



# Carbonite Server Backup

## Director 8.3

### Installation Guide



© 2017 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](http://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	December 2017	Guide provided for Director 8.3x general availability.

## Contents

<b>1</b>	<b>Overview .....</b>	<b>5</b>
1.1	Installation requirements.....	5
1.1.1	Ports .....	5
1.1.2	Permissions for running Director services .....	5
1.1.3	Windows optimization for background services.....	6
<b>2</b>	<b>Install a standard vault .....</b>	<b>7</b>
2.1	Specify an IP address or FQDN for a vault in Azure.....	8
<b>3</b>	<b>Configure and install a Satellite vault .....</b>	<b>9</b>
3.1	Add a customer .....	9
3.2	Configure a Satellite vault on a Base vault.....	10
3.3	Install a Satellite vault .....	10
3.4	Replace a failed Satellite vault .....	12
<b>4</b>	<b>Install the Director UI .....</b>	<b>13</b>
<b>5</b>	<b>Silently install or upgrade a vault .....</b>	<b>14</b>
5.1	Record a response file .....	14
5.2	Run a silent installation or upgrade .....	14
<b>6</b>	<b>Set up data replication between vaults .....</b>	<b>16</b>
6.1	Set up One-to-One (1:1) replication.....	16
6.1.1	Install an Active vault .....	16
6.1.2	Install a Passive vault.....	17
6.1.3	Set up the connection between the Active and Passive vault .....	18
6.2	Set up Many-to-One (N:1) replication.....	18
6.3	Set up Many-to-One-to-One (N:1:1) replication .....	19
6.3.1	Install an Active Base vault.....	19
6.3.2	Install a Passive Base vault .....	20
6.3.3	Set up the connection between the Active and Passive Base vaults .....	21
6.3.4	Install one or more Satellite vaults .....	21
<b>7</b>	<b>Upgrade a vault.....</b>	<b>22</b>
7.1	Upgrade a vault .....	22

7.2	Upgrade vaults for data replication .....	23
7.2.1	Upgrade standalone vaults for replication.....	23
7.2.2	Upgrade vaults in 1:1 replication .....	24
7.2.3	Upgrade vaults in N:1 replication.....	25
<b>8</b>	<b>Upgrade from Windows 2012 R2 to Windows 2016 on a server where Director 8.30 is installed.....</b>	<b>26</b>
8.1	Recover from a failed Windows upgrade.....	28
<b>9</b>	<b>Uninstall a vault .....</b>	<b>30</b>
<b>10</b>	<b>Carbonite Server Backup Support .....</b>	<b>31</b>
10.1	Contacting Carbonite.....	31

# 1 Overview

This guide includes procedures for installing:

- Standard vaults. You can use a standard vault as a standalone vault that does not replicate data to or receive data from another vault. You can also set up replication between a standard vault and another vault. See [Install a standard vault](#).
- Satellite vaults. A Satellite vault is installed at a customer location to allow for quick, local backups. Backups are then replicated to a standard vault in the cloud or in a secondary location in the customer's environment. See [Configure and install a Satellite vault](#).
- Director UI, the graphical user interface (GUI) for managing vaults, on its own. See [Install the Director UI](#). The Director UI is also installed when you install a vault.

The guide also includes information and procedures for:

- Silently installing and upgrading vaults. See [Silently install or upgrade a vault](#).
- Setting up data replication between vaults. See [Set up data replication between vaults](#).
- Upgrading and uninstalling vaults. See [Upgrade a vault](#) and [Uninstall a vault](#).

For supported platforms and prerequisites, see the Director release notes.

## 1.1 Installation requirements

For information about supported platforms and other prerequisites, see the Director release notes.

### 1.1.1 Ports

The following table lists ports used by Director:

Port	Direction	Protocol	Description
809	Inbound	TCP	Admin Service (communication with the Director UI and Vault API).
2546, 807	Inbound	TCP	Listener ports for backups and restores.
2547/12547	Outbound	TCP	Command and data ports on a source vault in replication.
2547/12547	Inbound	TCP	Command and data ports on a target vault in replication.

*Note:* For Web Reporting System programs, the vault allows outbound connections (usually TCP port 1433).

### 1.1.2 Permissions for running Director services

Each Director installation requires an Administrator account for running Director services. The Director installation process can automatically create a local VaultService account, or you can choose an existing account.

The Administrator account must have sufficient privileges to run the Director services (i.e., "Log on as a service"). The Director installation will fail if these privileges are not provided. Please ensure that the account and any relevant domain policies are configured properly before proceeding with the installation.

### **1.1.3 Windows optimization for background services**

For best Director performance, optimize Windows performance for background services.

## 2 Install a standard vault

A standard vault can act as a standalone vault that does not replicate data to or receive data from another vault. You can also set up replication between a standard vault and another vault. See [Set up data replication between vaults](#).

When you install a standard vault, SQL Server Express 2014 SP2 (64-bit) is installed as the vault database.

After installing a standard vault, you must activate vault licenses. See the *Director User Guide* or online help.

You can install a standard vault on a virtual machine (VM) in Microsoft Azure. The Director installer detects when a vault is being installed on a VM in Azure, and creates a primary storage location for all attached drives, except C and D. The maximum supported size for a vault in Azure is 12 TB.

After installing a vault in Azure, you must specify an externally-available IP address or fully-qualified domain name (FQDN) for connections for backups, restores and replication, and from the Director UI. See [Specify an IP address or FQDN for a vault in Azure](#).

To install a standard vault:

1. Double-click the Director installation kit.
2. On the Welcome page, click **Next**.
3. On the release notes page, click **Next**.
4. Read the software license agreement. Select **Accept**, and then click **Next**.
5. On the installation type page, select **Non-clustered vault**, and then click **Next**.
6. On the vault type page, select **Standard Vault**, and then click **Next**.
7. On the vault license page, enter the vault license key that you received from your service provider, and then click **Next**.
8. On the destination location page, choose the installation location for Director files, and then click **Next**.
9. On the primary storage locations page, choose All Local Disks or a specific disk for storing vault data, and then click **Next**.
10. On the vault database page, specify locations for the vault database engine and data files, and then click **Next**.
11. On the email notifications page, specify whether Director will send email notifications when a job fails or is successful, and then click **Next**.  
  
