CARBONITE™

Carbonite Server Backup vSphere Recovery Agent 8.6

User Guide

© 2018 Carbonite, Inc. All rights reserved.

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, Inc.
Two Avenue de Lafayette
Boston, MA 02111
www.carbonite.com

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

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

“Part of the software embedded in this product is gSOAP software. Portions created by gSOAP are Copyright 2001-2006 Robert A. van Engelen, Genivia Inc. All Rights Reserved. THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY GENIVIA INC AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.”

The Carbonite Server Backup Agent, Carbonite Server Backup CentralControl, and Carbonite Server Backup Director applications have the encryption option of AES (Advanced Encryption Standard). Advanced Encryption Standard algorithm (named Rijndael, pronounced “Rain Doll”) was developed by cryptographers Dr. Joan Daemen and Dr. Vincent Rijmen. This algorithm was chosen by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce to be the new Federal Information Processing Standard (FIPS).

The Carbonite Server Backup Agents and Carbonite Server Backup Director applications also have the added security feature of an over the wire encryption method.

Document History

Version	Date	Description
1	March 2018	Initial guide provided for vSphere Recovery Agent 8.6*x*.

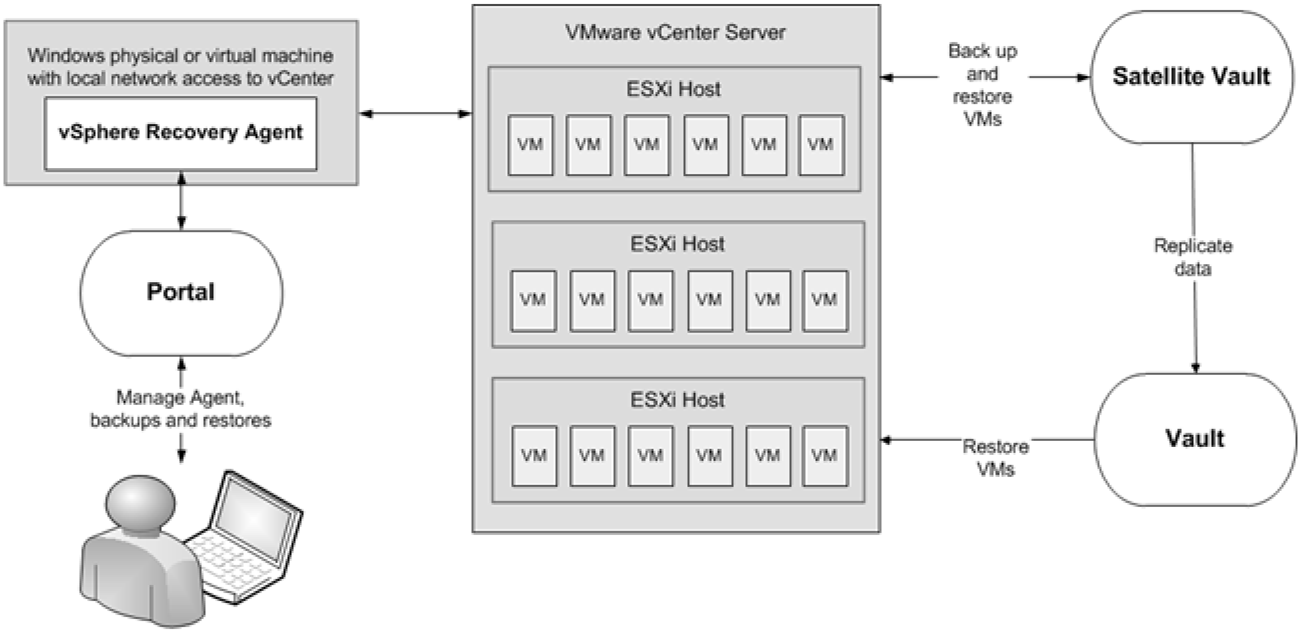
Contents

1 Introduction to the vSphere Recovery Agent

The vSphere Recovery Agent (VRA) provides data protection for VMware vSphere version 6.5 environments. We also recommend using VRA 8.6 to protect vSphere 6.0 environments.

A single VRA can back up VMs and templates across all hosts managed by a vCenter Server. The VRA must be installed on a Windows physical or virtual machine with local network access to the vCenter you want to protect.

As shown in the following diagram, you must use Portal to configure and manage the vSphere Recovery Agent, back up VMs and templates to a secure vault, and restore vSphere data. You cannot manage the VRA using the legacy Windows CentralControl interface.



To minimize backup time and space required on the vault, the VRA only reads and backs up disk blocks that are being used on each VM. To improve the performance of delta backups, the VRA can use Changed Block Tracking (CBT): a VMware feature that tracks changed disk sectors.

VRA 8.6 can back up and restore:

- VMs with VMDKs that are as large as 10 TB.
- VMs that reside partly or completely on vSAN storage. The VRA can back up and restore VMs on vSAN storage as long as the minimum number of nodes required for the vSAN cluster are up.

You can restore entire VMs using the vSphere Recovery Agent, and restore specific files and folders from Windows VMs.

2 Prepare for a vSphere Recovery Agent installation

Before installing a vSphere Recovery Agent, you must do the following:

- Obtain a Portal account for managing the Agent. See Portal for managing a vSphere Recovery Agent.
- Determine the destination vaults for vSphere backups. See Vaults for vSphere Recovery Agent backups.
- Determine where to install the Agent. See Recommended vSphere Recovery Agent deployment.

If you are upgrading a vSphere environment that was previously protected by vSphere Agent 7.3*x* to version 6.5, you must plan how to upgrade the environment and install the vSphere Recovery Agent. See Plan a VMware vSphere environment upgrade.

For best practices in a protected VMware vSphere environment, see vSphere Recovery Agent limitations and best practices.

2.1 Portal for managing a vSphere Recovery Agent

You must manage a vSphere Recovery Agent using Carbonite Server Backup Portal. You cannot manage a vSphere Recovery Agent using the legacy Windows CentralControl interface.

You must have a Portal account before you can install a vSphere Recovery Agent. The account can be on a Portal instance that is hosted by Carbonite, or installed on-premises.

2.2 Vaults for vSphere Recovery Agent backups

To provide fast, local vault access for backups and restores, back up vSphere data to a Carbonite appliance.

The data can then be replicated to the Carbonite cloud to ensure offsite protection in the case of a disaster.

If you choose not to use a Carbonite appliance, consider using a standalone vault to seed and restore large backups.

For system requirements and supported platform information, see the vSphere Recovery Agent release notes.

2.3 Recommended vSphere Recovery Agent deployment

The vSphere Recovery Agent must be installed on a Windows physical or virtual machine that has network access to the vCenter that you want to protect. For best performance, install the vSphere Recovery Agent on a machine in the same subnet as the vCenter.

To distribute the workload, up to five vSphere Recovery Agents can protect VMs in a single vCenter.

For system requirements and supported platform information, see the vSphere Recovery Agent release notes.

2.4 Plan a VMware vSphere environment upgrade

If a vSphere environment is protected by vSphere Agent 7.3*x*, you cannot upgrade the vSphere Agent to vSphere Recovery Agent 8.6 or 8.4. However, you can re-register VRA 8.6 or 8.4 with a vault as a version 7.3x vSphere Agent. You can then run backup jobs from the version 7.3x Agent without reseeding and restore VMs from existing backups. See Re-register a vSphere Recovery Agent as an existing vSphere Agent.

Note: The first backup after a re-registration will not reseed, but the backup could take longer than a normal delta backup. The VRA cannot use Changed Block Tracking (CBT) for the first backup, and has to read all VM data.

Note: A vCenter must be upgraded to version 6.5 before any hosts are upgraded.

2.5 vSphere Recovery Agent limitations and best practices

The VRA can back up and restore VMs with VMDKs that are as large as 10 TB in size. Avoid using VMDKs that are larger than 10 TB.

The VRA skips physical Raw Device Mapping (pRDM), shared disks and independent disks when backing up VMs, because VMware does not allow them to be included in snapshots for VM-level backups. To back up data on these disks, you must install an Agent within the VM. During backup, the VRA skips disks with these features with a warning message. If a VM contains one or more disks that can be protected, the VM will still be backed up.

3 Install, upgrade or uninstall the vSphere Recovery Agent

The vSphere Recovery Agent is a Windows application. You can install the vSphere Recovery Agent (VRA) on a Windows physical or virtual machine that has local network access to the vCenter that you want to protect. See Install the vSphere Recovery Agent.

After installing a VRA, you can configure vCenter, vault and other settings for the Agent. See Configure a vSphere Recovery Agent.

You can upgrade a VRA from version 8.4 to version 8.6. See Upgrade a vSphere Recovery Agent.

You cannot upgrade a vSphere Agent version 7.3*x* or earlier to VRA 8.4 or 8.6. However, you can re-register a VRA with a vault as a version 7.3x vSphere Agent, run backup jobs from the version 7.3x Agent without reseeding, and restore VMs from existing backups. See Re-register a vSphere Recovery Agent as an existing vSphere Agent.

You cannot modify a VRA installation. To change the Portal registration for a VRA, you must uninstall the VRA and then reinstall it. See Uninstall the vSphere Recovery Agent and Change the Portal registration for a vSphere Recovery Agent.

3.1 Install the vSphere Recovery Agent

To protect a VMware vSphere environment, you must install the vSphere Recovery Agent (VRA) on a Windows physical or virtual machine that has local network access to the vCenter. For best performance, install vSphere Recovery Agent on a machine in the same subnet as the vCenter.

Ensure that power management is disabled on the machine where you install VRA.

To install the vSphere Recovery Agent:

1. On a physical or virtual machine with a supported Windows platform, double-click the VRA installation kit.
2. In the confirmation message box, click **Yes**.
3. On the Welcome page, click **Next**.
4. On the End-User License Agreement page, read the license agreement. Click **I accept the terms in the License Agreement**, and then click **Next**.
5. On the Destination Folder page, do one of the following:
   - To install the VRA in the default location, click **Next**.
   - To install the VRA in another location, click **Change**. In the Change destination folder dialog box, browse to the new installation folder, or enter it in the **Folder name** box. Click **OK**. On the Destination Folder page, click **Next**.

6. On the Register Agent with Portal page, specify the following information:

   - In the **Network Address** box, type the host name or IP address of the Portal for managing the VRA. Specifying the host name of the Portal is recommended. This will allow DNS to handle IP address changes.
   - In the **Port** box, type the port number for communicating with the Portal.
   - In the **Username** box, type the name of the Portal user for managing the VRA.

     After the VRA is installed, the VRA appears on the Computers page of the Portal for this user and other Admin users in the user's site.
   - In the **Password** box, type the password of the specified Portal user.

7. Click **Next**.
8. When the installation is complete, click **Finish**.

3.1.1 Install the vSphere Recovery Agent in silent mode

To install the vSphere Recovery Agent in silent mode, run the following command with administrative rights in the directory where the installation kit is located:

```
installKitName -y /qn PORTAL_ADDRESS=PortalAddress
[PORTAL_PORT=portNumber] PORTAL_USER=PortalUser
PORTAL_PASSWORD=PortalPassword
```

Where *installKitName* is the name of the vSphere Recovery Agent installation kit.

The following table lists and describes command parameters:

Parameter	**Description**
PORTAL_ADDRESS=*PortalAddress*	Specifies the host name or IP address of the Portal for managing the Agent. Example: PORTAL_ADDRESS=portal.site.com Specifying the host name is recommended. This will allow DNS to handle IP address changes.
PORTAL_PORT=*portNumber*	Specifies the port number for communicating with Portal. If you do not specify this optional parameter, the default value (8086) is used.
PORTAL_USER=*PortalUser*	Specifies the name of the Portal user associated with the Agent. Example: PORTAL_USER=user@site.com
PORTAL_PASSWORD=*PortalPassword*	Specifies the password of the Portal user. Example: PORTAL_PASSWORD=password1234

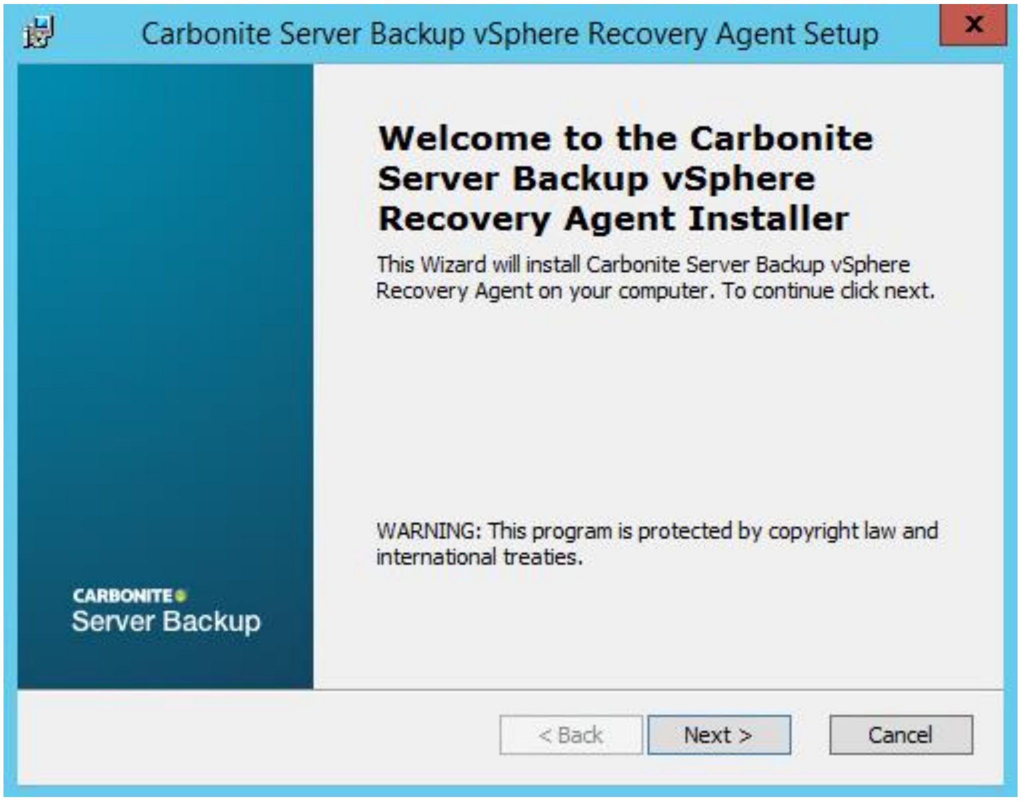
3.2 Upgrade a vSphere Recovery Agent

You can upgrade a vSphere Recovery Agent from version 8.4 to version 8.6.

You cannot upgrade vSphere Agent 7.3*x* to vSphere Recovery Agent 8.4 or 8.6. However, you can re-register VRA with a vault as a version 7.3x vSphere Agent. See Re-register a vSphere Recovery Agent as an existing vSphere Agent.

