the strategy for larger numbers of devices.

See *Activation codes* on page 46 and *Installation* on page 50 for details.



You can also use WCF or REST APIs to add users, assign devices, trigger email notifications, and so on. See the [Dashboard Service API documentation](#) for details.

Activation codes

The activation code option you select depends on what you want to happen when the client software is installed.

- **Add devices and add user accounts**—If you want to add both a device and a user in Carbonite Endpoint when the client software is installed and activated, use the **Enable full directory integration** option. (If the user already exists, only the device will be added.) This method requires the user to log in on the device when connected to the corporate network to capture the user information, and it requires a valid email address for the user in LDAP for the mail attribute.
- **Add devices for existing, individual user accounts**—If you want to add a device in Carbonite Endpoint for a user account that already exists, use the **Enable directory user integration** option. This method requires you to add individual user accounts in Carbonite Endpoint before the client software is installed.
- **Add devices for existing, single user account**—If you want to add a device in Carbonite Endpoint for a single user account that already exists, use the **Enable directory device integration** option. This method requires you to add a single user account in Carbonite Endpoint before the client software is installed. All devices will be associated with this single user account.
- **Do not add devices**—If you do not want to add any devices in Carbonite Endpoint when the client software is installed, do not select any option (or use the **Disable automatic creation** option if you selected another option and want to go back to no selection). This method requires you to add individual user accounts and devices in Carbonite Endpoint before the client software is installed.



Regardless of the method you choose, you should initially work with a small subset of devices until you are confident your deployment strategy is working. Once you are sure, you can implement the strategy for larger numbers of devices.

See the following sections for activation code details.

- *View available activation codes* on page 46
- *Add an activation code* on page 48
- *Edit an activation code* on page 49
- *Delete an activation code* on page 50

View available activation codes

Use this procedure to view the available activation codes.

- Go to the **Company** page and click the **Deployment (AD/LDAP)** tab.

The client software can be silently deployed via Active Directory or other deployment systems.
 Devices and users can be automatically created in the Dashboard using information from the AD or LDAP directory.
 Use the "Add activation code" button to create an activation code to use with a silent deployment.

+ Add activation code

WIN MAC

Show 10 entries Search: []

Activation code	Comment	Auto create
1ABC-2D34-5E67-8F90-123A		Create devices under existing dashboard users
4567-89A0-BC1D-234E-5F6A		Create devices under (user@domain.com)
7BC8-9012-D34E-567F-A890		Create devices and users

Showing 1 to 3 of 3 entries First Previous 1 Next Last

The following controls are available on the **Deployment (AD/LDAP)** tab.

- **Add activation code**—Click this button to add a new activation code. See *Add an activation code* on page 48 for details.
- **Installation download buttons**—These buttons may or may not be available, depending on your vault configuration.
 - **WIN**—If this button is available, click it to download a Windows Msiexec file.
 - **MAC**—If this button is available, click it to download a macOS package file.



See *Installation* on page 50 for choices and details on remote deployment and local installation using .msi and .pkg files.

- **Show Entries**—Specify the number of rows to be shown in the table on each page. Additional rows over the number you select are shown on additional pages and can be viewed by using the paging buttons at the bottom of the table.
- **Search**—Text entered in the box narrows the list displayed to only the rows that contain the search text. The search checks the entire table, not just the visible rows.
- **Sort**—You can sort the table by clicking on any column heading.
- **Table hyperlinks**—Click an activation code to manage that activation code. From the **Activation code details** page, you can do any of the following.
 - **View the details of the activation code**—You can view the code and its details.
 - **Delete activation code**—If you no longer need the activation code, click the **Delete activation code** button to delete the code. Click **Yes** in the confirmation box.
 - **Edit details**—You can modify the type of activation code or its settings. See *Edit an activation code* on page 49 for details.
- **Table paging buttons**—The paging buttons at the bottom of the table allow you to move more quickly between pages. Each button jumps to that respective page of the table.

Add an activation code

Use this procedure to add an activation code.

You require an activate code when installing Carbonite Endpoint, regardless of the installation method you select.

1. Go to the **Company** page and click the **Deployment (AD/LDAP)** tab.
2. Click **Add activation code**.
3. Determine type of activation code you want to add based on what you want to happen when the client software is installed.

The screenshot shows the 'Add activation code' page. It features a blue header with the title 'Add activation code'. Below the header, there is a section titled 'No automatic creation, match existing dashboard device name'. This section contains a 'Comment:' text input field on the left and three blue buttons on the right: 'Disable automatic creation', 'Enable full directory integration', and 'Enable directory device integration'. Each button has a corresponding description to its right. The 'Enable full directory integration' button is described as: 'Devices will be matched by name, or created, under the user who next logs into the computer - user will also be created if necessary'. The 'Enable directory user integration' button is described as: 'Devices will be matched by name, or created, under the user who next logs into the computer'. The 'Enable directory device integration' button is described as: 'Enable devices to be automatically created under one specified user'. At the bottom right of the form, there are two buttons: 'Add activation code' and 'Cancel'.

- **Add devices and add user accounts**—If you want to add both a device and a user in Carbonite Endpoint when the client software is installed and activated, use the **Enable full directory integration** option. (If the user already exists, only the device will be added.) This method requires the user to log in on the device when connected to the corporate network to capture the user information, and it requires a valid email address for the user in LDAP for the mail attribute.
- **Add devices for existing, individual user accounts**—If you want to add a device in Carbonite Endpoint for a user account that already exists, use the **Enable directory user integration** option. This method requires you to add individual user accounts in Carbonite Endpoint before the client software is installed.
- **Add devices for existing, single user account**—If you want to add a device in Carbonite Endpoint for a single user account that already exists, use the **Enable directory device integration** option. This method requires you to add a single user account in Carbonite Endpoint before the client software is installed. All devices will be associated with this single user account.
- **Do not add devices**—If you do not want to add any devices in Carbonite Endpoint when the client software is installed, do not select any option (or use the **Disable automatic creation** option if you selected another option and want to go back to no selection). This

method requires you to add individual user accounts and devices in Carbonite Endpoint before the client software is installed.

4. Select your activation code type.
 - **Enable full director integration**—Click this button to add an activation code to add device and add user accounts. Select the group you want the activation code to apply to from the **User group** list. Optionally, you can select the **Enable web retrieval** check box, which allows users to log into the dashboard and access their files online. This option allows users to download individual files from their browser. Click **Save changes**.
 - **Enable directory user integration**—Click this button to add an activation code to add devices for existing, individual user accounts. No additional options are required.
 - **Enable directory device integration**—Click this button to add an activation code to add devices for an existing, single user account. If the list exceeds the maximum number of results configured by your administrator, the table is blank and a dialog box displays, prompting you to use the **Search** function to narrow your list of results. You can click the link to view the limited list, if required. Select the user account you want the activation code to be associated with. Then click **Select user**.
 - **Disable automatic creation**—Click this button if you have selected one of the other activation code types but want to revert to the option to not add any devices. No additional options are needed.
5. Click **Add activation code**.
6. The **Activation code details** section appears and displays the activation code you will use in the installation.

Edit an activation code

Use this procedure to edit an existing activation code.

Editing an activation code impacts new devices attempting to activate but does not affect existing devices.

1. Go to the **Company** page and click the **Deployment (AD/LDAP)** tab.
2. Locate in the table the activation code you want to edit. See *View available activation codes* on page 46 for details on searching the table.
3. Click on the activation code you want to edit.
4. On the **Activation code details** page, click the **Edit details** button.
5. On the **Edit activation code** page, you can change the user or user creation settings, depending on your activation code type. You can also change activation codes types, if desired. See *Add an activation code* on page 48 for details on each of the activation types.

Company

Home / CompanyName / C322-75D7-6EE7-E7A7-960B / Edit activation code

Edit activation code

Activation code: C322-75D7-6EE7-E7A7-960B

Create devices under existing dashboard users

Comment:

Disable automatic creation

Enable full directory integration

Enable directory user integration

Enable directory device integration

Devices will be matched by name, or created, under the user who next logs into the computer - user will also be created if necessary

Devices will be matched by name, or created, under the user who next logs into the computer

Enable devices to be automatically created under one specified user

Save changes Cancel

6. Click **Save changes**.

Delete an activation code

Use this procedure to delete an activation code.

You can delete an activation code if you no longer need it. Deleting the code does not impact devices already using the it. It only prohibits new devices from using it.

1. Go to the **Company** page and click the **Deployment (AD/LDAP)** tab.
2. Locate in the table the activation code you want to delete. See *View available activation codes* on page 46 for details on searching the table.
3. Click the activation code.
4. On the **Activation code details** page, click **Delete activation code**.

About to delete activation code C322-75D7-6EE7-E7A7-960B, any future attempts to activate a device using this code will fail. Is this OK?

Yes No

5. Click **Yes** in the confirmation dialog box.

Installation

You can select the type of installation strategy to use. Carbonite Endpoint supports two strategies:

- **Remote deployment**—With this strategy, you can push the end-user client software to each device.
 - **Local installation**—With this strategy, the software is installed manually on each device.
-



Regardless of the method you choose, you should initially work with a small subset of devices until you are confident your deployment strategy is working. Once you are sure, you can implement the strategy for larger numbers of devices.

See the following sections for installation details.

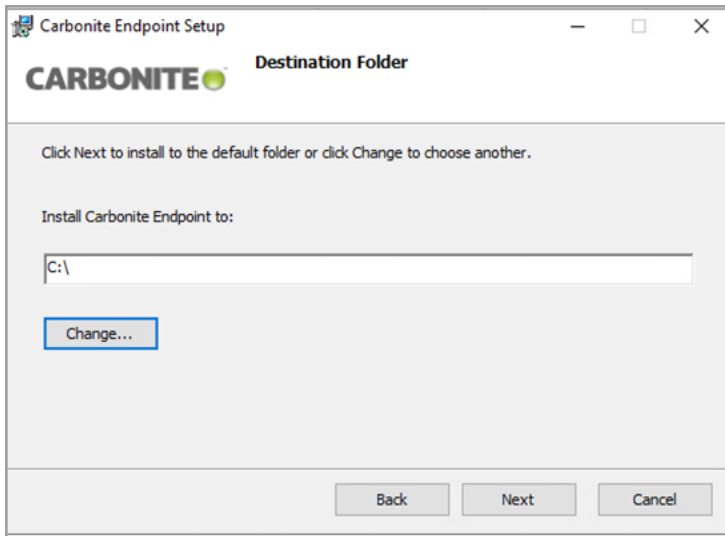
- *Install on Windows or macOS using the installation wizard on page 51*
- *Install on Windows using Msiexec on page 53*
- *Install on macOS using the installer app on page 57*

Install on Windows or macOS using the installation wizard

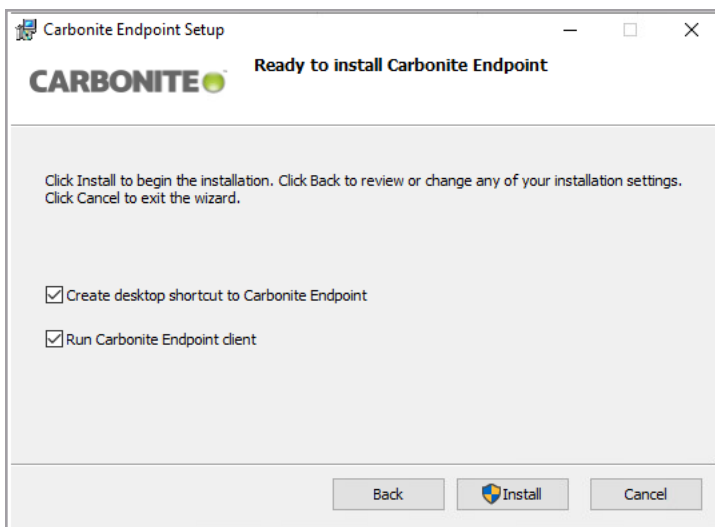
Use this procedure to manually install Carbonite Endpoint.

These instructions to install Carbonite Endpoint follow the Windows interactive installation wizard. At a high-level, the same process is used on macOS devices, except for a few differences outlined below and a different style interface, such as **Next** buttons that are labeled as **Continue** on macOS devices.

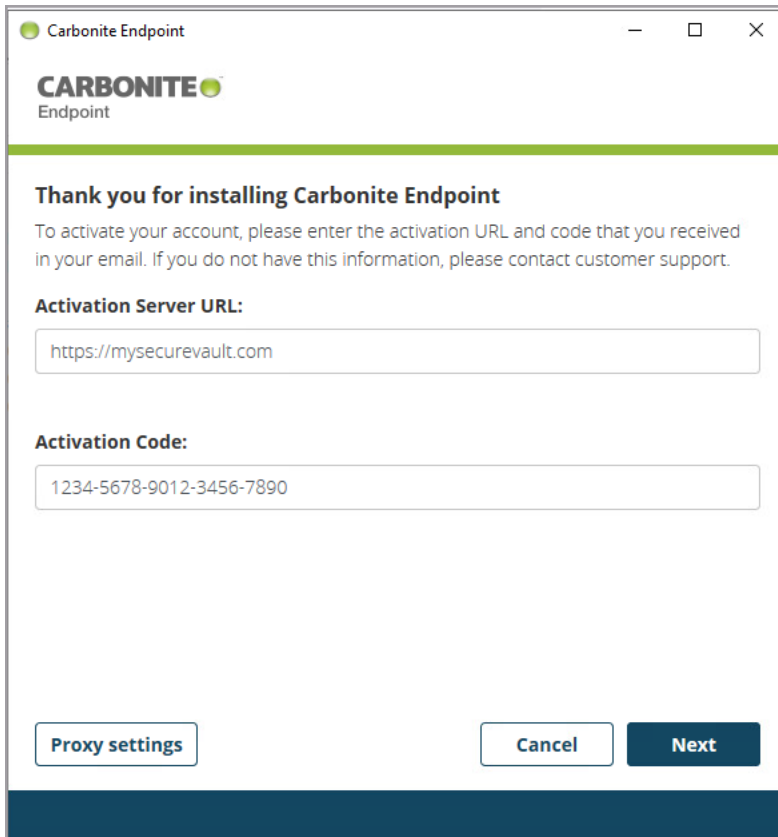
1. Launch the installation file.
2. At the **Welcome** page, click **Next** to continue.
3. Review the **Terms of Service**. You must accept the terms in order to continue with the installation program. Click **Next** to continue.
4. On Windows, modify the installation location, if desired. This option is not available on macOS devices. Carbonite Endpoint will be installed on Macintosh HD.
5. Click **Next** to continue.
6. On Windows, select an internal, local disk that will be used for the local data cache. The drive you select should have at least 1 GB free space. This option is not available for macOS devices. The local data cache will be installed on Macintosh HD.



7. Click **Next** to continue.
8. Optionally, deselect the options for the desktop shortcut and running the client after the installation. These options are not shown on macOS devices and will automatically be enabled.



9. When you are ready to begin the installation, click **Install**.
10. When the installation is completed, click **Finish**.
11. In the **Thank you** window that opens after the installation is complete, enter your activation information.



- **Activation Server URL**—This is the URL where files will be backed up.
 - **Activation Code**—This is the activation code for the device.
12. If you need to specify a proxy server for Internet access, click **Proxy settings** and complete the proxy information.
 13. Click **Next** to continue.
 14. If you are reactivating a previously used device, you are prompted to enter a **Passphrase**. Enter it and then click **Next** to continue. You will not see this page if you are not reactivating.
 15. Once the activation is complete and the account is activated, click **Close**.

Install on Windows using Msiexec

Use this procedure to install Carbonite Endpoint on Windows using Msiexec.

Msiexec is a Windows command-line based program that interprets and installs software installation packages. You can use Msiexec to install Carbonite Endpoint on any version of Windows 7 through Windows 11, except RT, Itanium, and Home versions. In most cases, you will use this method of installation when you are pushing the software using a remote deployment tool.

The following is the syntax for using Msiexec with Carbonite Endpoint.

```
msiexec /i PackageLocationAndName /qn PublicProperty1=Value
PublicProperty2=Value ... PublicPropertyN=Value
```

The following tables explains the parameters used with the command.

Parameter	Description
/i PackageLocationAndName	Identifies the location and name of the .msi installation package
/qn	Installs silently, hiding the installation user interface

<pre>PublicProperty1=Value PublicProperty2=Value . . . PublicPropertyN=Value</pre>	<p>One or more of the following arguments used when installing the Carbonite Endpoint package. Do not use a slash / before any of these parameters.</p> <ul style="list-style-type: none"> • ActivationCode—If you have generated a deployment activation code ahead of time, use this option to enter the code. If you do not use this option or this option is blank, the user will have to provide an activation code before being able to use Carbonite Endpoint. The default value is blank. • ActivationUrl—This option is the URL of the vault. If you do not use this option or this option is blank, the user will have to provide a URL before being able to use Carbonite Endpoint. The default value is blank. • CompanyId—Use this option as an alternative to ActivationCode when you are using directory user integration (adding devices for existing, individual user accounts). This is not a commonly used option, and you may be directed to Professional Services for assistance with this option. The default value is blank. • Drive—This option specifies an internal, local disk that will be used for the local data cache. If you do not use this option, the default value is C:\. • InstallDesktopShortcut—This option indicates if a Carbonite Endpoint shortcut will appear on the desktop, letting you decide if Carbonite Endpoint is visible to users. If you do not use this option, the default value is 1. <ul style="list-style-type: none"> • 0—A shortcut will not appear on the desktop. • 1—A shortcut will appear on the desktop. • PassphraseRequired—This option indicates if the end-user must enter a passphrase to decrypt the device key if the machine has been reset. If you do not use this option, no passphrase is needed. <ul style="list-style-type: none"> • 0—The user does not need to enter a passphrase. • 1—The user needs to enter a passphrase. • RunServiceAsLocalSystem—This option indicates what account will be used to run Carbonite Endpoint. If you do not use this option, the default value is 1. <ul style="list-style-type: none"> • 0—The new DCProtectService admin user will be used to run Carbonite Endpoint. • 1—The Local System account will be used to run Carbonite Endpoint.
--	---

	<ul style="list-style-type: none"> • Silent—This option indicates if the interactive activation workflow appears after the installation. If you do not use this option, the default value is 0. <ul style="list-style-type: none"> • 0—The silent workflow is not enabled, so the activation workflow will appear after the installation. • 1—The silent workflow is enabled, so the activation workflow will not appear after the installation. • StartClientPostActivate—This option indicates if the client will be started after the activation. If you do not use this option, the default value is 1. <ul style="list-style-type: none"> • 0—The client will not start after activation. • 1—The client will start after activation.
--	--

Use the following examples as a guideline, and modify them as needed for your environment and needs.

- **Unattended installation, unattended activation, client software available to users**—In this example, the client software is deployed and activated without any interaction from the end-user. The end-user can access the software.

```
msiexec /i "C:/temp/dcprotect.msi" /qn ActivationCode=1ab2-cdef-3g45-h67i-j890 ActivationUrl=https://mysecuredatavault.com Silent=1
```

- **Unattended installation, unattended activation, client software hidden from users**—This example is like the previous one, however, the end-user cannot access the software from a desktop shortcut.

```
msiexec /i "C:/temp/dcprotect.msi" /qn ActivationCode=1ab2-cdef-3g45-h67i-j890 ActivationUrl=https://mysecuredatavault.com Silent=1 InstallDesktopShortcut=0
```

Install on Windows using group policy

Group policy can be used as a software deployment tool with the .msi installer, however it does not support command-line arguments. The following alternatives are available:

- **Edit .msi**—You can edit the .msi using the Carbonite Endpoint MSI editor or another MSI editor. This method will break the MSI signature, so any future updates must also be installed using this method.
- **Transform file**—You can use a generic editor to create an MSI transform file. This method will not break the MSI signature, so future updates can be performed using another method if desired.
- **Script**—Create a script that runs Msiexec and run that script using the group policy. This method will avoid editing the .msi or creating a transform file. You could also perform a check at

the beginning of the script to make sure the installer is not downloaded every time the device is rebooted. The example script below would determine if Carbonite Endpoint is installed. If it is, the script exits. If it is not, the software would be installed.

```
IF EXIST
  "c:\dcprotectdata\service\serverstatus.xml" (
    ECHO "Carbonite Endpoint already installed"
    EXIT
  ) ELSE (
    Net use x: \\update_server\software
    msiexec /i x:\dcprotect.msi /qn ActivationCode=1ab2-cdef-3g45-h67i-j890
    ActivationUrl=https://mysecuredatavault.com Silent=1
  )
```

For details on using group policies, see your Windows documentation.

Install on macOS using the installer app

Use this procedure to install Carbonite Endpoint on macOS using the installer and a LocalAutoConfig.xml file.

1. Create a file called LocalAutoConfig.xml in the root Library folder (/Library). The file name is case-sensitive.



macOS 10.15 (Catalina) requires the LocalAutoConfig.xml file to be located in the root /Library folder. However, any previously supported version of macOS will work with the LocalAutoConfig.xml file in the root folder. To work with all versions, use /Library. If you have any existing scripts that had the LocalAutoConfig.xml file in the root rather than /Library, you need to update your scripts to /Library if you will be installing on macOS 10.15.

Once Carbonite Endpoint is activated, the LocalAutoConfig.xml file will automatically be moved to the DCProtect folder.

2. Edit the LocalAutoConfig.xml file.
3. Add the opening <AutoConfig> and closing </AutoConfig> tags.

```
<AutoConfig>
</AutoConfig>
```

4. Specify one or more of the properties listed in the following table by specifying them between opening and closing tags. Make sure the property tags are between the <AutoConfig> tags. See the examples after the table.

Parameter	Description
-----------	-------------

ActivationCode	If you have generated a deployment activation code ahead of time, use this option to enter the code. If you do not use this option or this option is blank, the user will have to provide an activation code before being able to use Carbonite Endpoint. The default value is blank.
ActivationUrl	This option is the URL of the vault. If you do not use this option or this option is blank, the user will have to provide a URL before being able to use Carbonite Endpoint. The default value is blank.
CompanyId	Use this option as an alternative to ActivationCode when you are using directory user integration (adding devices for existing, individual user accounts). This is not a commonly used option, and you may be directed to Professional Services for assistance with this option. The default value is blank.
InstallDesktopShortcut	This option indicates if a Carbonite Endpoint shortcut will appear on the desktop, letting you decide if Carbonite Endpoint is visible to users. If you do not use this option, the default value is 1. <ul style="list-style-type: none"> • 0—A shortcut will not appear on the desktop. • 1—A shortcut will appear on the desktop
PassphraseRequired	This option indicates if the end-user must enter a passphrase to decrypt the device key if the machine has been reset. If you do not use this option, no passphrase is needed. <ul style="list-style-type: none"> • 0—The user does not need to enter a passphrase. • 1—The user needs to enter a passphrase.
ProxyAutoDetect	If you need to use a proxy server, use this option to specify if the proxy server specified in System Preferences should be used. The default value is no proxy server. <ul style="list-style-type: none"> • 0—Use the proxy server specified in System Preferences • 1—Do not use the proxy server specified in System Preferences
ProxyScript	This option is the path and file name to the proxy script.

ProxyServer	This option is the proxy server IP address and port number. For example, you might use <code>http://112.42.7.56:808</code> .
Silent	This option indicates if the interactive activation workflow appears after the installation. If you do not use this option, the default value is 0. <ul style="list-style-type: none"> • 0—The silent workflow is not enabled, so the activation workflow will appear after the installation. • 1—The silent workflow is enabled, so the activation workflow will not appear after the installation.
StartClientPostActivate	This option indicates if the client will be started after the activation. If you do not use this option, the default value is 1. <ul style="list-style-type: none"> • 0—The client will not start after activation. • 1—The client will start after activation.

Examples for LocalAutoConfig.xml

- **Unattended installation, unattended activation, client software available to users**—In this example, the client software is deployed and activated without any interaction from the end-user. The end-user can access the software.

```
<AutoConfig>
  <ActivationCode>1ab2-cdef-3g45-h67i-j890</ActivationCode>
  <ActivationUrl>https://mysecuredatavault.com</ActivationUrl>
  <Silent>1</Silent>
</AutoConfig>
```

- **Unattended installation, unattended activation, client software hidden from users**—This example is like the previous one, however, the end-user cannot access the software from a desktop shortcut.

```
<AutoConfig>
  <ActivationCode>1ab2-cdef-3g45-h67i-j890</ActivationCode>
  <ActivationUrl>https://mysecuredatavault.com</ActivationUrl>
  <Silent>1</Silent>
  <InstallDesktopShortcut>0</InstallDesktopShortcut>
</AutoConfig>
```

5. Save the changes to the LocalAutoConfig.xml file.
6. Run the installer using the following command.

```
sudo installer -pkg /path/to/application.pkg -target /
```

Substitute the path and file name for the DCProtectInstaller.pkg for /path/to/application.pkg. For example, you might use `sudo installer -pkg /DCProtectInstaller.pkg -target /`.

Activate on macOS

If you disabled activation (RunActivatePostInstall is 0), then you can activate later. The following is the syntax for activating.

```
/Library/ApplicationSupport/DCProtect/DCProtect.app/Contents/MacOS/DCProtect -autoactivation -argument1=Value -argument2=Value ... -argumentN=Value
```

You must use the -email argument. The other arguments are optional

Argument	Description
-email	This argument is required. It is the email address that the device will be assigned to. You must specify this option. If you do not have an easy method of getting this address, you may want to fetch the user's USER variable and prepend the variable as part of the email address. Even though this may not be the user's actual email address, it allows the user to be identifiable by a login ID.
-activationCode	If you have generated a deployment activation code ahead of time, use this option to enter the code. If you do not specify this option or this option is blank, the user will have to provide an activation code before being able to use Carbonite Endpoint. The default value is blank. You do not need to use this option if you specified it in the LocalAutoConfig.xml.
-activationUrl	This option is the URL of the vault. If you do not specify this option or this option is blank, the user will have to provide a URL before being able to use Carbonite Endpoint. The default value is blank. You do not need to use this option if you specified it in the LocalAutoConfig.xml.
-deviceName	This option is the name of the device to be activated. If you do not specify this option, the value from the hostname utility will be used.
-displayName	This is the first and last name assigned to the user using the device. If you do not specify this option, the -firstName and -lastName fields will be used.

-firstName	This is the first name assigned to the user using the device. If you do not specify this option, the local-part of the email address (the text before @) will be used.
-lastName	This is the last name assigned to the user using the device. If you do not specify this option, the last name will be blank.
-timeoutMs	This is the amount of time to wait. If you do not specify this option, 120,000 will be used.
-timezoneId	This is the time zone assigned to the device. If you do not specify this option, the time zone of the device at installation time will be used.
-verbose	This option provides additional output details while running the activation.

Use the following examples as a guideline, and modify them as needed for your environment and needs.

