



# Carbonite Server Backup

## Portal 9.3

### Administration Guide



© 2024 Open Text. All rights reserved.

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

For terms and conditions, see <https://www.carbonite.com/terms-of-use/carbonite-general-enterprise-terms-of-service/>.

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

No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval System or translated into any language including computer language, in any form or by any means electronic, mechanic, magnetic, optical, chemical or otherwise without prior written permission of:

Carbonite LLC  
251 Little Falls Drive  
Wilmington, DE 19808  
[www.carbonite.com](http://www.carbonite.com)

Carbonite and the Carbonite logo are trademarks of Carbonite, LLC. Product names that include the Carbonite mark are trademarks of Carbonite, LLC. All other products or company names mentioned in this document are trademarks or registered trademarks of their respective owners.

## Version History

Version	Date	Description
1	April 2023	Initial admin guide for Portal 9.3x.
2	February 2024	Updated <a href="#">Create a parent site</a> , <a href="#">Site Details tab</a> and <a href="#">Create a child site</a> for Portal 9.31. These sections now indicate that site names cannot include some special characters. Updated authentication log example in <a href="#">Monitor Portal sign-in attempts</a> to show masked characters.

## Contents

<b>1 Introduction to Portal Administration</b>	<b>6</b>
<b>2 Create and manage sites</b>	<b>7</b>
2.1 Create a parent site	7
2.2 Create a child site	9
2.3 Assign child sites to a parent site	11
2.4 Change or remove a child site's parent site	12
2.5 Remove a site	12
2.6 Add a vault profile for a site	13
2.7 Add a short name for a site	16
2.8 Copy a site's Company ID	18
2.9 Allow Admin users to receive email notifications for encryption password changes	18
2.10 Set up email notifications for a child site	19
2.11 Show or hide the Usage Summary Report for a site	20
2.12 Enable usage tracking and alerting for a site	21
2.13 Enable or disable the welcome email option for new users in a site	22
<b>3 Create and manage users</b>	<b>24</b>
3.1 Create a Super user or Support user	25
3.2 Create a user in a site (Admin, User, Execute-only, or Read-only)	26
3.3 Users with single sign-on credentials	29
3.4 Assign child sites to a user in a parent site	30
3.5 Assign computers to a user or Execute-only user	30
3.6 Change a user's default page settings	31
3.7 Assign vault profiles to a user	32
3.8 Change a user's information	33
3.9 Require a user to set up two-factor account verification	33
3.10 Unlock a user's account	34
3.11 Delete a user	35
3.12 Monitor Portal sign-in attempts	35
<b>4 Add Dashboard messages and links</b>	<b>37</b>
4.1 Add Dashboard messages for users	37
4.2 Add quick links	39
<b>5 Create and manage policies</b>	<b>41</b>
5.1 Create a policy	41
5.2 Edit a policy	51
5.3 Assign a policy to computers	52

5.4 Unassign policies from computers .....	53
<b>6 Set security preferences .....</b>	<b>54</b>
6.1 Specify default security preferences .....	54
6.2 Set security preferences for a site .....	55
6.3 Set security preferences for your site .....	58
<b>7 Customize the Portal appearance .....</b>	<b>61</b>
7.1 Customize the default Portal appearance .....	61
7.2 Customize the Portal appearance for a site .....	63
7.3 Customize the Portal appearance for your site .....	65
<b>8 Create and manage default retention types .....</b>	<b>68</b>
8.1 Create default retention types .....	68
8.2 Change default retention types .....	69
8.3 Delete default retention types .....	70
8.4 Retention types for intra-daily backup schedules .....	71
<b>9 Manage Windows agent upgrades .....</b>	<b>73</b>
9.1 Set up an agent installer location and permissions .....	73
9.2 Upload agent installers .....	75
9.3 Activate, deactivate or delete an agent installer .....	75
9.4 Upgrade agents on eligible computers .....	76
9.5 Automatic agent upgrade process .....	79
<b>10 Set up features and automatic emails .....</b>	<b>81</b>
10.1 Enable data deletion .....	81
10.2 Disable data archiving .....	82
10.3 Enter email settings .....	82
10.4 Set up two-factor account verification .....	86
<b>11 Set up agent auto-configuration .....</b>	<b>89</b>
11.1 Create job templates .....	89
11.2 Enable agent auto-configuration in child sites .....	93
11.3 Create and edit custom job templates .....	95
<b>12 View information about the Portal instance .....</b>	<b>99</b>
<b>13 View information as a Support user .....</b>	<b>100</b>
13.1 View sites on the Support Dashboard .....	100
13.2 Monitor events and computers as a Support user .....	101
13.3 View computers and jobs as a Support user .....	102
13.4 View backup statuses as a Support user .....	103

13.5 View reports as a Support user .....	104
<b>14 Carbonite Server Backup Support .....</b>	<b>106</b>
14.1 Contacting Carbonite .....	106

## 1 Introduction to Portal Administration

Portal provides a central access point for remotely managing backups and restores for servers on large computer networks.

The Portal web application makes backup management and reporting easy through a simple web interface, status feeds and reports.

Portal is scalable, and can accommodate a variety of different-sized organizations. A simple system can run on a single computer and efficiently handle approximately 500 computers. A distributed farm system can handle much larger organizations with tens of thousands of computers.

This guide describes how to manage a Portal instance, including the following:

- Sites and users. See [Create and manage sites](#) and [Create and manage users](#).
- Policies that provide settings for computers and jobs. See [Create and manage policies](#).
- Security preferences. See [Set security preferences](#).
- Portal colors and appearance. See [Customize the Portal appearance](#).


For information about installing Portal, see the *Portal Installation and Configuration Guide*. For information about backing up and restoring data, see the *Portal User Guide*.

## 2 Create and manage sites

In Server Backup Portal, a site is an organization with one or more users.

Sites restrict the information that each user can access in Portal. Super users can manage all sites and users in Portal, and Support users can view logs and status information for all sites, but other users can only access information in their own sites. For more information, see [Create and manage users](#).

Portal can include two types of sites:

- **Parent sites.** A parent site represents an organization that is independent from other parent organizations. Parent sites are often identified by the word "Parent" in brackets or the Parent icon (  ) beside the parent site name.
- **Child sites.** A child site represents an organization that is related to a parent organization. For example, if a company has multiple locations, a parent site could represent the company as a whole, and a child site could represent each location.

Only parent sites can have child sites. Child sites cannot have their own child sites.

Only Super users can create parent sites. Super users can allow Admin users in a parent site to create and manage the parent site's child sites.

### 2.1 Create a parent site

Super users can create parent sites in Portal. A parent site represents an organization that is independent from other parent organizations.

Super users can also specify whether child sites can be added to a parent site, and whether Admin users can create and manage the parent site's child sites.

To create a parent site:

1. When signed in as a Super user, click **Sites** on the navigation bar.  
The Sites page shows existing sites.
2. Above the grid, click **Create New Site**.  
The Site Details tab opens.

3. In the **Parent** list, click **This site has no parent**.
4. In the **Site Name** box, enter a name for the new site.

The site name cannot exceed 255 characters and cannot include the following special characters:  
 = ^ + ` | % ;

Beginning in Portal 8.90, a parent site can have the same name as a child site. A parent site cannot have the same name as another parent site.

5. To allow the parent site to have child sites, select the **Allow Child Sites** check box.
6. To allow parent site Admin users to create and manage child sites, select the **Allow admins to manage child sites** check box.
7. Enter other site information on the [Site Details tab](#).
8. Click **Save Site**.

The Site Details tab closes, and the new parent site appears in the grid.

### 2.1.1 Site Details tab

When you create or edit a site, you can specify the following information on the **Site Details** tab:

Site Information	
Parent	Specifies whether the site is a parent site or a child site. If the site is a parent site, select <b>This site has no parent</b> in the list. If the site is a child site, select the parent site name in the list. The list only includes parent sites where child sites are allowed.



Site Name	<p>Name of the site. A site name cannot exceed 255 characters and cannot include the following special characters: = ^ + `   % ;</p> <p>Beginning in Portal 8.90, a parent site and one of its child sites can have the same name, and child sites in different parent sites can have the same name.</p> <p>Multiple parent sites in a Portal instance cannot have the same name, and multiple child sites in the same parent site cannot have the same name.</p>
Account Number	Account number of the site. This value can be used as an ID field for identifying the site to other systems. This value is not required.
Allow child sites	If selected, the site can have child sites. This option can only be selected for parent sites.
Allow admins to manage child sites	If selected, Admin users can manage the site’s child sites. This option can only be selected for parent sites where child sites are allowed.
Disable Account	If selected, the site’s account is disabled. For example, an account could be disabled after a free trial period ends. Users cannot sign in to disabled accounts.
<b>Contact Information</b>	
Contact	Contact person for the site.
Email	Site email address.
Phone	Site phone number.
Fax	Site fax number.
<b>Site Mailing Address</b>	
Address	Street address in the site’s mailing address.
City	City in the site’s mailing address.
State	State in the site’s mailing address.
Country	Country in the site’s mailing address.

When a Super user views or edits a site, the site's Company ID might also appear on the Site Details tab. A Company ID is generated when a site is created, cannot be edited, and is sometimes used in external business systems. The Company ID can appear in Portal beginning in version 8.89.

## 2.2 Create a child site

Super users can create child sites in Portal. Admin users can also create child sites in parent sites where Admin users are allowed to manage child sites.

A child site represents an organization that is related to a parent organization in Portal. For example, a child site could represent one location of a company with multiple offices.

To create a child site:

1. When signed in as a Super user, or as an Admin user who can manage child sites, click **Sites** on the navigation bar.

The Sites page shows existing sites.

2. Do one of the following:

- In the grid, find the parent site for the new child site. Open the site by clicking its row. On the Child Sites tab, click **Create New Site**.

The Child Sites tab only appears for parent sites where child sites are allowed.

- Above the grid, click **Create New Site**. In the Parent list, click the parent site for the new child site.

The Parent list only includes parent sites where child sites are allowed.

The screenshot shows a 'Site Details' form with three main sections: 'Site Information', 'Contact Information', and 'Site Mailing Address'. The 'Site Information' section contains a 'Parent' dropdown menu (currently showing 'This site has no paren'), 'Site Name', 'Account Number', and two checkboxes: 'Allow Child Sites' and 'Allow admins to create and manage child sites'. There is also a red 'Disable Account' button. The 'Contact Information' section includes fields for 'Contact', 'Email', 'Phone', and 'Fax'. The 'Site Mailing Address' section includes fields for 'Address', 'City', 'State', and 'Country'. At the bottom right of the form are 'Save Site' and 'Cancel' buttons.

3. In the **Site Name** box, enter a name for the new site.

The site name cannot exceed 255 characters and cannot include the following special characters:

= ^ + ` | % ;

Beginning in Portal 8.90, a child site can have the same name as a parent site, and child sites in different parent sites can have the same name. Multiple child sites in the same parent site cannot have the same name.

4. Enter other site information on the [Site Details tab](#).

5. Click **Save Site**.

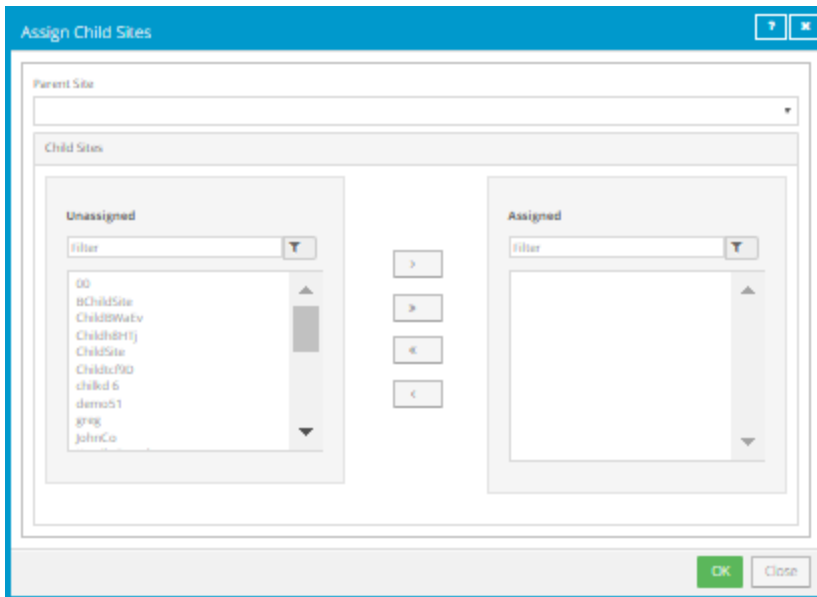
The Site Details tab closes. The new child site appears in the Sites grid, and on the Child Sites tab of the parent site.



## 2.3 Assign child sites to a parent site

Super users can assign multiple child sites to a parent site at the same time.

To assign child sites to a parent site:

1. When signed in as a Super user, click **Sites** on the navigation bar.  
The Sites page shows existing sites.
2. Click **Assign Child Sites**.
3. In the Assign Child Sites dialog box, choose a parent site from the **Parent Site** list.



4. Do one or more of the following until the **Assigned** box shows all child sites that you want to be assigned to the parent site:
  - To find one or more sites in the **Unassigned** or **Assigned** box, enter characters from the site names in the associated **Filter** box.
  - To assign all sites in the **Unassigned** box to the parent site, click the Assign All button. 
  - To assign some sites in the **Unassigned** box to the parent site, select the sites in the **Unassigned** box, and then click the **Assign** button. 
  - To select multiple sites in the list, press CTRL and click the site names. To select multiple consecutive sites in the list, press Shift and then click the first and last sites that you want to select.
  - To unassign all sites in the **Assigned** box from the parent site, click the Unassign All button.



- To unassign some sites in the **Assigned** box from the parent site, click the Unassign button.



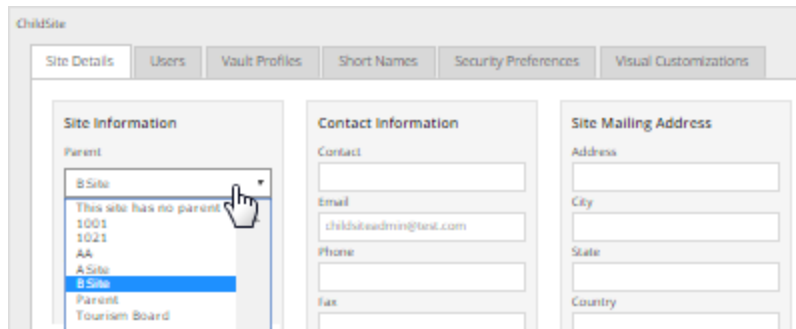
5. Ensure that all of the child sites that you want to be assigned to the parent site appear in the **Assigned** box.
6. Click **OK**.

## 2.4 Change or remove a child site's parent site

Super users can change or remove a child site's parent site. After a parent site is removed from a child site, the former child site becomes a parent site.

To change or remove a child site's parent site:

1. When signed in as a Super user, click **Sites** on the navigation bar.  
The Sites page shows existing sites. The Parent Name column shows the parent site name for each child site.
2. In the grid, find the child site with the parent site that you want to change or remove. Open the site by clicking its row.
3. Do one of the following:
  - To change the site's parent site, click the **Parent** list and then click the new parent site.
  - To remove the site's parent site, click the **Parent** list and then click **This site has no parent**.



4. Click **Save**.

## 2.5 Remove a site

Super users can remove sites from Portal. Admin users can remove child sites that they are allowed manage.

When a site is removed, all users and computers that are registered to the site are removed from Portal. However, Agent software is not removed from any computer, and backup data for the site remains on the vault.

To remove a site:

1. When signed in as a Super user, or as an Admin user who can manage child sites, click **Sites** on the navigation bar.  
The Sites page shows existing sites.
2. In the grid, find the site that you want to delete. Open the site by clicking its row.
3. Click **Remove Site**.
4. In the confirmation dialog box, read the warning message. Click **OK** to remove the site.

## 2.6 Add a vault profile for a site

Before a computer can back up data to or restore data from a vault, vault settings must be added for the computer. Vault settings provide vault information, credentials, and agent connection information required for accessing a vault.

When adding vault settings for a computer, Admin users and regular users can manually enter vault information, or select a vault profile with vault information and credentials.

Super users can add vault profiles for a site. Admin users can add vault profiles for their sites, and for any child sites. Admin users can also assign vault profiles to other users so that they can select vault profiles. For more information, see [Assign vault profiles to a user](#).

Beginning in Portal 9.30, each vault profile has a type:

- **Primary.** Primary vault profiles can be selected in vault settings for a computer. Super users and Admin users can add Primary vault profiles in Portal and assign them to users. Admin users can assign Primary vault profiles to policies.
- **Password Recovery Only.** Password Recovery Only vault profiles cannot be selected in vault settings and are intended only for recovering vault account passwords. See [View vault profiles for a site](#). Password Recovery Only vault profiles are created by business systems in some Portal instances and cannot be added manually. To make information from a Password Recovery Only vault profile available for vault settings, a Super user or Admin user must add a new vault profile using the Password Recovery Only vault profile information.

To add a vault profile for a site:

1. Do one of the following:
  - When signed in as an Admin user, click the user menu, and then click **My Site Settings** in the menu. On the **Vault Profiles** tab, click **Add New**.
  - When signed in as a Super user, or as an Admin user who can manage child sites, click **Sites** on the navigation bar. In the grid, find the site for which you want to add a vault profile. Open the site by clicking its row. On the **Vault Profiles** tab, click **Add New**.  
The Vault Settings dialog box appears.

2. In the **Vault Name** box, enter a vault profile name.
3. In the **Address** box, enter the vault IP address or hostname.
4. In the **Account**, **Username**, and **Password** boxes, enter a vault account and credentials for connecting to the vault.
5. Click **OK**.

### 2.6.1 View vault profiles for a site

When adding vault settings for a computer, Admin users and regular users can manually enter vault information, or select a vault profile with vault information and credentials.

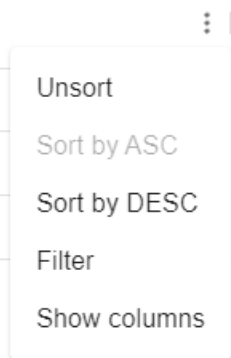
Super users can view vault profiles for sites. Admin users can view vault profiles for their sites, and for any child sites. Beginning in Portal 8.89, Super users and Admin users can view vault account passwords.

To view vault profiles for a site:


1. Do one of the following:
  - When signed in as an Admin user, click the user menu, and then click **My Site Settings** in the menu.
  - When signed in as a Super user, or as an Admin user who can manage child sites, click **Sites** on the navigation bar. In the grid, find the site for which you want to view vault profiles. Open the site by clicking its row. Click the **Vault Profiles** tab.

The Vault Profiles tab shows information about each vault profile.

2. To sort records by values in a column, point to the column heading, click the **Menu** button **:**, and then click **Sort by ASC** or **Sort by DESC**. If **Sort by ASC** or **Sort by DESC** is unavailable, records are already sorted by this value.





3. To stop sorting records by values in a column, point to the column heading, click the **Menu** button **:**, and then click **Unsort**. If **Unsort** is unavailable, records are not sorted by this column.
4. To filter records by values in a column, point to the column heading, click the **Menu** button **:**, and then click **Filter**. In the **Operator** list and **Value** box, specify how to filter records.

5. To change which columns appear, point to a column heading, click the **Menu** button , and then click **Show columns**. In the list of columns, turn on columns that you want to show and turn off columns that you want to hide.

*Note:* E3 appliance information appears in the Appliance Hardware Id and Appliance State (e.g., Online) columns.


6. To view information for a specific vault profile, click **Edit** in its **Select Action** menu.

The Vault Settings dialog box shows vault profile information, including the network address, account and username.

7. If an eye icon  appears in the Password field, click the icon to view the vault account password. After viewing the password, you can click the eye icon with a slash  to hide the vault account password.

## 2.6.2 Edit a vault profile for a site

Super users can edit vault profiles for a site. Admin users can also edit vault profiles for their sites and for child sites that they manage.


In some Portal instances, Admin users cannot change the account, username or password of a vault profile that was created by a Super user or automated provisioning system. A lock icon  appears beside these "system profiles".

You cannot change the type of a vault profile. To make information from a Password Recovery Only vault profile available for vault settings, a Super user or Admin user must add a new vault profile using the Password Recovery Only vault profile information. For more information, see [Add a vault profile for a site](#).

*Note:* If a Super user or Admin user changes the name of an E3 vault profile, the name is updated automatically in vault settings for agents that are registered to the E3.

To edit a vault profile for a site:

1. Do one of the following:
  - When signed in as an Admin user, click the user menu, and then click **My Site Settings** in the menu. On the My Site Settings page, find the vault profile that you want to edit, and click **Edit** in its **Select Action** menu.
  - When signed in as a Super user, or as an Admin user who can manage child sites, click **Sites** on the navigation bar. In the grid, find the site for which you want to edit a vault profile. Open the site by clicking its row. On the Vault Profiles tab, find the vault profile that you want to edit, and click **Edit** in its **Select Action** menu.

If you are signed in as an Admin user and a lock icon  appears beside a vault profile name, you cannot change the vault profile's account, username or password.

2. In the Vault Settings dialog box, do one or more of the following:

- In the **Vault Name** box, enter a vault profile name.
- In the **Address** box, enter the vault IP address or hostname.
- In the **Account**, **Username**, and **Password** boxes, enter a vault account and credentials for connecting to the vault.


If you are signed in as an Admin user and the Account, Username and Password fields are disabled, you cannot change these values.

You cannot change the type of a vault profile.

3. Click **OK**.

### 2.6.3 Remove a vault profile from a site


Super users can remove vault profiles from a site. Admin users can also remove vault profiles from child sites that they manage.

In some Portal instances, Admin users cannot remove a vault profile that was created by a Super user or automated provisioning system. A lock icon  appears beside these "system profiles".

To remove a vault profile from a site:

1. Do one of the following:

- When signed in as an Admin user, click the user menu, and then click **My Site Settings** in the menu. On the My Site Settings page, find the vault profile that you want to remove, and click **Remove** in its **Select Action** menu.
- When signed in as a Super user, or as an Admin user who can manage child sites, click **Sites** on the navigation bar. In the grid, find the site for which you want to edit a vault profile. Open the site by clicking its row. On the Vault Profiles tab, find the vault profile that you want to remove, and click **Remove** in its **Select Action** menu.

If you are signed in as an Admin user and a lock icon  appears beside a vault profile name, you cannot remove the vault profile.

2. In the confirmation dialog box, click **OK**.

## 2.7 Add a short name for a site

Super users can enter short names for sites.

Short names for a site are used to extract report data, and must match customer short names used on the vault. Each site must have a unique short name; sites cannot share the same short name.

To add a short name for a site:

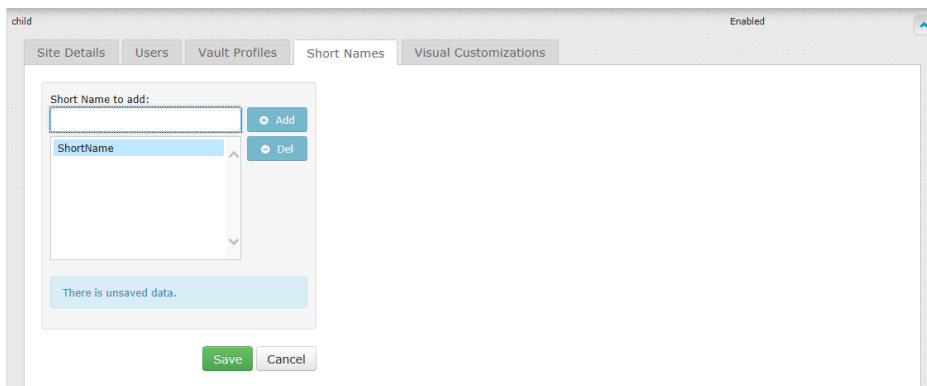
1. When signed in as a Super user, click **Sites** on the navigation bar.

