Agent 6.82 for Microsoft Windows
User's Guide

Published: March 7, 2011

Revision: This manual is updated for Version 6.82.

Software Version: 6.82 (February 2011)

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.

The Agent, Agent Console, and Vault applications have the added encryption option of 128/256 bit 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).
See:http://csrc.nist.gov/encryption/aes/round2/r2report.pdf for details.

The Agent and Vault applications have the added security feature of an over the wire encryption method.

Contents

1. Overview 1

1.1 Product Overview 1

1.1 What's New in Agent 6.82 for Microsoft Windows? 2

1.2 About the Windows Agent 2

1.3 About the Agent Console 3

1.4 About the Vault Console 3

1.5 Supported Agent 32-bit Plug-ins 3

1.6 Supported Agent 64-bit Plug-ins 4

1.7 Plug-In Behavior 4

1.8 About the Exchange Plug-In 5

1.9 About the Oracle Plug-In 5

1.10 About the SQL Server Plug-In 5

1.11 About the Cluster Support Plug-In 5

1.12 About the SharePoint Plug-In 5

1.13 Additional Resources 6

2 Installing and Modifying the Agent 7

2.1 Hardware Requirements 7

2.2 Permission Requirements 7

2.3 Operational Modes 8

2.4 Locking Agent Configuration and Program Files 8

2.5 Default Installation Directories 9

2.6 Agent Licensing 9

2.7 Agent InstallShield Wizard Fields 10

2.8 Installing the Agent 11

2.9 Silently Installing the Agent from the Command Line 12

2.10 Customizing a Silent Installation 12

2.11 Modifying an Agent Installation 14

2.12 Repairing an Agent Installation 14

2.13 Uninstalling an Agent 14

2.14 Silently Uninstalling an Agent 15

3 Upgrading the Agent 16

3.1 Hardware and Software Requirements 16
3.2 Preparing the Computer 16
3.3 Upgrading Program and Configuration Files 17
3.4 Upgrading an Agent that Uses OTM 17
3.5 Upgrading the Microsoft Exchange Server MAPI Plug-in 18
4 Configuring the Agent 19
4.1 Agent Properties Dialog Fields 19
4.2 Creating an Agent Profile 20
4.3 Adding an Agent Group 20
4.4 Renaming the Workspace 20
4.5 Encrypting a Workspace 21
4.6 Options Dialog Fields 21
4.7 Setting Workspace Options 22
4.8 Vault Configuration Wizard Fields 22
4.9 Configuring a New Vault Connection 22
4.10 Re-Registering an Agent 23
4.11 New Job Wizard Fields 23
4.12 Creating a Job 24
4.13 Adding Files and Directories to a Job 25
4.14 Wildcards in Directory Paths 25
4.15 Wildcard Rules for Directories 26
4.16 Selection Rules 26
4.17 Removing Files and Directories from a Job 27
4.18 Backing up System State Files 27
4.19 Backing up System Files 27
4.20 Additional Back up Options 28
4.21 Improving Agent Performance 29
4.22 Scheduling a Job 29
5 Manual Data Backup 30
5.1 About Seeding and Re-Seeding 30
5.2 Running an ad hoc Backup 30
5.3 Viewing Process Information 30
5.4 Viewing Safeset Properties 31

5.5 Viewing Log Files 31
5.6 About Email Notifications 31
6 Restoring Data 34
6.1 Restore Wizard Fields 34
6.2 Restoring a Safeset 35
6.3 Restoring Data from a CD or DVD 35
6.4 Viewing Restore Log Files 35
6.5 Restoring Data from Another Computer 36
6.6 Creating a Bare Metal Restore Backup 36
6.7 Migrating an Existing Job to Bare Metal Restore Job 37
7 Working with the Cluster Plug-In 38
7.1 Installing and Configuring the Cluster Plug-in 38
8 Working with the Command Line Interface 40
8.1 VV.exe CLI Command Mode 40
8.2 General Command Options 40
8.3 Backup Command Options 41
8.4 Restore Command Options 43
8.5 Sync Command Options 44
8.6 Inventory Command Options 44
8.7 List Command Options 44
8.8 Forcereseed Option 44
8.9 Abbreviated Command Syntax 45
8.10 Specifying File Names in Command Syntax 45
8.11 Directory Layout and Configuration Files 46
8.12 Configuration Files 46
8.13 Global Job Settings 47
8.14 Job Specific Settings 48
8.15 Using the Param_filename Command 49
8.16 Scheduling Backups on a Windows Operating System 49
8.17 Configuring the Microsoft AT Service 50
8.18 How Simultaneous Scheduled Backups are Processed 50
8.19 VVAgent CLI Command Mode 51