- **Activate with code, URL, and email address**—In this example, the software is activated using an activation code, activation URL, and an email address.

```
/Library/ApplicationSupport/DCProtect/DCProtect.app/Contents/MacOS/DCProtect -autoactivation -activationCode=1ab2-cdef-3g45-h67i-j890 -activationUrl=https://mysecuredatavault.com -email=name@domain.com
```

- **Activate with code, URL, and email address created from USER variable**—In this example, the software is activated using an activation code, activation URL, and an email address created from the USER environment variable.

```
/Library/ApplicationSupport/DCProtect/DCProtect.app/Contents/MacOS/DCProtect -autoactivation -activationCode=1ab2-cdef-3g45-h67i-j890 -activationUrl=https://mysecuredatavault.com -email=$USER@domain.com
```

- **Activate with code, URL, email address created from USER variable, and display name created from login name**—In this example, the software is activated using an activation code, activation URL, an email address created from the USER environment variable, and a display name created from the login name.

```
FULLNAME="$ (id -F) "
```

```
/Library/ApplicationSupport/DCProtect/DCProtect.app/Contents/MacOS/DCProtect -autoactivation -activationCode=1ab2-cdef-3g45-h67i-j890 -activationUrl=https://mysecuredatavault.com -email=$USER@domain.com -displayName="$FULLNAME "
```

Once you have activated the software, you can determine the activation status by using the `-getClientStatus` argument with `DTProtect`.

```
/Library/ApplicationSupport/DCProtect/DCProtect.app/Contents/MacOS/DCProtect -getClientStatus
```

You will get one of the following return codes.

Return Code	Status
-2	Timed out
-1	Unknown
0	Created but not activated
1	Activated
2	Reset
3	DataDelete
4	Suspended
5	PersistentAuthFailure
6	Canceled

You can optionally add `-verbose` to return additional status information.

Chapter 8 Create and manage groups

Groups provide a way to associate multiple users. You can then perform tasks for the users in a group. For example, you can define a policy for a group and all users in the group will use that policy.

The following tasks are available for groups.

- *View groups* on page 63
- *View group details* on page 64
- *Add a group* on page 65
- *Add users to a group* on page 66
- *Edit an existing group* on page 66
- *Delete a group* on page 67



You may not have access to groups if your partner has disabled this feature.

View groups

Use this procedure to view your available user groups.

Go to the **Company** page and click the **Groups** tab.

User group name	Number of devices	Usage / Quota (GB)
All users	58 (12 Activated)	33.76 / Unrestricted
SubsetGroup	8 (1 Activated)	27.49 / 307340 (<1%)
UserGroup	1 (0 Activated)	0 / 25 (0%)

The following controls are available on the **Groups** tab.

- **Add group**—Click this button to add a new group. See *Add a group* on page 65 for details.
- **Show Entries**—Specify the number of rows to be shown in the table on each page. Additional rows over the number you select are shown on additional pages and can be viewed by using the paging buttons at the bottom of the table.

- **Search**—Text entered in the box narrows the list displayed to only the rows that contain the search text. The search checks the entire table, not just the visible rows.
- **Table hyperlinks**—Click a group name to see details for that group. See *View group details* on page 64 for details.
- **Table paging buttons**—The paging buttons at the bottom of the table allow you to move more quickly between pages. Each button jumps to that respective page of the table.

View group details

Use this procedure to view the details and properties of a group.

1. Go to the **Company** page and click the **Groups** tab.
2. Locate the group that you want to view. See *View groups* on page 63 for details on searching the table.
3. Click on the group name.
4. In the **Group properties** section, you can view and manage the following group properties.

Group properties			
User group:	All users	Created at:	Oct 07 2019 01:54 PM
Company:	CompanyName	Activated devices:	12
User group Id:	c7a1eb23-af88-42bf-be6f-162a7162de0a	Last updated at:	Oct 07 2019 01:54 PM
Total devices:	58	Custom 1:	
Total storage quota:	102400 GB	Custom 2:	
Default policy set:	Base Policy (Inherited)	Custom 3:	

- **Delete user group**—Click this button to delete the group. Everything under the group (users, devices, and backed up data) will be deleted. You must confirm that you want to delete the group and then click **OK**. See *Delete a group* on page 67 for details.
 - **Edit group**—Click this button to edit the group. See *Edit an existing group* on page 66 for details.
 - **Table hyperlinks**—Click the hyperlinks in the table to open the corresponding pages in the dashboard.
 - **Company**—Click the hyperlink to open the group's **Company** page. See *View and manage your company* on page 19.
 - **Default policy set**—Click the hyperlink to open the policy details for the group's default policy. See *Edit an existing policy* on page 33 for details.
5. In the **Users in group** section, you can view and add users to the group.

Users in group

+ Add user

Show 10 entries Search:

User email	First name	Last name	Number of devices	Usage / Quota (GB)	Login allowed
email01@domain.com	FirstName01	LastName01	0 (0 Activated)	0 / 0	Yes
email02@domain.com	FirstName02	LastName02	0 (0 Activated)	0 / 0	Yes
email03@domain.com	FirstName03	LastName03	0 (0 Activated)	0 / 0	Yes
email04@domain.com	FirstName04	LastName04	0 (0 Activated)	0 / 0	Yes
email05@domain.com	FirstName05	LastName05	0 (0 Activated)	0 / 0	Yes
email06@domain.com	FirstName06	LastName06	0 (0 Activated)	0 / 0	Yes
email07@domain.com	FirstName07	LastName07	0 (0 Activated)	0 / 0	Yes
email08@domain.com	FirstName08	LastName08	0 (0 Activated)	0 / 0	Yes
email09@domain.com	FirstName09	LastName09	0 (0 Activated)	0 / 0	Yes
email10@domain.com	FirstName10	LastName10	0 (0 Activated)	0 / 0	Yes

Showing 1 to 10 of 58 entries

First Previous 1 2 3 4 5 6 Next Last

- **Add user**—Click this button to add a new user to this group. See *Add users to a group* on page 66 for details.
- **Show Entries**— Specify the number of rows to show on each page in the table. Additional rows over the number you select are shown on additional pages and can be viewed using the paging buttons at the bottom of the table. You can view a maximum of 100 rows in the table.
- **Search**—Text entered in the box narrows the list displayed to only the rows that contain the search text. The search checks the entire table, not just the visible rows.
- **Sort**—You can sort the table by clicking on any column heading.
- **Table hyperlinks**—Click an email address to view details for that user. See *View user details* on page 71 for details.
- **Table paging buttons**—The paging buttons at the bottom of the table allow you to move more quickly between pages. Each button jumps to that respective page of the table.

Add a group

Use this procedure to add a group to a company.

1. Go to the **Company** page and click the **Groups** tab.
2. Click **Add group**.
3. Specify the group information.

The screenshot shows a web interface for adding a new group. The breadcrumb navigation at the top indicates the user is in the 'Company' page, specifically in the 'Add group' section. The form itself has a blue header bar with the text 'Add group'. Below this, there are four input fields. The first field, labeled 'User group', contains the text 'UserGroup'. The other three fields, labeled 'Custom 1', 'Custom 2', and 'Custom 3', are currently empty. At the bottom right of the form, there are two buttons: a blue 'Add group' button and a grey 'Cancel' button.

- **User group**—Specify a unique name for the group.
 - **Custom**—If desired, enter custom information in the three provided fields. These fields allow you to enter your own custom information. Each field is limited to 500 characters.
4. When the group definition is complete, click **Add group**.

Add users to a group

Use this procedure to add one or more users to a group. You can also use this procedure to move a user into a different group.

1. Go to the **Company** page and click the **Groups** tab.
2. Locate the group that you want to edit. See *View groups* on page 63 for details on searching the table.
3. Click on the group name.
4. In the **Users in group** section, click **Add user**.
5. The User page appears.
6. Do one of the following:
 - If you are adding a new user to the group, configure the settings as described in *Add a single user* on page 73.
 - If you want to move an existing user into the group, edit the user. See *View user details* on page 71 for details.

Edit an existing group

Use this procedure to edit an existing group.

1. Go to the **Company** page and click the **Groups** tab.
2. Locate in the table the group that you want to edit. See *View groups* on page 63 for details on searching the table.
3. Click on the group name.
4. In the **Group properties** section, click **Edit group**.

CompanyName / All users / Edit group

Company

Edit group

User group: Default policy set:

Custom 1:

Custom 2:

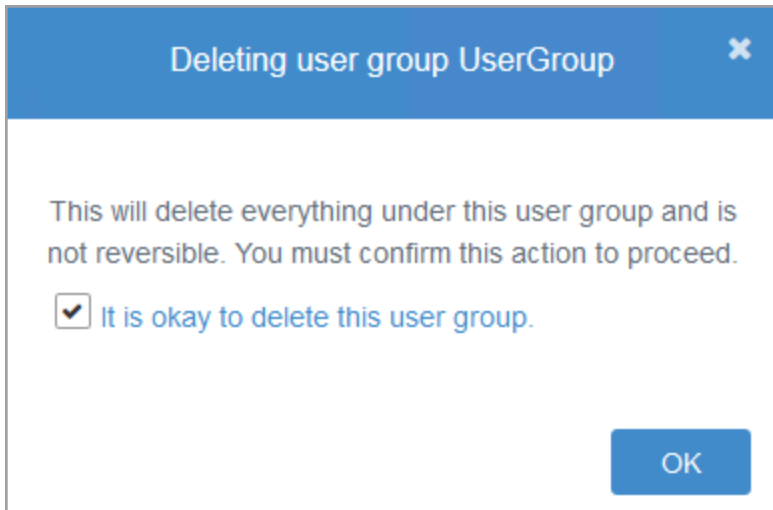
Custom 3:

5. Edit the group settings as desired. In addition to the settings available when you added the group, (see *Add a group* on page 65 for details), you can also set the default policy for the group. By default, a group's policy is set to inherit from the company the group is assigned to. However, you can override the inheritance and set a policy so that all users and devices assigned to the group use the policy assigned to the group. See *Set the policy for a group* on page 41 for details.
6. After you have modified the group settings, click **Save changes**.

Delete a group

Use this procedure to delete a group. Everything under the group (users, devices, and backed up data) will also be deleted.

1. Go to **Company** page and click the **Groups** tab.
2. Locate in the table the group that you want to delete. See *View groups* on page 63 for details on searching the table.
3. Click on the group name.
4. In the **Group Properties** section, click **Delete user group**.



5. Confirm that you want to delete the group and click **OK**.

Chapter 9 Create and manage users

In order to protect an endpoint device, a user must be associated with the device. You can think of a user as an organizational tool for devices. You must decide which type of organizational user account strategy you want to implement.

- **Multiple user accounts**—With this strategy, you add multiple user accounts, and each account has one or more devices associated with that particular user. Use this strategy when devices are used by only one person.
- **Single user account**—With this strategy, you add a single user account, and many devices are assigned to that account. Use this strategy when devices are shared by many people.

You can implement a combination strategy to meet the needs of individually used devices and shared devices. You have multiple methods for adding user accounts, from manual entry to bulk uploads to automation using LDAP. In some cases, you can add the user when you deploy the end-user software on the devices.

Consider the following questions when determining how to add user accounts.

- How many user accounts do you need to add? If you have only a few user accounts to add, it may be quicker and easier to add them manually. If you have many accounts to add, you may want to use a bulk upload or automated method.
- Do you need to add groups of users? Grouping user accounts allows you to assign policies to groups to meet your requirements. If you are going to use groups, you may want to start with group creation before you add users. See *Create and manage groups* on page 63 for details.
- Which method do you plan to use when deploying the software to the endpoint devices? Deployment strategies can impact the user account creation strategy. For example, if you use LDAP, users can automatically be added in Carbonite Endpoint. See *Manage deployment* on page 45 and *Manage users with LDAP* on page 99 for details.

The following tasks are available for users:

- *View users* on page 69
- *View user details* on page 71
- *Add users* on page 73
- *Edit user settings* on page 78
- *View devices for a user* on page 79
- *Manage user permissions* on page 80
- *Reset a user password* on page 84
- *Delete a user* on page 85

If you want to manage users using System for Cross-domain Identity Management (SCIM), see *Manage users with SCIM* on page 85. If you want to manage users using Lightweight Directory Access Protocol (LDAP), see *Manage users with LDAP* on page 99.

If you want to automate user creation, see *Manage deployment* on page 45.

View users

To view users and their information, go to the **Users** page.

If the list exceeds the maximum number of results configured by your administrator, the table is blank and a dialog box displays, prompting you to use the **Search** function to narrow your results. You can click the link to view the limited list, or you can click **Download list** to export the entire list of users.

The screenshot shows the 'Users' page interface. At the top left, there is a 'Users' header with a home icon and a '+ Add user' button. To the right of the header is a 'Download list' button. Below the header, there is a search bar and a 'Show 10 entries' dropdown menu. The main content is a table with 10 rows of user data. The table columns are: First name, Last name, Email, Number of devices, Activated devices, Usage (GB), Login allowed, and Company. The table shows 10 users with IDs from 01 to 10. At the bottom of the table, there is a pagination control showing 'Showing 1 to 10 of 58 entries' and buttons for 'First', 'Previous', '1', '2', '3', '4', '5', '6', 'Next', and 'Last'.

First name	Last name	Email	Number of devices	Activated devices	Usage (GB)	Login allowed	Company
FirstName01	LastName01	email01@domain.com	0	0	0	No	CompanyName
FirstName02	LastName02	email02@domain.com	0	0	0	No	CompanyName
FirstName03	LastName03	email03@domain.com	0	0	0	No	CompanyName
FirstName04	LastName04	email04@domain.com	0	0	0	No	CompanyName
FirstName05	LastName05	email05@domain.com	0	0	0	No	CompanyName
FirstName06	LastName06	email06@domain.com	0	0	0	No	CompanyName
FirstName07	LastName07	email07@domain.com	0	0	0	No	CompanyName
FirstName08	LastName08	email08@domain.com	0	0	0	No	CompanyName
FirstName09	LastName09	email09@domain.com	0	0	0	No	CompanyName
FirstName10	LastName10	email10@domain.com	0	0	0	No	CompanyName

The following toolbar and table controls are available on the **Users** page.

- **Add user**—Click this button to add a single, new user. See *Add a single user* on page 73 for details.
- **Download list**—Click this button to download a complete user list to your local computer. You can download a Microsoft Excel (.xlsx) file or a comma-delimited file (.csv). If you download the Excel format, you must enable editing for any hyperlinks to the portal to be active.
- **Show Entries**—Specify the number of rows to be shown in the table on each page. Additional rows over the number you select are shown on additional pages and can be viewed by using the paging buttons at the bottom of the table.



This table is limited to 100 rows. If you need to see a list of all entries, use **Download list**.

- **Search**—Text entered in the box narrows the list displayed to only the rows that contain the search text. The search checks the entire table, not just the visible rows.
- **Sort**—You can sort the table by clicking on any column heading.
- **Table hyperlinks**—Hyperlinks in the table will take you directly to a page in the dashboard.
 - **First name, Last name, and Email**—Each of these hyperlinks opens the **User details** tab on the **User** page. See *View user details* on page 71 for details.

- **Number of devices**—This hyperlink opens the **Devices** page for that user. See *View device details* on page 118 for details.
- **Company**—This hyperlink opens the **Company** page. See *View and manage your company* on page 19 for details.
- **Table paging buttons**—The paging buttons at the bottom of the table allow you to move more quickly between pages. Each button jumps to that respective page of the table.

View user details

On the User details tab, you can view detailed information and perform administrative tasks for a user.

To view details for a user:

1. Go to the **Users** page and click the name of the user you want to view. See *View users* on page 69 for details on searching the user table.

The **User** page shows information for the user. Information appears on multiple tabs.

2. Click the **User details** tab to view information such the user's name, email, company, ID and policy. The tab also shows the user's Authentication setting, which indicates how the user logs in to the vault dashboard. The Authentication setting can be:
 - **Default**—The user logs in with an email address and password.
 - **SSO**—The user logs in using single sign-on credentials.
 - **2FA - Email**—Two-factor authentication is enforced for the user. The user does not have a mobile authenticator and must enter an authentication code from an email when logging in.
 - **2FA - Authenticator**—Two-factor authentication is enforced for the user. The user has set up a mobile authenticator and can enter an authentication code from the mobile authentication app when logging in.

On the User details tab, you can access other administrative functions for the user. See

Administrative tasks on the User details tab on page 72.

The screenshot shows the 'User details' tab for a user. At the top, there is a breadcrumb trail: 'Users / UserFirstName UserLastName'. Below this, the user's name 'User' is displayed next to a profile icon. A navigation bar contains three tabs: 'User details' (selected), 'Devices', and 'Permissions'. To the right of the tabs are three buttons: 'Move user', 'Delete user', and 'Edit user details'. The main content area is a table of user information:

User name:	UserFirstName UserLastName	Created at:	Oct 12 2021 03:21 PM
Email:	email01@domain.com	Last updated at:	Oct 12 2021 03:21 PM
Company:	CompanyName	Last logged in at:	Oct 12 2021 03:22 PM
User Id:	961d8074-a814-4f11-98c7-db76605a80d9	Custom 1:	
LDAP Id:	Not synchronized	Custom 2:	
Time zone:	(UTC-05:00) Eastern Time (US & Canada)	Custom 3:	
Authentication:	2FA - Email	Default policy set:	Base Policy (Inherited)
User group:	All users		

At the bottom, there are two buttons with descriptions:

- Reset password**: Resetting the password will pop a dialog and let the user change their password without using a passcode.
- Remove authenticator**: Removing the authenticator will force the user to authenticate by email at the next log in. The user can set up a new authenticator once logged in.

Administrative tasks on the User details tab

On the User details tab, you can click the following buttons and hyperlinks to perform administrative tasks for the user you are viewing:

- **Move user**—Click this button to move the user to a different group. Select the new group for the user and click **OK**.
- **Delete user**—This button is available if you have permissions. Click the button to delete the user. All information associated with the user (devices and backed up data) will be deleted. You must confirm that you want to delete the user and then click **OK**. See *Delete a user* on page 85 for details.
- **Edit user details**—Click this button to edit the user. You will not be able to change the company or user group, but you can change any other settings associated with the user. See *Add a single user* on page 73 for details on the user settings.
- Table hyperlinks—Click one of the following hyperlinks opens the corresponding page in the dashboard:
 - **Company**—This hyperlink opens the **Company** page. See *View and manage your company* on page 19 for details.
 - **User group**—This hyperlink opens the group details for a company. This is the same as going to the **Company** page, then to the **Groups** tab, and then clicking a group name hyperlink in the groups table. See *View group details* on page 64 for details.

- **Default policy set**—This hyperlink opens the **Edit policy details** page. This is the same as going to the **Company** page, then to the **Policies** tab, and then clicking a policy name hyperlink in the policies table. See *Edit an existing policy* on page 33 for details.
- **Reset password**—Click this button to send a new passcode to the user's email address. The user will be prompted to update the password after logging in with the temporary passcode. See *Reset a user password* on page 84 for details.
- **Remove authenticator**—If a user has lost access to their mobile authenticator, an administrator can click this button to remove the mobile authenticator. During the next login, the user must enter an authentication code from an email, and can then set up a new mobile authenticator. This button appears for a user when an administrator is logged in, 2FA is enforced for the user, and the user has set up a mobile authenticator.

Users can also remove their own mobile authenticators. For more information, see *Set up or remove a mobile authenticator* on page 13.

Add users

You can manually add individual user accounts or you can import names to add user accounts in bulk.

- *Add a single user* on page 73—You can manually add a single user. Use this method when you only have a few users to add.
- *Import multiple users* on page 76—You can bulk import multiple users. Use this method when you have many users to add, but you are not using an automated method.

If you want to manage users using Lightweight Directory Access Protocol (LDAP), see *Manage users with LDAP* on page 99. If you want to automate user creation, see *Manage deployment* on page 45.

Add a single user

Use this procedure to add a new user.

1. Click **Add user** from the **Company** or **Users** page.
2. On the **User** page, in the **Add user** section, define the details for the new user.

The screenshot shows a web interface for adding a new user. At the top, there is a breadcrumb trail: 'Users / Add user'. Below this is a header 'User'. The main content area is titled 'Add user' and contains a form with the following fields:

- Email:** EmailAddress@domainc.com
- Company:** CompanyName
- First name:** UserFirstName
- User group:** All users (dropdown menu)
- Last name:** UserLastName
- Time zone:** (UTC-05:00) Eastern Time (US & Canada) (dropdown menu)
- Custom 1:** (empty text box)
- Custom 2:** (empty text box)
- Custom 3:** (empty text box)

- **Email**—Enter a valid email address for the user.
 - **First name**—Enter the user's first name.
 - **Last name**—Enter the user's last name.
 - **Custom**—If desired, enter custom information in the three provided fields. These fields allow you to enter your own custom information. Each field is limited to 500 characters.
 - **Company**—This field is display only and shows the company to which the user will be assigned.
 - **User group**—Select the group the user should be a member of.
 - **Time zone**—Select the time zone in which the user is located. This is the time zone the user will see in the vault dashboard. All times, including the last backup and restore times, will appear in the logged in user's time zone.
3. In the **Permissions** section, define the settings for the new user.

The screenshot shows a 'Permissions' form with the following fields and values:

- Login to Dashboard:
- Send New User Email:
- Login to Access:
- Personal permission: Administrator
- Company permission: Administrator

Buttons: Compare roles, Add user, Cancel

- **Login to Dashboard**—Select this check box to allow ability to log in to the vault dashboard. Without this permission, the user cannot log in to the vault dashboard.
- **Send New User Email**—If you are granting the user access to the vault dashboard, enable this option to send a welcome email to the specified email address after the user is added. The email will contain a login link for the user.
- **Login to Access**—Enable this option if you want to grant the user the ability to log in to the web retrieval site. This site is sometimes referred to as the Access page because the URL is *portal RL/access*. For example, if you are using <https://red-us.mysecuredatavault.com>, the web retrieval site URL is <https://red-us.mysecuredatavault.com/access>. This web retrieval site allows users to restore their own data without using their device. Without this permission, users can only restore data from their own device if they have access to the end-user client software on their device. An administrator can also still restore the user's data using the vault dashboard, regardless of this setting.
- **Personal permission**—These permissions specify whether and how users can access their data and devices. The permissions available and what those permissions grant access to depend on the logins you have enabled for the user.

	If only Login to Dashboard is enabled	If only Login to Access is enabled	If both Login to Dashboard and Login to Access are enabled
Administrator	<ul style="list-style-type: none"> • Full access to the user's data and devices in the vault dashboard • No access to the web retrieval site 	Not applicable	<ul style="list-style-type: none"> • Full access to the user's data and devices in the vault dashboard • Full access to the user's data through the web retrieval site
Read Only	<ul style="list-style-type: none"> • Read-only access to the user's data and devices in the vault dashboard • No access to the web retrieval site 	Not applicable	<ul style="list-style-type: none"> • Read-only access to the user's data and devices in the vault dashboard • No access to web retrieval site
Retrieve Only	Not applicable	<ul style="list-style-type: none"> • No access to the vault dashboard • Full access to the user's data through the web retrieval site 	<ul style="list-style-type: none"> • No access to the vault dashboard • Full access to the user's data through the web retrieval site

If neither login is enabled, the user will not have access to the vault dashboard or to the web retrieval site.

- **Company permission**—These permissions determine what access the user has to the company, including policies and other users and devices.
 - **Administrator**—This permission provides full access to the vault dashboard. You should limit this role to as few people as possible because each user with this access has full control over everything.
 - **Backup Administrator**—This permission provides full access to all users and devices, but only partial access to other areas of the vault dashboard. This role might be appropriate for a service desk team member who can assist other users with retrieving data.
 - **Legal Administrator**—This permission provides full access to legal holds and admin restores, but read-only access to other areas of the vault dashboard. This role is appropriate for those responsible for retrieving data that is on legal hold.

- **Support**—This permission provides the ability to reset devices. Read-only access is granted to the rest of the vault dashboard.
- **Read Only**—This permissions provides read-only access to all parts of the vault dashboard, except legal holds.
- **None**—This permission hides company level information from a user that has access to log in to the vault dashboard.

	Administrator	Backup Administrator	Legal Administrator	Support	Read Only
Company	Full access	Cannot add, edit, or delete	Read only	Read only	Read only
Users	Full access	Full access except cannot delete email	Read only	Read only plus password resets	Read only
Devices	Full access	Full access	Read only plus admin restore	Read only plus reset device and admin restore	Read only
Legal Hold	Full access	No access	Full access	No access	No access
QuickCache	Full access	Full access except cannot delete	No access	Read only	Read only
Reports	Full access	Full access	Read only	Read only	Read only



To view this comparison table in the vault dashboard, **Compare Roles**. From there, you can click **More details** to see detailed tables of permissions.

4. When the user definition is complete, click **Add user**.

Import multiple users

Use the following instructions to import multiple, new users.

1. Go to the **Company** page and click the **Company details** tab.
2. Click **Import users**.
3. If you have not already done so, prepare your import file.
 - a. Download the template which is used for the import user process by clicking **Download template**.
 - b. Save and open the Excel (.xlsx) file.
 - c. Enable editing of the file.

- d. For each user you want to add, enter the user's information in one row of the spreadsheet in the **First Name**, **Last Name**, and **Email** columns. Do not enter any data in the remaining pre-defined columns, and do not modify the Row ID entries.
 - e. You can optionally create additional columns for additional, optional information. You can skip this step if you only want to enter the name and email for each user.
 - i. In the Excel spreadsheet, right-click the **Users** sheet name and click **Unhide**.
 - ii. Select the sheet named **Dictionary** and click **OK**. The **Dictionary** sheet defines how the template is used when importing both users and devices.
 - iii. For each additional, optional field defined that want to include in your import, enter the **Name**, exactly as defined in the **Dictionary**, in a new column on the **Users** sheet.
 - iv. Populate the new columns with data as desired. Cells in the new columns that are not populated will use the default value, if any.
 - f. Repeat adding a row for each additional user.
 - g. After you have added all of the users you want to import, save the file.
4. Select the file to import by clicking **Choose file**.
 5. Browse to and select your file and click **Open**.
 6. The imported file displays in the table at the bottom of the page. By default, all rows will be imported. If you only want to import specific users, select the specific users from the table by selecting the check box in that user's table row.



The following table controls are available for the import users table.

- **Show Entries**—Specify the number of rows to be shown in the table on each page. Additional rows over the number you select are shown on additional pages and can be viewed by using the paging buttons at the bottom of the table.
 - **Search**—Text entered in the box narrows the list displayed to only the rows that contain the search text. The search checks the entire table, not just the visible rows.
 - **Sort**—You can sort the table by clicking on any column heading.
 - **Table paging buttons**—The paging buttons at the bottom of the table allow you to move more quickly between pages. Each button jumps to that respective page of the table.
-
7. You have three choices after you have opened an import file.
 - **Start over**—Click this button to abort the import of the selected file or to import another file after completing an import.
 - **Perform import**—Click this button to import all rows or the selected rows.
 - **Validate import**—Click this button to validate all rows or the selected rows, without actually importing the users.
 8. When the import or validation is complete, the overall status displays at the top of the page. Click **Download results spreadsheet** and open the Excel file to see individual status for each user. You can edit and use this generated spreadsheet as the basis of another import, if desired.