If emails will be sent when tasks fail or succeed, the notification recipients page appears. Enter a comma-separated list of email addresses for sending notifications, and then click **Next**.
12. On the account for running Director services page, do one of the following:
  - To automatically create a local Administrator account named “VaultService” for running Director services, select **Create an account automatically**, and then click **Next**.

- To specify a custom Administrator account for running Director services, select **Use a custom account**. Enter account information in the **Username** and **Password** fields, and then click **Next**.

For more information, see [Permissions for running Director services](#).

13. After Director is installed, click **Finish**.

If you installed a vault in Azure, you must specify an externally-available IP address or fully-qualified domain name (FQDN) for connections for backups, restores and replication, and from the Director UI. See [Specify an IP address or FQDN for a vault in Azure](#).

## 2.1 Specify an IP address or FQDN for a vault in Azure

After installing a vault on a virtual machine (VM) in Microsoft Azure, you must specify an externally-accessible IP address or fully-qualified domain name (FQDN) for connections for backups, restores and replication, and from the Director UI.

To specify an IP address or FQDN for a vault in Azure, run the following command on the vault:

```
vaultop update_node_in_cluster
externalAddress:<external_IPaddress_or_FQDN>
internalAddress:<internal_IPaddress_or_FQDN>
```

Specify the same externally-accessible IP address or FQDN for the *external\_IPaddress\_or\_FQDN* and *internal\_IPaddress\_or\_FQDN* parameters.



## 3 Configure and install a Satellite vault

A Satellite vault is installed at a customer location, to allow for quick, local backups. Backups are then replicated to a standard vault in the cloud or in a secondary location in the customer's environment.

Before installing a Satellite vault, you must install a Base vault for N:1 replication, or Active and Passive Base vaults for N:1:1 replication. See [Set up Many-to-One \(N:1\) replication](#) and [Set up Many-to-One-to-One \(N:1:1\) replication](#).

Then, for each Satellite vault that you want to install, do the following:

- a. Add a customer on the Base vault or Active Base vault. See [Add a customer](#).
- b. Configure a Satellite vault on the Base vault or Active Base vault. When you configure a Satellite vault, the Base vault provides an authorization key. When installing a Satellite vault, you must enter an authorization key from a Base vault instead of entering a license key. See [Configure a Satellite vault on a Base vault](#).
- c. Install the Satellite vault. See [Install a Satellite vault](#).

If a Satellite vault fails, you can install a new Satellite vault to replace it. See [Replace a failed Satellite vault](#).

*Note:* In procedures in this section, the term "Base vault" refers to Base vaults in N:1 replication and Active Base vaults in N:1:1 replication.

### 3.1 Add a customer

Before you can install a Satellite vault, a customer for the Satellite vault must be created on the Base vault or Active Base vault. When you create a customer, you must also create a location, account and user.

To add a customer:

1. In the left pane of the Director UI, expand the Base vault where you want to add a customer.
2. Right-click Manage Customers/Orgs, Safesets, Tasks, and select **Add New Customer**.
3. On the Welcome page of the New Organization/Customer wizard, click **Next**.
4. On the General Organization/Customer Information page, type the customer's name and address, and click **Next**.
5. On the Contact Information page, type the customer's phone number, email address, website, and contact person, and then click **Next**.
6. On the Default Location page, type a default location name and code, and then click **Next**.
7. On the Account and User Information page, type an account name, user name, and user password, and then click **Next**.

*Note:* The account name must be unique across the entire vault.

*Note:* The maximum password length is 32 characters.

8. On the Account Base Operating Mode page, select the operating mode for the account.

9. On the Account Storage Locations page, do one of the following:
  - If you do not want to select storage areas for the account, click **Next**. You can do this later.
  - If you want to select a secondary storage and/or archive storage location, and then click **Next**.  
To create a secondary or archive storage group, click **Storage locations**. In the Storage Locations dialog box, add secondary and/or archive storage group and locations. For more information, see the *Director User Guide* or online help.
10. On the Customer Quotas page appears, select each feature (Storage, or a type of Agent or plug-in) and click **Set Quota**. In the Organization/Customer Quota dialog box, select **Unlimited** or enter a quota number for the customer in the **Set quota** area.
11. Click **Finish**.

## 3.2 Configure a Satellite vault on a Base vault

After installing appropriate licenses and creating a customer, you can configure a Satellite vault on the Base vault or Active Base vault.

When you configure a Satellite vault, the Base vault provides an authorization key (previously known as the OTRK). When installing a Satellite vault, you must enter the authorization key.

To configure a Satellite vault on a Base vault:

1. In the Director UI, click the Base vault.  
The Base vault must be licensed for Many to one (N:1) replication.
2. In the **Base Replication** menu, click **Configure Satellites**.
3. In the Satellite Vaults Configuration dialog box, click **New**.
4. In the **Select the customer that will use this Satellite vault** list, select the customer. Only one customer can be associated with a Satellite vault.
5. In the **Select quota for this Satellite vault** field, select a Satellite vault storage quota. Available storage quotas are determined by the Satellite vault licenses added on the Base vault.
6. Record the authorization key. You use this key when installing a Satellite vault.
7. Click **OK**.
8. Click **Close**.

## 3.3 Install a Satellite vault

After configuring a Satellite vault on a Base vault or Active Base vault, you can install a Satellite vault.

When you install a Satellite vault, you must enter the authorization key that was generated when you configured the Satellite vault on the Base vault.

When you install a Satellite vault, SQL Server Express 2014 (64-bit) SP2 is installed as the vault database.