The Sites page shows existing sites.



2. Find the site for which you want to add a short name. Open the site by clicking its row.
3. Click the **Short Names** tab.
4. In the **Short Name to Add** box, enter a short name.
5. Click **Add**.

The new short name moves to the short name list, and the Save button appears.



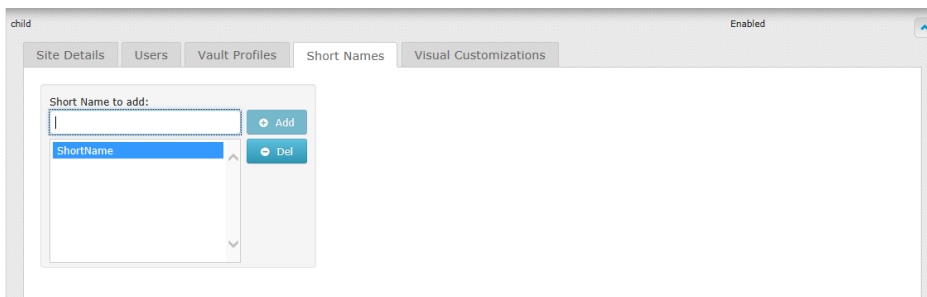
6. Click **Save**.

### 2.7.1 Remove a short name from a site

Super users can remove short names from a site.

To remove a short name from a site:

1. When signed in as a Super user, click **Sites** on the navigation bar.  
The Sites page shows existing sites.
2. Find the site with the short name that you want to remove. Open the site by clicking its row.
3. Click the **Short Names** tab.
4. In the list of short names, click the short name that you want to remove.



5. Click **Del**.

The short name is removed from the short name list, and the Save button appears.

6. Click **Save**.

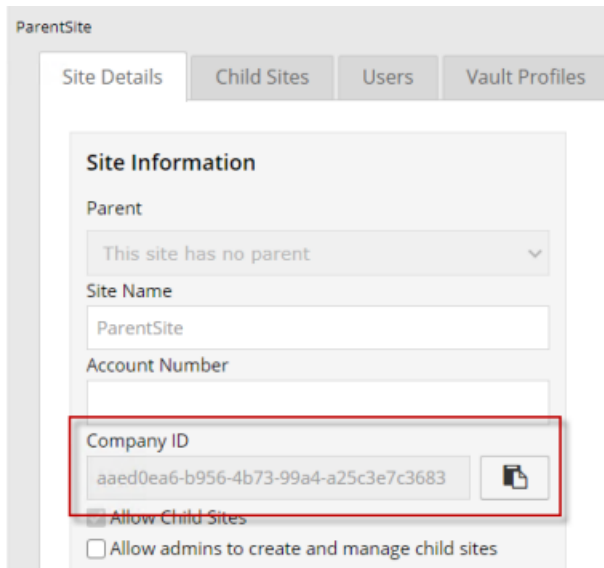
## 2.8 Copy a site's Company ID


Super users can view and copy the Company ID of a Portal site. This identifier is generated when a site is created, cannot be edited, and is sometimes used in external business systems.

To copy a site's Company ID:

1. When signed in as a Super user, click **Sites** on the navigation bar.  
The Sites page shows existing sites.
2. Find the site for which you want to copy the Company ID. Open the site by clicking its row.

The site's Company ID appears on the Site Details tab.



3. To copy the Company ID to the clipboard, click the copy button .

## 2.9 Allow Admin users to receive email notifications for encryption password changes

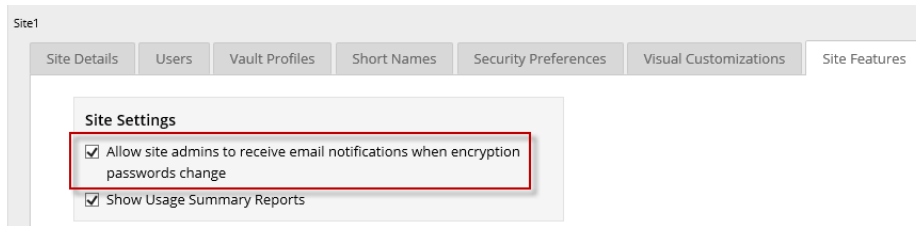
Super users can specify whether Admin users in a site can receive emails when job encryption passwords change in their site.

If encryption password change emails are allowed in a site, Admin users can choose whether they want to receive these notifications.

Email notifications for encryption password changes must also be configured in the Portal instance. For more information, see the *Portal Installation and Configuration Guide*.

To allow Admin users to receive email notifications for encryption password changes:

1. When signed in as a Super user, click **Sites** on the navigation bar.  
The Sites page shows existing sites.
2. Find the site where you want Admin users to receive email notifications for encryption password changes.
3. Click the **Site Features** tab.
4. To allow Admin users to receive email notifications for encryption password changes, select the **Allow site admins to receive email notifications when encryption passwords change** option.



## 2.10 Set up email notifications for a child site

In Portal instances where notifications are configured centrally and/or email notifications are set up for encryption password changes, Admin users in a parent site can specify the following for each of their child sites:

- One or more email addresses that will receive notifications. The email addresses do not have to be associated with Portal users.

**IMPORTANT:** For security reasons, be sure that the notification email addresses for each child site are correct.

- The language for notification emails. By default, American English (en-US) is selected for the emails. Depending on which languages are available in your Portal instance, UK English (en-GB), French (fr-FR), German (de-DE) or Spanish (es-ES) might also be available.

*Note:* Email notifications for child site email addresses are supported in multiple languages. Email notifications selected in Admin users' profile settings are only sent in English.

- The events (e.g., backup failures, backup cancellations, skipped backups, encryption password changes, potential threats detected) for which emails will be sent to the specified email addresses.

Email notification settings for child sites are only available when:

- Backup notifications are configured centrally and/or email notifications are set up for encryption password changes in the Portal instance.
- Admin users are allowed to manage the child sites (i.e., the **Allow admins to manage child sites** check box is selected in the parent site). See [Create a parent site](#).

To set up email notifications for a child site:

1. When signed in as an Admin user in a parent site, click **Sites** on the navigation bar.  
The Sites page shows child sites in the parent site.
2. Find the child site for which you want to set up email notifications. Open the site record by clicking its row.
3. On the Notifications tab for the site, in the **Language** list, select the language for email notifications for the child site.
4. In the **Email address** box, enter one or more email addresses that will receive notifications of events in the child site. Use commas to separate multiple email addresses.  
**IMPORTANT:** For security reasons, be sure that the notification email addresses for the child site are correct.
5. In the event list, click each event (e.g., backup failures, backup cancellations, skipped backups, encryption password changes, potential threats detected) for which emails will be sent to the specified email addresses.
6. Click **Save**.

### 2.10.1 Unblock notification email addresses for a child site

In some Portal instances, if emails cannot be delivered to one or more notification email addresses for a child site, the email addresses are blocked and a message appears on the site's Notifications tab.

When messages can be delivered to the email addresses again, an Admin user in the parent site can unblock the email addresses. Alternatively, an Admin user can enter different notification email addresses for the child site. See [Set up email notifications for a child site](#).

To unblock notification email addresses for a child site:

1. When signed in as an Admin user in a parent site, click **Sites** on the navigation bar.  
The Sites page shows child sites in the parent site.
2. Find the child site for which you want to unblock the notification email address. Open the site record by clicking its row.
3. Click the Notifications tab for the site.  
A message indicates that notification emails could not be delivered to one or more email addresses, so the email addresses have been blocked.
4. Click **Unblock**.

### 2.11 Show or hide the Usage Summary Report for a site

Super users can specify whether Admin users in a site can view the Usage Summary Report. Hiding the Usage Summary Report can be useful, for example, while you investigate data in the report.

To show or hide the Usage Summary Report for a site:

1. When signed in as a Super user, click **Sites** on the navigation bar.  
The Sites page shows existing sites.
2. Find the site where you want show or hide the Usage Summary Report.
3. Click the **Site Features** tab.
4. Do one of the following:
  - To hide the Usage Summary Report for the site, clear the **Enable Data Usage Features** option.
  - To show the Usage Summary Report for the site, select the **Enable Data Usage Features** option.

*Note:* In Portal versions earlier than 9.30, this option is named **Show Usage Summary Reports**. The option was renamed in Portal 9.30 because it is required for usage tracking and alerting as well as the Usage Summary Report. See [Enable usage tracking and alerting for a site](#).

## 2.12 Enable usage tracking and alerting for a site

Beginning in Portal 9.30 in some Portal instances, Admin users and Support users can view a Site Usage chart on the Dashboard. This chart shows the amount of data backed up for computers in a site compared to a specified limit, or usage checkpoint amount. When the Site Usage chart appears for a site, Admin users for the site also receive email alerts when the amount of data backed up in the current billing period first reaches 50%, 75%, 90% and 100% of the checkpoint amount. If a site's storage usage is above 50%, 75%, 90% or 100% of the specified limit at the start of a billing period, Admin users also receive an email alert at the start of the billing period.

Usage tracking and alerting is only available in some Portal instances that obtain data from billing systems. The feature can only be enabled for a site that has Data Usage Features enabled, at least one correctly-configured short name, and one billing ID. See [Show or hide the Usage Summary Report for a site](#) and [Add a short name for a site](#).

Admin users in a parent site can enable usage tracking and alerting for the parent site and for child sites that they are allowed to manage. An Admin user in a parent site can also specify a limit, or usage checkpoint amount, for each site where the feature is enabled. Admin users in a child site cannot enable this feature or specify a usage checkpoint amount.

To enable usage tracking and alerting for a site:

1. When signed in as an Admin user in a parent site, do one of the following:
  - To enable usage tracking and alerting for the parent site, click the user menu, and then click **My Site Settings** in the menu. On the My Site Settings page, click the **Usage Tracking** tab.
  - To enable usage tracking and alerting for a child site, click **Sites** on the navigation bar. On the Sites page, find the site where you want to enable the feature. Open the site by clicking its row, and then click the **Usage Tracking** tab.

If the **Usage Tracking** tab does not appear, you cannot enable the feature for the site. This could occur if your Portal instance does not obtain data from billing systems, the Usage Summary Report is not enabled for the site, a short name is not correctly configured for the site, or the site has more than one billing ID.

2. Select the **Enable Usage Tracking and Alerting** check box.
3. In the Usage Checkpoint box, enter the usage checkpoint amount in gigabytes (GB).

The Site Usage chart for the site will show the amount of data backed up for computers in the site in the current billing period compared to the specified usage checkpoint amount, or limit. Admin users for the site will receive email alerts when the amount of data backed up in the current billing period first reaches 50%, 75%, 90% and 100% of the usage checkpoint amount.

The amount of data backed up is the original size of the data before it was compressed.

4. Click **Save**.
5. In the confirmation dialog box, click **Yes**.

## 2.13 Enable or disable the welcome email option for new users in a site

Super users can specify whether new users in a site can receive emails with links for setting their Portal passwords. Alternatively, a password must be specified for each new user. See [Create a user in a site using the Users page](#) or [Create a user in a site using the Sites page](#).

*Note:* Welcome emails cannot be sent to new Super or Support users.

In some Portal instances, users can be created by an automated provisioning system. When a provisioning system creates new users in a site where the welcome email option is enabled, the users receive emails with links for setting their Portal passwords.

Before you can enable welcome emails in a site, the welcome email feature must be enabled in your Portal instance. Your Portal administrator can find instructions for enabling this feature in the *Portal Installation and Configuration Guide*.

To enable or disable the welcome email option for new users in a site:

1. When signed in as a Super user, click **Sites** on the navigation bar.  
The Sites page shows existing sites.
2. Find the site where you want to enable or disable the welcome email option.
3. Click the **Site Features** tab.
4. Do one of the following:
  - To enable the welcome email option for new users in the site, select the **Send "Welcome" email to new users** option.
  - To disable the welcome email option for new users in the site, clear the **Send "Welcome" email to new users** option.

*Note:* If the welcome email option does not appear, the welcome email feature might not be enabled in your Portal instance. Your Portal administrator can find instructions for enabling this feature in the *Portal Installation and Configuration Guide*.

### 3 Create and manage users

Six types of users can be created in Server Backup Portal. Each type of user can view different pages in Portal and perform different tasks. A user’s type also determines which items are available in the user menu at the top right corner of the Portal screen.

The six types of Portal users are:

- **Super user.** Super users can add and manage all sites and users in Portal. However, they cannot add or manage computers, backups, or restores in Portal. Super users can only view pages in the Portal that are used for managing sites and users.
- **Admin user.** Admin users in a site can create and manage users, and access all computers associated with users in the site. Admin users can add computers, delete offline computers, create and run backup jobs, and run restores. Admin users can also create policies and run reports.

When allowed, Admin users in a parent site can create and manage the site’s child sites. Super users specify whether Admin users in a parent site can create and manage child sites. For more information, see [Create a parent site](#).

- **Users.** Users in a site can add computers, create and run backup jobs, and run restores. Users can only access computers that they added, or that are assigned to them in the site.
- **Execute-only users.** Execute-only users can run existing jobs and view logs. However, these users cannot create, edit, or delete anything in Portal.
- **Read-only users.** Read-only users can only view certain logs, statuses, and reports in Portal.
- **Support users.** Support users can view information and reports for all sites in Portal, but cannot add or change computers or jobs, or run backups and restores. This user type is useful for troubleshooting.

The following table summarizes the tasks that each type of user can perform in Portal.

Task	User type					
	Super user	Admin user	User	Execute-only user	Read-only user	Support user
Add and manage sites	Yes – parent and child sites	Yes – child sites in the Admin user’s site (if it is a parent site where Admin users can manage child sites)	No	No	No	No
Add and manage users	Yes – all users in Portal	Yes – in the Admin user’s site and its child sites (if it is a parent site where Admin users can manage sites)	No	No	No	No



	User type					
Add computers	No	Yes	Yes	No	No	No
Delete offline computers	No	Yes – any computer in the Admin user’s site and its child sites (if it is a parent site)	No	No	No	No
Create backup jobs	No	Yes – on any computer in the Admin user’s site and its child sites (if it is a parent site)	Yes – on computers that they added or are assigned	No	No	No
Run backup jobs	No	Yes – on any computer in the Admin user’s site and its child sites (if it is a parent site)	Yes – on computers that they added or are assigned	Yes – on computers that are assigned	No	No
Run restores	No	Yes – on any computer in the Admin user’s site and its child sites (if it is a parent site)	Yes – on computers that they added or are assigned	Yes – on computers that are assigned	No	No
Create policies	No	Yes	No	No	No	No
View reports	No	Yes	No	No	No	Yes
View logs and status information	No	Yes – for any computer in the Admin user’s site and its child sites (if it is a parent site where Admin users can manage child sites)	Yes – for computers that they added or are assigned	Yes – for their assigned computers	Yes – for computers that are assigned	Yes – for all sites

### 3.1 Create a Super user or Support user

Two types of users can access all sites in Portal, and are not associated with a specific site:

- Super users. Super users can add and manage sites and users in Portal. However, Super users cannot add or manage computers, create or run backup jobs, or run restores. Super users can only view pages in Portal that are used for managing sites and users.
- Support users. Support users can view information and reports for all sites in Portal. However, Support users cannot add or manage computers, create or run backup jobs, or run restores.

For more information on user types, see [Create and manage users](#).

Super users can create other Super users and Support users in Portal.

*Note:* In some Portal instances, users are authenticated using an external identity server (e.g., Active Directory Federation Services). In these cases, Portal users are created automatically after a user signs in. For more information, see [Users with single sign-on credentials](#).

To create a Super user or Support user:

1. When signed in as a Super user, click **Users** on the navigation bar.
2. Click **Create New User**.
3. On the User Info tab, in the **Email Address (Username)** box, type the user’s email address.  
The user will sign in to Portal using this email address.
4. In the **First Name** box, type the user’s given name.
5. In the **Last Name** box, type the user’s surname.
6. In the **Role** list, click the type of user you want to create: **Super User** or **Support User**

When you are creating a Super user or Support user, only the User Info and User Settings tabs appear. Other tabs do not apply to these user types.

7. In the **Password** and **Confirm Password** fields, type the user’s password for signing in to Portal.
8. To require the user to change his or her password after the first sign-in, select the **User must change password** check box.
9. Click **Create**.

### 3.2 Create a user in a site (Admin, User, Execute-only, or Read-only)

Four types of user are associated with specific sites in Portal:

- Admin users. Admin users in a site can create and manage users, and access all computers associated with users in the site. Admin users can add computers, delete offline computers, create and run backup jobs, and run restores.

When allowed, Admin users in a parent site can create and manage the site’s child sites. Super users specify whether Admin users in a parent site can create and manage child sites. For more information, see [Create a parent site](#).

- Users. Users in a site can access computers that they added, or that are assigned to them in the site. Users can add computers, create and run backup jobs, and run restores.

- Execute-only users. Execute-only users in a site can run backups and restores on computers that are assigned to them.
- Read-only users. Read-only users in a site can only view logs and status information in the site.

For more information on user types, see [Create and manage users](#).

Super users and Admin users can create users in a site using the Users page or the Sites page. See [Create a user in a site using the Users page](#) and [Create a user in a site using the Sites page](#).

After creating a user, you can:

- [Assign computers to a user or Execute-only user](#)
- [Assign vault profiles to a user](#)

### 3.2.1 Create a user in a site using the Users page

Using the Users page, Super users can create Admin users, users, Execute-only users and Read-only users in any Portal sites.

Using the Users page, Admin users can create Admin users, users, Execute-only users and Read-only users in parent sites.

When creating a new user in a site, you can specify a password for the user. Alternatively, if the welcome email option is available in the site, the user can receive an email with a link for setting a Portal password. Super users specify whether new users in a site can receive welcome emails with links for setting their Portal passwords. See [Enable or disable the welcome email option for new users in a site](#).

To create a user in a site using the Users page:

1. When signed in as a Super user or Admin user, click **Users** on the navigation bar.
2. Click **Create New User**.
3. On the User Info tab, in the **Email Address (Username)** box, type the user's email address.  
The user will sign in to Portal using this email address.
4. In the **First Name** box, type the user's given name.
5. In the **Last Name** box, type the user's surname.
6. In the **Role** list, click the type of user you want to create: **Admin, User, Execute Only** or **Read Only**.
7. If you are signed in as a Super user, in the **Site** list, click the site where you want to create the user. Each parent site name in the list appears in bold. Each child site name is followed by its parent site name in brackets.
8. Do one of the following:
  - If the Send Welcome email option is available, and you want to send the new user an email with a "set password" link, select the **Select Welcome email** check box.

*Note:* This option is only available if welcome emails are enabled in the site. See [Enable or disable the welcome email option for new users in a site](#).

- To specify a password for the user, do the following:
  - a. If the Send Welcome email option is available, clear the **Select Welcome email** check box.
  - b. In the **Password** and **Confirm Password** fields, type the user's password for signing in to Portal.

*Note:* The password fields are disabled if the Select Welcome email check box is selected.

- c. (Optional) To require the user to change his or her password after the first sign-in, select the **User must change password** check box.

9. Click **Create**.

### 3.2.2 Create a user in a site using the Sites page

Using the Sites page, Super users can create Admin users, users, Execute-only users and Read-only users in any Portal sites.

In child sites that Admin users are allowed to manage, Admin users can create Admin users, users, Execute-only users, and Read-only users using the Sites page. To create users in a parent site, use the Users page. See [Create a user in a site using the Users page](#).

When creating a new user in a site, you can specify a password for the user. Alternatively, if the welcome email option is available in the site, the user can receive an email with a link for setting a Portal password. Super users specify whether new users in a site can receive welcome emails with links for setting their Portal passwords. See [Enable or disable the welcome email option for new users in a site](#).

To create a user in a site using the Sites page:

1. When signed in as a Super user, or as an Admin user who can manage child sites, click **Sites** on the navigation bar.

The Sites page shows existing sites.
2. In the list of sites, find the site where you want to create a user. Open the site by clicking its row.
3. Click the **Users** tab.
4. Click **Create New User**.
5. On the User Info tab, in the **Email Address (Username)** box, type the user's email address.

The user will sign in to Portal using this email address.
6. In the **First Name** box, type the user's given name.
7. In the **Last Name** box, type the user's surname.
8. In the **Role** list, click the type of user you want to create: **Admin**, **User**, **Execute Only** or **Read Only**.
9. If you are signed in as a Super user, in the **Site** list, click the site where you want to create the user.

10. Do one of the following:

- If the Send Welcome email option is available, and you want to send the new user an email with a "set password" link, select the **Select Welcome email** check box.

*Note:* This option is only available if welcome emails are enabled in the site. See [Enable or disable the welcome email option for new users in a site.](#)

- To specify a password for the user, do the following:
  - a. If the Send Welcome email option is available, clear the **Select Welcome email** check box.  
*Note:* Password fields are disabled if the Select Welcome email check box is selected.
  - b. In the **Password** and **Confirm Password** fields, type the user’s password for signing in to Portal.
  - c. (Optional) To require the user to change his or her password after the first sign-in, select the **User must change password** check box.

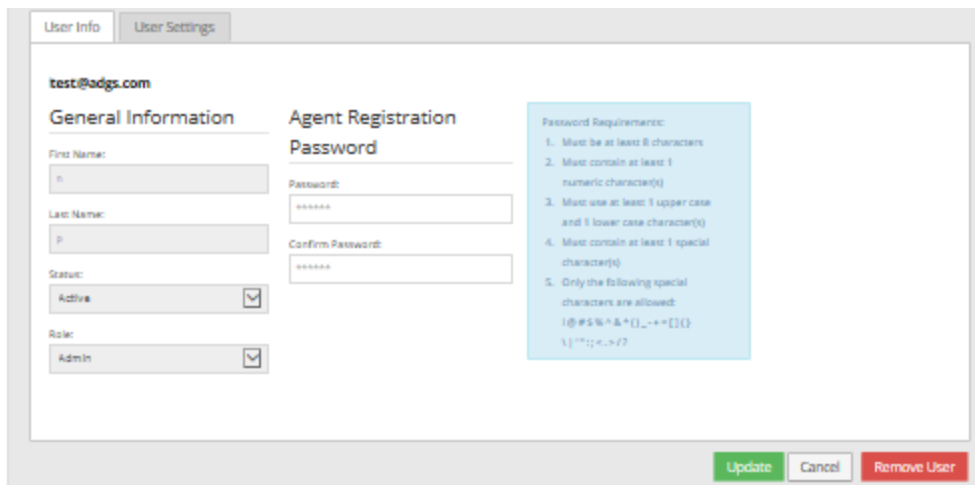
11. Click **Create**.

### 3.3 Users with single sign-on credentials

In some Portal instances, users sign in using credentials that are authenticated by a federated identity server (e.g., Active Directory Federation Services).

When a user signs in using single sign-on credentials, the identity server sends user name, type and site information to Portal. A Portal user is then automatically created with the specified name, type and site. If an automatically-created user already exists in Portal for the user that signs in, the user is updated with information from the identity server.

As shown below, the name, status and role of an automatically-created user is read-only in Portal. This information can only be updated by the identity server. However, you can specify user settings, assign computers and vault settings, and perform other management tasks for these users.