Company Name / Import users

User

• Import complete. Overall status: Success [Download results spreadsheet](#)

Template Excel file: [Download template](#)

Input Excel file: Uploaded 'User-Bulk-Import-Template.xlsx'. Contents shown below.

Actions: All rows will be imported

[Start over](#) [Perform import](#) [Validate import](#)

Show entries Search:

	Row Id	First Name	Last Name	Email
<input type="checkbox"/>	1	FirstName01	LastName01	Email01@domain.com
<input type="checkbox"/>	2	FirstName02	LastName02	Email02@domain.com
<input type="checkbox"/>	3	FirstName03	LastName03	Email03@domain.com
<input type="checkbox"/>	4	FirstName04	LastName04	Email04@domain.com
<input type="checkbox"/>	5	FirstName05	LastName05	Email05@domain.com
<input type="checkbox"/>	6	FirstName06	LastName06	Email06@domain.com
<input type="checkbox"/>	7	FirstName07	LastName07	Email07@domain.com
<input type="checkbox"/>	8	FirstName08	LastName08	Email08@domain.com
<input type="checkbox"/>	9	FirstName09	LastName09	Email09@domain.com

Edit user settings

Use this procedure to edit a user's settings.

1. Go to the **Users** page and click the name of the user you want to edit. See *View users* on page 69 for details on searching the user table.
2. Click the **User details** tab and then click **Edit user details**.
3. You will not be able to change the company or user group, but you can change any other default setting associated with the user. See *Add a single user* on page 73 for details on the default user settings.

Users / FirstName01 LastName01 / Edit user

User

Edit user details

<p>Email: <input type="text" value="email01@domain.com"/></p> <p>First name: <input type="text" value="FirstName01"/></p> <p>Last name: <input type="text" value="LastName01"/></p> <p>Custom 1: <input type="text"/></p> <p>Custom 2: <input type="text"/></p> <p>Custom 3: <input type="text"/></p>	<p>Company: <input type="text" value="CompanyName"/></p> <p>User group: <input type="text" value="All users"/></p> <p>Password managed locally: <input type="checkbox"/></p> <p>Time zone: <input type="text" value="(UTC-05:00) Eastern Time (US & Canada)"/></p> <p>Default policy set: <input type="text" value="Inherit policy from CompanyName - 'Base P..."/></p> <p>2FA: <input checked="" type="radio"/> Enforced <input type="radio"/> Disabled</p>
---	--



If you need to change the group a user belongs to, go back to the **User details** and click **Move user**. Select the user group from the list and click **OK**.

4. If two-factor authentication (2FA) is enforced for the company, the user must enter an authentication code when logging in to the dashboard. If you want to override that setting for a user, set **2FA** to **Disabled**. The 2FA options do not appear if 2FA is disabled at the company level.
5. Click **Save changes**.

View devices for a user

Use this procedure to view the devices that are assigned to a user.

1. Go to the **Users** page and click the name of the user in the list. See *View users* on page 69 for details on searching the user table.

If the list exceeds the maximum number of results configured by your administrator, the table is blank and a dialog box displays, prompting you to use the **Search** function to narrow your list of results. You can click the link to view the limited list, if required.

2. Click the **Devices** tab to view details about each device associated with that user.

- **Add device**—Click this button to add a device for this user. See *Add a single device* on page 114 for details.
- **Show Entries**— Specify the number of rows to show on each page in the table. Additional rows over the number you select are shown on additional pages and can be viewed using the paging buttons at the bottom of the table. You can view a maximum of 100 rows in the table.
- **Search**—Text entered in the box narrows the list displayed to only the rows that contain the search text. The search checks the entire table, not just the visible rows.
- **Sort**—You can sort the table by clicking on any column heading.
- **Table hyperlinks**—The **Device name** hyperlink will take you to the **Device details** tab on the **Device** page. See *View device details* on page 118 for details.
- **Table paging buttons**—The paging buttons at the bottom of the table allow you to move more quickly between pages. Each button jumps to that respective page of the table.



The statistics on this page will not be populated until the first backup has been completed. You can see detailed processing information for the device, including a pending files statistic that is useful before and after the first backup has been completed, on the device **Activity** page. See *View device activity* on page 127 for details.

Manage user permissions

Use this procedure to manage user permissions.

1. Go to the **Users** page and click the name of the user you want to view. See *View users* on page 69 for details on searching the user table.
2. Click the **Permissions** tab on the **User** page.
3. Configure the following user permissions, as required.



If the user is synchronized with LDAP, some changes might be overwritten during the next LDAP synchronization. For more information, see *Configure LDAP synchronization* on page 104.

- **Login to Dashboard**—Select this check box to allow ability to log in to the vault dashboard. Without this permission, the user cannot log in to the vault dashboard.
- **Login to Access**—Enable this option if you want to grant the user the ability to log in to the web retrieval site. This site is sometimes referred to as the Access page because the URL is *portal RL/access*. For example, if you are using <https://red-us.mysecuredatavault.com>, the web retrieval site URL is <https://red-us.mysecuredatavault.com/access>. This web retrieval site allows users to restore their own data without using their device. Without this permission, users can only restore data from their own device if they have access to the end-user client software on their device. An administrator can also still restore the user's data using the vault dashboard, regardless of this setting.
- **Personal permission**—These permissions specify whether and how users can access their data and devices. The permissions available and what those permissions grant access to depend on the logins you have enabled for the user.

	If only Login to Dashboard is enabled	If only Login to Access is enabled	If both Login to Dashboard and Login to Access are enabled
--	--	---	--

Administrator	<ul style="list-style-type: none"> • Full access to the user's data and devices in the vault dashboard • No access to the web retrieval site 	Not applicable	<ul style="list-style-type: none"> • Full access to the user's data and devices in the vault dashboard • Full access to the user's data through the web retrieval site
Read Only	<ul style="list-style-type: none"> • Read-only access to the user's data and devices in the vault dashboard • No access to the web retrieval site 	Not applicable	<ul style="list-style-type: none"> • Read-only access to the user's data and devices in the vault dashboard • No access to web retrieval site
Retrieve Only	Not applicable	<ul style="list-style-type: none"> • No access to the vault dashboard • Full access to the user's data through the web retrieval site 	<ul style="list-style-type: none"> • No access to the vault dashboard • Full access to the user's data through the web retrieval site

If neither login is enabled, the user will not have access to the vault dashboard or to the web retrieval site.

- **Admin role(s)**—If a user has been granted **Login to Dashboard** access, an additional section is available at the bottom of the **Permissions** tab for **Admin role(s)**. This table shows you the permissions, if any, assigned to the user for company and group access.
 - **Add role**—Click this button to add a new role to the user's permissions.
 - **Organization**—Select the company or group this user should be assigned to.
 - **Role**—Select the role the user should have assigned.
 - **Administrator**—This permission provides full access to the vault dashboard. You should limit this role to as few people as possible because each user with this access has full control over everything.
 - **Backup Administrator**—This permission provides full access to all users and devices, but only partial access to other areas of the vault dashboard. This role might be appropriate for a service desk team member who can assist other users with retrieving data.
 - **Legal Administrator**—This permission provides full access to legal holds and admin restores, but read-only access to other areas of the vault dashboard. This role is appropriate for those responsible for retrieving data that is on legal hold.
 - **Support**—This permission provides the ability to reset devices. Read-only access is granted to the rest of the vault dashboard.

- **Read Only**—This permissions provides read-only access to all parts of the vault dashboard, except legal holds.
- **None**—This permission hides company level information from a user that has access to log in to the vault dashboard.

	Administrator	Backup Administrator	Legal Administrator	Support	Read Only
Company	Full access	Cannot add, edit, or delete	Read only	Read only	Read only
Users	Full access	Full access except cannot delete email	Read only	Read only plus password resets	Read only
Devices	Full access	Full access	Read only plus admin restore	Read only plus reset device and admin restore	Read only
Legal Hold	Full access	No access	Full access	No access	No access
QuickCache	Full access	Full access except cannot delete	No access	Read only	Read only
Reports	Full access	Full access	Read only	Read only	Read only



To view this comparison table in the vault dashboard, **Compare Roles**. From there, you can click **More details** to see detailed tables of permissions.

Click **OK** to apply the role.

- **Show Entries**—Specify the number of rows to be shown in the table on each page. Additional rows over the number you select are shown on additional pages and can be viewed by using the paging buttons at the bottom of the table.



This table is limited to 100 rows. If you need to see a list of all entries, use **Download list**.

- **Search**—Text entered in the box narrows the list displayed to only the rows that contain the search text. The search checks the entire table, not just the visible rows.
- **Sort**—You can sort the table by clicking on any column heading.

- **Table hyperlinks**—Click an action hyperlink to delete or edit an assigned role.
 - **Remove rule**—Click this link to remove the role from the user's permissions.
 - **Change role**—Click this link to change the role for the specified company or group
- **Table paging buttons**—The paging buttons at the bottom of the table allow you to move more quickly between pages. Each button jumps to that respective page of the table.

Reset a user password

Use this procedure to reset a user password. This process sends a temporary passcode to the user's email address. The user is prompted to update the password after logging in with the temporary passcode.

1. Go to the **Users** page and click the name of the user. See *View users* on page 69 for details on searching the user table.
2. Click the **User details** tab and click **Reset password**.

The screenshot shows a user profile page with the following details:

- User name:** UserFirstName UserLastName
- Email:** email01@domain.com
- Company:** CompanyName
- User Id:** 961d8074-a814-4f11-98c7-db76605a80d9
- LDAP Id:** Not synchronized
- Time zone:** (UTC-05:00) Eastern Time (US & Canada)
- Authentication:** 2FA - Email
- User group:** All users
- Created at:** Oct 12 2021 03:21 PM
- Last updated at:** Oct 12 2021 03:21 PM
- Last logged in at:** Oct 12 2021 03:22 PM
- Default policy set:** Base Policy (Inherited)

At the bottom of the page, there are two buttons:

- Reset password:** Resetting the password will pop a dialog and let the user change their password without using a passcode
- Remove authenticator:** Removing the authenticator will force the user to authenticate by email at the next log in. The user can set up a new authenticator once logged in.

3. Click **OK** to email the temporary passcode to the user.
4. Ensure that the user clicks the **User Passcode** link in the Login dialog box. After the user logs in, Carbonite Endpoint prompts them to update their password.

Delete a user

Use this procedure to delete a user. When you delete a user, everything associated with the user (devices and backed up data) will be deleted.

1. Go to the **Users** page and click the name of the user. See *View users* on page 69 for details on searching the user table.
2. Click the **User details** tab and click **Delete user**. If you do not see this button, you do not have permissions to delete users.
3. Confirm that you want to delete the user and click **OK**.

Enable a disabled user

Use this procedure to enable a disabled user. If a user account has been disabled in the identity management system (using LDAP or SCIM protocol, for example), you can re-enable them on the **User details** page.

1. Go to the **Users** page and click the name of the user. See *View users* on page 69 for details on searching the user table.
2. Click the **User details** tab and click **Enable user**. If you do not see this button, the user has not been disabled in the identity management service.
3. Confirm that you want to delete the user and click **OK**.

User details		Devices		Permissions	
This user is disabled. They cannot login until they are enabled by the button below.					
				Move user Delete user Edit user details	
User name:	UserFirstName LastNameFromAzure	Created at:	Jun 06 2023 10:43 AM		
Email:	userPrincipalNameFromAzure@55bz2z.onmicrosoft.com	Last updated at:	Jun 07 2023 08:13 AM		
Company:	Company1	Last logged in at:			
Partner:	Partner	Custom 1:	City from Azure		
User id:	92cefa3f-587a-4ce8-9bb9-c6fe54b34cf4	Custom 2:	Company from Azure		
LDAP id:	Not synchronized	Custom 3:	Job title from Azure		
Time zone:	(UTC-05:00) Eastern Time (US & Canada)	Default policy set:	Base Policy (Inherited)		
Authentication:	Default				
User group:	Group1				
Last password reset code:	User login disabled				
Enable user		User has been disabled. Enable the user again. This will automatically activate suspended devices.			

The disabled user is now re-enabled.

Manage users with SCIM

If you set up SCIM synchronization, you can manage Carbonite Endpoint users using Microsoft® Azure® Active Directory (Azure AD) or Okta® Universal Directory.

SCIM (System for Cross-domain Identity Management) is an open standard for exchanging user data between an organization's identity provider and applications. Using SCIM synchronization, users can be automatically added and updated in Carbonite Endpoint based on their information in Azure AD or Okta Universal Directory. Users can be assigned roles and assigned to groups, allowing you to apply unique backup policies to different groups of users.

To set up SCIM synchronization, you must first create an API user in Carbonite Endpoint and create a SCIM access token. See *Create an API user and SCIM access token in Carbonite Endpoint* on page 86.

You can then set up SCIM synchronization using the Azure Portal or Okta Admin Console. For more information, see *Set up SCIM synchronization with Azure AD* on page 87 or *Set up SCIM synchronization with Okta* on page 93.

Create an API user and SCIM access token in Carbonite Endpoint

Before you can synchronize users with Azure AD or Okta Universal Directory, you must create an API user and SCIM access token in the Carbonite Endpoint vault dashboard. The API user must be in the company where you want to add and update users using SCIM, and must have Company Administrator permissions.

After you create a SCIM access token, you can set up SCIM synchronization using the Azure Portal or Okta Admin Console. For more information, see *Set up SCIM synchronization with Azure AD* on page 87 or *Set up SCIM synchronization with Okta* on page 93.

1. In the vault dashboard, do the following to create a company administrator with company administrator access:
 - a. When logged in to the vault dashboard as a company administrator, click **Add user** on the **Users** page or on a company page.
 - b. On the **User** page, in the **Add user** section, enter the email address and other information for the user.
 - c. In the **Company** list, ensure that your company name appears.



If you are signed in as a partner administrator, you are able to select the company to which you want to add and update users.

- d. In the **Permissions** section, select the **Login to Dashboard** check box.
 - e. In the **Personal permission** list, choose **Administrator**. In the **Company permission** list, choose **Administrator**.
 - f. Click **Add User**, and then click **OK**.
2. Contact [Customer Support](#) to enable API access for the user you created in [Step 1](#).
 3. In the vault dashboard, do the following to create a SCIM access token for the user you created in [Step 1](#).
 - a. When logged in to the vault dashboard as a system administrator, click **Users**, and then click the user that you created in [Step 1](#).
 - b. Click the user's **Key management** tab.

- c. Click **Create SCIM access token**. A **SCIM access token** page shows the SCIM access token. Click **Copy SCIM access token** and save the access token somewhere safe.



The SCIM access token will only be displayed once. Make sure you save the SCIM access token somewhere safe.

- d. Click **Close**. The **Key management** page now shows the date when the SCIM access token was created.

You can now set up SCIM synchronization using the Azure Portal or Okta Admin Console. For more information, see *Set up SCIM synchronization with Azure AD* on page 87 or *Set up SCIM synchronization with Okta* on page 93.

Set up SCIM synchronization with Azure AD

If you use Microsoft Azure Active Directory (Azure AD) to manage users in your company, you can set up SCIM synchronization to automatically add and update users in Carbonite Endpoint based on information in Azure AD. You can also assign roles to users and assign users to groups. When SCIM synchronization is set up with Azure AD, users are synchronized in Carbonite Endpoint almost immediately after they are created or updated in Azure AD.

Before setting up SCIM synchronization with Azure AD, you must create a SCIM access token in the vault dashboard. See *Create an API user and SCIM access token in Carbonite Endpoint* on page 86.

You can then set up SCIM synchronization with Azure AD using the following procedure in the Azure Portal. For ease of use, the procedure is divided into three sections:

- *Create an application in Azure AD* on page 87
- *Add required attributes and map values to the SCIM application* on page 88
- *Set up and test user provisioning* on page 91

Procedures in the Azure Portal may change. For current information, see SCIM synchronization information in [Microsoft Azure Active Directory documentation](#).

Create an application in Azure AD

1. In the Azure Portal, go to **Azure Active Directory**.
2. In the **Manage** list, click **Enterprise applications**.
3. Click **New application**.
4. Click **Create your own application**. In the **Create your own application** box, type a name for your application (e.g., EndpointIntegration). Leave **Integrate any other application you don't find in the gallery (Non-Gallery)** selected, and click **Create**.
5. After the application is created, click **Provisioning** in the **Manage** list.
6. Click **Get Started**.
7. In the **Provisioning Mode** list, choose **Automatic**.
8. In the **Tenant URL** box, enter the following: `vaultDashboardURL/api/scim`

Where `vaultDashboardURL` is the URL of your vault dashboard.

If your vault is not hosted in Azure, enter: `vaultDashboardURL/dashboard/api/scim`

- In the **Secret Token** box, type the SCIM access token that you created in the vault dashboard. See *Create an API user and SCIM access token in Carbonite Endpoint* on page 86.
- Click **Test Connection**.

If a message states that the supplied credentials are authorized to enable provisioning, click **Save**.

If the connection does not succeed, please check notifications in the Azure Portal for more information. Fix any issues and test the connection again.

Add required attributes and map values to the SCIM application

- After saving the credentials, click **Mappings** to expand the Mappings area.
- Click **Provision Azure Active Directory Groups**. On the **Attribute Mapping** page, in the **Enabled** toggle, click **No**. Click **Save**, click **Yes** to save the changes, and then click the **Close** button (X).

If users in the company are assigned to groups, you can map users to groups later in this procedure.

- Click **Provision Azure Active Directory Users**.
- In the **Attribute Mappings** area, keep the following four mappings:

- UserPrincipalName**
- Switch([IsSoftDeleted], , "False", "True", "True", "False")**
- givenName**
- surName**

Click the **Delete** button for every mapping except the four listed above.

- Select the **Show Advanced Options** check box, and then click **Edit attribute list for customappsso**.
- In the empty row at the bottom of the list, enter each of the four attributes shown in the table below.

	Name	Type	Required?
Attribute 1	urn:ietf:params:scim:schemas:extension:CustomExtensionName:2.0:User:CustomAttribute1	String	No
Attribute 2	urn:ietf:params:scim:schemas:extension:CustomExtensionName:2.0:User:CustomAttribute2	String	No
Attribute 3	urn:ietf:params:scim:schemas:extension:CustomExtensionName:2.0:User:CustomAttribute3	String	No
Attribute 4	urn:ietf:params:scim:schemas:extension:CustomExtensionName:2.0:User:CanLoginToAccessAttribute	Boolean	Yes

17. Click **Save**, click **Yes** to save the attributes, and then click the **Close** button (X) .
18. Do the following to add each of the mappings shown in the table below:
 - a. Click **Add New Mapping**.
 - b. In the **Source attribute** list, choose the source attribute from the table below.
 - c. In the **Target attribute** list, choose the target attribute from the table below.
Leave the default values in the remaining fields.
 - d. Click **OK**.



The custom attributes in the table below are examples; you can create your own mappings that suit your environment. For more information, see [Create custom attributes in Microsoft Azure AD](#).

Source attribute	Target attribute	Required?
employeeType	userType ¹	No
mobile	timezone ²	No
city	CustomAttribute1	No
companyName	CustomAttribute2	No
jobTitle	CustomAttribute3	No
employee ID	CanLoginToAccessAttribute	Yes

¹**userType** refers to the Company Permission role that will be assigned to each created user. If blank, the created users will have no company level access. For valid values, see [Employee type values](#).

²If the **timezone** is not specified, the system will default to the timezone of the user which the SCIM Access token is tied to.

19. If users in your company are assigned to groups in Carbonite Endpoint, click **Add New Mapping**. In the **Source attribute** list, choose **department**. In the Target attribute list, choose **urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:organization**. Click **OK**.

If users in your company are not assigned to groups in Carbonite Endpoint, do not set up this mapping.

20. Click **Save**, click **Yes** to save the changes, and then click the **Close** button (X) .

When you are finished, the Attribute Mappings table should include the following rows:

Azure Active Directory Attribute	customappsso Attribute	Required	Field in Carbonite Endpoint UI
---	-------------------------------	-----------------	---------------------------------------

UserPrincipalName	userName (Must be an email address)	Yes	Email address on User details page
Switch ([IsSoftDeleted], 'False', "True", "True", "False")	active	Yes	
givenName	name.givenName	Yes (givenName OR surname is required)	User name field on User details page
surname	name.familyName	Yes (givenName OR surname is required)	
employeeType	userType	No	Company Role in the Permissions tab on User details page
mobile	timezone	No	Timezone on User details page
city	urn:ietf:params:scim:schemas:extension:CustomExtensionName:2.0:User:CustomAttribute1	No	Custom 1 field on User details page

companyName	urn:ietf:params:scim:schemas:extension:CustomExtensionName:2.0:User:CustomAttributes2	No	Custom 2 field on User details page
jobTitle	urn:ietf:params:scim:schemas:extension:CustomExtensionName:2.0:User:CustomAttributes3	No	Custom 3 field on User details page
employeeId	urn:ietf:params:scim:schemas:extension:CustomExtensionName:2.0:User:CanLoginToAccessAttribute	Yes	Login to access in the Permissions tab on User details page
department	urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:organization	If your company uses groups, you will add this field.	



You can also customize fields in Azure and create your own customer extensions.

21. Click the **Close** button (X) to close the Provisioning page.

Set up and test user provisioning

22. On the **Overview** page, under **Manage provisioning**, click **Add scoping filters**.
23. Click **Settings** to expand the Settings area.
24. In the **Scope** list, choose **Sync all users and groups**.



In some cases, you might not want to select the filter **Sync all users and groups**, for example, if your company has a large number of users. If you do not want to sync all of your users to Carbonite Endpoint, you can limit synced users. For more information, see: [Scoping users or groups to be provisioned with scoping filters](#)

25. In the **Provisioning Status** toggle, click **Off**, and then click **Save**.
26. Click the **Close** button (X) to close the Provisioning page.

27. Edit a user in Azure AD to enter values that are mapped to Carbonite Endpoint:
 - a. In the Azure Portal, go to **Azure Active Directory**. Click **Users**.
 - b. Select a User, and then click **Edit Properties**.
 - c. Edit any of the following properties that are mapped to Carbonite Endpoint:
 - First name
 - Last name
 - User principal name
 - Job title—Enter a value for Custom Attribute 3 in Carbonite Endpoint.
 - Company name —Enter a value for Custom Attribute 2 in Carbonite Endpoint.
 - Department—Enter the user's Group name in Carbonite Endpoint. Leave this field blank if users are not assigned to groups in your company in Carbonite Endpoint.
 - Employee ID—Specify whether the user can log in to the Carbonite Endpoint Access site. Valid values are true and false.
 - Employee type—Enter the user's company permission in Carbonite Endpoint. Valid values are:
 - Administrator
 - Backup Administrator
 - Legal Administrator
 - Support
 - Read OnlyLeave the field blank for None.
 - City—Enter a value for Custom Attribute 1 in Carbonite Endpoint.
 - Mobile phone—Enter the user's time zone. Valid values are Windows time zones.
 - Account enabled—Specify whether the user's account is enabled.



If a provided value is not valid, the user will not be provisioned in Carbonite Endpoint.

- d. Click **Save**.
28. When viewing the SCIM application in the Azure Portal, click **Provisioning**, and then click **Provision On Demand**. Type the name of the user that you edited, and then click **Provision**.

The new user should appear almost immediately in the vault dashboard. If you edit the user's information in Azure AD and provision the user again, the user will be updated in the vault dashboard.

If the new user does not appear in the vault dashboard, please check notifications in the Azure Portal for more information. Fix any issues and try the provisioning again.

29. After a user has been successfully provisioned in Carbonite Endpoint, you can assign other users and groups to the SCIM application and turn on full provisioning. To turn on provisioning, in the Azure Portal, click **Enterprise applications**, click your project, click **Provisioning**, and then click **Start provisioning**. This will provision all your users.

Set up SCIM synchronization with Okta

If you use Okta Universal Directory to manage users in your organization, you can set up SCIM synchronization to automatically add and update users in Carbonite Endpoint based on information in Okta. You can also assign roles to users and assign users to groups. When SCIM synchronization is set up with Okta, users are synchronized in Carbonite Endpoint almost immediately after they are created or updated in Okta.

Before setting up SCIM synchronization with Okta Universal Directory, you must create a SCIM access token in the vault dashboard. See *Create an API user and SCIM access token in Carbonite Endpoint* on page 86.

You can then set up SCIM synchronization with Okta using the following procedure in the Okta Admin Console. For ease of use, the procedure is divided into four sections:

- *Add a SCIM application in Okta* on page 93
- *Specify a time zone value* on page 94
- *Add required attributes and map values to the SCIM application* on page 94
- *Assign the SCIM application to users and test the integration* on page 96

Procedures in the Okta Admin Console may change. For current information, see App integrations and User management information in the [Okta Help Center](#).

Add a SCIM application in Okta

1. In the Okta Admin Console, go to **Applications > Applications**.
2. Click **Browse App Catalog**. Search for the following: SCIM 2.0
3. Click **SCIM 2.0 Test App (OAuth Bearer Token)**, and then click **Add Integration**.
4. In the **Application label** box, add a label for the SCIM application. Leave **Do not display application icon to users** cleared. Leave **Automatically log in when user lands on login page** selected. Click **Next**.
5. In **Sign-On Options**, select **Secure Web Authentication**, and then select **User sets username and password**. In the **Application username format** list, leave **Okta username**.



The username value must be in the form of an email address, and this value is required.

In the **Update application username** list, leave **Create and update**. Leave the **Password reveal** check box selected. Click **Done**.

6. Click the **Provisioning** tab for the application, and then click **Configure API Integration**.
7. Select the **Enable API integration** check box, and specify the following settings:

- In the **Tenant URL** box, enter the following: `vaultDashboardURL/api/scim`
Where `vaultDashboardURL` is the URL of your vault dashboard.
If your vault is not hosted in Azure, enter: `vaultDashboardURL/dashboard/api/scim`
- **OAuth Bearer Token**—Enter the SCIM access token that you created in the vault dashboard. See *Create an API user and SCIM access token in Carbonite Endpoint* on page 86.

8. Click **Test API Credentials**.

If a message states that the application was verified successfully, click **Save**.

If a message states that an error occurred, please fix any issues and test the connection again.

9. In the Okta to SCIM settings, click **Edit**. Select the **Enable** check box for each of the following:
- **Create Users**
 - **Update User Attributes**
 - **Deactivate Users**

Leave the **Enable** check box for **Sync Password** cleared.

10. Click **Save**.

Specify a time zone value



Time zone values in Okta are different than in Carbonite Endpoint and could cause user provisioning to fail. For this reason, this procedure describes how to assign one time zone value (Eastern Standard Time) for all users. Alternatively, you can create a custom function that maps Okta timezones to .NET values accepted by Carbonite Endpoint.