To install a Satellite vault:

1. Double-click the Director installation kit.
2. On the Welcome page, click **Next**.
3. On the release notes page, click **Next**.
4. Read the software license agreement. Select **Accept**, and then click **Next**.
5. On the installation type page, select **Non-clustered vault**, and then click **Next**.
6. On the vault type page, click **Satellite vault**, and then click **Next**.
7. On the destination location page, choose the installation location for Director files, and then click **Next**.
8. On the primary storage locations page, choose All Local Disks or a specific disk for storing vault data, and then click **Next**.
9. On the vault database page, specify locations for the vault database engine and data files, and then click **Next**.
10. On the email notifications page, specify whether Director will send email notifications when a job fails or is successful, and then click **Next**.

If emails will be sent when tasks fail or succeed, the notification recipients page appears. Enter a comma-separated list of email addresses for sending notifications, and then click **Next**.

11. On the Director services account page, do one of the following:
  - To automatically create a local Administrator account named “VaultService” for running Director services, select **Create account automatically**.
  - To specify a custom Administrator account for running Director services, select **Use a custom account**. Enter account information in the **Username** and **Password** fields.

For more information, see [Permissions for running Director services](#).

12. Click **Next**.

Director is installed. SQL Server Express is also installed for the vault database.

13. On the Register the Satellite Vault to a Base Vault page, do the following:
  - In the **Base vault address** field, enter the Base vault address.
  - In the **TCP Port** field, enter the port number that the Satellite vault will use to communicate with the Base vault.

You can find this port in the Base vault’s Vault Settings dialog box, on the Replication tab, in the **Command channel port** field.
  - In the **Authorization key** field, enter the Base vault authorization key.

The authorization key (previously known as the OTRK) is provided when you configured the Satellite vault on the Base vault. See [Configure a Satellite vault on a Base vault](#).

14. On the Registration Confirmation page, click **Next**.

15. Click **Finish**.

## 3.4 Replace a failed Satellite vault

To replace a failed Satellite vault:

1. Select the Base vault or Active Base vault in the left pane of the Director UI.
2. Click **Base Replication** and select **Configure Satellites**.
3. Select the failed Satellite vault and click **Edit**.
4. Click the **Advanced** tab and select **Bypass Satellite**.
5. Click **OK**.
6. Select the failed Satellite vault and click **Edit**.
7. Click **Reset Key** and record the new authorization key. Click **OK**.
8. Click **Close**.
9. Uninstall the Satellite vault.
10. Install the new Satellite vault. Use the new authorization key and previous IP address. Allow replication to finish.
11. Select the Active Base vault in the left pane of the Director UI.
12. Click **Base Replication** and select **Configure Satellites**.
13. Select the Satellite vault and click **Edit**.
14. Click the **Advanced** tab and select **Normal Operation**. Click **OK**.
15. Click **OK** again.
16. Click **Close**.

## 4 Install the Director UI

You can install the Director UI, the graphical user interface (GUI) for managing vaults, without installing a vault. See. The Director UI is also installed when you install a vault.

A license is not required when you install the Director UI without installing the vault.

To install the Director UI only:

1. Double-click the Director installation kit.
2. On the Welcome page, click **Next**.
3. On the release notes page, click **Next**.
4. Read the software license agreement. Select **Accept**, and then click **Next**.
5. On the installation type page, select **Director UI only**, and then click **Next**.
6. On the destination location page, choose the location for installing Director UI files, and then click **Next**.
7. Click **Finish**.

## 5 Silently install or upgrade a vault

You can silently install or upgrade a vault. For supported upgrade paths, see the Director release notes.

A silent installation or upgrade does not require user interaction, and does not display any indication of its progress.

To silently install or upgrade a vault, do the following:

- a. [Record a response file](#)
- b. [Run a silent installation or upgrade](#)

### 5.1 Record a response file

To silently install a vault, you must first create an InstallShield response file. The response file is a text file that stores user options for the installation or upgrade.

After creating a response file, you can edit options in the file. For example, you can change the license key and installation folder in a response file.

*Note:* Sample response files are available. For more information, contact Support.

*Note:* Installations and upgrades require separate response files. A response file that is generated for a fresh installation cannot be used for an upgrade.

To record the response file:

1. At a command prompt, run the following command:

```
<DirectorInstallationKit> /r /f1c:\<responseFileName>.iss
```

2. Complete the installation wizard, selecting all options that you want to record for the silent installation or upgrade.

### 5.2 Run a silent installation or upgrade

After creating a response file, you can silently install or upgrade a Director vault. For supported upgrade paths, see the Director release notes.

A silent installation creates a new account named VaultService with administrative privileges. Vault services run under this account. The installation fails when you attempt to run services with a custom account.

Online activation is the only supported method of validating licenses during a silent installation. If the vault cannot access the activation server, the installation fails. There is no license validation for Satellite vaults in interactive or silent mode.

The installer returns zero for a successful installation and a return code when the installation fails or requires a reboot to complete. If the installation fails, the reason for the failure is added to the log file. If the installation requires a reboot to complete, the installer returns the value 3010.

After a Satellite vault silent installation, register the Satellite vault to a Base vault using the `replvault regsat` command. For more information, see the *Director User Guide* or online help.

Before an upgrade, we recommend bringing the vault offline. You can do this using the `vaultop` command. For more information, see the *Director User Guide* or online help.