To upgrade a vSphere Recovery Agent:

1. On the machine where VRA 8.4 is installed, double-click the VRA installation kit.
2. In the confirmation message box, click **Yes**.
3. On the Welcome page, click **Next.**



Carbonite Server Backup vSphere Recovery Agent Setup

Welcome to the Carbonite Server Backup vSphere Recovery Agent Installer

This Wizard will install Carbonite Server Backup vSphere Recovery Agent on your computer. To continue click next.

WARNING: This program is protected by copyright law and international treaties.

4. On the End-User License Agreement page, read the license agreement. Click **I accept the terms in the License Agreement**, and then click **Next**.
5. When the upgrade is complete, click **Finish**.

3.2.1 Upgrade a vSphere Recovery Agent in silent mode

You can upgrade a vSphere Recovery Agent from version 8.4 to version 8.6.

To upgrade the vSphere Recovery Agent in silent mode, run the following command with administrative rights in the directory where the installation kit is located:

```
installKitName -y /q
```

3.3 Uninstall the vSphere Recovery Agent

Note: To change the Portal registration for a VRA, you must uninstall the VRA and then reinstall it. See Change the Portal registration for a vSphere Recovery Agent. You cannot modify a VRA installation.

To uninstall a vSphere Recovery Agent, do one of the following:

- Right-click the VRA installer, and choose **Uninstall**. In the confirmation dialog box, click **Yes**.
- In the Control Panel, uninstall the vSphere Recovery Agent.

3.3.1 Uninstall the vSphere Recovery Agent in silent mode

To uninstall a vSphere Recovery Agent in silent mode, run the following command with administrative rights in the directory where the installation kit is located:

```
    installKitName -y /x /qn
```

4 Re-register a vSphere Recovery Agent as an existing vSphere Agent

You cannot upgrade vSphere Agent 7.3*x* to vSphere Recovery Agent (VRA) version 8.4 or 8.6. However, you can re-register VRA with a vault as a version 7.3x vSphere Agent, run backup jobs from the version 7.3x Agent without reseeding, and restore VMs from existing backups. If the version 7.3x vSphere Agent backed up data to multiple vaults, you can re-register VRA to multiple vaults using Portal version 8.50 or later.

Note: The first backup after a re-registration will not reseed, but the backup could take longer than a normal delta backup. The VRA cannot use Changed Block Tracking (CBT) for the first backup, and has to read all VM data.

When you re-register a VRA as a version 7.3*x* vSphere Agent, the vCenter address and backup jobs are automatically populated for the VRA. You must then specify credentials for authenticating with the vCenter, credentials for sending email notifications, and the encryption password for each backup job.

IMPORTANT: To avoid reseeding a job, you must enter the encryption password that was used when vSphere Agent 7.3*x* ran the backup job.

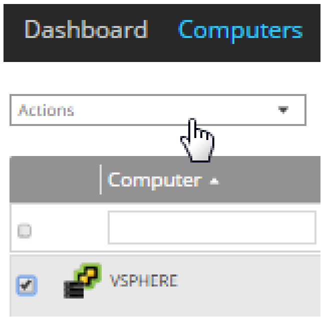
To re-register a vSphere Recovery Agent as a vSphere Agent:

1. Capture all logs from the version 7.3*x* vSphere Agent in a Support bundle. To do this, run the following command on the vSphere Agent:

   `support logs scp [`*user*`@`*host*`[:`*path*`]]`

   Where *path* is a Windows share where the Support bundle will be saved, and *user@host* is a user with access to the Windows share.

2. Disable all scheduled jobs for the version 7.3*x* vSphere Agent. To do this, on the Computers page in Portal, select the check box to the left of the version 7.3*x* vSphere Agent. In the **Actions** list, click **Disable Scheduled Jobs**.

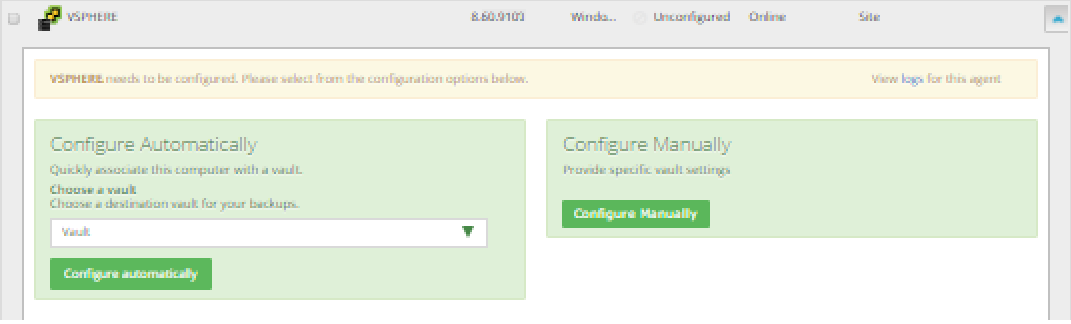
3. Install VRA on a Windows physical or virtual machine with local network access to the vCenter that you want to protect. See Install the vSphere Recovery Agent.

4. On the navigation bar in Portal, click **Computers**.

   The Computers page shows registered computers.

5. Find the VRA that you installed, and expand its view by clicking its row.

   The Configure Automatically and Configure Manually boxes appear.



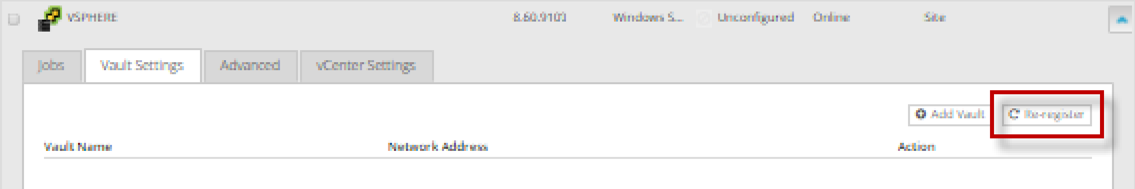
VSPHERE needs to be configured. Please select from the configuration options below.

Quickly associate this computer with a vault.

Choose a vault
Choose a destination vault for your backups.

Provide specific vault settings

6. Click **Configure Manually**.
7. On the Vault Settings tab, click **Re-register**.



8. In the Vault Settings dialog box, do one of the following:
   - In the **Vault Profile** list, select a vault with backups from the original vSphere Agent. Vault information and credentials are then populated in the dialog box.
   - In the **Vault Name** box, enter a name for the vault. In the **Address** box, enter the host name or IP address of the vault with backups from the original vSphere Agent. In the **Account**, **Username**, and **Password** boxes, enter an account and credentials for backing up data to and restoring data from the vault.

     Specifying the host name of the vault is recommended. This will allow DNS to handle IP address changes.
9. Click **Load Computers**.
10. In the list of computers, click the name of the version 7.3*x* vSphere Agent that previously backed up VMs in the vCenter. Click **Save**.
11. In the Confirmation message box, click **Yes**.
12. If the version 7.3*x* vSphere Agent backed up data to another vault, repeat Steps 7 to 11 to re-register the VRA to the other vault.
13. On the vCenter Settings tab, type the username and password for authenticating with the vCenter.
14. Confirm that the Changed Block Tracking (CBT) setting is correct.
15. Click **Save**. A Success message appears. Click **Okay**.
16. On the Advanced tab, if a Notifications tab appears and you can edit SMTP settings, enter and save SMTP credentials. Click **Save**.

17. On the Jobs tab, do the following for each backup job:

    a. In the **Select Action** menu for the job, click **Edit Job**.

    b. In the Edit Job dialog box, re-enter the encryption password for the job in the **Password** and **Confirm Password** boxes.

       IMPORTANT: To avoid reseeding the job, you must enter the encryption password that was used when the version 7.3*x* vSphere Agent ran the backup job.

    c. Save the job.

    d. In the **Select Action** menu for the job, click **Synchronize**.

5 Configure a vSphere Recovery Agent

Note: This section describes how to configure a VRA to protect a new vCenter. To replace a version 7.3*x* vSphere Agent and run existing jobs without reseeding, see Re-register a vSphere Recovery Agent as an existing vSphere Agent.

After a VRA is installed and registered with Portal, you must configure the Agent by doing the following:

- Provide information and credentials for the vCenter that you want to protect. The user should have administrative rights to the vCenter.
- Change the CBT setting. Changed Block Tracking (CBT) is a VMware feature that tracks changed disk sectors and improves the performance of VM backups. By default, the vSphere Agent enables Changed Block Tracking (CBT) for VMs.
- Add a vault connection. A vault connection provides vault information and credentials so that the Agent can back up data to and restore data from the vault.

You can also change these settings after the initial configuration. See Change vCenter information for a vSphere Recovery Agent, Change the CBT Setting for a vSphere Recovery Agent and Add vault settings.

Optionally, you can do the following:

- Add a description for the Agent. The description appears for the vSphere environment on the Computers page. See Add a description.
- Add retention types that specify how long backups are kept on the vault. See Add retention types.
- Configure email notifications so that users receive emails when backups complete, fail, or have errors. See Set up email notifications for backups on a computer.
- Specify the amount of bandwidth consumed by backups. See Configure bandwidth throttling.

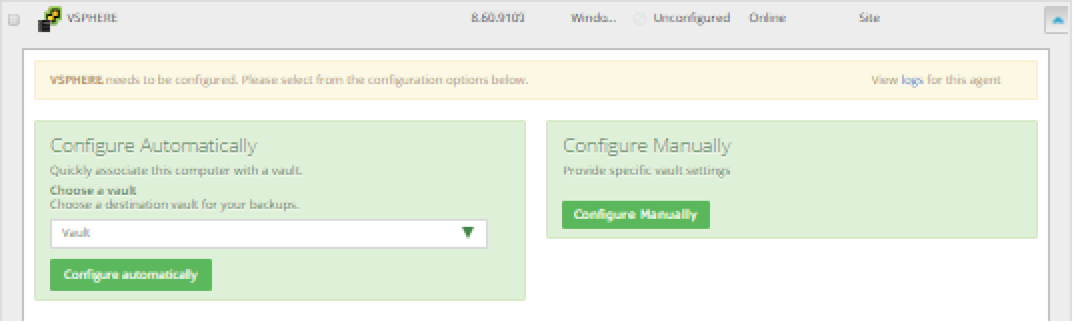
To configure the vSphere Recovery Agent:

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

   The Computers page shows registered computers.

2. Find the unconfigured vSphere Recovery Agent, and expand its view by clicking its row.

   If the Agent has not been configured, the Configure Automatically and Configure Manually boxes appear.



□ VSPHERE 8.60.9103 Windo... Unconfigured Online Site

VSPHERE needs to be configured. Please select from the configuration options below.

3. If an **Associate this computer with a site** list appears, choose a site for the Agent.

   The site list appears if you are signed in as an Admin user in a parent site that has child sites. The list includes the parent site if it has a vault profile, and all child sites in the parent site.

4. To add a vault connection for the Agent, do one of the following:

   - Choose a vault from the **Choose a vault** list, and then click **Configure Automatically**. If the vault connection is added successfully, a message appears. Click **Go to Agent**.

     If the vault connection is not added successfully, you can add the vault connection manually.

   - Click **Configure Manually**. On the Vault Settings tab, click **Add Vault**. In the Vault Settings dialog box, do the following:

     - In the **Vault Name** box, enter a name for the vault connection.
     - In the **Address** box, enter the vault host name or IP address.

       Specifying the host name is recommended. This will allow DNS to handle IP address changes.

     - In the **Account**, **Username**, and **Password** boxes, enter an account name and credentials for backing up data to and restoring data from the vault.

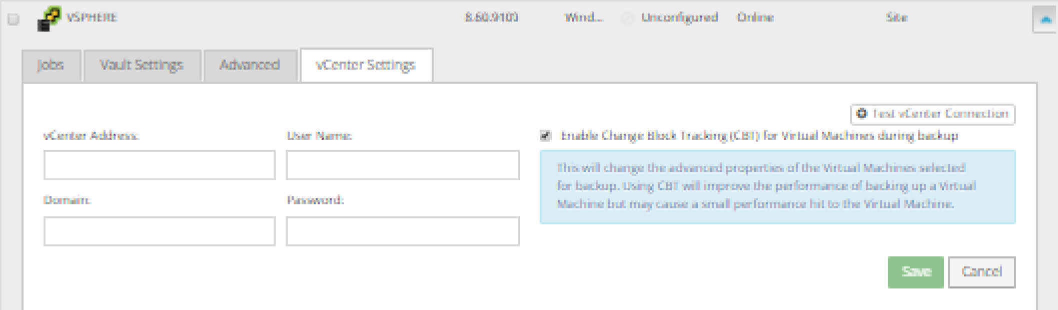
     Click **Save**.

5. On the vCenter Settings tab, do the following:

   - In the **vCenter Address** box, type the host name or IP address of the vCenter that you want to protect. Specifying the host name is recommended. This will allow DNS to handle IP address changes.
   - In the **Domain** box, type the domain of the account for authenticating with the vCenter. The domain is not required if you specify the domain in the **Username** box.
   - In the **Username** box, type the account that is used to authenticate with the vCenter. You can type the account as *username, domain\username,* or *username@domain.*

     The user must have administrator permissions for the vCenter.

   - In the **Password** box, type the password for the specified user.



☑ Enable Change Block Tracking (CBT) for Virtual Machines during backup

This will change the advanced properties of the Virtual Machines selected for backup. Using CBT will improve the performance of backing up a Virtual Machine but may cause a small performance hit to the Virtual Machine.

6. To validate the vCenter settings, click **Test vCenter Connection**. If the credentials are valid, a Success message appears. Click **Okay**.

7. Do one of the following:
   - To enable CBT for VMs that do not have it enabled, select **Enable Change Block Tracking (CBT) for Virtual Machines during backup**.
   - To stop the VRA from enabling CBT for VMs, clear **Enable Change Block Tracking (CBT) for Virtual Machines during backup**.
8. Click **Save**. A Success message appears. Click **Okay**.

   The VRA is now ready for creating backup jobs. See Add a vSphere backup job.

5.1 Change vCenter information for a vSphere Recovery Agent

To change vCenter information for a vSphere Recovery Agent:

1. In Portal, on the navigation bar, click **Computers**.

   The Computers page shows registered computers.
2. Find the vSphere Recovery Agent, and expand its view by clicking its row.
3. On the vCenter Settings tab, do the following:
   - In the **vCenter Address** box, enter the host name or IP address of the vCenter that you want to protect. Specifying the host name is recommended. This will allow DNS to handle IP address changes.
   - In the **Domain** box, type the domain of the account for authenticating with the vCenter. The domain is not required if you specify the domain in the **Username** box.
   - In the **Username** box, type the account that is used to authenticate with the vCenter. You can type the account as *username, domain\username,* or *username@domain***.**

     The user must have administrator permissions for the vCenter.
   - In the **Password** box, type the password for the specified user.
4. Click **Save**. A Success message appears. Click **Okay**.

