

EVault Software

Agent 7.3 for Microsoft Windows

User Guide



Revision: This manual has been updated for Version 7.33 (August 2014).  
Software Version: 7.33

© 2014 EVault Inc.

EVault, A Seagate Company, 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, EVault reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of EVault to notify any person of such revision of changes. All companies, names and data used in examples herein are fictitious unless otherwise noted.

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

EVault, A Seagate Company  
c/o Corporation Trust Center  
1209 Orange Street  
Wilmington, New Castle  
Delaware 19801  
[www.evault.com](http://www.evault.com)

EVault, EVault Software, EVault SaaS, and EVault DeltaPro, are registered trademarks of EVault Inc. All other products or company names mentioned in this document are trademarks or registered trademarks of their respective owners.

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

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

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

The EVault Software Agents and EVault Software Director applications also have the added security feature of an over the wire encryption method.

# Contents

<b>1</b>	<b>Introduction to the Windows Agent .....</b>	<b>1</b>
1.1	Windows Agent Plug-ins .....	2
<b>2</b>	<b>Installing and Modifying the Agent .....</b>	<b>4</b>
2.1	Hardware and Software Requirements .....	4
2.2	Required Permission .....	4
2.3	Operational Modes .....	5
2.4	Agent Licensing .....	5
2.5	Install the Windows Agent and Plug-ins .....	6
2.6	Installing or Upgrading the Windows Agent in silent mode .....	8
2.7	Modifying an Agent Installation.....	11
2.8	Repairing an Agent Installation.....	12
2.9	Installation Wizard Fields.....	12
2.10	Uninstalling an Agent.....	13
2.11	Uninstalling an Agent in Silent Mode .....	14
<b>3</b>	<b>Upgrading the Agent .....</b>	<b>15</b>
3.1	Preparing the Computer .....	15
3.2	Upgrading Program and Configuration Files.....	15
3.3	Upgrading an Agent that Uses OTM .....	16
3.4	Exchange backup reseeding after an upgrade.....	16
<b>4</b>	<b>Configuring the Agent .....</b>	<b>17</b>
4.1	Agent Properties Dialog Fields.....	17
4.2	Creating an Agent Profile.....	18
4.3	Bandwidth Throttling.....	18
4.4	Adding an Agent Group.....	19

4.5	Renaming the Workspace .....	19
4.6	Encrypting a Workspace .....	20
4.7	Options Dialog Fields .....	20
4.8	Setting Workspace Options .....	21
4.9	Vault Configuration Wizard Fields .....	21
4.10	Configuring a New Vault Connection.....	22
4.11	Reregistering an Agent.....	22
4.12	Improving Agent Performance.....	23
<b>5</b>	<b>Creating Jobs .....</b>	<b>24</b>
5.1	Creating a New Job .....	24
5.2	New Job Wizard Fields .....	24
5.3	Adding Files and Directories to a Job.....	25
5.4	Wildcards in Directory Paths.....	26
5.5	Wildcard Rules for Directories .....	26
5.6	Selection Rules.....	27
5.7	Removing Files and Directories from a Job.....	27
5.8	Backing Up System State Files .....	28
5.9	Backing Up System Files.....	28
5.10	Additional Backup Options .....	29
5.11	BMR-Type Backup Jobs.....	30
5.11.1	Creating a BMR Job with Windows CentralControl.....	30
5.11.2	Creating a BMR Job with Web CentralControl .....	30
5.12	Converting an Existing Job to a BMR Job .....	31
5.13	Scheduling a Job.....	31
5.14	NTFS Hard Links, Symbolic Links, Mount Points and Junctions .....	32
5.14.1	Hard Links .....	32
5.14.2	Symbolic Links.....	32

- 5.14.3 Mount Points ..... 32
- 5.14.4 Junctions ..... 32
- 6 Manual Data Backup; Process, Properties, Logs and Emails ..... 33**
  - 6.1 About Seeding and Reseeding ..... 33
  - 6.2 Running an ad hoc Backup..... 33
  - 6.3 Viewing Process Details ..... 33
  - 6.4 Viewing Safeset Properties ..... 34
  - 6.5 Viewing Log Files..... 34
    - 6.5.1 Notes on Agent Logs Behavior..... 34
  - 6.6 About Email Notifications ..... 35
- 7 Restoring Data ..... 38**
  - 7.1 Restoring with Web CentralControl..... 38
  - 7.2 Restoring with Windows CentralControl – Summary Steps ..... 42
  - 7.3 Restoring Data from a CD or DVD ..... 42
  - 7.4 Restoring Data from Another Computer ..... 43
  - 7.5 Restore Selection: Search Button Function ..... 43
  - 7.6 Viewing Restore Log Files ..... 44
  - 7.7 Restore Wizard Fields ..... 45
- 8 Working with the Cluster Plug-in ..... 47**
  - 8.1 Overview ..... 47
  - 8.2 Cluster Prerequisites and Configuration..... 47
  - 8.3 When using Web CentralControl..... 47
    - 8.3.1 Restarting the BUAgent Service..... 50
  - 8.4 When using Windows CentralControl..... 51
    - 8.4.1 Configuring the Virtual Cluster Agent..... 52

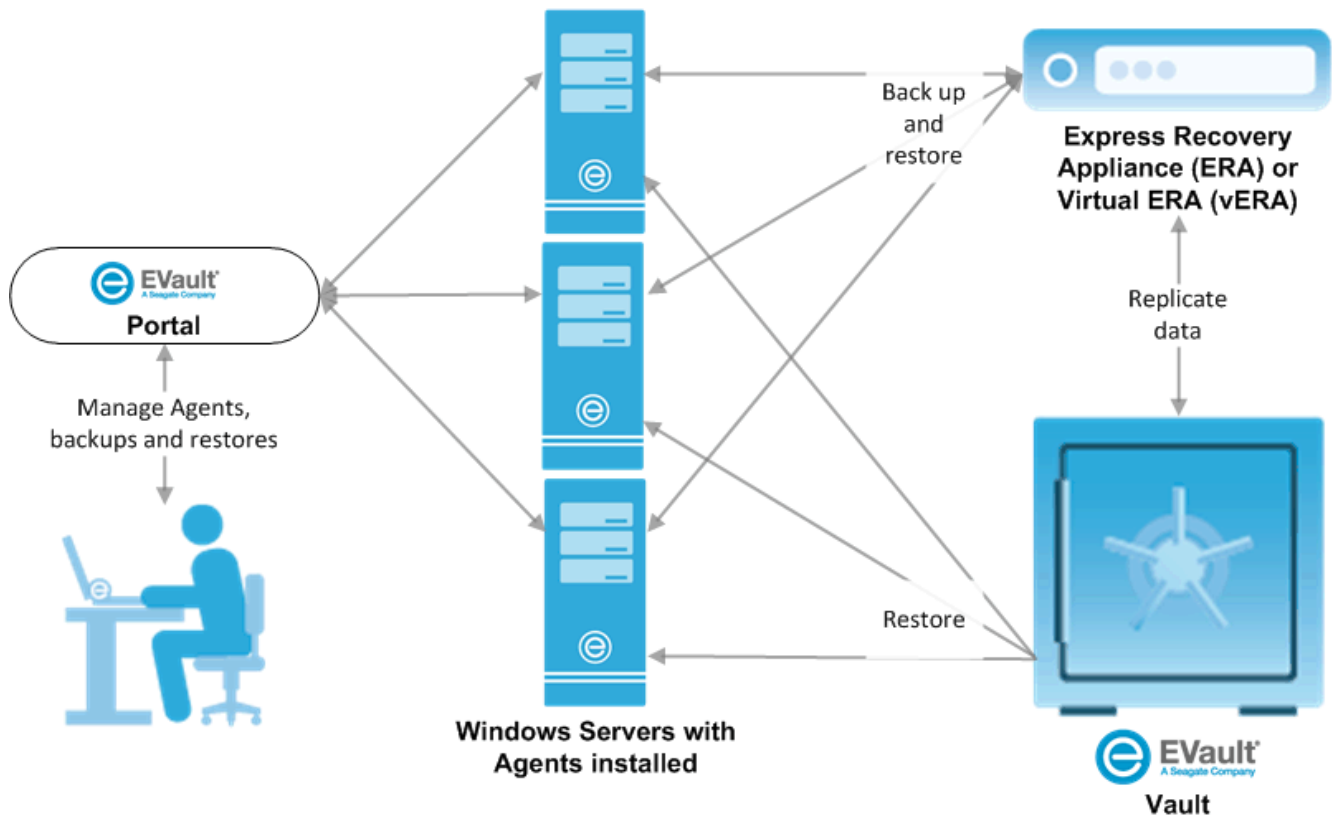
- 9 Working with the Command Line Interface ..... 53**
  - 9.1 VV.exe CLI Command Mode ..... 53
  - 9.2 General Command Options ..... 53
  - 9.3 Backup Command Options ..... 54
  - 9.4 Restore Command Options..... 56
  - 9.5 Synch Command Options..... 57
  - 9.6 Inventory Command Options..... 57
  - 9.7 List Command Options..... 57
  - 9.8 Forcereseed Option ..... 57
  - 9.9 Abbreviated Command Syntax ..... 58
  - 9.10 Specifying File Names in Command Syntax ..... 58
  - 9.11 Directory Layout and Configuration Files ..... 59
  - 9.12 Configuration Files ..... 60
  - 9.13 Global Job Settings..... 60
  - 9.14 Job Specific Settings ..... 61
  - 9.15 Using the Param\_filename Command ..... 63
  - 9.16 Scheduling Backups on a Windows Operating System ..... 63
  - 9.17 Configuring the Microsoft AT Service ..... 64
  - 9.18 How Simultaneously Scheduled Backups are Processed ..... 64
  - 9.19 VVAgent CLI Command Mode..... 65
  
- 10 Examples ..... 66**
  - 10.1 Example: Creating a Backup Job ..... 66
  - 10.2 Example: Running an ad hoc Backup ..... 68
  - 10.3 Example: Scheduling a Backup Job ..... 69
  - 10.4 Example: Checking Backup Results ..... 70
  - 10.5 Example: Running a Restore Job..... 70
  - 10.6 Example: Cross Computer Restore ..... 71

- 10.7 Example: Files Excluded from Backups ..... 72
- 10.8 Example: Ports Used by EVault Software ..... 73
- 11 Disaster Recovery ..... 74**
  - 11.1 Hardware Requirements..... 74
  - 11.2 Software Requirements ..... 74
  - 11.3 Windows Recovery Steps..... 75
  - 11.4 Windows Recovery Problems ..... 77
    - 11.4.1 2008 DR Special Procedures for Restoring with BCD..... 78
  - 11.5 Recovery Verification for Windows ..... 78
  - 11.6 Active Directory Restores ..... 79
    - 11.6.1 Troubleshooting..... 79

# 1 Introduction to the Windows Agent

EVault Windows Agent backs up data on Windows servers, and restores data from the backups.

The Agent is installed on Windows servers where you want to back up and restore data. As shown in the following diagram, you can use Portal to manage the Agent and jobs, back up data to a secure remote vault, and restore data from the backups. You can also use the legacy Web CentralControl and Windows CentralControl interfaces to manage the Agent and jobs.



The Windows Agent is available as a 64-bit and a 32-bit application. You must install the appropriate Agent on each Windows server (i.e., 64-bit Agent for a 64-bit system; 32-bit Agent for a 32-bit system).

The Windows Agent can back up:

- Files and folders on the Windows server.
- System files required for recovering the operating system, including registry and boot files.
- The entire system so that, in a disaster recovery situation, it can be restored to other hardware using System Restore.
- Files and folders on UNC shares.



## 1.1 Windows Agent Plug-ins

When installing a Windows Agent, you can install plug-ins and applications with additional functionality. The following table lists and describes plug-ins and applications that can be installed with the Windows Agent, and indicates whether they can be installed with the 64-bit or 32-bit Windows Agent.

Plug-in or component	Description
Agent Assistant	<p>Application that runs in the system tray of the server and indicates whether the Agent is operational, running a backup, or not ready for a backup.</p> <p>Available with both the 64-bit and 32-bit Windows Agent.</p>
Cluster Support Plug-in	<p>Backs up and restores files and folders on shared cluster disks. Also works with Exchange and SQL Server Plug-ins to protect Microsoft Exchange or SQL Server which use shared cluster disks. Jobs are automatically redirected to the active node on a failover.</p> <p>Available with both the 64-bit and 32-bit Windows Agent.</p>
Exchange 2010/2013 Plug-in	<p>Backs up and restores Exchange 2010 and 2013 databases. You can also restore individual mailboxes and messages using this plug-in and the Granular Restore for Microsoft Exchange application.</p> <p>Only available with the 64-bit Windows Agent.</p>
Exchange 2007 Plug-in	<p>Backs up and restores Exchange 2007 databases. You can also restore individual mailboxes and messages using this plug-in and the Granular Restore for Microsoft Exchange application.</p> <p>Only available with the 64-bit Windows Agent.</p>
Exchange 2007/2010 MAPI Plug-in	<p>Backs up and restores selected mailboxes and folders in a Microsoft Exchange 2007 or 2010 database.</p> <p><i>Note:</i> Support is ending for the Exchange MAPI Plug-in. You cannot create new backup jobs with this legacy plug-in. Existing jobs will be supported for a period of time.</p> <p><i>Note:</i> This Plug-in is not supported in Portal. To back up and restore using this plug-in, use the legacy Web CentralControl and Windows CentralControl interfaces.</p> <p>Only available with the 64-bit Windows Agent.</p>
Exchange 2003 Plug-in	<p>This plug-in is available in the 32-bit Windows Agent 7.33 installation kit, but is not supported. Exchange 2003 is not supported on Windows Agent 7.33 supported platforms.</p>

Plug-in or component	Description
Image Plug-in	<p>Backs up Windows volumes as images rather than backing up individual files and folders. You can restore complete volumes and specific files and folders from image backups. You can also restore entire systems from image backups using EVault System Restore. For more information, see Image Plug-in.</p> <p><i>Note:</i> You must use Portal to manage Image Plug-in backups and restores. This plug-in is not supported in the legacy Web CentralControl and Windows CentralControl interfaces.</p> <p>Only available with the 64-bit Windows Agent.</p>
Oracle Plug-in	<p>Backs up and restores Oracle databases.</p> <p>Available with both the 64-bit and 32-bit Windows Agent.</p>
SharePoint Plug-in	<p>Backs up and restores SharePoint 2007, 2003, and WSS 3.0 items, such as web sites, lists, and documents.</p> <p><i>Note:</i> Support is ending for the SharePoint Plug-in. You cannot create new backup jobs with this legacy plug-in. Existing jobs will be supported for a period of time. To back up and restore SharePoint 2013 or 2010 databases, use the SQL Server Plug-in. To restore items (e.g., site collections, web sites, lists, documents), use the SQL Server Plug-in and the Granular Restore for Microsoft SharePoint application.</p> <p><i>Note:</i> This Plug-in is not supported in Portal.</p> <p>Available with both the 64-bit and 32-bit Windows Agent.</p>
SQL Server Plug-in	<p>Backs up and restores SQL Server databases.</p> <p>Available with both the 64-bit and 32-bit Windows Agent.</p>

## 2 Installing and Modifying the Agent

This chapter provides information and procedures for installing the Agent on a computer with a supported Microsoft Windows operating system. For a list of supported platforms, see the Agent release notes.

### 2.1 Hardware and Software Requirements

The computer on which you install the Agent should meet the minimum hardware requirements for the operating system specified by Microsoft. In addition, a minimum of 200 MB of free disk space is required for the installation and operation of the Agent. An upgrade may require more.

If there is not enough disk space during installation, the application will issue a message. Also, for this installation, the system drive requires free space to decompress the package (regardless of which drive the installation targets). The actual amount of space will vary, but a recommended amount to 200 MB should suffice. The environment variables TEMP and TMP use %USERPROFILE% by default. Make sure that this variable points to a drive that has sufficient temporary space.

For specific requirements, see the Windows Agent release notes.

### 2.2 Required Permission

To install the Agent, you must have Administrator or equivalent permissions.

To manage an Agent from Windows CentralControl and Web CentralControl, the user identities and the BUAgent and VVAgent service accounts must be the same. If the service accounts are not identical, the BUAgent cannot perform status or administration functions. Use the VVAgent and BUAgent logs to determine the account under which the services are running.

If you are using Encrypting File System (EFS), you need additional permissions to back up files. If you do not have the correct permissions, you are denied access. ACLs for all subsequent files might not be backed up, and error messages might appear in the log. After you install the Agent, you need to change local security settings, or the default domain policy. To allow backups on an Agent using EFS, set the user right to **Act as part of the operating system** and add the **Logon as a service** right to the account.

**Note:** During an Agent installation (Modify/Repair/Upgrade), the Agent installation kit sets/resets the permissions on the Agent folder and all child items to full access for the Administrators and Backup Operators groups. Using the Modify option, the user has the choice to install Agent services under a Local System account, or another account (either created manually or automatically). For non Local System accounts, the created account is modified to be a part of the Administrators group, which allows full access to Agent folder. If a user requires access to Agent services, the user should be included in the Administrators or Backup Operators group.

## 2.3 Operational Modes

This table lists the Agent operational modes:

Operational Mode	Description
Ad-Hoc	A user can use Portal or a legacy CentralControl interface to configure backup and restore Jobs on an Agent. To configure backup and restore Jobs, the user must have Back Up Files and Directories permission.
Scheduled	A user can use Portal or a legacy CentralControl interface to schedule backup and restore Jobs on an Agent. The user does not need special privileges to run scheduled Jobs when the VVAGENT.EXE program is run as a system service by the system account user.
CLI	A user can use the command line interface (CLI) to execute backups and restores directly from the command line, or a batch file. To use the command line, a user must have Back Up Files and Directories permission. These permissions are automatically applied if the user is a member of the Backup Operators or Administrators groups.