To run a silent installation or upgrade, run the following command from a command prompt:

```
Director-8-3x-xxxx.exe /s /f1.\<responseFileName>.iss [KeepBackup]
[NoRegSAT] [NoAutoReboot] [NoOnline]
```

Where:

- `Director-8-3x-xxxx.exe` — the Director installation kit filename
- `<responseFileName>.iss` — the response file for the silent installation. The `.\` after `/f1` indicates that the response file is located in the same folder as the installer
- `KeepBackup` — Optional parameter. Keeps backup files and folders after the installation.
- `NoRegSAT` — Required for the installation of a Satellite vault. Removes the option to register the Satellite vault with the Base vault.
- `NoAutoReboot` — Optional parameter. When specified, the machine does not automatically restart after the installation if there is a pending reboot (when one or more files to be replaced were locked). If specified, the installer returns a value of 3010 if a reboot is required. Without this parameter, the system reboots automatically after the installation if there is a pending reboot.
- `NoOnline` — Optional parameter. When this parameter is specified, the installer will not request a transition of the node to Online when installation completes. This will prevent the node from coming Online and possibly starting new backup or restore operations prior to executing other manual upgrade operations. You can manually request an Online transition using the `vaultop` command. When this parameter is not specified, the system will automatically request transition to an Online state after a successful installation. In this case, the system will transition to the Online state when the services are restarted (after successful install, or after a pending reboot).

## 6 Set up data replication between vaults

To ensure that data is available for restore even if one vault is offline or unavailable, backup data can be replicated from one vault to another. This section describes how to set up:

- One-to-one (1:1) replication. In this configuration, which is typically used for Offsite Replication Services (ORS), data is replicated from an Active vault to a Passive vault.

For 1:1 replication, you must install and configure two standard vaults. See [Set up One-to-One \(1:1\) replication](#).

- Many-to-one (N:1) replication. In this configuration, which is typically used for Managed Service Providers (MSPs), data is replicated from Satellite vaults installed locally at customer locations to a Base vault in the cloud or at a secondary customer location.

For N:1 replication, you must install and configure one standard vault and one or more Satellite vaults. See [Set up Many-to-One \(N:1\) replication](#).

- Many-to-one-to one (N:1:1) replication. In this configuration, which is typically used for Cloud-Connected Service Providers (CCSPs), data is replicated from Satellite vaults to an Active Base vault and then to a Passive Base vault.

For N:1:1 replication, you must install and configure two standard vaults and one or more Satellite vaults. See [Set up Many-to-One-to-One \(N:1:1\) replication](#).

### 6.1 Set up One-to-One (1:1) replication

For 1:1 replication, you must install two standard vaults. One will be configured as the Active vault, and one will be configured as the Passive vault. The vaults must have approximately the same storage capacity.

To set up 1:1 replication between vaults, do the following:

- a. [Install an Active vault](#)
- b. [Install a Passive vault](#)
- c. [Set up the connection between the Active and Passive vault](#)

#### 6.1.1 Install an Active vault

When installing an Active vault for 1:1 replication, you must add a vault license and a Replication One to One license. You can then install a Passive vault, and add the same vault and Replication One to One license that is installed on the Active vault.

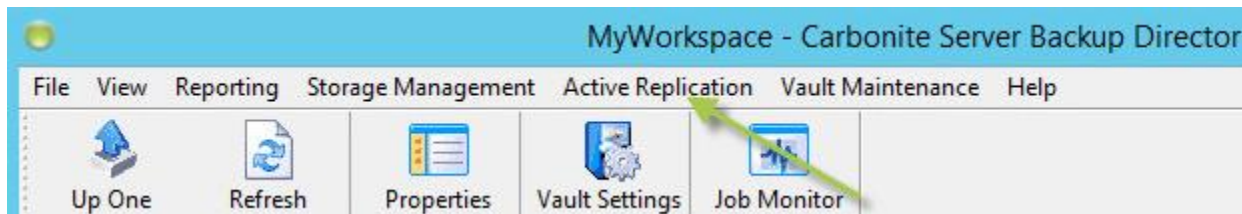
To install an Active vault:

1. Install a standard vault that will act as the Active vault. See [Install a standard vault](#).  
Data will be replicated from this vault to the Passive vault.
2. In the Director UI, add a vault connection for the Active vault.



- (If applicable) If the license you added during the installation did not include a Replication One to One license, add a Replication One to One license.

After a Replication One to One license is added, an Active Replication menu appears for the vault in the Director UI.



1:1 Replication services should be enabled automatically.

- Check that 1:1 replication services are enabled for the vault. Choose **Vault Settings** from the **Vault Maintenance** menu. On the Replication tab of the dialog box, ensure that the **Enable 1:1 replication services on 'vaultName'** check box is selected.

### 6.1.2 Install a Passive vault

When you install a Passive vault for 1:1 replication, you must add the same vault and Replication One to One licenses that are added on the Active vault.

The Active and Passive vaults must have approximately the same storage capacity. However, a Passive vault can require more storage space than an Active vault. When data is replicated after a safeset is deleted from an Active vault, the safeset is not deleted from the Passive vault until maintenance processes run.

To install a Passive vault:

- Install a standard vault that will act as the Passive vault. See [Install a standard vault](#).

Data will be replicated to this vault from the Active vault.

- In the Director UI, add a vault connection for the Passive vault.
- (If applicable) If the license you added during the installation did not include a Replication One to One license, add the same Replication One to One license that you added on the Active vault.

After a Replication One to One license is added, an Active Replication menu appears for the vault in the Director UI. This menu will change to a Passive Replication menu after you set up the connection between the Active and Passive vault.

1:1 Replication services should be enabled automatically.

- Check that 1:1 replication services are enabled for the vault. Choose **Vault Settings** from the **Vault Maintenance** menu. On the Replication tab of the dialog box, ensure that the **Enable 1:1 replication services on 'vaultName'** check box is selected.

### 6.1.3 Set up the connection between the Active and Passive vault

On the Active vault, you must specify connection information for the Passive vault.

When the Active vault first connects to the specified vault, the vault is automatically configured as the Passive vault. The Passive vault must be empty, or it cannot be configured as Passive.