11. In the **Attribute Mappings** section at the bottom of the page, click the pencil for the **Time zone** attribute.

In the Time zone dialog box, in the **Attribute value** list, choose **Same value for all users**. In the empty field, enter the following: `Eastern Standard Time`



If the **timezone** is not specified, the system will default to the timezone of the user which the SCIM Access token is tied to.

12. Click **Save**.

Add required attributes and map values to the SCIM application

13. In the Okta Admin Console, go to **Directory > Profile Editor**.
14. Click the SCIM application that you created in *Add a SCIM application in Okta* on page 93.
15. In the **Attributes** section, click **Add Attribute**.



The custom attributes in the table below are examples only; you can create your own mappings that suit your environment. For more information, see [Map custom attributes in Okta](#).

16. Using the **Add Attribute** page, add each of the attributes shown in the following table. Click **Save and Add Another** after adding each attribute. Click **Cancel** after you have added all four attributes.

	Attribute 1	Attribute 2	Attribute 3	Attribute 4 - Required
Data type	string	string	string	boolean
Display name	Custom1	Custom2	Custom3	CanLoginToAccessAttribute
Variable name	CustomAttribute1	CustomAttribute2	CustomAttribute3	CanLoginToAccessAttribute
External name	CustomAttribute1	CustomAttribute2	CustomAttribute3	CanLoginToAccessAttribute
External namespace	urn:ietf:params:scim:schemas:extension:CustomExtensionName:2.0:User			
Scope	Select the User personal check box.			
User Permission	Select the Read Only option.			

17. In the **Profile Editor**, in the **Attributes** section, click **Mappings**.
18. Click the **Okta User to SCIM 2.0 Test App** tab. A green arrow appears on the tab for each Okta field that is mapped to a field in the SCIM application.
19. Leave the green arrow for the following mappings:
- user.firstName → givenName
 - user.lastName → familyName
 - "Eastern Standard Time" → timezone
 - user.userType → userType
 - user.organization → organization

Map the following fields to the custom attributes you created in *Set up SCIM synchronization with Okta* on page 93.

- user.city → CustomAttribute1
- user.employeeNumber → CustomAttribute2

- user.division → CanLoginToAccessAttribute
- user.department → CustomAttribute3

For the remaining fields, click the green arrow and choose **Do not map**.

20. Click **Save Mappings** and then click **Don't apply updates**.

Assign the SCIM application to users and test the integration

21. In the Okta Admin Console, go to **Directory > People**.

22. Click a user that you want to synchronize with Carbonite Endpoint.

23. Edit the user to enter values that are mapped to Carbonite Endpoint:

- Click the user's **Profile** tab.
- Click **Edit**.
- Edit any of the following attributes that are mapped to Carbonite Endpoint:
 - Username
 - First name
 - Last name
 - City—Enter a value for Custom Attribute 1 in Carbonite Endpoint.
 - User type—Enter the user's Company permission in Carbonite Endpoint. Valid values are:
 - Administrator
 - Backup Administrator
 - Legal Administrator
 - Support
 - Read Only

Leave the field blank for None.

- Employee number—Enter a value for Custom Attribute 2 in Carbonite Endpoint.
- Organization—Enter the user's Group name in Carbonite Endpoint. Leave the field blank if users are not assigned to groups in your company in Carbonite Endpoint.
- Division—Specify whether the user can log in to the Carbonite Endpoint Access site. Valid values are true and false.
- Department —Enter a value for Custom Attribute 3 in Carbonite Endpoint.



If a provided value is not valid, the user will not be provisioned in Carbonite Endpoint.

d. Click **Save**.

24. Summary of user values in Carbonite Endpoint:

Otka Attribute	SCIM Attribute	Required	Field in Carbonite Endpoint UI
Username	userName (Must be an email address)	Yes	Email address on User details page
Active flag	active	Yes	The active flag passed automatically if the user is included in the application
firstName	name.givenName	Yes (givenName OR surname is required)	User name field on User details page
lastName	name.familyName	Yes (givenName OR surname is required)	
userType	userType	No	Company Role in the Permissions tab on User details page

timezone	timezone	No	Timezone on User details page
city	urn:ietf:params:scim:schemas:extension:CustomExtensionName:2.0:User:CustomAttributes1	No	Custom 1 field on User details page
employeeNumber	urn:ietf:params:scim:schemas:extension:CustomExtensionName:2.0:User:CustomAttributes2	No	Custom 2 field on User details page
department	urn:ietf:params:scim:schemas:extension:CustomExtensionName:2.0:User:CustomAttributes3	No	Custom 3 field on User details page
division	urn:ietf:params:scim:schemas:extension:CustomExtensionName:2.0:User:CanLoginToAccessAttribute	Yes	Login to access in the Permissions tab on User details page
organization	urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:organization	If your company uses groups, you will add this field.	

25. On the user's **Applications** tab, click the **Assign Applications** button.
26. In the **Assign Applications** box, click **Assign** beside the application you created in [Add a SCIM application in Okta](#).
27. Scroll to the bottom of the box, click **Save and Go Back**, then click **Done**. As soon as you add the user to the application, the user will be provisioned, and any changes moving forward will automatically be applied.

Manage users with LDAP

If you are using Lightweight Directory Access Protocol (LDAP), you can manage Carbonite Endpoint users by synchronizing Carbonite Endpoint and LDAP. This will add and disable users based on their status in your LDAP company directory. You can assign users to user groups based on LDAP queries, allowing you to apply unique backup policies to the different groups of users, and assign Admin roles to users based on LDAP queries.

See the following sections for LDAP synchronization tasks.

- *LDAP requirements* on page 99
- *Install the LDAP agent* on page 102
- *Configure LDAP synchronization* on page 104
- *Monitor and troubleshoot LDAP synchronization* on page 108

LDAP requirements

In order to use the LDAP feature, you must meet the following requirements and caveats.

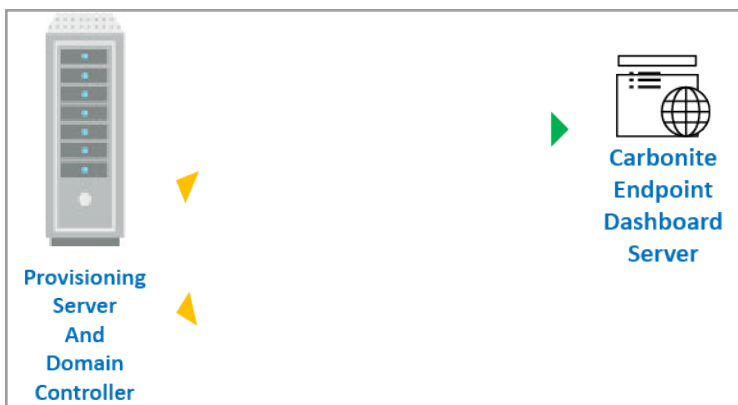
- **Provisioning server**—You must have a physical or virtual server for the provisioning server.
 - **Operating system**—The provisioning server must be running Windows 2016 or later.
 - **Microsoft .NET**—The provisioning server must be running Microsoft .NET version 4.7.2 or later.
 - **Availability**—The provisioning server does not need to be a high availability server. Carbonite Endpoint backups will function if the provisioning server is offline. However, user updates (add, move, disable) will be deferred until the provisioning sever is online.
 - **Colocation**—Your provisioning server and domain controller can be the same server or separate servers. See the sample configurations below.
 - **Network routes**—The provisioning server must have network routes between the server and the Carbonite Endpoint dashboard and between the server and a domain controller, a read-only domain controller, or another queryable LDAP server. See the sample configurations below.
 - **Ports**—Use the following ports for communication. See the sample configurations below.
 - Use LDAP on port 389 or LDAPS on port 636 for communication from the provisioning server to the domain controller.
 - Use TLS port 443 for communication from the provisioning server to the Carbonite Endpoint dashboard.
- **Account**—You must have an LDAP service account that has query rights in the search root you intended to use.
- **Single sign-on**—If you are using single sign-on (SSO) and have removed a user, the user will not be able to log in to Carbonite Endpoint even if the LDAP query to modify Carbonite Endpoint has not be executed yet, because the user will not be able to authenticate through SSO. However, if you add a user to SSO, you must run the LDAP query to add the user to Carbonite Endpoint before the user can log in, because SSO does not automatically add an account for the user in Carbonite Endpoint.

- **Multiple domains**—Keep in mind the following if you have multiple domains.
 - You should query domain controllers on a per-domain basis rather than a single global catalog across domains.
 - You should add a Carbonite Endpoint company for each domain and have a provisioning server for each company/domain. If that is not possible, you may have to reassign users to the correct company after they are added.
 - You may need to modify the search root for a per-user query.

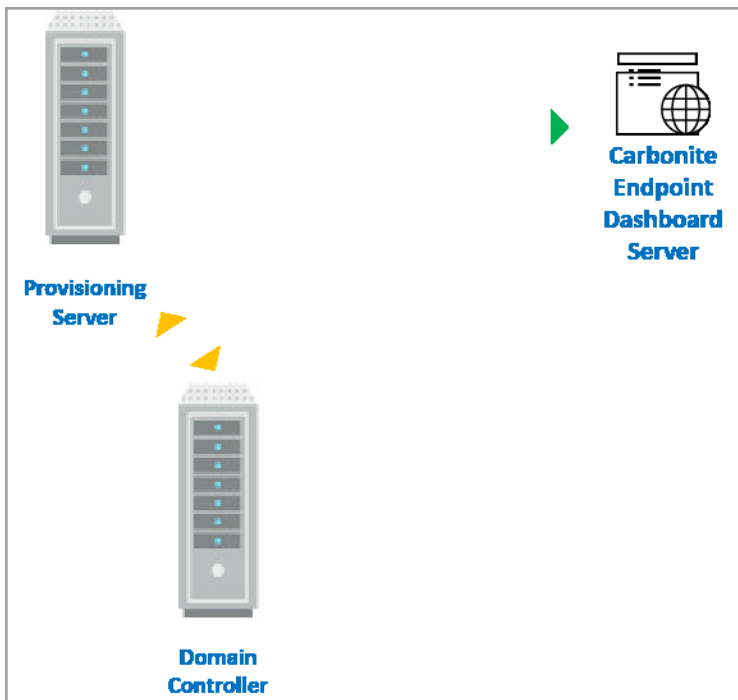
Sample configurations

Three of the most common LDAP configurations are:

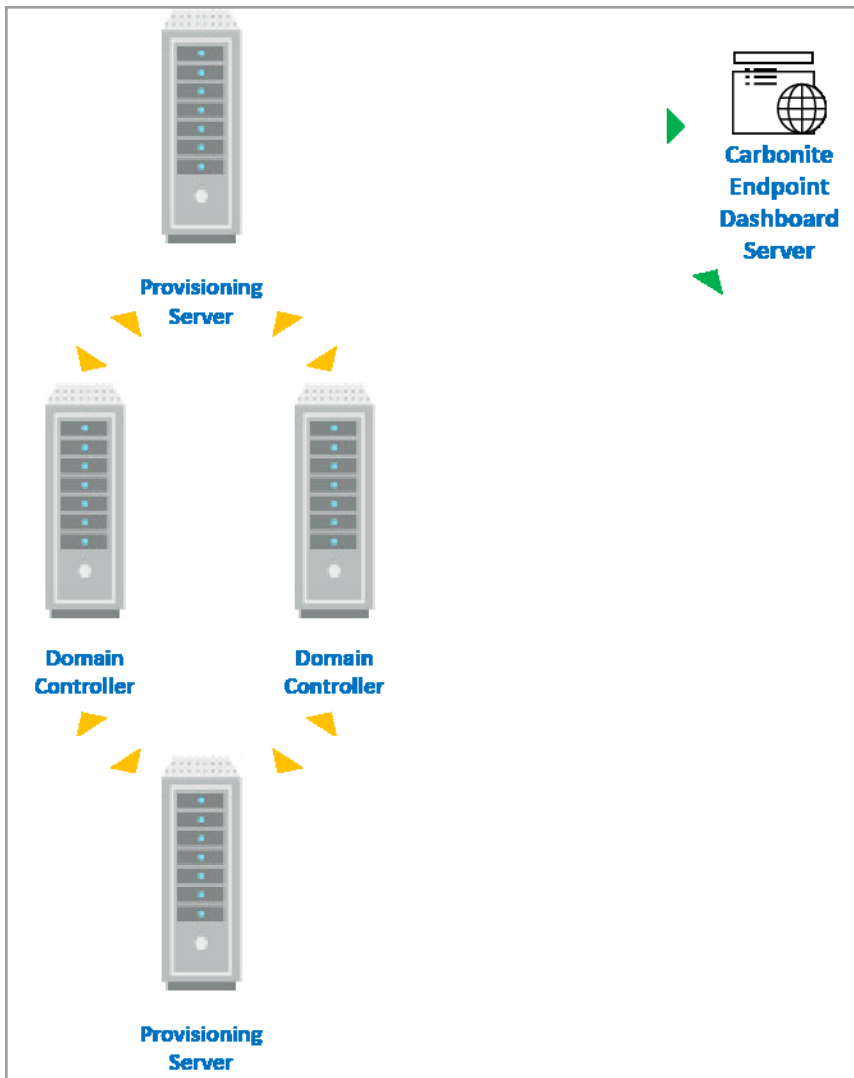
- Provisioning server installed on the domain controller





- Provisioning server separate from the domain controller



- Multiple provisioning servers and domain controllers



Complex scenarios, like multiple domains, may be referred to Professional Services for further assistance.

Component to Component	Communication and Port	Arrow Color
Provisioning Server to Domain Controller Domain Controller to Provisioning Server	LDAP port 389 or LDAPS port 636	
Provisioning Server to Carbonite Endpoint dashboard	TLS port 443	

Install the LDAP agent

Use this procedure to install the LDAP agent on your provisioning server. See *LDAP requirements* on page 99 for sample configurations.

1. On the **Company** page, click the **LDAP/SCIM synchronization** tab.
2. Select your next step depending on whether you have previously configured LDAP synchronization or not.
 - **No previous configuration**—Use the following steps if you have not previously configured LDAP synchronization.
 - a. Review the overview information and the requirements and click **Get Started**.
 - b. Review the **Getting Started** process outlined at the top of the **Synchronization status** section.
 - c. Click **Install and Activate the LDAP Synchronization Agent** to display the **Synchronization agents** section. You can also scroll down to that section.
 - **Previous configuration**—If you have previously configured LDAP synchronization, scroll down to the **Synchronization agents** section.
3. Click **Download installer** and then click the **For Windows** .msi link to save a copy of the installation file for the LDAP synchronization agent. Close the dialog box after the download is complete.
4. Copy an **Activation Code** with an **Available** status from the table and copy the **LDAP Activation URL** from under the table. You will need this information when you install the LDAP synchronization agent.

Name	Activation Code	Last online	Status/State	Manage
LDAP Sync Agent	1F7B-3BB9-CC6F-5EC0-E0A7	Jul 18 2019 03:57 PM	Activated	Edit
LDAP Sync Agent Secondary	86E9-5E2D-BAE8-B03D-BB27		Available	Edit

LDAP Activation URL: <https://mysecuredatavault.com>

[Return to top](#)

5. On your provisioning server, install the LDAP synchronization agent using the downloaded file.



If your LDAP agent needs to use a proxy server for communication, use the alternate instructions at the end of this section to install the agent.

- a. Review and accept the Terms of Service and click **Next** to continue
- b. If desired, change the destination folder and click **Next** to continue.
- c. Enter the **LDAP Activation URL** and **Activation Code** that you copied earlier and click **Next** to continue.

- d. Click **Install**.
 - e. When the installation is complete, click **Close**.
6. Verify that the **Status** of the agent is changed to **Activated**. Review the following if it is not.
- Make sure the provisioning server can access the Carbonite Endpoint dashboard. Try opening the dashboard URL in a browser on the provisioning server.
 - Make sure the LDAP Synchronization Service is running.
 - Make sure the user running the LDAP Synchronization Service has rights on the network to reach the Carbonite Endpoint dashboard.
 - Make sure the firewall or other security settings are not blocking communication.
 - If your LDAP agent needs to use a proxy server for communication, you must manually specify the proxy server information. See the alternate agent instructions for details.
-



If you need to install on another provisioning server, click **Add Agent** to obtain another **Activation Code** and then repeat the installation steps on the next server.

If you need to delete or suspend a provisioning server from queries, click **Edit** for that agent in the table in the **Synchronization agents** section and click the appropriate button. You can also edit the assigned name, if needed.

Alternate instructions for LDAP agent installation with a proxy server

1. On your provisioning server, open a command prompt.
2. Run the following command to launch the installation without requiring activation during the installation process.

```
msiexec /i C:\DownloadLocation\LdapSyncServiceInstaller.msi  
SKIPLDAPACTIVATION=1
```

Substitute your download location for C:\DownloadLocation.

3. When the installation begins, review and accept the Terms of Service and click **Next** to continue
 4. If desired, change the destination folder and click **Next** to continue.
 5. When prompted for activation information, leave the fields blank and click **Next** to continue.
 6. Click **Install**.
 7. When the installation is complete, click **Close**.
 8. Using a text editor, open C:\Program Files (x86)\Carbonite\LdapSyncService\LdapSynchronization.config.xml.
 9. Add a new section before the closing `</LdapSynchronizationConfiguration>` tag. The section you add will depend on the proxy server configuration.
-



The section you add is case-sensitive. Make sure you enter it exactly as shown.

- **Auto-detect**—If your proxy server is automatically detecting, add the following section.

```
<Proxy>
  <Type>Autodetect</Type>
</Proxy>
```

- **Server**—If your proxy server uses a specific IP and port, add the following section.

```
<Proxy>
  <Type>Server</Type>
  <Server>ServerIpAddress:Port</Server>
</Proxy>
```

- **Auto-config script**—If your proxy server is using a proxy auto-config (PAC) script, add the following section.

```
<Proxy>
  <Type>Script</Type>
  <Server>PacFilePath/PacFileName.pac</Server>
</Proxy>
```

10. Save the file changes.
11. Restart the LDAP service by running the following commands at a command prompt.
net stop LDAPSynchronizationService
net start LDAPSynchronizationService
12. Open a browser and go to <http://localhost:91>.
13. Provide the activation information, keeping in mind that the activation URL must be in the following format.

<https://vault.mysecuredatavault.com/DashboardService.v.1.0.svc>

For example, if you are using the red-US vault, you would use <https://red-us.mysecuredatavault.com/DashboardService.v.1.0.svc>.

Configure LDAP synchronization

Use this procedure to configure LDAP synchronization.

Make sure you have installed the LDAP agent on the provisioning server before proceeding with the configuration. See *Install the LDAP agent* on page 102 for details.

1. On the **Company** page, click the **User synchronization** tab.
2. In the **LDAP synchronization** section, click **Get started** or **Change connection**.

If a **Getting Started** section appears, click **Configure the Synchronization settings** to open the LDAP connection settings dialog box.

3. Configure your LDAP connection settings.

LDAP connection settings

Server:

Port:

TLS:

User name:

Password:

- **Server**—Specify the LDAP server name. Use the IP address or fully qualified domain name (FQDN) of the LDAP server. This must be resolvable by the provisioning server where you installed the LDAP agent.
- **Port**—Specify the port to use to communicate with the server. Use port 636 if you are using TLS. Use port 389 if you are not using TLS.
- **TLS**—Enable this option if you are using Transport Layer Security (secure communication) between the provisioning server and the LDAP server.
- **User name**—Specify a user that is an LDAP service account that has query rights in the search root you intended to use. Enter the account using the format domain\username.
- **Password**—Specify the password associated with the user. Make sure that the password does not use any of the following reserved operating system characters.
 - less than <
 - greater than >
 - colon :
 - quotation marks or double quote "
 - forward slash /
 - backslash \
 - vertical bar or pipe |
 - question mark ?
 - asterisk *

4. After you have configured your LDAP connection settings, click **Save changes**. Use the **Change connection** button again if you need to edit the connection settings later.
5. Click **Change mapping** to modify the mapping of Carbonite Endpoint attributes to LDAP attributes.

Change mapping settings

Mapping configuration:	<input type="text" value="ActiveDirectory"/>
Unique identifier:	<input type="text" value="objectGUID"/>
Email:	<input type="text" value="mail"/>
First name:	<input type="text" value="givenName"/>
Last name:	<input type="text" value="sn"/>
Custom 1:	<input type="text"/>
Custom 2:	<input type="text"/>
Custom 3:	<input type="text"/>

- **Mapping configuration**—Select the mapping configuration you want to use.
 - **Unique identifier**—Select the unique identifier for each attribute. Generally, you will not need to change the objectGUID default. However, in some cases where objectGUID is not implemented properly, you may need to use an alternate attribute, such as EmployeeID.
 - **Email**—This is the attribute Carbonite Endpoint uses to determine a user name. This attribute must be in email address format. Mail and userPrincipalName are the most commonly used attributes. If you are also implementing single sign-on (SSO), the attribute used here must also be used for Name-ID.
 - **First name**—This is the attribute Carbonite Endpoint uses for the user's first name. Generally, you will not need to change the givenName default. However, in some cases you may need to use another attribute, for example when the preferred name is identified using a different attribute or when non-Latin characters are used.
 - **Last name**—This is the attribute Carbonite Endpoint uses for the user's last name, or surname. Generally, you will not need to change the sn default. However, in some cases you may need to use another attribute.
 - **Custom**—If desired, enter custom information in the three provided fields. These fields allow you to enter your own custom information. Each field is limited to 500 characters. These fields will only be available if the LDAP synchronization agent you are using is from vault version 10.6 or later. Check with Carbonite if you do not know your vault version.
6. After you have configured your mappings, click **Save changes**. Use the **Change mapping** button again if you need to edit the mappings later.
 7. Click **Add user query** to specify the LDAP query to use. You can add multiple queries.

Add user query

Name:

Search root:

Filter: ?

User group: All Users ▼

Enable web retrieval:

Automatic Role Assignment:

Company Permission: No Access ▼

Save changes
Cancel

- **Name**—Specify a name for this query. Make it descriptive for the type of users you are querying.
- **Search root**—Specify the search root you want to use in the query. Parentheses are not required. For example, if domain.com is using the default Active Directory structure, the search root will be similar to CN=Users, DC=domain, DC=com. Keep in mind that you can define your search roots on a per-query basis for compatibility with global catalogs.



If your domain has more than 1000 users, narrow your search to a specific OU, otherwise, not all of your users will be synchronized.

- **Filter**—Specify an RFC4515 compatible string filter. See the [IETF specification](#) or the Microsoft TechNet article [Active Directory: LDAP Syntax Filters](#) for details. This is a query that is more or less the same as dsquery or other similar Active Directory tools. For example, you might use one of the following queries.
 - **All users**—(objectCategory=Person)
 - **All users with a valid email address**—(&(objectCategory=Person)(mail=*))
 - **All users that are a member of a group**—(&(memberof=CN=GroupName,OU=Users,DC=domain,DC=com)(objectCategory=Person))



Click the help icon (the question mark icon) to see more sample queries. Make sure you have validated your query before using it in Carbonite Endpoint.

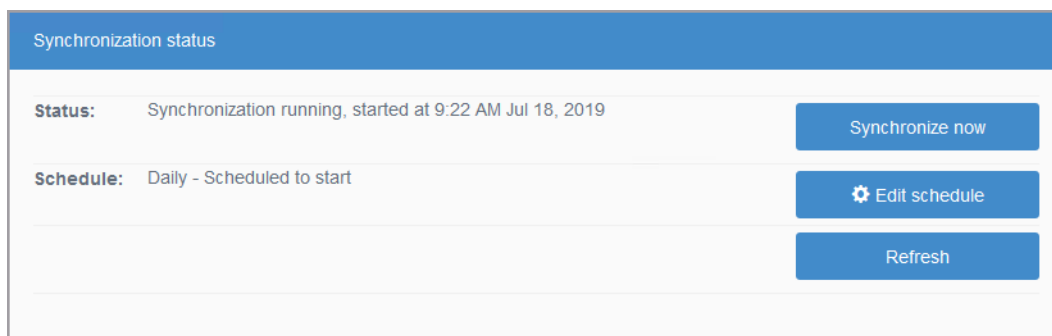
- **Enable web retrieval**—Select this option to allow users to log into the web retrieval site and access their files online. This allows them to restore files using a browser instead of the Carbonite Endpoint console.
 - **Automatic Role Assignment**—Select this option to automatically assign an Admin role for each user that matches the query. If this option is selected, each user that matches the query will automatically have the **Login to Dashboard** permission.
 - **Company Permission**—If you select **Automatic Role Assignment**, the Company Permission list appears. Click the Admin role for each user that matches the query. Options include:
 - **Administrator**—This permission provides full access to the company. You should limit this role to as few people as possible because each user who has this access has full control over everything.
 - **Backup Administrator**—This permission provides full access to all users and devices, but only partial access to other areas of the company. This role might be appropriate for a service desk team member who can assist other users with retrieving data.
 - **Legal Administrator**—This permission provides full access to legal holds and admin restores, but read-only access to other areas. This role is appropriate for those responsible for retrieving data that is on legal hold.
 - **Support**—This permission provides the ability to reset devices. Read-only access is granted to the rest of the company.
 - **Read Only**—This permission provides read-only access to all parts of the company, except legal holds.
 - **None**—This permission hides company-level information from a user that has access to log in to the company.
8. After you have configured your query, click **Save changes**. Use the **Edit** link if you need to edit the query later or the **Delete** link if you no longer want to use the query.
 9. Two summary reports display at the bottom of the screen, indicating the summary of roles changed and a summary of query rules. Click on any of the summary hyperlinks to view details.
 10. You can manage the queries in the query rules summary by using the following links in the **Action** column of the table. If users are found in multiple queries, the first query they are found in will take precedence.
 - **Move down**—Click this link to move the query down in the order of precedence.
 - **Move up**—Click this link to move the query up in the order of precedence.
 - **Edit**—Click this link to edit the query.
 - **Delete**—Click this link to delete the query.
 11. If you have not already enabled production mode, you can go to the top of the LDAP synchronization tab and click **Test synchronization**. The results display in the **Synchronization history** table.

Monitor and troubleshoot LDAP synchronization

After you have configured LDAP synchronization, you can monitor it through the **LDAP/SCIM synchronization** tab. You can also go to <http://localhost:91> on the provisioning server to see a log of

the synchronization process.

- **Synchronization status**—Initially, this section contains a **Getting Started** overview which outlines basically how to use the LDAP synchronization feature. Once you have clicked **Enable production mode**, the overview section is no longer displayed.



- **Status**—This read-only field indicates the latest status of the synchronization.
- **Schedule**— This read-only field indicates the synchronization schedule or manual if there is not a set schedule.
- **Test synchronization**—Click this button to test your settings. This button is only available before you have enabled production mode.
- **Synchronize now**—Click this button to synchronize Carbonite Endpoint with your LDAP server based on your defined queries. This manual synchronization can be used even if a schedule is set.
- **Edit schedule**—Click this button to add or modify a synchronization schedule. Select the **Synchronization frequency** and the **Approximate time**. The schedule applies to all provisioning servers.
- **Refresh**—Click this button to update the **Status**.
- **Synchronization history**—This table show each synchronization and the changes or issues that happened during the update. Use the **Previous** and **Next** buttons at the bottom of the table to move between pages of the table.