Agent Registration passwords must be specified for Admin and regular users who sign in to Portal. These passwords allow the users to register Agents to Portal, but do not affect users' sign-in passwords.

Information for an automatically-created user in Portal is not always consistent with information in the federated identity server. For example, if a user is deleted from Active Directory, the corresponding user is not automatically deleted from Portal. An automatically-created user can be deleted manually from Portal, however.

For information about setting up Portal single sign-on, see the *Portal Installation and Configuration Guide*.

### 3.4 Assign child sites to a user in a parent site

A Super user or Admin user can assign child sites to users, Execute-only users and Read-only users in a parent site.

Admin users can assign child sites to users, Execute-only users and Read-only users in parent sites.

To assign child sites to a user in a parent site:

1. When signed in as a Super user or Admin user, click **Users** on the navigation bar.
2. On the Users page, find a user in a parent site where Admin users are allowed to manage child sites. Open the user record by clicking its row.

*Note:* A parent site does not have a value in the Parent Name column.

3. Click the **Child Sites** tab.
4. Drag child sites that you want to assign to the user from the **Available** box to the **Assigned** box.
5. Drag child sites that you do not want to assign to the user from the **Assigned** box to the **Available** box.
6. Click **Update**.

### 3.5 Assign computers to a user or Execute-only user

To allow users back up and restore data for on computers in a site, Admin users can assign computers to users and Execute-only users.

Users can create backup jobs, run backup jobs, and run restores on computers that are assigned to them. Users can also back up and restore data on computers that they added in Portal.

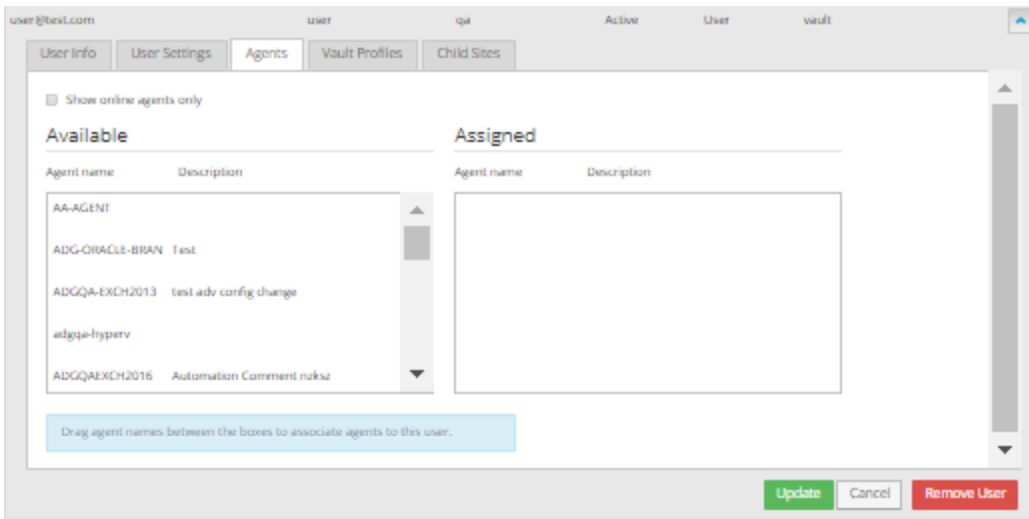
Execute-only users can run backup jobs and run restores on computers that are assigned to them. They cannot create backup jobs.

To assign computers to a user or Execute-only user:

1. When signed in as an Admin user, do one of the following:
  - On the navigation bar, click **Users**. In the list of users, find the user or Execute-only user for assigning computers. Open the user record by clicking its row.

- On the navigation bar, click **Sites**. In the list of sites, find the site where you want to assign computers to a user. Open the site by clicking its row. Click the **Users** tab. Find the user or Execute-only user for assigning computers. Open the user record by clicking its row.
2. Click the **Agents** tab for the user.

The Agents tab shows computers that are available for the user and that are assigned to the user.



3. Drag computers that you want to assign to the user from the **Available** box to the **Assigned** box.
4. Drag computers that you do not want to assign to the user from the **Assigned** box to the **Available** box.
5. Click **Update**.

### 3.6 Change a user's default page settings

To specify which items appear in Portal by default, you can change users' settings for the Status Feed, Computers page, and Monitor page.

Users can also change their default page settings.

To change a user's default page settings and views:

1. When signed in as a Super user or Admin user, do one of the following:
  - On the navigation bar, click **Users**.
  - On the navigation bar, click **Sites**. In the list of sites, find the site where you want to specify a user's settings. Open the site by clicking its row. Click the **Users** tab.
2. Find the user whose settings you want to change. Open the user record by clicking its row.

3. On the User Settings tab, do one or more of the following:
  - To specify items that appear in the user’s status feed, click the **Show in Status Feed** list. Click items in the list until a check mark appears beside each item that should appear in the status feed, and then click outside the **Show in Status Feed** list.
  - To change the user’s default view for the Computers page, click the view in the **Computer Page Default** list.
  - To change the user’s default view for the Monitor page, click the view in the **Monitor Page Default** list.
4. Click **Update**.

### 3.7 Assign vault profiles to a user

Super users can assign vault profiles to users, and Admin users can assign vault profiles to users in their sites.

Vault profiles provide vault information and credentials so that computers can back up data to and restore data from a vault.

After a vault profile is added for a site, Admin users in the site can select the vault profile for computers. Other users in the site can only select a vault profile if it is assigned to them. If a policy is assigned to a computer, users can only select a vault profile if it is assigned to them and it is also assigned to the policy. See [Vault profiles for policies](#).

Beginning in Portal 9.30, each vault profile has a type. Only vault profiles with the Primary type can be assigned to a user. For more information, see [Add a vault profile for a site](#).

To assign vault profiles to a user:

1. When signed in as a Super user or Admin user, do one of the following:
  - On the navigation bar, click **Users**.
  - On the navigation bar, click **Sites**. In the list of sites, find the site where you want to assign vault profiles to a user. Open the site by clicking its row. Click the **Users** tab.
2. Find the user for assigning vault profiles. Open the user record by clicking its row.
3. On the Vault Profiles tab for the user, drag vault profiles that you want to assign to the user from the **Available** box to the **Assigned** box. Drag vault profiles that you do not want to assign to the user from the **Assigned** box to the **Available** box

*Note:* On the Sites page and the Users page, the Vault Profiles tab does not appear for Admin users. Vault profiles do not have to be assigned to Admin users, because Admin users can select any vault profiles in a site. The Vault Profiles tab does not appear for Super users, because they cannot add or manage computers.

4. Click **Update**.



## 3.8 Change a user's information

Super users and Admin users can change information and settings for existing users.

Most user information and settings can be changed. However, a user's email address, which is used for signing in to Portal, cannot be changed. In addition, the name, status and role of a user with single sign-on credentials cannot be changed.

Super users can change information for every type of user in Portal. Admin users can change information for Admin users, regular users, Execute-only users, and Read-only users in sites that they manage.

To change a user's information:

1. When signed in as a Super user or Admin user, do one of the following:
  - On the navigation bar, click **Users**.
  - On the navigation bar, click **Sites**. In the list of sites, find the site where you want to edit a user. Open the site by clicking its row. Click the **Users** tab.
2. Find the user with information that you want to edit. Open the user record by clicking its row.
3. Edit information on any of the following tabs that appear:
  - On the User Info tab, you can change a user's name, status, role, or password. To require the user to change his or her password after the next sign-in, select the **User must change password** check box.  
*Note:* If users sign in using single sign-on credentials, you can only change a user's Agent Registration password on the User Info tab. See [Users with single sign-on credentials](#).
  - On the User Settings tab, you can specify the user's default page settings.
  - On the Vault Profiles tab, which can appear for regular users, Read-only users, and Execute-only users, you can assign vault profiles.
  - On the Child Sites tab, which can appear for regular users, Read-only users, and Execute-only users, you can assign child sites.
  - On the Agents tab, which can appear for regular users and Execute-only users, you can assign computers.
4. Click **Update**.

## 3.9 Require a user to set up two-factor account verification

Two-factor account verification is available in some Portal instances. With two-factor verification, users are sometimes prompted to enter verification codes when they sign in to Portal. A verification code is sent in a text message or automated voice call to a phone number that the user specifies.

You can require specific users to set up two-factor account verification when they sign in to Portal. In some Portal instances, users can skip setting up two-factor verification if they have not set it up before. However,

beginning in version 9.10, all users in a Portal instance can be required to set up two-factor account verification. See the *Portal Installation and Configuration Guide*.

You can also require a user to set up two-factor account verification if their phone number has changed and they can no longer receive account verification codes. The user is then prompted to enter a new phone number for receiving account verification codes when they try to sign in to Portal.

To require a user to set up two-factor account verification:

1. When signed in as a Super user or Admin user, do one of the following:
  - On the navigation bar, click **Users**.
  - On the navigation bar, click **Sites**. In the list of sites, find the site where you want to edit a user. Open the site by clicking its row. Click the **Users** tab.
2. Find the user that must set up two-factor account verification. Open the user record by clicking its row.
3. On the User Info tab, select the **User must configure two-factor authentication on login** check box.  
  
If this check box does not appear, two-factor account verification is not available in your Portal instance.
4. Click **Update**.

### 3.10 Unlock a user's account

A user's account will be automatically locked if the user tries to sign in unsuccessfully more times than the maximum number of failed logins specified in the site's security preferences.

A Super user or Admin user can unlock a user's account.

To unlock a user's account:

1. When signed in as a Super user or Admin user, do one of the following:
  - On the navigation bar, click **Users**.
  - On the navigation bar, click **Sites**. In the list of sites, find the site where you want to edit a user. Open the site by clicking its row. Click the **Users** tab.
2. Find the user account that you want to unlock. Open the user record by clicking its row.
3. On the User Info tab, click **Unlock account**.  
  
A message indicates that the account has been unlocked.
4. Click **Okay**.

### 3.11 Delete a user

Super users and Admin users can delete Portal users.

Super users can delete any user in Portal. Admin users can delete Admin users, regular users, Execute-only users, and Read-only users in sites that they manage.

To delete a user:

1. When signed in as a Super user or Admin user, do one of the following:
  - On the navigation bar, click **Users**.
  - On the navigation bar, click **Sites**. In the list of sites, find the site where you want to delete a user. Open the site by clicking its row. Click the **Users** tab.
2. Find the user that you want to delete. Open the user record by clicking its row.
3. Click **Remove User**.

### 3.12 Monitor Portal sign-in attempts

Portal sign-in attempts are logged in an authentication log file for each day. Authentication log files are saved in .csv format in C:\Logs\Portal UI\Audit. The log file for each day is named *yyyy-mm-dd.csv*.

As shown in the following example, the log file shows the following information for each sign-in attempt:

- the date and time in Coordinated Universal Time (UTC)
- the user name. To maintain data privacy, some characters in the user name are masked.
- the user's IP address. To maintain data privacy, some characters in the IP address are masked.
- the result of the sign-in attempt:
  - Successful – The user signed in successfully.
  - Failed – The sign-in was unsuccessful. This can occur, for example, if the user enters an incorrect email address and password combination or if the user belongs to a disabled site.
  - UserLocked – The user was notified that the account is locked.
  - UserDisabled – The user's account is disabled.
  - MultiFactorAuthenticationChallengeFailed – In a Portal instance where multi-factor authentication is enabled, the user entered an incorrect verification code when trying to sign in.

```
2023-08-09 19:45:23.5845,ad***@si***.com,192.168.14.***,Failed
2023-08-09 19:45:39.4968,ad***@si***.com,192.168.14.***,Failed
2023-08-09 19:45:43.6283,ad***@si***.com,192.168.14.***,Failed
2023-08-09 19:45:48.4086,ad***@si***.com,192.168.14.***,Failed
2023-08-09 19:45:52.2497,ad***@si***.com,192.168.14.***,Failed
2023-08-09 19:45:56.1232,ad***@si***.com,192.168.14.***,Failed
2023-08-09 19:46:03.1925,ad***@si***.com,192.168.14.***,UserLocked
2023-08-09 19:46:13.9931,su***@si***.com,192.168.14.***,Successful
2023-08-09 19:47:07.0882,ad***@si***.com,192.168.14.***,Successful
2023-08-09 19:48:16.2423,us***@si***.com,192.168.14.***,Successful
2023-08-09 19:48:37.1435,us***@si***.com,192.168.14.***,Failed
2023-08-09 19:50:57.4548,su***@si***.com,192.168.14.***,Successful
2023-08-09 19:52:27.2534,ad***@si***.com,192.168.14.***,Successful
2023-08-09 19:53:12.2159,us***@si***.com,192.168.14.***,UserDisabled
```

## 4 Add Dashboard messages and links

Super users can add “custom status feed messages” and links that appear for users on the Dashboard in Server Backup Portal.

Messages can be added for users in a specific site, or in all sites, and can be entered in each language in the Portal instance. See [Add Dashboard messages for users](#).

Super users can also add links that appear in a “Quick Links” area on the Dashboard in Portal. These links appear for users in all sites in a Portal instance. See [Add quick links](#).

### 4.1 Add Dashboard messages for users

Super users can add “custom status feed messages” that appear in the Dashboard for users in a specific site, or in all sites. Super users can format each message, include links, and specify a date range and display order. Super users can also specify whether users can hide a message.

A version of each message can be entered in each language in the Portal instance. When users view the Dashboard, they see messages in the language in which they are viewing Portal text (i.e., English (en-US), English (en-GB), French, German or Spanish).

An English (en-US) version is required for each message. When viewing Portal in another language, users see the English (en-US) version of any message that is not available in the other language. For example, when viewing Portal in French, users see the English (en-US) version of any message that was not entered in French.

To add a Dashboard message for users:

1. When signed in as a Super user, click **Custom Feed Items** on the navigation bar.
2. In the **Actions** list, click **Add New Custom Status Feed Item**.

An editor appears for entering the new message.

3. In the **Title** box, type a message title.

The title will not appear with the message. The title is only used to identify the message on the **Custom Feed Items** page.

4. In the **Site Name** list, do one of the following:
  - To show the message to users in all sites, select **All**.
  - To show the message to users in one site, select the name of the site. Each parent site name in the list appears in bold. Each child site name is followed by its parent site name in brackets.
5. Click the **Start Date** box. In the calendar that appears, click the first date to display the message.
6. Click the **End Date** box. In the calendar that appears, click the date when the message will no longer appear.

7. In the **Display Order** box, enter a number that represents the position of the message relative to other messages in the list.

If multiple messages for a user have the same display order number, the most recently-added messages appear higher in the Notification Center. For example, if two messages have a Display Order value of 1, the message that was added last appears at the top of the list.

8. Do one of the following:
  - To allow users to hide the message, select **Can Be Hidden**.
  - To prevent users from hiding the message, clear **Can Be Hidden**.
9. For each language in the Portal instance, do the following:
  - a. Click the language tab on the left side of the editor.
  - b. In the text box, enter the message in the specified language.
  - c. Format the message using tools in the editor.

An English version of the message is required.

10. Click **Save**.

#### 4.1.1 Edit Dashboard messages

Super users can edit existing messages for users, including the content, date range, display order, and other options.

To edit a Dashboard message:

1. When signed in as a Super user, click **Custom Feed Items** on the navigation bar.

The Custom Feed Items page lists existing messages.

2. Find the message that you want to edit, and expand it by clicking its row.
3. Do one or more of the following:

- In the **Title** box, type a title for the message.

The title does not appear with the message. The title is only used to identify the message on the **Custom Feed Items** page.

- In the **Site Name** list, do one of the following:

- To show the message to users in all sites, select **All**.

- To show the message to users in one site, select the name of the site. Each parent site name in the list appears in bold. Each child site name is followed by its parent site name in brackets.

- Click the **Start Date** box. In the calendar that appears, click the first date to display the message.

- Click the **End Date** box. In the calendar that appears, click the date when the message will no longer appear.
- In the **Display Order** box, enter a number that represents the position of the message relative to other messages in the list.
- Do one of the following:
  - To allow users to hide the message, select **Can Be Hidden**.
  - To prevent users from hiding the message, clear **Can Be Hidden**.
- For each language in the Portal instance, do the following:
  - a. Click the language tab on the left side of the editor.
  - b. In the text box, edit the message in the specified language.
  - c. Format the message using tools in the editor.

*Note:* An English version is required for each message.

4. Click **Save**.

### 4.1.2 Delete Dashboard messages

Super users can delete messages that appear in the Dashboard for users.

To delete a Dashboard message:

1. When signed in as a Super user, click **Custom Feed Items** on the navigation bar.  
The Custom Feed Items page lists existing messages.
2. Select the check box for each message that you want to delete.
3. In the **Actions** list, click **Delete Selected Feed Item(s)**.
4. In the confirmation dialog box, click **Yes**.

## 4.2 Add quick links

Super users can add links that appear for users in a Quick Links area at the right side of the Dashboard. For each link, Super users can specify the URL, and provide text in each language in the Portal instance.

To add a quick link:

1. When signed in as a Super user, click **Global Settings** on the navigation bar.
2. Click the **Quick Links** tab.
3. In the **Action** list, click **Add new Quick Link**.

An editor appears for entering the link.

Title and Description		
Culture	Title	Description
en-US	<input type="text"/>	<input type="text"/>
en-GB	<input type="text"/>	<input type="text"/>
fr-FR	<input type="text"/>	<input type="text"/>
de-DE	<input type="text"/>	<input type="text"/>
es-ES	<input type="text"/>	<input type="text"/>

4. In the **Uri** box, type the URL for the link. The URL must begin with one of the following: `http://`, `https://` or `ftp://`
5. In the **Order** box, type a number that represents the position of the link relative to other links. If multiple links have the same display order number, the links appear in alphabetical order by title.
6. For each language in the Portal instance, do the following:
  - In the **Title** box, type a link title. The title will be used as the quick link text. The URL will not be shown.  
If a title is not specified for a language, the link does not appear when that language is selected in Portal. For example, if a link title is specified in English but not French, the link will not appear when users view Portal text in French.
  - In the **Description** box, type a description. The description will appear under the link title.
7. Click **Save**.

### 4.2.1 Delete quick links

Super users can delete links that appear in a Quick Links area at the right side of the Dashboard.

To delete a quick link:

1. When signed in as a Super user, click **Global Settings** on the navigation bar.
2. Click the **Quick Links** tab.  
The Quick Links tab lists existing links.
3. Select the check box for each message that you want to delete.
4. In the **Action** list, click **Delete Selected Quick Link(s)**.
5. In the confirmation dialog box, click **Yes**.



## 5 Create and manage policies

A policy is a collection of settings that Admin users can create and assign to computers in Server Backup Portal. Policy settings include:

- Agent settings that are used for all backup jobs on a computer. See [Policy schedule, hibernation and shutdown options](#), and [Policy execution priority and bandwidth options](#). Email notification settings are also available in some policies. See [Policy email notification settings](#).

When a policy is assigned to a computer, these settings appear on the computer's Advanced tab, and cannot be modified. To change the settings, you must unassign the policy from the computer, or edit values in the policy.

- Vault profiles that users can select when adding vault settings for a computer, instead of manually entering vault information and credentials. See [Vault profiles for policies](#).

When adding vault settings for a computer where a policy is assigned, Admin users can select any vault profile from the policy. Regular users can only select policy vault profiles that are assigned to them. When a policy is not assigned to a computer, Admin users can select any vault profile in the site, while regular users can select vault profiles that are assigned to them.

- Job settings that can be selected. See [Policy compression and log settings](#) and [Policy filters for backup jobs](#).

These settings are not applied automatically to jobs. When creating, editing or scheduling a backup job on a computer where a policy is assigned, users can select these policy settings or select other values.

- Retention types that users can select when scheduling or running a job. Retention types specify the number of days a backup is kept on the vault, how many copies of a backup are stored online, and how long backup data is stored offline. See [Policy retention types](#).

When scheduling or running a job on a computer where a policy is assigned, users can select a retention type from the policy. If a policy is not assigned to a computer, users add retention types on the computer itself or select a default retention type.

### 5.1 Create a policy

Admin users can create policies that provide settings for computers and jobs. Policy settings include log file options, and bandwidth settings. Email notification settings are also available in some policies.

After a policy is created, Admin users can assign the policy to one or more computers to provide settings for the computers and their jobs. See [Assign a policy to computers](#).

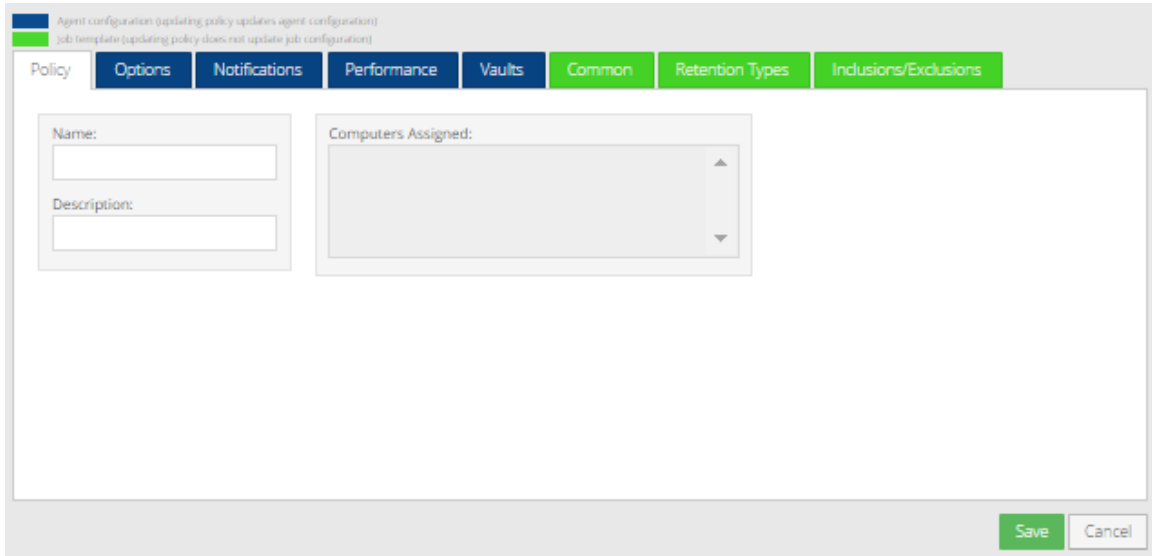
To create a policy:

1. On the navigation bar, click **Policies**.

The Policies page lists existing policies.

2. In the **Actions** list, click **Create Policy**.
3. On the **Policy** tab, enter a name for the policy. Optionally, you can add a policy description.

*Note:* At any time during policy creation, you can click **Save**. If you click **Save** after providing only the policy name, your policy will consist of the policy name only.



4. Specify one or more of the following policy settings for computers:
  - [Policy schedule, hibernation and shutdown options](#)
  - [Policy email notification settings](#)  
*Note:* Email notification settings are not available in all policies.
  - [Policy execution priority and bandwidth options](#)
  - [Vault profiles for policies](#)
5. Specify one or more of the following policy settings for jobs:
  - [Policy compression and log settings](#)
  - [Policy retention types](#)
  - [Policy filters for backup jobs](#)
6. Click **Save**.

The new policy appears on the Policies page.

### 5.1.1 Policy schedule, hibernation and shutdown options

When Admin users create or edit policies, they can specify schedule, hibernation, and shutdown options for computers on the **Options** tab.