## 2.4 Agent Licensing

A quota system is used to control Agent licensing. When an Agent connects to a vault, the vault automatically supplies the license. Licenses are required for most Agents and Plug-ins.

If an Agent connects to a vault and a license is unavailable, the backup for the new Agent fails. However, you can still complete a restore. Previously licensed Agents are unaffected by the failure. Contact your service provider to purchase additional licenses.

These error messages might appear when an Agent connects to a vault:

- Vault storage limit exceeded,
- Vault limit for Agent type exceeded, or type not found,
- Vault limit for Plug-in type exceeded, or type not found,
- Customer Quota for Plug-in type exceeded (Agent 5.6 and above only).

This table displays the tasks you can perform on the vault when an error or warning message appears:

Agent (pre-5.6)	If vault base license is invalid	If vault storage limit is exceeded	If vault limit for Agent type is exceeded	If vault limit for Plug-in type is exceeded	If customer quota for Plug-in type is exceeded
Registration	Allow	Allow	Allow	Client Key	N/A
Job Creation	Disallow	Allow	Disallow	Client Key	N/A



Backup	Allow	Allow	N/A	Client Key	N/A
Restore	Disallow	Disallow	N/A	Client Key	N/A
<b>Agent (5.6 and above)</b>					
Registration	Allow	Allow	Allow	Allow	Allow
Job Creation	Disallow	Allow	Warn	Warn	Warn
Backup	Disallow*	Allow	Disallow*	Disallow*	Disallow*
Restore	Disallow	Disallow	Disallow*	Disallow*	Disallow*
<b>System I (pre- 5.6)</b>					
Registration	Allow	Allow	Client Key	N/A	N/A
Job Creation	Disallow	Allow	Disallow	N/A	N/A
Backup	Allow	Allow	N/A	N/A	N/A
Restore	Disallow	Disallow	N/A	N/A	N/A

\* If the Agent already has a claim on the necessary licenses (it has previously done a backup of that type), the backup or restore operation is allowed.

“Client Key” refers to an older license key for the Agent. The vault does not use this key.

When you successfully register an Agent with a vault, you can perform backups and restores.

## 2.5 Install the Windows Agent and Plug-ins

*Note:* The Windows Agent is available as a 64-bit or 32-bit application. You must install the appropriate Agent for the system (i.e., 64-bit Agent for a 64-bit system; 32-bit Agent for a 32-bit system).

To install the Windows Agent and Plug-ins:

1. Double-click the Windows Agent installation kit.

The language selection dialog box appears.

2. In the language list, click the language for the Agent, and then click **OK**.


The installation wizard starts.


3. On the **Welcome** page, click **Next**.
4. On the **Support Information and Release Notes** page, click **Next**.



5. On the **License Agreement** page, read the license agreement. Click **I accept the terms in the license agreement**, and then click **Next**.
6. On the **Setup Type** page, do one of the following:
  - To install the Agent only, click **Typical**, and then click **Next**. Go to step 12.  
*Note:* The Agent is only installed if .NET Framework 2.0 is installed on the system.
  - To choose Plug-ins and components to install with the Agent, click **Custom**, and then click **Next**.
7. On the **Logon Credentials for Agent Services** page, specify an account for running Agent services:  
*Note:* The account must be in the Administrators group and have the “Log on as a service” right.
  - To run Agent services using the local system account, select **Use ‘Local System’ Account**.  
*Note:* A local system account cannot be used to back up UNC files and folders.
  - To automatically create an account for running Agent services, select **Create account automatically**.
  - To run Agent services using a custom account, select **Use custom account**. In the **Username** and **Password** boxes, enter the custom account username and password.
8. Click **Next**.
9. On the **Destination Folder** page, do one of the following:
  - To install the Agent in the default location (C:\Program Files\EVault Software), click **Next**.
  - To install the Agent in another location, click **Change**. In the **Change Current Destination Folder** dialog box, browse to the new installation folder, or enter it in the **Folder name** box. Click **OK**. On the **Destination Folder** page, click **Next**.

The **Custom Setup** page lists each Windows Agent component and plug-in that can be installed with the Agent that you are installing (64-bit or 32-bit). For more information, see [Windows Agent Plug-ins](#).

The following icon appears for each component that will be installed: 

The following icon appears for each component that will not be installed: 

*Note:* The “Backup Agent” is the Windows Agent and is always selected and installed.
10. On the **Custom Setup** page, do the following:
  - For each component that you want to install, click the button to the left of the component name, and then click **This feature will be installed on local hard drive**.
  - For each component that you do not want to install, click the button to the left of the component name, and then click **This feature will not be available**.
11. Click **Next**.

12. On the **Register Agent with Web CentralControl** page, specify the following information:
  - In the **Network Address** box, type the IP address or host name of the Portal for managing the Agent.
  - In the **Port** box, type the port number for communicating with the Portal. The default port is 8086.
  - In the **Username** box, type the name of the Portal user for the Agent. The user must be an Admin user or regular user. Typically, the user name is an email address.
  - In the **Password** box, type the password of the specified Portal user.
13. Click **Next**.
14. On the **Ready to Install the Program** page, click **Install**.
 

The **Installing EVault Software Agent** page appears while the Agent is being installed.
15. On the **InstallShield Wizard Completed** page, click **Finish**.
 

The unconfigured Windows computer appears on the Computers page for the specified user, and for other Admin users in the user's site. To configure the computer, add a backup job.

## 2.6 Installing or Upgrading the Windows Agent in silent mode

To install, upgrade, or uninstall the Windows Agent in silent mode, run the following command in the directory where the installation kit is located:

```
installKitName /s /v" /qn" [parameters] [featureParameters]
```

Where:

- *installKitName* is the name of the Windows Agent installation kit: Agent-Windows-x64-x-xx-xxxx.exe for 64-bit systems or Agent-Windows-x-xx-xxxx.exe for 32-bit systems. *x-xx-xxxx* represents the Agent version number.
- *parameters* are optional parameters for running the installation kit in silent mode. If a parameter is not included in the command, the default parameter value is used. For a list of available parameters, see [Table 1: Parameters](#).
- *featureParameters* are optional parameters for installing plug-ins and features in silent mode. See [Table 2: Feature parameters](#).

**Table 1: Parameters**

Parameter	Default Value	Description
ACCOUNTTYPE	LocalSystem	Possible values are LocalSystem, AutoCreate, and Custom.



Parameter	Default Value	Description
SERVICEACCOUNTNAME		If ACCOUNTTYPE is Custom, this field is required.
SERVICEACCOUNTPASSWORD		If ACCOUNTTYPE is Custom, this field is required.
REGISTERWITHWEBCC	False	Turns on/off registration of the Agent with Web CentralControl.
AMPNWADDRESS		If REGISTERWITHWEBCC is True, this field is required.
AMPPASSWORD		If REGISTERWITHWEBCC is True, this field is required.
AMPPORT	8086	
AMPUSERNAME		If REGISTERWITHWEBCC is True, this field is required.
EXTRACTMSI	False	Turns on/off extraction of the Microsoft Installer (MSI) package.
KEEPAMPREGISTRATION	True	Set this property to True to retain the previous Web CentralControl registration.
<i>/"language"</i>	1033 (English)	Specifies the language for the Agent. Available <i>language</i> values are: <ul style="list-style-type: none"> <li>• 1033 - English (United States)</li> <li>• 1036 - French (Standard)</li> <li>• 1031 - German</li> <li>• 1046 - Portuguese (Brazilian)</li> <li>• 1034 - Spanish</li> </ul> For example, to install the French version of the Agent, include the following parameter: <i>/L"1036"</i>
MSIPATH	C:\	If EXTRACTMSI is True, this property denotes the location of the extracted MSI and MST files.
SILENTINSTALLDIR= <i>\installFolder</i>	C:\Program Files\EVault Software\	Specifies an installation folder for the Agent. The installation folder must be enclosed in double quotation marks if there are spaces in the name or path.  Example: SILENTINSTALLDIR=" <i>c:\Program Files\EVault</i> "
TOTALUNINSTALL	False	If this property is <i>False</i> , uninstalling will only remove the program files.



**Table 2: Feature parameters**

Feature Parameter	Default Value	Description
FEATURECLUSTER={On Off}	Off	Turns on/off installation of the Cluster Plug-in.
FEATUREEXCHANGEMAPI={On Off}	Off	Turns on/off installation of the Exchange 2007/2010 MAPI Plug-in.  <i>Note:</i> Support is ending for the Exchange MAPI Plug-in. You cannot create new backup jobs with this legacy plug-in. Existing jobs will be supported for a period of time.  <i>Note:</i> This Plug-in is only available with the 64-bit Windows Agent, and is not supported in Portal.
FEATUREEXCHANGE={On Off}	Off	Turns on/off installation of the Exchange 2007 DR Plug-in.  <i>Note:</i> This Plug-in is only available with the 64-bit Windows Agent.
FEATUREEXCHANGE2010={On Off}	Off	Turns on/off installation of the Exchange 2010/2013 DR Plug-in.  <i>Note:</i> Only available with the 64-bit Windows Agent.
FEATUREMAESTRO={On Off}	Off	Turns on/off installation of the Agent Assistant.
BCKHELPURL		If FEATUREMAESTRO is True, this field is required.
BCKLOGINURL		If FEATUREMAESTRO is True, this field is required.
FEATUREORACLE={On Off}	Off	Turns on/off installation of the Oracle Plug-in.
FEATURESHAREPOINT={On Off}	Off	Turns on/off installation of the SharePoint Plug-in.
FEATURESQL={On Off}	Off	Turns on/off installation of the SQL Server Plug-in.
FEATUREVOLUMEIMAGE={On Off}	Off	Turns on/off installation of the Image Plug-in.  <i>Note:</i> Only available with the 64-bit Windows Agent.  <i>Note:</i> After the Image Plug-in is installed silently, the machine must be restarted before the Plug-in can use Changed Block Tracking (CBT) to identify data that has changed since a previous backup. Without CBT, the Agent reads all data when backing up a volume.

For example, to install the 64-bit Agent in a different directory, run the following command:

```
Agent-Windows-x64-x-xx-xxxx.exe /s /v" SILENTINSTALLDIR="C:\Program Files\Acme Software\" /qn"
```

*Note:* In each example shown, *x-xx-xxxx* represents the Agent version number.

To install the French version of the 32-bit Agent, run the following command:

```
Agent-Windows-x-xx-xxxx.exe /s /v" /qn" /l"1036"
```

where 1036 indicates that the French version of the Agent is installed.

To install the 64-bit Agent and register it with Web CentralControl, run a command similar to this:

```
Agent-Windows-x64-x-xx-xxxx.exe /s /v" REGISTERWITHWEBCC=True  
AMPNWADDRESS=123.456.com AMPUSERNAME=user@test.com AMPPASSWORD=password  
/qn"
```

To install the 32-bit Agent, and then register the Agent with Web CentralControl, run a command similar to this:

```
Agent-Windows-x-xx-xxxx.exe /s /v" FEATUREMAESTRO=on  
REGISTERWITHWEBCC=True AMPNWADDRESS=123.456.com AMPUSERNAME=test@test.com  
AMPPASSWORD=LetMeIn3 BCKLOGINURL=http://123.456.com/login/login.aspx  
BCKHELPURL=http://123.456.com/help/help.htm /qn"
```

To install the 64-bit Agent and the SQL Server Plug-in:

```
Agent-Windows-x64-x-xx-xxxx.exe /s /v" FEATURESQL=On /qn"
```

## 2.7 Modifying an Agent Installation

**Note:** To change the language of an Agent, uninstall the Agent program files, and then reinstall the Agent.

To modify the Agent:

1. Log on to the computer on which you want to modify the Agent.
2. Double-click the Agent Windows .exe file. To obtain the self-extracting installation file, contact your licensed service provider of EVault Software products.
3. Click **Next**.
4. Select **Modify**.
5. Complete the Agent installation wizard. For field descriptions, see [Installation Wizard Fields](#).
6. Click **Install**.

## 2.8 Repairing an Agent Installation

To repair an Agent installation:

1. Log on to the computer on which you want to repair the Agent.
2. Double-click the Agent Windows .exe file. To obtain the self-extracting installation file, contact your licensed service provider of EVault Software products.
3. Click **Next**.
4. Select **Repair**.
5. Complete the Agent installation wizard. For field descriptions, see [Installation Wizard Fields](#).
6. Click **Install**.

## 2.9 Installation Wizard Fields

These fields appear in the Agent installation wizard:

Field	Description
Typical	Installs the Windows Agent only.
Custom	Allows you to select the program options to install.
Install EVault Software Agent to	The path where the EVault Software Agent is installed. Click <b>Change</b> to select another location.
Register Agent with Web CentralControl	Registers the Agent with Web CentralControl. If you do not register the Agent with Web CentralControl, you manage it through Windows CentralControl.
Network Address	The IP address or Domain Name System (DNS) name for the Web CentralControl computer.
Port	The port used to communicate with the Web CentralControl computer.
Username	The user name used to access the Web CentralControl computer.
Password	The password used to access the Web CentralControl computer.
Skip Registration	Select this option if you want to manage the Agent with Windows CentralControl only.
Use 'Local System' Account	Uses a local system account.
Create account automatically	Creates an account to access and run Agent services automatically.

Field	Description
Use custom account	Creates a custom account to access and run Agent services.
Leave unchanged	Leaves the account credentials for Agent services unchanged.
Backup Agent	Installs or uninstalls the Agent.
Agent Assistant	Installs or uninstalls the Agent Assistant.
Cluster Support Plug-in	Installs or uninstalls the Cluster Support Plug-in.
Exchange 2003 Plug-in	This plug-in is available in the 32-bit Windows Agent 7.33 installation kit, but is not supported. Exchange 2003 is not supported on Windows Agent 7.33 supported platforms.
Exchange 2007 Plug-in	Installs or uninstalls the Exchange 2007 DR Plug-in.
Exchange 2010/2013 Plug-in	Installs or uninstalls the Exchange 2010/2013 DR Plug-in.
Exchange 2007/2010 MAPI Plug-in	Installs or uninstalls the Exchange 2007/2010 MAPI Plug-in.
Image Plug-in	Installs or uninstalls the Image Plug-in.
Oracle Plug-in	Installs or uninstalls the Oracle Plug-in.
SharePoint Plug-in	Installs or uninstalls the SharePoint Plug-in.
SQL Server Plug-in	Installs or uninstalls SQL Server Plug-in.
You are currently registered to Web CentralControl at the following address	Displays the Web CentralControl registration information.
Keep my current registration	Keeps the Web CentralControl registration.
Change registration	Changes the Web CentralControl registration.
Program files only	Removes the Agent program files.
Total Uninstall	Uninstalls the Agent.

## 2.10 Uninstalling an Agent

To uninstall an Agent:

1. Log on to the computer where you want to uninstall the Agent.
2. Double-click the Windows Agent installation kit. To obtain the self-extracting installation file, contact your licensed service provider of EVault Software products.



3. Click **Next**.
4. Select **Remove**.
5. Select **Total Uninstall**.
6. Click **Remove**.
7. Click **Finish**.

## 2.11 Uninstalling an Agent in Silent Mode

To uninstall an Agent in silent mode:

1. Log on to the computer on which you want to uninstall the Agent.
2. Open a command prompt and do one of the following:
  - To remove the Agent and all of its configuration files, run this command:

```
installKitName /s /x /v"/qn TOTALUNINSTALL=True"
```

- To remove the Agent but leave its configuration files, run this command:

```
installKitName /s /x /v"/qn TOTALUNINSTALL=False"
```

Where *installKitName* is the name of the Windows Agent installation kit: Agent-Windows-x64-x-xx-xxxx.exe for 64-bit systems or Agent-Windows-x-xx-xxxx.exe for 32-bit systems. x-xx-xxxx represents the Agent version number.

## 3 Upgrading the Agent

This chapter provides information and procedures for upgrading the Agent for Microsoft Windows. If you are upgrading an Agent that is earlier than version 5.6, you must upgrade the Agent to version 5.6, and then upgrade to the current Agent version.

### 3.1 Preparing the Computer

To prepare the computer for an Agent upgrade, complete these tasks:

- Back up all files and subdirectories in the Agent installation directory. Do not attempt an upgrade without a backup.
- Remove unused server profiles in Global.vvc.
- Delete or reassign all jobs that back up to a vault you deleted from Global Settings.  
Do not delete or reassign jobs that back up to a directory on disk. When you upgrade the Agent, the Jobs are registered on the first vault listed in Global Settings.
- Synchronize all backup jobs.
- Check the backup logs for each job for **Validation failed** errors. Verify the validity of the error messages. If the latest backup log does not contain error messages, synchronize with the vault and check the Synch log.
- Verify that you have the correct version of EVault Director Software installed. See the Agent release notes for the specific requirements for each operating system.

### 3.2 Upgrading Program and Configuration Files

Do not run multiple upgrade processes at the same time.

To upgrade the Agent program and configuration files:

1. Log on to the computer on which you want to upgrade the Agent program and configuration files.
2. Double-click the Agent Windows .exe file. To obtain the self-extracting installation file, contact your licensed service provider of EVault Software products.
3. Click **Yes**.
4. Complete the Agent installation wizard. For field descriptions, see [Installation Wizard Fields](#).
5. Click **Finish**.

6. Open the log file and verify that the upgrade was successful. If the upgrade failed, the Global.vvc, Job vvc, and Delta files revert to the previous versions. However, they do not work with new executables unless you manually replace them with the backup files. Try the upgrade again. If it fails, contact your service provider.
7. Create a backup for each Job. This uploads new configuration files from the Agent to the Director.

### 3.3 Upgrading an Agent that Uses OTM

To upgrade an Agent that has older jobs configured to use Open Transaction Manager (OTM):

1. Log on to the computer on which you want to upgrade the Agent.
2. Double-click the Agent Windows .exe file. To obtain the self-extracting installation file, contact your licensed service provider of EVault Software products.
3. Click **Yes**.
4. Complete the Agent installation wizard. For field descriptions, see [Installation Wizard Fields](#).
5. Click **Finish**.