To see further information on issues identified in the table, go to <http://localhost:91> on the provisioning server to see a log of the synchronization process. Common issues include the following:

- The LDAP server name cannot be resolved by the provisioning server. Try using an IP address if name resolution is an issue.
- The LDAP binding failed. Make sure the user specified to connect to the LDAP server has a valid password, is active in LDAP, and has not been locked out due to failed login attempts. Also, make sure the search root has no parentheses and is typed correctly.
- No users are provisioned. Test a more simple query, such as a single mail address. Make sure it succeeds before adding and running more advanced queries. Make sure the email address is unique and has not already been provisioned in another account. Check Active Directory for duplicate objects. You may need to consider using a UPN-based query.

- Attributes are blank. Validate using PowerShell or another tool that the attributes are populated in Active Directory.
-

- **Synchronization agents**—This section is where you can download the agent to install on your provisioning servers. This section also has the activation codes that need to be used on the provisioning server during the installation. See *Install the LDAP agent* on page 102 for details.
- **Synchronization settings**—This section is where you configure the LDAP connection settings, the mappings to Active Directory objects, and manage the queries. See *Configure LDAP synchronization* on page 104 for details.

Chapter 10 Create and manage devices

Devices are the endpoints (desktops, laptops, and tablets) that contain the files you are protecting. You can add devices manually in Carbonite Endpoint, use bulk uploads, or add the device when you deploy the end-user software on the device.

The following tasks are available for devices.

- *View devices* on page 112
- *Add devices* on page 114
- *View device details* on page 118
- *Edit device settings* on page 119
- *Manage a device* on page 120
- *View device activity* on page 127
- *View device issues* on page 129
- *View device events* on page 129
- *View and/or delete device messages* on page 130
- *Transfer a device to a different user* on page 131
- *Restore files from a device* on page 132
- *Locate a device* on page 136
- *Delete a device* on page 126

If you want to automate device creation, see *Manage deployment* on page 45.



Starting with macOS 10.14 Mojave, the operating system includes a security feature called Full Disk Access (FDA) which blocks applications from accessing specific locations. This may prevent Carbonite Endpoint from backing up and restoring files, such as Apple Mail, Photos, Calendar, and so on. In order to back up and restore these files, you must enable Full Disk Access for Carbonite Endpoint. You can enable Full Disk Access on each macOS 10.14 or later device individually or you can use Jamf to push the change out to groups of devices.

Enable Full Disk Access on a macOS 12, 11, 10.15 or 10.14 device

1. Under the Apple icon, click **System Preferences, Security & Privacy**, and on the **Privacy** tab, select **Full Disk Access**.
2. If the padlock icon is locked, click the icon and enter your macOS credentials. Do not use your Apple ID or Carbonite Endpoint credentials.
3. Click **Add an application** (the plus icon), click **Applications** on the left, select Carbonite Endpoint in the list, and click **Open**.
4. If desired, click the padlock icon again to lock Full Disk Access.

Enable Full Disk Access on a macOS 13 device

1. Under the Apple icon, click **System Settings, Privacy & Security**, and select **Full Disk Access**.
2. Click the plus icon.

3. In the Privacy & Security box, enter your macOS credentials. Do not use your Apple ID or Carbonite Endpoint credentials.
4. Click **Applications** on the left, select Carbonite Endpoint in the list, and click **Open**.

Enable Full Disk Access for groups of devices using Jamf

1. If you do not already have it, download the Privacy Preferences Policy Control (PPPC) Utility from <https://github.com/jamf/PPPC-Utility>.
2. Create a configuration file and add Carbonite Endpoint by clicking **Add** (plus sign in the bottom left corner) and locating and selecting Carbonite Endpoint.
3. Set the permissions for **All Files** to **Allow**.
4. Save the changes.
5. Upload the configuration file to your Jamf server.
6. Go to **Configuration Profiles** and select the configuration file and settings. Be sure to select **Install Automatically** and **Computer Level**.
7. Save the changes.
8. Deploy the configuration using Jamf.

See the PPPC and Jamf documentation for additional details.

View devices

To view available devices and their information, go to the **Devices** page.



The first time a device is connected, zero (0) appears in the **Usage** column until all of the data has been uploaded to the vault. Data upload can take several days if you are using a QuickCache with a schedule limitation, have bandwidth limitations, or have large amounts of data. You can remove bandwidth limitations or QuickCache schedules to speed up the process.

The following toolbar and table controls are available on the **Devices** page:

- **Add device**—Click this button to add a new device. For more information, see *Add a single device* on page 114.
- **Download list**—Click this button to download a complete device list to your local computer. You can download a Microsoft Excel (.xlsx) file or a comma-delimited file (.csv). If you download the Excel format, you must enable editing for any hyperlinks to the portal to be active.
- **Show Entries**—Specify the number of rows to be shown in the table on each page. Additional rows over the number you select are shown on additional pages and can be viewed by using the paging buttons at the bottom of the table.



This table is limited to 100 rows. If you need to see a list of all entries, use **Download list**.

- **Search**—Text entered in the box narrows the list displayed to only the rows that contain the search text. The search checks the entire table, not just the visible rows.
- **Sort**—You can sort the table by clicking on any column heading.
- **Table hyperlinks**—There are hyperlinks in the table that will take you directly to a page in the dashboard.
 - **Device name**—This hyperlink will take you to the **Device details** tab on the **Device** page. See *View device details* on page 118 for details.
 - **Email**—This hyperlink will take you to the **User details** tab on the **User** page. See *View user details* on page 71 for details.

- **Company**—This hyperlink will take you to the **Company** page. See *View and manage your company* on page 19 for details.
- **Table paging buttons**—The paging buttons at the bottom of the table allow you to move more quickly between pages. Each button jumps to that respective page of the table.

If the list exceeds the maximum number of results configured by your administrator, the table is blank and a dialog box appears, prompting you to use the **Search** function to narrow your results. You can click the link to view the limited list, or you can click **Download list** to export the entire list of devices.

Add devices

Carbonite Endpoint supports the following methods for adding devices:

- *Add a single device* on page 114—You can manually add a single device. Use this method when you only have a few devices to add.
- *Import multiple devices* on page 116—You can bulk import multiple devices. Use this method when you have many devices to add, but you are not using an automated method.

If you want to automate device creation, see *Manage deployment* on page 45.

Add a single device

Use this procedure to add a single, new device.

1. On the **Company** or **Devices** page, click **Add device**.
2. Enter search criteria in the text box to find the user for the device and click **Search**.



If you do not enter search criteria and the list exceeds the maximum number of results configured by your administrator, the table is blank and a dialog box displays, prompting you to use the **Search** function to narrow your list of results. You can click the link to view the limited list, if required.

If the user you want does not exist, click **Add user** and after you finish adding the user, you will return to this page and you can search for the user you just added. See *Add a single user* on page 73 for details on adding a new user.

3. In the search results, select the user for the device. Use the standard page and table functionality if the search returns a long list.
 - **Show Entries**— Specify the number of rows to show on each page in the table. Additional rows over the number you select are shown on additional pages and can be viewed using the paging buttons at the bottom of the table. You can view a maximum of 100 rows in the table.
 - **Search**—Text entered in the box narrows the list displayed to only the rows that contain the search text. The search checks the entire table, not just the visible rows.
 - **Table paging buttons**—The paging buttons at the bottom of the table allow you to move more quickly between pages. Each button jumps to that respective page of the table.
4. Click **Select user**.

The **Current context** area of the **Device** page shows the company and user associated with the new device. Make sure that you have selected the correct user. If you have not, click **Cancel** and search again for the correct user.

5. Specify the following information for the new device:

- **Device name**—You can optionally enter a name to identify the device. If you do not enter a device name, it will be named Device x, where x is an incremental number, for example Device 1, then Device 2, and so on.
- **Do not sync device/computer name**—This setting indicates whether the device name in Carbonite Endpoint is automatically synchronized with the computer name on the endpoint device. When this feature is enabled, if the computer name of the endpoint device changes, the device name is automatically updated in Carbonite Endpoint. If the user already has a device with the new name, a space and number are added to the new device name in Carbonite Endpoint (e.g., *deviceName 2*).

To synchronize the device name with the computer name on the endpoint device, clear the **Do not sync device/computer name** check box. If you do not want the device name to be synchronized with the computer name on the endpoint device, select the **Do not sync device/computer name** check box.

- **Select device policy set**—Select the policy you want applied to the device. See *Create and manage policies* on page 22 for details.
- **Select storage quota**—Select the amount of space this device can use for backing up files. If you select **Unlimited**, the device will not have any space restrictions. If you select **Custom**, enter the size, in GB, that the device will be limited to.

The screenshot shows the 'Add device' form in Carbonite Endpoint. The form is titled 'Device' and has a breadcrumb 'Devices / Add device'. The 'Add device' section contains the following fields:

- Current context:** A table with the following data:

Company	CompanyName
User group	All users
User email	user@domain.com
User name	UserFirstName UserLastName
- Device name (optional):** A text input field with the placeholder 'DeviceName'.
- Do not sync device/computer name:** A checkbox that is currently unchecked.
- Select device policy set:** A dropdown menu showing 'Inherit policy from CompanyName - Base Policy'.
- Select storage quota:** Two radio buttons: 'Unlimited' (selected) and 'Custom' (with a text input field for GB).

At the bottom right, there are two buttons: 'Create device' (highlighted in blue) and 'Cancel'.

6. Once you have configured the device details, click **Create device**.

An email is sent to the user to download the end-user software. The email contains the activation URL and activation code.

Import multiple devices

Use this procedure to import multiple, new devices. (Existing devices will not be overwritten.)

1. Go to the **Company** page and click the **Company details** tab.
2. Click **Import devices**.
3. If you have not already done so, prepare your import file.
 - a. Click **Download template** to obtain the template used for the device import process.
 - b. Save and open the Excel (.xlsx) file.
 - c. Enable editing of the file.
 - d. For each device you want to add, enter the device's information in one row of the spreadsheet in the **First Name**, **Last Name**, and **Email** columns. You can optionally enter data for the columns listed below, however, do not enter any data in the remaining pre-defined columns, and do not modify the Row ID entries.
 - **GB**—Set the amount of disk space, in GB, that the that the device will be limited to when backing up files. If you leave this blank, the policy setting is used.
 - **Policy Set**—Specify the policy you want the device to use. If you leave this blank, the policy will be inherited.
 - **Device Name**—Specify a name to identify the device. This name is optional.
 - **QuickCache Name**—Specify the name of the QuickCache to use.
 - e. You can optionally create additional columns for additional, optional information. You can skip this step if you only want to enter the information above for each device.
 - i. In the Excel spreadsheet, right-click the **Devices** sheet name and click **Unhide**.
 - ii. Select the sheet named **Dictionary** and click **OK**. The **Dictionary** sheet defines how the template is used when importing both users and devices.
 - iii. For each additional, optional field defined that want to include in your import, enter the **Name**, exactly as defined in the **Dictionary**, in a new column on the **Devices** sheet.
 - iv. Populate the new columns with data as desired. Cells in the new columns that are not populated will use the default value, if any.
 - f. Repeat adding a row for each additional device.
 - g. After you have added all of the devices you want to import, save the file.
4. Select the file to import by clicking **Choose file**.
5. Browse to and select your file and click **Open**.
6. You will see the imported file in the table at the bottom of the page. By default, all rows will be imported. If you only want to import specific devices, select the specific devices from the table by clicking the check box in that device's table row.



The following table controls are available for the import devices table.

- **Show Entries**—Specify the number of rows to be shown in the table on each page. Additional rows over the number you select are shown on additional pages and can be viewed by using the paging buttons at the bottom of the table.
- **Search**—Text entered in the box narrows the list displayed to only the rows that contain the search text. The search checks the entire table, not just the visible rows.
- **Sort**—You can sort the table by clicking on any column heading.
- **Table paging buttons**—The paging buttons at the bottom of the table allow you to move more quickly between pages. Each button jumps to that respective page of the table.

7. You have three choices after you have opened an import file.
 - **Start over**—Click this button to abort the import of the selected file or to import another file after completing an import.
 - **Perform import**—Click this button to import all rows or the selected rows.
 - **Validate import**—Click this button to validate all rows or the selected rows, without actually importing the devices.
8. When the import or validation is complete, the overall status appears at the top of the page. Click **Download results spreadsheet** and open the Excel file to view the individual status for each device. You can edit and use this generated spreadsheet as the basis of another import, if desired.

Company Name / Import devices

Device

• Import complete. Overall status: Success [Download results spreadsheet](#)

Template Excel file: [Download template](#)

Input Excel file: Uploaded 'Device-Bulk-Import-Template.xlsx'. Contents shown below.

Actions: All rows will be imported

[Start over](#) [Perform import](#) [Validate import](#)

Show entries Search:

Row Id	First Name	Last Name	Email
1	FirstName01	LastName01	Email01@domain.com
2	FirstName02	LastName02	Email02@domain.com
3	FirstName03	LastName03	Email03@domain.com
4	FirstName04	LastName04	Email04@domain.com
5	FirstName05	LastName05	Email05@domain.com
6	FirstName06	LastName06	Email06@domain.com
7	FirstName07	LastName07	Email07@domain.com
8	FirstName08	LastName08	Email08@domain.com
9	FirstName09	LastName09	Email09@domain.com
10	FirstName10	LastName10	Email10@domain.com

View device details

Use this procedure to view the details for a specific device.

1. Go to the **Devices** page to display the device list and click the name of the device you want to view. For more information, see *View devices* on page 112.
2. Click the **Device details** tab. The tab shows information about the selected device, including the device name, policy and backup information.

The tab also shows the device's **Auto sync device/computer name** setting. This setting indicates whether the device's name in Carbonite Endpoint is automatically synchronized with the computer name on the endpoint device. When this feature is enabled, if the computer name of the endpoint device changes, the device name is automatically updated in Carbonite Endpoint.



To view information about multiple devices at the same time, download the device list from the **Devices** page. See *View devices* on page 112 for details.

Device details		Manage device	Activity	Issues	Events	Messages	Restore	Location	
Device name:	DeviceName01	Auto sync device/computer name:		Yes				Move device	Edit device
Device ID:	5bc341d9-4fb3-4ec0-9ba7-3859992745f3								
State:	Activated	Email:		email01@domain.com					
Policy set:	Base Policy (Inherited)	User name:		FirstName01 LastName01					
Usage / Quota (GB):	35.73 / Unrestricted	User group:		All users					
Last backup:	Apr 13 2020 10:17 AM (1 minute ago)								
Last complete backup:	Yes	Company:		CompanyName					
QuickCache:	None								
Last client status update:	Apr 13 2020 10:16 AM	Custom 1:							
Operating system:	Mac OS X	Custom 2:							
OS edition:	10.14.6	Custom 3:							
Service pack:	unavailable	Client version:		10.5.451.8451					
OS bit size:	64	Created at:		Apr 13 2020 10:15 AM					
Cache used:	4 GB	Initial activation:		Apr 13 2020 10:16 AM					
Cache available:	76 GB	Last reset:							
Physical memory installed:	Unavailable	Activation code:		6C88-CE9A-2799-2EF5-32C1					
IP location:	OK	Activation Code Expiration:		Not available					
Enhanced location:	OK	Last user state scan :		Not available					

[Help activating device](#)

The following options appear on the Device details tab:

- **Move device**—Click this button to move the device to a different user. If the number of users exceeds the maximum number of results configured by your administrator, a dialog box displays, prompting you to use the **Search** function to narrow your results. Select the user from the table by clicking the circle in that user's table row and click **Select user**. The following table controls are available when selecting a new user. See *Transfer a device to a different user* on page 131 for details.
 - **Show Entries**— Specify the number of rows to show on each page in the table. Additional rows over the number you select are shown on additional pages and can be viewed using the paging buttons at the bottom of the table. You can view a maximum of 100 rows in the table.
 - **Search**—Text entered in the box narrows the list displayed to only the rows that contain the search text. The search checks the entire table, not just the visible rows.
 - **Sort**—You can sort the table by clicking on any column heading.
 - **Table paging buttons**—The paging buttons at the bottom of the table allow you to move more quickly between pages. Each button jumps to that respective page of the table.
- **Edit device**—Click this button to modify the device settings. See *Edit device settings* on page 119 for details.
- **Table hyperlinks**—There are hyperlinks in the table that will take you directly to a page in the dashboard.
 - **Policy set**—Opens the **Edit policy details** page. This is the same as going to the **Company** page, clicking the **Policies** tab, and then clicking a policy name hyperlink in the policies table. See *Edit an existing policy* on page 33 for details.
 - **QuickCache**—Opens the **QuickCache activity** tab on the the **QuickCache** page. See *View QuickCache activity* on page 150 for details.
 - **Retrieve protected file**—Opens another tab or window to allow you to search for a file to retrieve.
 - **Email** and **User name**—Both of these hyperlinks open the **User details** tab on the **User** page. See *View user details* on page 71 for details.
 - **User group**—Opens the group details for a company. This is the same as going to the **Company** page, clicking the **Groups** tab, and then clicking a group name hyperlink in the groups table. See *View group details* on page 64 for details.
 - **Company**—Opens the **Company** page. See *View and manage your company* on page 19 for details.
- **Help activating device**—Click this hyperlink to see useful information for activating this device. Links to the installation file and the activation URL are provided. If you need to reinstall Carbonite Endpoint on this device, you must reset the device and then reinstall. See *Manage a device* on page 120 for details.

Edit device settings

Use this procedure to edit device settings.

1. Go to the **Devices** page and click the name of the device you want to edit. See *View devices* on page 112 for details on searching the device table.
2. Click the **Device details** tab and click **Edit device**.

3. Modify the device settings as needed. See *Add a single device* on page 114 for details on the device settings.

The screenshot shows the 'Edit device' configuration page. At the top, there's a breadcrumb 'Devices / DeviceName / Edit device' and a 'Device' icon. Below is a blue header 'Edit device'. A note states: 'Device name is synchronized with computer name. Device name changes may be reversed during the next synchronization.' The form contains several sections: 'Device name (defaults to device id if no name is provided):' with a text input 'DeviceName'; 'Do not sync device/computer name:' with a checkbox; 'Custom 1:', 'Custom 2:', and 'Custom 3:' each with a text input; 'Select device policy set:' with a dropdown menu showing 'Inherit policy from CompanyTest - 'Base Policy''; 'Policy set description:' with the text 'A Starter Policy'; 'Select storage quota: (Current client usage is 0.00 GB)' with radio buttons for 'Unlimited' (selected) and 'Custom' followed by a 'GB' input; and 'QuickCache this device can use:' with a dropdown menu showing 'None'. At the bottom right, there are 'Save changes' and 'Cancel' buttons.

4. After you have modified the device settings, click **Save changes**.

Manage a device

Carbonite Endpoint supports different options for managing or administering a device under the Manage device tab. The available tasks depend on the state of the device.

1. To manage a device, go to the **Devices** page and click the name of the device. See *View devices* on page 112 for details on searching the device table.
2. Click the **Manage device** tab.

The screenshot shows the 'Manage device' tab selected in the 'Device' view. The breadcrumb is 'Devices / DeviceName01'. The 'Device' icon is present. The tab bar includes 'Device details', 'Manage device' (active), 'Activity', 'Issues', 'Events', 'Messages', 'Restore', and 'Location'. Below the tab bar, there are six action buttons, each with a description:

- Put on legal hold**: This will stop backup data from being deleted from the vault by disabling retention and erase. It will also prevent this device from being deleted.
- Suspend device**: Suspending the device will stop protection of the device; this is reversible.
- Delete data from device**: Data will be deleted from the device but will remain stored in the vault.
- Delete device**: Device will be permanently deleted; this action is not reversible.
- Reset device**: Device will be reset; device will need to be reinstalled and reactivated.
- Scan user state**: Device will scan and backup the user state using User State Migration Tool and policy settings. To restore the state, use the restore tab.

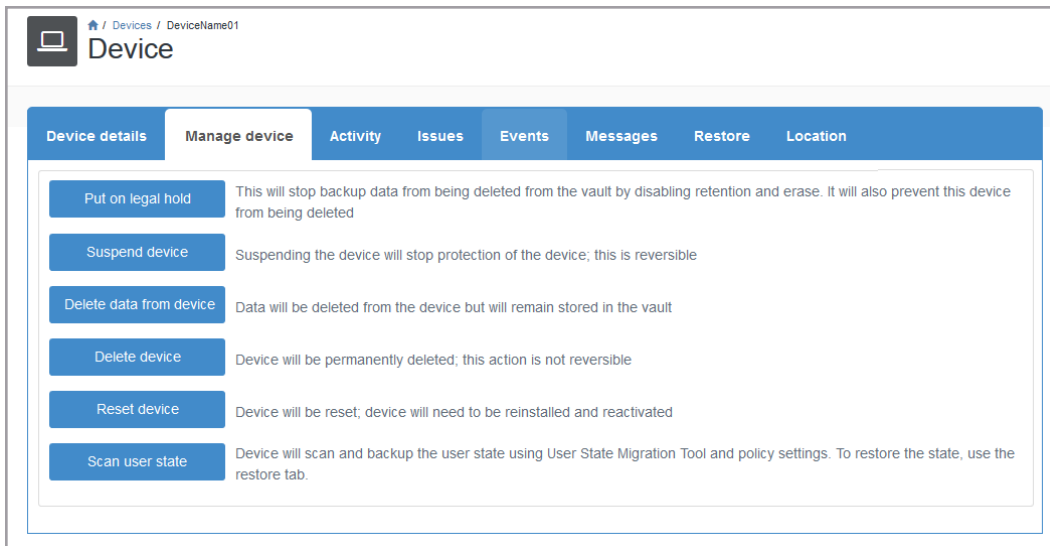
Carbonite Endpoint supports the following methods for managing devices.

- **Put on legal hold**—Putting a device on legal hold prevents device data from being deleted from the vault, and also prevents the device itself from being deleted. This feature is useful if you are legally required to preserve data, for example because of a lawsuit or a user investigation. The data can be made available upon request. The data is immutable and therefore forensically defensible. A legal hold prevents someone from deleting files or entire backups. When prompted, specify any notes pertaining to the legal hold. You can remove a device from a legal hold when it is no longer required. See *Put a device on legal hold* on page 121 for details on putting a device on, or removing a device from, legal hold.
- **Suspend device**—Suspending a device stops device protection. This feature is useful when you do not want additional data backed up from a device, but you want to preserve the data that has already been backed up. You can reactive the device when the suspension is no longer required. See *Suspend a device* on page 122 for more information about suspending or reactivating a device.
- **Delete data from device**—Deleting data from a device deletes all protected data from the device without deleting it from the vault; unprotected data on the device is not deleted. This feature is useful if a laptop is lost or stolen, and there is concern that someone malicious could access the laptop and the files on it. This option also resets the license so that you can reuse it again later, on the same or a different device. After deleting data from a device, you must generate a new license for the device using the **Reset device** feature. See *Delete data from a device* on page 123 for details.
- **Delete device**—Deleting a device deletes the device from Carbonite Endpoint and deletes all of the protected data from the vault. You will not be able to restore any data and the device will no longer be protected. This feature allows you to stop using the license. Deleting a device is not reversible, and after it is deleted the backed up data cannot be accessed. This feature is useful when you want to remove the data from the vault or no longer need the backup. It also allows you to stop using the license. See *Delete a device* on page 126 for details.
- **Reset device**—Resetting a device means that the device is unprotected until you install and activate (if you are using a new device) or reinstall and reactivate (if you are reusing a device). This feature is useful when you need to reinstall on the same device or when a user has a new device. Resetting a device prevents you from needing two licenses. When prompted, enter and confirm a passphrase that will be used to activate or reactivate the device, then click **Reset device**. Copy the activation code that is presented. The same code will also be displayed on the **Device details** tab on the **Device** page. You will need the activation code for the device. See *Reset a device* on page 124 for details.
- **Scan user state**—Click this button to start a manual scan of the user state. Carbonite Endpoint uses Microsoft User State Migration Tool (USMT) to provide a process for replacing or refreshing Windows computers. The utility captures operating system settings, application settings, user accounts, and user files and migrates them to a new Windows installation. You must be familiar with using and configuring USMT. See <https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-topics> for details on this utility. Once a scan is completed, you can restore the user state. See *Scan the user state of a device* on page 125 for details.

Put a device on legal hold

Use this procedure to put a device on legal hold. When a device is on legal hold, backup data cannot be removed from the vault and the device cannot be deleted.

1. Go to the **Devices** page and click the name of the device you want to put on legal hold. See *View devices* on page 112 for details on searching the device table.
2. Click the **Manage device** tab.



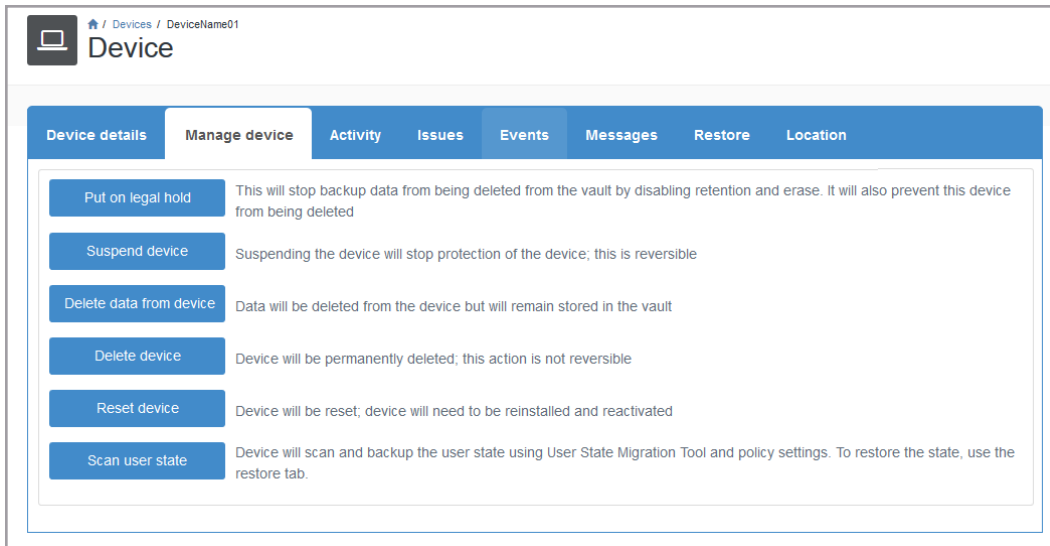
3. Click **Put on legal hold**.
4. In the dialog box that appears, type any relevant notes in the **Comment** box and click **Put on legal hold**.
The message "device is on legal hold" and the legal hold comment display under the **Manage device** tab.
5. To remove the device from legal hold, click the **Manage device** tab and click the **Remove from legal hold** button.
6. Confirm that you want to remove the device from legal hold and click **OK**.

The device reverts to the normal retention and erasure settings and backup data is enabled for the vault.