When a policy is assigned to a computer, these settings appear on the computer's Advanced tab, are used for all backup jobs on the computer, and cannot be modified. To change the settings, you must unassign the policy from the computer, or edit values in the policy.

## Advanced schedule options

Specifies whether to run backup jobs that have been missed or failed. Select one or both of the following options:

- **Start scheduled backup jobs if they have been missed.** If selected, the scheduler will attempt to start any backups that are still waiting to run. If this option is selected, you can select **Ask for confirmation before starting missed backup jobs** to prompt for user confirmation before missed backup jobs are started.

If backup schedules overlap, only the last one will have its status reported.

- **Restart scheduled backup jobs if they have failed.** This option only applies to Windows Agent version 7.3x and earlier. If selected, if any backup jobs have started, but failed to finish (because of network failure or the computer shutting down), those jobs will be started again. If this option is selected, you can select **Ask for confirmation before rerunning failed backup jobs** to prompt for user confirmation before failed backup jobs are started.

*Note:* If the same job has been missed several times in a row, only one occurrence of it will run when the backup does occur. So, for example, if you have a backup (the same job) scheduled for midnight every day, and your computer is off for three days, you will only get one “missed and rerun” backup (rather than three).

## Hibernation options

Specifies whether a computer can go into sleep or hibernation mode when backups are running.

If **Prevent standby/hibernation when backups are running** is selected, the computer cannot go into sleep or hibernation mode when a backup job is running. When the standby/hibernation tries to start again, and there is no backup running, the standby or hibernation will occur.

## Shutdown options

Specifies whether a computer can shut down when backups are running. Select one or both of the following options:

- **Prevent shutdown when backups are running.** If selected, the computer cannot shut down when a backup job is running. When a shutdown is next attempted, and there is no backup running, the shutdown will proceed. If this option is selected, you can select **Ask the logged on user what to do if backups are running** to prompt for user confirmation before shutdown.
- **Ask the user to do a backup before shutdown.** If selected, the user is prompted to run a backup before the system shuts down.

## Miscellaneous

The **Detect Network Presence Every** list specifies how often a computer’s network connectivity is checked.

If there is a network outage, the Agent causes the scheduler to pause. The scheduler resumes when the network becomes available again. By checking for a valid network, you can make sure that missed or failed

backups will still occur. This assumes that you have selected the advanced options for starting or restarting the schedule after missed or failed backups.

If **Never** is selected from the **Detect Network Presence Every** list, the Agent is not notified about network outages, so backups may be missed. That is, the Agent will fail the backup, and there is nothing to cause it to retry. This option is normally used for troubleshooting.

If a backup does fail because of a network outage, the backup can be restarted (provided that you have selected the advanced options for missed/failed backups). Normally every **5 minutes** is a good choice. It does not require much overhead on the system, and it means that your backups can start/continue when the network presence is detected again.

### 5.1.2 Policy email notification settings

When Admin users edit policies with email notification settings, Admin users can edit email notifications for computers on the **Notifications** tab. These settings specify whether users receive emails after successful backups, failed backups, or backups that complete with errors.

*Note:* If email notification settings have not been configured in a policy, the **Notifications** tab does not appear and the settings cannot be added.

When a policy with email notification settings is assigned to a computer, notification settings appear on the computer's Advanced tab, are used for all backup jobs on the computer, and cannot be modified. To change the settings, you must unassign the policy from the computer, or edit values in the policy.

#### Notification email

Specifies whether specified users receive email notification after a successful or failed backup, or after a backup completes with errors.

Select one or more of the following checkboxes:

- **On failure.** If selected, users receive an email notification when a backup or restore fails. If a backup fails, you cannot recover any files from the backup.
- **On error.** If selected, users receive an email notification when a backup or restore completes with errors in the log file. You cannot recover files that are backed up with errors, but you can restore other files from the backup (safeset).
- **On successful completion.** If selected, users receive an email notification when a backup or restore completes successfully. You can recover files from a backup that completes, even if there are warnings in the log file.

Email notifications are sent separately for each backup and restore. For example, if three backup jobs fail on a computer and **On failure** is selected for the computer, three notification emails are sent.

*Note:* If you clear all of the checkboxes, you will no longer be able to edit notification settings in the policy and the **Notifications** tab will no longer appear.

## SMTP settings and credentials

If users will receive email notifications after backups and restores, specify the following email notification information:

Email "From" Address	Email address from which email notifications will be sent.
Outgoing Mail Server (SMTP)	Network address of the SMTP that will send the email.
Recipient Address(es)	Email notification recipient email addresses, separated by commas. These should be real, valid email addresses. If one or more is not valid, the transmission to those addresses will fail, and errors will appear in the log files.
Outgoing Server Port (SMTP)	Port number for sending email notifications.
SMTP Credentials	If required, SMTP username, domain, and password.

### 5.1.3 Policy execution priority and bandwidth options

When Admin users create or edit policies, they can specify job execution priority and bandwidth settings for computers on the **Performance** tab.

When a policy is assigned to a computer, these settings appear on the computer's Advanced tab, are used for all backup jobs on the computer, and cannot be modified. To change the settings, you must unassign the policy from the computer, or edit values in the policy.

#### Execution priority

Specifies the processing priority of a backup or restore.

To set the execution priority, drag the slider. **High** is the highest priority, and **Low** requires the least CPU priority. **Normal** (the default setting) is usually adequate, depending on the applications being run on the computer during the assigned job.

#### Bandwidth

Bandwidth throttling settings specify the amount of bandwidth consumed by an Agent for backups and, in the case of most Agents, restores. For example, you might want to restrict the amount of bandwidth used for daytime backups so that online users are not affected, and allow unlimited bandwidth usage at night so that scheduled backups run as fast as possible.

Bandwidth throttling values are set at the computer (Agent) level for most Agents, and apply to both backups and restores. If three jobs are running at the same time on the same computer, each job gets 1/3 of the specified maximum bandwidth. For the Hyper-V Agent, bandwidth throttling is applied at the Host level, and applies only to backups. If three VMs are being backed up on a node, each gets 1/3 of the

specified maximum bandwidth on the node. The total bandwidth sent to the vault can be as high as the specified maximum multiplied by the number of nodes where the Host service is installed.

Bandwidth settings include:

- Maximum bandwidth (upper limit), in megabits per second, to be consumed by the Agent for all backups and restores
- Period of time during the day that throttling is in effect. Only one time window can be specified. Outside the window, no throttling takes place.
- Days of the week that throttling is in effect

If the bandwidth throttling time period begins when a backup is underway, the maximum bandwidth is applied dynamically to the running backup. Similarly, if the bandwidth throttling time period ends when a backup is running, bandwidth throttling is ended for the backup.

If you edit an Agent's bandwidth settings while a backup is running, the new Agent settings do not affect the backup that is running. Bandwidth settings are applied when a backup starts, and are not applied to backups that are already running.

#### 5.1.4 Vault profiles for policies

When Admin users create or edit policies, they can assign vault profiles to policies. A vault profile provides vault information and credentials that users can select when adding vault settings for a computer.

When adding vault settings for a computer where a policy is assigned, a user can select a vault profile from the policy instead of manually entering vault information and credentials.

Beginning in Portal 9.30, each vault profile has a type. Only vault profiles with the Primary type can be assigned to a policy. For more information, see [Add a vault profile for a site](#).

To assign a vault profile to a policy, on the **Vaults** tab, drag the vault profile from the **Available Vault Profiles** box to the **Assigned to Policy** box.

To unassign a vault profile from a policy, on the **Vaults** tab, drag the vault profile from the **Assigned to Policy** box to the **Available Vault Profiles** box.

#### 5.1.5 Policy compression and log settings

When Admin users create or edit policies, they can specify data compression and log settings for backup jobs on the **Common** tab.

When a policy is assigned to a computer, the policy compression level and log options are not automatically applied to jobs on the computer. When creating, editing or scheduling a job, a user can use these settings or select other values.

##### Compression Level

The compression level specifies the amount of compression, if any, for backup data. Compression levels optimize the amount of data stored vs. the backup speed. In some cases, it might be better to use

additional time and processing to compress the data before sending it.

The more that data is compressed, the smaller its “footprint” (size) is on the vault.

From the list, select one of the following options:

- **Better** — Minimizes backup size, possibly at the expense of extra processing
- **Maximum** — Always minimizes backup size, regardless of the amount of processing required
- **Minimum** — Minimizes processing, possibly at the expense of a larger backup size
- **None** — Does not compress data
- **Normal** — Balances processing against backup size

The compression levels shown above are not available for Agent versions 7.5 and later. For Agents version 7.5 and later, the following options are available:

- **Faster** — Minimizes the amount of time that is required for backing up the data
- **Smaller** — Minimizes the size of the backup data, but can take longer to process the data

If you upgrade an earlier Agent version to version 7.5 or later, existing jobs are run with the Faster compression option unless you change the compression option to Smaller.

## Log File Options

Select one of the following job logging levels from the list:

- **Files** — Provides the most detailed information, and is typically used for troubleshooting. Provides information about files that are backed up.
- **Directory** — Provides less detail than the Files logging level. Provides information about folders that are backed up.
- **Summary** — Provides high-level information, including the vault and Agent version, and backup sizes.
- **Minimal** — Provides high-level information, including the vault and Agent version.

Changing the logging level only affects log files that are created from that point and after. It does not affect previously-created log files.

*Note:* For Image Plug-in jobs, the selected logging level does not affect the content of the logs.

### 5.1.6 Policy retention types

When Admin users create or edit policies, they can create retention types in the policies. Retention types specify the number of days a backup is kept on the vault, how many copies of a backup are stored online, and how long backup data is stored offline.

When running or scheduling a job on a computer where a policy is assigned, the user can select a retention type from the policy. Retention types cannot be added or changed on a computer when a policy is assigned.

### Predefined Retention Types

There are three predefined retention types in a policy: Daily, Weekly, and Monthly. You can modify the predefined retention types.

The predefined (default) retentions are as follows:

Retention	Days Online	Copies Online	Days Archived
Daily	7	7	0
Weekly	31	5	0
Monthly	365	12	0

If data archiving is disabled in your Portal instance, the Days Archived value does not appear.

You can create retention types until there are as many as ten (including the three predefined retentions) for each policy.

### Create a policy retention type

When Admin users create or edit policies, they can create retention types in the policies. Retention types specify the number of days a backup is kept on the vault, how many copies of a backup are stored online, and how long backup data is stored offline.

To create a retention type:

1. On the Policies page, on the Retention Types tab for a policy, click **Create Retention Type**.
2. In the Retention Type dialog box, complete the following fields:

Name	Specifies a name for the retention type.
Backup Retention	Specifies the number of days a safeset is kept on the vault. A safeset is deleted when its expiry date is reached. <i>Note:</i> Safesets are not deleted unless the specified number of copies online has also been exceeded.
Number of Backup Copies to Keep	Specifies how many safesets from a backup job are stored online. It functions in a first in/first out manner. Once the number of safesets is exceeded, the oldest safesets are automatically deleted until the actual number of safesets matches the definition. <i>Note:</i> Safesets are not deleted unless the specified number of days online has also been exceeded.
Create archived copies	Select this check box to create archived copies of safesets.




Keep Archives For	<p><i>Note:</i> If data archiving is disabled in your Portal instance, this value does not appear.</p> <p>Specifies how long the data is stored offline. Archive storage is used to store data offline for long periods of time. This data is not immediately accessible since it is stored remotely. A greater amount of time is required to restore from archive media. Typically, only long-term data archives are stored offline. The parameters for archived data are from 365 to 9999 days.</p> <p>Assuming that at least one successful backup has been completed for the job, there will never be less than one copy of its backup online. This is true even if all retention settings are zero, expiry conditions have been met, and the job definition is deleted from your system. Deleting the job does not affect data on the vault. Only your service provider can remove jobs and their associated data from the vault. This is a safeguard against accidental or malicious destruction of data.</p>
-------------------	---

3. Click **Save**.

### Delete a policy retention type

When Admin users edit policies, they can delete retention types from the policies. Retention types specify the number of days a backup is kept on the vault, how many copies of a backup are stored online, and how long backup data is stored offline.


To delete a retention type:

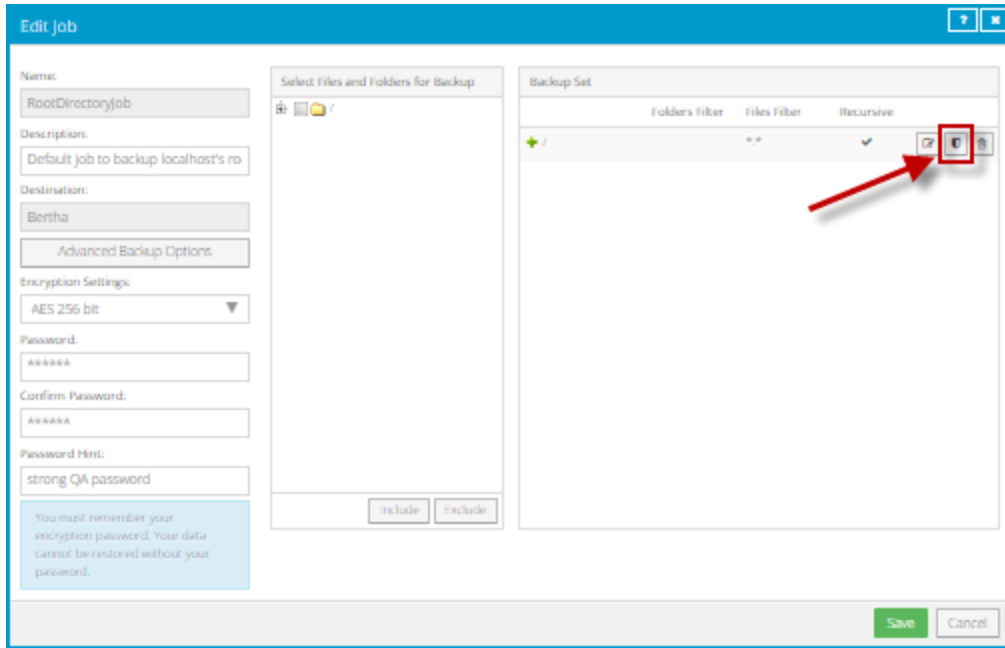
1. On the Policies page, on the Retention Types tab for a policy, locate the row for the retention within the table of retention types.
2. In the row for the retention type that you want to delete, click the **Delete** button. 

### 5.1.7 Policy filters for backup jobs

When Admin users create or edit policies, they can specify files and folders to include in or exclude from backups using the **Inclusions/Exclusions** tab.

File and folder filters are not applied automatically in backup jobs on computers where the policy is assigned. Instead, when creating or editing a Local System, UNC or NFS job, a user can click the **Apply Policy**

**Filters** button  in the **Backup Set** box to apply filters from the policy.



### Include subdirectories

Specifies whether subdirectories are included in backups. Select this check box to back up subdirectories of directories that are selected in a backup job.

### Filters to include

Specifies names of files and subdirectories to back up. Users can apply these filters to a folder in a backup job so that only files and subdirectories with the specified names are backed up. For example, you can specify that only files with the “.docx” extension in a selected folder should be backed up.

In the **Files** field, enter the names of files to include in a backup. Separate multiple file names with commas, and use asterisks (\*) as wildcard characters. For example, to only back up files in a selected folder that have the “.docx” extension or have file names that start with “tax”, enter the following filter: \*.docx, tax\*

In the **Folders** field, enter the names of subdirectories to include in a backup. Separate multiple folder names with commas, and use asterisks (\*) as wildcard characters. For example, to only back up subdirectories in a selected folder that start with the letter “a” or end with “2013”, enter the following filter: a\*, \*2013

*Note:* Asterisks (\*) are the only supported wildcards in filter fields.

### Filters to exclude

Specifies names of files and folders to exclude from a backup. Users can apply these filters to a folder that is excluded from a backup job so that only files and subdirectories with the specified names are excluded from the backup. For example, you can specify that files with the “.jpg” extension in a selected folder should not be backed up.

In the **Files** field, enter the names of files to exclude from a backup. Separate multiple file names with commas, and use asterisks (\*) as wildcard characters. For example, to exclude files in a selected folder that have the “.jpg” extension or have file names that end with “2001”, enter the following filter: \*.jpg, \*2001

In the **Folders** field, enter the names of subdirectories to exclude from a backup. Separate multiple folder names with commas, and use asterisks (\*) as wildcard characters. For example, to exclude subdirectories from a backup if their names end with “-old” or start with “2001”, enter the following filter: \*-old, 2001\*

*Note:* Asterisks (\*) are the only supported wildcards in filter fields.

## 5.2 Edit a policy

Admin users can edit policies that provide settings for computers and jobs. Policy settings include log file options, email notifications and bandwidth settings.

When you edit a policy that is assigned to one or more computers, you can choose whether or not to apply the changes to computers where the policy is assigned. Policy changes are only applied to settings that apply to all backup jobs on the computer and appear on a computer’s Advanced tab. Job-specific settings, such as log file options, are not changed on existing jobs.

To edit a policy:

1. On the Policies page, locate the policy that you want to change.
2. Click the policy row to expand its view.
3. Specify one or more of the following policy settings for computers:
  - [Policy schedule, hibernation and shutdown options](#)
  - [Policy email notification settings](#)
  - [Policy execution priority and bandwidth options](#)
  - [Vault profiles for policies](#)
4. Specify one or more of the following policy settings for jobs:
  - [Policy compression and log settings](#)
  - [Policy retention types](#)
  - [Policy filters for backup jobs](#)
5. Click **Save** when you have finished.
6. If a message asks whether you want to reconcile policy details with computers where the policy is assigned, do one of the following:
  - To apply policy changes on computers where the policy is assigned, click **OK**.  
*Note:* Policy changes are only applied to settings on the computer’s Advanced tab that apply to all backup jobs on the computer. Job-specific settings, such as log file options, are not changed on existing jobs.
  - To leave existing settings on computers where the policy is assigned, click **Cancel**.

## 5.3 Assign a policy to computers

Admin users can assign policies to computers to provide settings for computers and jobs. When a policy is assigned to a computer:

- Some settings are used for all backup jobs on the computer. These settings appear on the computer's Advanced tab, and cannot be modified. To change the settings, you must unassign the policy from the computer, or edit values in the policy. See [Policy schedule, hibernation and shutdown options](#), [Policy email notification settings](#) and [Policy execution priority and bandwidth options](#).
- Some settings are not automatically applied to jobs. When creating or editing a job on the computer, a user can select these policy settings or select other values. See [Policy compression and log settings](#) and [Policy filters for backup jobs](#).
- A user can select a vault profile from the policy when adding vault settings, instead of manually entering vault information and credentials. See [Vault profiles for policies](#).
- A user can select a retention type from the policy when running or scheduling a job. See [Policy retention types](#).

When you assign a policy to a computer, existing retention types on the computer are removed if they are not used in jobs. Retention types that are used in jobs are not removed from the computer. If a retention type in the policy has the same name as an existing retention type that is used in a job, the retention type from the policy is renamed on the computer (e.g., Daily to Daily\_1).

Admin users can assign the same policy to more than one computer at the same time.

*Note:* You cannot assign a policy to a Hyper-V Agent until Hyper-V environment settings are configured for the agent.

*Note:* You cannot assign a policy to a vSphere Recovery Agent until vault and vSphere environment settings are configured for the agent.

To assign a policy to computers:

1. On the navigation bar, click **Computers**.  
The Computers page lists computers assigned to users in the site.
2. Select the check box for each computer to which you want to assign the policy.
3. In the **Actions** list, click **Assign Policy to Selected Computer(s)**.  
The Assign Policy dialog box opens.
4. Click the policy to assign to each selected computer.
5. Click **Assign**.  
The Assign Policy dialog box closes, and the policy name that you have chosen appears in the Policy column for the computer.

## 5.4 Unassign policies from computers

Admin users can unassign policies from one or more computers at the same time.

When you unassign a policy from a computer, settings on the computer do not change unless you edit them.

To unassign policies from computers:

1. On the navigation bar, click **Computers**.  
The Computers page lists computers for users in the site.
2. Select the check box for each computer from which you want to remove policies.
3. In the **Actions** list, click **Unassign Policy from Selected Computer(s)**.  
A confirmation message asks whether you want to unassign policies from the selected computers.
4. Click **Yes**.

## 6 Set security preferences

Super users and, if allowed, Admin users can set security preferences for sites in Server Backup Portal.

Security preferences include:

- Account locking settings, such as the number of failed logins before an account is locked, and the amount of time that an account remains locked. If a user tries to sign in when his or her account is locked, Admin users for the site will receive an email notification.
- Password requirements, such as the number of characters in a password, and the number of days after which users must change their passwords.
- Amount of idle time before a Portal session is timed out.

Portal is installed with “factory” security preferences that can be applied to any site. Super users can also create default security preferences that can be applied to any site. See [Specify default security preferences](#).

Super users can set security preferences for any site. Admin users can set security preferences for child sites that they manage, and may be allowed to set security preferences for their own sites. See [Set security preferences for a site](#) and [Set security preferences for your site](#).

### 6.1 Specify default security preferences

Super users can specify default security preferences that can be applied to sites in the Portal instance. Security preferences include password requirements and policies for failed login attempts.

The default security preferences can be:

- “Factory” security preferences that are installed with Portal. Factory security preferences cannot be edited.
- Custom security preferences, created by a Super user.

Super users can set security preferences for any site. Admin users can set security preferences for child sites that they manage, and may be allowed to set security preferences for their own sites. See [Set security preferences for a site](#) and [Set security preferences for your site](#).

To specify default security preferences for the Portal instance:

1. When signed in as a Super user, click **Global Settings** on the navigation bar.
2. Click the **Security Preferences** tab.
3. Do one of the following:
  - To use the security preferences that are installed with Portal as the default security preferences, select **Factory preferences**.
  - To create custom default security preferences, select **Custom preferences**. Change values in

any of the following fields:

<b>Password Validity</b>	
Maximum Consecutive Failed Logins	Specifies the number of consecutive failed login attempts after which an account is locked. The value must be between 1 and 999.
Lockout Time (minutes)	Specifies the number of minutes an account is locked after a user reaches the maximum number of failed login attempts. The value must be between 1 and 1440 minutes.  Admin users and Super users can unlock locked accounts. See <a href="#">Unlock a user's account</a> .
Password Expiry (in days)	Specifies the number of days after which a user's password expires and the user must change the password.  If you do not want passwords to expire, enter 0 (zero).
Password Reuse History	Specifies the number of previous passwords that a user cannot repeat. The value must be between 1 and 24.
<b>Password Strength</b>	
Minimum Password Length	Specifies the minimum number of characters in a password. The value must be between 6 and 30.
Minimum Uppercase Characters	Specifies the minimum number of uppercase letters in a password. The value must be between 0 and 30.
Minimum Lowercase Characters	Specifies the minimum number of lowercase letters in a password. The value must be between 0 and 30.
Minimum Numeric Characters	Specifies the minimum number of numeric characters in a password. The value must be between 0 and 30.
Minimum Special Characters	Specifies the minimum number of special characters in a password. The value must be between 0 and 30.
Allowed Special Characters	Specifies special characters that are allowed in a password. Commas, letters, and numbers cannot be allowed as special characters.
<b>User Session</b>	
Session Timeout (minutes)	Specifies the amount of idle time in minutes before a session is timed out. The value must be between 1 and 1440 minutes.

4. Click **Save**.

## 6.2 Set security preferences for a site

Super users can set security preferences for any site, and Admin users can set security preferences for child sites that they manage.