VSS open file manager becomes the default open file manager and OTM is disabled. However, otmlapi.dll/otman5.sys is still on the upgraded system. Backups created after you upgrade the Agent are deltas and complete successfully. New Jobs use VSS open file manager, but you can select OTM.

### 3.4 Exchange backup reseeding after an upgrade

The following condition can cause your backups to reseed after an upgrade: Microsoft Exchange mailbox names in Agent 7.0 and later use the same name as the Exchange System Manager Console. If the mailbox names are not identical, a reseed occurs.

This condition only applies if you upgrade older Agents with Jobs that were created and backed up with 4 KB blocks (from 4.x to 5.6 to 6.0) to 6.01 to 6.10, 6.3, 6.5, or 6.6. During the upgrade from 6.0 to 6.01 to 6.10, 6.30, 6.5, or 6.60, the older 4 KB blocks change to the newer 32 KB blocks, causing a reseed on the next backup.

## 4 Configuring the Agent

This chapter provides information and procedures for configuring the Agent. To configure an Agent to run a backup, complete these tasks:

- Create an Agent profile
- Save the workspace
- Configure the vault
- Create a Job
- Schedule a Job

You use CentralControl to manage and configure the Agent. You can use a single CentralControl instance to control multiple Agents. Before you can perform backups and restores:

- You must install an Agent on the computer that you want to back up.
- You must connect CentralControl to the Agent.
- You must supply a Name, IP or DNS address, and user and password credentials.
- You must register the computer on which the Agent is installed on the vault. Registration allows the Agent to connect to the vault.

If you are restoring from another computer, you must reregister the Agent computer on the vault.

### 4.1 Agent Properties Dialog Fields

These fields appear in the **Agent Properties** dialog:

Field	Description
Description	The Agent profile name.
Network address	The IP address or Domain Name System (DNS) name for the Agent computer.
Default port	The default port used to communicate with the Agent computer.
Custom port	A custom port used to communicate with the Agent computer.
User name	The user name used to access the Agent service.
Password	The password used to access the Agent service. This field is case sensitive.
Save password	Saves the password used to access the Agent service.
Domain	The Microsoft Windows domain on which the Agent computer is installed. If you are not using a domain name, enter a period (.).



## 4.2 Creating an Agent Profile

You create an Agent profile for every computer that you want to back up. To create an Agent profile:

1. Open CentralControl.
2. Right-click **Workspace (untitled)** in the left pane and select **New Agent**.
3. Complete the fields in the Agent Properties dialog. For field descriptions, see [Agent Properties Dialog Fields](#).
4. Click **Get Status** to test the Agent profile.
  - a. In the DNS or IP information is incorrect, the message `Failed to connect to <...>` appears. If the authorization information is incorrect, the message `Failed to authorize user () or user () possesses insufficient privilege` appears. Contact your service provider
5. Click **OK**.
6. Click **OK** again.

## 4.3 Bandwidth Throttling

Bandwidth throttling settings specify the amount of bandwidth consumed by an Agent for backups and restores. For example, you might want restrictions on daytime backups and restores so that online users are not affected, and then unlimited usage at night so that scheduled backups run as fast as possible.

Bandwidth throttling values are set at the computer (Agent) level. If three jobs are running at the same time on the same computer, each job gets 1/3 of the specified maximum bandwidth.

Bandwidth settings include:

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

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

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

## 4.4 Adding an Agent Group

To save time, you can apply Agent information to multiple Agents through an Agent group.

To add an Agent group:

1. Open CentralControl.
2. Right-click **Workspace (untitled)** in the left pane and select **New Group**.
3. Enter a name for the Agent group in the **Group name** field. Click **OK**.
4. Right-click the group in the left pane and select **Import Agents**.
5. Browse to the location of the Agent comma separated values (CSV) file.
6. Click **Open**.

## 4.5 Renaming the Workspace

To save Agents, Jobs, and other settings you must save your workspace. You can change the workspace name, or keep the default name MyWorkspace. You can save multiple workspaces, but you can only open one workspace at a time.

You use workspaces to organize your Agent connections into logical groups. For example, you can create a workspace for individual company departments.

To rename and save a workspace:

1. Open CentralControl.
2. Select **Workspace (untitled)** in the left pane.
3. Click **File** and then **Save Workspace As**.
4. Enter a name for the workspace in the File name field.
5. Click **Save**.

## 4.6 Encrypting a Workspace

Workspaces contain user names and passwords. It is recommended that you encrypt your workspaces to prevent unauthorized access. To encrypt your workspace:

1. Open CentralControl.
2. Select a workspace in the left pane.
3. Click **File** and then **Workspace Password**.
4. Select an encryption type in the **Encryption type** list.
5. Enter a password in the **New password** field.
6. Enter the password in the **Confirm password** field.
7. Click **OK**.

## 4.7 Options Dialog Fields

These fields appear in the **Options** dialog:

Field	Description
Automatically reload last workspace on startup	Automatically loads the last saved workspace when you start the CentralControl application. If you do not select this option, you must select one manually.
Auto-refresh display for selected agent every <#> minutes	The number in minutes that the Agent is polled for updated information. Valid numbers are 1 to 15. To refresh data manually, click <b>Refresh</b> , or press <b>F5</b> .  Do not add a separator, such as a decimal point, or comma in the field.
Update progress display every <#> seconds	The number in seconds information in the Progress Monitor updates. Valid numbers are 5 to 10000.  Do not add a separator, such as a decimal point, or comma in the field.
Return maximum <#> of files and directories	The maximum number of files and directories returned when you select to view them. Valid numbers are 10 to 10000000. This setting optimizes the system when there are large directories, and you have to wait while the filenames are read and displayed. If more entries are returned than the specified number, a prompt appears asking if you want to see them all.  Do not add a separator, such as a decimal point, or comma in the field.

Field	Description
Default Text Viewer	This is the viewer that is used to show logs (XML based), and other text based files

## 4.8 Setting Workspace Options

To set workspace options:

1. Open CentralControl.
2. Select a workspace in the left pane.
3. Click **Tools** and then **Options**.
4. Complete the fields in the **Options** dialog. For field descriptions, see [Options Dialog Fields](#).
5. Click **OK**.

## 4.9 Vault Configuration Wizard Fields

These fields appear in the **Vault Configuration** wizard:

Field	Description
Register as a new computer	Registers the Agent as a new computer on the vault.
Reregister previously registered computer	Changes existing Agent connection settings.
Profile name for the new vault	The name of the Agent profile.
New address	The IP address or Domain Name System (DNS) name for the Agent computer.
New ports	The Agent computer communication port.
Try to reconnect every <> seconds	The time in seconds that the vault attempts to reconnect to an Agent when a connection is interrupted.
Stop reconnection attempts after <> minutes	The time in minutes that the vault stops trying to reconnect to the Agent.
Enable over the wire encryption for transmission to/from the vault	Applies over the wire encryption to secure data sent from the Agent to the vault.
Account	The name of the vault.

Field	Description
User name	The user name used to access the vault.
Password	The password used to access the vault. This field is case sensitive.

## 4.10 Configuring a New Vault Connection

To provide fast, local vault access for backups and restores, back up Windows data to an Express Recovery Appliance (ERA) or virtual ERA (vERA). The data can then be replicated to the EVault cloud to ensure offsite protection in the case of a disaster.

If you choose not to use an ERA or vERA, consider using a QuickShip vault (QSM) to seed Hyper-V backups locally. The data can then be imported into the EVault cloud.

To configure a vault connection:

1. Open CentralControl.
2. Right-click an Agent in the left pane and select **Agent Configuration**.
3. Click the **Vaults** tab.
4. Click **New**.
5. Complete the fields in the Vault Configuration wizard. For field descriptions, see [Vault Configuration Wizard Fields](#).
6. Click **Finish**.

## 4.11 Reregistering an Agent

When you delete an Agent from a vault, the Agent profile is deleted from the computer on which the Agent is installed. If you add an Agent to the vault with a name that you deleted, the vault recognizes it and prompts you for a reregistration. You must reregister an Agent when you restore from another computer.

When the original Agent profile is downloaded from the vault to the Agent, these fields are removed:

- The encrypted password.
- The domain, username, and password of the account used to perform a MAPI backup.
- The domain, username, and password of the account used to back up an SQL Server.
- The domain, username, and password of the account used to back up a networked drive.

When a reregistration or restore from another computer occurs, and the backup or restore fails, messages similar to this appear in the error log:

```
PARS-W-0002    Due to a computer registration, configuration file
"weekend" is missing the following information:
```

```
PARS-W-0002    Enc_Password (Encryption Password)
```

```
please use the CentralControl to re-enter the missing information.
```

The Agent reregistration process creates a Register log file that lists missing Job file settings.

You must reconfigure the Job file before you can perform a backup or restore on a Job file with missing settings. The backup or restore log files indicate which Job settings are missing.

## 4.12 Improving Agent Performance

When you install the Agent on a computer with dual processors you can use multi-threading to improve the performance of backups and restores for files larger than 32 KB. You can use these threading models:

- Single threading – A single thread is used for all data processing.
- Combined threading – Two threads are used for all data processing.
- Block Processor threading – Four or more threads are used for all data processing.

This table lists the threading options that you can specify for a backup or a restore in the Job CFG file or the command line with VV.EXE:

Option	Description
Default	The Agent checks the both backup settings and the current hardware to determine which model it should use. This is the default setting.  On a single CPU system, the single threading model is used.  On a multi-CPU system the threading model used is dependent on the backup settings. If compression or encryption is turned ON, the Block Processor threading model is used, otherwise the Combined threading model issued.
Single	A Single threading model is used.
Combined	The Combined threading model is used.
Block Processor	The Block Processor threading model is used with up to four processing threads.
Maximum Block Processor	The Block Processor threading model is used with up to five processing threads. You cannot specify this option for a restore.

## 5 Creating Jobs

This chapter provides information about creating and scheduling backup jobs.

### 5.1 Creating a New Job

To create a job:

1. Open Windows CentralControl.
2. Right-click an Agent in the left pane and select **New Job**.
3. Complete the fields in the New Job wizard. For field descriptions, see [New Job Wizard Fields](#).
4. Click **Finish**.

### 5.2 New Job Wizard Fields

These fields appear in the **New Job** wizard:

Field	Description
Backup source type	The source of the data to back up.
ANSI: Files with filenames not in the current language may not be backed up	Excludes files with filenames that are not in the current language from the backup.
Unicode: All files will be backed up. Some filenames will display improperly in the file selection screens.	Includes all files in the backup.
Destination	Select an existing vault profile, or click New and create a new profile.
Job name	The name of the Job. The name must be 1-30 characters in length and must consist of letters (A-Z and a-z), numbers (0-9) and/or <code>_</code> , <code>-</code> , <code>\$</code> (underscore, dash, dollar sign). The following names cannot be used as Job names when connected to an Agent: PRN, CON, LPT1, LPT2, LPT3, LPT4, COM1, COM2, COM3, COM4, NUL, AUX, Register, or Global.)
Data Files	Backs up data files.
Bare Metal Restore	Back up the entire drive.
System State	Back up system files.

Field	Description
RSM database	Back up Removable Storage Media (RSM) database.
Event logs	
Quick file scanning	
Disable deferring	
Backup time window	The time in hours that the backup runs.
Encryption type	The encryption type for the Job.
Password	The encryption password. Data cannot be recovered if you lose or forget the password.
Verify password	The encryption password.
Create log file	Creates a log file. Sets the log file options.
Log detail level	The amount of detail included in the log file.
Automatically purge expired log files only	Deletes log files when the safeset expires.
Keep the last <> log files	The number of log files to keep.
Run the Job immediately	Runs the Job immediately.
Schedule a backup	Creates a schedule to complete the Job weekly or monthly.
Just exit from this wizard	Saves the Job without running it.

### 5.3 Adding Files and Directories to a Job

Exclude any files and directories that do not need to be backed up, and files and directories that will be open during the backup. This includes the Agent installation directory. Although the backup works, error messages such as `error opening file` are added to the log file.

To add files and directories to a Job:

1. Open Windows CentralControl.
2. Right-click a Job in the left pane and select **Properties**.
3. Click the **Source** tab.



4. Select **Data Files** in the top pane.
5. Click **Add**.
6. Select files or directories in the top pane.
7. Click **Include**.

If you include a directory, the **Confirm Include** dialog appears. Select **Recursive** to include all files in the directory, or create a filter to specify the files you want to include. Use an asterisk (\*) to include files that match the partial name or extension, or the start, middle, or end of a directory name.

8. Click **OK**.
9. Click **OK** again.

## 5.4 Wildcards in Directory Paths

EVault Software Director does not support or recognize wildcard folder selections for restores. However, the Agent supports wildcards in paths for both inclusion and exclusion.

For example, assume you have on your server, a directory named Users, and below it are directories for each user's name, in alphabetical order (C:\Users\

If you use a wildcard with each letter, A\*, B\*, C\*, D\*, E\*, (and recursive) for one backup, you can get all the data, automatically including any new ones added, and excluding old ones deleted. Another backup Job may use F\*, G\*, H\*, I\*, J\* (for example).

You can filter further using "include only files matching this filter".

When you have finished selecting (and including) all the files and directories you want for this backup Job, click **Yes** and you will return to the Source screen. Here, you can click **Next** to continue to the next step of the New Job Wizard.

## 5.5 Wildcard Rules for Directories

In these examples, a path element is a part of the path (\ ... \) of a directory. If the wildcards are not used in this way, you will see an error message. Note that the \*.\* at the end of the selection represents wildcards for the files. This is different from the wildcards for the folders.

- Only the last path element of the selection can contain a wildcard:

- Supported: C:\Projects\A\*\.\*.\*
- NOT supported: C:\P\*\Active\.\*.\*
- A path element of a selection can only contain one wildcard:
  - Supported: C:\Project\*\.\*.\*
  - NOT supported C:\P\*j\*\.\*.\*
- The wildcard can appear anywhere in the path element:
  - Supported: C:\Project\*\.\*.\*
  - Supported: C:\\*rojects\.\*.\*
- The Agent supports one path element with a wildcard per selection:
  - Supported: C:\Projects\User\*\.\*.\*
  - NOT supported: C:\P\*\U\*\.\*.\*

## 5.6 Selection Rules

The more specific path is selected first if the file specification is the same. For example:

```
C:\DIR1\DIR2\.*.DAT wins over C:\DIR1\.*.DAT
```

The more specific path is selected first if the file specification is the same. For example:

```
C:\DIR1\.*.DAT wins over C:\DIR1\.*.*
```

If there is a conflict, and one has a more specific path and the other has a more specific file, then the exclude wins. For example:

Exclusion of C:\.\*.DAT wins over inclusion of C:\DATA\.\*.\*. However inclusion of C:\.\*.DAT does not win over exclusion of C:\DATA\.\*.\*

## 5.7 Removing Files and Directories from a Job

To remove files or directories from a job:

1. Open Windows CentralControl.
2. Right-click a Job in the left pane and select **Properties**.
3. Click the **Source** tab.

4. Select a file or directory in the lower pane.
5. Click **Remove**.
6. Click **Yes**.
7. Click **OK**.

## 5.8 Backing Up System State Files

You can back up System State files. System and state files are critical to the recovery of the operating system. Your operating system determines what files are necessary for a System State backup. Typically, a System State backup includes these files:

- COM+ Class Registration database
- Registry
- Boot files (except for Boot Configuration Data (BCD))
- Windows system files
- Performance Counter

To back up System State files:

1. Open Windows CentralControl.
2. Right-click a job in the left pane and select **Properties**.
3. Click the **Source** tab.
4. Select **System State** in the top pane.
5. Click **OK**.

## 5.9 Backing Up System Files

System and state files are critical to the recovery of the operating system. Including system files with your backup allows you to recover from a corrupted file system, unintentionally removed service packs, or a bare metal restore. When you back up the system files, you can return to the state of the backup without reinstalling the operating system and service packs.

The operating system and service packs that you install determine what files are included with the system files backup. Windows makes a dynamic list of these DLLs when you include them in your backup.

To back up system files:

1. Open Windows CentralControl.

2. Right-click a job in the left pane and select **Properties**.
3. Click the **Source** tab.
4. Select **System State** in the top pane.
5. Click **Options**.
6. Select **Backup system files**.
7. Click **OK**.
8. Click **OK** again.

## 5.10 Additional Backup Options

When you create a new job and select **Network UNC Share** as the backup source type, you can only include data files in the backup.

When you create a new job and select **Local Drive Only** as the backup source type, you can include these items in your backup:

- **Data Files** – Select this option to back up files and directories.
- **Bare Metal Restore** – Select this option to create a BMR-type backup.
- **System State** – Select this option to back up System State and system files.
- **RSM database** – Select this option to back up the Removable Storage Manager (RSM) database. An RSM database allows multiple applications to share local robotic media libraries and disk drives, and manage removable media within a single-server system. The RSM database store persistent data.  
The RSM database option is available as a job option if the RSM service is installed and functioning on the client.
- **Event logs** – Select this option to back up the Windows event logs. Event logs store events that you can view with the Windows Event Viewer program.
- **IIS Metabase** – Select this option to back up the Internet Information Services (IIS) Metabase. The IIS Metabase is a database similar in structure to the Windows Registry. The IIS Metabase is optimized for IIS, and provides hierarchical storage and fast retrieval of IIS configuration properties for websites, virtual directories, FTP sites, SMTP, and NNTP sites.
- **Terminal Services Licensing Database** – Select this option to back up the Terminal Service licensing database. This option is available when Terminal Services is installed and licensed on Windows Server 2003 or a Windows Server 2008 server.
- **Active Directory** – Select this option to back up the Windows Active Directory. It supports the recovery of replicated data where the target is the primary Active Directory server.

## 5.11 BMR-Type Backup Jobs

You can use data from a Bare Metal Restore (BMR) type backup to apply a complete system backup to a new computer. You use the EVault System Restore (ESR) application to apply the BMR data. See the *ESR User Guide* for more information.

