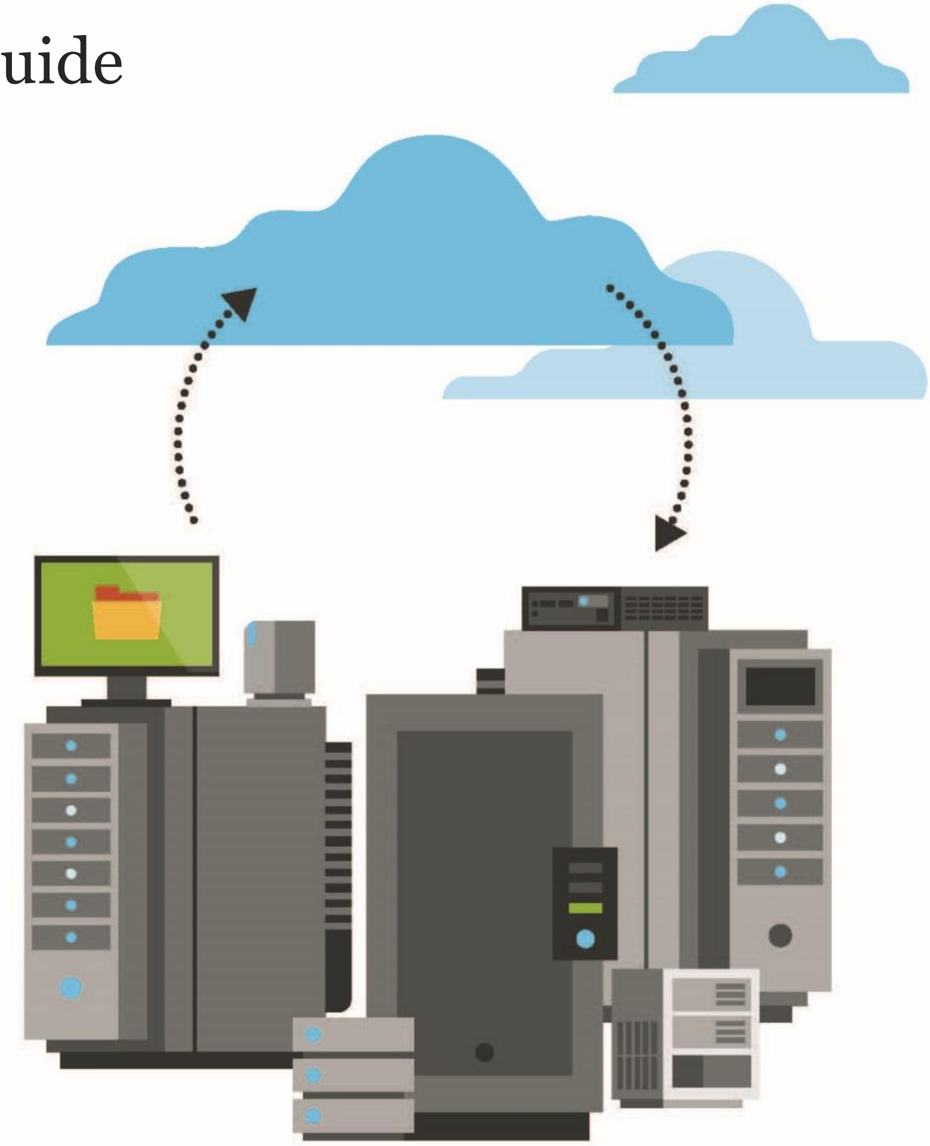
CARBONITE®
an opentext™ company

Carbonite Server Backup Director 8.7

Installation Guide



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.

Carbonite LLC
251 Little Falls Drive
Wilmington, DE 19808
www.carbonite.com

Document History

Version	Date	Description
1	July 2023	Installation guide provided for Director 8.7*x*.

Contents

1 Overview

Carbonite Server Backup Director is an online data vault that securely receives, stores and manages backup data from servers where Agents are installed.

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.

When installing a vault, you can also install the Reporting service and register it to Carbonite Server Backup API – Monitoring. The Reporting service sends vault data to API – Monitoring and is required for deleting data from vaults in response to requests from Carbonite Server Backup Portal. See Install and register the Reporting service.

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

IMPORTANT*:* A new port (12546) is used for replicating data between Director 8.70 vaults. Before upgrading vaults to Director 8.70, be sure that replication source vaults (i.e., Satellite and Active vaults) can connect to replication target vaults (i.e., Base and Passive vaults) on port 12546.

The following table lists ports used by Director 8.7:

Port	Direction	Protocol	Description
443	Outbound	TCP	Communication with license activation server.
809	Inbound	TCP	Admin service (communication from Director UI and Vault API).
8080	Outbound	TCP	Admin service and Reporting service (registration with API – Monitoring).
5671, 5672, 8081	Outbound	TCP	Admin service and Reporting service (communication with API – Monitoring).

Port	Direction	Protocol	Description
2546, 807	Inbound	TCP	Listener ports for backups and restores.
12546	Outbound	TCP	Command port on a Director 8.7 source vault in replication. *Note:* This command port is new in Director 8.7. This port is used instead of port 2547, which is used for replication in previous Director versions. After all source vaults have been upgraded to Director 8.70, port 2547 can be closed at the firewall.
12547	Outbound	TCP	Data port on a source vault in replication.
12546	Inbound	TCP	Command port on a target vault in replication with a Director 8.7 source vault.
2547	Inbound	TCP	Command port on a target vault in replication with a Director 8.6*x* or earlier source vault.
12547	Inbound	TCP	Data port 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 account name, including any domain name (i.e., *domainName\username*), can have a maximum of 20 characters. When a local VaultService account is created, the generated password for the account is 20 characters long and includes uppercase, lowercase, numeric and special characters.

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.

Note: If you change the account for running Director services after the Reporting service is registered to API – Monitoring, you must re-register the Reporting service to the API to retain Reporting service and data deletion functionality.

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 Director 8.7 vault, SQL Server 2019 Express is installed as the vault database engine. Please keep the Director SQL Server instance updated with the latest security and critical updates from Microsoft.

When you install a standard vault, you can also install the Reporting service and register it to Carbonite Server Backup API – Monitoring. The Reporting service sends data to API – Monitoring and is required for deleting data in response to requests from Carbonite Server Backup Portal.

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. Please note that Reporting service functionality is not supported on a VM in Azure.

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

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 **I accept the terms of the license agreement**, and then click **Next**.
5. On the installation type page, select **Director, including UI**, 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, note that email notifications can be configured using the Director UI or VaultOp command. 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**.