Security preferences include password requirements and policies for failed login attempts. An option also specifies whether Admin users in a site can change the site’s security preferences as described in [Set security preferences for your site](#).

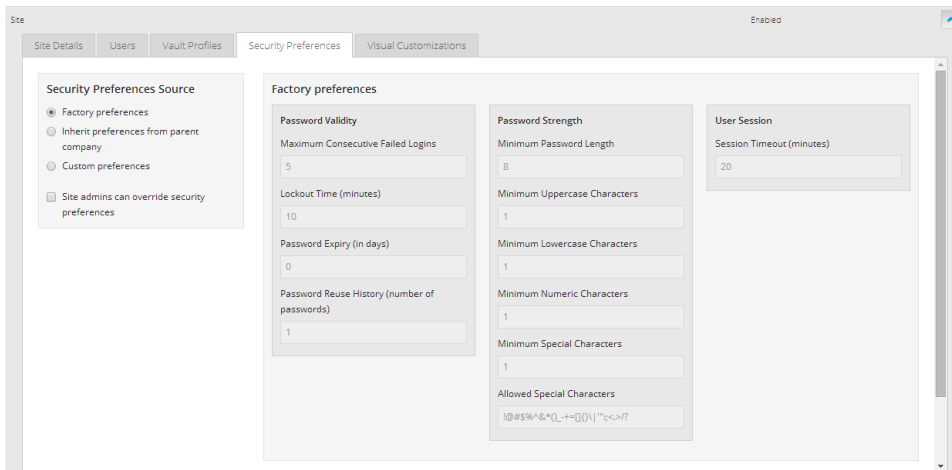
To set a site’s security preferences, you can do one of the following:

- Apply “factory” security preferences that are installed with Portal.
- If the site is a parent site, apply the default security preferences for the Portal instance.  
*Note:* Super users specify the default security preferences. See [Specify default security preferences](#).
- If the site is a child site, apply the parent site’s security preferences.
- Create custom security preferences.

To set security preferences for a site:

1. When signed in as a Super user or as an Admin user who can manage child sites, click **Sites** on the navigation bar.
2. Find the site for setting security preferences, and expand its view by clicking the site row.
3. Click the **Security Preferences** tab.

The tab shows the site’s current security preferences.



4. Do one of the following:
  - To apply the security preferences that are installed with Portal, select **Factory preferences**.
  - If the site is a parent site, to apply the default security preferences for the Portal instance, select **Inherit preferences from Portal instance**.
  - If the site is a child site, to apply the parent site’s security preferences, select **Inherit preferences from parent company**.

If you select factory, default, or parent site security preferences, values in the Password Validity, Password Strength, and User Session boxes cannot be edited.



- To create custom security preferences for the site, select **Custom preferences**. Change values in any of the following fields:

<b>Password Validity</b>	
Maximum Consecutive Failed Logins	Specifies the number of consecutive failed login attempts after which an account is locked. The value must be between 1 and 999.
Lockout Time (minutes)	Specifies the number of minutes an account is locked after a user reaches the maximum number of failed login attempts. The value must be between 1 and 1440 minutes. Admin users and Super users can unlock locked accounts. See <a href="#">Unlock a user's account</a> .
Password Expiry (in days)	Specifies the number of days after which a user's password expires and the user must change the password. If you do not want passwords to expire, enter 0 (zero).
Password Reuse History	Specifies the number of previous passwords that a user cannot repeat. The value must be between 1 and 24.
<b>Password Strength</b>	
Minimum Password Length	Specifies the minimum number of characters in a password. The value must be between 6 and 30.
Minimum Uppercase Characters	Specifies the minimum number of uppercase letters in a password. The value must be between 0 and 30.
Minimum Lowercase Characters	Specifies the minimum number of lowercase letters in a password. The value must be between 0 and 30.
Minimum Numeric Characters	Specifies the minimum number of numeric characters in a password. The value must be between 0 and 30.
Minimum Special Characters	Specifies the minimum number of special characters in a password. The value must be between 0 and 30.
Allowed Special Characters	Specifies special characters that are allowed in a password. Commas, letters, and numbers cannot be allowed as special characters.
<b>User Session</b>	
Session Timeout (minutes)	Specifies the amount of idle time in minutes before a session is timed out. The value must be between 1 and 1440 minutes.

5. To allow Admin users in the site to change the site's security preferences, select the **Site admins can override security preferences** option.
6. Click **Save**.

## 6.3 Set security preferences for your site

Admin users in a site may be allowed to set security preferences for the site. Security preferences include password requirements and policies for failed login attempts.

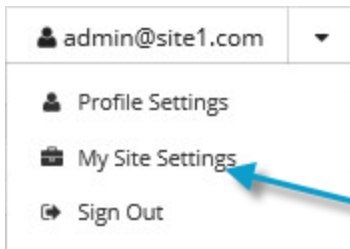
A Super user or Admin user who manages child sites can specify whether Admin users in a site can customize the site's security preferences. See [Set security preferences for a site](#).

If you are an Admin user who is allowed to set security preferences for your site, you can do one of the following:

- Apply “factory” security preferences that are installed with Portal.
- If the site is a parent site, apply the default security preferences for the Portal instance.  
Super users specify the default security preferences. See [Specify default security preferences](#).
- If the site is a child site, apply the parent site's security preferences.
- Create custom security preferences.

To set security preferences for your site:

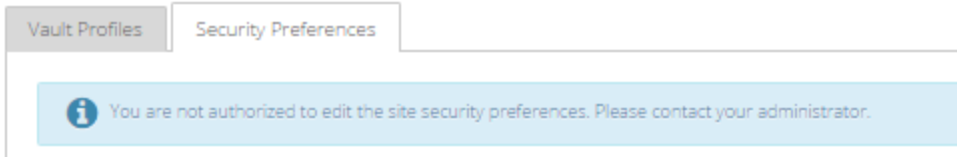
1. When signed in as an Admin user, click the email address that you used to sign in to Portal at the top right of the Portal page.



2. Click **My Site Settings**.
3. Click the **Security Preferences** tab.

The tab shows your site's current security preferences.

If a message states that you are not authorized to edit the site security preferences, you cannot set security preferences for your site. Please contact your Portal administrator to request permission to set security preferences.



4. Do one of the following:

- To apply the security preferences that are installed with Portal, select **Factory preferences**.
- If the site is a parent site, to apply the default security preferences for the Portal instance, select **Inherit preferences from Portal instance**.
- If the site is a child site, to apply the parent site’s security preferences, select **Inherit preferences from parent company**.

If you select factory, default, or parent site security preferences, values in the Password Validity, Password Strength, and User Session boxes cannot be edited.

- To create custom security preferences for the site, select **Custom preferences**. Change values in any of the following fields:

Password Validity	
Maximum Consecutive Failed Logins	Specifies the number of consecutive failed login attempts after which an account is locked. The value must be between 1 and 999.

Lockout Time (minutes)	Specifies the number of minutes an account is locked after a user reaches the maximum number of failed login attempts. The value must be between 1 and 1440 minutes. Admin users and Super users can unlock locked accounts. See <a href="#">Unlock a user's account</a> .
Password Expiry (in days)	Specifies the number of days after which a user's password expires and the user must change the password. If you do not want passwords to expire, enter 0 (zero).
Password Reuse History	Specifies the number of previous passwords that a user cannot repeat. The value must be between 1 and 24.
<b>Password Strength</b>	
Minimum Password Length	Specifies the minimum number of characters in a password. The value must be between 6 and 30.
Minimum Uppercase Characters	Specifies the minimum number of uppercase letters in a password. The value must be between 0 and 30.
Minimum Lowercase Characters	Specifies the minimum number of lowercase letters in a password. The value must be between 0 and 30.
Minimum Numeric Characters	Specifies the minimum number of numeric characters in a password. The value must be between 0 and 30.
Minimum Special Characters	Specifies the minimum number of special characters in a password. The value must be between 0 and 30.
Allowed Special Characters	Specifies special characters that are allowed in a password. Commas, letters, and numbers cannot be allowed as special characters.
<b>User Session</b>	
Session Timeout (minutes)	Specifies the amount of idle time in minutes before a session is timed out. The value must be between 1 and 1440 minutes.

5. Click **Save**.

## 7 Customize the Portal appearance

Super users and, if allowed, Admin users can customize the Server Backup Portal appearance so that users see their company or service provider’s logo, colors, and contact information when they sign in.

Super users can create a default Portal appearance that can be applied to any site in Portal. See [Customize the default Portal appearance](#).

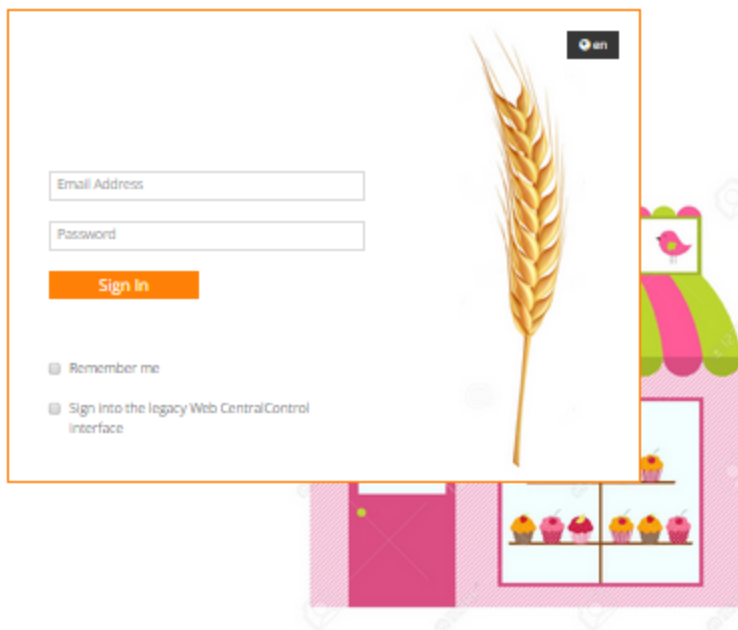
Super users can customize the Portal appearance for any site. Admin users can customize the Portal appearance for child sites that they manage, and may be allowed to customize the Portal appearance for their own sites. See [Customize the Portal appearance for a site](#) and [Customize the Portal appearance for your site](#).

### 7.1 Customize the default Portal appearance

Super users can create a default appearance that can be applied to any site in the Portal instance. Customizations can include:

- Logo settings, including an image, tooltip, and link
- Header and font colors
- Company text, email address, and website link
- Sign-in page appearance. As shown in the following example, the sign-in page can be completely customized. A web developer is required who can inspect the sign-in page markup and create custom CSS for the page.

**Angies Bakery**



The Portal appearance can also be customized for a specific site. See [Customize the Portal appearance for a site](#).

To customize the default Portal appearance for the Portal instance:

1. When signed in as a Super user, click **Global Settings** on the navigation bar.
2. Click the **Default Visual Customizations** tab.
3. To change the logo settings, do one or more of the following in the **Logo** area:
  - To display a different logo, click **Upload Logo**. In the dialog box, click the logo image file, and then click **Open**.  
The logo must not exceed 115 x 40 pixels or 1 MB in size.
  - To change the logo tooltip text, enter the text in the **Logo Hover Over Title** box.
  - To change the logo link, enter the URL in the **Logo URL Link** box.
  - To not display a logo on the Sign In page, click **Delete Logo**.
4. To change the logo that appears on the Sign In page, do one of the following in the **Login Page Logo** area:
  - To display a different logo, click **Upload Logo**. In the dialog box, click the logo image file, and then click **Open**.  
The logo will be resized to 100 pixels in height. The file must not exceed 1 MB in size.
  - To not display a logo on the Sign In page, click **Delete Logo**.
5. To change the sign-in page appearance, enter custom CSS in the **Login Page Custom CSS** box.

Do not include line breaks in selector lists or before the opening curly brace in a declaration. For example, you can use the following css:

```
.btn, .btn-success {  
color: #ffffff;  
}
```

The following css will not work because of the line breaks between `.btn,` and `.btn-success`, and between `.btn-success` and the opening curly brace:

```
.btn,  
.btn-success  
{  
color: #ffffff;  
}
```

6. To change header and font colors, do one or more of the following in the **Color Scheme** area:
  - To change the header color, click the **Header Background Color** box. In the color palette, click or enter the new color, and then click **Save**.
  - To change the header text color, click the **Header Font Color** box. In the color palette, click or enter the new font color, and then click **Save**.
  - To change the dialog box header color, click the **Popup Header Background Color** box. In the color palette, click or enter the new color, and then click **Save**.
  - To change the dialog box header text color, click the **Popup Header Font Color** box. In the color palette, click or enter the new font color, and then click **Save**.
  - To change the Support icon color, click the **Support Icon Color** box. In the color palette, click or enter the new color, and then click **Save**.
7. To change text and links, do one or more of the following in the **Custom Text** area:
  - To change the text that appears on the Sign In page and on the web page tab, enter the new text in the **Page Title** box.
  - To change the copyright text that appears on the Sign In page and at the bottom of each page, enter the new text in the **Copyright** box.
  - To change the Support website link, enter the new URL in the **Support URL** box.
  - To change the Support email address, enter the new email address in the **Support Email** box.
8. Click **Save**.

## 7.2 Customize the Portal appearance for a site

Super users can customize the Portal appearance for any site, and Admin users can customize the Portal appearance for child sites that they manage.

Admin users in the site may also be allowed to change the logo, colors, or company information for the site. See [Customize the Portal appearance for your site](#).

Customizations can include:

- Logo settings, including an image, tooltip, and link
- Header and font colors
- Company text, email address, and website link

If a parent site's appearance has been customized, the settings can also be applied to the site's child sites.

Reports in Microsoft Excel (.xls) and Adobe Acrobat (.pdf) format are also customized using the site's logo, color, and company text.

To customize the Portal appearance for a site:

1. When signed in as a Super user or as an Admin user who can manage child sites, click **Sites** on the navigation bar.

2. Find the site for customizing the Portal appearance, and expand its view by clicking the site row.
3. Click the **Visual Customizations** tab.
4. To change logo settings, do one of the following in the Logo area:
  - To use the logo settings that are installed with Portal, click **Factory Settings**.
  - To use the logo settings from the default Portal appearance, click **Inherit Global Settings**.
  - If the site is a child site, to use the parent site's logo settings, click **Inherit Parent Site Settings**.
  - To customize logo settings for the site, click **Custom Settings**, and then do one or more of the following:
    - To display a different logo, click **Upload Logo**. In the Choose File to Upload dialog box, click the logo image file, and then click **Open**.

The logo must not exceed 115 x 40 pixels or 1 MB in size.

The logo also appears on site reports in Microsoft Excel (.xls) and Adobe Acrobat (.pdf) format.
    - To not display a logo, click **Delete Logo**.
    - To change the logo tooltip text, enter the text in the **Logo Hover Over Title** box.
    - To change the logo link, enter the URL in the **Logo URL Link** box.
    - To allow Admin users in the site to change the logo settings, select the **Admins can override logo** check box.
5. To change header and font colors, do one of the following in the Color Scheme area:
  - To use colors that are installed with Portal, click **Factory Settings**.
  - To use colors from the default Portal appearance, click **Inherit Global Settings**.
  - If the site is a child site, to use the parent site's colors, click **Inherit Parent Site Settings**.
  - To specify custom colors, click **Custom Settings**, and then do one or more of the following:
    - To change the header color, click the **Header Background Color** box. In the color palette, click or enter the new color, and then click **Save**.

The header background color is also used for column headings in site reports.
    - To change the header text color, click the **Header Font Color** box. In the color palette, click or enter the new font color, and then click **Save**.

The header text color is also used for column heading text in site reports.
    - To change the dialog box header color, click the **Popup Header Background Color** box. In the color palette, click or enter the new color, and then click **Save**.
    - To change the dialog box header text color, click the **Popup Header Font Color** box. In the color palette, click or enter the new font color, and then click **Save**.



- To change the Support icon color, click the **Support Icon Color** box. In the color palette, click or enter the new color, and then click **Save**.

To allow Admin users in the site to change the colors, select **Admins can override color scheme**.

6. To change text and links, do one or more of the following in the Custom Text area:

- To use text and links that are installed with Portal, click **Factory Settings**.
- To use text and links from the default Portal appearance, click **Inherit Global Settings**.
- If the site is a child site, to use text and links from the parent site, click **Inherit Parent Site Settings**.
- To specify custom text and links, click **Custom Settings**, and then do one or more of the following:
  - To change the text that appears on a web page tab for the Portal, enter the new text in the **Page Title** box. To allow Admin users in the site to change the text, select the **Admins can override title** check box.  
  
The page title also appears on site reports in Microsoft Excel (.xls) and Adobe Acrobat (.pdf) format.
  - To change the copyright text that appears at the bottom of the Portal, enter the new text in the **Copyright** box. To allow Admin users in the site to change the text, select the **Admins can override copyright** check box.  
  
The copyright text also appears on site reports in Microsoft Excel (.xls) and Adobe Acrobat (.pdf) format.
  - To change the Support website link, enter the new URL in the **Support URL** box. To allow Admin users in the site to change the link, select the **Admins can override URL** check box.
  - To change the Support email address, enter the new email address in the **Support Email** box. To allow Admin users in the site to change the email address, select the **Admins can override Email** check box.

7. Click **Save**.

## 7.3 Customize the Portal appearance for your site

Admin users in a site can be allowed to customize the Portal appearance for the site. A Super user or Admin user can specify whether Admin users in a site can customize the site's Portal appearance. See [Customize the Portal appearance for a site](#).

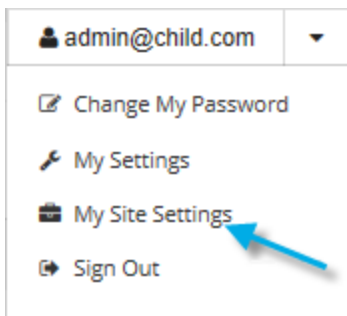
Customizations can include:

- Logo settings, including an image, tooltip, and link
- Header and font colors
- Company text, email address, and website link

Reports in Microsoft Excel (.xls) and Adobe Acrobat (.pdf) format are also customized using the site's logo, color, and company text.

To customize the Portal appearance for your site:

1. When signed in as an Admin user, click the email address that you used to sign in to Portal at the top right of the Portal page.



2. Click **My Site Settings**.

If the Visual Customizations tab does not appear on the page, you are not allowed to customize the Portal appearance for your site. Please contact your Portal administrator to request permission to customize the Portal appearance.

3. If the Logo box appears on the page, to change logo settings, do one or more of the following:

- To display a different logo, click **Upload Logo**. In the Choose File to Upload dialog box, click the logo image file, and then click **Open**.

The logo must not exceed 115 x 40 pixels or 1 MB in size.

The logo also appears on site reports in Microsoft Excel (.xls) and Adobe Acrobat (.pdf) format.

- To not display a logo, click **Delete Logo**.
- To change the logo tooltip text, enter the text in the **Logo Hover Over Title** box.
- To change the logo link, enter the URL in the **Logo URL Link** box.

4. If the Color Scheme box appears on the page, do one or more of the following:

- To change the header color, click the **Header Background Color** box. In the color palette, click or enter the new color, and then click **Save**.

The header color is also used for column headings in site reports.

- To change the header text color, click the **Header Font Color** box. In the color palette, click or enter the new font color, and then click **Save**.

The header text color is also used for column heading text in site reports.

- To change the dialog box header color, click the **Popup Header Background Color** box. In the color palette, click or enter the new color, and then click **Save**.
- To change the dialog box header text color, click the **Popup Header Font Color** box. In the color palette, click or enter the new font color, and then click **Save**.

- To change the Support icon color, click the **Support Icon Color** box. In the color palette, click or enter the new color, and then click **Save**.
5. If the Custom Text box appears on the page, to change text and links, do one or more of the following:

*Note:* You might not be allowed to change all of the text and links. If one of the following boxes does not appear, you are not allowed to change the associated text or link.

- To change the text that appears on a web page tab for the Portal, enter the new text in the **Page Title** box. To allow Admin users in the site to change the text, select the **Admins can override title** check box.

The page title also appears on site reports in Microsoft Excel (.xls) and Adobe Acrobat (.pdf) format.

- To change the copyright text that appears at the bottom of the Portal, enter the new text in the **Copyright** box. To allow Admin users in the site to change the text, select the **Admins can override copyright** check box.

The copyright text also appears on site reports in Microsoft Excel (.xls) and Adobe Acrobat (.pdf) format.

- To change the Support website link, enter the new URL in the **Support URL** box. To allow Admin users in the site to change the link, select the **Admins can override URL** check box.
- To change the Support email address, enter the new email address in the **Support Email** box. To allow Admin users in the site to change the email address, select the **Admins can override Email** check box.

6. Click **Save**.

## 8 Create and manage default retention types

Before you can run or schedule a backup job for a computer, the computer must have at least one retention type. A retention type specifies the number of days a backup is kept on the vault and how many copies of a backup are stored online. If data archiving is available in your Portal instance, the retention type also specifies how long backup data is stored offline.

If an agent does not have a retention type when it registers to Portal, Portal applies default retention types to the computer for backups that run daily or less often. In particular, Portal applies these retention types to computers with Agent versions 8.10 and later. These Agent versions do not have retention types when they are installed.

Super users can create, change and delete default retention types for backups that run daily or less often. If the default retention types have not been changed, two default retention types are available:

- Daily (30 days online, 30 copies, no archiving). With this retention type, each backup is kept for at least 30 days and at least 30 backups with the same retention type are stored online.
- Monthly (365 days online, 11 copies, no archiving). With this retention type, each backup is kept for at least 365 days and at least 11 backups with the same retention type are stored online.

*Note:* In some Portal instances, the Daily and Monthly default retention types cannot be changed or deleted.

*Note:* If data archiving is disabled in your Portal instance, archiving values do not appear in the Portal UI.

Beginning in Portal 8.88, retention types are also available for intra-daily schedules. These retention types are applied to a computer when you create an intra-daily schedule. See [Retention types for intra-daily backup schedules](#).

### 8.1 Create default retention types

Super users can create default retention types for backups that run daily or less often.

Beginning in Portal 8.88, a maximum of eight default retention types are allowed for backups that run daily or less often. An additional two retention types are available for backups that are scheduled by intra-daily schedules. See [Retention types for intra-daily backup schedules](#).

To create a default retention type:

1. When signed in as a Super user, click **Global Settings** on the navigation bar.
2. Click the **Default Retention Types** tab.  
The tab shows the current default retention types.
3. Click **Add New Default Retention Type**.  
The Add New Default Retention Type box appears.

4. Complete the following fields:

Name	Specifies a name for the retention type.
Days Online	Specifies the number of days a safeset is kept on the vault. A safeset is deleted when its expiry date is reached. <i>Note:</i> Safesets are not deleted unless the specified number of copies online has also been exceeded.
Copies Online	Specifies how many safesets from a backup job are stored online. It functions in a first in/first out manner. Once the number of safesets is exceeded, the oldest safesets are automatically deleted until the actual number of safesets matches the definition. <i>Note:</i> Safesets are not deleted unless the specified number of days online has also been exceeded.
Archive Days	<i>Note:</i> If data archiving is disabled in your Portal instance, this value does not appear. Specifies how long the data is stored offline. Archive storage is used to store data offline for long periods of time. This data is not immediately accessible since it is stored remotely. A greater amount of time is required to restore from archive media. Typically, only long-term data archives are stored offline. The parameters for archived data are from 365 to 9999 days. Assuming that at least one successful backup has been completed for the job, there will never be less than one copy of its backup online. This is true even if all retention settings are zero, expiry conditions have been met, and the job definition is deleted from your system. Deleting the job does not affect data on the vault. Only your service provider can remove jobs and their associated data from the vault. This is a safeguard against accidental or malicious destruction of data.