Suspend a device

Use this procedure to suspend or reactivate a device. Suspending a device stops protection of the device.

1. Go to the **Devices** page and click the name of the device you want to suspend. See *View devices* on page 112 for details on searching the device table.



2. Click the **Manage device** tab.
3. Click **Suspend device**.
4. Click **OK** in the confirmation dialog box that appears.

The Device details page opens and displays the **State** of the device as "Suspended".
5. To re-enable protection for the device, click the **Manage device** tab and click the **Reactivate device** button.
6. Click **OK** in the confirmation dialog box that appears.

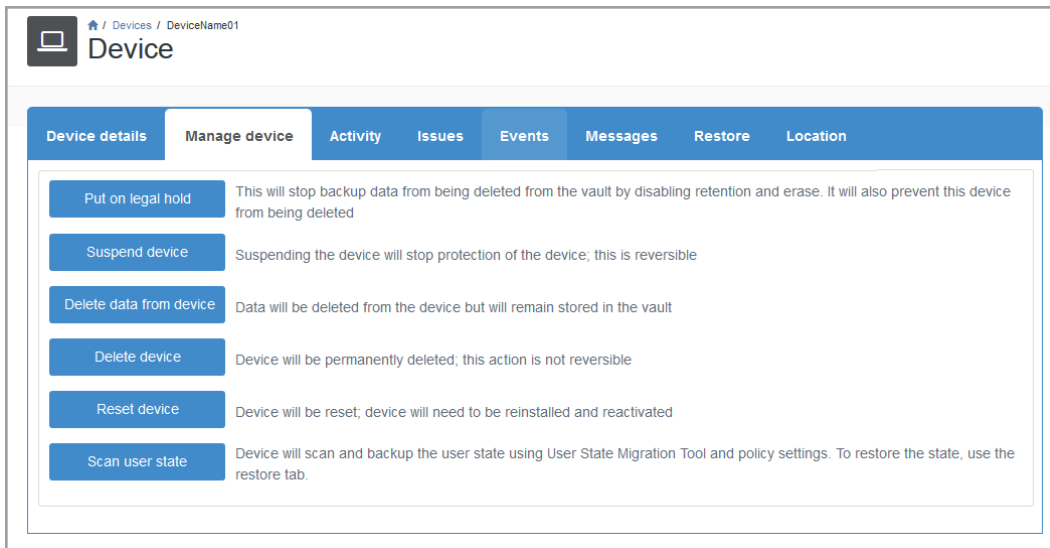
The Device details page opens and displays the **State** of the device as "Activated".

Delete data from a device

Use the following procedure to delete all protected data from a device without deleting the data from the vault. Unprotected data is not deleted from the device. The device must then be reset and restored. See *Reset a device* on page 124 for details.

1. Go to the **Devices** page and click the name of the device you want to manage. See *View devices* on page 112 for details on searching the device table.

2. Click the **Manage device** tab.

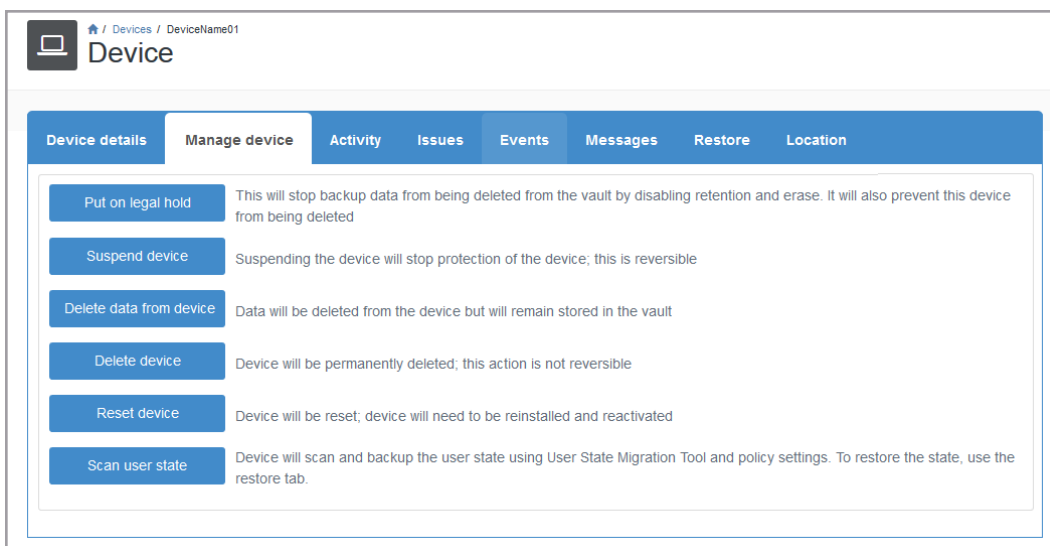


3. Click **Delete data from device**.
4. Click **OK** in the confirmation dialog box.

Reset a device

Use this procedure to reset a device. After a device is reset, it must be reinstalled and reactivated.

1. Go to the **Devices** page and click the name of the device you want to reset. See *View devices* on page 112 for details on searching the device table.
2. Click the **Manage device** tab.



3. Click **Reset device**.
4. In the Reset device dialog box, type a passphrase in the **Passphrase** box. This is a one-time passphrase that you use to reinstall the client.
5. Retype the passphrase in the **Confirm passphrase** box.
6. Click the **Reset device** button.

The Device details page opens and displays the **State** of the device as "Reset". The device will remain in this state for 14 days or until Carbonite Endpoint is authenticated on the new or existing device.

7. Copy the activation code provided. The same code is also displayed on the **Device details** tab on the **Device** page. The activation code is required when reactivating the device.



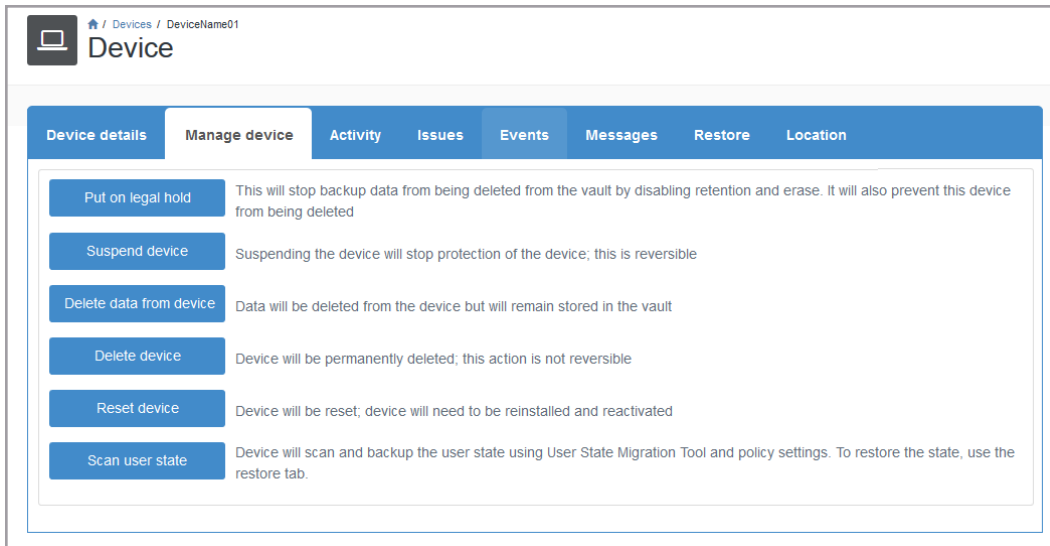
The passphrase expires after 14 days. If the passcode expires, you will need to reset the device again to generate a new passphrase.

If you are using macOS 10.14 Mojave or later and you are uninstalling and reinstalling on a device, you may need to reboot the machine after the uninstall or at least wait a few minutes before attempting to reinstall. This is due to macOS Full Disk Access impacting the uninstall process, making uninstall process take longer to fully finish. If you do not wait long enough or reboot, the reinstall will not be clean and the client will be in the same state it was in before the uninstall was started.

Scan the user state of a device

Use the following procedure to scan and back up the user state of the device using the User State Migration Tool and policy settings. You can then restore the device state, if required.

1. Go to the **Devices** page and click the name of the device you want to scan. See *View devices* on page 112 for details on searching the device table.
2. Click the **Manage device** tab.



3. Click **Scan user state**.
4. Click **OK** in the confirmation dialog box that appears.

The Manage device page displays the current state of the scan. The Scan user state button is disabled while Carbonite Endpoint performs the scan.



You can schedule periodic user state scans using a policy setting. See *Device Settings* on page 27 for details.

Delete a device

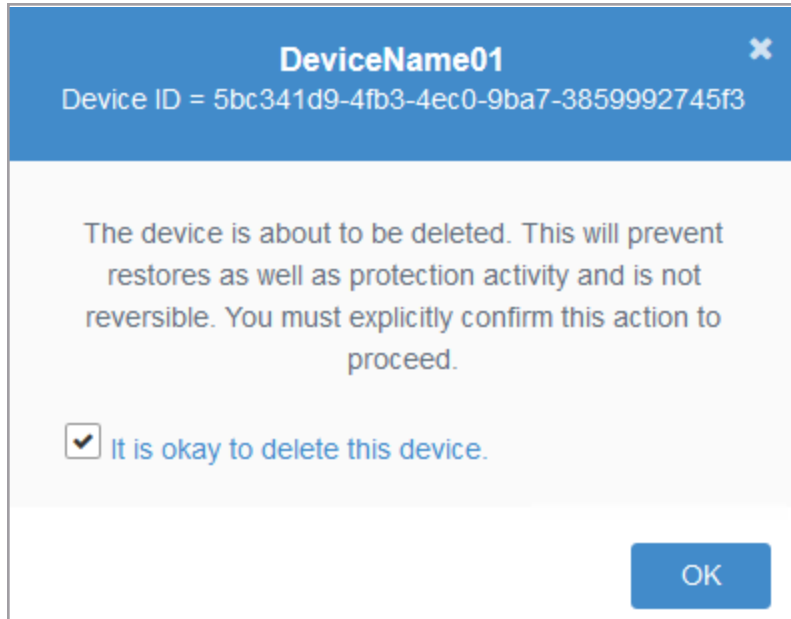
Use this procedure to delete a device.

Deleting a device is an irreversible action. Review the following information before you delete a device:

- If you delete a device, all protected data from the device will be deleted from the vault.
 - If you delete a device, you will not be able to restore any data, even retained data.
 - If you delete a device, the device and the data will no longer be protected.
 - You cannot free a license but keep the protected data by deleting a device. If you delete the device, the protected data will be deleted.
 - If you are no longer using a device but want to keep the protected data, you should not delete the device. If you delete the device, the protected data will be deleted.
 - If you need to ensure protected data cannot be deleted, put the device on legal hold. See *Manage a device* on page 120 for details.
1. Go to the **Devices** page and click the name of the device you want to delete. See *View devices* on page 112 for details on searching the device table.
 2. Click the **Manage device** tab on the **Device** page and click **Delete device**.



Remember, once a device is deleted, all protected data is also deleted. You will not be able to restore any data, even retained data.



3. Confirm that you want to delete the device and click **OK**.

View device activity

Use this procedure to view activity for a device.

1. Go to the **Devices** page and click the name of the device you want to view. See *View devices* on page 112 for details on searching the device table.
2. Click the **Activity** tab to display the device activity.

Device details Manage device **Activity** Issues Events Messages Restore Location

Status

LAST STATUS UPDATE FROM CLIENT ON OCT 07 2019 04:11 PM (1 MINUTE AGO)
Snapshot of current activity at the time of the last update:

Number of files protected:	9771	Current processing filename:	None
Number of files pending protection:	0	Current processing file size:	NA
Size of upload queue:	Empty	Current processing percent complete:	NA
Average upload transfer rate:	NA	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

Recent activity

Recent activity: Type filter: All activity types

Show 10 entries Search:

Type	Start time	Finish time	State	Total files	Changed files	User state	Upload/Download size
Protect	Sep 05 2019 10:05 AM	Sep 05 2019 10:06 AM	Complete	14	14	No	5 KB
Protection confirmation	Sep 05 2019 12:06 AM	Sep 05 2019 12:06 AM	Complete			No	
Protection confirmation	Sep 03 2019 11:57 PM	Sep 03 2019 11:57 PM	Complete			No	

The following activity information is displayed:

- **Status**—The top section identifies when the last status information was captured. The activity at the time the status information was captured is listed.
- **Recent activity**—The bottom section shows the protection and restore activity on the device. The most recent 50 activities are shown. Using the **Type filter** drop-down, you can filter the table to see only specific types of activity. The following table controls are available when viewing the recent activity.
 - **Show Entries**—This table is limited to 50 rows. Specify the number of rows to be shown in the table on each page. Additional rows over the number you select are shown on additional pages and can be viewed by using the paging buttons at the bottom of the table.
 - **Search**—Text entered in the box narrows the list displayed to only the rows that contain the search text. The search checks the entire table, not just the visible rows.
 - **Sort**—You can sort the table by clicking on any column heading.
 - **Table paging buttons**—The paging buttons at the bottom of the table allow you to move more quickly between pages. Each button jumps to that respective page of the table.

View device issues

Use this procedure to view issues on a specific device. Issues are problems with files on a device that are being backed up. These issues may require manual intervention to be resolved, depending on the issue.

1. Go to the **Devices** page and click the name of the device you want to view. See *View devices* on page 112 for details on searching the device table.
2. Click the **Issues** tab to display the issues, if any. For example, if a file is too large to back up, it will be flagged as an issue.

Time	Issue description	Event action	Aspects blocked by issue	Info value 1	Info value 2	Additional info
Feb 27 2020 04:59 AM	Processing paused while data is uploaded to server.	raised	File and folder encryption File backup	0	0	

- **Show Entries**—This table is limited to 50 rows. Specify the number of rows to be shown in the table on each page. Additional rows over the number you select are shown on additional pages and can be viewed by using the paging buttons at the bottom of the table.
- **Search**—Text entered in the box narrows the list displayed to only the rows that contain the search text. The search checks the entire table, not just the visible rows.
- **Sort**—You can sort the table by clicking on any column heading.
- **Table paging buttons**—The paging buttons at the bottom of the table allow you to move more quickly between pages. Each button jumps to that respective page of the table.

View device events

Use this procedure to view events on a device. Events are problems or alerts that can be related to the environment or due to a policy violation. These events generally do not need manual intervention and will resolve on their own.

1. Go to the **Devices** page and click the name of the device you want to view. See *View devices* on page 112 for details on searching the device table.
2. Click the **Events** tab to display the device events, if any. For example, an event may be "processing paused for upload", meaning that the client momentarily stopped processing in order to upload.

Time	Issue description	Event action	Aspects blocked by issue	Info value 1	Info value 2	Additional info
Aug 29 2019 11:59 AM	Processing paused while data is uploaded to server.	raised	File and folder encryption File backup	0	0	
Aug 29 2019 12:36 PM	Processing paused while data is uploaded to server.	raised	File and folder encryption File backup	0	0	
Aug 29 2019 12:36 PM	Processing paused while data is uploaded to server.	cleared				
Aug 29 2019 01:04 PM	Processing paused while data is uploaded to server.	cleared				
Aug 29 2019 01:05 PM	Processing paused while data is uploaded to server.	raised	File and folder encryption File backup	0	0	
Aug 29 2019 01:17 PM	Processing paused while data is uploaded to server.	cleared				
Aug 29 2019 01:18 PM	Processing paused while data is uploaded to server.	raised	File and folder encryption File backup	0	0	
Aug 29 2019 01:32 PM	Processing paused while data is uploaded to server.	raised	File and folder encryption File backup	0	0	
Aug 29 2019 01:32 PM	Processing paused while data is uploaded to server.	cleared				
Aug 29 2019 01:52 PM	Processing paused while data is uploaded to server.	raised	File and folder encryption File backup	0	0	

- **Show Entries**—This table is limited to 50 rows. Specify the number of rows to be shown in the table on each page. Additional rows over the number you select are shown on additional pages and can be viewed by using the paging buttons at the bottom of the table.
- **Search**—Text entered in the box narrows the list displayed to only the rows that contain the search text. The search checks the entire table, not just the visible rows.
- **Sort**—You can sort the table by clicking on any column heading.
- **Table paging buttons**—The paging buttons at the bottom of the table allow you to move more quickly between pages. Each button jumps to that respective page of the table.

View and/or delete device messages

Use this procedure to view device messages. Messages contain information about the device and its backup. The messages may lead to events or issues that may or may not require manual intervention to be resolved, depending on the message.

1. Go to the **Devices** page and click the name of the device you want to view. See *View devices* on page 112 for details on searching the device table.
2. Click the **Messages** tab to display the device messages, if any. By default, the most recent

message displays at the top of the table.

The screenshot shows a web interface for managing a device. The top navigation bar includes tabs for 'Device details', 'Manage device', 'Activity', 'Issues', 'Events', 'Messages', 'Restore', and 'Location'. The 'Messages' tab is selected. Below the navigation bar, there is a 'Delete messages' button, a 'Show 10 entries' dropdown menu, and a search box. A table displays a single message entry with the following columns: 'Type', 'Message', 'More information', and 'Message time'. The message text is 'Error getting USMT executable' and the time is 'Jun 26 2019 02:55 PM'. At the bottom of the table, there are pagination buttons: 'First', 'Previous', '1', 'Next', and 'Last'.

- To delete all of the messages, click **Delete messages**. Additionally, the following table controls are available when viewing the recent activity.
 - **Show Entries**—This table is limited to 20 rows. Specify the number of rows to be shown in the table on each page. Additional rows over the number you select are shown on additional pages and can be viewed by using the paging buttons at the bottom of the table.
 - **Search**—Text entered in the box narrows the list displayed to only the rows that contain the search text. The search checks the entire table, not just the visible rows.
 - **Sort**—You can sort the table by clicking on any column heading.
 - **Table paging buttons**—The paging buttons at the bottom of the table allow you to move more quickly between pages. Each button jumps to that respective page of the table.

Transfer a device to a different user

Use this procedure to transfer a device between users. Existing devices can be moved between users on the Device details page. Before you delete a user, you may want to move their backed-up devices to a different user.

- Go to the **Devices** page and click the name of the device you want to transfer. See *View devices* on page 112 for details on searching the device table.
- Click the **Device details** tab and click **Move device**.
- In the dialog box that appears, select the target user from the list.



You can use the **Search** function to refine the list of users.

- Click the **Select user** button.
- Verify that the information is accurate and click **Yes** to confirm the move.

Restore files from a device


You can use this procedure to restore files from a user's device, if you have permission to perform admin restores. Admin restores are restores performed by an administrator instead of by the person whose device is protected by Carbonite Endpoint

1. Go to the **Devices** page and click the name of the device with files that you want to restore. To search for a device, see *View devices* on page 112.

The Device page shows information about the selected device.

2. On the **Device** page, click the **Restore** tab.

If you do not have permission to perform admin restores, the **Restore** tab is not available.

3. To view a list of files that can be restored, do one or more of the following:
 - Select a **File category** to narrow your search.
 - Modify the **Sort order** of the results that will be returned.
 - Enter a specific file name or a wildcard pattern in the **Search** field.
4. Click **Search**. The Restore tab shows files that match the search criteria. When viewing the list of files, you can use the following controls:
 - **Show Entries**— Specify the number of rows to show on each page in the table. Additional rows over the number you select are shown on additional pages and can be viewed using the paging buttons at the bottom of the table. You can view a maximum of 100 rows in the table.
 - **Table hyperlinks**—Volume and folders are hyperlinks that you can click on to drill down into that volume or folder. The path is displayed above the table. If you want to navigate up in the path, click the arrow button to the left of the displayed path .
 - **Table paging buttons**—The paging buttons at the bottom of the table allow you to move more quickly between pages. Each button jumps to that respective page of the table.

Devices / DeviceName01

Device

Device details Manage device Activity Issues Events Messages **Restore** Location

File category: All files ▾

Sort order: Date modified ▾

Search: *.docx

Search

Restore all matches

Showing first 100 search matches

Show 10 entries

	Name	Date	Size	Backup	Location
<input type="checkbox"/>	Endpoint.docx	Oct 07 2019 02:56 PM	18 KB	Oct 07 2019 02:58 PM	C:\Users\Desktop
<input type="checkbox"/>	Weekly Status 10-4-2019.docx	Oct 02 2019 01:23 PM	13 KB	Oct 02 2019 01:27 PM	C:\Users\Desktop
<input type="checkbox"/>	Notes .docx	Aug 26 2019 09:45 AM	12 KB	Aug 26 2019 06:02 PM	C:\Users\Desktop
<input type="checkbox"/>	Prep Sheet.docx	Aug 08 2019 04:09 PM	46 KB	Aug 08 2019 04:15 PM	C:\Users\Desktop

5. Do one of the following:

- To restore all files listed in the table, click **Restore all matches**.
- To restore specific files, select the check box for each file that you want to restore, and then click **Restore selection**.

The Add admin restore page shows available restore options.

6. On the Add admin restore page, specify restore options:

- **Restore time**—By default, the most recent version of the file will be restored. To restore an older version, click **Change**, select the date and time of the file version that you want to restore, and click **Save changes**. If you change your mind, click **Reset to most recent** to restore the most recent version of the file.



If you select a previous date and time, the file you restore will be the most recently changed version of the file at that date and time. Do not expect the time stamp of the file to be that date and time. For example, a file was updated on Monday and the changes were backed up at 3:30pm. The file was not updated again until Friday at 11:00am, so the next back up of that file will be after Friday at 11:00am. If you restore the file and select Wednesday at 4:00pm, you will not get a file with a time stamp of Wednesday at 4:00pm. You will get the version of the file that existed in the backup on Wednesday at 4:00pm, which would be the file from Monday. Any date and time between Monday at 3:30pm and before the file was backed up after the Friday at 11:00am update, you will get the Monday version of the file. If you need to get the version of the file before Monday, you must select a date and time before that version was backed up. To get the Friday at 11:00am version, you must select a date and time after that version was backed up and before the file was updated and backed up again. In other words, the file you will get will not have the date and time you specify but the version of the file that existed in the backup at the date and time you specify.

- **Include deleted files**—Select this option if you want to restore files that were deleted.

- **Restore location**—Select where you want to restore the file to. Click **Original location** to restore to the original location, which is the location the file existed when it was backed up. If you want to restore to a new location, click **Change**. Specify the volume and path where you want to restore the file. UNC paths are supported. You can click any combination of the **Add tokens to path** buttons to include that information in the path name. Click **Save changes** after specifying the path.
-



Before restoring files, whether you are restoring to the original location or a different location, make sure you have enough free space for the amount of data being restored. In most cases, the free space must be at least as large as the amount of data you are restoring. In some unique situations, such as restoring a single, large, non-compressible file, you may require free space that is at least two times as large as the file you are restoring so that the non-compressed blocks can be downloaded and the final file created.

- **Overwrite behavior**—Specify how you want to handle the case where a file with the same name already exists.
 - **Overwrite**—Overwrite any existing files.
 - **Rename**—The file that is being restored will be renamed and have `.restored` appended to the file name.
 - **Skip restoring**—If the file already exists, do not restore the file.
 - **Overwrite with newer files and skip matching files**—If the existing file is older, overwrite it. If the existing file has the same or a newer date, do not restore the file.
- **Restoring device**—By default, the file will be restored to the original device. If you want to restore to a different device, click **Change** and select the device you want to restore to and click **Select device**. If the list of devices exceeds the maximum number configured by your administrator, a dialog box displays, prompting you to use the **Search** function to narrow your list of results.

An alternate device must have Carbonite Endpoint installed and activated. If you change your mind, click **Reset to original device** to restore back to the same device.



The following table controls are available when selecting the device to restore to.

- **Show Entries**—Specify the number of rows to be shown in the table on each page. Additional rows over the number you select are shown on additional pages and can be viewed by using the paging buttons at the bottom of the table.
-



This table is limited to 100 rows. If you need to see a list of all entries, use **Download list**.

- **Search**—Text entered in the box narrows the list displayed to only the rows that contain the search text. The search checks the entire table, not just the

visible rows.

- **Sort**—You can sort the table by clicking on any column heading.
 - **Table paging buttons**—The paging buttons at the bottom of the table allow you to move more quickly between pages. Each button jumps to that respective page of the table.
-

- **Include user state load**—Select this option if you want to restore the user state data. You must have backed up the user state using the User State Migration Tool for this functionality to work.
7. Click **Submit** to start the restore. You will be redirected to the **Company** page **Admin restores** tab where you can monitor and control the progress of the restore. For more information, see *View and manage admin restores* on page 140 .

Locate a device

Use this procedure to determine the physical location of a device if the device is using a policy that has **Track device location** enabled.

1. Go to the **Devices** page and click the name of the device you want to locate. See *View devices* on page 112 for details on searching the device table.
2. Click the **Location** tab and wait for the map to appear. The device location is identified with icons for **IP location** and/or **Enhanced location**. You can zoom in or out on the map and change the view of the map between Road, Aerial (similar to a satellite view), and Streetside (a street-level view).
3. If you want to delete the history of captured locations for the device, click **Erase location**. The device will start reporting its location the next time it connects.

Consider the following when viewing the device location.

- There are different methods for reporting locations. For example, the location may be based on WiFi or an IP address based on network traffic. Some devices may not support all reporting methods.
- For macOS devices, Carbonite Endpoint requests permission to use location services when the application is first launched. Click **OK** in the dialog box to allow location services.
- Some devices, for example a virtual machine with a virtual network adapter or a device on a VPN, may not be found because the device cannot be located.
- The **IP location** may not be exact. The **Enhanced location** should be more precise, but depends on the method used to determine the location.
- The last known location is maintained if an error occurs, so that you can view the last location of the device before any errors started.



If Carbonite Endpoint raises a "Location services not authorized" error message, the user must check and then adjust their Windows settings and/or the location registry key so that the device location can be retrieved by Carbonite Endpoint. Both of these settings must be set to **Allow** for the device to report its enhanced location.

To change the location permissions in the Windows settings, go to **Settings > Privacy > Location** and ensure that the **Location for this device** is set to **on**.

The user must also ensure that the following registry key is set to **Allow**:

```
HKEY_
USERS\ .DEFAULT\Software\Microsoft\Windows\CurrentVersion\Capability
AccessManager\ConsentStore\location
```

Some operating systems, for example macOS 10.15 Catalina and later, may have to have location services enabled before they will report location.