To set up the connection between the Active and Passive vault:

1. In the Director UI, click the Active vault connection.
2. Click **Active Replication** and select **Configure**.  
The Active Vault Replication Configuration – *activeVaultname* dialog box appears.
3. On the **Connectivity** tab, enter Passive vault information, including the IP address, command port and data port. Enter a Windows account user name and password for connecting to the Passive vault.
4. Click **OK**.

In the Director UI, the Active Replication menu for the Passive vault changes to a Passive Replication menu.

## 6.2 Set up Many-to-One (N:1) replication

In many-to-one (N:1) replication, data is replicated from one or more Satellite vaults to a Base vault. For this replication configuration, you must install:

- One standard vault that is licensed as a Base vault.
- One or more Satellite vaults.

To set up N:1 replication:

1. Install a Base vault by doing the following:
  - a. Install a standard vault. See [Install a standard vault](#).  
This vault will act as the Base vault. Data will be replicated from one or more Satellite vaults to this Base vault.
  - b. In the Director UI, add a vault connection for the Base vault.
  - c. (If applicable) If the license you added during the installation did not include a Replication Many to One license and Satellite vault licenses, add the required licenses.
2. Install one or more Satellite vaults. See [Install a Satellite vault](#).

## 6.3 Set up Many-to-One-to-One (N:1:1) replication

In many-to-one-to-one (N:1:1) replication, data is replicated from Satellite vaults to an Active Base vault and then to a Passive Base vault.

For this replication configuration, you must install:

- Two standard vaults. One will be configured as the Active Base vault, and one will be configured as the Passive Base vault. The vaults must have approximately the same storage capacity.
- One or more Satellite vaults.

To set up N:1:1 replication between vaults, do the following:

- a. [Install an Active Base vault](#)
- b. [Install a Passive Base vault](#)
- c. [Set up the connection between the Active and Passive Base vaults](#)
- d. [Install one or more Satellite vaults](#)

### 6.3.1 Install an Active Base vault

To set up N:1:1 replication, you must first install an Active Base vault. On the Active Base vault, you must add a vault license, a Replication Many to One license, a Replication One to One license, and a vault license for each Satellite vault.

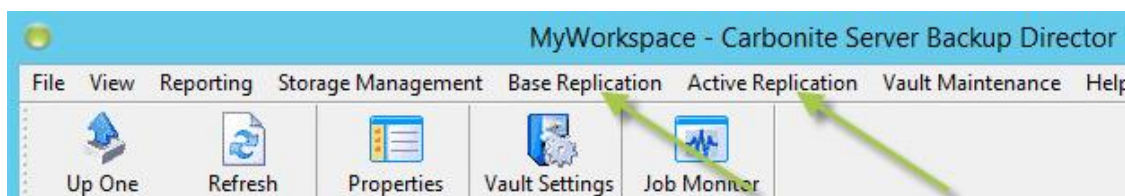
Satellite vault licenses are managed on the Active Base vault.

*Note:* Because each vault can have only one vault license, one of the replication licenses must be added using an add-on replication license key that is not bundled with a vault license.

To install an Active Base vault:

1. Install a standard vault that will act as the Active Base vault. See [Install a standard vault](#).  
Data will be replicated from Satellite vaults to this vault, and from this vault to a Passive Base vault.
2. In the Director UI, add a vault connection for the Active Base vault.
3. (If applicable) If the license you added during the installation did not include a Replication Many to One license or a Replication One to One license, add the required licenses.

After a Replication Many to One license is added, a Base Replication menu appears for the vault in the Director UI. After a Replication One to One license is added, an Active Replication menu appears for the vault in the Director UI.



N:1 and 1:1 replication services should be enabled automatically.

4. Check that replication services are enabled for the vault. Choose **Vault Settings** from the **Vault Maintenance** menu. On the Replication tab of the dialog box, ensure that the **Enable N:1 replication services** and **Enable 1:1 replication services** check boxes are selected.

### 6.3.2 Install a Passive Base vault

After installing an Active Base vault, you can install a Passive Base vault. On the Passive Base vault, you must add the same vault, Replication Many to One, Replication One to One, and Satellite vault licenses that you added on the Active Base vault. When the Active Base vault first communicates with the Passive Base vault, the vault is automatically configured as passive.

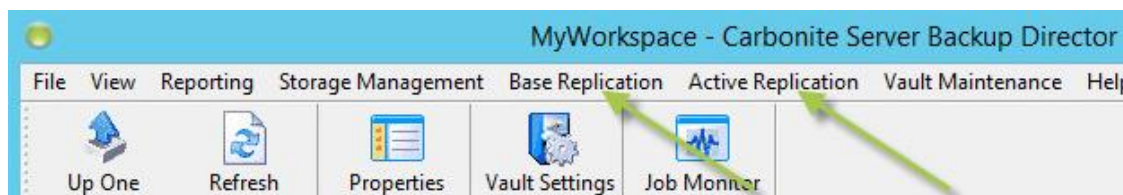
The Active Base vault and Passive Base vault must have approximately the same storage capacity. However, a Passive Base vault can require more storage space than an Active Base vault. When data is replicated after a safeset is deleted from an Active Base vault, the safeset is not deleted from the Passive Base vault until maintenance processes run.

To install a Passive Base vault:

1. Install a standard vault that will act as the Passive Base vault. See [Install a standard vault](#).  
Data will be replicated to this vault from the Active Base vault.
2. In the Director UI, add a vault connection for the Passive Base vault.
3. (If applicable) If the license you added during the installation did not include a Replication Many to One license or a Replication One to One license, add the same license or licenses that you added on the Active Base vault.

After a Replication Many to One license is added, a Base Replication menu appears for the vault in the Director UI.

After a Replication One to One license is added, an Active Replication menu appears for the vault in the Director UI. This menu will change to a Passive Replication menu after you set up the connection between the Active and Passive vault.



N:1 and 1:1 replication services should be enabled automatically.

4. Check that replication services are enabled for the vault. Choose **Vault Settings** from the **Vault Maintenance** menu. On the Replication tab of the dialog box, ensure that the **Enable N:1 replication services** and **Enable 1:1 replication services** check boxes are selected.