The account name, including any domain name (i.e., *domainName\username*), can have a maximum of 20 characters.

For more information, see Permissions for running Director services.

The Director installation begins. Messages show the installation progress.

Note: If you are installing a vault on a server where a SQL Server Express version earlier than SQL Server Express 2019 was already installed, a reboot might be required during the Director installation process.

13. In the message box that recommends enabling updates for Microsoft products to ensure that SQL Server remains up to date, click **OK**.
14. When the Welcome page for the Reporting service installation wizard appears, do one of the following:

- Install the Reporting service as described in Install and register the Reporting service.
- Finish installing Director without installing the Reporting service by doing the following:

i. On the Welcome page for the Reporting service installation wizard, click **Cancel**.

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

iii. On the InstallShield Wizard Complete page, click **Finish**.

Note: An *Installing Reporting Service* message appears, even though you are not installing the Reporting service. Please wait while the Director installation finishes.

A message box tells you how to activate the Director license.

iv. Click **OK**.

v. On the InstallShield Wizard Complete page, 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 billing code, and then click **Next**.

   The billing code (also known as a location code) can be 5-20 characters in length, and can only include alphanumeric characters and dashes (-).
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 31 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, and then click **OK**.
11. Click **Next**.
12. 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. See Configure a Satellite vault on a Base vault.

When you install a Director 8.7 vault, SQL Server 2019 Express is installed as the vault database engine. Please keep the Director SQL Server instance updated with the latest security and critical updates from Microsoft.

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 **I accept the terms of the license agreement**, and then click **Next**.
5. On the installation type page, select **Director, including UI**, 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, note that email notifications can be configured using the Director UI or VaultOp command. 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 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**.

      The account name, including any domain name (i.e., *domainName\username*), can have a maximum of 20 characters.

    For more information, see Permissions for running Director services.

    The Director installation begins. Messages show the installation progress.

    Note: If you are installing a vault on a server where SQL Server was already installed, a reboot might be required during the Director installation process.
12. In the message box that recommends enabling updates for Microsoft products to ensure SQL Server remains up to date, click **OK**.
13. When the Register the Satellite Vault to a Base Vault page appears, do the following:
    - In the **Base vault address** field, enter the Base vault address.
    - 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.

      The **Port** field shows the port that the Satellite vault will use to communicate with the Base vault.

14. Click **Register**.
15. On the Registration Confirmation page, click **Next**.
16. When the Welcome page for the Reporting service installation wizard appears, do one of the following:
    - Install the Reporting service as described in Install and register the Reporting service.
    - Finish installing Director without installing the Reporting service by doing the following:
        i. On the Welcome page for the Reporting service installation wizard, click **Cancel**.

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

        iii. On the InstallShield Wizard Complete page, click **Finish**.

        Note: An *Installing Reporting Service* message appears, even though you are not installing the Reporting service. Please wait while the Director installation finishes.

        A message box tells you how to activate the Director license.

        iv. Click **OK**.

        v. On the InstallShield Wizard Complete page, 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 Manage the vault certificate and certificate pinning

When you install a Director 8.7 vault or upgrade a vault from Director 8.56 or earlier to Director 8.7, a self-signed TLS certificate is generated for the vault. The certificate is valid for 10 years and is stored in the Local Computer certificate store in \Carbonite Server Backup\Certificates.

The self-signed certificate that was generated for Director 8.6*x* vaults was valid for one year. If you upgrade a Director 8.6*x* vault to Director 8.7 and the vault has its original generated self-signed certificate, the certificate is regenerated with a 10-year validity period. When the certificate is regenerated, the certificate's public and private keys are preserved so that backups continue to function without interruption if agent-vault certificate pinning is enabled on the vault.

You can replace the generated vault certificate with another self-signed certificate or a certificate from an enterprise or commercial Certificate Authority (CA). See Import a vault certificate. You can also export the certificate from a vault. See Export a vault certificate.

The vault certificate is used in:

- Agent-vault certificate pinning. When this security feature is enabled in a vault, when an agent that supports certificate pinning tries to connect to the vault (e.g., to run a backup or restore), it checks whether the public key of the vault's TLS certificate is the same as when the agent previously connected to the vault. If the public key of the vault certificate is different, the agent reports a certificate failure and will not connect to the vault until the certificate failure is resolved.

  Agent-vault certificate pinning must be manually enabled in a vault. See Enable agent-vault certificate pinning. If you upgrade a Director 8.6*x* vault where agent-vault certificate pinning was enabled, the feature remains enabled after the vault is upgraded to version 8.7.

- Certificate verification and pinning for vault-to-vault communications. Vault certificates are verified when a Director 8.7 source vault connects to a Director 8.7 target vault to replicate data, copy or clone data, or run a replication report. If the certificate verification fails, the source vault does not connect to the target vault and the replication, copy, clone or replication report fails. For more information, see the *Director User Guide*.

  If the certificate verification passes, the source vault pins or records the target vault's certificate when it first connects to the target vault. When the source vault tries to connect to the target vault again, it checks whether the target vault certificate has changed. If the target vault certificate has changed to a self-signed certificate, the source vault will not connect to the target vault unless the pinned or recorded certificate is deleted from the source vault. For more information, see Manage pinned and recorded vault certificates.

  Certificate verification and pinning for vault-to-vault communications is always performed when the source and target vaults are Director version 8.7. You do not have to manually enable this security feature.

Vault certificates are not verified when the Portal UI or Vault API connects to a vault.

4.1 Import a vault certificate

You can replace a vault certificate with a self-signed certificate or a certificate from an enterprise or commercial Certificate Authority (CA). The certificate can be a wildcard certificate and must be in .pfx format.

Beginning in Director 8.70, when you import a new vault certificate using the vaultop import_certificate command, the new certificate is verified. If the root certificate is not found on the vault server, the import fails. If another issue is found with the certificate (e.g., the certificate has expired), a warning is logged but the certificate is imported.

Note: Director services must be restarted after any change to the vault certificate or vault certificate chain (e.g., new signing certificate for a CA-signed certificate). The vaultop import_certificate command automatically restarts Director services.

IMPORTANT: If you import a new vault certificate, additional actions might be required to allow backups and vault-to-vault communications (e.g., replication) to continue:

- If you import a vault certificate with a different public key than the previous vault certificate, and agent-vault certificate pinning is enabled in the vault, a Portal user must resolve agent certificate failures before backups can continue. For more information, see Enable agent-vault certificate pinning and Ensure that agents can connect to a vault after a vault certificate change.
- If you replace a Director 8.7 target vault certificate with a new self-signed certificate, Director 8.7 source vaults (i.e., Satellite vaults or Active vaults) will not connect to the target vault again unless you delete the pinned or recorded certificate from the source vaults. For more information, see Manage pinned and recorded vault certificates.
- If you replace a Director 8.7 target vault certificate with a CA-signed certificate and the signing certificate is from a Microsoft trusted certificate authority, Director 8.7 source vault servers automatically download the signing certificate to the Trusted Root Certification Store. In rare cases, you might have to manually import the root signing certificate on the source vault server.