5.2 Change the CBT Setting for a vSphere Recovery Agent

Changed Block Tracking (CBT) is a VMware feature that tracks changed disk sectors and improves the performance of VM backups. By default, the vSphere Agent enables Changed Block Tracking (CBT) for VMs.

However, because CBT requires some virtual disk processing overhead, you can stop the Agent from enabling CBT for VMs. This does not disable CBT for VMs that already have it enabled through the Agent or another mechanism. It only stops the Agent from enabling CBT in the future for VMs that do not already have it enabled.

To change the CBT setting for a vSphere Recovery Agent:

1. In Portal, on the navigation bar, click **Computers**.

   The Computers page shows registered computers.

2. Find the vSphere Recovery Agent, and expand its view by clicking its row.
3. On the vCenter Settings tab, do one of the following:
    - To enable CBT for VMs that do not have it enabled, select **Enable Change Block Tracking (CBT) for Virtual Machines during backup**.
    - To stop the VRA from enabling CBT for VMs, clear **Enable Change Block Tracking (CBT) for Virtual Machines during backup**.
4. Click **Save**.

5.3 Change the Portal registration for a vSphere Recovery Agent

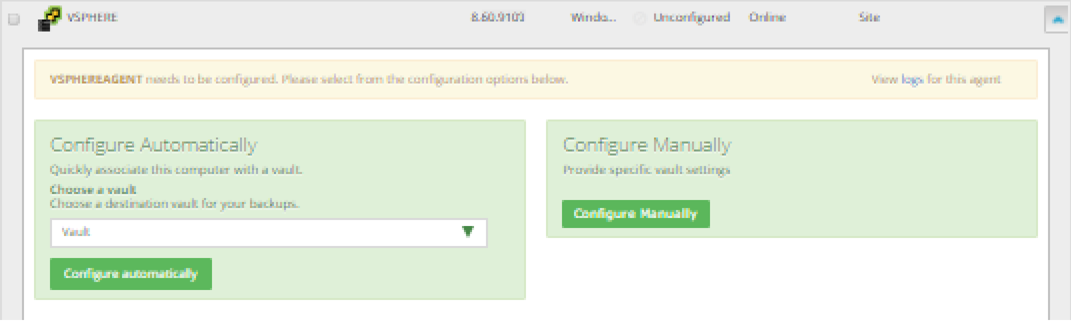
You cannot change the Portal registration of a VRA by running the installation kit. To change the Portal address or user information for a vSphere Recovery Agent, you must uninstall the VRA, reinstall it with the new Portal registration, and then reregister the VRA with the vault.

To change the Portal registration for a vSphere Recovery Agent:

1. On the machine where the VRA is installed, back up the log files in the folder where the Agent is installed (by default, C:\Program Files\Carbonite Server Backup\VMware Recovery Agent).
2. Uninstall the VRA. See [Uninstall the vSphere Recovery Agent]().
3. Reinstall the VRA. When prompted to register the Agent with Portal, enter the new Portal registration information. See [Install the vSphere Recovery Agent]().
4. On the navigation bar in Portal, click **Computers**.

    The Computers page shows registered computers.
5. Find the VRA that you installed, and expand its view by clicking its row.

    The Configure Automatically and Configure Manually boxes appear.



VSPHEREAGENT needs to be configured. Please select from the configuration options below.

Configure Automatically

Quickly associate this computer with a vault.

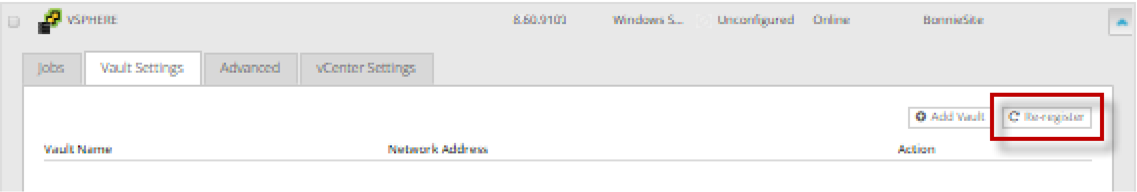
Choose a vault

Choose a destination vault for your backups.

Configure Manually

Provide specific vault settings

6. Click **Configure Manually**.
7. On the Vault Settings tab, click **Re-register**.



8. In the Vault Settings dialog box, do one of the following:

   - In the **Vault Profile** list, select the vault with backups from the original vSphere Agent. Vault information and credentials are then populated in the dialog box.
   - In the **Vault Name** box, enter a name for the vault. In the **Address** box, enter the host name or IP address of the vault with backups from the original VRA. In the **Account**, **Username**, and **Password** boxes, enter an account and credentials for backing up data to and restoring data from the vault.

     Specifying the host name of the vault is recommended. This will allow DNS to handle IP address changes.

9. Click **Load Computers**.
10. In the list of computers, click the name of the original VRA. Click **Save**.
11. In the Confirmation message box, click **Yes**.
12. On the vCenter Settings tab, type the username and password for authenticating with the vCenter.
13. Click **Save**. A Success message appears. Click **Okay**.
14. On the Jobs tab, do the following for each backup job:

    a. In the **Select Action** menu for the job, click **Edit Job**.

    b. In the Edit Job dialog box, re-enter the encryption password for the job in the **Password** and **Confirm Password** boxes.

       IMPORTANT: To avoid reseeding the job, you must enter the encryption password that was used when the original VRA ran the backup job.

    c. Save the job.

    d. In the **Select Action** menu for the job, click **Synchronize**.

15. On the Advanced tab, if a Notifications tab appears and you can edit SMTP settings, enter and save SMTP credentials. Click **Save**.

5.4 Add vault settings

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

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

If a policy is assigned to a VRA, Admin users can select any vault profile from the policy. Regular users can only select policy vault profiles that are also assigned to them.

If a policy is not assigned to a VRA, Admin users can select any vault profile in the site. Regular users can only select vault profiles that are assigned to them.

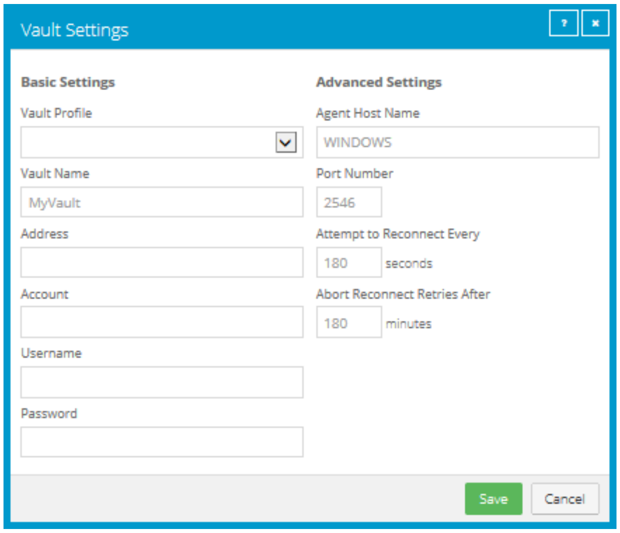
In previous Portal versions, you could specify whether data is encrypted using AES encryption when it is transmitted to and from the vault. Over-the-wire encryption is now automatically enabled when you add vault settings or save existing vault settings.

When an E2 appliance reports a new IP address, the IP address is updated in Portal vault settings for Agents that are registered to the E2, and in the E2 vault profile. Agent versions 8.10 and later contact Portal to check for vault IP address changes. If a Super user or Admin user changes the name of an E2 vault profile, the name is updated automatically in vault settings for Agents that are registered to the E2.

To add vault settings:

1. On the navigation bar, click **Computers**.
2. Find the VRA for which you want to add vault settings, and click the computer row to expand its view.
3. On the **Vault Settings** tab, click **Add Vault**.

   The Vault Settings dialog box appears.



Vault Settings

Basic Settings

Vault Profile

Vault Name: MyVault

Address

Account

Username

Password

Advanced Settings

Agent Host Name: WINDOWS

Port Number: 2546

Attempt to Reconnect Every: 180 seconds

Abort Reconnect Retries After: 180 minutes

4. Do one of the following:

   - In the **Vault Name** box, enter a name for the vault. In the **Address** box, enter the vault host name or IP address. In the **Account**, **Username**, and **Password** boxes, enter an account and credentials for backing up data to and restoring data from the vault.

     Specifying the host name of the vault is recommended. This will allow DNS to handle IP address changes.

- Click the **Vault Profile** box. If one or more vault profiles appear, click the vault profile that you want to add for the computer. Vault information and credentials are then populated in the **Vault Settings** dialog box.

  If a policy is assigned, the **Vault Profile** list includes vault profiles from the policy. If a policy is not assigned, the list includes vault profiles from the site. For a regular user, the list only includes vault profiles that are also assigned to the user.

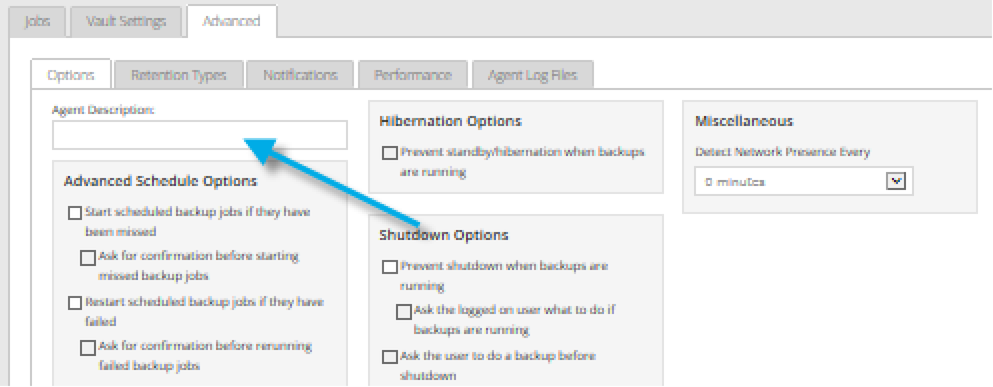
5. (Optional) Change one or more of the following Advanced Settings for the vault connection:
   - **Agent Host Name**. Name to use for the computer on the vault.
   - **Port Number**. Port used to connect to the vault. The default port is 2546.
   - **Attempt to Reconnect Every**. Specifies the number of seconds after which the Agent should try to connect to the vault, if the vault becomes unavailable during a backup or restore.
   - **Abort Reconnect Retries After**. Specifies the number of times the Agent tries to reconnect to the vault, if the vault becomes unavailable during a backup or restore. If the Agent cannot connect to the vault successfully in the specified number of tries, the backup or restore fails.
6. Click **Save**.

5.5 Add a description

You can add a description for a VRA in Portal. The description appears on the Computers page, and can help you find and identify a particular VRA.

To add a description:

1. On the navigation bar, click **Computers**.
2. Find the VRA for which you want to add a description, and click the row to expand its view.
3. On the **Advanced** tab, click the **Options** tab.
4. In the **Agent Description** box, enter a description for the VRA.



Agent Description:

Advanced Schedule Options

□ Start scheduled backup jobs if they have been missed

□ Ask for confirmation before starting missed backup jobs

□ Restart scheduled backup jobs if they have failed

□ Ask for confirmation before rerunning failed backup jobs

Hibernation Options

□ Prevent standby/hibernation when backups are running

Shutdown Options

□ Prevent shutdown when backups are running

□ Ask the logged on user what to do if backups are running

□ Ask the user to do a backup before shutdown

Miscellaneous

Detect Network Presence Every

0 minutes

5. Click **Save**.

5.6 Add retention types

When you schedule or run a backup job, you must select a retention type for the resulting safeset. A 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.

Portal Admin users and regular users can add retention types for a VRA where a policy is not assigned.

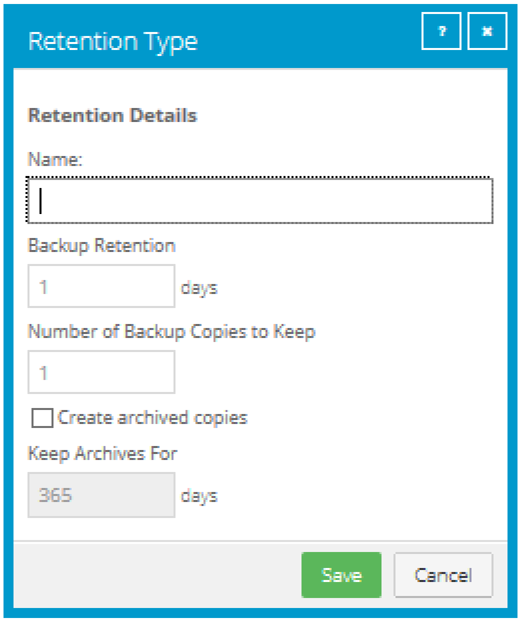
If a policy is assigned to a VRA, retention types cannot be added or modified on the Computers page. Instead, retention types can only be added or modified in the policy.

To add a retention type:

1. On the navigation bar, click **Computers**.
2. Find the VRA for which you want to add a retention type, and click the row to expand its view.
3. On the **Advanced** tab, click the **Retention Types** tab.

   If a policy is assigned to the VRA, you cannot add or change values on the **Retention Types** tab. Instead, retention types can only be added or modified in the policy.
4. Click **Create Retention Type**.

   The Retention Type dialog box appears.



Retention Details

Name:

Backup Retention

1 days

Number of Backup Copies to Keep

1

□ Create archived copies

Keep Archives For

365 days

5. 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. *Note:* 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. *Note:* 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	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.

6. Click **Save**.

5.7 Configure bandwidth throttling

Bandwidth throttling settings specify the amount of bandwidth consumed by an Agent for backups. 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 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.

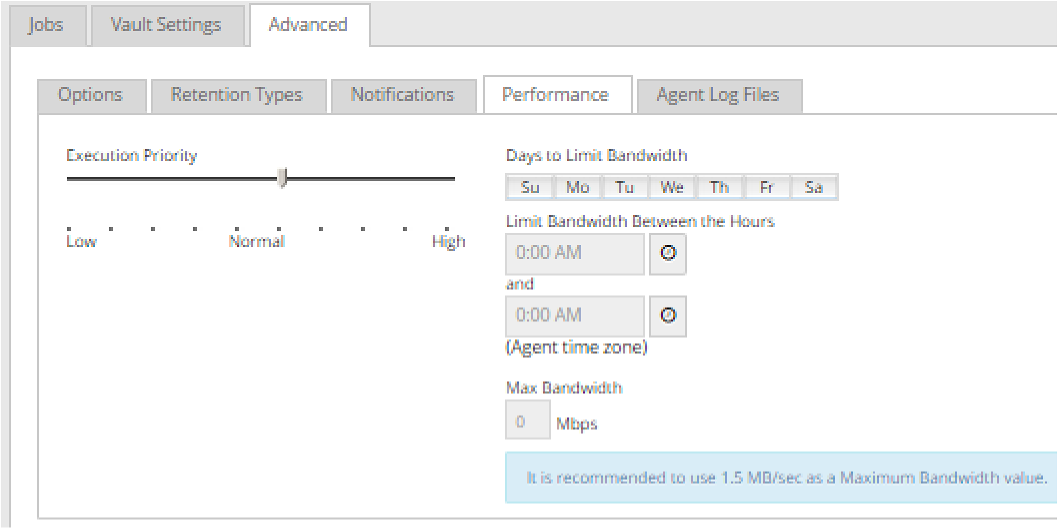
If you edit an Agent's bandwidth settings while a backup is running, the new Agent settings do not affect the backup that is running. Bandwidth settings are applied when a backup starts, and are not applied to backups that are already running.