To create a BMR-type job, you include the Bare Metal Restore directory in a local backup job. When you select Bare Metal Restore, the information necessary for an EVault System Restore is added to your backup.

BMR jobs consume an EVault System Restore license when they run.

**Note:** Encrypted volumes (BitLocker, TrueCrypt, etc.) are not supported with BMR jobs.

### 5.11.1 Creating a BMR Job with Windows CentralControl

To create a BMR-type backup job:

1. Make sure that the appropriate license is available on the vault account.
2. Open Windows CentralControl.
3. Create a new job. Select **Local Drive Only** and **Unicode** on the Backup Source Type menu. See [Creating a Job](#).
4. Select a vault.
5. Name your job.
6. From the New Job Wizard - Source page, select **Bare Metal Restore**.
7. If you wish, add more data to the backup (even if it is not part of BMR).
8. Proceed and finish creating the job as you normally would.

### 5.11.2 Creating a BMR Job with Web CentralControl

To create a BMR-type backup job:

1. Make sure that the appropriate license is available on the vault account.
2. Open Web CentralControl.
3. Highlight a Windows Agent, and select **Add > Job**.
4. Name your job. Select **Local System** for the Backup Source Type.

5. On the data selection page, select **Bare Metal Restore**.
6. If you wish, add more data to the backup (even if it is not part of BMR).
7. Proceed and finish creating the job as you normally would.

## 5.12 Converting an Existing Job to a BMR Job

You can change an existing local system job to a BMR job. Selecting **Bare Metal Restore** does not alter existing data selections.

To convert to a BMR-type backup job:

1. Make sure that the appropriate license is available on the vault account.
2. Open Windows CentralControl.
3. Right-click on a job and select **Properties**.
4. Click the **Source** tab.
5. Select **Bare Metal Restore** in the top pane. If the data in **Data Files** overlaps with BMR data, clear the **Data Files** selection.
6. Save the job and run it to create the BMR safeset.
7. Check the job log to make sure that the backup does not reseed.

## 5.13 Scheduling a Job

To schedule a backup or synchronize job to run at a scheduled time:

1. Open Windows CentralControl.
2. Right-click an Agent in the left pane and select **Schedule Entries**.
3. Click **New**.
4. Complete the fields in the **Schedule** wizard.
5. Click **Finish**.
6. Click **OK**.

## 5.14 NTFS Hard Links, Symbolic Links, Mount Points and Junctions

### 5.14.1 Hard Links

Backing up and restoring hard links locally will preserve the link(s). When restoring remotely, the link is preserved only if the files are both restored to their original location and overwrite the existing files. If the original files are not overwritten, or if the incoming files are restored to an alternate location, the link breaks.

**Note:** Remote hard links are not supported (e.g. UNC paths).

### 5.14.2 Symbolic Links

Restored symbolic links point to their target's new location, if the target is also part of the backup and restore.

### 5.14.3 Mount Points

The above functionality also applies to Mount Point recovery.

**Note:** Remote mount points are not supported (e.g. UNC paths).

### 5.14.4 Junctions

If junctions are restored to their original location, all link functionality will be preserved. If restored to an alternate location, the junction will revert to a normal, empty directory. If recovery to an alternate location is desired, the junction must be explicitly selected for backup and will duplicate the contents of its target directory without preserving junction functionality.

**Note:** Remote/alternate junctions are not supported.

## 6 Manual Data Backup; Process, Properties, Logs and Emails

This chapter provides information and procedures for running a manual or ad-hoc backup as well as viewing process details, safeset properties, logs and email notifications.

### 6.1 About Seeding and Reseeding

When you run your first backup, a full safeset is created on the vault. This first safeset is called a seed and it contains all of the selected backup data. Subsequent backups are deltas that are applied to the first full backup to create subsequent safesets. This way a current full backup is always available.

If the Agent detects a change, such as the encryption type or password changing, the next backup is a reseed.

With a reseed, your backup takes longer to complete and a message about reseeding is added to the log file.

### 6.2 Running an ad hoc Backup

To run an unscheduled or ad hoc backup:

1. Open Windows CentralControl.
2. Right-click a job in the left pane and select **Backup**.
3. Complete the fields in the **Backup** wizard.
4. Click **Finish**.
5. Click **Close**.

### 6.3 Viewing Process Details

Processes are the backups, synchronizations, and restores performed by the Agent. Process information is normally deleted within an hour. To delete process information manually, click **Delete Entry**. Information about the job is retained in the log files. To view process information:

1. Open Windows CentralControl.
2. Expand an Agent in the left pane.
3. Click **Processes**.
4. Double-click a process in the right pane.
5. Click **Close**.





## 6.4 Viewing Safeset Properties

Safesets are sets of sequentially numbered backup data on the vault. Safesets remain on the vault until their retention date expires. To view safeset properties:

1. Open Windows CentralControl.
2. Expand an Agent in the left pane.
3. Expand a job.
4. Click **Safesets**.
5. Double-click a safeset in the right pane.
6. Click **OK**.

## 6.5 Viewing Log Files

Log files provide details of events that occurred during a backup, synchronization, or restore. To view log files:

1. Open Windows CentralControl.
2. Expand an Agent in the left pane.
3. Expand a job.
4. Click **Logs**.
5. Double-click a log in the right pane.

### 6.5.1 Notes on Agent Logs Behavior

1. XLOG files - updating:
  - a. Backup removes the backup logs (log and xlog) based on the log setting. If a log setting is not specified, retention settings are used.
  - b. Synchronization does NOT remove any logs (log and xlog).
  - c. Restore removes restore logs (log and xlog) based on the log setting. If a log setting is not specified, restore logs are not removed.

2. DTA/DTX files - updating:
  - a. Backup removes the DTA/DTX files except the previous one. If a backup is completed successfully, you should see two sets of DTA/DTX files: one for the previous backup and one for the current backup.
  - b. Synchronization removes DTA/DTX files except from the last backup.
  - c. Restore does not remove delta files.
3. CAT file - updating:
  - a. Backup removes CAT files based on retention only.
  - b. Synchronization removes CAT files based on retention only.
  - c. Restore does not remove CAT files.
4. Backup.xlog, Sync.xlog are never removed (deleted).

## 6.6 About Email Notifications

When you add an Agent, you can request an email notification when a backup succeeds or fails.

This sample email is an example of the text that is sent after a first backup (seed):

```
Agent: PCACCT
Date and time: 23-NOV-2012 10:17:26.25 -0500
The Job BACKUP DailyBak completed successfully.
BKUP-I-0000 errors encountered:                36
BKUP-I-0000 warnings encountered:              0
BKUP-I-0000 files/directories examined:        54,678
BKUP-I-0000 files/directories filtered:         9,731
BKUP-I-0000 common files excluded:              0
BKUP-I-0000 files/directories deferred:         0
BKUP-I-0000 files/directories backed-up:       44,919
BKUP-I-0000 files backed-up:                   42,338
BKUP-I-0000 directories backed-up:              2,581
BKUP-I-0000 data stream bytes processed:    6,973,189,793 (6.5 GB)
BKUP-I-0000 all stream bytes processed:    6,978,110,221 (6.5 GB)
```



```
BKUP-I-0000 pre-delta bytes processed:      6,978,110,221 (6.5 GB)
BKUP-I-0000 deltized bytes processed:      6,978,110,221 (6.5 GB)
BKUP-I-0000 compressed bytes processed:    5,095,823,625 (4.7 GB)
BKUP-I-0000 approximate bytes deferred:    0 (0 bytes)
BKUP-I-0000 reconnections on recv fail:    0
BKUP-I-0000 reconnections on send fail:    0
BKUP-I-0033 elapsed time 00:46:23
```

This sample email is an example of the text that is sent after a delta backup. A delta backup transmits less data, and uses less vault storage space. However, it is a complete backup and you can use it to restore all of the data.

Agent: PCACCT

Date and time: 24-NOV-2012 10:15:18.89 -0500

The Job BACKUP DailyBak completed successfully.

```
BKUP-I-0000 errors encountered:            48
BKUP-I-0000 warnings encountered:         0
BKUP-I-0000 files/directories examined:   54,690
BKUP-I-0000 files/directories filtered:   9,736
    BKUP-I-0000 common files excluded:     0
BKUP-I-0000 files/directories deferred:   0
BKUP-I-0000 files/directories backed-up:  44,920
BKUP-I-0000 files backed-up:              42,339
BKUP-I-0000 directories backed-up:        2,581
BKUP-I-0000 data stream bytes processed:  6,973,190,632 (6.5 GB)
BKUP-I-0000 all stream bytes processed:   6,978,111,212 (6.5 GB)
BKUP-I-0000 pre-delta bytes processed:    34,083,596 (32.5 MB)
BKUP-I-0000 deltized bytes processed:     29,660,588 (28.3 MB)
BKUP-I-0000 compressed bytes processed:   8,711,184 (8.3 MB)
BKUP-I-0000 approximate bytes deferred:   0 (0 bytes)
BKUP-I-0000 reconnections on recv fail:   0
```



BKUP-I-0000 reconnections on send fail: 0

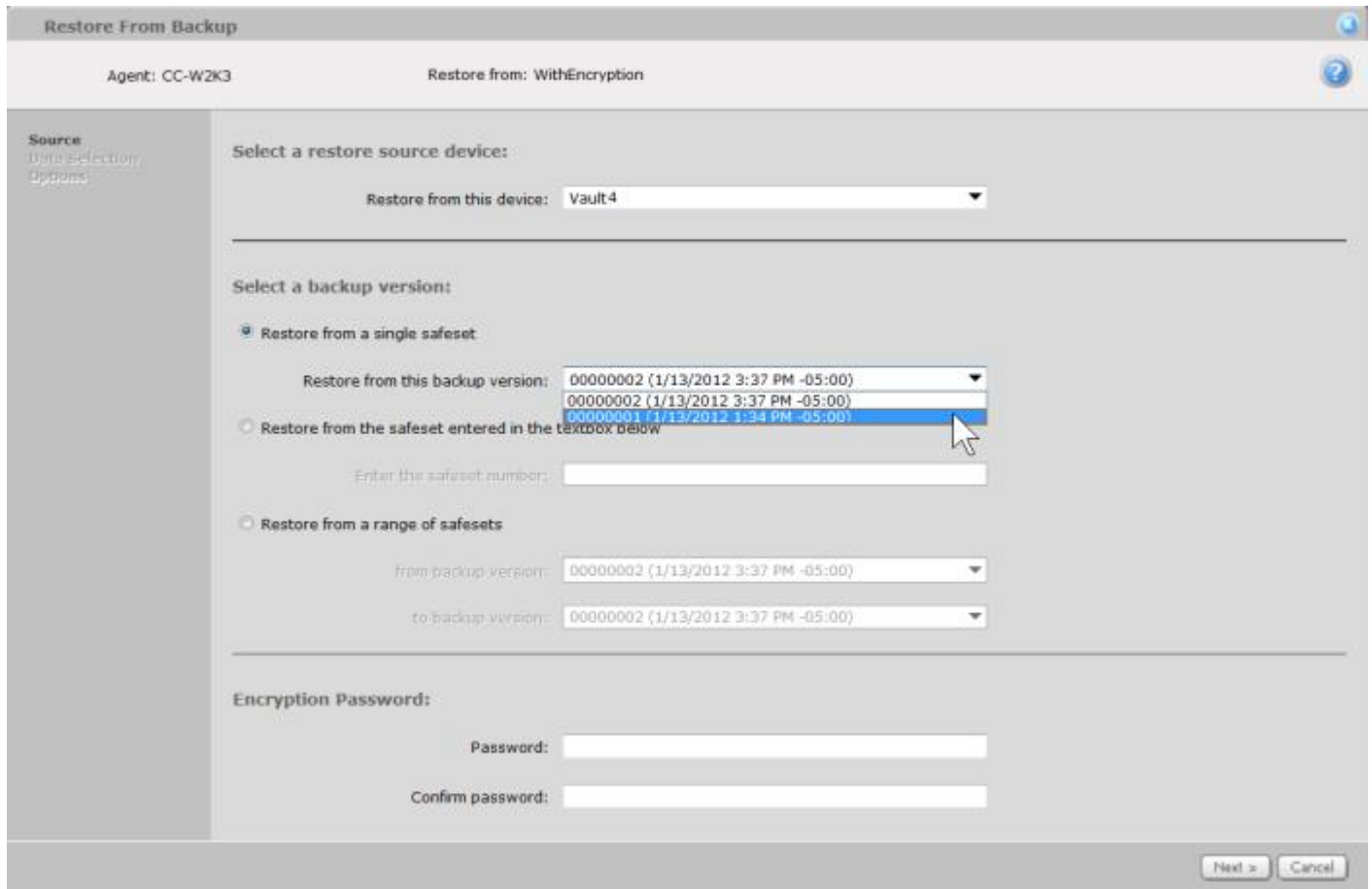
BKUP-I-0033 elapsed time 00:03:03

## 7 Restoring Data

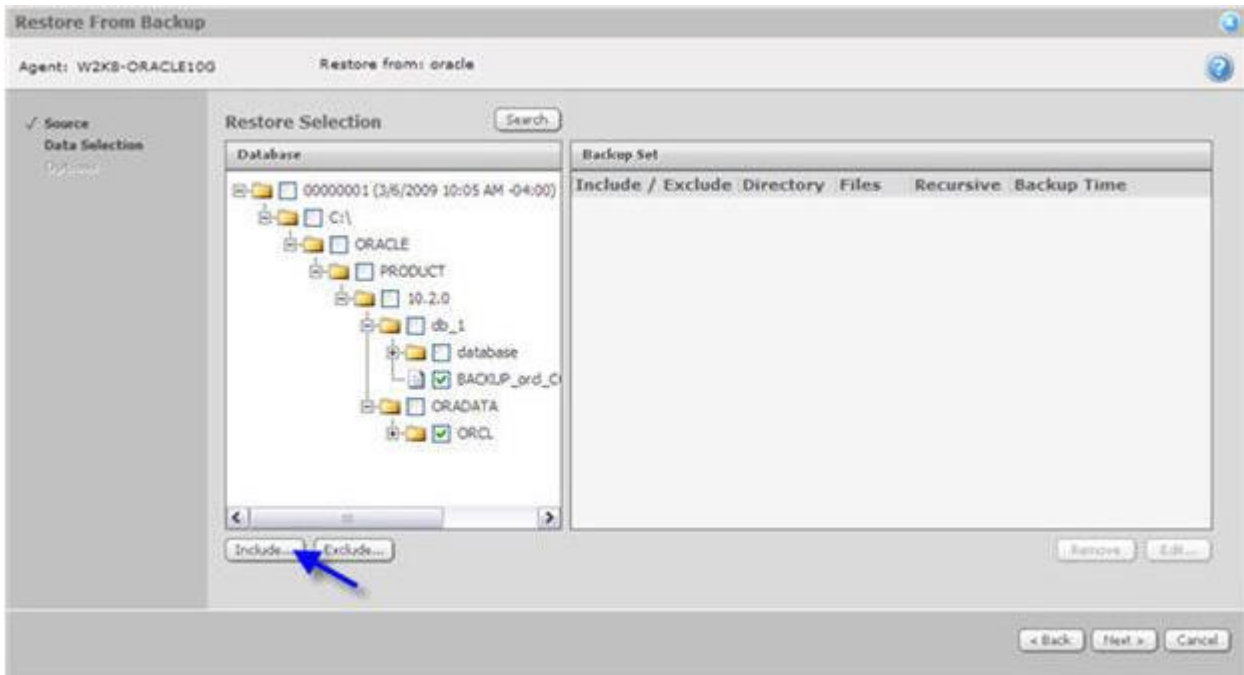
This chapter provides information and procedures for restoring data via Web CentralControl or Windows CentralControl. Restoring from a safeset allows you to recover a single file, or a directory, with or without folders and sub folders. You can run multiple restore operations at the same time. Each restore starts a new process that you can monitor.

### 7.1 Restoring with Web CentralControl

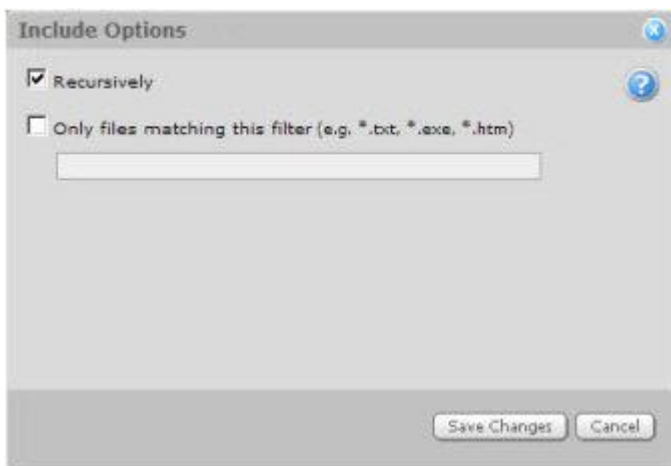
1. To run a restore, select an Agent and a backup job whose data you want to restore. Click the Run Restore button. The **Restore From Backup** window will open.
2. Select a source device (a vault or alternate safeset location) from which to restore and specify a safeset. Choose to restore from a single safeset, restore from the safeset entered in the textbox, or restore from a range of safesets.



3. For an encrypted safeset, you must provide the encryption password that was specified during job configuration. If you have lost this password, you will **NOT** be able to restore. Note that the password is case-sensitive. You will not see this option unless the backup has been encrypted. Click Next to choose the specific items to restore.
4. Specify the data that you want to restore by expanding the directory trees as necessary, and selecting the files that you require. Click the **Include** button to add these files to your selection. You can continue to add files as required.



When you click **Include**, the Include Options page appears.



Select **Recursively** to restore all files and folders in this directory and subdirectories. This is the default selection.

For the Only files matching this filter option, wildcards are supported for file folders and MAPI containers.

