



Carbonite Server Backup Secondary Restore Server 8.4

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, and Carbonite Server Backup, Carbonite Server Backup SaaS, and Carbonite Server Backup DeltaPro, 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	July 2018	Initial guide provided for Secondary Restore Server 8.4x.

Contents

1	Introduction	4
1.1	Prerequisites.....	4
1.2	Run Secondary Restore Server	4
1.3	Restore Secondary Restore Server data using Portal.....	6
1.4	Restore Secondary Restore Server data using CentralControl.....	7
2	Carbonite Server Backup Support	9
2.1	Contacting Carbonite.....	9

1 Introduction

Using Secondary Restore Server, you can restore backup data from a detached secondary storage pool to the original or to another computer. The vault is not required to complete the restore, and a vault license is not required.

After mounting a secondary storage pool location using Secondary Restore Server, use Portal or Windows CentralControl to add the Secondary Restore Server as a vault for an Agent. You can then perform a **Restore from another computer**. You must know the encryption password to recover encrypted data.

The device with the secondary storage pool, such as a USB drive, must be local to or mapped on the computer where you run Secondary Restore Server. You cannot enter or choose a UNC location when mounting a secondary storage location.

1.1 Prerequisites

Microsoft .NET Framework version 4.5 must be installed and running before you can use the Secondary Restore Server.

Do not run other vault services or applications on the computer where you run Secondary Restore Server.

1.2 Run Secondary Restore Server

When you run Secondary Restore Server, executable files are copied to the hard disk. By default, Secondary Restore Server files are saved in the temp directory defined by an environment variable on your computer (e.g., C:\Users\Administrator\AppData\Local\Temp\SecondaryRestoreServer).

After you exit from Secondary Restore Server, application files do not remain on disk. Only the following files remain in the SecondaryRestoreServer directory:

- vaultDB.cfg - stores vault settings
- RestoreServerInstall.log - records Secondary Restore Server activity and errors.

You need Administrator rights to run Secondary Restore Server.

To run Secondary Restore Server:

1. Double-click the Secondary Restore Server executable on the computer with a local or mapped secondary storage pool location.

The Secondary Restore Server dialog box appears.

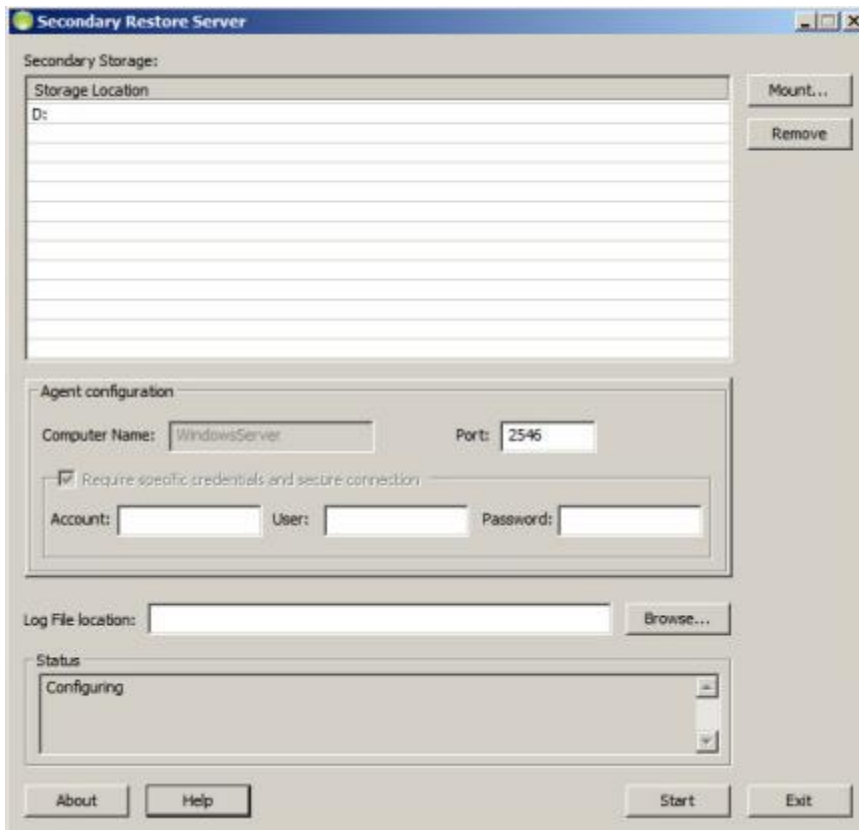
2. Click **Mount**. In the **Browse for Folder** dialog box, select the location with the secondary storage pool that you want to make available for restores, and then click **OK**.

If the secondary storage location is on a different machine than the Secondary Restore Server, the network drive must be mapped on the machine where the Secondary Restores Server is running. You cannot enter or choose a UNC location for mounting a secondary storage location.

Note: Repeat this step for each secondary storage pool location that you want to make available for restores.

- Complete the following fields in the **Secondary Restore Server** dialog box:

Field	Description
Port	The port used to communicate with the secondary storage location.
Account	The account for connecting to the secondary storage.
User	The user name for connecting to the secondary storage.
Password	The password for connecting to the secondary storage.
Log File location	Location for Secondary Restore Server logs. Click Browse to select a location.