If a policy is assigned to a computer, bandwidth throttling settings cannot be modified on the Computers page. Instead, settings can only be added or modified in the policy.

To configure bandwidth throttling:

1. On the navigation bar, click **Computers**.
2. Find the VRA for which you want to configure bandwidth throttling, and click the row to expand its view.
3. Click the **Advanced** tab, click the **Performance** tab, and then edit the bandwidth settings.

   If a policy is assigned to the VRA or protected environment, you cannot add or change values on the **Performance** tab. Instead, bandwidth settings can only be modified in the policy.



Limit Bandwidth Between the Hours

0:00 AM

and

0:00 AM

(Agent time zone)

Max Bandwidth

0 Mbps

It is recommended to use 1.5 MB/sec as a Maximum Bandwidth value.

5.8 Add a vSphere backup job

After a VMware vSphere environment is added in Portal, you can create a backup job that specifies which virtual machines (VMs) to back up, and where to save the backup data.

You must add vault settings and vCenter information before you can add a backup job. See Configure a vSphere Recovery Agent.

To back up the data, you can run the backup job manually or schedule the backup job to run. See Run and schedule backups and synchronizations.

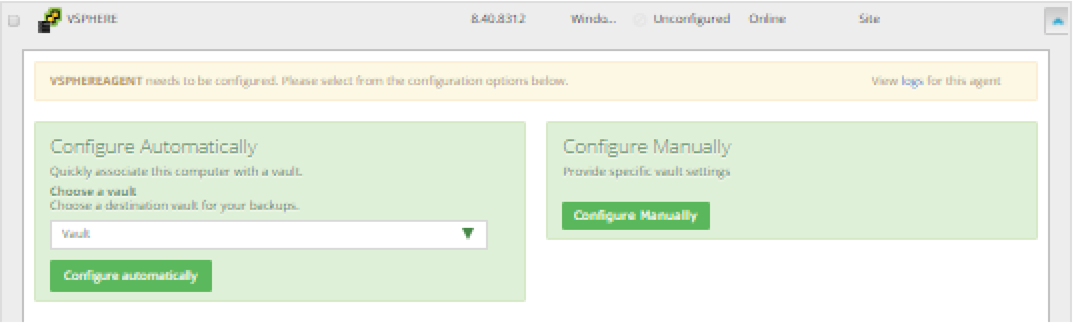
To add a vSphere backup job:

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

   The Computers page shows registered computers and environments.

2. Click the vSphere environment row.

   If a message states that the Agent needs to be configured, you must add vault settings and vCenter information before adding a backup job. See Configure a vSphere Recovery Agent.



VSPHEREAGENT needs to be configured. Please select from the configuration options below.

Configure Automatically

Quickly associate this computer with a vault.

Choose a vault
Choose a destination vault for your backups.

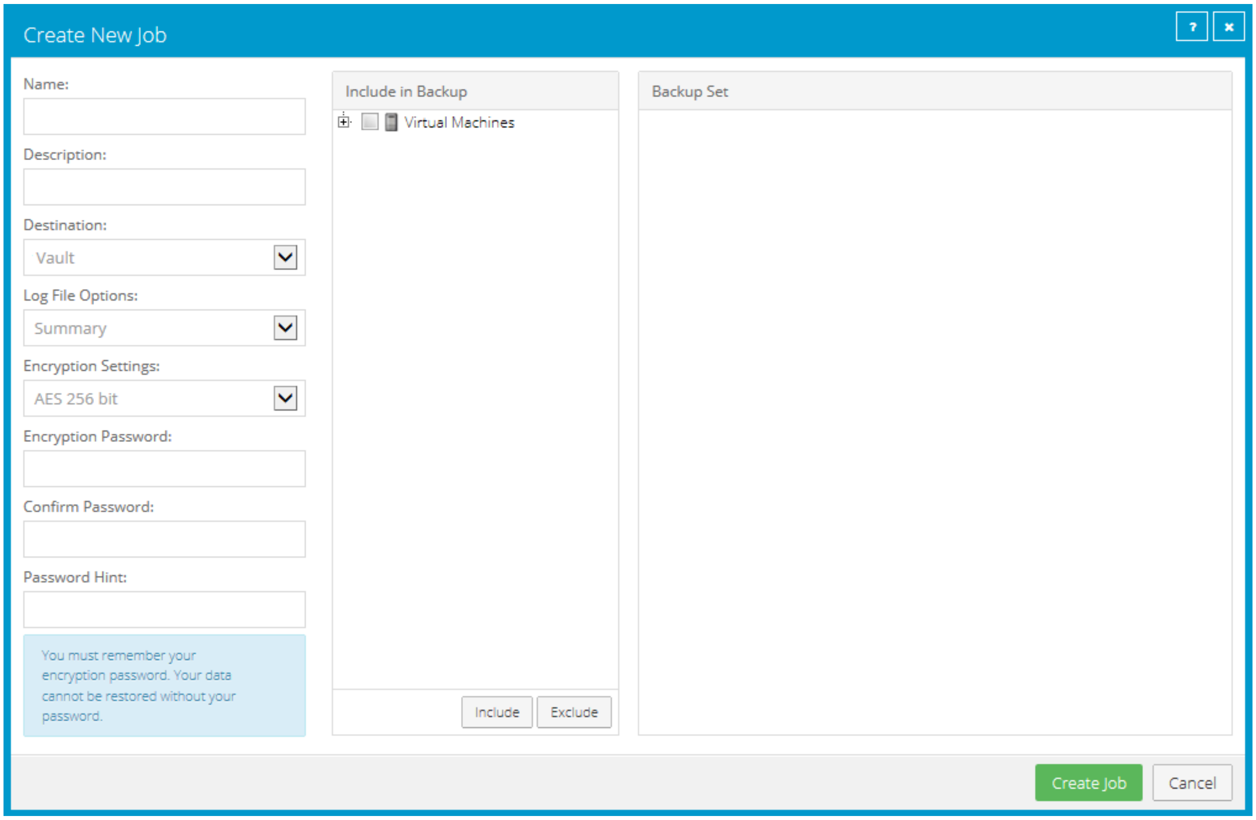
Configure Manually

Provide specific vault settings

3. Click the **Jobs** tab.
4. In the **Select Job Task** menu, click **Create New VMware vCenter Job**.
5. In the **Create New Job** dialog box, specify the following information:

   - In the **Name** box, type a name for the backup job.
   - In the **Description** box, optionally type a description for the backup job.
   - In the **Destination** list, select the vault where you want to save the backup data.

     A vault only appears in the list if it assigned to the user, or if the user added it on the computer's Vault Settings tab.
   - In the **Log File Options** list, select the level of detail for job logging. For more information, see Log file options.
   - For new backup jobs, the encryption method is AES 256 bit. Existing jobs can have other encryption methods. See Encryption settings.
   - In the **Password** and **Confirm Password** boxes, enter an encryption password. You can also enter a password hint in the **Password Hint** box.



Destination: Vault

Log File Options: Summary

Encryption Settings: AES 256 bit

Encryption Password:

Confirm Password:

Password Hint:

You must remember your encryption password. Your data cannot be restored without your password.

6. In the **Include in Backup** box, do one or more of the following until the **Backup Set** box shows the VMs that you want to include and exclude in the backup job:

   - To add specific VMs to the backup job, select the check box for each VM, and then click **Include**.
   - To exclude specific VMs from the backup job, select the checbox for each VM, and then click **Exclude**.
   - To add VMs to the backup job by name, select the **Virtual Machines** check box, and then click **Include**. In the **Filter** field, enter names of VMs to include. Separate multiple names with commas, and use asterisks (*) as wildcard characters. For example, to include VMs in a backup if their names end with "x64" or start with "SQL", enter the following filter: *x64, SQL*

     Note: Asterisks (*) are the only supported wildcards in filter fields.
   - To exclude VMs from the backup job by name, select the **Virtual Machines** check box, and then click **Exclude**. In the **Filter** field, enter names of VMs to exclude. Separate multiple names with commas, and use asterisks (*) as wildcard characters. For example, to exclude VMs from a backup if their names start with "test" or end with "x32", enter the following filter: test*, *x32
   - To remove an inclusion or exclusion record from the **Backup Set** box, click the Delete button beside the record. 🗑

   Click **Apply Now** to consolidate and simplify records in the **Backup Set** box, if changes need to be applied.

7. Click **Create Job**.

The job is created, and the **View/Add Schedule** dialog box appears. Now you can create a schedule for running the backup. Click **Cancel** if you do not want to create a schedule at this time.

For information about how to run and schedule the backup job, see Run and schedule backups and synchronizations.

5.9 Log file options

When you create or edit a backup job, you can specify the level of detail for job logging. 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.

5.10 Encryption settings

Encryption settings specify the encryption type for backup data at rest on the vault. AES 256 bit encryption is the only encryption type available for new backup jobs.

If an existing job uses another encryption type (e.g., AES 128 bit, Blowfish, DES, Triple DES), you can continue to encrypt the job using that type. However, if you change the encryption type for an existing job, you cannot change the encryption type back to the original type. Only AES 256 bit will be available.

If you change encryption options for an existing job, it will force a new full backup (i.e., a reseed). The next backup will take longer than previous delta backups, and the amount of data stored on the vault will increase temporarily, depending on your retention settings.

Encryption password

You must enter a password for the encrypted backup data. The password is case-sensitive. To recover the data, you must provide the encryption password that was entered when the files were backed up.

You can also enter a password hint. When restoring data, you can view the password hint to remind you of the encryption password for this job.

IMPORTANT: The encryption password is required for restoring the data, so be sure to store it somewhere safe. If you forget your password, you will not be able to restore your data. The password is not maintained anywhere else and cannot be recovered.

6 Run and schedule backups and synchronizations

After a backup job is created, you can run it manually (ad-hoc) at any time and schedule it to run.

When running or scheduling a backup, you can specify the following settings:

- Retention type.
- Deferring. You can use deferring to prevent large backups from running at peak network times. When deferring is enabled, the backup job does not back up any new data after the specified amount of time and commits the safeset to the vault, even if some data in the job is not backed up. Changes to data that was previously backed up will be backed up, regardless of the specified amount of time.

  When the job runs again, the Agent checks for changes in data that was previously backed up, backs up those changes, and then backs up the remaining data.
- When you schedule a job to run, you can also set the compression level for the data. The compression level optimizes the volume of data sent to the vault against the speed of processing. The default compression level is usually the optimal setting.
- When a backup job first runs, all data selected in the job is backed up to the vault. This initial backup is called a “seed” backup. In subsequent backups, only data that has changed is backed up to the vault, unless a reseed is required (e.g., after a job’s encryption password has changed). In a reseed, all data selected in a backup job is sent to the vault again, even though it has already been backed up.
- After running a backup, you can view logs to check whether the backup completed successfully.

In some cases, you must synchronize a backup job before you run it or restore data from the job. When you synchronize a job, the Agent checks which safesets for the job are online and available for restore. See Synchronize a job.

6.1 Schedule a backup

After creating a backup job, you can add one or more schedules for running the job automatically.

You can create complex schedules for a job by creating multiple schedules. For example, you can schedule a backup job to run at midnight every Friday, and schedule the job to run at 8 pm on the first day of every month.

If a 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. For example, in the following screenshot, the job is scheduled to run at 12 AM each Saturday with the Weekly retention type, and every day at 12 AM with the Daily retention type. On Saturdays, the job runs only once at 12 AM. Because the schedule with the Weekly retention type is higher in the list than the schedule with the Daily retention type, the Weekly retention type is applied to the safeset.

Note: If a job is scheduled to run at slightly different times, the Agent attempts to run the job according to each schedule. For example, if a job is scheduled to run at 11 PM by one schedule and 11:01 PM by another schedule, the Agent will attempt to run the job twice. Try to avoid overlapping schedules; problems can occur if a job is scheduled to run twice in a short period of time.

To schedule a backup:

1. Do one of the following:

   - On the navigation bar, click **Computers**. Find the computer with the backup job that you want to schedule, and click the computer row to expand its view. On the **Jobs** tab, find the job that you want to schedule. In its **Select Action** menu, click **View/Add Schedule**.

   - Create a new backup job. The **View/Add Schedule** dialog box appears when you save the job.

2. In the **View/Add Schedule** dialog box, click **Add Schedule**.

   A new row appears in the dialog box.

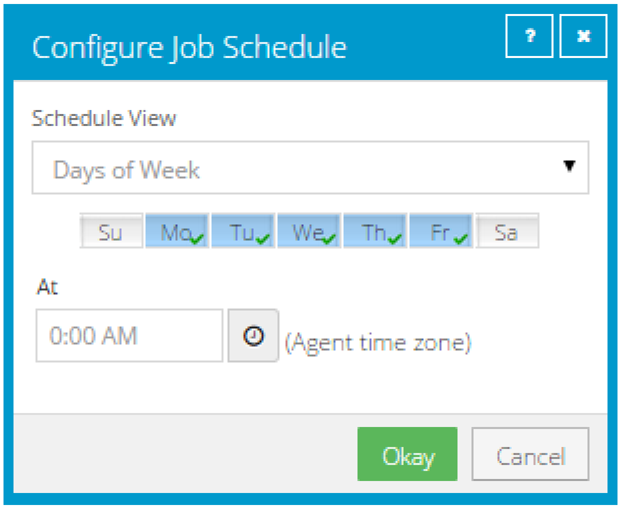
3. In the new schedule row, in the **Retention** list, click a retention type.

4. In the **Schedule** box, click the arrow.

   The **Configure Job Schedule** dialog box opens.

5. In the **Configure Job Schedule** dialog box, do one of the following:

   - 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. Then use the **At** field to specify the time when you want to run the job.