### 6.3.3 Set up the connection between the Active and Passive Base vaults

On the Active Base vault, you must specify connection information for the Passive Base vault.

When the Active Base vault first connects to the specified vault, the vault is automatically configured as the Passive vault. The Passive Base vault must be empty, or it cannot be configured as Passive.

To set up the connection between the Active and Passive Base vaults:

1. If a vault is being configured as the Passive Base vault, ensure that the vault includes at least two worker nodes.
2. In the Director UI, click the Active Base vault connection.
3. Click **Active Replication** and select **Configure**. The Active Vault Replication Configuration – *activeBaseVaultname* dialog box appears.
4. On the **Connectivity** tab, enter the Passive Base vault IP address, command port, and data port. Enter a Windows account user name and password for connecting to the Passive Base vault.
5. Click **OK**.

In the Director UI, the Active Replication menu for the Passive Base vault changes to a Passive Replication menu.

### 6.3.4 Install one or more Satellite vaults

After installing an Active Base vault and configuring a Satellite vault for N:1:1 replication, you can install one or more Satellite vaults.

Satellite vault licenses are added on the Active Base vault. When you configure a Satellite vault, the Active Base vault provides an authorization key. When installing a Satellite vault, you must enter the authorization key from the Active Base vault instead of a license key.

*Note:* The Satellite vault configuration from the Active Base vault is not replicated to the Passive Base vault until the Satellite vault is installed and registered.

To install a Satellite vault, see [Install a Satellite vault](#).

## 7 Upgrade a vault

You can upgrade a vault. For supported upgrade paths, see the Director release notes.

To upgrade a vault for 1:1, N:1, or N:1:1 replication, see [Upgrade vaults for data replication](#).

It is recommended that you upgrade Carbonite Server Backup applications in the following order:

- Vault
- Portal
- Agent
- Plug-ins

### 7.1 Upgrade a vault

You can upgrade a vault. For supported upgrade paths, see the Director release notes.

After a successful upgrade, existing Agents and jobs continue to function and your vault licenses remain valid. You can restore new and previous backups.

If an upgrade fails, new directories are added to the Director installation folder. The new directories are prefaced with ~Admin, ~conf, ~database, ~prog, and ~registry. You can use these directories to reverse an unsuccessful upgrade. You can delete these directories if you do not need to reverse an unsuccessful upgrade.

Before upgrading a vault, review the Director release notes and verify that the vault computer meets the minimum requirements for memory, disk space, hardware, and software.

To upgrade a vault:

1. Back up the vault. For database backup methods, see the *Director User Guide* or online help.
1. Make sure that there are no pending reboots on the machine.
2. Close any Powershell windows.
3. Do one of the following:
  - (Recommended) Transition the vault into an offline state by doing the following:
    - i. In the left pane of the Director UI, click the + sign beside the vault.
    - ii. Click **Nodes**.
    - iii. Right-click the node and click **Offline** (to safely terminate in-progress backups before bringing the vault offline) or **Rampdown** (to allow backups to complete before bringing the vault offline. This might take a long time).
  - Stop the Listener service, and make sure that no backups or restores are running.

*Note:* In either case, if a backup, restore or other vault process is running during the upgrade, it will be terminated.

4. Close the Director UI.
5. Double-click the Director installation kit.
6. On the Welcome page, click **Upgrade**, and then click **Next**.
7. If you are upgrading a Satellite vault, on the Director Setup Type page, select the **Do not perform reregistration on Base Vault** option.

If a warning message states that you cannot upgrade Director because the 'VMAdmin.exe' process is running, the Director UI is still open. To continue the upgrade, close the Director UI and click **Try Again**. If you click **Continue**, the upgrade will continue but a reboot will be required before vault services will start. You will be prompted to restart at the end of the installation. You can choose **Restart Now** (after which the services will start) or **Restart Later** (after which you will need to manually restart the machine before services will start).

8. Click **Finish**.
9. Check that the vault services are running.
10. If the vault was transitioned to Offline in Step 3, set it back to Online using the Director UI.

## 7.2 Upgrade vaults for data replication

You can upgrade a vault to version 8.3. For supported upgrade paths, see the Director release notes.

When you upgrade a vault that is involved in data replication, you must upgrade target vaults (vaults that receive replicated data) before upgrading the source vaults. Data cannot be replicated if the target vault is an earlier version than the source vault. For example, in a many-to-one (N:1) scenario, you must upgrade the Base vault before upgrading the Satellite vaults. In a many-to-one-to-one (N:1:1) scenario, you must upgrade the Passive Base vault, then the Active Base vault, and then the Satellite vaults.

After you upgrade the Passive vault in a one-to-one (1:1) replication scenario, the Active vault will continue to work at the earlier version until it is upgraded. However, failover will not function correctly until the Active vault is upgraded to the same version as the Passive vault. Similarly, in an N:1:1 replication scenario, an Active Base vault will work at the earlier version but failover will not function correctly until it is upgraded.

### 7.2.1 Upgrade standalone vaults for replication

You can upgrade a vault to version 8.3 and set up replication with the vault in a one-to-one (1:1), many-to-one (N:1) or many-to-one-to-one (N:1:1) scenario.

To upgrade a standalone vault to a 1:1 configuration:

1. Upgrade the existing standalone vault. This vault will act as the Active vault.
2. Install a second vault to act as the Passive vault.
3. On the Active vault and Passive vault, add the same Replication – One to One license.

To upgrade a standalone vault to an N:1 configuration:

1. Upgrade the existing standalone vault. This vault will act as the Base vault.
2. On the Base vault, add a Replication – Many to One license.
3. On the Base vault, add a satellite license for each Satellite vault.
4. Install Satellite vaults. Each Satellite vault must be a new installation with no existing data.