\* (asterisk) - signifies a wildcard string up to the next separator character

? (question mark) - signifies a single wildcard character

. (period) - signifies a recursive directory

#### Examples:

\*.txt selects all files that have the txt file type.

C:\.\*.doc selects all files on drive C that have the doc file type.

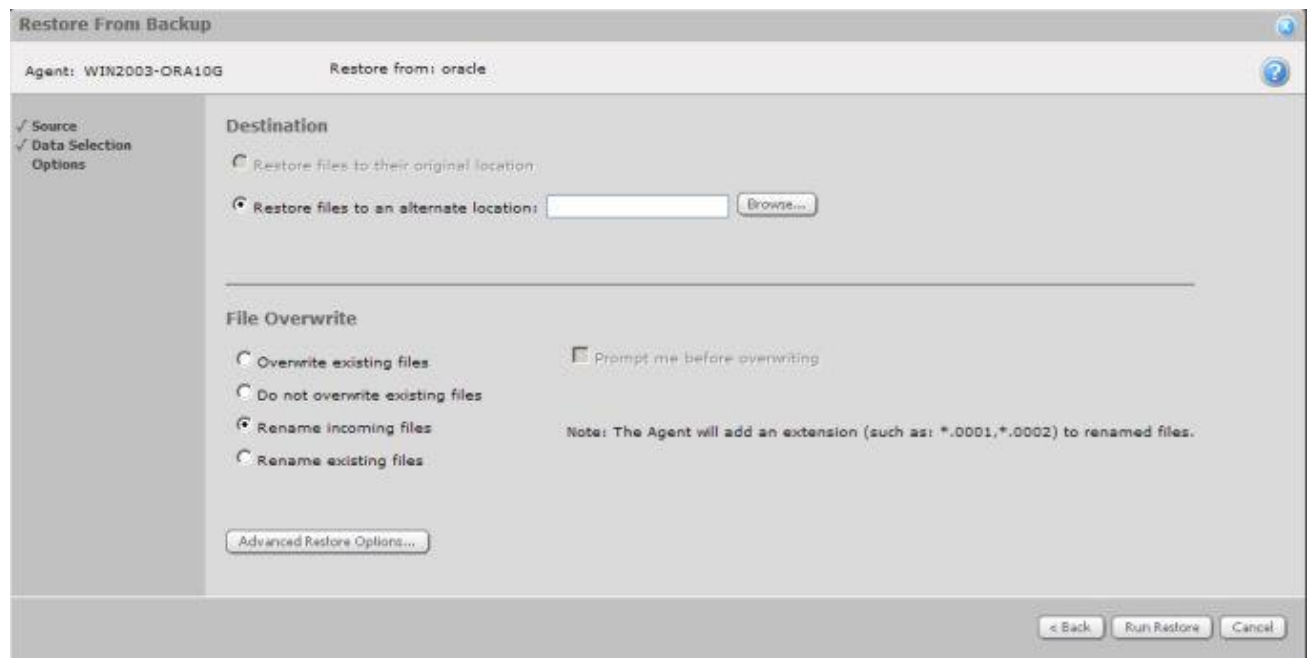
t\*.\* selects all files that begin with the letter t.

5. Click **Save Changes** when your selection is complete.
6. To exclude files or folders, select them, and then click the **Exclude** button. Click **Next** when your selection is complete.
7. Enter the restore destination and File Overwrite Options. You can choose to restore files to their original locations or to alternate locations, create subdirectories, and overwrite or rename existing files.

#### Restore Destination: Original or alternate location

If you restore to the original location, the initial directory structure will be recreated. Also, you may choose to overwrite existing files.

To specify an alternate location, enter the location in the text box, or click Browse to search for a location. If previously you have chosen to restore recursively, the directory structure will be restored to the alternate location (starting from the selection point of the included item).



## Notes on File Overwriting and Options

If two files have the same name, but are located in different volumes, Web CentralControl does not distinguish between volume names when you restore the files to the same alternate location. The first file is restored, but then it is overwritten by the second file.

For example, a user copies some system files from C:\WINDOWS to D:\WINDOWS. After some time, the user restores files from C: and D: to an alternate location. The first WINDOWS file is restored and then overwritten by the second WINDOWS file. The restored directory will contain a mix of old and new files.

This issue can be resolved by restoring the files to separate alternate locations (or their original locations), or by using one of the Rename options.

### File Overwrite Options

- Overwrite existing files (with the restored ones). Note: The overwriting prompts become available when you select Prompt me before overwriting along with this option.
- Do not overwrite existing files
- Rename incoming files from your restore (so that they do not conflict with existing ones)
- Rename existing files (so that they do not conflict with restored ones)

**Note:** Renaming will append serial file extensions. These extensions are .0001, .0002, .0003, etc.

### Prompt Before Overwriting / Operator Request / Restart

If you have selected Overwrite existing files and Prompt me before overwriting, an Operator Request page will display during your restore if a file with the same name exists at the destination location. The prompt asks whether or not you want to overwrite an existing file.

The available response answers are:

- Yes - (will overwrite existing file)
- Yes To All - (will overwrite all existing files that are being restored with the same names; will not prompt you for each one individually)
- No - (will not overwrite but keeps existing file)
- No To All - (will not overwrite any existing files with the same names; will not prompt you for each one individually)
- Cancel - (cancels the restore)
- Respond To Request Later - (will close the restore screen and will not continue with the restore until you come back and make an alternative selection). This can be used to allow you to attend to



other functions. To respond to an operator request that is waiting as Respond To Request Later, select the Agent and job that you used, and click the Process Monitor tab. You will see that the restore process is still active. Click on the Process ID to open the request dialog. The Operator Request (same as above) will appear. Make a selection to proceed.

**Operator Request: Restart:** In some cases, you may be prompted to restart your computer to fully apply the new settings. You can choose Reboot Now, Reboot Later, or Respond To Request Later.

**Note:** The default time limit for the Agent to wait for a response is 3 hours (180 minutes). If no response has been received within this period, the restore will fail. The default value for stopping reconnection attempts with the vault can be changed in Advanced Vault Settings

8. Click **Run Restore** to start the restore process. When you click Run Restore, the Process Details monitor pops up. Here you can monitor the restore progress, or close the monitor to focus elsewhere while the restore runs.

## 7.2 Restoring with Windows CentralControl – Summary Steps

Restoring from a safeset allows you to recover a single file, or a directory, with or without folders and sub folders. Note that the restore steps and options available in Windows CentralControl are virtually the same as in Web CentralControl. For detailed descriptions on the available options, see the previous section ([7.1 Restoring with Web CentralControl](#)).

To restore from a safeset:

1. Open Windows CentralControl.
2. Expand an Agent in the left pane.
3. Right-click a job and select **Synchronize**.
4. Click **Close** to close the **Process Information** dialog.
5. Right-click a job and select **Restore**.
6. Complete the fields in the **Restore** wizard. For field descriptions, see [Restore Wizard Fields](#).
7. Click **Finish**.
8. Click **Close** to close the **Process Information** dialog.

## 7.3 Restoring Data from a CD or DVD

You can restore data directly from a CD or DVD, without copying the safesets to the hard disk. The Safeset Image file (SSI) on the CD or DVD must correspond to the safeset number that you specify in the **safeset** field.

*Note:* You must import the SSI files into the vault before you can restore data from a CD or DVD.

To restore data from a CD or DVD:

1. Open Windows CentralControl.
2. Expand an Agent in the left pane.
3. Right-click a job and select **Restore**.
4. Select **Directory on Disk** in the **Select which type of source device to restore from** list.
5. Insert the CD or DVD in the computer on which the Agent is installed.
6. Click **Browse** and browse to the location of the CD or DVD.
7. Complete the fields in the **Restore** wizard. For field descriptions, see [Restore Wizard Fields](#).
8. Click **Finish**.
9. Click **Close** to close the **Process Information** dialog.

## 7.4 Restoring Data from Another Computer

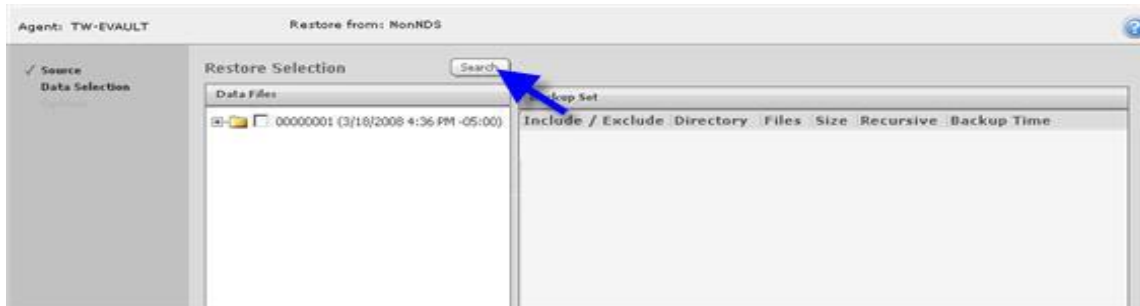
To restore data from another computer:

1. Open Windows CentralControl.
2. Select an Agent in the left pane.
3. Click **Actions** and then **Restore from another computer**.
4. Complete the fields in the **Import Job** wizard.

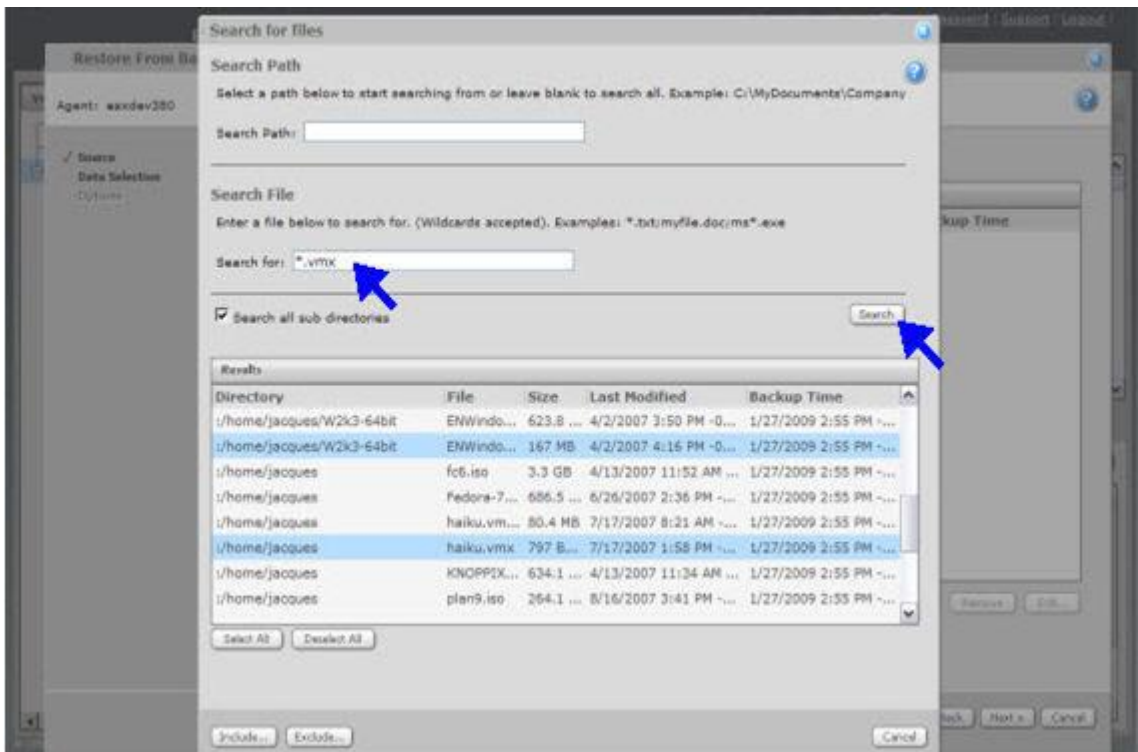
Complete the fields in the **Restore** wizard. For field descriptions, see [Restore Wizard Fields](#).  
Click **Finish**. Click **Close** to close the **Process Information** dialog.

## 7.5 Restore Selection: Search Button Function

The Search Button can be used to refine the selection for what to include in your restore.



1. Click the **Search** button to open the **Search for Files** page.
  - **Search Path:** You can narrow your search by entering a path in the Search Path field.
  - **Search File:** You can enter specific search criteria (and also use wild cards) in your searches.
  - Enable **Search all sub directories** to include subdirectories in your search.



Your search results will appear in the **Results** window.

2. From the search results, select a file(s) that you wish to restore. You can select multiple files by holding **Ctrl** as you click on the file names that you want.
3. Click **Include** to proceed.

## 7.6 Viewing Restore Log Files

To review the log files for events that occurred during a restore:

1. Open Windows CentralControl.
2. Expand an Agent in the left pane.
3. Expand a job.
4. Click **Logs**.
5. Double-click a log in the right pane. Restore logs have this format: RSTyyyymmdd-hhmmss.

## 7.7 Restore Wizard Fields

These fields appear in the **Restore** wizard:

Field	Description
Select which type of source device to restore from	Selects the location for the restore data.
Restore from the following vault	Selects a specific vault for the restore.
safeset	Restores data from a specific safeset.
range of safesets	Restores data from a group of safesets. Select safesets in the <b>from</b> and <b>to</b> fields. When restoring from multiple safesets, you cannot select System State.
Restore files to their original locations	Restores files to their original location. Selecting this option might overwrite existing files with the same name.
Restore files to an alternate location	Restores files to an alternate location.
Prompt me before overwriting files	A prompt appears asking you to confirm a file overwrite.
Overwrite existing files	Overwrites existing files with the same name.
Do not overwrite existing files	Files with the same name are not overwritten.
Rename incoming files	Incoming files that are identical to existing files are renamed.
Rename existing files	Existing files with the same name as incoming files are renamed.
Yes, overwrite locked files	Overwrites locked files.
No, do not restore locked files	Locked files are not restored.
All streams	Selects all streams.
Data streams only	Selects only data streams.

<b>Field</b>	<b>Description</b>
Create log file	Creates a log file during the restore.
Log detail level	The amount of detail included in the log file.
Use all available bandwidth	Uses all available bandwidth for a restore. This is the default.

## 8 Working with the Cluster Plug-in

### 8.1 Overview

A cluster consists of two or more computers that work together to provide higher availability, reliability, and scalability than can be obtained with a single computer.

The Cluster Plug-in allows you to configure an Agent and jobs on the Virtual Node of the Cluster. This allows jobs to redirect the workflow to the active node when a failover happens on the Cluster.

An Agent must be installed on every physical node in a cluster. The Cluster Plug-in is licensed on a per Agent basis, and licenses are distributed automatically by the Vault.

Single Copy Cluster (SCC), Local Continuous Replication (LCR), Cluster Continuous Replication (CCR), and Standby Continuous Replication (SCR) are supported for Microsoft Exchange 2007.

### 8.2 Cluster Prerequisites and Configuration

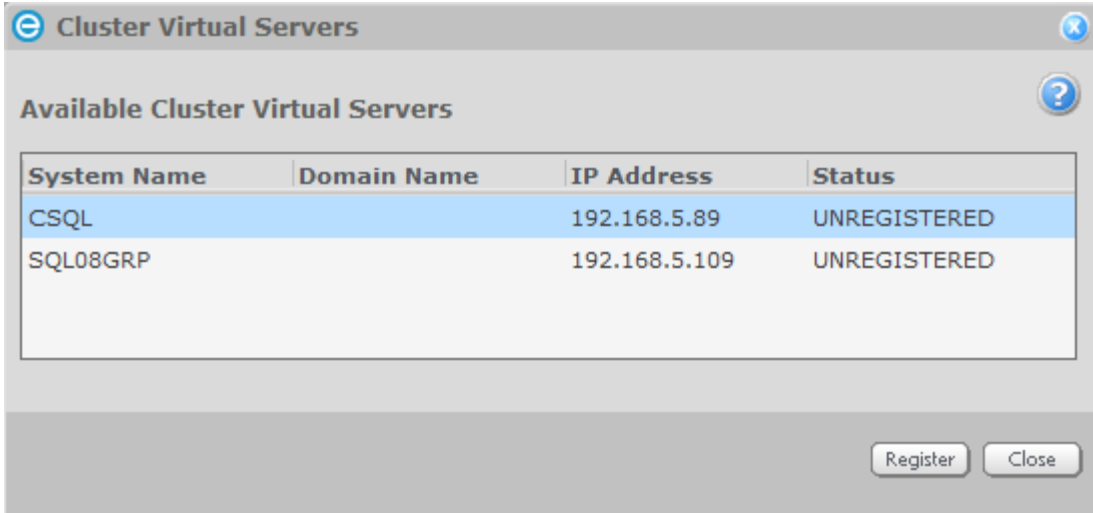
To use the Agent and the Cluster Plug-in in a Windows Cluster environment, the following need to be done:

- The Agent, Cluster Plug-in and any other Plug-ins required to protect the data on the cluster must be installed on each physical node in the cluster. All of the Agents must be installed with the same set of Plug-ins on all the servers in the cluster.
- To configure jobs that protect the applications and files that are associated with the Virtual Nodes in the cluster, a Virtual Cluster Agent must first be registered. The Virtual Cluster Agent is an Agent that is associated with the Virtual Node. Its configuration files and jobs are stored on a shared drive in the cluster and will failover between the physical nodes as the Virtual Node fails over.
- Jobs may be configured on each of the Physical nodes in the cluster to protect the physical systems, however, these jobs will not failover when there is a cluster failover. It is recommended that a Bare Metal Restore job be created on each system to protect it.