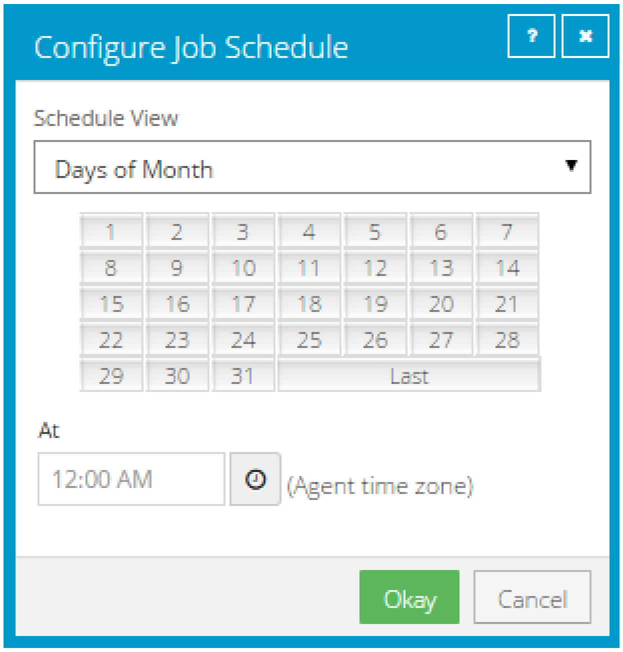
Configure Job Schedule

Schedule View: Days of Week

Su □ Mo ✓ Tu ✓ We ✓ Th ✓ Fr ✓ Sa □

At: 0:00 AM (Agent time zone)

   - 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. Then use the **At** field to specify the time when you want to run the job.



Configure Job Schedule

Schedule View

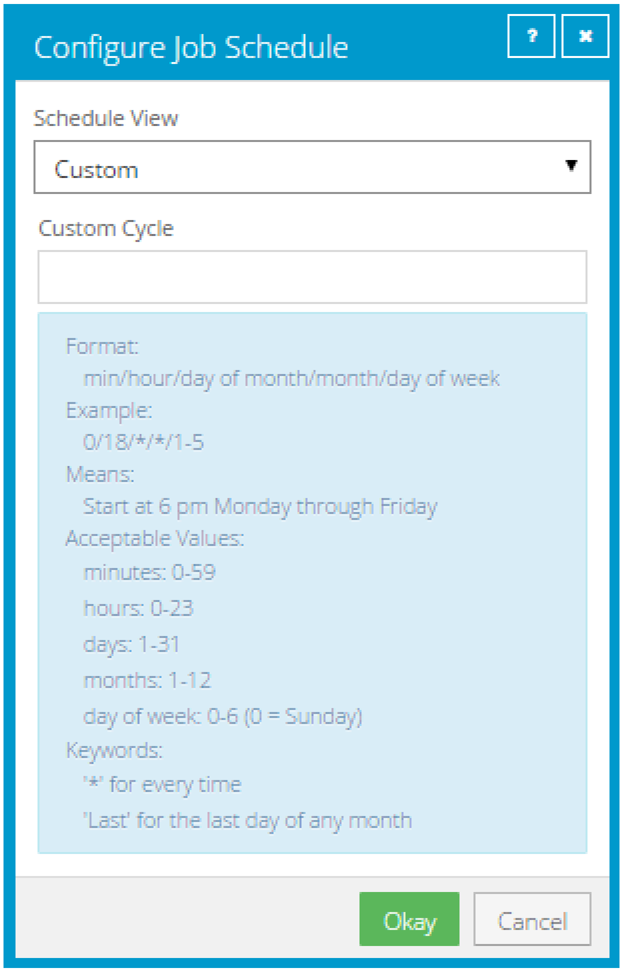
Days of Month

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	Last			

At

12:00 AM (Agent time zone)

- 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.



Configure Job Schedule

Schedule View

Custom

Custom Cycle

Format:
min/hour/day of month/month/day of week
Example:
0/18/*/*/1-5
Means:
Start at 6 pm Monday through Friday
Acceptable Values:
minutes: 0-59
hours: 0-23
days: 1-31
months: 1-12
day of week: 0-6 (0 = Sunday)
Keywords:
'*' for every time
'Last' for the last day of any month

6. Click **Okay**.

   The new schedule appears in the **Schedule** box.

7. 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.

8. 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.

   Note: 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.

9. To run the job on the specified schedule, select the **Enable** check box near the end of the row.

10. If there is more than one schedule row, you can use the **Priority** arrows to change the order of the schedule rows. Schedules higher in the list have a higher priority than schedules lower in the list.

    If a job is scheduled to run at the same time by multiple schedules, the job only runs once at the scheduled time. If the schedules have different retention types, the job only runs with the retention type of the schedule that is highest in the list.

11. Click **Save**.

6.2 Run an ad-hoc backup

After a backup job is created, you can run the backup at any time, even if the job is scheduled to run at specific times.

To run an ad-hoc backup:

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

   A grid lists available computers.

2. Find the computer with the backup job that you want to run, and expand its view by clicking the computer row.

3. Click the **Jobs** tab.

4. Find the job that you want to run, and click **Run Job** in its **Select Action** menu.

   The **Run Job** dialog box shows the default settings for the backup.

   Note: Beginning at this point, you can click **Start Backup** to immediately start the job. If you prefer, you can change backup options before running the job.

5. In the **Retention Scheme** 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.

6. Click **Start Backup**.

   The **Process Details** dialog box shows the backup progress, and indicates when the backup is completed. Other recent job processes might also be listed in the dialog box. See View current process information for a job.

7. If you want to stop the backup, click **Stop**.
8. To close the **Process Details** dialog box, click **Close**.

6.3 Synchronize a job

When a backup job is synchronized, the Agent checks which safesets for the job are online and available for restore.

A job is synchronized automatically when you restore data from the job. You can also synchronize a job manually at any time. A manual synchronization is recommended or required in the following cases:

- Before running backup jobs on reregistered computers..
- Before restoring data from jobs that are backed up to a Satellite vault and replicated to the cloud or another vault.
- To rebuild a delta (.dta) file for a job. If an error message in a log file says that the delta mapping file is corrupt, delete the delta (.dta) file from the job folder on the protected computer and then synchronize the job to rebuild the delta file.

To synchronize a job:

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

   The Computers page shows registered computers.

2. Find the computer with the job that you want to synchronize. Expand its view by clicking its row.
3. Click the **Jobs** tab.
4. Find the job that you want to synchronize, and click **Synchronize** in its **Select Action** menu.

   The **Process Details** dialog box shows the backup progress, and indicates when the backup is completed. Other recent job processes might also be listed in the dialog box. See View current process information for a job.

5. If you want to stop the backup, click **Stop**.

   To close the **Process Details** dialog box, click **Close**.

7 Restore vSphere data

When VMs are protected in a vSphere environment, you can:

- Restore vSphere VMs
- Restore files and folders using a vSphere Recovery Agent

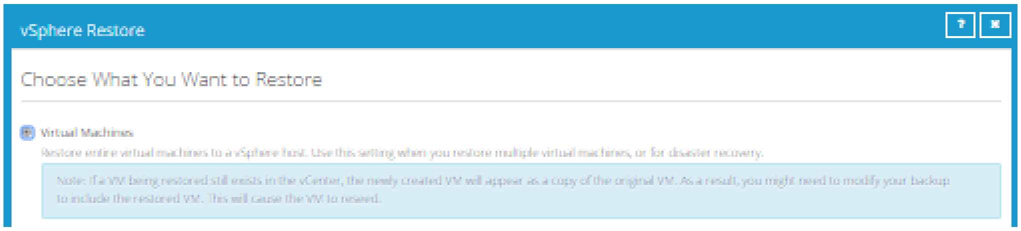
7.1 Restore vSphere VMs

To restore vSphere VMs:

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

   A grid lists available computers.

2. Find the vSphere environment with the VM that you want to restore, and expand its view by clicking the row.
3. Click the **Jobs** tab.
4. Find the backup job with the VM that you want to restore, and click **Restore** in the job's **Select Action** menu.
5. In the **Choose What You Want to Restore** dialog box, select **Virtual Machines**.



vSphere Restore

Choose What You Want to Restore

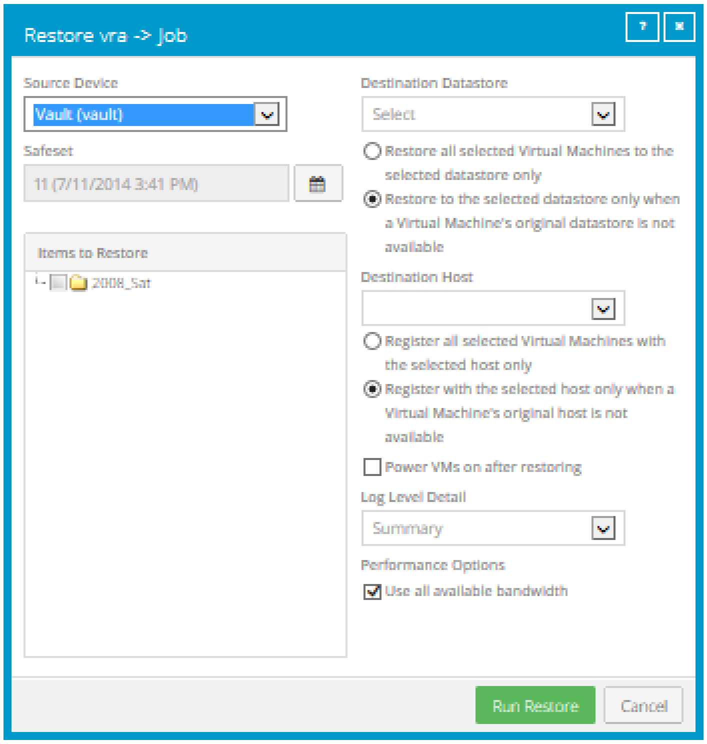
● Virtual Machines

Restore entire virtual machines to a vSphere host. Use this setting when you restore multiple virtual machines, or for disaster recovery.

Note: If a VM being restored still exists in the vCenter, the newly created VM will appear as a copy of the original VM. As a result, you might need to modify your backup to include the restored VM. This will cause the VM to reseed.

6. Click **Continue**.

   The **Restore** dialog box shows the most recent safeset for the job.



Source Device: Vault (vault)

Safeset: 11 (7/11/2014 3:41 PM)

Items to Restore

- □ 2008_Sat

Destination Datastore: Select

○ Restore all selected Virtual Machines to the selected datastore only

● Restore to the selected datastore only when a Virtual Machine's original datastore is not available

Destination Host

○ Register all selected Virtual Machines with the selected host only

● Register with the selected host only when a Virtual Machine's original host is not available

□ Power VMs on after restoring

Log Level Detail: Summary

Performance Options

☑ Use all available bandwidth

7. To restore data from another source, click a source (usually a vault) in the **Source Device** list.

8. To restore from an older safeset, click the **Browse Safesets** button. 📅 In the calendar that appears, click the date of the safeset from which you want to restore. To the right of the calendar, click the specific safeset from which you want to restore.

9. In the **Items to Restore** box, select the check box for each VM that you want to restore.

10. In the **Encryption Password** box, enter the data encryption password. To view the password hint, click the **Hint** button. ❓

11. In the **Destination Datastore** list, click the datastore for the restored VMs.

12. Select one of the following options for restoring VMs to the selected datastore:

    - **Restore all selected Virtual Machines to the selected datastore only**

    - **Restore to the selected datastore only when a Virtual Machine's original datastore is not available**. If the backed-up VM contains multiple VMDKs that resided on two or more datastores, and one or more of the datastores is unavailable, the entire VM will be restored to the selected datastore.

    Note: If you restore a VM or template to a vCenter, and the original VM is present, the VM will be restored as a clone of the original with the following name: <*VMname*>-vra-restored-<*Date*>. The VM will be restored as a clone whether the original VM is powered on, off, or suspended. If the original VM is powered on and using a static IP address, you may encounter an IP address conflict when the newly-restored cloned VM is powered on.

13. In the **Destination Host** list, click the host where you want to register the VMs.

    The list only shows hosts that have access to the selected datastore.

14. Select one of the following options for registering restored VMs with the selected host:
    - **Register all selected Virtual Machines with the selected host only**
    - **Register with the selected host only when a Virtual Machine's original host is not available**
15. To power on the VMs after they are restored, select **Power VMs on after restoring**.
16. In the **Log Level Detail** list, click the logging level. See Advanced restore options.
17. To use all available bandwidth for the restore, select **Use all available bandwidth**.
18. Click **Run Restore**.

7.2 Restore files and folders using a vSphere Recovery Agent

You can restore files and folders from a protected Windows VM using the vSphere Recovery Agent (VRA).

Note: You cannot restore files and folders from Linux VMs using the VRA.

During a file and folder restore, volumes from the selected VM are mounted as drives on the machine where the VRA is running. You can then:

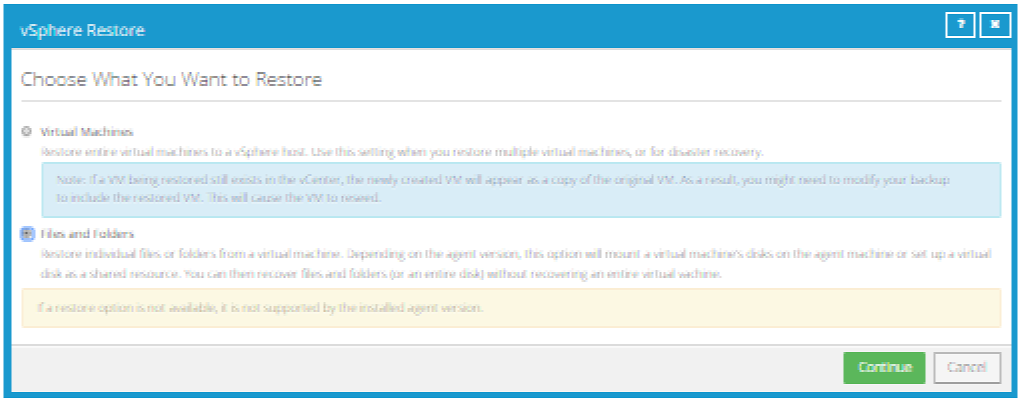
- Share some or all of the mounted drives so that users can copy files and folders from the drives.
- Sign in to the VRA machine and copy files and folders from the mounted drives. Files and folders on the disks will be accessible to anyone on the VRA system, including non-Admin users. If you are concerned about security, secure the Agent machine and prevent users from logging in to the machine locally.

You can restore files and folders from more than one VM at the same time.

To restore files and folders using a vSphere Recovery Agent:

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

   A grid lists available computers.
2. Find the vSphere environment with the VM that you want to restore, and expand its view by clicking the row.
3. Click the **Jobs** tab.
4. Find the backup job with the VM that you want to restore, and click **Restore** in the job's **Select Action** menu.
5. In the **Choose What You Want to Restore** dialog box, select **Files and Folders**.



vSphere Restore

Choose What You Want to Restore

○ Virtual Machines

Restore entire virtual machines to a vSphere host. Use this setting when you restore multiple virtual machines, or for disaster recovery.