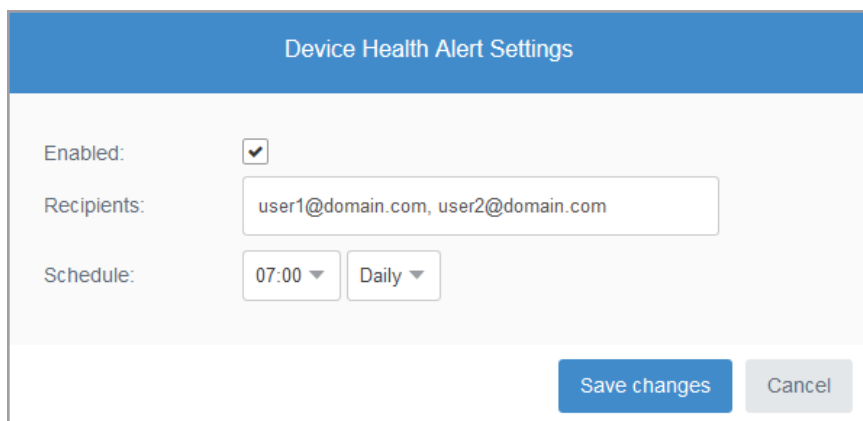
To enable location services for Carbonite Endpoint on a macOS device

1. Under the Apple icon, click **System Preferences > Security & Privacy**, click **Security & Privacy**, then click **Privacy**.
 2. Click **Location Services**.
 3. If the padlock icon is locked, click it to unlock the Preferences Pane.
 4. Select the checkbox next to **Protection Service** to allow Carbonite Endpoint to use location services. You can also select the **Enable Location Services** checkbox at the top of the pane to enable location services for all of the listed apps.
-

Chapter 11 Manage alerts

You can enable alerts (email notifications) to notify you when specific device and QuickCache criteria have been met. You can configure Carbonite Endpoint to email alerts on a daily or weekly interval.

- **Device alerts**—This alert is for devices that have not been backed up in the past seven days, devices that have never been backed up, and for devices that are approaching or have exceeded their storage quota. Devices are excluded from the device alert in the following cases.
 - The device is not actively contacting the vault. If the device was on the report but goes offline for more than three days, it will no longer be on the report regardless of the conditions that placed it on the report originally.
 - The device is experiencing quota issues and either of the following conditions are met.
 - The date and time the device was approaching the quota limit is more than 14 days ago.
 - The device is over quota, quota is not enforced, and the date and time the device reached the quota limit is more than 14 days ago.
 - The device is experiencing backup issues, but the last time the device finished a backup was less than seven days before the device last checked in.
 - The device has never completed a backup, but the last time the device checked in was less than 14 days after the device was activated.
 - **QuickCache alerts**—This alert is for QuickCaches that have been offline for a specified number of days, when the QuickCache is approaching or has exceeded the storage quota for more than 14 days, and when the oldest block is older than a specified number of days.
1. To view or modify your alerts, go to the **Company** page and click the **Alerts** tab.
 2. For the device alert, click **Enable alert** or **Edit alert settings**, depending on if you have an alert configured already.



The screenshot shows a dialog box titled "Device Health Alert Settings". It contains the following fields and controls:

- Enabled:** A checked checkbox.
- Recipients:** A text input field containing "user1@domain.com, user2@domain.com".
- Schedule:** Two dropdown menus. The first is set to "07:00" and the second is set to "Daily".
- At the bottom right, there are two buttons: "Save changes" (highlighted in blue) and "Cancel" (greyed out).

- **Enabled**—Select this option to enable the alert. Clear this check box to disable the alert.
- **Recipients**—Specify a comma-separated list of email addresses. This is where the alerts will be sent.

- **Schedule**—Select an hour of the day, using a 24-hour clock, and the day of the week to indicate when you want the alert emailed. Select **Daily** if you want the alert emailed every day.
3. Click **Save changes**.
 4. For the QuickCache alert, click **Enable alert** or **Edit alert settings**, depending on if you have an alert configured already.

The screenshot shows a dialog box titled "QuickCache Health Alert Settings". It contains several configuration options:

- Enabled:** A checked checkbox.
- Recipients:** A text input field containing "user1@domain.com, user2@domain.com".
- Schedule:** Two dropdown menus, one showing "07:00" and the other showing "Daily".
- Offline for more than:** A dropdown menu showing "1" followed by the text "days".
- Free space is less than:** A dropdown menu showing "50" followed by the text "GB".
- Oldest block is older than:** A dropdown menu showing "7" followed by the text "days".

At the bottom right of the dialog box, there are two buttons: "Save changes" (highlighted in blue) and "Cancel".

- **Enabled**—Select this option to enable the alert. Clear this check box to disable the alert.
 - **Recipients**—Specify a comma-separated list of email addresses. This is where the alerts will be sent.
 - **Schedule**—Select an hour of the day, using a 24-hour clock, and the day of the week to indicate when you want the alert emailed. Select **Daily** if you want the alert emailed every day.
 - **Offline for more than**—Select the number of days a QuickCache has to be offline to trigger the alert.
 - **Free space is less than**—Specify the amount of free space left to trigger the alert.
 - **Oldest block is older than**—Select the number of days the oldest block must be older than to trigger the alert.
5. Click **Save changes**.

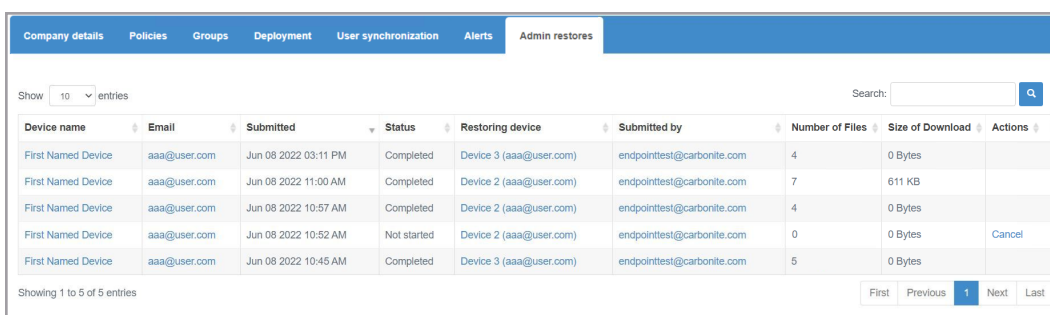
Chapter 12 View and manage admin restores

You can view information about admin restores in the vault dashboard, and cancel admin restores that are in progress.

An admin restore occurs when an administrator restores files from a device. For more information, see *Restore files from a device* on page 132.

1. Go to the **Company** page and click the **Admin restores** tab.

The Admin restores tab lists admin restores, and provides information such as the date and time that the restore was submitted, the status of the restore, the number of files restored and the amount of data that was downloaded from the vault for the restore. Data might not be downloaded from the vault during a restore if some backup data is cached on the device.



Device name	Email	Submitted	Status	Restoring device	Submitted by	Number of Files	Size of Download	Actions
First Named Device	aaa@user.com	Jun 08 2022 03:11 PM	Completed	Device 3 (aaa@user.com)	endpointtest@carbonite.com	4	0 Bytes	
First Named Device	aaa@user.com	Jun 08 2022 11:00 AM	Completed	Device 2 (aaa@user.com)	endpointtest@carbonite.com	7	611 KB	
First Named Device	aaa@user.com	Jun 08 2022 10:57 AM	Completed	Device 2 (aaa@user.com)	endpointtest@carbonite.com	4	0 Bytes	
First Named Device	aaa@user.com	Jun 08 2022 10:52 AM	Not started	Device 2 (aaa@user.com)	endpointtest@carbonite.com	0	0 Bytes	Cancel
First Named Device	aaa@user.com	Jun 08 2022 10:45 AM	Completed	Device 3 (aaa@user.com)	endpointtest@carbonite.com	5	0 Bytes	

2. To find a particular admin restore, do one or more of the following:
 - In the **Search** box, enter text to narrow your list of results. You can search by the source device name, source device username (email), restoring device name, and restoring device username (email).
 - **Show Entries**— Specify the number of rows to show on each page in the table. Additional rows over the number you select are shown on additional pages and can be viewed using the paging buttons at the bottom of the table. You can view a maximum of 100 rows in the table.
 - **Sort**—You can sort the table by clicking on any column heading.
 - **Table paging buttons**—The paging buttons at the bottom of the table allow you to move more quickly between pages. Each button jumps to that respective page of the table.
3. To view more information, click one of the following hyperlinks for an admin restore:
 - **Device name**—Indicates the source device name. Clicking this hyperlink opens the **Device details** tab on the **Devices** page. See *View device details* on page 118 for details.
 - **Email**—Indicates the source device user name. Clicking this hyperlink opens the **User details** tab on the **User** page for the user whose device is being restored. See *View user details* on page 71 for details.
 - **Restoring device**—Indicates the target device name. Clicking this hyperlink opens the **Activity** tab on the **Devices** page. See *View device activity* on page 127 for details.
 - **Submitted by**—Indicates the user who initiated the restore. Clicking this hyperlink opens the **User details** tab on the **User** page. See *View user details* on page 71 for details.

4. To cancel an admin restore that is in progress, click the **Cancel** hyperlink in the admin restore row.

Chapter 13 Manage reports

You can add, view, and delete reports that detail your Carbonite Endpoint activity. The following tasks are available for reports.

- *View a list of available reports* on page 142
- *Add a report* on page 143
- *View a report* on page 144
- *Delete a report* on page 145

View a list of available reports

Use this procedure to view a list of available reports.

- Go to the **Reports** page to display high-level information for your reports.

Home / Reports

Reports

+ Add new report

Show 10 entries Search:

Report name	Report type	Level	Organizational unit	Date range
Company report	Organizational breakdown report	Company	CompanyName	Current
Current jobs	Time based report	Depends on user's roles	Depends on user's roles	Current
Device report	Device details report	Depends on user's roles	Depends on user's roles	Current
Recent jobs	Time based report	Depends on user's roles	Depends on user's roles	Last 30 days
Users report	User details report	Depends on user's roles	Depends on user's roles	Current

Showing 1 to 5 of 5 entries

First Previous 1 Next Last

You have the following toolbar and table controls available on the **Users** page.

- **Add new report**—Click this button to add a new report. See *Add a report* on page 143 for details.
- **Show Entries**—Specify the number of rows to show on each page in the table. Additional rows over the number you select are shown on additional pages and can be viewed using the paging buttons at the bottom of the table. You can view a maximum of 100 rows in the table.
- **Search**—Text entered in the box narrows the list displayed to only the rows that contain the search text. The search checks the entire table, not just the visible rows.

- **Sort**—You can sort the table by clicking on any column heading.
- **Table hyperlinks**—Click on any hyperlink in the table and it will take you to the view for that report. See *View a report* on page 144.
- **Table paging buttons**—The paging buttons at the bottom of the table allow you to move more quickly between pages. Each button jumps to that respective page of the table.

Add a report

Use this procedure to add a new report.

1. Open the **Reports** page and click **Add new report**.
2. Specify the report settings.

The screenshot shows the 'Add new report' form with the following settings:

- Report name:** Company report
- Report layout:** Stretch report to full width of screen
- Report visibility:** Personal report
- Report type:** Time based report
- Report dates:** Current
- Organization:** Depends on user's roles
- Policy sets to include:** Include all policy sets

Available data points:

- Last backup job
- Last restore job
- Last vault erase job
- All backup jobs
- All restore jobs
- All vault erase jobs
- All jobs
- Devices created
- Devices activated
- Devices reset
- Devices data deleted

Report data points:

Data point	Show	
All jobs	Count	Move up
All backup jobs	Count	
All restore jobs	Count	Move down
Active devices	Count	
Users	Count	

Buttons: Add data point >, Show: Count, < Remove data point, Load report preview, Save report, Cancel

- **Report name**—Specify a unique name for the report.
- **Report layout**—Select a layout for the report.
- **Report visibility**—Select if you want the report to be only visible to you or to be shared with others. You may not be able to share the report with others depending on your login permissions. If a report is shared, users can only see the data they have access to.

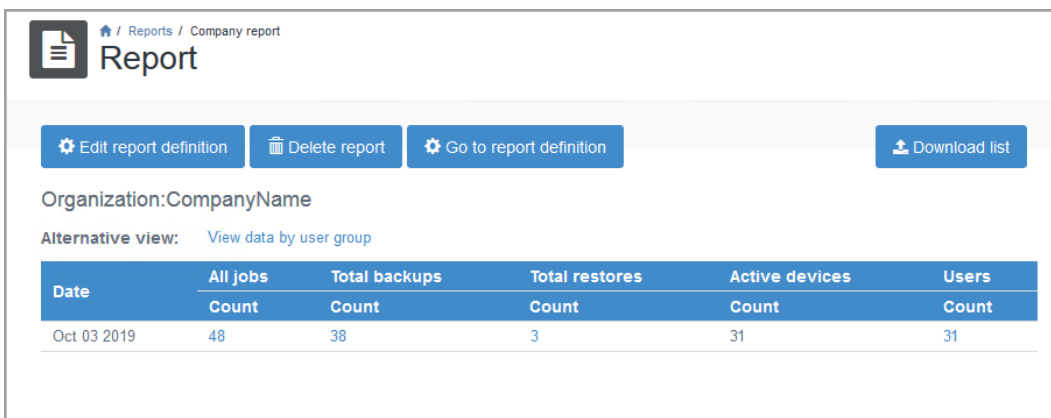
- **Report type**—Specify the type of report you want to add.
 - **Time based report**—These reports are based on time.
 - **Organizational breakdown report**—These reports are based on the company or group.
 - **Device details report**—These reports list all devices.
 - **User details report**—These reports list all users.
- **Report dates**—For time-based reports, select the time frame you want to use when generating the report.
- **Organization**—Select the organization you want the report data to be generated from. These options will depend on your login permissions.
- **Policy sets to include**—Select if you want to include all policy sets in the report data.
- **Available data points**—Select the data you want in the report by selecting an item in the **Available data points** list and clicking **Add data point**. Some data points have choices under **Show** to allow you to select how you want the data point displayed. If you want to remove a data point from the report, select it in the **Report data points** list and click **Remove data point**.

Once you have all of your data points in the **Report data points** list, click **Move up** or **Move down** to organize the data.

3. As you are adding your report, click **Load report preview** at any time to see what your report will look like.
4. When your report is complete, click **Save report**.

View a report

After you have added a report, you can view it by going to the **Reports** page and clicking the name of the report you want to view. See *View a list of available reports* on page 142 for details on searching the reports table. The view of the report will vary depending on the type of report and the data in the report, but you will find the report in a table on the displayed page. The controls and links on the report will also vary.



The screenshot shows a report view for 'Company report'. It includes a breadcrumb trail, a title 'Report', and several action buttons: 'Edit report definition', 'Delete report', 'Go to report definition', and 'Download list'. Below the buttons, the organization is identified as 'CompanyName'. An 'Alternative view' option is available to 'View data by user group'. A table displays the following data:

Date	All jobs Count	Total backups Count	Total restores Count	Active devices Count	Users Count
Oct 03 2019	48	38	3	31	31

The following lists the functions and controls when viewing a report, however, what you see will vary based on the type of report you are viewing.

- **Edit report definition**—Click this button to edit a report. The report options are the same as when you added the report. See *Add a report* on page 143 for details.
- **Delete report**—Click this button to delete a report. See *Delete a report* on page 145 for details.
- **Go to report definition**—Click this button to view the definition and criteria used to generate the report.
- **Download list**—Click this button to download the report in a list format. The list will be downloaded to your local computer. You can download a Microsoft Excel (.xlsx) file or a comma-delimited file (.csv). If you download the Excel format, you must enable editing for any hyperlinks to the portal to be active.
- **Alternative view**—Click this link to see the report data in a different view. For example, instead of seeing the data by a date, you might want to see it by groups.
- **Show Entries**—Specify the number of rows to be shown in the table on each page. Additional rows over the number you select are shown on additional pages and can be viewed by using the paging buttons at the bottom of the table.



This table is limited to 100 rows. If you need to see a list of all entries, use **Download list**.

- **Table hyperlinks**—Many of the report table entries are hyperlinks. Click on any hyperlink to go to the related page that shows details for that data set.
- **Additional row information**—If all of the report data cannot be shown in the table easily for the size screen you are viewing, you will see a plus sign at the left of the table row. Click this button to see additional report data for that table row.
- **Table paging buttons**—The paging buttons at the bottom of the table allow you to move more quickly between pages. Each button jumps to that respective page of the table.

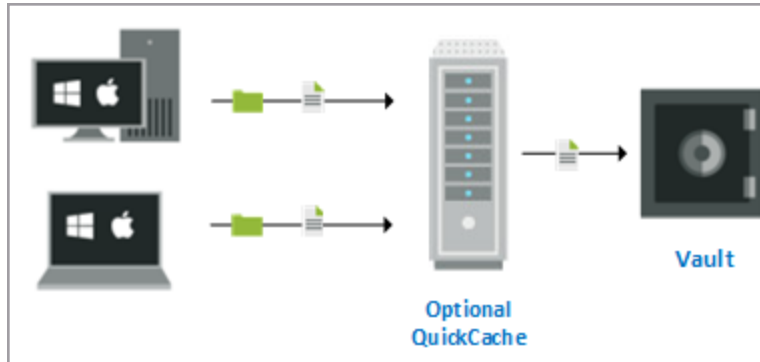
Delete a report

If you no longer need a report, you can delete it.

1. Go to the **Reports** page and click the name of the report you want to delete. See *View a list of available reports* on page 142 for details on searching the report table.
2. On the report view, click **Delete report**.
3. Click **OK** to delete the report.

Chapter 14 Create and manage a QuickCache

QuickCache is an optional backup location used for faster backups in local environments and increased bandwidth management to the vault. It is also used for faster restores of recent data.



If there is no QuickCache or it is offline, devices send all backup data directly to the vault, however, when a QuickCache is online on the network, each device configured to use that QuickCache will send all backup data to the QuickCache. Devices will still send activity updates directly to the vault so that information can be displayed in the dashboard. Devices will upload to the QuickCache as fast as the local network allows, unless device to QuickCache limits are configured.

All data on the QuickCache is then sent to the vault. The QuickCache can be configured for peak and off-peak speeds when transferring data from the QuickCache to the vault. Peak and off-peak hours are configurable and are based on the time zone configured for the QuickCache.

During a restore, if the data is still on the QuickCache, the restore will use that data. If the data is not on the QuickCache, the QuickCache will download the data from the vault and send it to the device. Like backing up the data, you can configure download speeds from the vault to the QuickCache for peak and off-peak hours.

Keep in mind the QuickCache is not a write-through queue. One advantage of a QuickCache is to have a local copy of recent data for faster restores. The QuickCache uses as much storage as it has been allocated, and when the allocated storage has been used, it removes the oldest data, keeping just enough free space for incoming data. If there is nothing pending on the QuickCache, that does not indicate the QuickCache is empty, only that all data on it has been uploaded to the vault. The QuickCache will upload as soon as the configured schedule allows it. It does not remove any data after it uploads. It only removes data when it needs space.

The QuickCache machine must have Windows Server 2016 (English, EN-US locale) with a least 1 TB of disk space and a minimum of 2 GB of RAM. Ideally, you should have 4 GB of RAM.

The following tasks are available for QuickCaches.

- *View available QuickCaches* on page 147
- *Add a QuickCache* on page 148
- *View QuickCache activity* on page 150
- *View QuickCache details* on page 150
- *Edit QuickCache server settings* on page 151

- *Manage the QuickCache bandwidth schedule* on page 152
- *Manage a QuickCache* on page 154
- *Assign a QuickCache to a device* on page 156
- *Delete a QuickCache* on page 156

View available QuickCaches

Use this procedure to view available QuickCaches.

- Go to the **QuickCaches** page to display high-level information for your QuickCaches.

You have the following toolbar and table controls available on the **QuickCaches** page.

- **Add QuickCache**—Click this button to add a new QuickCache. See *Add a QuickCache* on page 148 for details.
- **Download list**—Click this button to download a complete QuickCache list to your local computer. You can download a Microsoft Excel (.xlsx) file or a comma-delimited file (.csv). If you download the Excel format, you must enable editing for any hyperlinks to the portal to be active.
- **Show Entries**—Specify the number of rows to be shown in the table on each page. Additional rows over the number you select are shown on additional pages and can be viewed by using the paging buttons at the bottom of the table.



This table is limited to 34 rows. If you need to see a list of all entries, use **Download list**.

- **Search**—Text entered in the box narrows the list displayed to only the rows that contain the search text. The search checks the entire table, not just the visible rows.
- **Sort**—You can sort the table by clicking on any column heading.
- **Table hyperlinks**—There are hyperlinks in the table that will take you directly to a page in the dashboard.

- **QuickCache name**—This hyperlink will take you to the **QuickCache activity** tab on the **QuickCache** page. See *View QuickCache activity* on page 150 for details.
- **Company**—This hyperlink will take you to the **Company** page. See *View and manage your company* on page 19 for details.
- **Table paging buttons**—The paging buttons at the bottom of the table allow you to move more quickly between pages. Each button jumps to that respective page of the table.

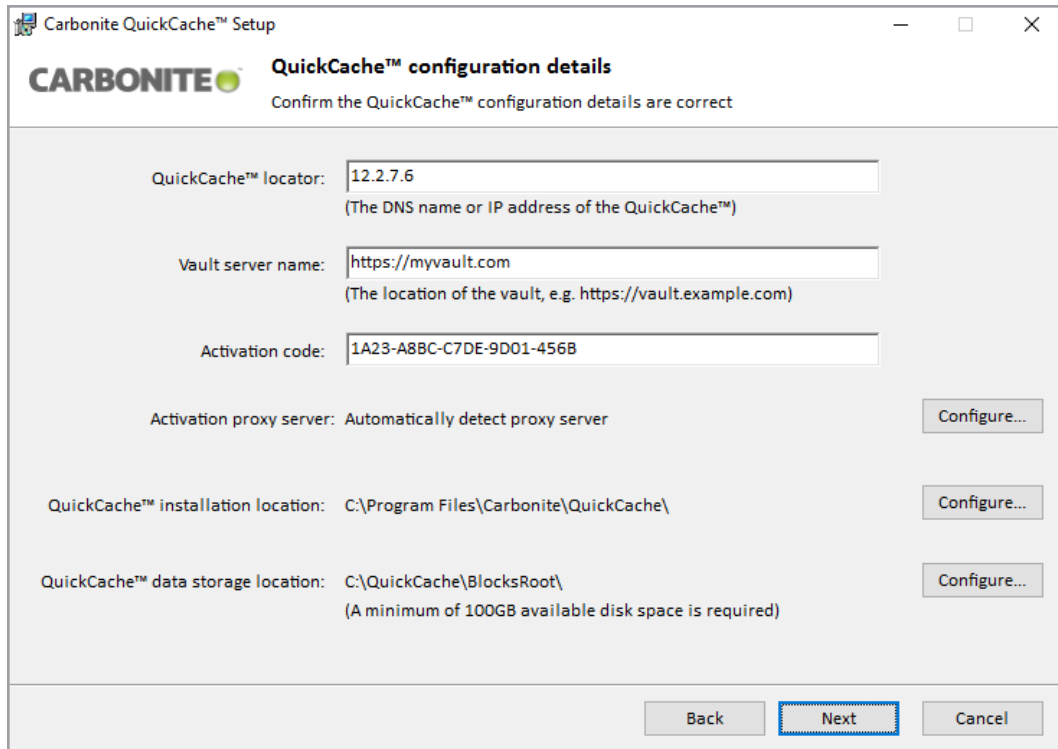
Add a QuickCache

Use this procedure to add a QuickCache.

1. On the **Company** or **QuickCaches** page, click **Add QuickCache**.
2. Configure the following QuickCache settings.

The screenshot shows the 'Add QuickCache' form in the QuickCache™ interface. The form has a blue header with the title 'Add QuickCache'. Below the header, there are four input fields: 'QuickCache name' with the value 'QuickCache1', 'Company' with the value 'CompanyName', 'Time zone' with a dropdown menu showing '(UTC-05:00) Eastern Time (US &...)', and 'Comment' which is empty. At the bottom right of the form, there are two buttons: 'Add QuickCache' (highlighted in blue) and 'Cancel' (greyed out).

- **QuickCache name**—Specify a unique name for the QuickCache.
 - **Time zone**—Specify the time zone where the QuickCache is located. This time zone will be used to determine peak hours and off-peak hours for bandwidth management.
 - **Comment**—Specify a comment to describe the QuickCache.
3. Click **Add QuickCache**.
 4. The **QuickCache details** tab appears. Copy the **Activation code** that is displayed. This code is required for the next section of the creation process.
 5. Complete the following steps on the server you want to use as the QuickCache.
 - a. Download the QuickCache installation package from <http://dcgeneral.blob.core.windows.net/ceb/QuickCache/KB/QuickCacheInstaller.EXE>.
 - b. Start the QuickCache installation and wait for the license agreement page to open. This may take several minutes while the installation configures the server.
 - c. Accept the terms of the license agreement and click **Next**.
 - d. Configure the QuickCache.

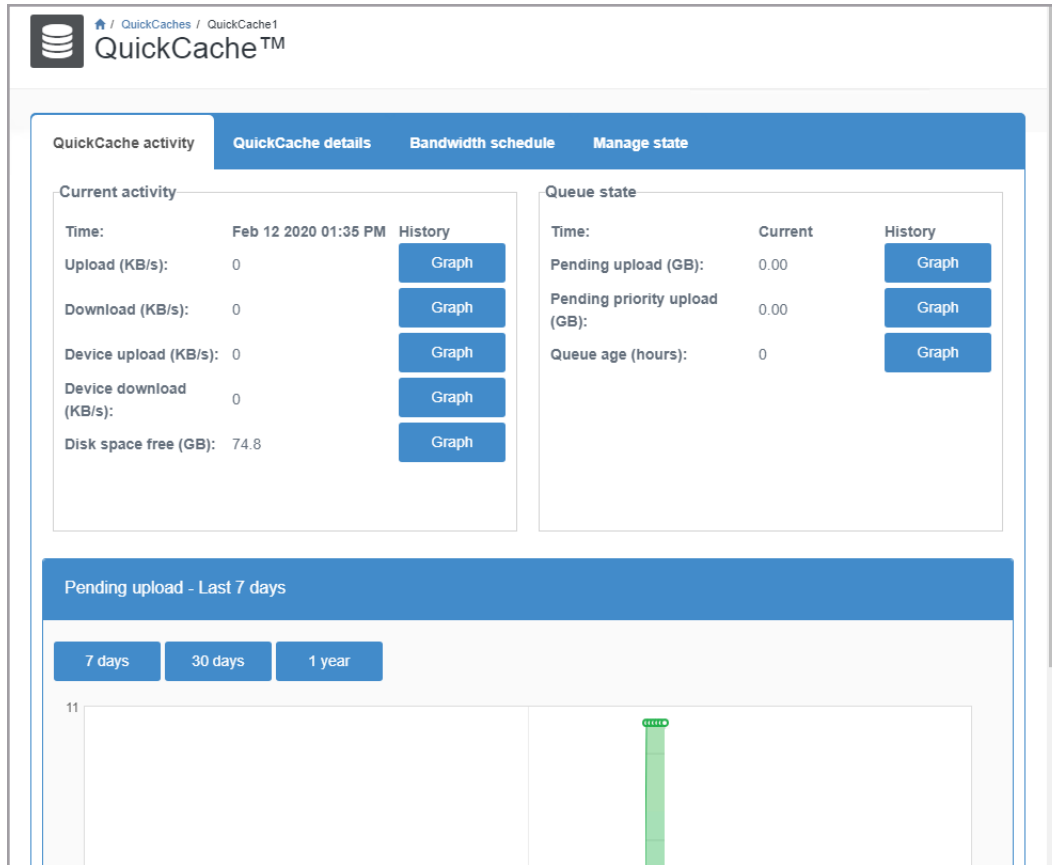


- **QuickCache locator**—Specify the DNS name or IP address of your QuickCache server. Devices will connect to the QuickCache using this locator.
 - **Vault server name**—Specify the URL for the vault where the QuickCache should send data.
 - **Activation code**—Specify the activation code that you copied above in step 4 when you added the QuickCache in the dashboard.
 - **Activation proxy server**—If you need to specify no proxy server or configure specific settings for a proxy server for QuickCache to vault communication, click **Configure**. Specify no server or the proxy server configuration to use and, if needed, authentication credentials and click **OK**.
 - **QuickCache installation location**—If you want to change the default installation location, click **Configure**. Select a new location and click **OK**.
 - **QuickCache data storage location**—If you want to change the location where device data is stored, click **Configure**. Select a new location and click **OK**. You must select a location with a least 100 GB of disk space.
- e. Click **Next** to continue.
 - f. Click **Install** to begin the installation.
 - g. When the installation is complete, click **Finish**.
6. Open the **QuickCache** page and to display the updated information.