To upgrade a standalone vault to an N:1:1 configuration:

1. Upgrade the existing standalone vault. This vault will act as the Active Base vault.
2. Install a second vault to act as the Passive Base vault.
3. On the Active Base vault and on the Passive Base vault, add the same Replication – One to One license and Replication – Many to One license.
4. On the Active Base vault and on the Passive Base vault, add a satellite license for each Satellite vault.
5. Install Satellite vaults.

## 7.2.2 Upgrade vaults in 1:1 replication

You can upgrade vaults in one-to-one (1:1) replication, or set up many-to-one (N:1) or many-to-one-to-one (N:1:1) replication with upgraded vaults.

To upgrade vaults in a 1:1 configuration:

1. Upgrade the Passive vault. This vault will continue to act as the Passive vault.
2. Upgrade the Active vault. This vault will continue to act as the Active vault.

*Note:* The Active vault will work at the earlier version until it is upgraded. However, failover will not function correctly until the Active vault is upgraded to the same version as the Passive vault.

To upgrade vaults from 1:1 replication to an N:1 configuration:

1. Upgrade one of the existing vaults. This vault will act as the Base vault.
2. Uninstall the other existing vault.
3. On the Base vault, remove the existing Replication – One to One license.
4. On the Base vault, add a Replication – Many to One license.
5. On the Base vault, add a satellite license for each Satellite vault.
6. Install Satellite vaults. Each Satellite vault must be a new installation with no existing data.

To upgrade vaults from 1:1 replication to an N:1:1 configuration:

1. Upgrade the Passive vault. This vault will act as the Passive Base vault.
2. Upgrade the Active vault. This vault will act as the Active Base vault.
3. On the Active Base vault and Passive Base vault, add the same Replication – Many to One replication license.



*Note:* The vaults should already be licensed for 1:1 replication

4. On the Active Base vault and Passive Base vault, add a satellite license for each Satellite vault.
5. Install Satellite vaults.

### 7.2.3 Upgrade vaults in N:1 replication

You can upgrade Director vaults in a many-to-one (N:1) configuration, or set up many-to-one-to-one (N:1:1) replication with the vaults.

To upgrade vaults in an N:1 configuration:

1. Upgrade the Base vault.
2. Upgrade each Satellite vault.

To upgrade vaults from N:1 replication to an N:1:1 configuration:

1. Upgrade the Base vault. This vault will act as the Active Base vault.
2. Install another vault to act as the Passive Base vault.
3. On the Active Base vault and the Passive Base vault, add the same Replication – One to One license and Replication – Many to One license.
4. Upgrade each Satellite vault.

## 8 Upgrade from Windows 2012 R2 to Windows 2016 on a server where Director 8.30 is installed

This section describes how to upgrade the operating system from Windows Server 2012 R2 to Windows Server 2016 on a server where a Director 8.30 vault is installed.

*Note:* This procedure does not describe how to upgrade Director or other Carbonite products.

You can use this procedure to upgrade the operating system for a Director 8.30 vault which:

- Acts as:
  - An Active vault or Passive vault in 1:1 replication.
  - A Satellite vault or Base vault in N:1 replication.
  - An Active Base vault or Passive Base vault in N:1:1 replication.
  - A standalone vault.
- Uses SQL Server Express 2014 SP2 for the vault database, with either an EVAULT\_DB or EVAULT\_DB\_V800 instance.

To upgrade from Windows Server 2012 R2 to Windows Server 2016 on a server where Director 8.30 is installed:

1. Declare a maintenance window for the vault.
2. In the Director UI, select the vault and go to **Storage Management > Storage Groups and Locations**. Check whether any storage locations are located on the boot volume (e.g., C:\Vault8412558963).

If any storage locations are located on the boot volume, you must copy pool data from the boot volume in Step 7 of this procedure.

3. Using the Director UI, take the vault “Offline”.
4. After you confirm that the vault is “Offline”, stop all of the Director services:
  - Carbonite Server Backup Admin Service
  - Carbonite Server Backup Listener
  - Carbonite Server Backup Monitor
  - Carbonite Server Backup Queue Manager
  - Carbonite Server Backup Replication Service
  - Carbonite Server Backup Scheduler
5. Use the dbbackup command to back up the vault database. Follow the database backup instructions in the Director User Guide. The backup produces a data.bin file.
6. Stop the SQL Server service used by Director, and set the service startup to “Manual”.

If Director has not been upgraded from version 7.11, the SQL Server instance name is “EVAULT\_DB”.

If Director was previously upgraded from version 7.11, the active SQL Server instance name is “EVAULT\_DB\_V800”. In this case, there will also be a SQL Server instance named “EVAULT\_DB” that

is already turned off and disabled. Do not change the startup setting for the EVAULT\_DB SQL service in this case.

7. Save the following items in a secure location, in case you need to roll back the system or reinstall the operating system after a failed upgrade as described in [Recover from a failed Windows upgrade](#):

IMPORTANT: Do not save these items on the system being upgraded.

- **Server hostname and IP addresses.** Record the hostname of the server and the IP addresses, if they are static.
- **Drive letter configuration.** Record the letters and sizes of drives on the server. We recommend adding a text file in the root of each volume with the appropriate drive letter assignment as well as each location indicated.
- **Exported Director registry values.** To export and save Director registry values, do the following:
  - i. At a command prompt, run the following command: `REGEDIT`
  - ii. In the Registry Editor, go to: `HKEY_LOCAL_MACHINE\Software\EVault\InfoStage\Director`
  - iii. Right-click the “Director” key, and select **Export**.
  - iv. Save the exported .reg file in a secure location.
- **Vault configuration folder (CONF folder).** Copy the `<Director root installation folder>\conf` folder, and save it in a secure location.
- **Database.** Save the vault database backup (data.bin file) that was generated in Step 5 using the `dbbackup` command.
- **Logs folder.** Copy the `<Director root installation folder>\logs` folder, and save it in a secure location.
- **Reports Extractor.** If Reports Extractor is installed, copy the `<Director root installation folder>\data` folder, and save it in a secure location.
- **Director UI workspace.** Save any Director UI workspace (.vmw) files in a secure location. By default, workspace files are found in `\Users\<user>\Documents\Carbonite Server Backup` for new Director 8.30 installations, and `\Users\<user>\Documents\EVault InfoStage` for upgraded Director installations.
- **Pool data.** If any pool data is located on your boot volume (as determined in Step 2 of this procedure), copy the entire folder structure, including all data files, from the system to a secure storage location. Make sure you have enough space to copy all of the pool data.