To import a vault certificate:

1. At a command prompt, navigate to the Director Utils folder (C:\Program Files\Carbonite Server Backup\Director\Utils, by default).
2. Run the following command:

   `vaultop import_certificate` *certPathAndFilename certPassword*

   Where:

   - *certPathAndFilename* is the full path and filename of the certificate that you are importing. The certificate must be in .pfx format. Enclose the path and filename in quotation marks if it includes spaces.
   - *certPassword* is the password of the .pfx file that you are importing.

For example, to import a certificate from a C:\Certificate\cert.pfx file with the password "password1", run the following command:

```
vaultop import_certificate C:\Certificate\cert.pfx password1
```

4.2 Export a vault certificate

You can export a vault certificate in .pfx format. This can be useful if you want to import the certificate into another vault.

To export a vault certificate:

1. At a command prompt, navigate to the Director Utils folder (C:\Program Files\Carbonite Server Backup\Director\Utils, by default).
2. Run the following command:

   `vaultop export_certificate` *certPathAndFilename certPassword*

   Where:

   - *certPathAndFilename* is the full path and filename for the exported certificate, including the .pfx extension. Enclose the certificate path and filename in quotation marks if it includes spaces.

     Note: The specified path must exist before you export the certificate.

   - *certPassword* is the password for the exported .pfx file.

   For example, to export a vault certificate to a C:\Exported Cert\cert.pfx file with the password "password2", run the following command:

   ```
   vaultop export_certificate "C:\Exported Cert\cert.pfx" password2
   ```

4.3 Enable agent-vault certificate pinning

Beginning in Director 8.60, you can enable agent-vault certificate pinning in a vault. Certificate pinning is designed to prevent attackers from redirecting network traffic intended for legitimate vaults to servers under their control.

When this security feature is enabled, when an agent that supports certificate pinning tries to connect to the vault (e.g., to run a backup or restore), it checks whether the public key of the vault's TLS certificate is the same as when the agent previously connected to the vault. If the public key of the vault certificate is different, the agent reports a certificate failure and will not connect to the vault.

If a certificate failure occurs, system administrators must determine whether the certificate change was expected or whether further investigation is required. If the certificate change was expected, a Portal user can resolve the certificate failure. The agent then records the new public key of the vault certificate, and backups and restores can continue. For more information, see the Server Backup online help.

If agent-vault certificate pinning was enabled in a Director 8.6 vault, the feature remains enabled after the vault is upgraded to version 8.7.

IMPORTANT: Do not enable agent-vault certificate pinning in a vault until the intended vault certificate is installed. If you enable this feature and then import a certificate with a different public key, agents that support certificate pinning will not connect to the vault again until the certificate failure is resolved.

IMPORTANT: Agent-vault certificate pinning cannot be turned off in a vault after it is enabled.

To enable agent-vault certificate pinning:

1. At a command prompt, navigate to the Director Utils folder (C:\Program Files\Carbonite Server Backup\Director\Utils, by default).
2. Run the following command:

   ```
   vaultop certificate_pinning
   ```

4.3.1 Ensure that agents can connect to a vault after a certificate change

If agent-vault certificate pinning is enabled in a vault and the public key of the vault certificate changes, some agents stop connecting to the vault. For more information, see Enable agent-vault certificate pinning.

To ensure that agents continue connecting to a vault after you replace the vault certificate, you can generate a Certificate Signing Request (CSR) with the same public key as the current certificate. You can then submit the CSR to a Certificate Authority to obtain a new certificate with the same public key.

To ensure that agents can connect to a vault after a vault certificate change:

1. Export the current certificate from a vault in .pfx format. See Export a vault certificate.
2. On a server where OpenSSL 1.1.1 is installed, save the certificate (.pfx) file exported in Step 1.
3. Open a command prompt as administrator and navigate to the OpenSSL bin directory.
4. Run the following command to generate a key file from the vault certificate exported in Step 1.

   ```
   openssl pkcs12 -in vaultCertificateFile.pfx -nocerts -out keyFile.key
   ```

   Where:

   - *vaultCertificateFile*.pfx is the full path and name of the vault certificate .pfx file exported in Step 1. Enclose the path and filename in quotation marks if it includes spaces.
   - *keyFile*.key is the full path and name for the generated key file. Enclose the path and filename in quotation marks if it includes spaces.

   When prompted, enter the following information:

   - **Import Password** – Enter the password of the vault certificate .pfx file.
   - **PEM pass phrase** – Enter a password for the generated key file.

5. Run the following command to generate a certificate signing request with the key file you generated in Step 4.

   ```
   openssl req -new -nodes -key keyFile.key -out CSRfile.csr
   ```

   Where:

   - *keyFile*.key is the full path and name of the key file generated in Step 4. Enclose the path and filename in quotation marks if it includes spaces.
   - *CSRfile*.csr is the full path and name for the generated certificate signing request file. Enclose the path and filename in quotation marks if it includes spaces.

   When prompted, enter the following information:

   - **Pass phrase for *keyfile*** – Enter the PEM pass phrase entered in Step 4.
   - Information for the distinguished name for the certificate:
     - **Country Name** – Enter the two-letter code for the country (e.g., US).
     - **State or Province Name** – Enter the full name of the state or province.
     - **Locality Name** – Enter the name of the city.
     - **Organization Name** – Enter the company or organization name.
     - **Organizational Unit Name** – Enter an organizational unit name.
   - **Common Name** – Enter a common name for the certificate (e.g., *.example.com).

   You do not need to enter values at the following prompts:

   - Email Address
   - A challenge password
   - An optional company name

   A CSR file is then generated. You can provide this file to a Certificate Authority to generate a new certificate with the same public key as the existing vault certificate. When you receive the new certificate, you can import it into the vault. See Import a vault certificate.

4.4 Manage pinned and recorded vault certificates

To improve the security of vault-to-vault communications, vault certificates are verified when a Director 8.7 source vault connects to a Director 8.7 target vault to replicate data, copy or clone data, or run a replication report. For more information, see the *Director User Guide.*

When a Director 8.7 source vault (e.g., a Satellite vault or Active vault) first connects to a Director 8.7 target vault, if the certificate verification passes, the source vault pins or records the target vault's certificate.