View QuickCache activity

Use this procedure to view activity on a QuickCache.

1. Go to the **QuickCaches** page and click the name of the QuickCache you want to view. See *View available QuickCaches* on page 147 for details on searching the QuickCache table.
2. Click the **QuickCache activity** tab to view the QuickCache activity.



The following QuickCache activity information is provided:

- **Current activity**—This section displays the current activity on the QuickCache at the date and time indicated.
- **Queue state**—This section displays the state of the QuickCache queue from the QuickCache to the vault.
- **Graph**—Click any **Graph** button to change the graph shown at the bottom of the page to that activity. The graph data is the average over an hour for the time period selected.

View QuickCache details

Use this procedure to view details for a QuickCache.

1. Go to the **QuickCaches** page and click the name of the QuickCache you want to view. See *View available QuickCaches* on page 147 for details on searching the QuickCache table.

2. Click the **QuickCache details** tab to display details for the QuickCache.

QuickCache activity		QuickCache details		Bandwidth schedule		Manage state	
QuickCache name:		QuickCache1		Company:		CompanyName	
QuickCache id:		123abc-4d56-789e-fab0-123c45d678e9		Locator:		112.42.7.56:5010	
Status:		Activated		Activation code:		1A23-456B-C7DE-A8BC-9D01	
Free space:		74.8 of 110.00 GB (68%)		QuickCache version:		9.5.0.2910	
Last status update time:		Feb 12 2020 01:35 PM		Created time:		Feb 12 2020 07:52 AM	
Operating system:		Microsoft Windows Server 2016 Datacenter		Activated time:		Feb 12 2020 09:35 AM	
OS edition:		Server Datacenter (full installation)		Upload rate (KB/s):			
Service pack:				Download rate (KB/s):			
OS revision:		0		Device upload rate (KB/s):			
OS build:		9200		Device download rate (KB/s):			
OS version:							
OS bit size:		64					
Memory installed:		4 GB					

The following details are provided.

- **Edit QuickCache**—Click this button to modify the QuickCache settings. See *Edit QuickCache server settings* on page 151 for details.
- **Table hyperlinks**—The **Company** hyperlink will take you to the **Company** page. See *View and manage your company* on page 19 for details.

Edit QuickCache server settings

Use this procedure to edit QuickCache server settings.

1. To edit the QuickCache server settings, go to the **QuickCaches** page and click the name of the QuickCache you want to edit. See *View available QuickCaches* on page 147 for details on searching the QuickCache table.
2. Click the **QuickCache details** tab and click **Edit QuickCache**.
3. Modify the QuickCache server settings as needed. See *Add a QuickCache* on page 148 for details on the QuickCache settings.

Edit QuickCache details

QuickCache name:

Locator host name:

Note: This name is used by devices to locate the QuickCache. An IP address or machine name can be used. Devices will pickup any change automatically. Ensure your network and QuickCache is configured to respond to this.

Locator port number:

Note: This port is used by devices to locate the QuickCache. A change is automatically picked up by devices and the QuickCache. You need to manually make firewall changes to allow traffic to the QuickCache.

Comment:

4. After you have modified the QuickCache settings, click **Save changes**.

Manage the QuickCache bandwidth schedule

Use this procedure to manage the QuickCache bandwidth schedule.

1. Go to the **QuickCaches** page and click the name of the QuickCache you want to manage. See *View available QuickCaches* on page 147 for details on searching the QuickCache table.
2. On the **QuickCache** page, click the **Bandwidth schedule** tab.
3. Review the **Speed limits**. If you want to modify any of the limits, click **Edit speed limits**.

The screenshot shows the QuickCache™ management interface. At the top, there is a navigation bar with four tabs: "QuickCache activity", "QuickCache details", "Bandwidth schedule", and "Manage state". Below the navigation bar is a section titled "Speed limits" with a blue header. In the top right corner of this section is a button labeled "Edit speed limits" with a gear icon. The main content is divided into two sections: "Peak time period" and "Off-peak time period". Each section contains a table of speed limits.

Peak time period	
Maximum upload speed from QuickCache to vault:	300 KB/s
Maximum priority upload speed from QuickCache to vault:	1000 KB/s
Maximum priority download speed from vault to QuickCache:	1000 KB/s
Note: Priority speed limits are used when a device requests data for restore.	

Off-peak time period	
Maximum upload speed from QuickCache to vault:	2000 KB/s
Maximum priority upload speed from QuickCache to vault:	5000 KB/s
Maximum priority download speed from vault to QuickCache:	5000 KB/s
Note: Priority speed limits are used when a device requests data for restore.	

In the Edit speed limits dialog box, change any of the following settings:

- **Peak time period**
 - **Maximum upload speed from QuickCache to vault**—Indicates the speed, in KB/s, that will be used when sending data during the peak time period from the QuickCache to the vault.
 - **Maximum priority upload speed from QuickCache to vault**—When a device is attempting to restore, the files in the upload queue will use this speed, in KB/s, to send the data during the peak time period from the QuickCache to the vault.
 - **Maximum priority download speed from vault to QuickCache**—When a device is attempting to restore, files that are not on the vault will use this speed, in KB/s, to send the data during the peak time period from the vault to the QuickCache.
- **Off-peak time period**
 - **Maximum upload speed from QuickCache to vault**—This is the speed, in KB/s, that will be used when sending data during the off-peak time period from the QuickCache to the vault.
 - **Maximum priority upload speed from QuickCache to vault**—When a device is attempting to restore, the files in the upload queue will use this speed, in KB/s, to send the data during the off-peak time period from the QuickCache to the vault.
 - **Maximum priority download speed from vault to QuickCache**—When a device is attempting to restore, files that are not on the vault will use this speed, in

KB/s, to send the data during the off-peak time period from the vault to the QuickCache.

- **Device to QuickCache limits**

- **Maximum upload speed from a device to QuickCache**—This is the speed, in KB/s, that will be used, unless a lower limit is established by policy, when sending data from a device to the QuickCache.
- **Maximum download speed from QuickCache to device**—This is the speed, in KB/s, that will be used, unless a lower limit is established by policy, when sending data from the QuickCache to a device.

4. Click **Save changes**.
5. Review the Off-peak hours. If you want to modify the hours, click **Edit off-peak hours**, make the modifications, and then click **Save changes**. Off-peak hours are indicated by a green check mark. Peak hours have no indicator.

Off-peak hours

Time (UTC-05:00) Eastern Time (US & Canada)
zone:

Edit off-peak hours

Off-peak hours:

Time	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Mon	✓	✓	✓	✓	✓	✓	✓	✓											✓	✓	✓	✓	✓	✓
Tue	✓	✓	✓	✓	✓	✓	✓	✓											✓	✓	✓	✓	✓	✓
Wed	✓	✓	✓	✓	✓	✓	✓	✓											✓	✓	✓	✓	✓	✓
Thurs	✓	✓	✓	✓	✓	✓	✓	✓											✓	✓	✓	✓	✓	✓
Fri	✓	✓	✓	✓	✓	✓	✓	✓											✓	✓	✓	✓	✓	✓
Sat	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Sun	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Manage a QuickCache

Use this procedure to manage a QuickCache.

1. Go to the **QuickCaches** page and click the name of the QuickCache you want to manage. See *View available QuickCaches* on page 147 for details on searching the QuickCache table.
2. On the **QuickCache** page, click the **Manage state** tab to view the available tasks.

QuickCache™

QuickCaches / QuickCache1

QuickCache activity QuickCache details Bandwidth schedule Manage state

This QuickCache is Activated. Devices allocated to this QuickCache will backup and restore through it. The QuickCache will upload queued data to the vault. Changing the state will mean that devices allocated to this QuickCache will backup and restore directly with the vault.

Pause QuickCache	Devices restoring data will wait for the QuickCache to be available if the data needed is in the upload queue on this QuickCache.
Suspend QuickCache	Devices restoring data will get errors for files if the data needed is in the upload queue on this QuickCache.
Make unavailable to devices	Enable the QuickCache to keep uploading or downloading data but don't allow devices to use it.
Cancel QuickCache	QuickCache will be permanently cancelled; this action is not reversible.



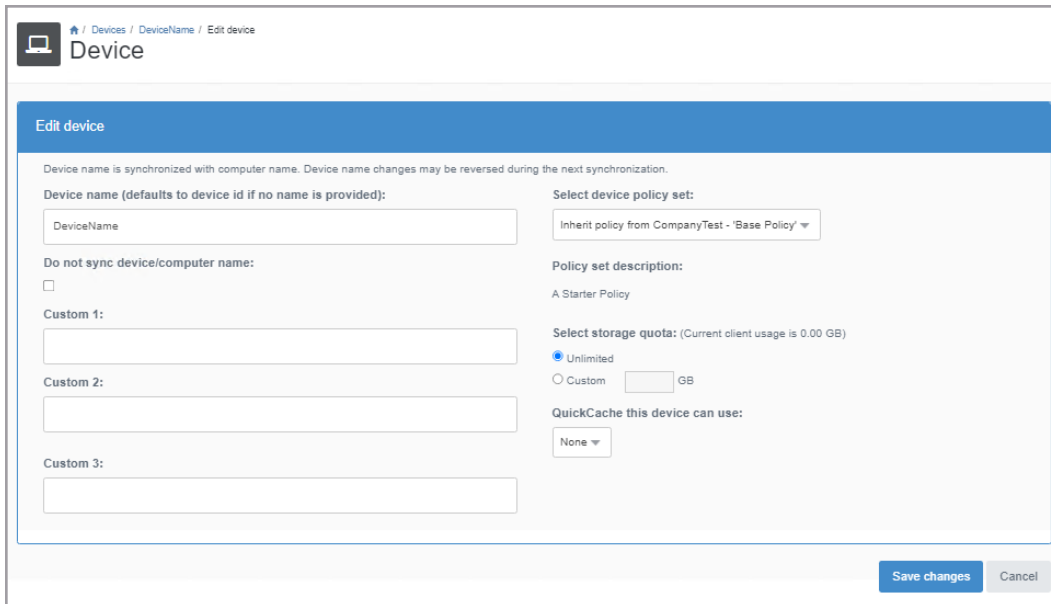
The available tasks depend on the state of the QuickCache.

- **Pause QuickCache**—Click this button to pause the QuickCache. This will stop all upload activity from devices to the QuickCache and from the QuickCache to the vault. It will also stop all download activity from the vault to the QuickCache and from the QuickCache to all devices. Devices will upload and download directly from the vault when the QuickCache is paused. Keep in mind that devices that are restoring data that is in the QuickCache upload queue will have to wait until the QuickCache is restarted before the restore will complete. When prompted, confirm the pause by clicking **OK**.
 - **Reactivate QuickCache**—Click this button when you want to restart a paused QuickCache. All uploads and downloads will use the QuickCache once it is reactivated. When prompted, confirm the reactivation by clicking **OK**.
- **Suspend QuickCache**—Click this button to suspend the QuickCache. This action is identical to pausing a QuickCache, except devices that are restoring data that is in the QuickCache upload queue will get errors instead of waiting to complete the restore. When prompted, confirm the suspension by clicking **OK**.
 - **Reactivate QuickCache**—Click this button when you want to restart a suspended QuickCache. All uploads and downloads will use the QuickCache once it is reactivated. When prompted, confirm the reactivation by clicking **OK**.
- **Make unavailable to devices**—Click this button to make the QuickCache unavailable to devices only. Data will continued to be uploaded to and downloaded from the vault. When prompted, confirm making the QuickCache unavailable by clicking **OK**.
 - **Reactivate QuickCache**—Click this button when you want to make the QuickCache available to devices again. When prompted, confirm the reactivation by clicking **OK**.
- **Cancel QuickCache**—Click this button if you want to delete the QuickCache. This action cannot be undone. Confirm you want to delete the QuickCache and click **OK**.

Assign a QuickCache to a device

Use this procedure to assign a QuickCache to a device.

1. Go to the **Devices** page and click the name of the device to which you want to assign the QuickCache. See *View devices* on page 112 for details on searching the device table.
2. Click the **Device details** tab and click **Edit device**.
3. Select a QuickCache in the **QuickCache this device can use** list.



4. After you have modified the device settings, click **Save changes**.

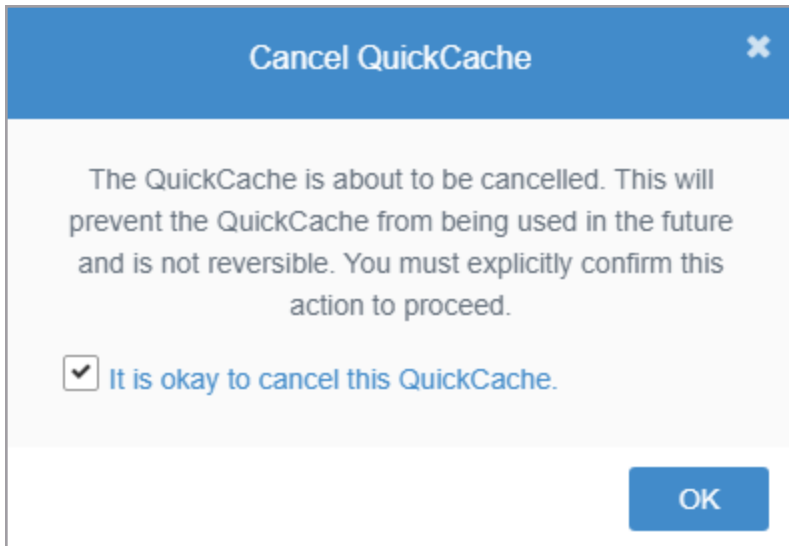
The QuickCache displays under the Device details tab as a hyperlink.

Delete a QuickCache

Use this procedure to delete a QuickCache.

When you delete a QuickCache, devices will upload and download directly from the vault. Deleting a QuickCache cannot be undone. Any devices that were assigned to the QuickCache you are deleting will be assigned to no QuickCache.

1. Go to the **QuickCaches** page and click the name of the QuickCache you want to delete. See *View available QuickCaches* on page 147 for details on searching the QuickCache table.
2. Click the **Manage state** tab on the **QuickCache** page and click **Cancel QuickCache**.



3. Confirm you want to delete the QuickCache and click **OK**.

Chapter 15 Single sign-on

Single sign-on allows users to log in using their existing company user name and password. If your company has a SAML 2.0 compliant identity provider, you can use this service to validate user identity. When using single sign-on, all logins go to the identity provider. The identity provider passes SAML tokens to Carbonite Endpoint, which uses the email address in the SAML token to find the user in the Carbonite Endpoint database. Users' permissions within Carbonite Endpoint are defined by their Carbonite Endpoint user configuration, not their identity provider configuration.



Users must exist in Carbonite Endpoint even if you are using single sign-on. You can use the LDAP feature to automatically add users from a company directory. See *Manage users with LDAP* on page 99 for details.

If you want to have two-factor authentication, you will need to integrate with a SAML-compliant single sign-on provider.

The ability to enable and configure single sign-on through the console is hidden by default on all Carbonite vaults. If you are using another vault, you will need to work with Carbonite Professional Services to expose single sign-on in the console. Once it is visible in the console, you can enable and configure it.

The following tasks are available for single sign-on.

- *View single sign-on details* on page 158
- *Enable single sign-on for the first time* on page 159
- *Edit single sign-on configuration* on page 161
- *Disable single sign-on for one user* on page 162
- *Disable single sign-on* on page 163



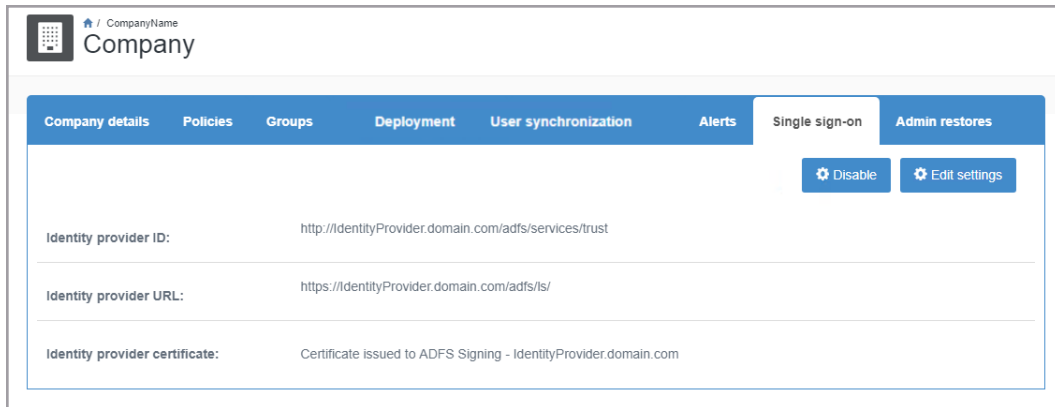
You may want to consider having an admin user in your company that has single sign-on disabled specifically for that user. That way if there are issues with your single sign-on or your identity provider, you can still have an admin user who can log in to Carbonite Endpoint. See *Disable single sign-on for one user* on page 162 for details.

View single sign-on details

Use this procedure to view single sign-on details.

- Go to the **Company** page and click **Single sign-on**.

The single sign-on details for your company display. (The ability to enable and configure single sign-on through the console is hidden by default on all Carbonite vaults. If you are using another vault, you will need to work with Carbonite Professional Services to expose single sign-on in the console. Once it is visible in the console, you can enable and configure it.)



You have the following toolbar controls available on the **Single sign-on** tab.

- **Disable**—Click this button to disable single-sign on. Users will no longer be using the identity service provider for single sign-on. They will be logging in to Carbonite Endpoint directly.
- **Enable**—Click this button to re-enable single-sign on that has been disabled. Users will go back to using the identity service provider for single sign-on.



If you see the **Enable** button but do not see the identity provider details, you have not yet configured single sign-on. See *Enable single sign-on for the first time* on page 159 for details.

- **Edit settings**—Click this button to edit the identity provider configuration. See *Edit single sign-on configuration* on page 161 for details.

Enable single sign-on for the first time

Use this procedure to enable single sign-on for the first time.

The ability to enable and configure single sign-on through the console is hidden by default on all Carbonite vaults. If you are using another vault, you will need to work with Carbonite Professional Services to expose single sign-on in the console. Once it is visible in the console, you can enable and configure it.

1. On the **Company** page, click **Single sign-on**.

CompanyName
Company

Company details Policies Groups Deployment User synchronization Alerts Single sign-on Admin restores

Single sign-on allows users to login to the Dashboard and Access sites using their existing company username and password. If your company has set up a SAML 2.0 compliant Identity Provider, such as Active Directory Federation Services 2.0 (ADFS), you can use this service to validate user identity. Once single sign-on is enabled, all logins will go to the Identity Provider. Users must exist in the dashboard and it is common to use the LDAP sync feature to automatically create users from the company directory. Click "Enable" to configure single sign-on.

Enable

2. Specify your single sign-on configuration.

CompanyName
Company

Company details Policies Groups Deployment User synchronization Alerts Single sign-on Admin restores

Identity provider ID:

Identity provider URL:

Identity provider certificate:

Save Cancel



After each field description are two examples for Active Directory Federation Services 2.0 (ADFS) and Okta. If you are uncertain about how to configure ADFS or Okta or are using a different identity provider (Azure AD, Google, and so on), see the documentation for your identity provider. Okta provides Carbonite Endpoint specific single sign-on documentation at https://saml-doc.okta.com/SAML_Docs/How-to-Configure-SAML-2.0-for-Carbonite-Endpoint-Protection.html.

Keep in mind that Okta cannot use URLs that contain an underscore. If your identity provider server has an underscore in the name, you will need to change that before using Okta for single sign-on.

- **Identity provider ID**—Specify the ID of the identity provider.
 - **ADFS**—Specify the **Federation Service Identifier** found in the **Federation Service Properties**.
 - **Okta**—Specify the **Identity Provider Issuer** found in the **View Setup Instructions** on the **Sign-On** settings for the new application you added using the Okta classic UI.
- **Identity provider URL**—Specify the URL of your identity provider.
 - **ADFS**—Specify secure http (meaning use https://), the host name of your ADFS server, and /adfs/ls. For example, if the identity provider ID is

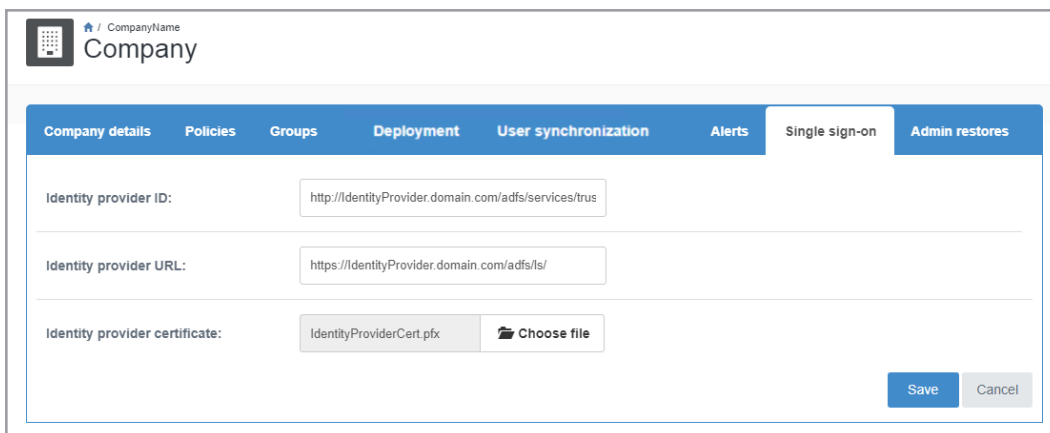
`http://IdentityProvider.domain.com/adfs/services/trust`, then your URL would be `https://IdentityProvider.domain.com/adfs/ls`.

- **Okta**—Specify the **Identity Provider Single Sign-On URL** found in the **View Setup Instructions** on the **Sign-On** settings for the new application you added using the Okta classic UI.
 - **Identity provider certificate**—Specify the secure certificate to use with the identity provider.
 - **ADFS**—Use the exported .cer file from the ADFS server.
 - **Okta**—Use the X.509 certificate downloaded from the **View Setup Instructions** on the **Sign-On** settings for the new application you added using the Okta classic UI.
3. Once the identity provider and certificate are configured, click **Save**.

Edit single sign-on configuration

Use this procedure to edit your single sign-on configuration.

1. Go to the **Company** page and click **Single sign-on**.
2. Click **Edit settings**.
3. Modify the identity provider configuration as needed.



The screenshot shows the 'Single sign-on' configuration page in the Okta Admin Console. The page is titled 'Company' and has a navigation bar with tabs for 'Company details', 'Policies', 'Groups', 'Deployment', 'User synchronization', 'Alerts', 'Single sign-on', and 'Admin restores'. The 'Single sign-on' tab is active. The configuration fields are:

- Identity provider ID:** `http://IdentityProvider.domain.com/adfs/services/trust`
- Identity provider URL:** `https://IdentityProvider.domain.com/adfs/ls/`
- Identity provider certificate:** `IdentityProviderCert.pfx` and a **Choose file** button.

At the bottom right, there are **Save** and **Cancel** buttons.



After each field description are two examples for Active Directory Federation Services 2.0 (ADFS) and Okta. If you are uncertain about how to configure ADFS or Okta or are using a different identity provider (Azure AD, Google, and so on), see the documentation for your identity provider. Okta provides Carbonite Endpoint specific single sign-on documentation at https://saml-doc.okta.com/SAML_Docs/How-to-Configure-SAML-2.0-for-Carbonite-Endpoint-Protection.html.

Keep in mind that Okta cannot use URLs that contain an underscore. If your identity provider server has an underscore in the name, you will need to change that before using Okta for single sign-on.

- **Identity provider ID**—Specify the ID of the identity provider.
 - **ADFS**—Specify the **Federation Service Identifier** found in the **Federation Service Properties**.
 - **Okta**—Specify the **Identity Provider Issuer** found in the **View Setup Instructions** on the **Sign-On** settings for the new application you added using the Okta classic UI.
 - **Identity provider URL**—Specify the URL of your identity provider.
 - **ADFS**—Specify secure http (meaning use https://), the host name of your ADFS server, and /adfs/ls. For example, if the identity provider ID is http://IdentityProvider.domain.com/adfs/services/trust, then your URL would be https://IdentityProvider.domain.com/adfs/ls.
 - **Okta**—Specify the **Identity Provider Single Sign-On URL** found in the **View Setup Instructions** on the **Sign-On** settings for the new application you added using the Okta classic UI.
 - **Identity provider certificate**—Specify the secure certificate to use with the identity provider.
 - **ADFS**—Use the exported .cer file from the ADFS server.
 - **Okta**—Use the X.509 certificate downloaded from the **View Setup Instructions** on the **Sign-On** settings for the new application you added using the Okta classic UI.
4. Once the identity provider and certificate are configured, click **Save**.

Disable single sign-on for one user

Use this procedure to disable single sign-on for one user.

You can disable single sign-on for a specific user, if needed. For example, if there are issues with your single sign-on or your identity provider. In this case, you can still have an admin user who can log in to Carbonite Endpoint.

1. Go to the **Users** page and click the name of the user you want to disable single sign-on for. See *View users* on page 69 for details on searching the user table.
2. Click the **User details** tab and then click **Edit user details**.
3. Click the **Password managed locally** check box.

4. Click **Save changes**.

Disable single sign-on

Use this procedure to disable single sign-on.

1. Go to the **Company** page and click **Single sign-on**.
2. Click **Disable**. When disabled, users will no longer be using the identity service provider for single sign-on. They will be logging in to Carbonite Endpoint directly.

3. To re-enable single sign-on, click **Enable**.