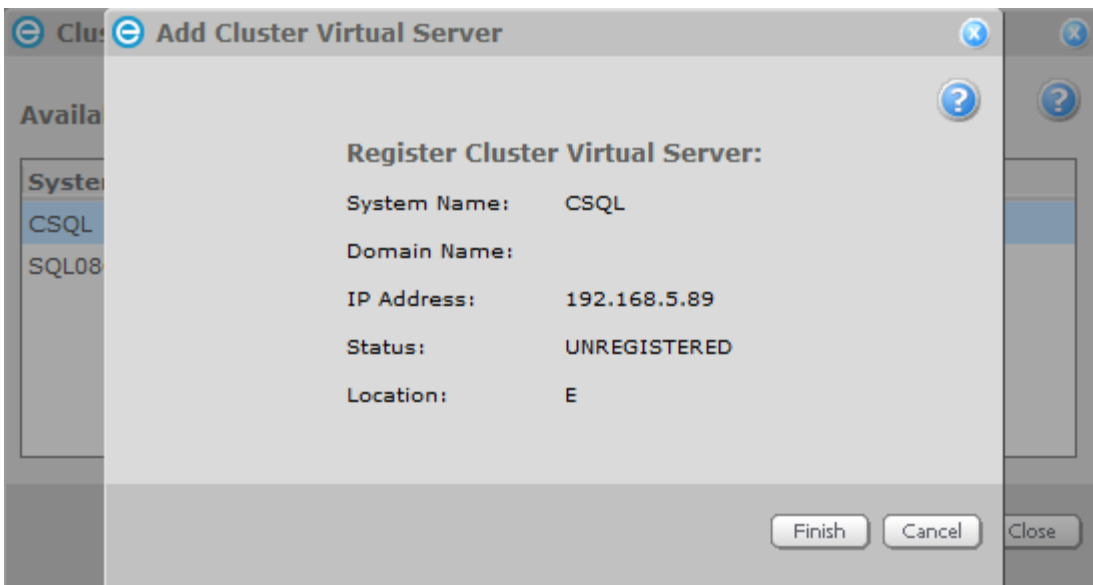
### 8.3 When using Web CentralControl

To configure the Virtual Cluster Agent with Web CentralControl, first select an Agent that is installed on one of the physical nodes in the Cluster. Under the "Edit" menu, select "Configure Cluster Virtual Servers".

This will bring up a dialog that shows the Virtual Nodes in the cluster. It will also provide the status information for each Virtual Node (Registered or Unregistered).

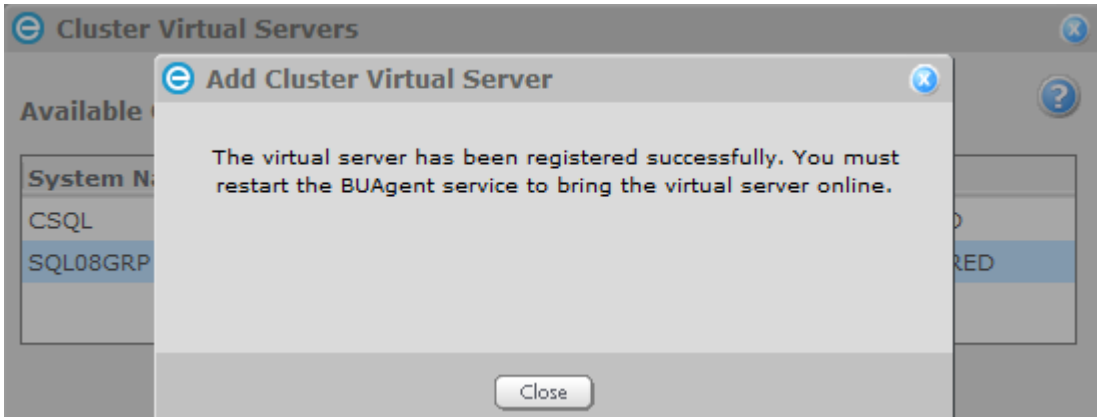


Before you can use the Virtual Agent, you must first register it. To do that, select a Virtual Node with a status of Unregistered and click the **Register** button. This will bring up the registration dialog.

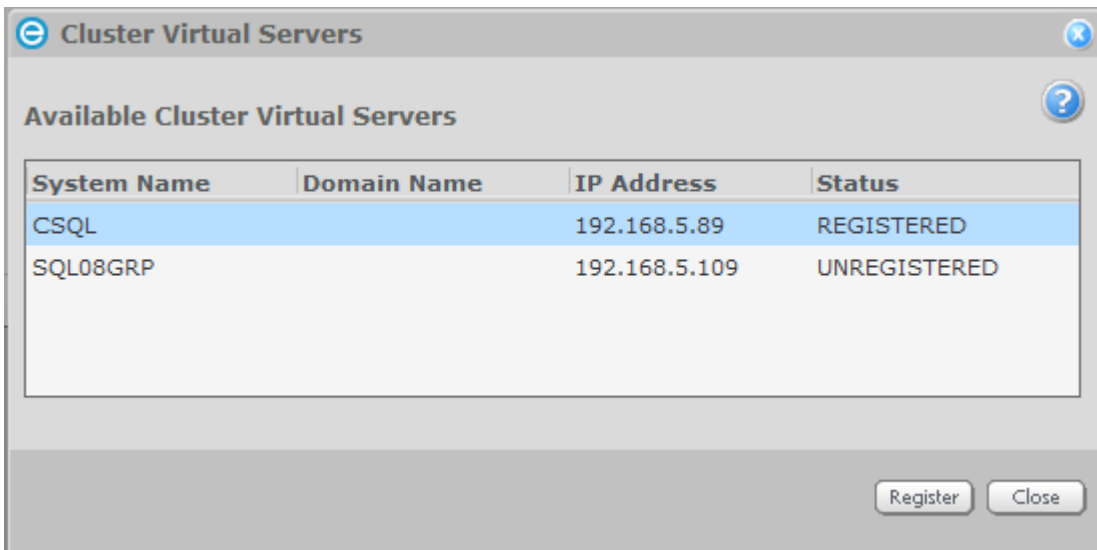


To register the Virtual Agent, click **Finish**. This will create and register the Virtual Agent to Web CentralControl.

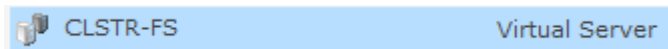
The following message will pop up indicating that you have successfully registered the virtual server. It is required that you restart the BUAgent service on the virtual server to make the virtual server accessible to Web CentralControl (see, “Restarting the BUAgent Service”).



When you click Close you will see the virtual server status as registered.



After restarting the BUAgent service, a new Agent will be available in Web CentralControl with a Virtual Server icon and System Type.



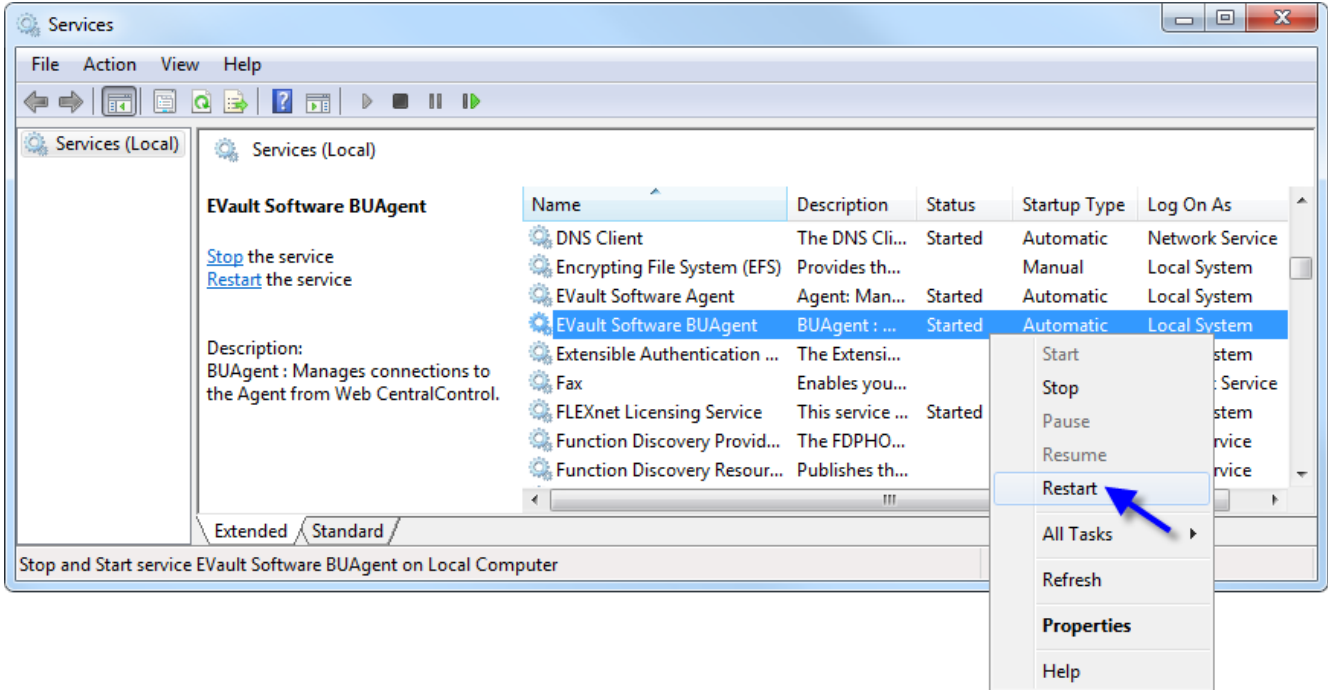
**Note:** If you have multiple Virtual Nodes in the cluster, each node will be configured with a different drive location to store that Virtual Cluster Agent's configuration files.



### 8.3.1 Restarting the BUAgent Service

You must restart the BUAgent on the virtual server either locally or by remote access to the virtual server’s IP. To restart the BUAgent, type into the Run... command “services.msc” to launch Windows services. Alternatively you can select Computer > Manage > Services and Applications > Services.

Locate the BUAgent service, right-click and select **Restart**.



This will stop and then restart the BUAgent service on the Agent that is on the active physical node.

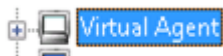
## 8.4 When using Windows CentralControl

**Note:** If you are using both Windows CentralControl and Web CentralControl, use the Web CentralControl method to configure the Virtual Cluster Agents, as the Windows CentralControl method will not register the Virtual Cluster Agent to Web CentralControl.

To configure the Virtual Cluster Agent with Windows CentralControl, add a new Agent using the File/New Agent or right clicking on the Workspace and selecting New Agent.

When prompted for the Agent information, enter the information for the Virtual Node that you want to configure. Under Network Address, provide the IP address or Domain name that has been configured for the Virtual Node.

Once you have filled in the dialog, click OK to add the Agent. Once you have connected to the Agent, the icon will change to look like the following:



Upon BUAgent startup, a cluster shared disk resource will be configured automatically. This is where the configuration files will be stored for this Virtual Cluster Agent.

### 8.4.1 Configuring the Virtual Cluster Agent

From this point, you can configure the Virtual Cluster Agent. The virtual cluster Agent is where you should create the jobs to protect the application that is running on the virtual node of the cluster. Jobs created on this Agent will failover with the virtual node so they can continue to protect these applications without reseeding (no matter which physical node the virtual node is running on). However, if a failover happens when a backup is in progress, the backup will fail and will need to be rerun. To be notified of failures, configure the Agent notification settings.

If there are multiple virtual nodes in the cluster, where each virtual node is setup to protect a specific application, the job created to protect that application must be configured on the virtual cluster Agent on that virtual node.

## 9 Working with the Command Line Interface

This chapter provides information and procedures for using the Command Line Interface (CLI).

You can use the CLI to run Agent commands without opening Windows CentralControl. Typically, CLI commands are used to restore data when the Windows CentralControl application is unavailable. You can use the CLI to perform functions on VV.exe and VVAgent.

### 9.1 VV.exe CLI Command Mode

You can use the CLI to perform these jobs:

Job	Description
BACKUP	Backs up files to disk or a remote Vault Service Provider.
RESTORE	Restores files from disk or a remote Vault Service Provider.
SYNCH	Resynchronizes files with a remote Vault Service Provider.
LIST	Lists files backed up to disk.
RECOVER	Menu driven restores files from disk or a remote Vault Service Provider.
INVENTORY	
ENCPASSWORD	
SETDIR	

### 9.2 General Command Options

The following qualifiers apply to all commands:

Qualifier	Description
/PROGRESS[=YES]	Shows progress messages.
/LOG[=YES]	Logs messages to a file.
/DETAIL=<detail>	Determines how verbose the logging messages will be.
/ENCPASSWORD=<password>	Safeset encryption password (case-sensitive).
/ASSIST[=YES]	Requests operator assistance, if necessary.

Qualifier	Description
/DIAGNOSTICS[=YES]	
/PARAM=<file_spec>	Specifies a parameter file that is used as input to the program.
FORMAT	
PRIORITY[=5]	
DIRECTORY	This setting specifies the location of job-specific files and the root of the job data subdirectories.

### 9.3 Backup Command Options

The following qualifiers apply to all backup commands:

Qualifier	Description
/COMPRESSION=<type>	<p>These are the available options:</p> <ul style="list-style-type: none"> <li>• NONE – Do not compress any data.</li> <li>• MINIMUM – Minimize CPU consumption, possibly at the expense of a larger safeset size.</li> <li>• NORMAL – Balance CPU consumption against safeset size.</li> <li>• DEFAULT – same as normal</li> <li>• STANDARD – same as normal</li> <li>• BETTER – Minimize safeset size, possibly at the expense of extra CPU consumption.</li> <li>• MAXIMUM – Always minimize safeset size, regardless of the amount of CPU consumption required.</li> </ul>
/DEFERAFTER=<time>	The defer time in minutes.
/DESTINATION=<destination>	The safeset location.
/ENCTYPE=<type>	<p>These are the available options:</p> <ul style="list-style-type: none"> <li>• NONE – no encryption used</li> <li>• BLOWFISH56 – 56 bit Blowfish encryption</li> <li>• BLOWFISH128 – 128 bit Blowfish encryption</li> <li>• DES – 56 bit DES encryption</li> <li>• TRIPLEDES – 112 bit DES encryption</li> <li>• AES – 128/256 bit Advanced Encryption Standard encryption</li> </ul>
/EXCLUDE=<filelist>	The list of files to exclude from the backup.

Qualifier	Description
/IGNLOCKING[=YES]	Backs up locked files.
/IGNSECURITY[=YES]	Does not save file ownership and permission information.
/INCLUDE=<filelist>	Outlines list of files to include in the backup.
/RETENTION=<retention>	States the retention name.
/TYPE=<type>	States the type of backup. (e.g. FULL)
/INIT[=YES]	
/IGNALTDATA[=YES]	
/QUICKSCAN[=YES]	
/RETRY[=YES]	
/DELAY	
/DELTA[=YES]	
/IGNNOBACKUP[=YES]	
/SVRADDRESS	Server/vault address.
/SVRACCOUNT	Server/vault account name.
/SVRUSERNAME	Server/vault user name.
/SVRPASSWORD	Server/vault user password (case sensitive).

The following qualifiers apply to Windows backup commands:

Qualifier	Description
/REGISTRY[=YES]	Backs up the Windows Registry under Windows.
/AD[=YES]	Active Directory
/INCLUDEEXCH	
/EXCHTYPE[=INCR]	
/DELEXCHLOG[=YES]	
/SQLTYPE[=FULL]	

## 9.4 Restore Command Options

These qualifiers apply to all restore commands:

Qualifier	Description
/CREATESUBDIRS[=YES]	Creates all necessary subdirectories.
/DESTINATION=<destination>	States the destination to restore to. (e.g. c:\.*.*)
/INCLUDE=<filelist>	Outlines the list of files to include.
/EXCLUDE=<filelist>	Outlines the list of files to exclude.
/IGNSECURITY[=YES]	Does not restore file ownership and permission information.
/OVRWRITE[=YES]	Overwrites existing files. If this option is not specified, the user will be notified of each existing file.
/OVRLOCKED[=YES]	Overwrites locked files.
/SOURCE=<source>	Names the location of the safeset file.
/IGNDATA[=YES]	
/SVRADDRESS	Server/vault address.
/SVRACCOUNT	Server/vault account name.
/SVRUSERNAME	Server/vault user name.
/SVRPASSWORD	Server/vault user password (case sensitive).

The following qualifiers apply to Windows restore commands:

Qualifier	Description
/REGISTRY[=YES]	Restores the Windows Registry under Windows.
/AD[=YES]	Active Directory.
/SYSST[=YES]	
/INCLUDEEXCH	
/ROLLFORWARD[=YES]	
/EXCHLOGALTLOC	Restore Exchange log alternate location.

## 9.5 Synch Command Options

This qualifier applies to the synchronize command (synch):

Qualifier	Description
/SOURCE=<source>	The name of the server from which to resynchronize. By default, the backup destination is used.

## 9.6 Inventory Command Options

The following qualifier applies to the INVENTORY command:

Qualifier	Description
/OUTPUT	

## 9.7 List Command Options

The following qualifiers apply to the list command:

Qualifier	Description
/INCLUDE=<filelist>	The files to include in the listing.
/SOURCE=<source>	The location of the safeset file.
/LOG	Sends VV List output to a file named LIST.LOG. If a job name is specified with the command, the file is created in the job directory, otherwise it is created in the root directory of the VCS.
/FORMAT	Determines the amount of detail included in the VVList log. Choose either BRIEF, FULL or DUMP.
/EXCLUDE	

## 9.8 Forcereseed Option

Delta recreation allows the user to rebuild a delta (DTA) file using job synchronization. This command forces a reseed when delta recreation fails.

Before the delta is recreated, the backup is forced to reseed if the backup detects that the required DTA file is missing or corrupt. With delta recreation on a missing or corrupt delta file, the job fails and logs a message. Then the user is able to rebuild the DTA file through job synchronization.



The parameter only applies to the CLI. The UI is not affected. In case of a failure in rebuilding a delta file, this is an alternative approach. With this parameter, if the vault supports delta recreation, and the recreated file is unusable, the backup is forced to reseed.