When the source vault tries to connect to the target vault again, it checks whether the target vault certificate is the same as the pinned or recorded certificate. If the vault certificate is the same or has changed to a CA-signed certificate that passes verification, the source vault connects to the target vault. If the target vault certificate has changed to a self-signed certificate, the source vault will not connect to the vault and “certificate verify fail” messages appear in the Replication Service log. The source vault will only connect to the target vault again if you delete the pinned or recorded certificate from the source vault.

IMPORTANT: Do not delete a pinned or recorded vault certificate unless you are sure that there is no security risk. Please contact your IT security staff or service provider to determine whether the certificate change was expected or whether further investigation is required.

Certificate verification and pinning for vault-to-vault communications is always performed when the source and target vaults are Director version 8.7. You do not have to manually enable this security feature. Vault certificates are not verified or pinned when a Director version 8.6*x* or earlier vault connects to a Director 8.7 vault.

To view target vault certificates that are pinned or recorded on a source vault, see List pinned and recorded vault certificates on a source vault. To delete a pinned or recorded vault certificate from a source vault, see Delete a pinned or recorded vault certificate from a source vault.

4.4.1 List pinned and recorded vault certificates on a source vault

You can run a command that lists target vault certificates that are pinned or recorded on a source vault.

When a Director 8.7 source vault (e.g., a Satellite vault or Active vault) first connects to a Director 8.7 target vault, the source vault pins or records the target vault’s certificate. When the source vault tries to connect to the target vault again, it checks whether the target vault certificate is the same as the pinned or recorded certificate.

To list pinned and recorded vault certificates on a source vault:

1. At a command prompt on the vault server, navigate to the Director Utils folder (C:\Program Files\Carbonite Server Backup\Director\Utils, by default).
2. Run the following command:

   ```
   vaultop list_certificates [verbose]
   ```

   For each pinned self-signed certificate, the command returns the target vault address, certificate thumbprint and certificate subject name. If you include the `verbose` parameter, the command also returns each self-signed certificate in PEM format.

   For each recorded CA-signed certificate, the command returns the target vault address and indicates that the vault certificate is not self-signed.

4.4.2 Delete a pinned or recorded vault certificate from a source vault

When a Director 8.7 source vault (e.g., a Satellite vault or Active vault) first connects to a Director 8.7 target vault, the source vault pins or records the target vault’s certificate. When the source vault tries to connect to the target vault again, if the target vault certificate has changed to a self-signed certificate, the source vault will not connect to the target vault unless you delete the pinned or recorded certificate from the source vault.

IMPORTANT: Do not delete a pinned or recorded vault certificate unless you are sure that there is no security risk. Please contact your IT security staff or service provider to determine whether a certificate change was expected or whether further investigation is required.

To delete a pinned or recorded vault certificate from a source vault:

1. At a command prompt on the vault server, navigate to the Director Utils folder (C:\Program Files\Carbonite Server Backup\Director\Utils, by default).
2. Run the following command:

   ```
   vaultop delete_pinned_certificate serverAddress
   ```

   Where *serverAddress* is the IP address or hostname of the target vault whose certificate is pinned or recorded on the source vault.

5 Install and register the Reporting service

When installing a vault or when upgrading a vault where the Reporting service is not installed, you can install the Reporting service. The Reporting service sends data to API – Monitoring and is required for deleting data in response to requests from Portal.

For data deletion, the Reporting service must be installed with each standalone, Base and Active vault and registered to Carbonite Server Backup API – Monitoring 1.30 or later. The Reporting service does not have to be installed with each Satellite and Passive vault; replication processes delete data from these vaults after a data deletion request. However, we recommend installing the Reporting service with each Passive vault and registering it to the API so that it is available if you have to fail over to the (formerly) Passive vault.

Note: Although it is not required for data deletion, the Reporting service must be installed with Satellite and Passive vaults and registered to API – Monitoring to provide data through API – Monitoring calls.

To register a Reporting service to API – Monitoring, we recommend using a registration token and registration URL. An API – Monitoring administrator can generate a registration token using the ObtainRegistrationTokenScript provided with API – Monitoring. For more information, contact the system administrator who installed API – Monitoring.

Note: You can also register the Reporting service to API – Monitoring using Client ID and Client Secret values from the last page of the API – Monitoring installation wizard. However, to ensure the security of your data, access to these values should be limited. Keep the Client ID and Client Secret private and secure.

To obtain values for registering the Reporting service to the API, contact the system administrator who installed API – Monitoring.

You can also register the Reporting service to the API using a command after the Reporting service is installed. See Register the Reporting service to API – Monitoring.

The Reporting Service can only communicate with API – Monitoring with a secured channel using TLS. If API – Monitoring is installed with the HTTP communication protocol, a TLS termination proxy is required.

If the Reporting service will send data to an API – Monitoring instance with a certificate from a Certificate Authority (CA), the Director vault server must meet the following requirements:

- the trusted root certificate and intermediary certificate must be installed on the vault server, either manually or through Windows updates (for a certificate from a commercial CA).
- the vault server must be able to reach the CRL (certificate revocation list) to validate the certificate.

To install the Reporting service and register it to API – Monitoring:

1. Install or upgrade a vault as described in Install a standard vault, Install a Satellite vault or Upgrade a vault.
2. When the Welcome page for the Reporting service installation wizard appears, click **Next**.
3. On the License Agreement page, read the license agreement. Select **I accept the terms in the license agreement**, and then click **Next**.

4. If a Password for Director services account page appears, enter the password of the custom Administrator account used to run Director services on the server.

   Note: The Password for Director services account page only appears if vault services are running using a custom Administrator account (i.e., not the VaultService account).

   Note: If vault services are running using the VaultService account, the Vault Reporting service installer resets the VaultService account password.

5. On the Ready to Install the Program page, click **Install**.

   The Reporting service is installed in a ReportingService subdirectory in the location where Director is installed (e.g., C:\Program Files\Carbonite Server Backup\Director\ReportingService).

   After the registration service is installed, the API Registration Method page appears.

6. Do one of the following:

   - To register the Reporting Service to API – Monitoring using a registration token, select **Register using a registration token**, and then click **Next**. On the API registration information page, enter values in the following fields:
     - **Registration URL** – Enter the Registration URL from the last page of the API installation wizard (e.g., `https://api.carbonite.com:8080`).

       Note: Only HTTPS connections to API – Monitoring are supported.
     - **Registration Token** – Enter a registration token from your API system administrator.

   Note: To obtain values for registering the Reporting service to the API, contact the system administrator who installed API – Monitoring.