- Click **Start**.

Secondary Restore Server makes data in the specified storage locations available for restore.

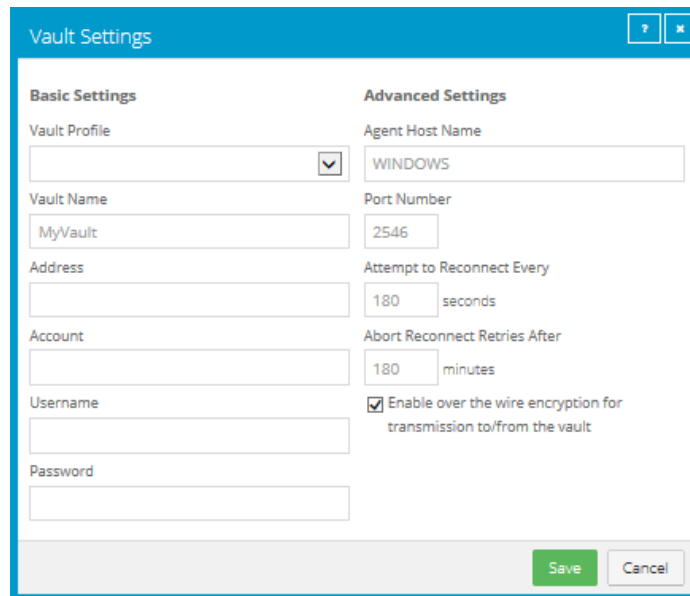
- (Optional) To remove a secondary storage pool location, click the secondary storage location, and then click **Remove**.
- To stop running Secondary Restore Server, click **Exit**.

1.3 Restore Secondary Restore Server data using Portal

To restore Secondary Restore Server data using Portal:

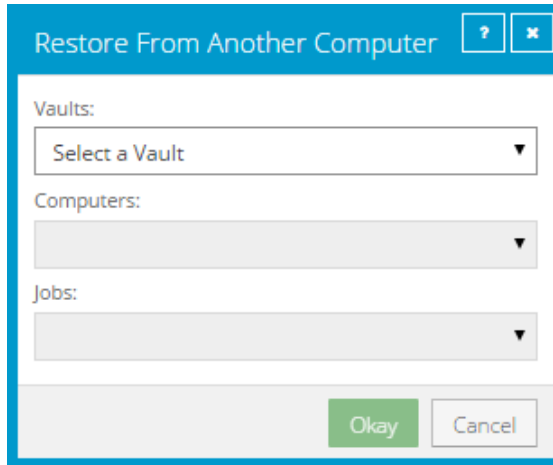
1. On the navigation bar, click **Computers**.
2. Click a computer row to expand its view.
3. Click the **Vault Settings** tab.
4. On the Vault Settings tab, click **Add Vault**.

The Vault Settings dialog box appears.



5. In the **Vault Name** field, enter a name for the Secondary Restore Server connection.
6. In the **Address** field, enter the IP address of the Secondary Restore Server.
7. In the **Account**, **Username**, and **Password** fields, enter an account and credentials for connecting to the Secondary Restore Server.
8. Click **Save**.
9. Click the **Jobs** tab.
10. In the **Job Tasks** menu, click **Restore from Another Computer**.

The Restore From Another Computer dialog box appears.



11. In the **Vaults** list, select the Secondary Restore Server connection.
12. In the **Computers** list, select the computer.
13. In the **Jobs** list, select the job from which you want to restore data.
14. Click **Okay**.
15. Complete the restore.

1.4 Restore Secondary Restore Server data using CentralControl

To restore Secondary Restore Server data using CentralControl:

1. In CentralControl, right-click an Agent in the left pane and select **Agent Configuration** from the menu.
2. Click the **Vaults** tab and then click **New**.
3. In the Vault Configuration wizard, click **Next**.
4. Select **Register as a new computer**, and then click **Next**.
5. In the **Profile name for the new vault** field, enter a vault profile name, and then click **Next**.
6. In the **New address** field, enter the IP address of the Secondary Restore Server and click **Add**.
7. Click **Next**.
8. In the **New ports** field, enter the port number of the Secondary Restore Server and click **Add**.
9. Click **Next**.
10. Select the reconnection and encryption settings and click **Next**.
11. Enter authentication information for connecting to the Secondary Restore Server and click **Next**.
12. Click **Finish**.

13. In the left pane, click the Agent.
14. Go to **Actions > Restore from another computer**.
15. Complete the Restore from Another Computer wizard.
16. Click **Finish**.

2 Carbonite Server Backup Support

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

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

What can we help you with?

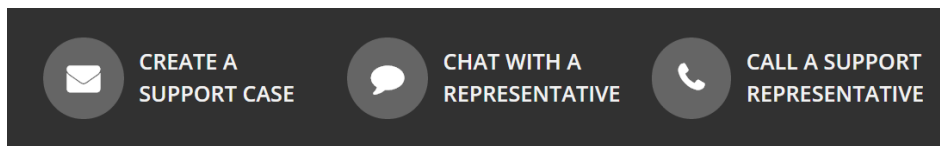
Search

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

2.1 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.