1. Overview

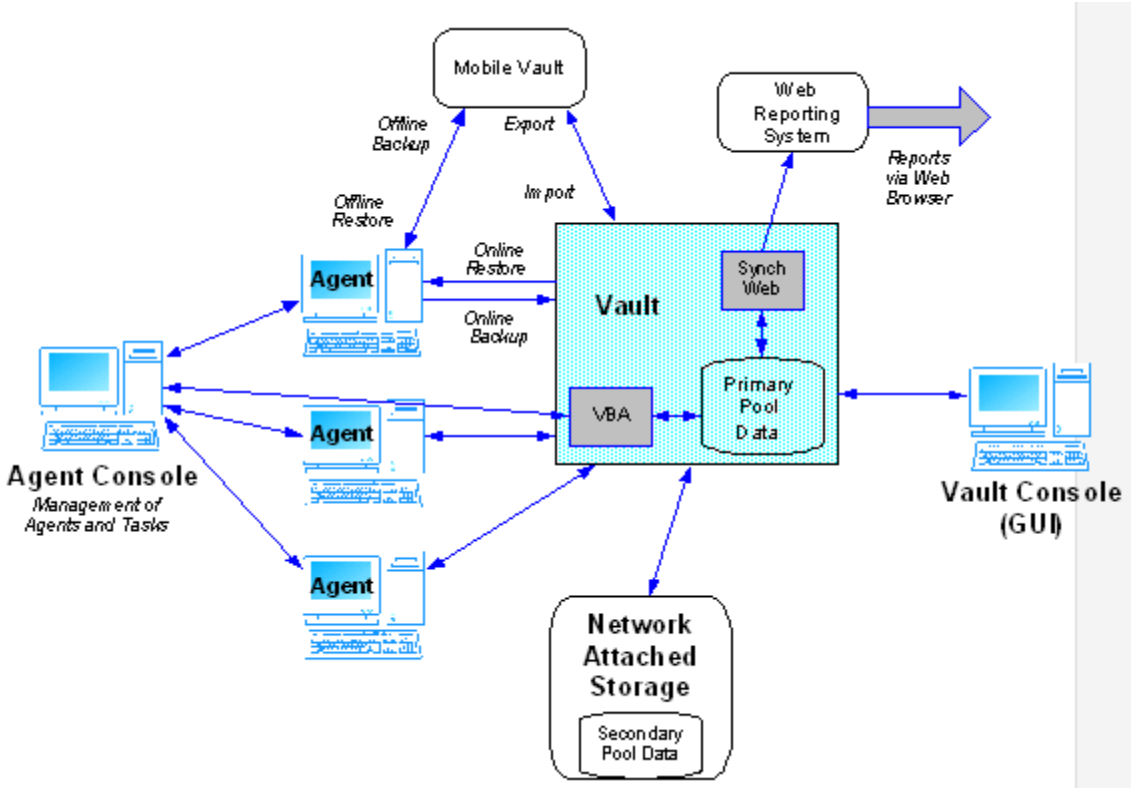
This Guide is intended for System Administrators who are responsible for ensuring that network computers are properly configured for back up, and that backups and restores can run successfully.

This Guide provides information and procedures for installing the Agent, selecting data for back up, configuring Agents for back up, scheduling backups, and restoring data.

For information about using Windows Agent Console and Agents, see the Windows Agent Console Operations Guide. For information about BUAgents running on the Web Agent Console, see the Web Agent Console documentation.

1.1 Product Overview

This diagram shows the relationship between different software products:



The arrows illustrate the communication paths of a typical standalone Vault Console installation.

The Vault Console, Agents, and Agent Console are the primary components of the data protection application. You use these components to back up and restore system and file data from your network computers to a local or remote Vault. These applications protect your data without the need for tape devices or other non-disk backup media.