   - To register the Reporting Service to API – Monitoring using a Client ID and secret, select **Register using a Client ID and secret**, and then click **Next.** On the API registration information page, enter values in the following fields:
     - **Registration Service URL** – Enter the Registration URL from the last page of the API installation wizard (e.g., `https://api.carbonite.com:8080`).

       Note: Only HTTPS connections to API – Monitoring are supported.
     - **Client ID** – Enter the Client ID value from the last page of the API installation wizard (`Carbonite-Registration-Client`).
     - **Client Secret** – Enter the Client Secret value from the last page of the API installation wizard (e.g., `fnrGRhlYTgZ8CGOFcH+qAfpCroV2g6+UDoIPaUDlycqr`).
   - If you do not want to register the Reporting service to API – Monitoring, or you do not have the required registration information, select **I do not want to register the Reporting service to the API at this time,** click **Next,** and end the installation process. Later, you must register the Reporting service to the API as described in Register the Reporting service to API - Monitoring.

     Important: The Reporting service on any standalone, Base or Active vault must be registered to API – Monitoring before Director can delete data from these vaults in response to requests from Portal. Replication processes then delete the data from any associated Satellite or Passive vault.

7. Click **Register**.

When the Reporting service has been successfully registered to API – Monitoring, a confirmation message appears. Click **OK** in the message box.

8. Click **Next.**
9. Click **Finish**.

   Messages appear while the installation finishes.

5.1 Register the Reporting service to API – Monitoring

You can register the Reporting service on a vault to API – Monitoring using a command. This is required if:

- You do not register the Reporting service to the API when you install the Reporting service.
- The password changes for the VaultService account or custom Administrator account used to run Director services.
- The account for running Director services changes after the Reporting service was already registered to API – Monitoring.

To register a Reporting service to API – Monitoring, we recommend using a registration token and registration URL. An API – Monitoring administrator can generate a registration token using the ObtainRegistrationTokenScript provided with the API. For more information, contact the system administrator who installed API – Monitoring.

Note: You can also register the Reporting service to the API using Client ID and Client Secret values from the last page of the API – Monitoring installation wizard. However, to ensure the security of your data, access to these values should be limited. Keep the Client ID and Client Secret private and secure.

To register the Reporting service to API – Monitoring:

1. In a PowerShell window, navigate to the directory where the Reporting service is installed.

   By default, the Reporting service is installed in the following location: C:\Program Files\Carbonite Server Backup\Director\ReportingService

2. Do one of the following:

   - To register the Reporting service to the API using a registration token, run the following command:

     ```
     .\ReportingService.exe -cmdline -register -uri registrationURL -token
     registrationToken
     ```

     To obtain the *registrationURL and registrationToken* values, contact the system administrator who installed API – Monitoring.

     Note: Only HTTPS connections to API – Monitoring are supported.

     For example, you could run the following command to register the Reporting service to the API:

     ```
     .\ReportingService.exe -cmdline -register -uri
     https://api.carbonite.com:8080 -token eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9
     .eyJqdGkiOiJtd1FIN0hWbE1tN3ZpVWZCMTFiU0xYZVEiLCJzdWIiOiJWYXVsdCIsImh0dHA6L
     y9zY2hlbWFzLm1pY3Jvc29mdC5jb20vd3MvMjAwOC8wNi9pZGVudGl0eS9jbGFpbXMvZXhwaXJ
     hdGlvbiI6IjA3LzEyLzIwMTggMTM6NDA6MzAiLCJuYmYiOjE1MzE0MDEwMzAsImV4cCI6MTUzM
     TQwMjgzMCwiaWF0IjoxNTMxNDAxMDMwLCJhdWQiOiJ1cm46Y2FyYjpvYzpyZWdpc3RyYXRpb24
     ```

```
ifQ.XxFL4RS76L0S4hNGyilubf7g3Faz3bzoCVe87Q86Cx5TN6O4mn08Oyjg1ea_ZetBxkRCBB
_XL3vde7eSQTQdBSAksjvmw_A8QAmnW9dOnwb-T4F32snU_9XnHygYDaK3zMHfyAX-aUjk6DNP
HKJ11v8UTkIu6scM9_bxwi2vUzDC_8iGnVk26PcyADPMDbt82KqFccIhyU006v3Gmm9ZhB3dbs
iBKXw9WnRc12ZACJqzCidnFYj483_34qJNLFs1tFcIa2n-bVdOKs_XIK6AQEClf6eJwt8NIt41
Ih3naHR5s-UtbxfU5ZK7cCGWFxhmWTGR7KGcjSQN4d_bqx5h7Q
```

- To register the Reporting service to the API using a Client ID, Client Secret and Registration URL, run the following command:

  ```
  .\ReportingService.exe -cmdline -register -uri registrationURL -id
  ClientID  -secret ClientSecret
  ```

  The *registrationURL, ClientID* and *ClientSecret* values are provided on the last page of the API installation wizard.

  Note: Only HTTPS connections to API – Monitoring are supported.

  For example, you could run the following command to register the Reporting service to the API:

  ```
  .\ReportingService.exe -cmdline -register -uri
  https://api.carbonite.com:8080 -id Carbonite-Registration-Client -secret
  YVR2TNq/h6AWGAwOGzeUz4xq4qEMdrwd7Jc70VTOf5bQX
  ```

6 Install the Director UI

You can install the Director UI, the graphical user interface (GUI) for managing vaults, without installing a vault. 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 **I accept the terms of the license agreement**, 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. On the InstallShield Wizard Complete page, click **Finish**.

7 Silently install or upgrade a vault

You can silently install or upgrade a vault. A silent installation or upgrade does not require user interaction and does not display any indication of its progress. For supported upgrade paths, see the Director release notes.

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

a. Record a response file

b. Run a silent installation or upgrade

IMPORTANT: For a silent Director 8.7 installation or upgrade, you must record a response file (.iss file) using the Director 8.7 installation kit. You cannot use a response file created using a previous Director version.

7.1 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 an installation or upgrade. Installations and upgrades require separate response files. A response file that is created for a fresh installation cannot be used for an 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.

Sample response files are available. For more information, please contact Support.

Before recording a response file, make sure that there are no pending reboots on the server.

To record the response file:

1. At a command prompt, navigate to the directory where the Director installation kit is saved and run the following command:

   ```
   Director-8-7x-xxxx.exe /r /f1"responseFilePathAndName.iss"
   ```

   Where:

   - Director-8-7*x-xxxx*.exe — Name of the Director installation kit.
   - *responseFilePathAndName* — Absolute path to the response file and the response file name. Do not specify a relative path to the response file.