The syntax of this parameter is:

```
VV backup job1 /param=job1.vpb /forcereseed
```

Delta files can be recreated only if a backup was done by a version 6 Agent to a version 6 vault. If you back up a safeset using a version 6 Agent to a version 5 vault, and then upgrade the vault to version 6, delta information cannot be recreated. If you back up a safeset using a version 5 Agent to a version 6 vault, and then upgrade the Agent to version 6, delta information cannot be recreated.

In these cases, the interface reports errors in the restore log that the DTA recreation failed for the version 5 files. The restore itself still functions properly. In this case, you can use the `forcereseed` option to create new delta files that are compatible with the version 6 vault.

(However, if you back up a safeset using a version 6 Agent to a version 6 vault, the delta information can be recreated.)

When you back up to a non-vault location, delta recreation information is included by default. To suppress this behavior, run the backup via the Command Line Interface with:

```
/FORCEDELTAREC=No
```

## 9.9 Abbreviated Command Syntax

You can abbreviate commands if the result is not ambiguous. The first four characters of most commands and parameters are unique. So, you could enter a command similar to this:

```
VV [<command> [<Job>] [/<para> ...]]
```

The parameters override any associated parameters in the job and global configuration files. Each time a command is performed, the parameters provided on the command line, `<job>.vvc` file and the `Global.vvc` are used to form the complete syntax of the command.

## 9.10 Specifying File Names in Command Syntax

Enter file names in this format:

```
/INCLUDE=C:\WINNT\.*.*
```

Use commas to separate file names in a list. For example:

```
/INCLUDE=C:\WINNT\.*.*,C:\TEST\.*
```

To add a file name containing a blank space to your file list, enclose the file name in quotation marks. Alternatively, replace the blank space with its ASCII hexadecimal code value.



Example of quotation marks:

```
vv /include="c:\Program Files\EVault\.*", "C:\Documents and Settings\.*"
```

Example of ASCII hexadecimal code value:

```
vv/include=c:\Program^20Files\EVault\.*,C:\Documents^20and^20Settings\.\
```

Note: The hexadecimal code for a blank space is 20.

To add a filename containing a comma to your file list, enclose the file name in backslashes and quotation marks. As an alternative, replace the comma with its ASCII hexadecimal equivalent.

Example of backslash and quotation marks:

```
vv/include=\"c:\Program,Files\EVault\.*\", \"C:\Documents,and,Settings\.\
```

Example of ASCII hexadecimal equivalent:

```
vv/include=c:\Program^2cFiles\EVault\.*,C:\Documents^2cand^2cSettings\.\
```

Note: The hexadecimal code for a comma is 2c.

Any character, even nonprintable ones, can be used as a part of a filename. To do this, enter ^ followed by the character's hexadecimal code. These are valid hexadecimal codes:

- SPACE ( ) – 20
- COMMA (,) - 2c
- CIRCUMFLEX (^) - 5e
- DASH (-) - 2d
- ASTERISK (\*) - 2a
- PLUS (+) - 2b
- QUESTION MARK (?) - 3f

Refer to the Windows character map utility for a complete list of hexadecimal codes.

## 9.11 Directory Layout and Configuration Files

The executable directory contains the VV.exe and Global.vvc files.

The data directory contains the job configuration files. For example, MyJob.vvc.

As backups are run, subdirectories are created under the data directory for each job, with the same name as the job.

Local catalog files, DeltaPro™ information files, and other related files would be stored in the job-specific subdirectory.

Configuration files such as Global.vvc, <JobName>.vvc, and Schedule.cfg and the backup data are stored in the Data Protection vault. They are available for a bare-metal restore.

## 9.12 Configuration Files

The global configuration file is named Global.vvc. This file resides in the same location as the executable.

The job-specific configuration files reside in the directory specified by the data\_directory value in the global configuration file.

A job-specific setting overrides a global setting and a command-line parameter overrides all settings. Spaces before and after a value are ignored. Anything after two forward slashes '/' is treated as a comment. If the last character on the line is a dash ('-'), it is treated as a line-continuation character.

This syntax:

```
license {
    account = xyz
    key = 12345
}
```

is equivalent to this syntax

```
license.account = xyz
license.key = 12345
```

## 9.13 Global Job Settings

Setting	Description
Data_directory	Specifies the location of all the job-specific files and the root of the job data subdirectories.
license.account, license.expiry, license.key, license.options, license.version, license.vendor	Your Service Provider or software provider provides the license settings. All settings are sensitive to case and spacing.
retentionN	These are settings for retention #N where N is from 0 to 9 (e.g. "retention1").
retentionN.name	At least one retention name should match the name specified by the "Backup.retention" parameter.
retentionN.online_days	The minimum number of days to keep the safeset online. The parameters are 0-9999.



Setting	Description
retentionN.online_copies	The minimum number of copies to keep online. For all backups, the minimum value is 1 and the maximum value is 999.
retentionN.archive_days	The minimum number of days to archive the safeset offline. A value of 0 will cause online safesets to be deleted when the online days/copies expire. The parameters are 0-9999.
serverN	The settings for server #N where N is from 0 to 9 (e.g. "server1").
serverN.net_address	The TCP/IP address of Vault Service Provider.
serverN.account	The Vault Service Provider account.
serverN.username	The Vault Service Provider username.
serverN.password	The Vault Service Provider password.

## 9.14 Job Specific Settings

Setting	Description
Backup.destination	The destination for the backup. For example: 1) server1: (server backup – a colon is required) 2) device:\dir\abc.ssi (disk backup) If you plan to use spaces or commas in your command line, see section 5.4.2
Backup.type	The type of backup to create. The categories are Full, and Incremental and Differential.
Backup.include	A comma-separated list of files to back up. To specify a whole directory tree, use the syntax "\.\". For example, "C:\TEMP\.*.DOC" would include all the DOC files in C:\TEMP or any of its subdirectories. See section 5.4.2 for more data on filenames.
Backup.exclude	A comma-separated list of files to exclude from the backup. The set of files that will be backed up is the set of files specified in the include list minus the set of files specified in the exclude list.
Backup.ignore_security	Ignores security-related information for the backup file.
Backup.allow_writers	Backs up files that are locked for writing by another process.

Setting	Description
Backup.enc_type	The encryption type. These are the options: <ul style="list-style-type: none"> <li>• NONEDES</li> <li>• TRIPLEDES</li> <li>• BLOWFISH</li> <li>• AES</li> </ul>
Backup.log_maxcopies	The number of logs to keep. The oldest logs are removed automatically in order to allow new logs to be created.
Backup.local_catalog	When set to YES, a local catalog file is created in the job subdirectory.
Backup.retention	The retention name.
Backup.registry	Backs up the Windows registry. The values are YES or NO. The default is NO. This only applies to Windows 2003/2008.
Backup.nds	Backs up the Novell Directory Service (NDS). The values are YES or NO. The default is NO. This only applies to NetWare 4.2x. or greater
Backup.defer_after	The number of minutes the backup skips any new files or parts of new files that were not backed up completely previously.
enc_password	The encryption password for the file data. This is the password (case sensitive) that is used to encrypt or decrypt safesets.
log.log_to_file	Logs, messages to a file. The file is written to the job directory and has the same name as the current command (e.g. "%data_directory%\myJob\Restore.log"). <b>NOTE</b> that upon successful completion of a backup, the file "Backup.log" is renamed to a numbered file (e.g. "00000099.log").
log.detail	The level of detail in the log file. The levels, in increasing order of detail, are NONE, SUMMARY, DIRECTORIES and FILES. The default is FILES.
nds_pass	The password for the account when backing up the NDS.
nds_path	The starting point in an NDS tree for the NDS backup.
nds_user	The account used when backing up the NDS.
Restore.source	For server restores, the safeset number can be shortened (e.g. server1:3). For other types of safesets, it should be the full name (e.g. disk9:monday1.ssi).
Restore.include	A comma-separated list of files to back up. To specify a whole directory tree, use the syntax "\.\". For example, "C:\TEMP\.\*.DOC" would include all the DOC files in C:\TEMP or any of its subdirectories.
Restore.exclude	A comma-separated list of files to exclude from the backup. The set of files that will be backed up is the set of files specified in the include list minus the set of files specified in the exclude list.

Setting	Description
Restore.overwrite	Specifies whether files are overwritten during a restore. The values are YES or NO. The default is NO. It overwrites existing files.
Restore.replace_locked	Overwrites locked files.
Restore.ignore_security	Does not restore security-related information for the file.
Restore.use_orig_dirs	Restores data to the original directories.
Restore.destination	The location to restore to. For example: <ul style="list-style-type: none"> <li>• \\.*. Restores to original locations and creates subdirectories</li> <li>• c:\*. Restores to C:, creating subdirectories</li> <li>• c:\temp\*. Restores to c:\temp, without creating subdirectories</li> </ul>
Restore.registry	Restore the Windows Registry. The values are YES or NO. The default is NO.
Restore.nds	Restore the Novell Directory Service (NDS). The values are YES or NO. The default is NO. This only applies to NetWare 4.2x or greater.
show_progress	Show progress messages.

## 9.15 Using the Param\_filename Command

Param\_filename

Use this command to use a parameter file for input to the program instead of command-line arguments. This file is created by the Windows CentralControl application to execute immediate functions, such as backup and restore.

## 9.16 Scheduling Backups on a Windows Operating System

VVAgent is a service that enables the automatic scheduling and execution of other services to be loaded. When the VVAgent service is loaded, it reads the contents of the configuration file, Schedule.cfg, located in the directory where the CLI is installed. Each entry in the configuration file contains a time entry and a command name to run, optionally followed by the command arguments for the target Service.

This is an example of the syntax for a Schedule.cfg file entry:

```
<mins>/<hours>/<days>/<months>/<dayofweek> <command name> [command arguments....]
```

This table lists the valid values for each portion of the time entry:

<mins>	0..59
--------	-------



<hours>	0..23
<days>	1..31
<months>	1..12
<dayofweek>	0..6 (Sunday..Saturday)

You can use a comma to separate multiple values. To specify a value range, separate the two values with a dash. Use an asterisk to specify a wildcard (all valid values).

This example loads the vv command with the backup and netback parameters daily at 11:30 a.m. and 11:30 p.m.:

```
30/11,23/*/*/* vv Backup netback
```

This example loads the vv command with the backup and netback parameters at 11:00 a.m. Monday to Friday:

```
30/11/**/1-5 vv Backup netback
```

The configuration file is checked for changes every minute. If any changes occur, the schedule is reloaded. There is no need to stop and restart the service.

## 9.17 Configuring the Microsoft AT Service

On a Windows operating system, you use the AT service to schedule commands and programs to run on a computer at a specific time and date. The AT Service must be configured for automatic startup. Refer to your Microsoft Windows documentation for information about the AT service for your operating system.

## 9.18 How Simultaneously Scheduled Backups are Processed

The position of the entries within the Schedule.cfg file determines which entry takes precedence. For example, a file has these two entries:

```
45/2/last/*/* vv Backup full /retention=Monthly
45/2/**/0-6 vv Backup full
```

The first entry is a backup of the full job, using the monthly retention schedule, and it occurs at 2:45 a.m. on the last day of every month. The second entry is a backup of the full job, using the default retention schedule, and it occurs at 2:45 a.m. every day of the week.

Because the scheduled backup with the monthly retention setting appears at the top of the file, it has priority. On the last day of the month at 2:45 a.m., the scheduler runs the topmost schedule entry and reschedules the second scheduled entry to run at the next available time.

Only jobs using the same command (Backup, Restore, Synchronize) and job name are automatically rescheduled if they conflict.

## 9.19 VVAgent CLI Command Mode

You can use the command line interface and VVAgent to execute Agent commands. VVAgent is included with the Agent installation and it is used for scheduling, configuration, and communication with the backup computer and Windows CentralControl.

These are valid command line options:

- -d : start VVAgent in the daemon mode (background). This is the most common mode because it enables the user to continue using the command prompt while VVAgent operates.
- -f : start VVAgent as a foreground process. In this mode, the command prompt cannot be used while the VVAgent is operating.
- -s : stop the VVAgent that is currently running.
- -p : set the working directory path.
- -n : set the port number for the Windows CentralControl application connection. The default is 808.

This is the command line syntax:

```
./VVAgent (-d|-f|-s) [-p <Agent path>] [-n <port number>]
```

Parameters:

( . . . | . . . | . . . ) choose -d,-f, or -s.

[ . . . ] optional.

< . . . > a value you provide.



## 10 Examples

The examples in this section are intended to allow a new user to be able to step through the major pieces of a backup/restore process in CentralControl. By using the beginning steps outlined in the chapters of this manual, and then by following the steps listed here, you should be able to complete a simple backup and restore.

**Note:** The examples in this appendix apply to Windows CentralControl only. Examples for Web CentralControl are available in the Web CentralControl help.

### 10.1 Example: Creating a Backup Job

1. Right-click on an Agent and select **New Job**, or select **New Job** from the File menu. The New Job Wizard will launch.
2. Give the job a name that is unique from all the other Backup jobs you may have created for the computer being backed up. This name will need to be 1 to 30 characters long. It is good to be descriptive rather than generic. Click **Next** to continue.
3. Select a vault for the backup. The list of Vaults should have at least one vault Profile name in it. Click **Next** to continue.
4. Select a Backup Source Type. Different types of backups include: local files, network files, application backups such as Microsoft Exchange. The list of types will vary depending on what you have installed on the computer you are being backed up. Select "Local Drive Only". Click **Next** to continue.
5. You should be now on the "Source" window. This window allows you to select the files you want backed up. This selection section will vary depending on the Backup Source Type. This part of the job creation may be *complex*, depending on what you are backing up.
6. Double-click the **Data Files** checkbox, and then click the **Add** button. A pop-up dialog box should appear where you can select all the files you want to back up. For the purposes of this example, choose a few small text files.
7. Select your files and click the **Include** button.
8. Repeat the previous step until your backup file selection list is complete. Click **OK** when all your files you want backed up have been selected.
9. The pop-up dialog box should have disappeared and you should be back at the Source window. Click **Next** to continue.
10. You should be now on the Options window. This window allows you to enable/disable Quick File Scanning and to configure the amount of time to allow the backup to complete and also to specify if you want the backup to "defer" to the next day if it can't complete on time.

11. By default, Quick File Scanning is on. This option allows the Agent to quickly scan the system to figure out if any file has changed by reading the “header” information on each file that the system supplies. The alternative is for the Agent to read every file in the backup completely to see if the file has changed. It is a slower method, but it will find all of the changes. For almost all situations you should leave Quick File Scanning on.
12. Disabling deferring means that the Backup Time Window settings will be ignored and all your selection will be backed up in one pass regardless of how long it takes. Normally it is preferable to defer a long backup to the next time the backup is scheduled; when this happens the backup simply starts where it left off from the previous time.
13. The Backup Time Window indicates how long you are giving the backup to complete before stopping. It is normally set to 8 hours.
14. Accept all the defaults on this window and click **Next**.
15. You should be on the Encryption window. This allows you to indicate whether you want your data encrypted when it is stored on the vault. If you do then you can select an encryption option and choose an encryption password. **Be careful** if you do because the vault operator will not know your password when you want to restore your data. Only you will know it. Note that the password is case sensitive.
16. Regardless of whether you choose to encrypt your data for storage on the vault, during the actual transmission of the data over the network the Agent will (by default) encrypt the communications session to ensure privacy during the transfer of information. This Over The Wire encryption may be disabled in Agent Properties, under the Connectivity tab.
17. You should now be on the Log options window. Whenever a backup is run, a log file of the activity is created. On this window you can select how detailed the logging information should be. The more detailed, the larger the log file and the more disk space the backup uses. You can also select for how long the logs should be kept around. Viewing the backup logs periodically is a good way to ensure that everything is working. After the very first backup is run you should check the first log to make sure everything happened correctly.
18. For now use all of the defaults, and simply click **Next**.
19. You should now be on the last window of the Wizard. This is the Finished window. Here you can choose to run the job, schedule it, or simply create it and do nothing more. The default should be to simply “exit” and do nothing more. If this is not selected, select it now.
20. Click **Finish**. At this point the application will attempt to contact the vault that was selected in order to register this new job. If the network is down or the vault is otherwise unavailable or there are other unforeseen problems then an Error dialog box will pop up. Normally everything is working ok and this step completes quickly in a few seconds.
21. This section should now be completed and the Wizard has disappeared from the screen. Your new job should be listed in the list of job under the Agent icon on the left hand pane of the screen. If instead you received an error message then you should contact your support staff to troubleshoot the problem.

22. You should now go to the next example (“Running an Ad-Hoc Backup”) to run the backup job that was newly created.

## 10.2 Example: Running an ad hoc Backup

An “ad hoc” backup is usually a one-time, unscheduled backup, run for a special or unique reason.

1. Right-click a job, and choose “Backup”.
2. Select a backup destination: a vault or a disk directory.
3. There is an option to “Back Up Now” if you wish to run the backup immediately without further configuration, but for this exercise, click Next.
4. The next screen has the Backup Options. This screen allows you to enable/disable Quick File Scanning, select a retention scheme, and to configure the backup time options.
5. By default, Quick File Scanning is on. This option allows the backup to quickly scan the System to figure out if any file has changed by reading the “header” information on each file that the System supplies. The alternative is for the Agent to read every file in the backup completely to see if the file has changed. It is a slower method, but it will find all of the changes. For almost all situations you should leave Quick File Scanning on.
6. Choose a Retention scheme (used to specify how long the backup safesets will be kept on the vault) – daily, weekly or monthly. There are defaults that used for this example: Daily is retained for seven days; Weekly is retained for a month; and Monthly is retained for a year.
7. Disabling deferring means that the Backup Time Window settings will be ignored and your backup selection will be backed up in one pass, regardless of how long it takes. Normally it is preferable to defer a long backup to the next time the backup is scheduled; when this happens the backup simply starts where it left off from the previous time.
8. The Backup Time Window indicates how long you are giving the backup time to complete before stopping. It is normally set to 8 hours. Make your selection or accept the defaults and click Next.
9. Click Finish and the Backup job will start. The progress of the backup will be displayed.