5. Click **Save**.

## 8.2 Change default retention types

Super users can edit default retention types for backups that run daily or less often.

*Note:* In some Portal instances, the Daily and Monthly default retention types cannot be changed.

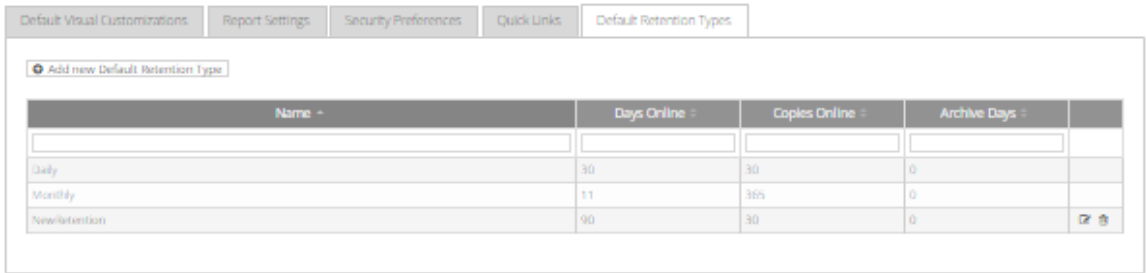
If an agent does not have a retention type when it registers to Portal, Portal applies default retention types to the computer for backups that run daily or less often. In particular, Portal applies default retention types to computers with Agent versions 8.10 and later. These Agent versions do not have retention types when they are installed.


To change a default retention type:

1. When signed in as a Super user, click **Global Settings** on the navigation bar.
2. Click the **Default Retention Types** tab.

The tab shows the current default retention types.

*Note:* If data archiving is disabled in your Portal instance, the Archive Days column does not appear.



3. In the row of the default retention type that you want to change, click the Edit button. 

*Note:* If the Edit button does not appear in a row, you cannot change that default retention type. The Edit Retention Type box appears.
4. Change values in one or more of the following fields:

Name	Specifies a name for the retention type.
Days Online	Specifies the number of days a safeset is kept on the vault. A safeset is deleted when its expiry date is reached. <i>Note:</i> Safesets are not deleted unless the specified number of copies online has also been exceeded.
Copies Online	Specifies how many safesets from a backup job are stored online. It functions in a first in/first out manner. Once the number of safesets is exceeded, the oldest safesets are automatically deleted until the actual number of safesets matches the definition. <i>Note:</i> Safesets are not deleted unless the specified number of days online has also been exceeded.
Archive Days	<i>Note:</i> If data archiving is disabled in your Portal instance, this value does not appear. Specifies how long the data is stored offline. Archive storage is used to store data offline for long periods of time. This data is not immediately accessible since it is stored remotely. A greater amount of time is required to restore from archive media. Typically, only long-term data archives are stored offline. The parameters for archived data are from 365 to 9999 days. Assuming that at least one successful backup has been completed for the job, there will never be less than one copy of its backup online. This is true even if all retention settings are zero, expiry conditions have been met, and the job definition is deleted from your system. Deleting the job does not affect data on the vault. Only your service provider can remove jobs and their associated data from the vault. This is a safeguard against accidental or malicious destruction of data.

5. Click **Save**.

### 8.3 Delete default retention types

Super users can delete default retention types for backups that run daily or less often.

*Note:* In some Portal instances, the Daily and Monthly default retention types cannot be deleted.

If an agent does not have a retention type when it registers to Portal, Portal applies default retention types to the computer for backups that run daily or less often. In particular, Portal applies default retention types to computers with Agent versions 8.10 and later. These Agent versions do not have retention types when they are installed.

To delete a default retention type:

1. When signed in as a Super user, click **Global Settings** on the navigation bar.
2. Click the **Default Retention Types** tab.

The tab shows the current default retention types.

*Note:* If data archiving is disabled in your Portal instance, the Archive Days column does not appear.

Name	Days Online	Copies Online	Archive Days
Daily	30	30	0
Monthly	11	365	0
NewRetention	90	30	0

3. In the row of the default retention type that you want to change, click the Delete button.

*Note:* If the Delete button does not appear in a row, you cannot delete that default retention type.

4. In the confirmation message box, click **Yes**.

## 8.4 Retention types for intra-daily backup schedules

Beginning with Windows Agent 8.90, Linux Agent 8.90, AIX Agent 9.00 and vSphere Recovery Agent (VRA) 9.11, when an agent is backing up data to a Director version 8.60 or later vault, you can schedule the backup job to run multiple times per day by creating an intra-daily schedule. You can create an intra-daily schedule for a Windows, Linux or AIX backup job using Portal 8.88 or later. You can create an intra-daily schedule for vSphere backup jobs beginning in Portal 9.20.

Two default retention types are available for intra-daily schedules:

- 24-Hours (1 day online, 1 copy online, no archiving). With this retention type, each backup is kept for at least 24 hours and at least one backup with this retention type is stored online.
- 48-Hours (2 days online, 1 copy online, no archiving). With this retention type, each backup is kept for at least 48 hours and at least one backup with this retention type is stored online.

These retention types can only be selected when you create an intra-daily schedule. Unlike default retention types for backups that run daily or less often, intra-daily retention types appear on a computer's Retention Types tab after you create an intra-daily schedule for the computer, not when an agent first registers to Portal.

The 24-Hours and 48-Hours retention types are the only retention types available for intra-daily schedules. You cannot create, change or delete default retention types for intra-daily schedules.



## 9 Manage Windows agent upgrades

Windows agent installers can be provided through Server Backup Portal. Agents can then download the installers and upgrade themselves automatically; you do not have to manually run an installer on each computer.

To provide agent installers through Portal and start automatic agent upgrades:

- Super users specify a UNC location for saving the installers. Super users can also specify whether Admin users can start upgrades on all eligible computers in their sites and whether agent installers can be signed by another service provider. See [Set up an agent installer location and permissions](#),
- Super users upload agent installers to the UNC location and specify which installers are active (i.e., available for automatically upgrading agents). See [Set up an agent installer location and permissions](#), [Upload agent installers](#) and [Activate, deactivate or delete an agent installer](#).
- Super users and Admin users, if allowed, can start agent upgrades on all eligible computers in selected sites. Admin users can also start agent upgrades on specific computers in their sites and view the agent upgrade status of each computer. See [Upgrade agents on eligible computers](#).

To be eligible for an automatic upgrade, a computer must have Windows Agent version 8.70 or later installed. If a previous Windows Agent version is installed, the agent must be manually upgraded to version 8.70 or later before it can be upgraded automatically. The installed Windows Agent must also have a lower major, minor or patch version than an active agent installer in Portal. For example, if Windows Agent 8.70.9513 is installed on a computer, the agent can be automatically upgraded by a version 8.71, 8.8x or 9.xx installer in Portal. The first digit of an agent version number represents the major version (e.g., 8 in 8.70.9513), the second digit represents the minor version (e.g., 7 in 8.70.9513) and the third digit represents the patch version (e.g., 0 in 8.70.9513).

An agent is not eligible for an automatic upgrade if it only has a lower build number than an active installer. For example, Windows Agent 8.81.0001 cannot be automatically upgraded by a version 8.81.9999 installer in Portal. The last four digits of an agent version number represent the build number (e.g., 9513 in 8.70.9513).

For an automatic upgrade to succeed, outbound port 443 must be open on the Windows server where the agent is installed.

*Note:* A Windows agent with the Cluster Plug-in cannot be upgraded automatically. You must upgrade agents with the Cluster Plug-in by running the installation kit.

For a description of how Windows agents are upgraded automatically, see [Automatic agent upgrade process](#).

### 9.1 Set up an agent installer location and permissions


Before Portal can provide installers for automatically upgrading agents on Windows computers, a Super user must specify:

- a UNC location for saving agent installers. We highly recommend specifying a UNC location that is not on the same server as Portal.
- a user that has read/write access to the UNC share. The Local System account on the machine that hosts the UNC share must have read/write access to the share.

A Super user can also specify whether Admin users can start agent upgrades on all eligible computers in their sites at the same time and whether agent installers can be signed by another company (e.g., a managed service provider).

To set up an agent installer location and permissions:

1. When signed in as a Super user, click **Global Settings** on the navigation bar.
2. Click the **Agent Upgrades** tab.

If a warning icon  appears on the Agent Upgrades tab, a UNC location for saving agent installers has not been specified and the Edit Agent Installer Location dialog box appears automatically.

3. If the Edit Agent Installer Location dialog box does not appear, click **Edit** in the Agent Installer Location box.

The Edit Agent Installer Location dialog box appears.

4. In the Edit Agent Installer Location dialog box, do the following:

- a. In the **Path to Network UNC Share** box, enter the path to a UNC location where you want to save Windows Agent installers. We highly recommend specifying a UNC share that is not on the same machine as Portal.

**IMPORTANT:** If a UNC location has already been specified and you enter a new one, any agent installers that have been uploaded to Portal remain in the UNC location but cannot be used for agent upgrades.

- b. In the **User Name** and **Password** boxes, enter credentials for connecting to the UNC share. The specified user must have read/write access to the UNC share.

You can enter the user name as *username* or *domain\username*. Do not enter the user name in the following format: *.\username*

The Local System account on the machine that hosts the UNC share must have read/write access to the share.

- c. Click **Save**.

5. Do one of the following:

- To allow Admin users to start agent upgrades on all eligible computers in their sites at the same time, turn on the **Allow admins to deploy automatic agent upgrades to their sites** toggle.
- To only allow Super users to start agent upgrades on all eligible computers in sites at the same time, turn off the **Allow admins to deploy automatic agent upgrades to their sites** toggle.

6. (Optional) To allow agent installers to be signed by another company (e.g., a managed service provider), select the **I acknowledge that this option is not recommended due to possible security risks** option and turn on the **Allow agent installers that are not signed by Carbonite** toggle.

## 9.2 Upload agent installers


After a UNC location for saving agent installers is specified, Super users can upload installers for automatically upgrading Windows agents. To be uploaded, an installer must be for a Windows agent version later than 8.70 and be signed with a valid certificate.

Installers are automatically activated (i.e., made available for upgrading agents) when you upload them. When an agent installer is activated in Portal, admin users receive a notification email.

If you upload an agent installer for the same platform (i.e., 64-bit) as an existing installer, Portal activates the newly-uploaded installer and deactivates the installer that was previously uploaded. Only one 64-bit agent installer can be active at one time. See [Activate, deactivate or delete an agent installer](#).

To upload an agent installer:

1. When signed in as a Super user, click **Global Settings** on the navigation bar.
2. Click the **Agent Upgrades** tab.

If a warning icon  appears on the Agent Upgrades tab, a UNC location for saving agent installers has not been specified. You must specify a UNC location before you can upload installers. See [Set up an agent installer location and permissions](#).

If a UNC location for saving agent installers has been specified, the Agent Upgrades tab appears.

3. Click **Upload a new agent installer**.

The Upload a New Agent Installer dialog box appears.

4. In the Agent Installer Name box, enter a name to use in Portal for the agent installer.
5. Click **Select agent installer**.
6. In the Choose File to Upload dialog box, navigate to the agent installer that you want to upload. Select the installer and then click **Open**.

The agent installer file name appears in the dialog box.

7. Click **Verify & Continue**.

The Upload a New Agent Installer dialog box shows agent installer information.

8. Confirm that the agent installer information is correct and then click **Upload & Activate**.

After the installer is uploaded, it appears in the agent installer list on the Agent Upgrades tab.

## 9.3 Activate, deactivate or delete an agent installer

To be available for automatic agent upgrades, a Windows agent installer in Portal must be “active”.

Installers are automatically activated when you upload them. You can also activate an inactive installer. Admin users receive a notification email when an agent installer is activated in Portal.


To prevent an agent installer from being used for automatic upgrades, you can deactivate the installer (i.e., make it “inactive”).

Only one 64-bit Windows agent installer can be active at one time. If you activate a 64-bit installer when another 64-bit agent installer is active, Portal deactivates the installer that was previously active.

To permanently remove an agent installer from Portal, you can delete an inactive installer.

To activate, deactivate or delete an agent installer:

1. When signed in as a Super user, click **Global Settings** on the navigation bar.
2. Click the **Agent Upgrades** tab.

If a warning icon  appears on the Agent Upgrades tab, a UNC location for saving agent installers has not been specified. See [Set up an agent installer location and permissions](#).

The State column in the agent installer list indicates whether each installer is active or inactive.

3. Do one of the following:
  - To activate an inactive installer (i.e., make it available for automatic agent upgrades), select the check box for the installer and then click **Activate** in the **Actions** list. In the Confirm Activation message box, click **Confirm**.
  - To deactivate an active installer (i.e., prevent it from being used for automatic agent upgrades), select the check box for the installer and then click **Deactivate** in the **Actions** list.
  - To permanently remove an inactive installer from Portal, select the check box for the installer and then click **Delete** in the **Actions** list. In the Confirm Deletion dialog box, click **Confirm**.

You cannot delete an active agent installer from Portal.

## 9.4 Upgrade agents on eligible computers

Super users and, if allowed, Admin users can start the agent upgrade process on all eligible Windows computers in sites. See [Upgrade agents on all eligible computers in sites](#). Super users specify whether Admin users can start agent upgrades on all eligible computers in their sites. See [Set up an agent installer location and permissions](#).

Admin users can also start agent upgrades on specific computers in their sites and view the agent upgrade status of each computer. See [Upgrade agents on specific computers](#).

To be eligible for an automatic upgrade, a computer must have Windows Agent version 8.70 or later installed. If a previous Windows Agent version is installed, the agent must be manually upgraded to version 8.70 or later before it can be upgraded automatically. The installed Windows Agent must also have a lower major, minor or patch version than an active agent installer in Portal. For example, if Windows Agent 8.70.9513 is installed on a computer, the agent can be automatically upgraded by a version 8.71, 8.8x or 9.xx installer in Portal. The first digit of an agent version number represents the major version (e.g., 8 in

8.70.9513), the second digit represents the minor version (e.g., 7 in 8.70.9513) and the third digit represents the patch version (e.g., 0 in 8.70.9513).

An agent is not eligible for an automatic upgrade if it only has a lower build number than an active installer. For example, Windows Agent 8.81.0001 cannot be automatically upgraded by a version 8.81.9999 installer in Portal. The last four digits of an agent version number represent the build number (e.g., 9513 in 8.70.9513).

*Note:* A Windows agent with the Cluster Plug-in cannot be upgraded automatically. You must upgrade Agents with the Cluster Plug-in by running the installation kit.

### 9.4.1 Upgrade agents on all eligible computers in sites

Super users and, if allowed, Admin users can start the agent upgrade process on all eligible Windows computers in sites.

Super users specify whether Admin users can start agent upgrades on all eligible computers in their sites at the same time. See [Set up an agent installer location and permissions](#).

To upgrade agents on all eligible computers in sites:

1. When signed in as a Super user or as an Admin user who can start agent upgrades, click **Agent Upgrade Center** on the navigation bar.

The Agent Upgrade Center shows active agent installers in Portal.

*Note:* Only “active” agent installers are available for automatic agent upgrades. See [Activate, deactivate or delete an agent installer](#).

2. In the Available Agents list, select an agent installer for upgrading agents.

The Agent Upgrade Center lists sites and indicates how many agents in each site are eligible for upgrade to the selected agent version. If a site is a parent site, a parent site icon (🏠) appears beside the site name. The “Agents Eligible” count includes both online and offline agents but agents cannot be upgraded until they are online.

3. Select the check box for each site where you want to start the agent upgrade process on eligible computers.
4. Click **Auto upgrade selected sites**.

The Upgrade Agents in Selected Sites dialog box appears.

5. Do one of the following:

- To start the upgrade process when agent systems are idle and contact Portal, select **Upgrade automatically (recommended)**.
- To send a message to online agents to start the upgrade process, select **Start upgrades now**.


*Note:* The Start Upgrades Now upgrade method is not recommended because it could affect Portal performance.

Offline agents will not be upgraded until they come online.

6. Click **Upgrade agents**.

A blue check mark (✓) appears beside each site where agent upgrade processes are starting using the **Upgrade automatically (recommended)** or **Start upgrades now** option. An Auto label ( Auto ) also appears beside each site where agent upgrades are starting using the **Upgrade automatically (recommended)** option.

After an agent has been upgraded in a site, the agent is removed from the Agents Eligible count and added to the Agents Upgraded count. If an error occurs during an agent upgrade, the agent is added to the Errors count for the site. To determine which agents have been upgraded or have upgrade errors, Admin users can view agent upgrade statuses on the Computers page. See [Upgrade agents on specific computers](#).

If an agent requires a reboot after an upgrade, a notification email is sent to Super users and to the site’s Admin users. The agent’s upgrade status is  (Reboot required) on the Computers page.

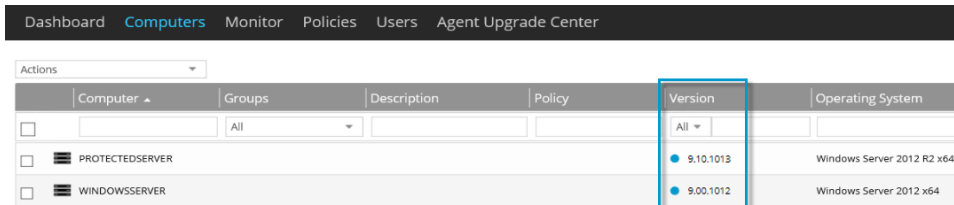
### 9.4.2 Upgrade agents on specific computers

Admin users can start the agent upgrade process on specific eligible Windows computers in their sites.



To upgrade agents on specific computers:

1. When signed in as an Admin user, click **Computers** on the navigation bar.



The Computers page shows registered computers. Icons in the Version column show each computer’s agent upgrade status. You can use a filter in the Version column to view computers with a particular upgrade status.





You can upgrade agents on computers with the following agent upgrade statuses:

-  Upgrade available — Indicates that the agent can be upgraded by an agent installer in Portal. Beginning in Portal 9.30, this status only appears for a computer if its operating system is supported with the new agent version.
-  Pending upgrade — Indicates that the agent can be upgraded by an agent installer in Portal and automatic upgrades have started for agents in the computer’s site. You can start the upgrade or wait for it to begin automatically.

Other possible agent upgrade statuses are:

-  Up to date — Indicates that the agent version is up-to-date and does not need to be upgraded by an installer in Portal.
-  Upgrade in progress — Indicates that an agent upgrade is in progress on the computer.




-  Upgrade error — Indicates that your action is required because an agent upgrade error occurred on the computer. You can check the agent logs for more information.
-  Reboot required — Indicates that the agent has been upgraded successfully but the computer needs to be restarted.

*Note:* An agent upgrade status icon does not appear for Windows Agent versions earlier than 8.70. These agents must be manually upgraded to version 8.70 or later before they can be upgraded automatically.

2. Select the check box for each eligible computer where you want to upgrade the agent.
3. In the **Actions** list, click **Upgrade Agent on Selected Computer(s)**. This action is only available if each selected computer has the Upgrade available status.

A Success dialog box indicates that the agent upgrade process has started.

4. Click **Okay**.

The agent upgrade status icon for each agent that is being upgraded is  (Upgrade in Progress). After an agent is upgraded, the agent status icon changes to  (Up to date). If an agent requires a reboot after an upgrade, the agent's upgrade status is  (Reboot required) and a notification email is sent to Super users and the site's Admin users.

## 9.5 Automatic agent upgrade process

When automatic agent upgrades are set up as described in [Manage Windows agent upgrades](#), an agent upgrade process begins when a Windows Agent version 8.70 or later:

- Finds an upgrade for computers in its site. This occurs when the Upgrade Automatically upgrade method is selected for a site, as described in [Upgrade agents on all eligible computers in sites](#). Windows agents check for upgrades once every 24 hours.
- Receives a message that it should start an upgrade. This can occur when:
  - The Start Upgrades Now upgrade method is selected for a site, as described in [Upgrade agents on all eligible computers in sites](#).
  - Agents are upgraded on specific computers, as described in [Upgrade agents on specific computers](#).

When an agent upgrade process starts, the agent checks whether:

- A reboot is required on the system. If a reboot is required, the agent upgrade will not proceed until the server has been restarted.
- A backup or restore is running. If a backup or restore is running, the agent upgrade will not proceed. The agent will check for running backups and restores once each hour, 11 more times. If a backup or restore is running each time, the agent waits for 24 hours and then tries the upgrade process again.

- The CPU usage on the system is high. This check is only performed if the agent found the upgrade for computers in its site. If the CPU usage is high in this case, the agent upgrade will not proceed. The agent will check the CPU usage once each hour, 11 more times. If the CPU usage is high each time, the agent waits for 24 hours and then tries the upgrade process again.

*Note:* If the agent received a message to start the upgrade, the upgrade will proceed even if the CPU usage is high.

If these conditions are met, the agent downloads and verifies the agent installer and starts the upgrade.

If an agent requires a reboot after an upgrade, a notification email is sent to Super users and to the site's Admin users. The agent's upgrade status on the Computers page is Reboot Required. Until the agent is rebooted, the agent will try to run backups and restores but these processes may not succeed.



## 10 Set up features and automatic emails

Super users can enable, disable and set up the following features using the Portal UI:

- [Enable data deletion](#)
- [Disable data archiving](#)
- [Enter email settings](#)
- [Set up two-factor account verification](#)

### 10.1 Enable data deletion

When deleting a job or computer from Server Backup Portal, an Admin user can request that backup data for the job or computer be deleted from all vaults. If the data deletion request is not canceled during a 72-hour waiting period, the deletion request is sent to vaults through API – Monitoring. In response to the request, the data is deleted from any standalone, Base or Active vault where the data is stored. Replication processes then delete the data from any associated Satellite or Passive vault.

If a deletion request fails, an email notification is sent to a vault administrator whose email address is specified in Portal. The vault administrator can then manually delete the data.

Using the following procedure, a Super user can enable data deletion functionality in Portal. In addition, Portal must be registered to the same API – Monitoring instance as vaults. Email notifications and machine keys must also be configured in the Portal instance. For more information, see the *Portal Installation and Configuration Guide*.

To enable data deletion:

1. When signed in as a Super user, click **Global Settings** on the navigation bar.
2. Click the **API Settings** tab.
3. In the Registration Service Settings area, enter values in the following boxes:
  - **Registration URL** — Enter the Registration URL from the last page of the API installation wizard.
  - **Registration Client ID** — Enter the Client ID value from the last page of the API installation wizard.
  - **Registration Secret** — Enter the Client Secret value from the last page of the API installation wizard (e.g., fnrGRhIYTgZ8CGOFcH+qAfpCroV2g6+UDoIPaUDlycqr).

*Note:* To obtain the Registration URL, Client ID and Secret values, contact the system administrator who installed API – Monitoring.
4. Click **Save**.

Portal registers to API – Monitoring and a message states that Registration Service Settings are saved.

5. Click **Okay**.

API registration information appears in the Messaging and Monitoring boxes.

6. Click the **Settings** tab and then click the **Product Settings** tab.

7. In the Data Deletion area, select the **Enable** check box.

Beginning in Portal 9.30, the **Enable** check box is only available if the Portal instance is registered to API – Monitoring.

8. In the **Vault Admin Email Address** box, enter the email address for a vault administrator or distribution list.

Notifications are sent to this email address if a data deletion request cannot be completed. A vault administrator can then delete the data manually.