   For example, to create a response file named responseFile.iss in a C:\silentInstall directory, run the following command:

   ```
   Director-8-7x-xxxx.exe /r /f1"C:\silentInstall\responseFile.iss"
   ```

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

   If the installation wizard does not appear, make sure that there are no pending reboots on the server.

   If you record a response file while upgrading a vault and the NoAutoReboot parameter is not included in the command, the server restarts automatically after the vault database engine is upgraded to SQL Server 2019 Express. At this point, the response file is incomplete and cannot be used. After the server restarts and an administrator signs in to the server, the Director upgrade restarts automatically and the response file will be generated correctly.

7.2 Run a silent installation or upgrade

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

When you install a Director 8.7 vault, SQL Server 2019 Express is installed as the vault database engine. When you upgrade a vault to version 8.7, the vault database engine is upgraded to SQL Server 2019 Express. Please keep the Director SQL Server instance updated with the latest security and critical updates from Microsoft.

During a silent Director upgrade, if the NoAutoReboot parameter is not included in the command, the server restarts after the vault database engine is upgraded. After the server restarts and an administrator signs in to the server, the Director upgrade restarts automatically.

A new port (12546) is used for replicating data between Director 8.7 vaults. After silently upgrading a replication source vault (i.e., a Satellite or Active vault), check the Director upgrade log to see whether the vault can connect to port 12546 on the target vault. If the source vault cannot connect to the replication target vault, data will not replicate until you address the connection issues.

Note: Port 12546 is used instead of port 2547, which is used for replication in previous Director versions. After all source vaults have been upgraded to Director 8.70, port 2547 can be closed at the firewall.

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

When you install or upgrade a vault silently, the Reporting service is installed with the vault. The Reporting service sends data to API – Monitoring and is required for deleting data in response to requests from Carbonite Server Backup Portal. After the Reporting service is installed, you can register the Reporting service to the API as described in Register the Reporting service to API – Monitoring.

The installer returns zero (0) 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.

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

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*.

Before a silent installation or upgrade, make sure that there are no pending reboots on the server.

To run a silent installation or upgrade, at a command prompt, navigate to the directory where the Director installation kit is saved and run the following command:

```
Director-8-7x-xxxx.exe /s /f1"absolutePathToResponseFile.iss" [KeepBackup]
[NoRegSAT] [NoAutoReboot] [NoOnline] [svServiceAccountUsername=userName
svServiceAccountPassword=password]
```

Where:

- Director-8-7*x-xxxx*.exe — Name of the Director installation kit.

- *absolutePathToResponseFile*.iss — Absolute path to the response file and the response file name. Do not specify a relative path to the response file.
- 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 this parameter is specified, the server does not automatically restart if a reboot is required. By default during a silent Director upgrade, the server restarts automatically after the vault database engine is upgraded to SQL Server 2019 Express. When the NoAutoReboot parameter is specified for a silent upgrade, the following message appears in the log and you must restart the server manually: *You will need to reboot the computer. Director installation will run automatically after the 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 prevents 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).
- svServiceAccountUsername=<*userName*> svServiceAccountPassword=<*password*> — Optional parameters. These parameters are only required if you are installing the Reporting service on a vault that uses a custom account to run Director services or where the password for the local VaultService account has changed. These parameters specify the name and password of the Administrator account used for running Director services.

For example, to silently install Director using a response file named responseFile.iss in the C:\silentInstall directory, run the following command:

```
Director-8-7x-xxxx.exe /s /f1"C:\silentInstall\responseFile.iss"
```

If the silent installation or upgrade does not start, make sure that there are no pending reboots on the server.

After the server restarts and an administrator signs in to the server, the Director upgrade restarts automatically.

If the NoAutoReboot parameter is not specified, the server restarts automatically after the vault database engine is upgraded. After the server restarts and an administrator signs in to the server, the Director upgrade restarts automatically.

8 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.

IMPORTANT: Be sure that each replication source vault (i.e., Satellite or Active vault) can connect to the replication target vault (i.e., Base or Passive vault) on the required ports. A new command port (12546) is used for replicating data between Director 8.7 vaults. For more information, see Ports.

8.1 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

8.1.1 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.

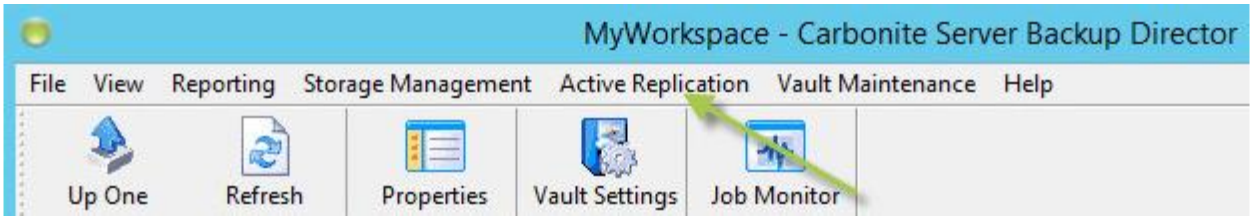
To install an Active vault:

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.
3. (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.
4. 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.

8.1.2 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:

1. 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.
2. In the Director UI, add a vault connection for the Passive vault.
3. (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.
4. 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.

8.1.3 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.

8.2 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 Configure and install a Satellite vault.

8.3 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

8.3.1 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:

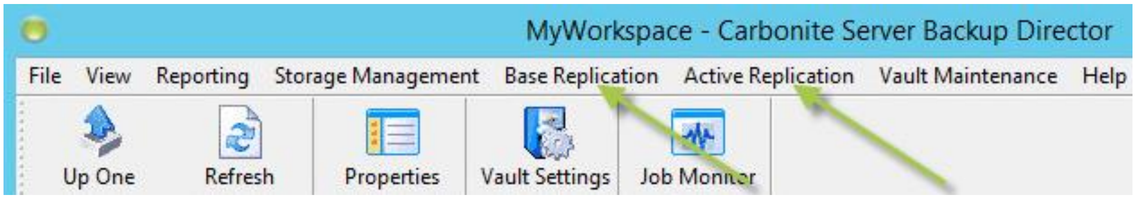
1. Install a standard vault that will act as the Active Base vault. See Install a standard vault.

   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.

8.3.2 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.