Note: If a VM being restored still exists in the vCenter, the newly created VM will appear as a copy of the original VM. As a result, you might need to modify your backup to include the restored VM. This will cause the VM to reseed.

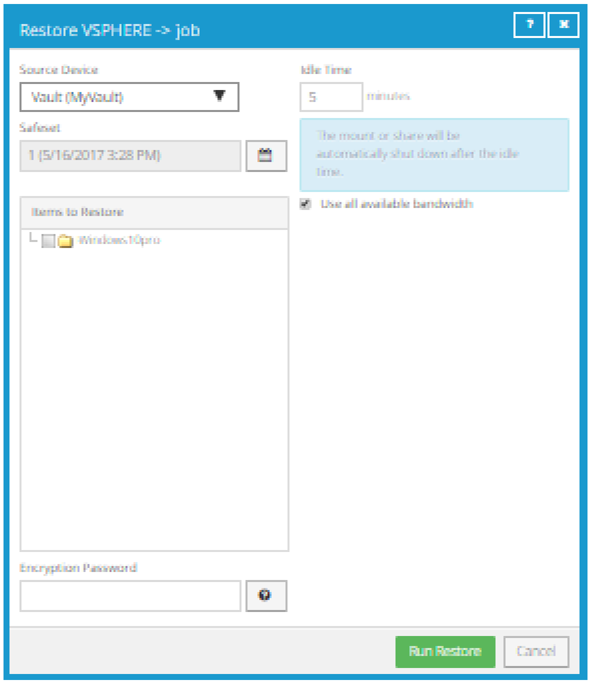
● Files and Folders

Restore individual files or folders from a virtual machine. Depending on the agent version, this option will mount a virtual machine's disks on the agent machine or set up a virtual disk as a shared resource. You can then recover files and folders (or an entire disk) without recovering an entire virtual machine.

If a restore option is not available, it is not supported by the installed agent version.

6. Click **Continue**.

   The Restore dialog box shows the most recent safeset for the job.



Restore VSPHERE -> job

Source Device: Vault (MyVault)

Safeset: 1 (5/16/2017 3:28 PM)

Items to Restore

└ □ Windows10pro

Encryption Password

Idle Time: 5 minutes

The mount or share will be automatically shut down after the idle time.

☑ Use all available bandwidth

7. To restore data from another source, click a source in the **Source Device** list.

8. To restore from an older safeset, click the **Browse Safesets** button. 📅 In the calendar that appears, click the date of the safeset from which you want to restore. To the right of the calendar, click the specific safeset from which you want to restore.

9. In the **Items to Restore** box, select the check box for the VM with files or folders that you want to restore.

10. In the **Encryption Password** box, enter the data encryption password. To view the password hint, click the **Hint** button.

11. In the **Idle Time** box, enter the number of minutes of inactivity after which the shared drive will automatically unshare. The **Idle time** can range from 2 to 180 minutes.

Note: The drive will not unshare as long as new data is being copied. If you copy the same data from a shared drive more than once, the system could time out because no new data is being read.

12. To use all available bandwidth for the restore, select **Use all available bandwidth**.
13. Click **Run Restore**.

    Volumes from the selected VM are mapped as drives on the machine where the VRA is running, and are available in a RestoreMount folder on the VRA machine.

14. On the machine where the VRA is running, do one of the following:
    - Copy files and folders that you want to restore from the mapped drives.
    - Share one or more mapped drives with other users. Users can then access the UNC share, and copy files and folders that they want to restore.
    - Share one or more directories from the RestoreMount folder on the VRA machine. Users can then access the UNC share, and copy files and folders that they want to restore.

7.3 Advanced restore options

When restoring data, you can specify the following options:

Log 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.

Performance Options

To use all available bandwidth for the restore, select **Use all available bandwidth**.

Bandwidth throttling settings specify the amount of bandwidth consumed by an Agent for backups. 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 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.

8 Monitor computers, jobs and processes

You can monitor backups, restores and protected environments using the following Portal features:

- Computer page. The Computer page shows status information for protected environments and their jobs. See View computer and job status information. You can also access logs for unconfigured computers from this page. See View an unconfigured computers logs.
- Process Details dialog box. This dialog box shows information about all running, queued and recently-completed processes for a job. See View current process information for a job.
- Email notifications. To make it easier to monitor backups, users can receive emails when backups finish or fail. See Monitor backups using email notifications.
- Process logs and safeset information. Process logs indicate whether each backup and restore completed successfully, and provide information about any problems that occurred. You can also view information about the safeset created by a specific backup. See View a jobs process logs and safeset information.
- Monitor page. The Monitor page shows the most recent backup status for each job, and allows you to navigate to the computer and job for each backup. See View and export recent backup statuses.

8.1 View computer and job status information

On the Computer page in Portal, you can view status information for protected environments and their jobs.

To view computer and job status information:

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

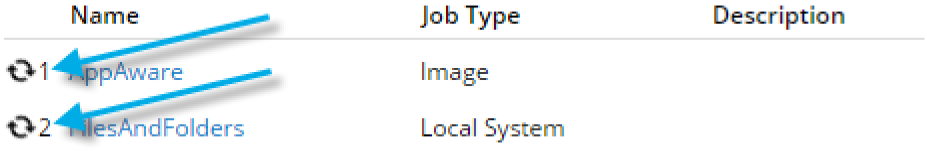
   The Computers page shows registered VRAs.

   The **Availability** column indicates whether each VRA is online or offline. Online computers are in contact with Portal, while offline computers are not currently available. A computer can be offline if it is turned off, if the Agent has been uninstalled from the system, or if the system has been lost.

   The **Status** column shows the status of each computer. Possible statuses include:

   - ✓ OK — Indicates that all jobs on the computer ran without errors or warnings.
   - ! OK with warnings — Indicates that one or more of the computer’s jobs completed with warnings.
   - ❗ Attention — Indicates that one or more of the computer’s jobs failed or completed with errors.
   - ⊘ Unconfigured — Indicates that no jobs have been created for the computer.
2. Find the VRA for which you want to view logs, and click the row to expand its view.
3. View the **Jobs** tab.

If a backup or restore is running for a job, an "In Progress" symbol ⟳ appears beside the job name, along with the number of processes that are running.



Name	Job Type	Description
⟳1 AppAware	Image	
⟳2 FilesAndFolders	Local System	

If you click the symbol, the **Process Details** dialog box shows information about running, queued and recently-completed processes for the job. See View current process information for a job.

The **Last Backup Status** column shows the result of the last backup attempt for each job. Possible statuses include:

- ✓ Completed — Indicates that the last backup completed successfully, and a safeset was created.
- ! Completed with warnings — Indicates that the last backup completed and a safeset was created, but problems occurred during the backup. For example, a warning could indicate that a file or volume that was selected in the backup job was not available for backup.
- ! Deferred — Indicates that the last backup was deferred. A safeset was created, but not all data that was selected was backed up.

  Deferring is used to prevent large backups from running at peak network times. When deferring is enabled, a backup job does not back up any new data after a specified amount of time.
- ⊘ Never Run — Indicates that the backup job has never run.
- ! Missed — Indicates that the job has not run for 7 days.
- ! Completed with errors — Indicates that the backup completed and a safeset is available for restore, but problems occurred.
- ! Failed — Indicates that the backup failed and no safeset was created.
- ! Cancelled

To view logs for a job, click the job status. For more information, see View a jobs process logs and safeset information.

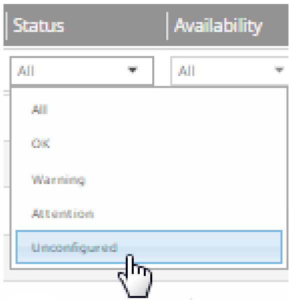
8.2 View an unconfigured computer's logs

You can view logs for unconfigured computers. Unconfigured computers do not have any backup jobs.

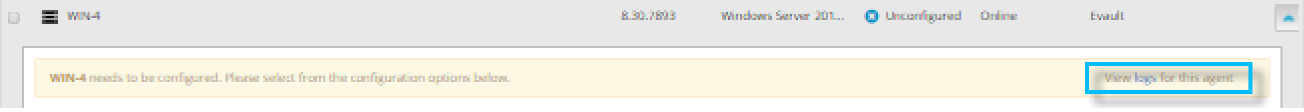
To view an unconfigured computer's logs:

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

   The Computers page shows registered computers. To only show unconfigured computers, click "Unconfigured" in the **Status** filter.



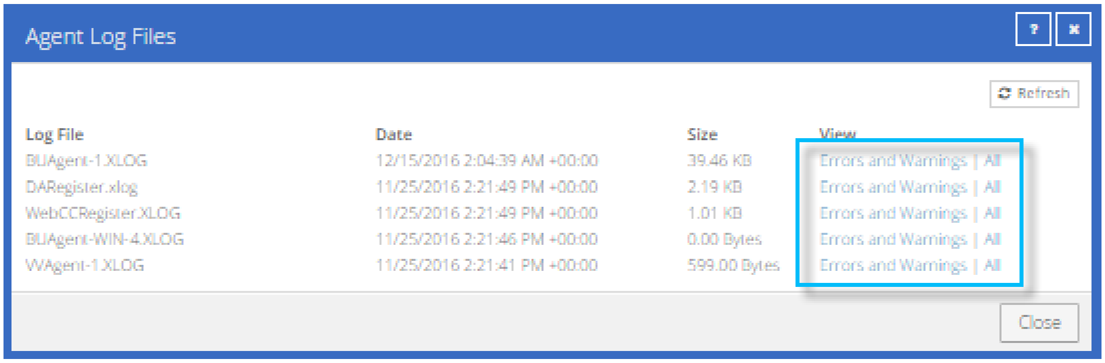
2. Find the unconfigured computer, and expand its view by clicking the computer row.



WIN-4 needs to be configured. Please select from the configuration options below.

3. Click the **logs** link for the unconfigured computer.

   The Agent Log Files window shows a list of logs for the computers. Links to the logs appear at the right side of the window.

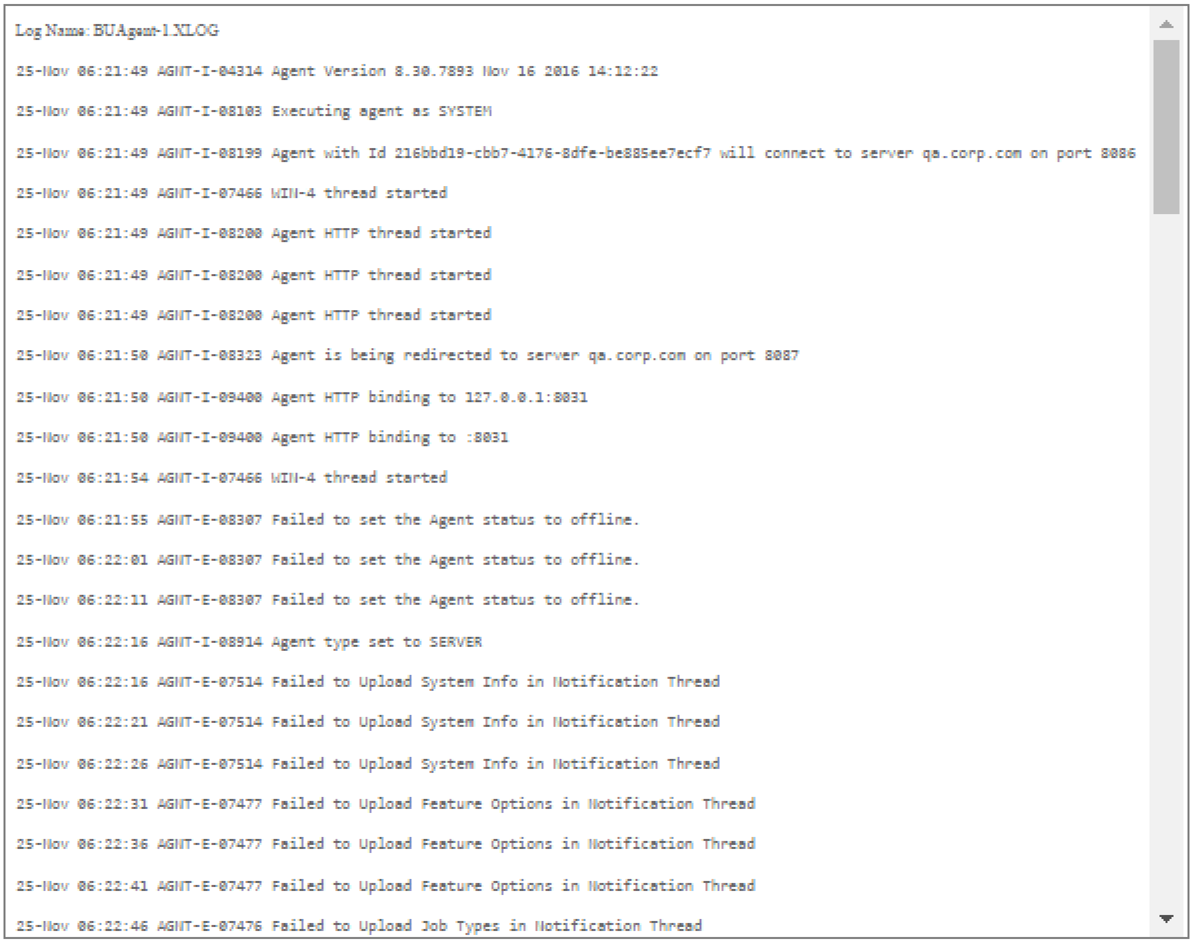


Log File	Date	Size	View
BUAgent-1.XLOG	12/15/2016 2:04:39 AM +00:00	39.46 KB	Errors and Warnings | All
DARegister.xlog	11/25/2016 2:21:49 PM +00:00	2.19 KB	Errors and Warnings | All
WebCCRegister.XLOG	11/25/2016 2:21:49 PM +00:00	1.01 KB	Errors and Warnings | All
BUAgent-WIN-4.XLOG	11/25/2016 2:21:46 PM +00:00	0.00 Bytes	Errors and Warnings | All
VVAgent-1.XLOG	11/25/2016 2:21:41 PM +00:00	599.00 Bytes	Errors and Warnings | All

4. Do one of the following:

   - To only view errors and warnings in a log, click **Errors and Warnings** for the log.
   - To view an entire log, click **All** for the log.

   The log appears in a new browser tab.