9. Click **Save**.

A message states that the settings have been saved successfully.

## 10.2 Disable data archiving

Super users can disable data archiving in Server Backup Portal if backup data will never be stored in archive storage.

When data archiving is disabled, the Archive Days setting is not available in retention types and the “Keep Archives for x days” setting does not appear in policy retention types.

To disable data archiving:

1. When signed in as a Super user, click **Global Settings** on the navigation bar.
2. Click the **Settings** tab and then click the **Product Settings** tab.
3. In the Data Archiving area, select **Disable**.
4. Click **Save**.

A message states that the settings have been saved successfully.

## 10.3 Enter email settings

Portal uses an SMTP server to send automatic emails, such as welcome emails and backup notifications, and emailed reports. Beginning in version 9.10, a Super user can:

- Enter SMTP server information and other email settings in the Portal UI. In previous versions, email settings were entered in Portal configuration files.
- Enable centrally-configured backup notifications using the Portal UI. In previous versions, centrally-configured backup notifications were enabled by running a script on the Portal database.

During an upgrade to version 9.10, email settings are moved from configuration files to the Portal database and appear in the Portal UI.

Portal can send some automatic emails using Amazon Web Services (AWS). However, we do not recommend using AWS to send Portal emails in most cases. Specialized knowledge is required for setting up AWS mail services and an SMTP server is still required, since Portal reports and some automatic emails cannot be sent using AWS. If you must use AWS to send Portal emails, see [AWS email requirements](#) for more information.

To enter email settings:

1. When signed in as a Super user, click **Global Settings** on the navigation bar.
2. Click the **Settings** tab and then click the **Email Options** tab.
3. In the SMTP Configuration area, enter values in the following boxes:
  - **SMTP Server** — Fully qualified domain name for your SMTP server (e.g., mail.yourdomain.com).
  - **Port** — Port that your SMTP server uses for sending emails (e.g., 587).
  - **From Email Address** — Email address that will appear as the From address in emailed reports and automatic emails.
  - **Username and Password** — If required, a username and password for authenticating with your SMTP server.
  - **SSL** — If your SMTP server port supports SSL encryption (e.g., port 587), select **On**. If your SMTP server port does not support encryption (e.g., port 25), select **Off**.
4. In the Email Notification area near the bottom of the page, do one of the following:
  - To enable centrally-configured backup notification emails, select the **Enable Backup Notification Emails** check box. To specify how often email notifications are sent from Portal, enter the number of minutes in the **Notification Interval (minutes)** box.  
  
If centrally-configured backup notifications are enabled, users can select the backup notifications they want to receive in their profile settings. Backup notifications can also be selected for child site email addresses.
  - To disable backup notification emails, clear the **Enable Backup Notification Emails** check box.
5. (Optional) To send some automatic emails using Amazon Web Services (AWS), enter values in the following boxes in the Amazon SES area:
  - **From Email Address** — Email address that will appear as the From address in automatic emails sent using AWS. This email address should be the one used to track email bounces and complaints.
  - **AWS Region** — AWS region for the Simple Queue Service (SQS) (e.g., us-east-1).
  - **AWS Access Key** — AWS API access key ID for an IAM user with the required permissions.
  - **AWS Secret Key** — AWS secret access key for an IAM user with the required permissions.

- **Amazon SQS Bounce Queue URL** — SQS queue for bounced emails.
- **Amazon SQS Complaints Queue URL** — SQS queue for complaint emails.

*Note:* We do not recommend using AWS to send Portal emails in most cases. Specialized knowledge is required for setting up AWS email systems and an SMTP server is still required, since Portal reports and some automatic emails cannot be sent using AWS. If you must use AWS to send Portal emails, see [AWS email requirements](#) for more information.

6. Click **Save**.

### 10.3.1 AWS email requirements

Portal can send some automatic emails using Amazon Web Services (AWS). To send automatic Portal emails using AWS, you must set up the following:

- [An Identity and Access Management \(IAM\) user](#)
- [Simple Email Service](#)
- [Simple Queue Service](#)
- [Simple Notification Service](#)
- [\(Optional\) Simple Storage Service](#)

After these requirements are set up in AWS, you can enter required information in the Portal UI. See [Enter email settings](#).

*Note:* We do not recommend using AWS to send Portal emails in most cases. Specialized knowledge is required for setting up email systems in AWS and an SMTP server is still required, since Portal reports and some automatic emails cannot be sent using AWS.

#### **An Identity and Access Management (IAM) user**

An IAM user with the following permissions is required for sending Portal emails using AWS:

- Send Message
- Receive Message
- Delete Message
- List Queues

The IAM user's permissions should be limited to the actions and resources required for a functional email system.

The user can have API access only (i.e., with no console access). An AWS API access key must be generated for the user.

#### **Required IAM user permissions**

```
{  
  "Action": [  
    "sqs:DeleteMessage",  
    "sqs:ListQueues",
```

```
"sqs:ReceiveMessage",
"sqs:SendMessage"
],
"Resource": "arn:aws:sqs:{region}:{accountNumber}:environmentName",
"Effect": "Allow"
}
```

### Simple Email Service

The Simple Email Service (SES) sends emails and collects email bounces and complaints and routes them to a Simple Notification Service (SNS) topic.

New SES accounts are placed in an Amazon SES sandbox where sending limits and restrictions apply. Before granting full access to Amazon SES, Amazon requires customers to prove that they can handle email bounces and complaints. Once your email system is completely configured, you must submit a request to move your SES account out of the sandbox.

For the purpose of setting up email notifications:

- An email address must be verified in SES. You can verify one email address, or verify an entire domain so you have many email addresses to use. If you have more than one verified identity, make note of the one used to track bounces and complaints.
- A verified email address must be configured to receive feedback notifications for bounces and complaints, and point to Simple Notification Service (SNS) topics configured in [Simple Notification Service](#). Use this email address as the "From Email Address" for Amazon email settings in Portal. See [Enter email settings](#).
- Email feedback forwarding must be disabled in Amazon SES.

You can also set up a configuration ruleset in SES to track events like failures and rejects, and route them to another SNS topic (i.e., not the bounce and complaint SNS topics). For example, you could route errors to an S3 bucket that collects all tracked events for troubleshooting.

### Simple Queue Service

The Simple Queue Service (SQS) handles cases where emails should no longer be sent to email addresses because:

- Email sending fails and the recipient server sends back a bounce response.
- A recipient flags an email as spam and the email service provider of the recipient responds with a complaint.

An SQS queue must be created for bounced emails (e.g., email-bounce-queue) and complaint emails (e.g., email-complaint-queue).

### Simple Notification Service

The Simple Notification Service (SNS) is required to receive bounces and complaint messages from SES and route them to an SQS queue. SNS must have a topic with a subscription to the relevant SQS queue (e.g., email-bounce-topic with a subscription to email-bounce-queue).

No permissions are required for this service.

### (Optional) Simple Storage Service

An S3 bucket is useful if you want to set up an email rule that routes bounced emails to the S3 bucket. This can be useful when troubleshooting service errors.

## 10.4 Set up two-factor account verification

When two-factor account verification is set up in Portal, each user is prompted to provide a phone number for receiving account verification codes. Users who provide a phone number are then prompted to enter a code periodically when they sign in to Portal and when they reset their passwords.

Beginning in Portal 9.10, a Super user can set up two-factor account verification by entering settings in the Portal UI. In previous Portal versions, account verification settings were entered in Portal configuration files. If you upgrade a Portal instance to version 9.10, account verification settings are moved from configuration files to the Portal database and appear in the Portal UI.

Before you set up two-factor account verification in Portal, you must sign up for services from one of the following providers:

- Twilio (<https://www.twilio.com/>). Sign up for Verify from Twilio. You must also ensure that the following URLs can be reached on port 443 from the system(s) where the Portal UI is installed: <https://verify.twilio.com> and <https://lookups.twilio.com>
- TeleSign (<https://www.telesign.com/>). Sign up for the SMS Verify and Voice Verify products from TeleSign. You must also ensure that the following URL can be reached on port 443 from the system(s) where the Portal UI is installed: <https://rest-ww.telesign.com>

*Note:* Support for two-factor account verification with Twilio was added in Portal 9.10. In previous Portal versions, account verification was only supported with TeleSign.

Users in a Portal instance can be required to set up two-factor account verification. When two-factor account verification is required, a **Skip this step** option does not appear on the Portal page for setting up two-factor account verification. For more information, see the *Portal Installation and Configuration Guide*.

To set up two-factor account verification:

1. When signed in as a Super user, click **Global Settings** on the navigation bar.
2. Click the **Settings** tab and then click the **Third Party MFA/2FA** tab.
3. Do one of the following:
  - If you signed up for Verify from Twilio, do the following in the Twilio Multi-Factor Authentication area:
    - a. Select the **Turn on Twilio MFA** check box.
    - b. Enter values in the following boxes:
      - **Verification Service ID** — Your Twilio Verify Service SID.
      - **Authentication Token** — Your Twilio Auth Token.

- **Account SID** — Your Twilio Account SID.

You can obtain these values from the Twilio console.

- c. In the **MFA Expiration in Days** box, enter the number of days after which a user must enter a verification code again when signing in from a trusted web browser. A web browser is trusted if the user has selected the **Remember me on this device** check box when signing in from the browser.

The MFA Expiration in Days value can range from 0 to 90. If the value is 0, users must verify their accounts every time they sign in to Portal. Users must also verify their accounts every time they sign in to Portal from web browsers that are not trusted.

*Note:* You must also ensure that the following URLs can be reached on port 443 from the system(s) where the Portal UI is installed: <https://verify.twilio.com> and <https://lookups.twilio.com>

- If you signed up for SMS Verify and Voice Verify from TeleSign, do the following in the TeleSign Multi-Factor Authentication area:

- a. Select the **Turn on Telesign MFA** check box.
- b. Enter values in the following boxes:

- **Customer ID** — Your TeleSign Customer ID.
- **Secret Key** — Your TeleSign API Key.

You can obtain these values from the TeleSign portal.

- c. In the **MFA Expiration in Days** box, enter the number of days after which a user must enter a verification code again when signing in from a trusted web browser. A web browser is trusted if the user has selected the **Remember me on this device** check box when signing in from the browser.

The MFA Expiration in Days value can range from 0 to 90. If the value is 0, users must verify their accounts every time they sign in to Portal. Users must also verify their accounts every time they sign in to Portal from web browsers that are not trusted.

*Note:* You must also ensure that the following URL can be reached on port 443 from the system(s) where the Portal UI is installed: <https://rest-ww.telesign.com>

4. Click **Save**.

5. Do the following to verify the MFA Settings that you entered:

- a. In the Test MFA Settings dialog box, in the **Phone Number** box, enter a phone number (including the country code) where you can receive an account verification code. If you do not know the country code, click the X in the **Phone Number** box and select the country.
- b. Click **Send Code**.
- c. Check your phone for an account verification code.

If you do not receive a code, check that the phone number you entered is correct. If the phone number is incorrect, enter a new phone number and click **Send Code**.

- d. Enter the code in the **Code** box. Click **Verify**.

If a message states that the MFA configuration has been saved and enabled, two-factor account verification is now set up. Click **Finish**.

If a message states that the code could not be verified, do the following:

- Enter the account verification code again. Click **Verify**.
- Click **Cancel** and check your Telesign or Twilio information. If the information is not correct, repeat steps [Step 3](#) to [Step 5](#).

If the code still cannot be verified, the two-factor account verification service might be temporarily available. Please try to set up two-factor account verification again later. If the problem persists, please contact Support for assistance.



## 11 Set up agent auto-configuration

Beginning with Portal 8.89 and Windows Agent 8.90a, backups on Windows servers can be configured automatically based on job templates. When agent auto-configuration is set up in Portal, you do not have to manually select a vault account and create a backup job and schedule for each Windows server.

To set up agent auto-configuration:

- Super users create job templates that are available for all child sites in Portal. A job template specifies the name and type of job (Image or Local System) to create, the data to back up, whether to retry failed backups, and schedules for running the job. See [Create job templates](#).
- Parent site admin users enable agent auto-configuration in child sites that they manage, and select job templates and vault profiles for configuring new agents that register to the sites. Parent site admin users can also customize job templates for their child sites. See [Enable agent auto-configuration in child sites](#) and [Create and edit custom job templates](#).

*Note:* Agent auto-configuration cannot be enabled in parent sites.

You can then install Windows agents with default encryption passwords, and register the agents to Portal child sites where agent auto-configuration is enabled. Agent auto-configuration must be enabled in the site when an agent first registers to Portal. An agent will not be automatically configured if you enable this feature after the agent is registered to Portal.

Every three minutes, Portal finds and auto-configures eligible Windows agents. When an agent is successfully configured, a backup job for the Windows server is created that has:

- The name, description, settings and schedules specified by the job template selected for the child site.
- A randomly-assigned time for running backups with “Days of Week” and “Days of Month” schedules. By default, the time is between 8 PM and 8 AM, but a different time window might be specified in your Portal instance.
- The vault profile selected for the child site.
- The data encryption password specified when the agent was installed.

To determine whether an agent has been configured automatically, you can view the agent on the Computers page in Portal. If the agent has been configured, a backup job appears. If the agent has not been configured, an auto-configuration status message appears.

*Note:* In Portal instances and sites where agent auto-configuration is not available, agents can be configured when you click the "Configure Automatically" button, but the resulting jobs cannot be customized using job templates.

### 11.1 Create job templates

Super users can create job templates for automatically configuring backups on Windows servers. Job templates specify the name and type of job (Image or Local System) to create, the data to back up, whether

to retry failed backups, and schedules for running the job.

Super users can also edit and delete job templates. See [Edit job templates](#) and [Delete job templates](#).

After a Super user creates at least one job template, Parent site admin users can enable agent auto-configuration in child sites that they manage. Parent site admin users can also customize job templates for their child sites. See [Enable agent auto-configuration in child sites](#) and [Create and edit custom job templates](#).

To create a job template:


1. When signed in as a Super user, click **Global Settings** on the navigation bar.
2. Click the **Job Templates** tab.
3. In the **Actions** list, click **Create Job Template**.

The Create New Job Template dialog box appears.

Retention	Schedule	Compression	Deferring (0 for none)	Priority
Daily	Su,Mo,Tu,We,Th,Fr,Sa	Smaller	0	None

4. In the **Select Job Type** list, do one of the following:
  - To create a template for configuring Image backup jobs on Windows servers, select **Image**.
  - To create a template for configuring Local System backup jobs on Windows servers, select **Local System**.
5. In the **Job Name** box, type a name for the template. This name will be used for any job that is automatically configured using the template.
6. (Optional) In the **Job Description** box, type a description for the template. This description will be used for any job that is automatically configured using the template.
7. To back up all volumes on the system, including non-removable volumes that are added after the backup job is created, select the **Protect Entire Server** option.

The Bare Metal Restore option is automatically selected when you select the Protected Entire Server option. This ensures that a protected server can be restored using the System Restore application, if required.

8. To back up volumes that are needed to boot up the system after a system recovery, select the **Bare Metal Restore** option.
9. (Optional) If you are creating a template for Local System backup jobs, do one or both of the following until the Backup Set box shows the drives and folders that you want to include and exclude in the backup job:
  - To include specific folders or drives in the backups, enter the folder or drive name (e.g., C:\) in the **Enter Folders/Drives** box, and then click **Include**.  
*Note:* If the Protect Entire Server option is selected, you cannot include specific folders or drives.
  - To exclude specific folders or drives from the backups, enter the folder or drive name (e.g., D:\test) in the **Enter Folders/Drives** box, and then click **Exclude**.
  - To remove a row from the Backup Set box, click the Delete button  in the row.
10. Do one of the following:
  - To specify that scheduled backups should retry after failed backup attempts, select the **Retry failed job** option. In the **Number of retries** box, enter the number of times that the backup should try again. In the **Retry wait time in minutes** box, enter the number of minutes before each retry attempt.
  - To specify that scheduled backups should not retry after failed backup attempts, clear the **Retry failed job** check box.
11. In the Schedules pane, do the following:
  - In the **Retention** list, click a retention type.  
The retention type specifies the number of days a backup is kept on the vault, how many copies of a backup are stored online, and how long backup data is stored offline.
  - In the **Schedule** list, do one of the following:  
*Note:* You cannot create an intra-daily schedule in a job template.
    - To run the backup on specific days each week, select **Days of Week** in the **Schedule View** list. Select the days when you want to run the job.  
  
When an agent is auto-configured using this template, the backup will be scheduled at a randomly-assigned time on the selected days of the week. If multiple Days of Week and Days of Month schedules are specified in the template, they will each be scheduled at the same randomly-assigned time. By default, the time will be between 8 PM and 8 AM in the

time zone of the Windows server. A different time window might be specified in your Portal instance.

- To run the backup on specific dates each month, select **Days of Month** in the **Schedule View** list. On the calendar, select the dates when you want to run the job.

When an agent is auto-configured using this template, the backup will be scheduled at a randomly-assigned time on the selected days of the month. If multiple Days of Week and Days of Month schedules are specified in the template, they will each be scheduled at the same randomly-assigned time. By default, the time will be between 8 PM and 8 AM in the time zone of the Windows server. A different time window might be specified in your Portal instance.

- To create a custom schedule, select **Custom** in the **Schedule View** list. In the Custom Cycle dialog box, enter a custom schedule. Be sure to follow the format and notation as described.

When an agent is auto-configured using this template, the backup will be scheduled at the time specified in the custom schedule (not at a randomly-assigned time).


- In the **Compression** list, click a compression level for the backup data. Compression levels optimize the volume of data sent against the speed of processing.
- Do one of the following:
  - To allow the backup job to run without a time limit, click **None** in the **Deferring** list.
  - To specify a maximum amount of time that the backup job can run, click **Minutes** or **Hours** in the **Deferring** list. In the adjacent box, type the maximum number of minutes or hours that the job can run.

When deferring is used, the backup job does not back up any new data after the specified amount of time, even if some data is not backed up. Changes to data that was previously backed up will be backed up, regardless of the amount of time specified.

12. To add another schedule to the template, click **Add schedule** and then repeat [Step 11](#) for the new schedule row.

13. If there is more than one schedule row, use the **Priority** arrows to change the order of the schedule rows.

If the job is scheduled to start at exactly the same time by multiple schedules, the job only runs once at the scheduled time. If the jobs have different retention types, the retention type of the schedule that is highest in the list is applied to the resulting safeset.

14. To remove a schedule from the template, click the Delete button  in the schedule row.

15. Click **Create Job Template**.

### 11.1.1 Edit job templates

Super users can edit job templates for automatically configuring backups on Windows servers.

*Note:* Super users can edit "global" job templates which are created by Super users and available for all child sites in a Portal instance. Super users cannot edit "custom" job templates created by parent site Admin users.

To edit a job template:

1. When signed in to Portal as a Super user, click **Global Settings** on the navigation bar.
2. Click the Job Templates tab.  
The tab shows the current job templates.
3. Click the name of the template that you want to edit.  
The Update Existing Job Template dialog box shows the job template settings.
4. Change the template settings. For setting descriptions, see [Create job templates](#).
5. Click **Update Job Template**.

### 11.1.2 Delete job templates

Super users can delete job templates for automatically configuring backups on Windows servers.

*Note:* Super users can delete "global" job templates which are created by Super users and available for all child sites in a Portal instance. Super users cannot delete "custom" job templates created by parent site Admin users.

To delete a job template:

1. When signed in to Portal as a Super user, click **Global Settings** on the navigation bar.
2. Click the Job Templates tab.  
The tab shows the current Global job templates.
3. Select the check box for each job template that you want to delete.
4. In the **Actions** list, click **Delete Job Templates**.  
The Confirmation box lists the job templates to be deleted. An asterisk (\*) appears beside any templates that are used for automatically configuring backups in a child site.  
If you delete a template that is used for automatically configuring backups in a child site, auto-configuration will be disabled in the child site.
5. To delete the job templates, click **Delete**.

## 11.2 Enable agent auto-configuration in child sites

Parent site Admin users can enable agent auto-configuration in child sites that they manage. When agent auto-configuration is enabled in a child site, new Windows agents that are installed with default encryption

passwords and registered to the site are configured as specified by a selected job template and vault profile.

Before agent auto-configuration can be enabled in a child site:

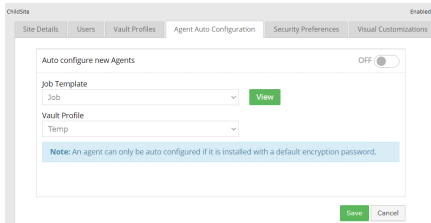
- At least one job template must be created in Portal. See [Create job templates](#).
- At least one vault profile must be available in the site. See [Add a vault profile for a site](#).

To enable agent auto-configuration in a child site:

1. When signed in to Portal as an Admin user who can manage child sites, click **Sites** on the navigation bar.
2. Find the child site for which you want to enable agent auto-configuration. Open the site record by clicking its row.

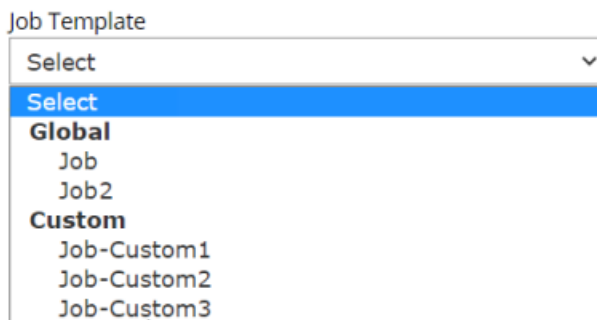
If you cannot open the site record, the **Allow admins to manage child sites** check box might not be selected in the parent site.

3. Click the Agent Auto Configuration tab for the site.



4. On the Agent Auto Configuration tab, turn on the **Auto configure new agents** toggle.
5. In the **Job Template** list, select a template for automatically-created backup jobs.

The Job Template list includes any global templates (created by a Super user) and custom templates (created by an Admin user for the parent site).



6. To view the selected template, click the **View** or **Edit** button.

The View button appears if the selected template is a global template that was created by a Super user. The Edit button appears if the selected template is a custom template that was created by a parent site Admin user.

To customize a template, see [Create and edit custom job templates](#).

7. In the **Vault Profile** list, select the vault profile for automatically creating backup jobs in the site.
8. Click **Save**.

### 11.2.1 Disable agent auto-configuration in child sites

Parent site admin users can disable agent auto-configuration in child sites that they manage.

To disable agent auto-configuration in a child site:

1. When signed in to Portal as an Admin user who can manage child sites, click **Sites** on the navigation bar.
2. Find the child site for which you want to disable agent auto-configuration. Open the site record by clicking its row.

If you cannot open the site record, the **Allow admins to manage child sites** check box might not be selected in the parent site.

3. Click the Agent Auto Configuration tab for the site.
4. On the Agent Auto Configuration tab, turn off the **Auto configure new agents** toggle.

*Note:* You do not have to remove selections from the Job Template and Vault Profile lists. These values can remain in case you want to re-enable agent auto-configuration later.

5. Click **Save**.

## 11.3 Create and edit custom job templates

Admin users in parent sites can create and edit custom job templates for automatically configuring agents in child sites that they manage.

Before a parent site Admin user can create a custom job template, at least one global job template must be created in Portal. Global job templates are created by Super users and are available for all sites in a Portal instance. See [Create job templates](#).