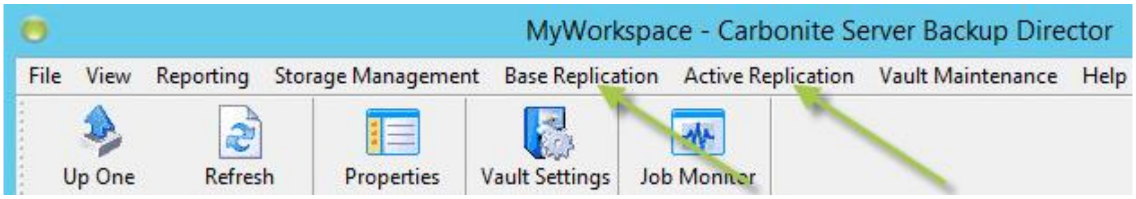
   Data will be replicated to this vault from the Active Base vault.

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.

8.3.3 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. In the Director UI, click the Active Base vault connection.
2. Click **Active Replication** and select **Configure**. The Active Vault Replication Configuration – *activeBaseVaultname* dialog box appears.
3. 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.
4. Click **OK**.

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

8.3.4 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 Configure and install a Satellite vault.

9 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
- Agents and Plug-ins

9.1 Upgrade a vault

Before upgrading a vault, check the Director release notes for supported platforms and upgrade paths. If your current operating system is not supported with Director 8.7, you must upgrade the operating system to a supported version before upgrading the vault to version 8.7. See Upgrade Windows on a server where a Director vault is installed. You should also verify that the vault server meets the minimum requirements for memory, disk space, hardware and software.

When you upgrade a vault to version 8.7, the vault database engine is upgraded to SQL Server 2019 Express. Please keep the Director SQL Server instance updated with the latest security and critical updates from Microsoft.

After SQL Server is upgraded during the Director upgrade, the server must be rebooted. After the server restarts and an administrator signs in to the server, the Director upgrade restarts automatically.

A new port (12546) is used for replicating data between Director 8.7 vaults. When you upgrade a replication source vault (i.e., a Satellite or Active vault), the installer checks whether the vault can connect to port 12546 on the replication target vault. If port 12546 is not accessible, you can cancel or continue the upgrade. If you continue the upgrade, data will not replicate until you address the connection issues.

Note: Port 12546 is used instead of port 2547, which is used for replication in previous Director versions. After all source vaults have been upgraded to Director 8.70, port 2547 can be closed at the firewall.

If you upgrade a vault where the Reporting service is installed, the installer upgrades the Reporting service. If the Reporting service is registered to API – Monitoring before the upgrade, the Reporting service remains registered to the API after the upgrade. If you upgrade a vault where the Reporting service is not installed, you can choose to install it during the upgrade.

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.

To upgrade a vault:

1. Back up the vault. For database backup methods, see the *Director User Guide* or online help.
2. Close any PowerShell windows.

3. Take the vault offline by doing the following:
    a. In the left pane of the Director UI, click the + sign beside the vault.
    b. Click **Nodes**.
    c. 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).

    Note: 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. Read the software license agreement. Select **I accept the terms of the license agreement**, and then click **Next**.
7. On the Welcome page, click **Upgrade**, and then click **Next**.

    If a message states that the Base vault or Passive vault is not responding, you are upgrading a replication source vault that cannot connect to port 12546 on the replication target vault. You can upgrade the vault but data will not replicate until you address the connection issues. Click **Yes** to continue the upgrade or **No** to stop the upgrade.

    Messages show the upgrade progress.

    If a 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 server before services will start).

8. In the message box that recommends enabling updates for Microsoft products to ensure SQL Server remains up to date, click **OK**.
9. In the Reboot Required dialog box, click **Reboot Now** to restart the server.
10. After the server restarts, sign in to the server as an administrator.

    The Director upgrade restarts automatically. Messages show the upgrade progress.

11. If you are upgrading a Satellite vault, on the Director Setup Type page, select the **Do not reregister the Satellite vault to the Base vault** option, and then click **Next**.

    The Reporting service installer then begins.

12. Do one of the following:
    - Install the Reporting service as described in Install and register the Reporting service.
    - Upgrade the Reporting service by doing the following:
        i. On the software license agreement page, select **I accept the terms of the license agreement**, and then click **Next**.

ii. On the Welcome page for the Reporting service installation wizard, select **Upgrade** and then click **Next**.

iii. If the API registration method page appears, you can register the Reporting service to API – Monitoring as described in Install and register the Reporting service or choose **I do not want to register the Reporting service to the API at this time** to skip the registration, and then click **Next**.

The API registration method page does not appear if the Reporting service is already registered to API – Monitoring. The Reporting service will remain registered to the API after the upgrade.

iv. On the Maintenance Complete page, click **Finish**.

v. On the Maintenance Operation Complete page, click **Finish.**

- Finish upgrading Director without installing the Reporting service by doing the following:

i. On the Welcome page for the Reporting service installation wizard, click **Cancel**.

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

iii. On the InstallShield Wizard Complete page, click **Finish**.

Note: An *Installing Reporting Service* message appears, even though you are not installing the Reporting service. Please wait while the Director upgrade finishes.

iv. On the Maintenance Operation Complete page, click **Finish**.

13. Check that the vault services are running.

14. If the vault was transitioned to Offline in Step 3, set it back to Online using the Director UI.

9.2 Upgrade vaults for data replication

Before you upgrade vaults that are involved in data replication, please see the Director release notes to determine which vault versions are supported in many-to-one (N:1), one-to-one (1:1) or many-to-one-to-one (N:1:1) replication scenarios.

A target vault (that receives replicated data) must be upgraded to a supported version for replication before source vaults are upgraded. For example, in an N:1 scenario, the Base vault must be upgraded to a supported version for replication before Satellite vaults are upgraded. In an N:1:1 scenario, the Passive Base vault must be upgraded before the Active Base vault, and the Active Base vault must be upgraded before the Satellite vaults.

IMPORTANT: Be sure that each replication source vault (i.e., Satellite or Active vault) can connect to the replication target vault (i.e., Base or Passive vault) on the required ports. A new command port (12546) is used for replicating data between Director 8.7 vaults. For more information, see Ports.

9.2.1 Upgrade standalone vaults for replication

You can upgrade a standalone vault and set up replication with the vault in a 1:1, N:1 or N:1:1 scenario.

Before you upgrade vaults for data replication, please see the Director release notes to determine which vault versions are supported in 1:1, N:1 and N:1:1 replication scenarios.

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.

9.2.2 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.

Before you upgrade vaults that are involved in data replication, please see the Director release notes to determine which vault versions are supported in 1:1, N:1 and N:1:1 replication scenarios.

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.

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.

9.2.3 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.

Before you upgrade vaults that are involved in data replication, please see the Director release notes to determine which vault versions are supported in N:1 and N:1:1 replication scenarios.

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.