1.1 What's New in Agent 6.82 for Microsoft Windows?

These are the new or improved features in Agent 6.82 for Microsoft Windows:

- To complete backup and restores on 64-bit Agents with the Microsoft Exchange 2010 DR plug-in, you must install the Vault Console version 6.0 or newer. In addition, you must be using Windows Agent Console version 6.80 and newer.
- The Microsoft Exchange 2010 DR plug-in supports Database Availability Groups (DAG). Microsoft Exchange 2007 and Microsoft Exchange 2003 are not supported.
- The Microsoft Exchange 2010 DR plug-in does not support MAPI backups.
- Windows Agent Console version 6.80 displays the Agent Status and the installed plug-ins.
- The default port for Agent 6.80 and newer is 2548. Older Agents can continue to use 808.
- Agent 6.82 supports bare metal restore (BMR) type backup Jobs. For full BMR type restores, ESR software version 1.1 or newer is required.
- Agent 6.82 does not support backups of virtual hard drives (VHD).

1.2 About the Windows Agent

You install the Agent software on every computer that you want to back up. You use Windows or the Web Agent Console and the Windows Agent to back up data from network computers to a remote Data Protection Vault. The applications provide an automated, unattended method for protecting your valuable computer data without using removable backup media devices.

The Agent includes these components:

- VV.exe - performs the backup and restore functions to the Vault.
- VVAgent.exe – used for scheduling, configuration, and communication with Windows Agent Console. It runs as a Windows Service on supported Windows operating systems.
- BUAgent.exe – used for scheduling, configuration, and communication with Web Agent Console. It runs as a Windows Service on supported Windows operating systems.

Each computer that you want to back up must meet these requirements:

- The Agent software must be installed and running.
- The computer and the Agent must be connected to a network.
- The Agent must be able to access a Vault.

Each backup is considered a full backup because you can use it to perform a restore without using incremental or differential backups. The Agent runs on the computer as a background service. It starts automatically when the system starts.

You use Agent Console to set up Agents, Jobs, scheduling, and monitoring. The backup data moves from the Agent computer to the Vault computer. Backup data does not go through Agent Console. To receive Agent commands and data, you must create an account for the Agent on the Vault.

After you configure the Agent and create schedules, backups occur automatically. You do not need to keep Windows Agent Console running. Use Windows Agent Console to configure the Agent, check the progress of backups, and to view error logs.

1.3 About the Agent Console

You use Windows or Web Agent Console to manage all of the computers that are running the Agent software. You do not require a license to use Agent Console. However, you must have Administrator privileges to create and modify backups and manage restores.

Web Agent Console runs on a web server and has the same functionality as Windows Agent Console. However, it uses an Internet browser to connect to the network.

It is recommended that you use only one type of Agent Console to manage an Agent.

1.4 About the Vault Console

The primary purpose of Vault Console application is the management of storage pool data at a remote secure Vault location. Data is sent from the Agent to the Vault Console over a Wide Area Network (WAN) or Local Area Network (LAN) connection, the Internet, or imported from media.

Vault Console does not interact with the Agent Console program. The Agent Console communicates with, and manages the remote Agents.

1.5 Supported Agent 32-bit Plug-ins

Some plug-ins are optional and require an extra license. When you install the Agent, you can install the plug-ins and activate them later with the repair or upgrade options.

The 32-bit Agent supports these plug-ins:

- Microsoft SQL Server
- Microsoft Exchange 2003 DR and MAPI
- Cluster
- SharePoint
- Oracle

If you install the Oracle plug-in, you must install the Oracle Instant Client for Windows after you install the 32-bit Agent. The Oracle Instant Client for Windows is available on the i365 Support website (csp.i365.com.

1.6 Supported Agent 64-bit Plug-ins

You can install a 64-bit Agent on a supported 64-bit Microsoft Windows operating system. For a list of supported operating systems, see the Agent-Win64 release notes.

You use the same Agent Console to control 64-bit and 32-bit Agents. When you check the Agent status after you configure a 64-bit Agent, the operating system version is listed as one of the supported platforms.

Some plug-ins are optional and require an extra license. When you install the Agent, you can install the plug-ins and activate them later with the repair or upgrade options.

The 64-bit Agent supports these plug-ins:

- Microsoft SQL Server
- Microsoft Exchange 2010 DR and MAPI
- Microsoft Exchange 2007 DR and MAPI
- Cluster
- Microsoft Office SharePoint 2007
- Microsoft Office SharePoint Server 2007
- Microsoft Sharepoint Portal Server 2003
- Microsoft SharePoint Services 3.0 SP 2

When you connect an Agent to a Vault version 5.53 or older, you need a license for each plug-in. If you connect the Agent to a Vault version 5.53 or newer, the Vault supplies the license automatically. See the Agent Console Operations Guide and the plug-in guides for more information about licensing and installation.