## 10.3 Example: Scheduling a Backup Job

When you are creating a new job, at the end of the New Job Wizard, you have the option to Run, Schedule or Exit. If you select the Schedule radio button and click **Finish** in the Job Wizard, the Schedule List panel appears.

To schedule an existing job in CentralControl, right-click the Agent, and choose Schedule Entries from the menus. The Schedule List panel appears.

To schedule a backup:

1. Click the **New** button on the Schedule List panel. The schedule Wizard launches.
2. Welcome. Click Next.
3. Select **Backup** from the schedule command list. Click Next.
4. The Select a Backup Type window appears, but is grayed out. Click Next.
5. The Retention window appears. Choose a Retention scheme (used to specify how long we will keep the backups on the vault) – daily, weekly or monthly. There are defaults that we will use for this exercise: Daily is retained for seven days; Weekly is retained for a month; and Monthly is retained for a year. For this exercise, choose (default) Daily, and Click Next.
6. You should be now on the Options window. This window allows you to enable/disable Quick File Scanning and to configure the amount of time to allow the backup to complete, and also to specify if you want the backup to “defer” to the next day if it can’t complete on time.
7. By default, Quick File Scanning is on. This option allows the Agent to quickly scan the system to figure out if any file has changed by reading the “header” information on each file that the system supplies. The alternative is for the Agent to read every file in the backup completely to see if the file has changed. It is a slower method, but it will find all of the changes. For almost all situations you should leave Quick File Scanning on.
8. Disabling deferring means that the Backup Time Window settings will be ignored, and all of your selections will be backed up in one pass regardless of how long it takes. Normally it is preferable to defer a long backup to the next time the backup is scheduled; when this happens the backup simply starts where it left off from the previous time.
9. The Backup Time Window indicates how long you are giving the backup time to complete before stopping. It is normally set to 8 hours. Accept all the defaults on this window and click Next.
10. Command cycle. Choose Weekly or Monthly. The screen describes how to select the schedules.
11. Click Finish. The Schedule List panel appears.
12. Click OK.

## 10.4 Example: Checking Backup Results

When your backup is complete, the results appear in the log files in your CentralControl window. To confirm a successful backup:

1. Click an Agent on the left pane of the CentralControl window.
2. Click a job. The Safesets and Log files for the selected job appear in the right pane of the CentralControl window.
3. Click on the Logs folder. A log report for your backup appears in the right pane. Double click the Log file to view the details of the backup. The bottom (last) portion of the Log file should indicate that the backup was completed with no errors. If your job was not completed or you encountered errors, contact your service provider.

## 10.5 Example: Running a Restore Job

After you have completed one or more backups, you can execute a file restore at any time.

1. Select the job from which you want to restore the file(s).
2. Click the Restore button on the standard toolbar. This starts the Restore Wizard.
3. From the Select a Source dialog, you can view the most recent type of source device (e.g. vault), specific source (e.g. name of Service Provider) and safeset (e.g. number of safeset – safesets are numbered starting at one and in increasing order). Typically, these are what you want to restore from. However, you may change any of them as required. Click Next.
4. From the Encryption Options dialog, enter your encryption password in the Password text box if your data was encrypted during backup. Also, enter your password in the Verify Password text box. Note that the password is case sensitive. Click Next.
5. From the Select Restore Objects dialog, select the file(s) you would like to include/exclude from the restore.
6. From the Destination Options dialog, establish the location to which the files are to be restored, whether or not you want subdirectories created and if existing files should be overwritten. The defaults are to restore to an alternate location (you need to specify the location), create sub-directories and overwrite existing files.
7. From the Advanced Restore Options dialog, set any desired options. The defaults are to not restore locked files, to not restore the Local Registry/Novell Bindery/NDS (depending on the operating system) and to restore all data and security streams. You may change any or all of the defaults.
8. Click Finish.
9. Check the restore log to see if the restore was successful.

## 10.6 Example: Cross Computer Restore

Normally when a job is created to do a backup, the client uses a unique configuration file. You must create a profile for the server from which you want to restore, with the same authentication information as the original computer used for backup. You may want to use this method for a disaster recovery plan, as well as for normal data migration.

There are limitations on which operating Systems can successfully transfer data in this way. For example, different versions of the same operating system, such as Windows 2003 and 2008, are acceptable. Operating systems that are part of the same family, or share similar origins (such as Linux and Solaris), are also acceptable.

What the “restore from another computer” option (via a Wizard) does is allows the User to redirect the (original) Restore job to a different client (location). It reregisters where the configuration file was originally pointing, so that the Restore job can be redirected to another location. It does this by getting, authenticating and copying configuration information - vault name, computer name, and job name - from the original configuration, and adding it to your location so that the restore can be accomplished there.

### Steps in the Restore

1. Ensure that the data is fully available for restore (i.e. updated) on the vault. This means that the backup is current, and will properly restore all needed data.
2. Log on to the System that you will restore the data to. This is the different System than the one that did (created) the backup.
3. Ensure that this System does not have a production job with the same name as the job used to back up the data originally. This process will destroy any Safeset information for an existing job and lead to a reseed of data being protected by this job.
4. Create a Vault Profile for the vault on which the data is stored. Use the authentication information that was used for the original backups.
5. From the Tools menu select “Restore from another computer”, from the Vault Profile dialog select the Vault Profile that was created above. Click **Next**.
6. On the Registered Computers dialog select the computer that originally stored the data being restored. Click **Next**.
7. On the job dialog select the job that protects the data to be retrieved. Click **Next**.
8. On the Import job you are told that all information required has been collected to accomplish the restore. Click **Next**.
9. If the job is already created the System will tell you be prompted to overwrite it. Click “Yes” to overwrite.
10. This process downloads catalogs for all available Safesets for this job.

11. This process, when complete, spawns the Restore Wizard starting with the Select a Source dialog.
  - a. The restore now continues like a restore from the original computer – select safeset, select restore objects, etc.

Note that now you will have a “new” job in your list of jobs, which came from the other Agent. It only does restores, and does not allow backups.

## 10.7 Example: Files Excluded from Backups

Files that are automatically excluded from backups are listed below. The built-in exclusions are different depending on the job type and plug-in.

### Exclusions from regular file backups:

1. The registry list (HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup)
2. The job folder (e.g., C:\Program Files (x86)\EVault Software\CentralControl\

### System State (VSS) exclusions:

1. The registry list (HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup)
2. The Agent folder (e.g., C:\Program Files (x86)\EVault Software\CentralControl)
3. Additional exclusions such as:

C:\Windows\System32\config\SECURITY  
C:\Windows\System32\config\SOFTWARE  
C:\Windows\System32\config\SYSTEM  
C:\Windows\System32\config\DEFAULT  
C:\Windows\System32\config\SAM  
C:\Windows\System32\config\COMPONENTS  
C:\Boot\BCD  
C:\Windows\System32\SMI\Store\Machine\SCHEMA.DAT

### BMR exclusions:

\$SV\$:\VSS\_FILE\?\msdownld.tmp\.\*.tmp  
\$SV\$:\VSS\_FILE\C\Windows\msdownld.tmp\.\*.tmp  
\$SV\$:\VSS\_FILE\\*\hiberfil.sys  
\$SV\$:\VSS\_FILE\\*\Pagefile.sys

## 10.8 Example: Ports Used by EVault Software

From	To	Protocol	Destination Ports
Agent	Vault	TCP	<b>2546, 8031</b> * (legacy port 807)
Windows CentralControl	Agent	TCP	<b>808</b> : used by vvagent for Windows CentralControl VSMP calls. <b>2548</b> ** : used by vvagent for Windows CentralControl VSMP calls (includes Exchange 2010/2013 systems). <b>8021</b> : used by buagent for Agent Assistant <b>8031</b> : used by buagent for Windows CentralControl 7.00.1032+
Director Console	Vault	TCP	<b>809</b>
Agent	Web CentralControl	TCP	<b>8086, 8087</b>
Client	Web CentralControl	TCP	<b>80, 443</b> (SSL)

\* EVault Agent for Windows 7 and later

\*\* EVault Agent version 6.8x and later



## 11 Disaster Recovery

In a disaster recovery scenario, you can restore your system from a System State and data file backup or from a bare metal restore (BMR) backup.

*Note:* In a disaster recovery scenario, you can also restore your system from BMR backups created using the Image Plug-in. For more information, see the *Image Plug-in User Guide*.

You can only restore a system from a System State and data file backup if the data file backup includes all partitions from the original system. You can restore the backup using CentralControl, but you must restore the system to a machine with the same hardware and configuration as the original system; any hardware or driver differences can cause problems.

You can restore BMR backups to different hardware than the original machine. However, you must use the separately-licensed EVault System Restore application; you cannot restore BMR backups using CentralControl. For more information, see the *EVault System Restore User Guide*.

The following procedure describes how to recover a Windows system using a System State and data file backup that includes all partitions from the original system.

### 11.1 Hardware Requirements

Ensure that the hardware where you are restoring the Windows System State is the same as the hardware where the data was originally backed up. This may involve simply replacing a crashed disk device.

### 11.2 Software Requirements

Ensure that the appropriate installation media is available. The minimum system software includes:

- Windows installation CD identical to that used during original installation. The Windows version, including service packs, should be **identical** to the version installed on the original system.

**Note:** The service pack level that was previously installed is displayed in the Web CentralControl OS column for that system's Agent.

- Agent for Windows Installation media identical to that installed on the original system and/or,
- CentralControl Installation media identical to that installed on the original system.

**Note:** The primary storage device where the OS is installed must contain enough storage to accommodate a full OS installation AND the contents of a full backup. In situations where the primary storage device accommodates a paging file, the maximum size of the paging file should be added to the total space required.

## 11.3 Windows Recovery Steps

To restore your Windows operating system:

1. Start the system using the setup disks.

**Note:** If your system can start from a CD-ROM, you can use the CD-ROM to start the system here.

2. Verify that the CD-ROM installed on the system is recognized by the setup.
3. Insert the Windows installation CD when prompted.
4. When prompted to partition the drive, make sure that the partition is at least as large as the original partition. The setup of the partitioning must be the same as in the system where the data was backed up.
5. When asked where to install the Windows directory, specify the same location as in the original system installation.
6. Continue the system installation process until the basic functionality of the OS is restored.
7. Install the Service Pack identical to the one on the original system. After this, restart as prompted.

**Note:** The service pack level that was previously installed is displayed in the Web CentralControl OS column for that system's Agent.

8. Ensure that the TCP/IP stack is installed and configured according to the settings in the Hardware Configuration Settings Checklist. Verify that the network adapter is correctly identified. Also, apply any service patches required.
9. Ensure that basic networking structure is in place (e.g. connectivity between internal networks where the system to be restored resides) and that a connection is established between the system and the vault. A router, if required, must be properly connected and configured. Test the TCP/IP connectivity between the local system and the vault by pinging the IP address of the vault.

### Continue with Client Installation

1. Install the version of CentralControl listed on your previously-completed Configuration Settings Checklist.
2. Install the version of the Client Agent for Windows described on your Configuration Settings Checklist.
3. Using CentralControl, name the untitled Workspace. Choose File > Save Workspace As. Enter a name in the File Name text box. The name does not have to be, but can be, the same as the workspace on the original system. Press Save. If desired, enter a password in the Password text

box and confirm it. Note that the password is case-sensitive. Choose an encryption type from the Encryption type drop-down list. Click OK.

### **Create an Agent**

1. Right-click your workspace. Click on New Agent. This opens the Agent Properties dialog box.
2. Enter the Description and Network Address. The Description is the name of the Agent. It can be the same as or different than the name on the original system. The Network Address can be specified using either a numerical IP format (192.0.0.1) or a textual DNS format (myAgent.myco.com). The default Port is 808.
3. Enter the Username and Password. The Username authenticates this program with the remote Agent System. When restoring under Windows, specify a Username with Backup Operator or Administrator privileges.
4. Click on the Save Password check box.
5. Specify the domain name in the Domain text box. The domain can optionally be left blank under the following circumstances: you are not specifying a Windows Agent, you belong to the same domain as the Windows Agent System, or your network does not utilize a domain name server.
6. After entering the agent and authentication information, click on Get Status. If the information is validated, your data will be displayed in the Agent Status window. Click OK. However, if the information is not validated, a message from CentralControl will appear. Check your information and revise it as required. Once again, click on Get Status, and click OK.

### **Set up Notification**

1. With the Agent highlighted, click on the Agent Configuration file. If you want to receive email notification upon success or failure of the restore process, choose the Notification tab. Click on the Send Email on Successful Completion and Send Email on Failure check boxes.
2. Enter the address from which the notification is sent. This can be any valid email address.
3. Enter the SMTP Server Network Address and recipient's address in the designated text boxes.

### **Reregister the computer**

1. Reregistering the computer brings back all Agent information from the vault. This includes configuration and scheduling information. Reregistering basically reassigns this information to the new computer.

### **Perform a Synchronize, only if you choose Directory on Disk for Source.**

1. With the job highlighted, choose the Synch button on the Standard toolbar.
2. When asked to confirm the Synch, click Yes. This starts the Synch process. The Process Information dialog box is displayed.



3. When the Synch is complete, click Close.

### Using the Restore Wizard

1. With the job highlighted, click the Restore button on the Standard toolbar. The Restore Wizard leads you through the remaining recovery steps.
2. From the Select a Source dialog box, select which type of source device to restore from. From the drop-down list, choose vault, Directory on Disk. If you choose vault, you need to choose which vault to restore from. Choose one from the drop-down list. You also need to choose the Safeset to restore from. Choose a Safeset from the drop-down list.
3. Next, from the Encryption Options dialog box, enter your password if your backup was encrypted. Note that the password is case-sensitive.
4. Select the files to include or exclude from the recovery in the Select Files dialog box. From the Select Files dialog box, you can choose to Add files, Remove files or Search for files.
5. Next, select one of the following destination options:
6. Do you wish to restore files to their original locations? (If you select no, enter the alternate location in the text box.)
7. Do you wish to create subdirectories?
8. Do you wish to overwrite files that already exist?
9. From the Advanced Restore Options dialog, set the Advanced Options:
10. Do you wish to overwrite files that are locked by another process?
11. Do you wish to restore the local registry?
12. Do you wish to restore security information?
13. What detail level to choose?
14. Select whether or not you want to restore the Active Directory.
15. Once you have set your options, click Finish. A Process Information Window indicates the status of the restore.
16. When completed, you have two choices: Reboot Now or Reboot Later. Choose Reboot Now. After you restart, the recovery procedure is complete, and the process of verifying the integrity of the restore can begin.

## 11.4 Windows Recovery Problems

Should any of the restores fail, consider each of the following questions carefully:

- Was the system restored using the same OS version?
- Were the proper service packs applied before recovering the system?
- Was the latest version of ASPI installed?



- What possible differences were there in the hardware or software settings that could have affected the recovery?
- Were any errors reported in the Restore.log file?
- Were all the necessary drivers installed?

#### 11.4.1 2008 DR Special Procedures for Restoring with BCD

When performing a Disaster Recovery using a backup of the entire system volume, it is recommended to exclude the Boot Configuration Data (BCD), which is usually located at C:\Boot\BCD, from the restore selection. In most circumstances, the existing BCD should be sufficient to recover the system.

In some circumstances it may be desired to restore the BCD (for example, if it was previously configured with customized boot options). In this case, the BCD may be included in the restore selection. It should be noted, however, that the BCD that was backed up may not match the currently installed hard disk on the recovery system. When restoring the BCD, the following steps should be performed:

1. After the restore successfully completes, reboot the system as prompted.
2. Log in to the restored system, and type the following command into a command prompt:

```
bcdedit /enum all /store c:\boot\bcd
```

3. In the section with identifier "{bootmgr}", if the device shows as "boot", issue the following command (assuming that the C: drive is the drive that the system boots from):

```
bcdedit /store c:\boot\bcd /set {bootmgr} device partition=c:
```

4. In all other sections (i.e. with identifier "{default}"), if the device shows as "unknown" and the osdevice shows as "unknown", issue the following commands (assuming that the C: drive is the system volume):

```
bcdedit /store c:\boot\bcd /set {default} device partition=c:
```

```
bcdedit /store c:\boot\bcd /set {default} osdevice partition=c:
```

Failing to follow these steps will result in an unbootable system that will need to be recovered using the Windows installation media.

## 11.5 Recovery Verification for Windows

Once the restore procedure is complete, you must determine and validate whether the recovery is complete and correct. The listing and testing of the jobs should be performed as part of the systems recovery planning. The specific jobs to be performed for verification will depend on the application environment deployed and the system's importance.

Once the system is restored, it is crucial to verify the integrity of the recovery. The test can be as simple as placing a duplicate file in a different directory structure and testing for any differences within the file. Then, confirm that the file can be opened using a known application and that you are able to send email to a known address. It can also be as complex as completing an SQL query on a known database set. Whatever the test, both the list and the test itself must be planned and executed during normal system operation.

## 11.6 Active Directory Restores

For information about active directory restores, see the *CentralControl Operations Guide*. This guide includes information about primary restores, non-authoritative restores, and authoritative restores.

### 11.6.1 Troubleshooting

If you experience problems starting your system after restoring the Active Directory, you may try the following:

Restart the computer. If the computer does not restart after recovery because of HAL mismatches, you can start from the Windows installation disk to perform an in-place installation or repair. This type of repair occurs after you accept the licensing agreement, and Setup searches for previous versions to repair. When the installation that is damaged or needs repair is found, press R to repair the selected installation. Setup re-enumerates your computer's hardware (including HAL) and performs an in-place upgrade while maintaining your programs and User settings. This also refreshes the SystemRoot%\Repair folder with accurate information that you can use for normal repairs.

If the computer does restart after recovery, log on as Administrator and initiate an in-place upgrade by running Winnt32.exe from the I386 folder on the Windows installation disk. This refreshes the Setup.log and registry files in the %SystemRoot%\Repair folder, and ensures the proper HAL is in use.