10 Upgrade Windows on a server where a Director vault is installed

This section describes how to upgrade the operating system on a server where Director is installed, while preserving the vault and its data. This might be required, for example, if you want to upgrade to a Director version that is not supported on the current operating system.

Note: This procedure does not describe how to upgrade a Director vault. See Upgrade a vault.

You can use this procedure to upgrade the operating system for a Director 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 2019 Express, SQL Server 2017 Express or SQL Server 2014 SP2 Express for the vault database engine, with either an EVAULT_DB or EVAULT_DB_V800 instance.

To upgrade Windows on a server where a Director vault 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. Take the vault offline by doing the following:

   a. In the left pane of the Director UI, click the + sign beside the vault.

   b. Click **Nodes**.

   c. Right-click the node and click **Rampdown**

   Note: Ramping down the vault allows backups to complete before the vault goes offline. This might take a long time.
4. 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.
5. 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 Reporting Service
   - Carbonite Server Backup Scheduler

6. Stop the SQL Server service used by Director and set the service startup to "Manual".

   If Director was not 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" and there will be a SQL Server instance named "EVAULT_DB" that is turned off and disabled. Do not change the startup setting for the EVAULT_DB SQL service.

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.

     Note: Starting with Director 8.6x, administrative permissions are required to copy the \conf folder.
   - **Database.** Save the vault database backup (data.bin file) that was generated in Step 4 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 installations. Workspace files are found in \Users\<*user*>\Documents\EVault InfoStage for some 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 by following documentation from 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 to "Automatic" and start the service if it is not already running.

b. Start all of the Director services that you stopped in Step 5 if they are not already running. For each service, set the startup type to “Automatic”.

c. Using the Director UI, bring the vault 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.

10.1 Recover from a failed Windows upgrade

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

To proceed with the recovery, you need the items saved in Upgrade Windows on a server where a Director vault 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.
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. Take the vault offline by doing the following:

   a. In the left pane of the Director UI, click the + sign beside the vault.

   b. Click **Nodes**.

   c. Right-click the node and click **Rampdown** (to allow backups to complete before bringing the vault offline. This might take a long time).

6. 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 Reporting Service
   - Carbonite Server Backup Scheduler

   Leave the SQL service (EVAULT_DB) running.

7. Restore the vault database backup (data.bin) from Step 4 of Upgrade Windows on a server where a Director vault is installed to the new vault installation:

    a. Copy the data.bin file into a folder on a local drive (e.g., C:\CSBrecovery\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.

8. Start all of the Director services (listed in Step 6).

9. Using the Director UI, bring the vault online.

10. Using the Director UI, verify that the vault configuration (Storage Groups and Locations) and metadata (Customer, Locations, Accounts, Users, Agents and Tasks) are now available.

11. Take the vault offline by doing the following:

    a. In the left pane of the Director UI, click the + sign beside the vault.

    b. Click **Nodes**.

    c. Right-click the node and click **Rampdown** (to allow backups to complete before bringing the vault offline. This might take a long time).

12. After you confirm that the vault is offline, stop all of the Director services (listed in Step 6). Leave the SQL service (EVAULT_DB) running.

13. Ensure that the server has the same drive letters as before the failed operating system upgrade.

14. 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.

15. If the Reports Extractor is used to upload data to EVault Reports, copy the Synchweb.cfg file (in …\Director\conf) to the server.

16. Start all of the Director services (listed in Step 6).

17. Using the Director UI, bring the vault online.

18. Using the Director UI, activate the vault licenses.

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

11 Uninstall a vault

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

You can also uninstall the Reporting service without uninstalling the vault. See Uninstall the Reporting service.

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. Click **Uninstall a program**.
3. Click **Carbonite Server Backup Director** in the list of programs.
4. Click **Uninstall**.
5. In the Carbonite Server Backup Director Setup Maintenance wizard, click **Next**.
6. In the confirmation message box, click **OK**.

   Messages appear while Director is being uninstalled.
7. On the Uninstallation Complete page, select **Yes, I want to restart my computer now**, and then click **Finish**.

11.1 Uninstall the Reporting service

You can uninstall the Reporting service without uninstalling the vault.

The Reporting service is also uninstalled when you uninstall a vault. See Uninstall a vault.

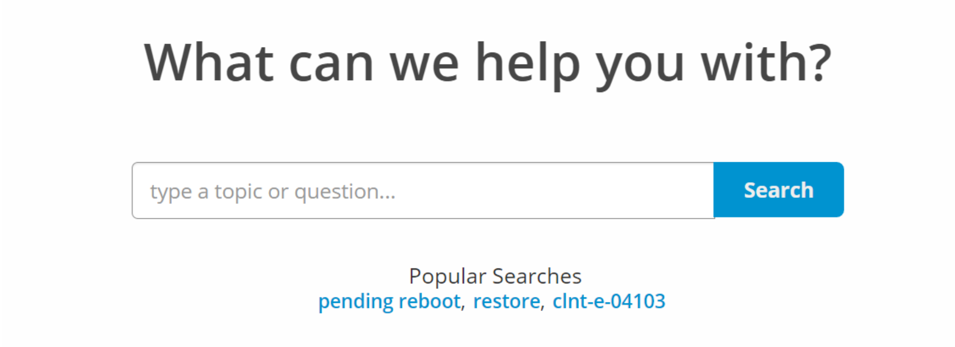
To uninstall the Reporting service:

1. Click **Start** and then **Control Panel**.
2. Click **Uninstall a program**.
3. Click **Carbonite Server Backup Reporting Service** in the list of programs.
4. Click **Uninstall**.
5. In the confirmation message box, click **Yes.**
6. On the Uninstall Complete page, click **Finish**.

12 Carbonite Server Backup Support

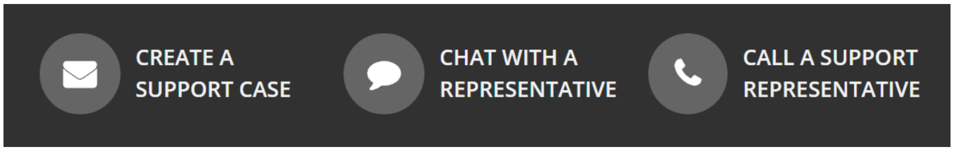
If you have a question about Carbonite Server Backup that isn't covered in this guide, our frequently-updated Knowledge Base contains comprehensive information. The Knowledge Base is your first stop when searching for any Carbonite Server Backup solutions you may need. We highly recommend searching here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

Knowledge Base: support.carbonite.com/evault


What can we help you with?
type a topic or question...
Search
Popular Searches
pending reboot, restore, clnt-e-04103

12.1 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: 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.