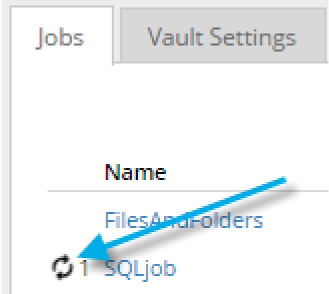
```
Log Name: BUAgent-1.XLOG

25-Nov 06:21:49 AGNT-I-04314 Agent Version 8.30.7893 Nov 16 2016 14:12:22

25-Nov 06:21:49 AGNT-I-08103 Executing agent as SYSTEM

25-Nov 06:21:49 AGNT-I-08199 Agent with Id 216bbd19-cbb7-4176-8dfe-be885ee7ecf7 will connect to server qa.corp.com on port 8086

25-Nov 06:21:49 AGNT-I-07466 WIN-4 thread started

25-Nov 06:21:49 AGNT-I-08200 Agent HTTP thread started

25-Nov 06:21:49 AGNT-I-08200 Agent HTTP thread started

25-Nov 06:21:49 AGNT-I-08200 Agent HTTP thread started

25-Nov 06:21:50 AGNT-I-08323 Agent is being redirected to server qa.corp.com on port 8087

25-Nov 06:21:50 AGNT-I-09400 Agent HTTP binding to 127.0.0.1:8031

25-Nov 06:21:50 AGNT-I-09400 Agent HTTP binding to :8031

25-Nov 06:21:54 AGNT-I-07466 WIN-4 thread started

25-Nov 06:21:55 AGNT-E-08307 Failed to set the Agent status to offline.

25-Nov 06:22:01 AGNT-E-08307 Failed to set the Agent status to offline.

25-Nov 06:22:11 AGNT-E-08307 Failed to set the Agent status to offline.

25-Nov 06:22:16 AGNT-I-08914 Agent type set to SERVER

25-Nov 06:22:16 AGNT-E-07514 Failed to Upload System Info in Notification Thread

25-Nov 06:22:21 AGNT-E-07514 Failed to Upload System Info in Notification Thread

25-Nov 06:22:26 AGNT-E-07514 Failed to Upload System Info in Notification Thread

25-Nov 06:22:31 AGNT-E-07477 Failed to Upload Feature Options in Notification Thread

25-Nov 06:22:36 AGNT-E-07477 Failed to Upload Feature Options in Notification Thread

25-Nov 06:22:41 AGNT-E-07477 Failed to Upload Feature Options in Notification Thread

25-Nov 06:22:46 AGNT-E-07476 Failed to Upload Job Types in Notification Thread
```

8.3 View current process information for a job

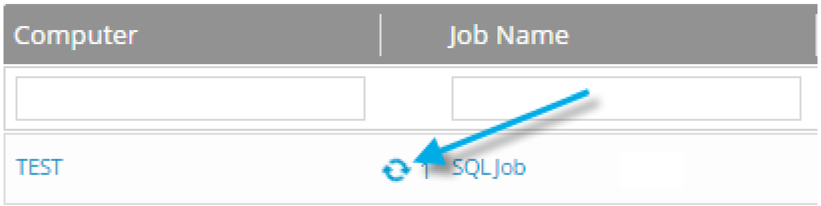
In the Process Details dialog box, you can view information about running, queued and recently-completed processes for a job. Processes include backups, restores and synchronizations. Process information is typically deleted within an hour after the process ends.

To view current process information for a job:

1. Do one of the following:
   - On the Computers page, on the Jobs tab, start a backup, restore or synchronization.
   - On the Computers page, on the Jobs tab, click the “In Progress” symbol ↻ beside the job name.

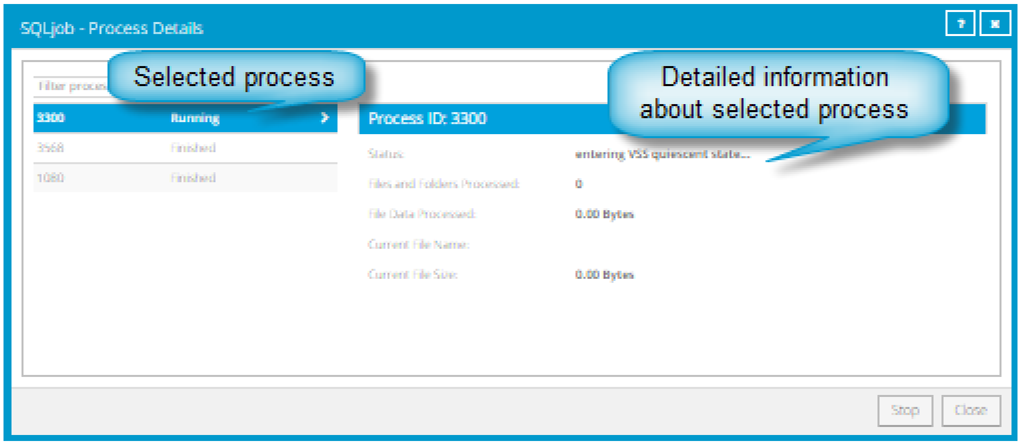


- On the Monitor page, click the "In Progress" symbol ⟳ beside the job name.



Computer	Job Name
TEST	⟳ 1 SQL Job

The **Process Details** dialog box lists processes that are running, queued and recently completed for the job. Detailed information is shown for the process that is selected on the left side of the dialog box.



3300	Running
3568	Finished
1080	Finished

Process ID: 3300

Status: entering VSS quiescent state...

Files and Folders Processed: 0

File Data Processed: 0.00 Bytes

Current File Name:

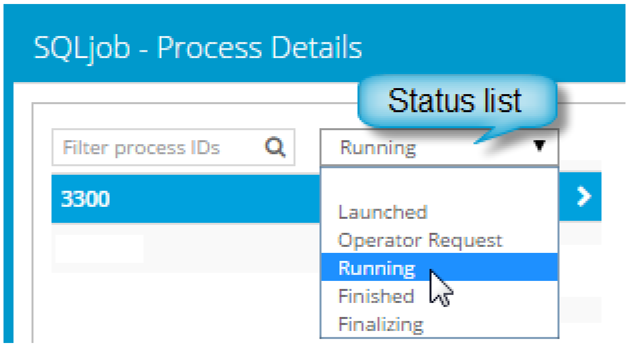
Current File Size: 0.00 Bytes

2. To view information about a different process, click the process on the left side of the dialog box.

   Detailed information for the process is shown at the right side of the dialog box.

3. To show only some processes in the dialog box, do one of the following in the status list:

   - To only show queued processes, click **Launched**.
   - To only show processes that are waiting for user action, click **Operator Request**.
   - To only show processes that are in progress, click **Running**.
   - To only show completed processes, click **Finished**.
   - To only show processes that are finishing, click **Finalizing**.



8.4 Monitor backups using email notifications

To make it easier to monitor backups, users can receive emails when backups finish or fail. Admin users and regular users in Portal can set up email notifications for a computer. See Set up email notifications for backups on a computer.

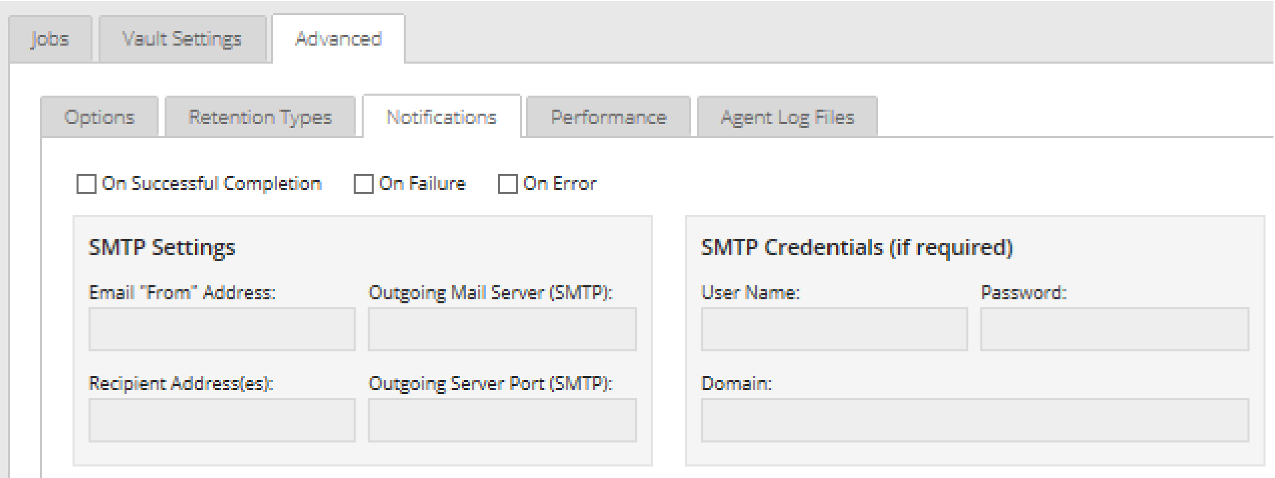
In some Portal instances, email notifications are configured centrally for vSphere Recovery Agent 8.40 or later, instead of separately for each computer. See .

8.4.1 Set up email notifications for backups on a computer

To set up email notifications for a computer:

1. On the navigation bar, click **Computers**.
2. Find the VRA for which you want to configure email notifications, and click the row to expand its view.
3. On the **Advanced** tab, click the **Notifications** tab.

   If the **Notifications** tab appears, but a policy is assigned to the VRA, you cannot change values on the **Notifications** tab. Instead, notifications can only be modified in the policy.



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.

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.

4. Click **Save**.

8.4.2 Set up email notifications for backups on multiple computers

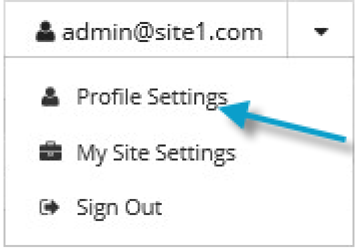
By default in some Portal instances, Admin users receive emails when backups fail, or are cancelled, deferred, missed or completed. Admin users can select backup statuses for which they want to receive email notifications. These email notifications are sent for vSphere Recovery Agent 8.40 or later, instead of separately for each computer.

For other computers, and in Portal instances where Admin users do not automatically receive email notifications, notifications must be configured separately for each computer. See Set up email notifications for backups on a computer.

To set up email notifications for backups on multiple computers:

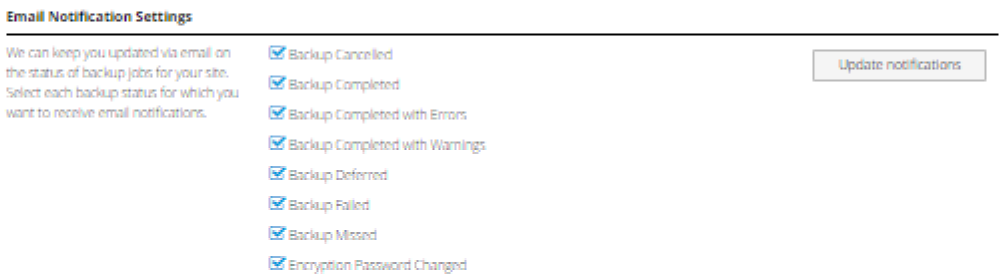
1. When signed in as an Admin user, click your email address at the top right of the Portal page.

   The user menu appears.



2. Click **Profile Settings**.

Your user profile appears. If your profile includes an Email Notification Settings section with a list of backup events (e.g., Backup Canceled, Backup Completed), you can select events for which you want to receive emails.



Email Notification Settings

We can keep you updated via email on the status of backup jobs for your site. Select each backup status for which you want to receive email notifications.

☑ Backup Canceled
☑ Backup Completed
☑ Backup Completed with Errors
☑ Backup Completed with Warnings
☑ Backup Deferred
☑ Backup Failed
☑ Backup Missed
☑ Encryption Password Changed

If Email Notifications Settings do not appear, you must set up notifications separately for each computer. See Set up email notifications for backups on a computer.

3. In the Email Notification Settings list, select any of the following events for which you want to receive emails:
   - Backup Cancelled
   - Backup Completed
   - Backup Completed with Errors
   - Backup Completed with Warnings
   - Backup Deferred
   - Backup Failed
   - Backup Missed
4. Click **Update notifications**.

8.5 View a job’s process logs and safeset information

To determine whether a backup or restore completed successfully, or to determine why a process failed, you can view a job’s process logs.

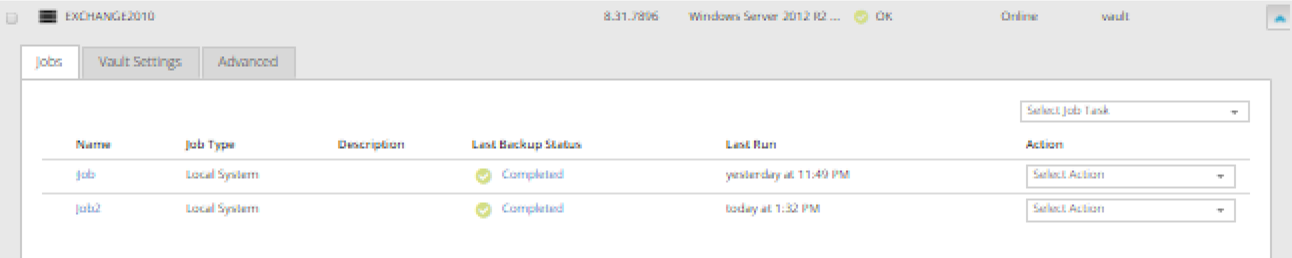
You can also view information about safesets created for the job. A safeset is an instance of backup data on the vault. For most Agents, one safeset is created by each successful backup.

To view a job’s process logs and safeset information:

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

   The Computers page shows registered VRAs.
2. Find the VRA for which you want to view logs, and click the row to expand its view.

   On the **Jobs** tab, the **Last Backup Status** column shows the status of each backup job.