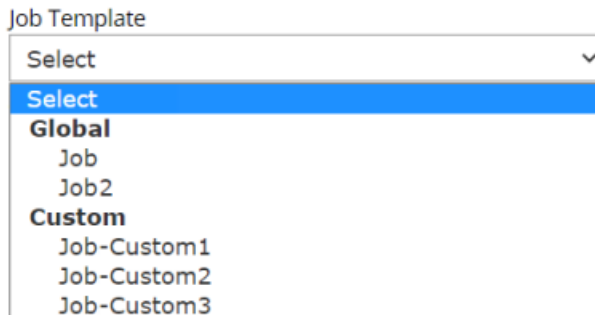
To create or edit a custom job template:

1. When signed in to Portal as an Admin user who can manage child sites, click **Sites** on the navigation bar.
2. Open a child site record by clicking its row.

*Note:* If you cannot open the site record, the **Allow admins to manage child sites** check box might not be selected in the parent site.

3. Click the **Agent Auto Configuration** tab for the site. See [Enable agent auto-configuration in child sites](#).
4. Click the **Job Template** list.

The Job Template list includes any global templates (available for all Portal child sites) and custom templates (available for child sites in the parent site).



5. Do one of the following:
  - To create a custom job template based on a Global template, select the Global template in the **Job Template** list, and then click **View**. The job template appears. Click **Create a Copy (Editable)**. An editable copy of the template appears.
  - To edit a custom job template, select the custom template in the **Job Template** list and then click **Edit**. The editable template appears.
  - To create a custom job template based on an existing custom template, select a custom template in the **Job Template** list and then click **Edit**. An editable copy of the template appears.
6. In the **Select Job Type** list, do one of the following:
  - To create a template for configuring Image backup jobs on Windows servers, select **Image**.
  - To create a template for configuring Local System backup jobs on Windows servers, select **Local System**.
7. In the **Job Name** box, type a name for the template. This name will be used for any job that is automatically configured using the template.
8. (Optional) In the **Job Description** box, type a description for the template. This description will be used for any job that is automatically configured using the template.
9. To back up all volumes on the system, including non-removable volumes that are added after the backup job is created, select the **Protect Entire Server** option.
 


The Bare Metal Restore option is automatically selected when you select the Protect Entire Server option. This ensures that a protected server can be restored using the System Restore application, if required.
10. To back up volumes that are needed to boot up the system after a system recovery, select the **Bare Metal Restore** option.



11. (Optional) If you are creating a template for Local System backup jobs, do one or more of the following until the Backup Set box shows the drives and folders that you want to include and exclude in the backup job:

- To include specific folders or drives in the backups, enter the folder or drive name (e.g., C:\) in the **Enter Folders/Drives** box, and then click **Include**.

*Note:* If the Protect Entire Server option is selected, you cannot include specific folders or drives.

- To exclude specific folders or drives from the backups, enter the folder or drive name (e.g., D:\test) in the **Enter Folders/Drives** box, and then click **Exclude**.
- To remove a row from the Backup Set box, click the Delete button  in the row.

12. Do one of the following:

- To specify that scheduled backups should retry after failed backup attempts, select the **Retry failed backup** option. In the **Number of retries** box, enter the number of times that the backup should try again. In the **Retry wait time in minutes** box, enter the number of minutes before each retry attempt.
- To specify that scheduled backups should not retry after failed backup attempts, clear the **Retry failed backup** check box.

13. In the Schedules pane, do the following:

- In the **Retention** list, click a retention type.

The retention type specifies the number of days a backup is kept on the vault, how many copies of a backup are stored online, and how long backup data is stored offline.

- In the **Schedule** list, do one of the following:

*Note:* You cannot create an intra-daily schedule in a job template.

- To run the backup on specific days each week, select **Days of Week** in the **Schedule View** list. Select the days when you want to run the job.

When an agent is auto-configured using this template, the backup will be scheduled at a randomly-assigned time on the selected days of the week. If multiple Days of Week and Days of Month schedules are specified in the template, they will each be scheduled at the same randomly-assigned time. By default, the time will be between 8 PM and 8 AM in the time zone of the Windows server. A different time window might be specified in your Portal instance.

- To run the backup on specific dates each month, select **Days of Month** in the **Schedule View** list. On the calendar, select the dates when you want to run the job.

When an agent is auto-configured using this template, the backup will be scheduled at a randomly-assigned time on the selected days of the month. If multiple Days of Week and Days of Month schedules are specified in the template, they will each be scheduled at the

same randomly-assigned time. By default, the time will be between 8 PM and 8 AM in the time zone of the Windows server. A different time window might be specified in your Portal instance.

- To create a custom schedule, select **Custom** in the **Schedule View** list. In the Custom Cycle dialog box, enter a custom schedule. Be sure to follow the format and notation as described.


When an agent is auto-configured using this template, the backup will be scheduled at the time specified in the custom schedule (not at a randomly-assigned time).

- In the **Compression** list, click a compression level for the backup data. Compression levels optimize the volume of data sent against the speed of processing.
- Do one of the following:
  - To allow the backup job to run without a time limit, click **None** in the **Deferring** list.
  - To specify a maximum amount of time that the backup job can run, click **Minutes** or **Hours** in the **Deferring** list. In the adjacent box, type the maximum number of minutes or hours that the job can run.

When deferring is used, the backup job does not back up any new data after the specified amount of time, even if some data is not backed up. Changes to data that was previously backed up will be backed up, regardless of the amount of time specified.

14. To add another schedule to the template, click **Add schedule** and then repeat [Step 11](#) for the new schedule row.
15. If there is more than one schedule row, use the **Priority** arrows to change the order of the schedule rows.

If the job is scheduled to start at exactly the same time by multiple schedules, the job only runs once at the scheduled time. If the jobs have different retention types, the retention type of the schedule that is highest in the list is applied to the resulting safeset.

16. To remove a schedule from the template, click the Delete button  in the schedule row.
17. Click **Save**.

## 12 View information about the Portal instance

Super users can view information about a Server Backup Portal instance, including:

- The status of Portal components such as the Redirector and Proxies. For more information about these components, see the *Portal Installation and Configuration Guide*.
- The number of sites, users, agents and jobs in the instance.

To view information for the Portal instance, when signed in as a Super user, click **Usage Metrics** on the navigation bar.

The Usage Metrics page shows information about Portal components, sites, users and agents.

The screenshot displays the Usage Metrics page. On the left, under 'Infrastructure Utilization', there are two tables. The first table, 'Redirector', shows one entry for 'PORTALPROD' with host 'portalprod', IP 'fe80::1d7a:a689:88a6:5297%13', port '8086', last update '3/4/2015 4:48 PM', and status 'Online'. The second table, 'Proxies', shows one entry for 'PORTALPROD' with host '192.168.0.168', IP '192.168.0.168', port '8087', '# of Agents connected' '126', last update '3/4/2015 4:49 PM', and status 'Online'. Below these tables are summary statistics: 'Number of active proxies: 1', 'Number of connected agents: 2477 (125 online)', 'Average number of connected agents per proxy: 2477 (125 online)', and 'Number of jobs across all agents: 3081'. On the right, the 'Entity Count' section shows 'Number of companies: 18' and 'Number of users: 114'.

Infrastructure Utilization						
Redirector						
Name	Host	IP	Port	Last Update	Status	
PORTALPROD	portalprod	fe80::1d7a:a689:88a6:5297%13	8086	3/4/2015 4:48 PM	Online	

Proxies						
Name	Host	IP	Port	# of Agents connected	Last Update	Status
PORTALPROD	192.168.0.168	192.168.0.168	8087	126	3/4/2015 4:49 PM	Online

Number of active proxies:	1		
Number of connected agents:	2477 (125 online)	Average number of connected agents per proxy:	2477 (125 online)
Number of jobs across all agents:	3081		

Entity Count	
Number of companies:	18
Number of users:	114

## 13 View information as a Support user

Support users can view sites on a Support Dashboard in Server Backup Portal. This Dashboard lists every site in the Portal instance, and shows the number of Agents with failures, errors, missed backups and deferred backups in each site.

From the list of sites on the Support Dashboard, Support users can select a specific site for viewing computers, jobs, process logs, and reports.

Support users can view information for any site, but cannot add or change computers or jobs, or run backups and restores.

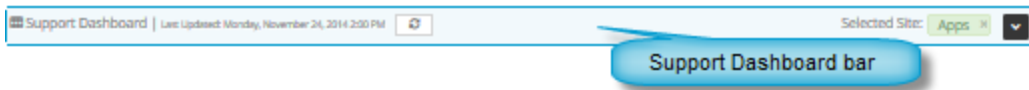
### 13.1 View sites on the Support Dashboard

Support users can view a Support Dashboard in Portal that lists every site in the Portal instance, lists the parent site of every child site, and shows the number of Agents with failures, errors, missed backups and deferred backups in each site.


From the list of sites, Support users can select a specific site for viewing computers, jobs, process logs, and reports.

To view sites on the Support Dashboard:

1. When signed in as a Support user, if a list of sites does not appear, click the Support Dashboard bar at the top of any page.



A list of sites appears. If a site is selected, the site name appears in the Selected Site box, and the site is highlighted in the Dashboard.

2. To change the order of sites, click the name of a column for determining the site order. To reverse the site order, click the column name again.
3. To filter the sites that appear, do one or both of the following:
  - In the **Site Name** box, enter text that site names must match.
  - In the **Parent Name** box, enter text that parent site names must match.
4. To refresh data, click the **Refresh dashboard** button. 
5. To select a site for viewing detailed information, click the **Select** button in the site row.

Information for the selected site appears on the page. To view more information for the site, navigate to another page in Portal.

## 13.2 Monitor events and computers as a Support user

On the Dashboard page in Portal, Support users can monitor events and computers in any site.

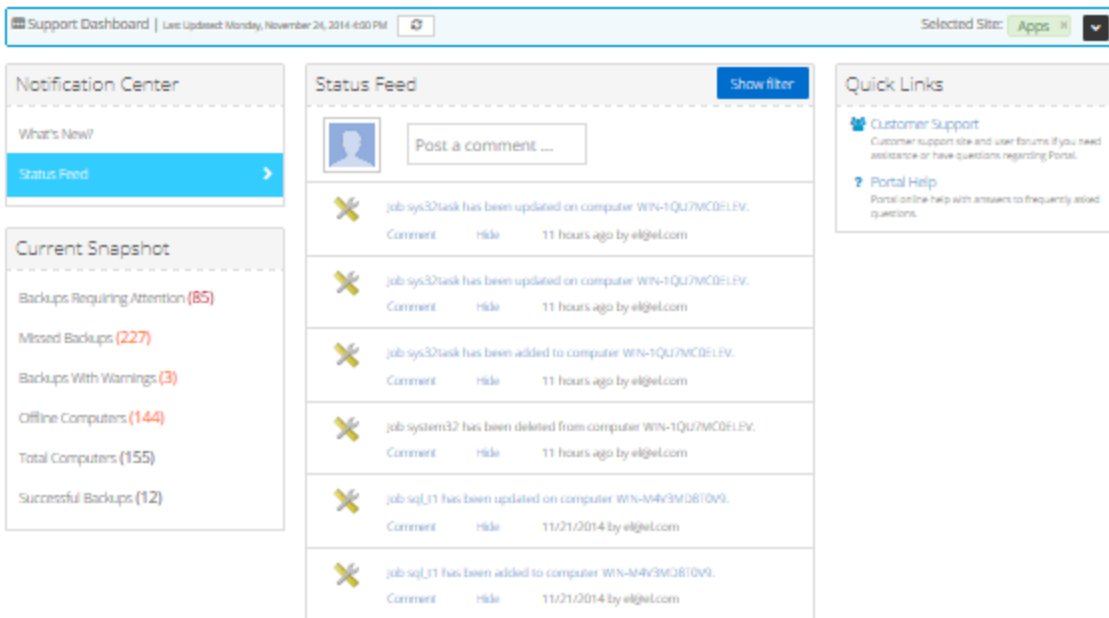
To monitor events and computers as a Support user:

1. When signed in as a Support user, click **Dashboard** on the navigation bar.

If a site is not selected, the Support Dashboard appears. Click **Select** in the row of the site for which you want to view information.

The Current Snapshot shows backup job and computer statistics for the site and any child sites. The site name appears in the **Selected Site** box.

2. To view notifications about recent events in the site, click **Status Feed**.



3. If a Site Usage chart appears, you can view the amount of data backed up for computers in the site in the current billing period compared to a specified usage checkpoint amount. If you are viewing a parent site, a separate Site Usage chart could appear for the parent site and any child sites where usage tracking is enabled.
4. To monitor events and computers in another site, click the Support Dashboard bar at the top of the page. The Support Dashboard appears. In the row of the site for which you want to monitor events and computers, click the **Select** button.

The page shows information for the selected site and any child sites.

### 13.3 View computers and jobs as a Support user

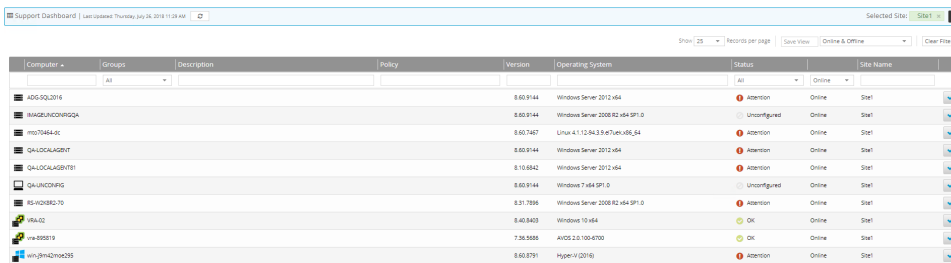
On the Computers page in Portal, Support users can view information about computers and jobs in any site. Support users cannot add or configure computers or jobs, or run backups and restores. They can only view computer and job information.

To view computers and jobs as a Support user:

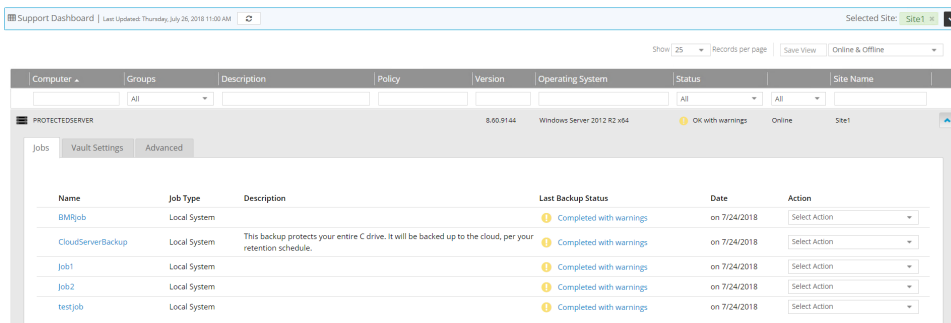
1. When signed in as a Support user, click **Computers** on the navigation bar.

If a site is not selected, the Support Dashboard appears. Click **Select** in the row of the site for which you want to view information.

The Computers page shows computers in the selected site and in any child sites. The site name appears in the **Selected Site** box.



2. To view information about a specific computer and its jobs, click the computer row to expand its view.



3. To view information about the computer’s jobs, do one or more of the following:
  - To view a job’s configuration, click the **Jobs** tab. In the **Select Action** menu for the job that you want to view, click **View Job**.
  - To view a job’s schedule, click the **Jobs** tab. In the **Select Action** menu for the job with the schedule that you want to view, click **View Schedule**.
  - To view process logs for a job, in the **Select Action** menu for the job, click **History/Logs**. The History / Logs window shows the log for the most recent process: backup, restore or synchronization.

4. To view the computer's vault information and credentials, click the **Vault Settings** tab. In the **Select Action** menu for the vault settings that you want to view, click **View Settings**.
5. To view advanced computer settings, click the **Advanced** tab. On the Advanced tab, view information on the **Options**, **Retention Types**, **Notifications**, **Performance**, and **Agent Log Files** tabs.
6. If you are viewing a vSphere environment, to view vSphere environment information, click the **vSphere Settings** tab.
7. If you are viewing a Hyper-V environment, to view Hyper-V environment information, do one or more of the following:
  - To view hosts in the environment, click the **Hosts** tab.
  - To view virtual machines (VMs) in the environment, click the **Virtual Machines** tab. The tab shows all VMs in the Hyper-V environment. To view VMs that have been backed up and can be restored, click **Protected Inventory**, in the Current Inventory/Protected Inventory filter list.
8. To view computers and jobs for another site, click the Support Dashboard bar at the top of the page. The Support Dashboard appears. In the row of the site for which you want to view computers and jobs, click the **Select** button.

The Computers page shows computers in the selected site and in any child sites.

## 13.4 View backup statuses as a Support user

On the Monitor page in Portal, Support users can view the last backup status for jobs in any site, and navigate to computer and job information and process logs.

To view backup statuses as a Support user:

1. When signed in as a Support user, click **Monitor** on the navigation bar.

If a site is selected, the site name appears in the **Selected Site** box.

If a site is not selected, the Support Dashboard appears. Click **Select** in the row of the site for which you want to view backup statuses.

The page shows backup jobs that are running or have run in the selected site and in any child sites.

Computer...	Job Nam...	Job Type	Last Backup Status	Last Backup Date	Skipped	Last Completed Backup	Backup Size
QA-AGENT-01	AJsvO_Ret...	Local System	Completed	yesterday at 8:00 PM		yesterday at 8:00 PM	224.00 Bytes
qa-hyper-	automation...	Hyper-V	Completed	today at 5:30 PM		today at 5:30 PM	776.23 MB
qa-hyper-g	automation...	Hyper-V	Completed	today at 5:45 PM		today at 5:45 PM	34.52 GB
qa-hyper-	automation...	Hyper-V	Completed	today at 5:45 PM		today at 5:45 PM	34.52 GB
qa-hyper-	automation...	Hyper-V	Completed	today at 5:10 PM		today at 5:10 PM	11.70 GB
qa-hyper-g	automation...	Hyper-V	Missed	on 3/2/2021		on 3/2/2021	11.70 GB
VRA-QA	BackupJob	vSphere	Completed	yesterday at 4:08 AM		yesterday at 4:08 AM	17.22 GB
WINDOW32B	BT-Backup2	Local System	Missed	on 3/26/2021		on 3/26/2021	13.76 MB
QA-AGENT-01	CloudServer...	Volume Image	Completed	yesterday at 11:48 PM		yesterday at 11:48 PM	28.59 GB
QA-WIN2019	CloudServer...	Local System	Completed	yesterday at 9:35 PM		yesterday at 9:35 PM	9.62 GB
QBACKUPNO1	CloudServer...	Local System	Completed	yesterday at 9:21 PM		yesterday at 9:21 PM	13.46 GB
QA-	CloudServer...	Local System	Missed	on 1/30/2021		on 1/30/2021	39.26 GB
WIN-	CloudServer...	Local System	Never Run				
QA-AGENT-01	cTuoO_Ret...	Local System	Completed	yesterday at 8:00 PM		yesterday at 8:00 PM	224.00 Bytes
QA-AGENT-01	DWYSu_Ret...	Unc File	Completed	yesterday at 11:30 PM		yesterday at 11:30 PM	175.00 Bytes

- To change the order of backup jobs on the page, click the name of the column for determining the sort order. To reverse the order of jobs, click the name of the column again.
- To change which jobs appear on the page, enter criteria that records must match. In the filter row under the column headings, in each column where you want to apply a filter, do one of the following:
  - In the empty box, type text that records must match.
  - In the list, click the value that records must match.

Records only appear on the page if they match all specified criteria.

- To view an online computer on the Computers page, click the computer name or job name. The Computers page shows information for the computer. For more information, see [View computers and jobs as a Support user](#).
- To view an online computer’s process logs in the History / Logs window, click the last backup status for the job.

### 13.5 View reports as a Support user

On the Reports page in Portal, Support users can view reports for any site and save customized report views. Support users can also schedule the Daily Status report to be emailed to users.

To view a report as a Support user:

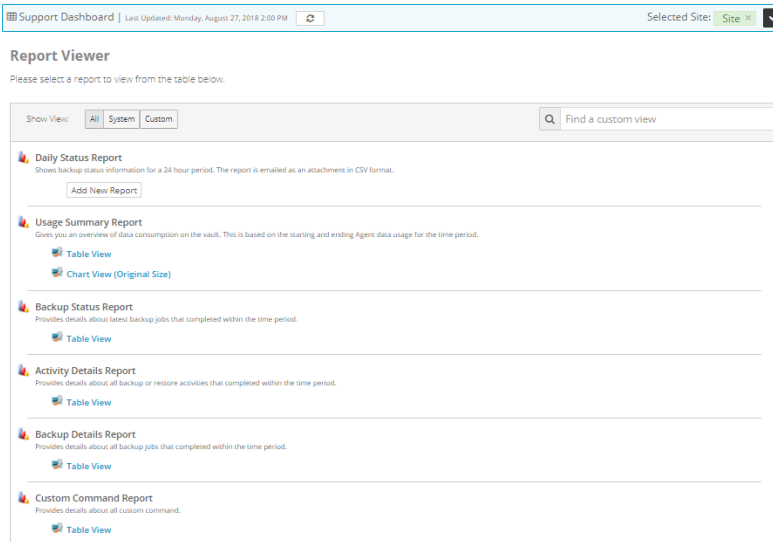
- When signed in as a Support user, click **Reports** on the navigation bar.

If a site is selected, the site name appears in the **Selected Site** box.

If a site is not selected, the Support Dashboard appears. Click **Select** in the row of the site for which you want to view reports.



The page lists available report views.



2. Do one of the following:

- To view another report, click a report view. You cannot click a report name (which appears in bold text). You can only click a report view.

Report data appears on the Reports page. If a scroll bar appears at the right side of the page, you can scroll down to see more records in the report.

## 14 Carbonite Server Backup Support

If you have a question about Carbonite Server Backup that isn't covered in this guide, our frequently-updated Knowledge Base contains comprehensive information. The Knowledge Base is your first stop when searching for any Carbonite Server Backup solutions you may need. We highly recommend searching here first for the quickest answers to your questions.

Knowledge Base: <http://support.carbonite.com/evault>

# What can we help you with?

Search

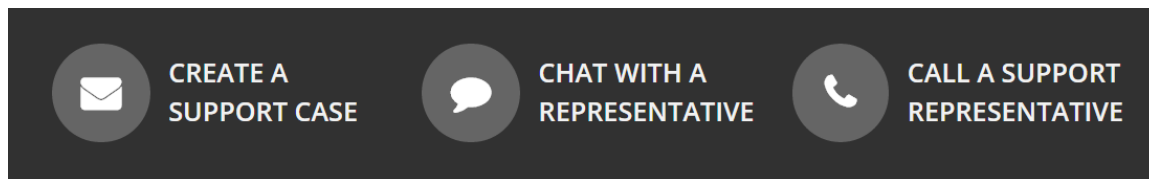
Popular Searches

[pending reboot](#), [restore](#), [clnt-e-04103](#)

### 14.1 Contacting Carbonite

If you need live assistance from a qualified support agent, Carbonite Support is here for you 24 hours a day, 7 days a week (excluding US holidays). Please feel free to get in touch with us, and we'll help out any way we can! You can find the contact information for Carbonite Support in the Knowledge Base:

<http://support.carbonite.com/evault>



*Tip:* When contacting Support with a technical issue, please have both the program's log files and the store you are having difficulty with ready.

Compress the program's log files in a .zip file and attach it to your support request.

If the log archive exceeds 10MB, you may not be able to send them as an email attachment. In that case, upload instructions will be provided to you upon request.