1.7 Plug-In Behavior

The Agent treats a plug-in as a separate component. This is the behavior when a component fails:

- One component backup – When the component fails the Job fails.
- Two component backup - When one component fails and another finishes (with or without errors or warnings), the Job finishes successfully. If both components fail, the Job fails.

1.8 About the Exchange Plug-In

You use the Exchange plug-in for full Microsoft Visual Source Safe disaster recovery on Microsoft Exchange databases and for backing up and restoring individual mailboxes, archiving mailboxes and public folders, and folders with MAPI.

1.9 About the Oracle Plug-In

You use the Oracle plug-in to backup an Oracle database. The plug-in is installed on top of the Agent on the database host to perform the backups.

When you install the Oracle plug-in, Agent Software wizard detects that the Oracle Instant Client is not installed and you are directed to a location where you can download it.

The Oracle Instant Client is installed in the Server Agent installation directory. If you attempt to install the Oracle Instant Client without installing the Agent first, the installation terminates gracefully.

1.10 About the SQL Server Plug-In

You use the SQL Server plug-in to back up a Microsoft SQL Server 2000, 2005, or 2008 database. The plug-in is installed on top of the Agent on the database host to perform the backups. You can upgrade previous versions of the plug-in, without reconfiguring your settings or reseeding existing data.

1.11 About the Cluster Support Plug-In

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

You use the Cluster Support plug-in to redirect the workload from a failed computer to another computer in a cluster. The existing configuration is automatically applied to the server after a failover. Single Copy Cluster (SCC), LCR, CCR, and SCR are supported.

Clusters do not guard against a loss of a user data.

You must install an Agent on every computer in a cluster and each Agent must have a separate license. You must register every Agent with a Vault. When a failure occurs, you must manually re-start Jobs.

1.12 About the SharePoint Plug-In

You use the SharePoint plug-in to complete brick-level backups and restores of SharePoint items including webs, lists, libraries, folders, and documents. This granularity allows you to

complete backups and restores of the entire site, including individual document versions. You can restore a document to the file system as a document or as a document version.

The SharePoint plug-in, on a restore, allows browsing and selection to the file level. You can also search for a file to restore.

The SharePoint plug-in installs directly on the Agent computer.

1.13 Additional Resources

Release Notes for this product are available from your service provider. Release Notes contain the most current information about the product, including an overview of new features, any known defect (bug) fixes incorporated since the last release, and a description of any Known Issues.

The Windows Agent Console application includes an online help that contains the same information that is contained in this manual. To access the help, select **Help** on the toolbar or press **F1**. To view context-sensitive or field level help, click and drag the **Help** icon () to a field.

If the F1 Help screen is open or minimized, the context-sensitive help is not active. Close the F1 help view context-sensitive help.

2 Installing and Modifying the Agent

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

To configure and manage the VVAgent, you must install the Web or Windows Agent Console application on a supported Microsoft Windows computer and make it accessible to the Agent.

If you are using replication, you can configure the Agent to use alternate Vaults. To assign an alternate Vault, you modify the list of alternate vaults that is kept in the installation folder. This file has an .ALT extension.

2.1 Hardware Requirements

The computer on which you install Agent 6.82 should meet the minimum hardware requirements for the operating system specified by Microsoft. In addition, a minimum of 100 MB of free disk space is required for the installation and operation of the Agent. More disk space might be required if your backups are large or you install plug-ins.

For the specific requirements for each operating system, see the Shipping Products Chart or the Release Notes.

2.2 Permission Requirements

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

To manage an Agent from Windows Agent Console and Web Agent Console, 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 and ACL's 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.

2.3 Operational Modes

This table lists the Agent 6.82 operational modes:

Operational Mode	Description
Ad-Hoc	A user can use the Agent Console application to configure backup and restore Jobs on an Agent. To configure backup and restore Jobs, the user must have Backup Files and Directories permissions.
Scheduled	A user can use the Agent Console application 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 Backup Files and Directories permissions. These permissions are automatically applied if the use is a member of the BackupOperators or Administrators groups.