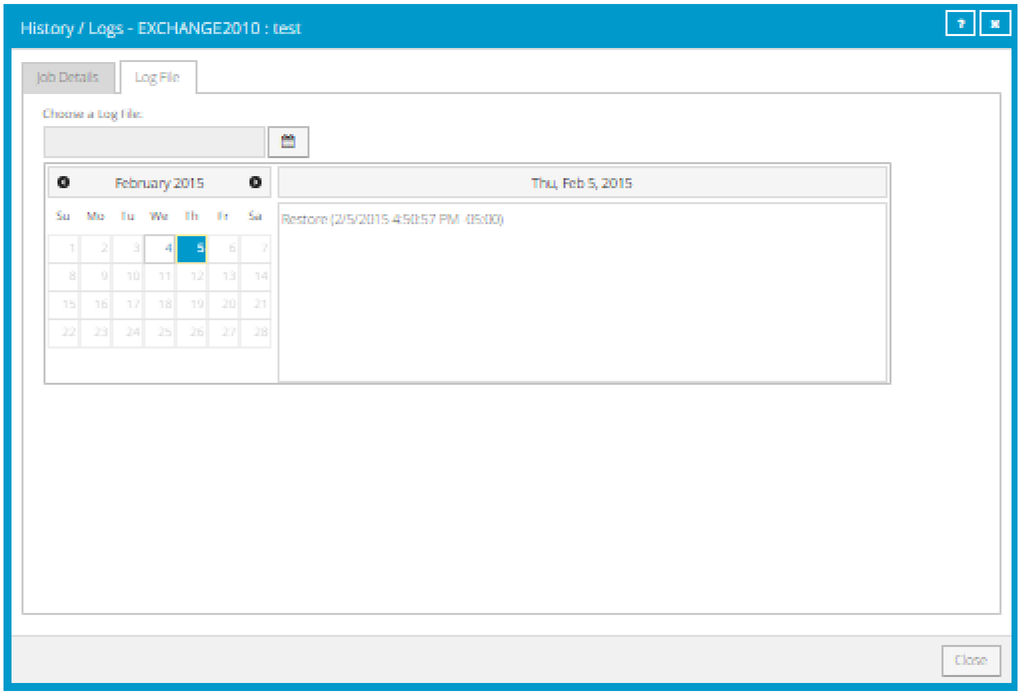
EXCHANGE2010 8.31.7896 Windows Server 2012 R2 ... OK Online vault

Name	Job Type	Description	Last Backup Status	Last Run	Action
Job	Local System		Completed	yesterday at 11:49 PM	Select Action
Job2	Local System		Completed	today at 1:32 PM	Select Action

3. To view log files for a job, do one of the following:

   - In the job’s **Select Action** menu, click **History / Logs**.
   - In the **Last Backup Status** column, click the job status.

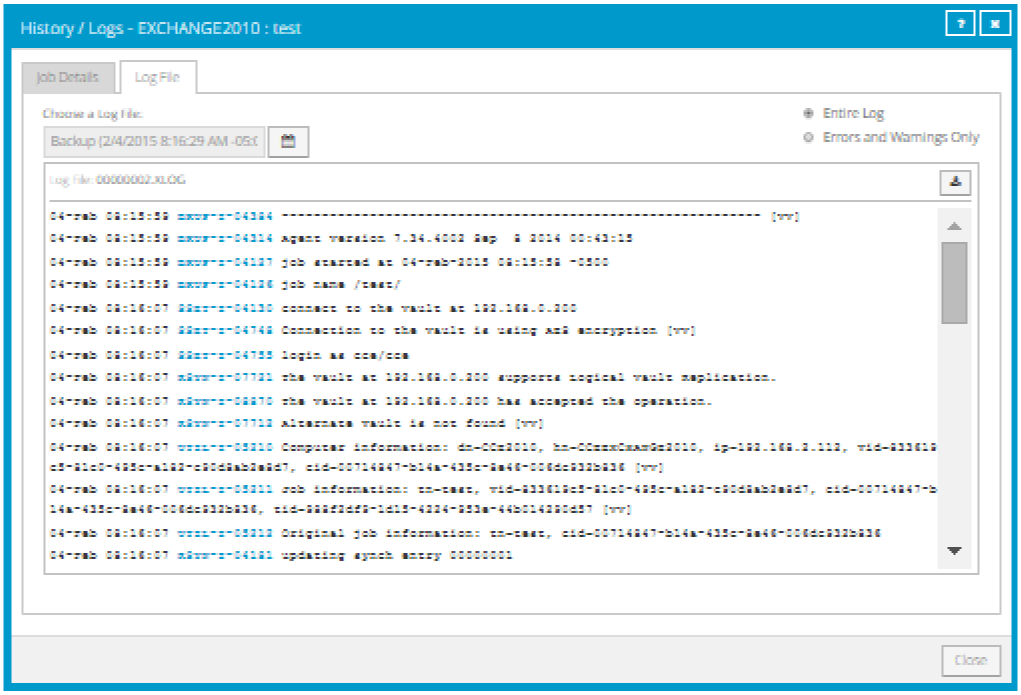
   The **History / Logs** window lists the most recent backups, restores and synchronizations on the computer.



Restore (2/5/2015 4:50:57 PM -05:00)

4. To view processes for a different day, click the calendar button. 📅 In the calendar that appears, click the date of the log that you want to view. In the list of processes on the selected date, click the process for which you want to view the log.

   The **History / Logs** window shows the selected log.



Choose a Log File:
Backup (2/4/2015 8:16:29 AM -05:(

● Entire Log
○ Errors and Warnings Only

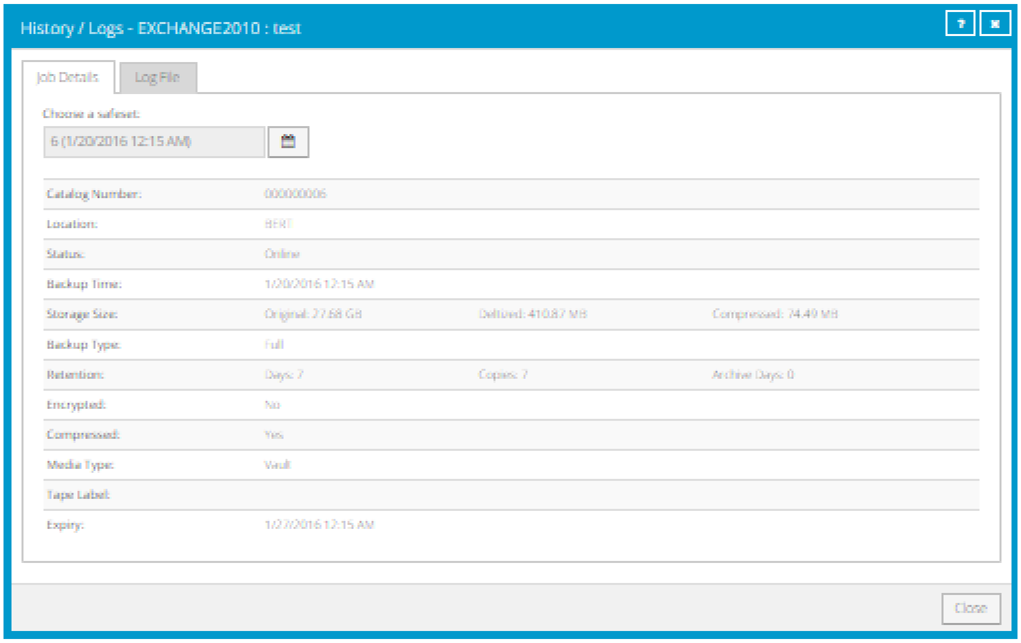
Log File: 00000002.XLOG

```
04-Feb 08:15:59 BKUP-I-04384 ------------------------------------------------------------ [vv]
04-Feb 08:15:59 BKUP-I-04314 Agent version 7.34.4002 Sep  8 2014 00:43:15
04-Feb 08:15:59 BKUP-I-04127 job started at 04-Feb-2015 08:15:58 -0500
04-Feb 08:15:59 BKUP-I-04126 job name /test/
04-Feb 08:16:07 SSET-I-04130 connect to the vault at 192.168.0.200
04-Feb 08:16:07 SSET-I-04748 Connection to the vault is using AES encryption [vv]
04-Feb 08:16:07 SSET-I-04755 login as ccs/ccs
04-Feb 08:16:07 ASYN-I-07721 the vault at 192.168.0.200 supports logical vault replication.
04-Feb 08:16:07 ASYN-I-06870 the vault at 192.168.0.200 has accepted the operation.
04-Feb 08:16:07 ASYN-I-07712 alternate vault is not found [vv]
04-Feb 08:16:07 UTIL-I-05210 Computer information: dn-CCm2010, hn-CCmsxCmsmGe2010, ip-192.168.2.112, vid-833619
c5-81c0-485c-a182-c80d8ab2e8d7, cid-00714847-b14a-435c-8a48-008dc832b836 [vv]
04-Feb 08:16:07 UTIL-I-05211 Job information: tn-test, vid-833619c5-81c0-485c-a182-c80d8ab2e8d7, cid-00714847-b
14a-435c-8a48-008dc832b836, sid-888f2df9-1d15-4224-853a-44b014280d57 [vv]
04-Feb 08:16:07 UTIL-I-05212 Original job information: tn-test, cid-00714847-b14a-435c-8a48-008dc832b836
04-Feb 08:16:07 ASYN-I-04181 updating synch entry 00000001
```

5. To only show errors and warnings in the log, click the **Errors and Warnings Only** option at the top right of the window.

6. To view safeset information for a particular backup, click the **Job Details** tab. The tab shows safeset information for the job's most recent backup.

   To view information for a different safeset, click the calendar button. 📅 In the calendar that appears, click the date of the backup for which you want to view information. In the list of backups on the selected date, click the backup for which you want to view information. The tab shows safeset information for the selected backup.



Choose a safeset:
6 (1/20/2016 12:15 AM)

Catalog Number:	000000006		
Location:	BERT		
Status:	Online		
Backup Time:	1/20/2016 12:15 AM		
Storage Size:	Original: 27.68 GB	Deltized: 410.87 MB	Compressed: 74.49 MB
Backup Type:	Full		
Retention:	Days: 7	Copies: 7	Archive Days: 0
Encrypted:	No		
Compressed:	Yes		
Media Type:	Vault		
Tape Label:			
Expiry:	1/27/2016 12:15 AM		

8.6 View and export recent backup statuses

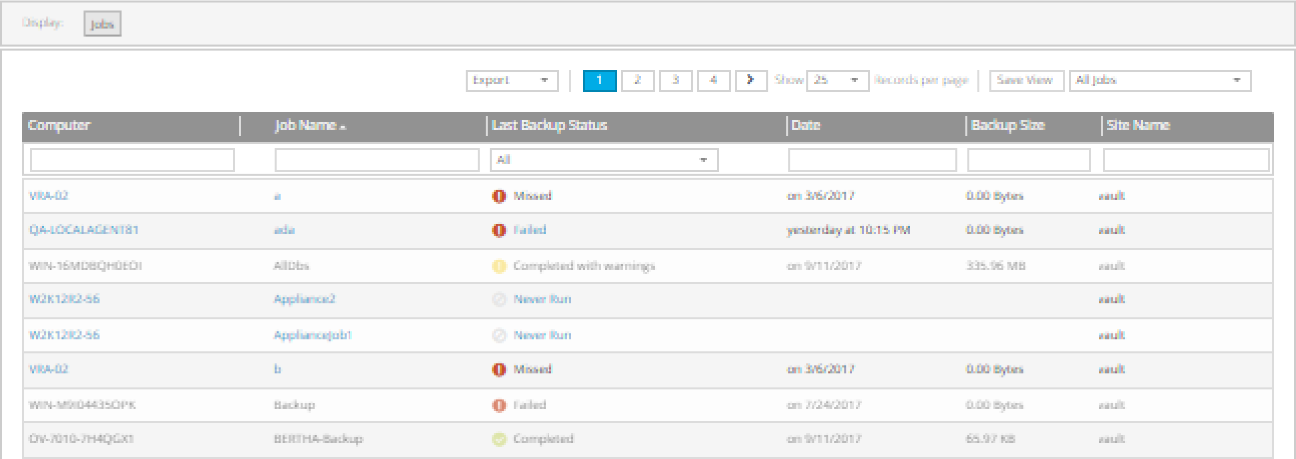
You can view recent backup statuses for computers on the Monitor page in Portal. You can also export the information in comma-separated values (.csv), Microsoft Excel (.xls), or Adobe Acrobat (.pdf) format.

From the Monitor page, you can navigate to related information on the Computers page or in the Logs window.

To view and export recent backup statuses:

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

   The Monitor page shows recent backup statuses for jobs in your site.



Computer	Job Name	Last Backup Status	Date	Backup Size	Site Name
		All			
VRA-02	a	Missed	on 3/6/2017	0.00 Bytes	vault
QA-LOCALAGENT81	ada	Failed	yesterday at 10:15 PM	0.00 Bytes	vault
WIN-16MDBQHOEOI	AllDbs	Completed with warnings	on 9/11/2017	335.96 MB	vault
W2K12R2-56	Appliance2	Never Run			vault
W2K12R2-56	Appliancejob1	Never Run			vault
VRA-02	b	Missed	on 3/6/2017	0.00 Bytes	vault
WIN-M9I04435OPK	Backup	Failed	on 7/24/2017	0.00 Bytes	vault
OV-7010-7H4QGX1	BERTHA-Backup	Completed	on 9/11/2017	65.97 KB	vault

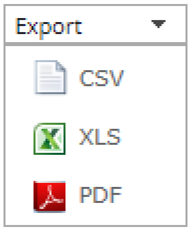
2. To change which backup statuses appear on the page, click the views list at the top of the page, and then click the view that you want to apply.

3. To view information for a job or computer on the Computers page, click the name of an online computer or job.

4. To view the job's logs in the History/Logs window, click the job's last backup status.

5. To export backup status information from the page, click the **Export** box. In the list that appears, click one of the following formats for the exported data file:

   - CSV (comma-separated values)
   - XLS (Microsoft Excel)
   - PDF (Adobe Acrobat)

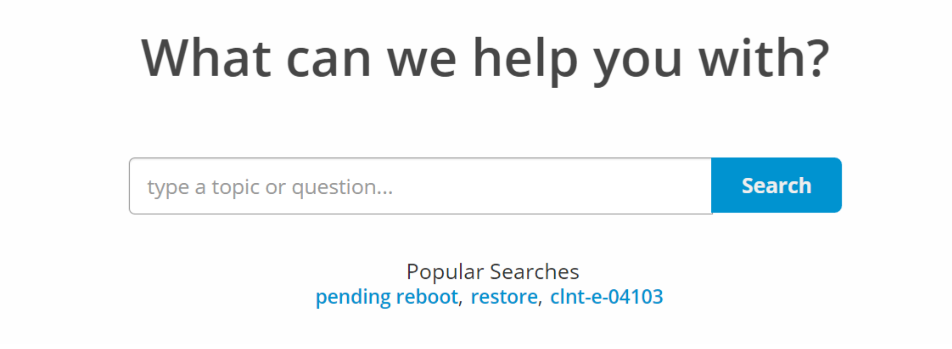


   The data file is downloaded to your computer in the specified format.

9 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?

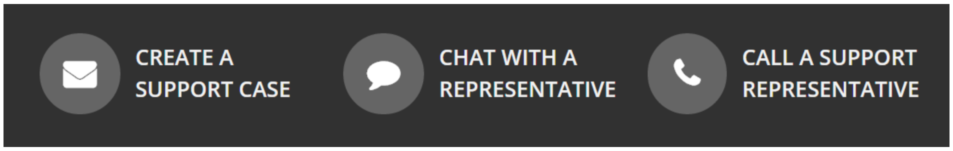
type a topic or question...

Search

Popular Searches
pending reboot, restore, clnt-e-04103

9.1 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.

To gather log files, click **File** menu and choose *Open log folder*. Compress the contents of the folder in a .zip file and attach it to your support request.

If the log archive and/or mail store 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.