8. Upgrade the operating system from Windows 2012 R2 to Windows 2016, as documented by Microsoft.

*Note:* You must upgrade to the same edition of the operating system. Otherwise, all applications, settings and local files (including Director and vault data) will be removed.

9. Once the operating system has been upgraded and all Windows updates have been applied, do the following:

- a. Set the SQL Server EVAULT\_DB or EVAULT\_DB\_V800 service startup back to “Automatic” and start the service if it is not already running.

- b. Start all of the Director services that you stopped in Step 4.
- c. Launch the Director UI and set the vault to ONLINE.
- d. Activate licenses on the vault. Vault processes will not operate without a new activation.
- e. When the vault is ready, run some backup and restore tests to ensure that everything is running as expected.

## 8.1 Recover from a failed Windows upgrade

If an operating system upgrade fails on a server where a Director 8.30 vault is installed, and the system cannot automatically return to its previous state, you might need to recover the server by reinstalling Windows Server 2012 R2 and reinstalling Director.

To proceed with the recovery, you need the items saved in [Upgrade from Windows 2012 R2 to Windows 2016 on a server where Director 8.30 is installed](#). During the recovery, you must install the same operating system as before the failed Windows upgrade, and install the same version of Director.

To recover from a failed Windows upgrade:

1. Install the exact same operating system (i.e., same edition, service pack, etc.) that was used before the failed Windows upgrade. Set up the system using the same drive letter and volume size scheme that was used before the failed upgrade.
2. Rename the server to the exact same hostname that was used before the failed upgrade.
3. Install the exact same version of Director that was used before the failed upgrade (in this case, Director 8.30).
4. Connect to the new vault with the Director UI to confirm that it is working. At this point, the vault is empty, with no configuration or data.
5. Stop all of the Director services:
  - Carbonite Server Backup Admin Service
  - Carbonite Server Backup Listener
  - Carbonite Server Backup Monitor
  - Carbonite Server Backup Queue Manager
  - Carbonite Server Backup Replication Service
  - Carbonite Server Backup SchedulerLeave the SQL service (EVAULT\_DB) running.
6. Restore the vault database backup (data.bin) from Step 5 of [Upgrade from Windows 2012 R2 to Windows 2016 on a server where Director 8.30 is installed](#) to the new vault installation:
  - a. Copy the data.bin file into a folder on a local drive (e.g., C:\CSB recovery\data.bin).
  - b. At a command prompt, go to the Director “prog” folder where DBBACKUP.exe resides.

- c. Enter the following command:

```
dbbackup restore <path to data.bin file>
```

(e.g., `dbbackup restore c:\CSBrecovery`)

*Note:* Do not include “\data.bin” in the path.

7. Start all of the Director services (listed in Step 5).
8. Launch the Director UI and verify the vault configuration (Storage Groups and Locations) and metadata (Customer, Locations, Accounts, Users, Agents and Tasks) are now available.
9. Stop all of the Director services (listed in Step 5). Leave the SQL service (EVAULT\_DB) running.
10. Ensure that the server has the same drive letters as before the failed operating system upgrade.
11. If any pool data was copied from the boot volume before the upgrade, copy all pool data folders and files that were copied from the boot volume. The folder structure must be exactly the same as before the failed Windows upgrade.  
  
*Note:* If you are replacing just the head (because all of the vault's pool files reside on an external storage system such as a SAN or NAS), skip this step; you do not need to copy pool files. Ensure the drive letters are the same as they were before the failed upgrade. For a NAS device, you should not need to make any changes to the storage. The UNC path locations are stored in the vault database, so once the new operating system is set up, it should automatically attach to the NAS locations.
12. If the Reports Extractor is used to upload data to EVault Reports, copy the Synchweb.cfg file (in ...\Director\conf) to the server.
13. Start all of the Director services (listed in Step 5).
14. Launch the Director UI and activate the vault licenses.

Once you complete this procedure, the new vault will come up as an exact copy of the old one.

## 9 Uninstall a vault

Uninstalling a vault removes the Director programs, services, and most configuration data. However, you must remove the backup data manually.

When you uninstall a vault, you can choose to keep the existing database files. The database files are named Vault.ldf, and Vault.mdf, and are usually saved in the <...>\Director\database directory.

To uninstall a vault:

1. Click **Start** and then **Control Panel**.
2. Double-click **Uninstall a program**.
3. Click **Carbonite Server Backup Director** in the list of programs.
4. Click **Uninstall**.
5. Complete the Carbonite Server Backup Director Setup Maintenance wizard.  
Messages appear while Director is being uninstalled.
6. On the Uninstallation Complete page, select **Yes, I want to restart my computer now**, and then click **Finish**.

## 10 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

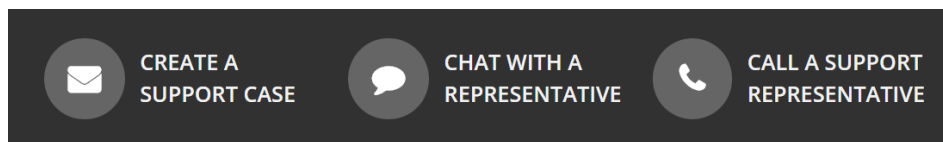
Popular Searches

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

### 10.1 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.