2.4 Locking Agent Configuration and Program Files

To prevent unauthorized access to Agent program and configuration files, you can lock the directories. When you lock a directory, only users in these groups can access program and configuration files:

- .\Administrators group
- .\BackupOperators group
- .\LocalSystem user

Agent 6.82 supports these two optional file-locking management software utilities:

- Open Transaction Manager™ (OTM) from Columbia Data Products
- Open File Manager™ (OFM) from i365

Typically, you use OTM on small or medium sized computers and OFM on large computers. OTM and OFM are intended to protect open files, such as user data files, and databases.

Do not install OTM and OFM on the same computer. Do not use file-locking management utilities on Agent installation and application directories, or AV directories.

With OFM version 9.1 and earlier, directories that cannot be opened during a backup are automatically excluded from the backup. With OFM version 9.1 and later, you must define the directories and subdirectories that you want to exclude from the backup.

If you are using the Vault Backup Agent (VBA), it is recommended that you exclude the Vault Console storage locations from anti-virus scanning.

When you use OFM for Microsoft Exchange Volume Shadow Copy Service (VSS) backups, you must select the **VSS aware** option within the OFM application.

If you are using anti-virus software, it is recommended that you disable real time scanning on reads.

If the Agent computer fails, you can re-install the directories that contain the AV programs, and the Agent installation and application programs. If you intend to re-install the operating system, you should back up the system state.

2.5 Default Installation Directories

These are the default installation directories:

- C:\Program Files\EVault Software\Agent
- C:\Program Files\EVault Software\Agent Assistant

If the top-level directory is not empty, it is not removed when the installation is complete.

2.6 Agent Licensing

On Vault versions 5.53 and later, 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, plug-ins, and other Agent products that use a Vault. These Agent applications require a license:

- Vault Backup Agent (VBA)
- Exchange Plug-In
- SQL Server Plug-In
- SharePoint Plug-In
- Cluster Support Plug-In
- Oracle Plug-In for Windows
- ArcWare
- Bare Metal Restore (BMR)

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 you connect an Agent 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
Agent (5.6 and above)					
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*
System I (pre- 5.6)					
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 the older license key that was installed on the Agent. The Vault did not see or use this key.

When an Agent is successfully registered with a Vault, it can perform backups and restores.

2.7 Agent InstallShield Wizard Fields

These fields appear in the **Agent InstallShield** wizard:

Field	Description
Typical	Installs the Agent and the default plug-ins.
Custom	Allows you to select the program options to install.
Install Agent to	The path where the Agent is installed. Click **Change** to select another location.

Register Agent with Web Agent Console	Registers the Agent with the Web Agent Console and allows it to be managed with the application. If you do not register the Agent with the Web Agent Console, you manage it with the Windows Agent Console.
Network Address	The IP address or Domain Name System (DNS) name for the Web Agent Console computer.
Port	The port used to communicate with the Web Agent Console computer.
Username	The user name used to access the Web Agent Console computer.
Password	The password used to access the Web Agent Console computer.
Skip Registration	The Agent is not registered with a Web Agent Console computer and you manage the Agent with Windows Agent Console.
Use 'Local System' Account	Uses a local system account.
Create account automatically	Creates an account to access and run Agent services automatically.
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 Backup 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	Installs or uninstalls the Exchange 2003 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 Agent Console at the following address	Displays the Web Agent Console registration information.
Keep my current registration	Keeps the Web Agent Console registration.
Change registration	Changes the Web Agent Console registration.
Program files only	Removes the Agent program files.
Total Uninstall	Uninstalls the Agent.

2.8 Installing the Agent

You can install the Agent from the Internet or CD. You can run the installation on the Internet, or save the Agent Windows.exe file locally and then run the installation.

Before you start the Agent installation, install and configure the Microsoft operating system. You use the same installation procedure for 32-bit and 64-bit Agents.

To install the Agent:

1. Log on to the computer on which you want to install the Agent.
2. Double-click the Agent Windows .exe file. To obtain the self-extracting installation file, contact your licensed software provider.
3. Select a language for the installation.
4. Complete the **Agent InstallShield** wizard. For field descriptions, see Agent InstallShield Wizard Fields.
5. Click **Finish**.

2.9 Silently Installing the Agent from the Command Line

To silently install the Agent from the command line:

1. Log on to the computer on which you want to upgrade the Agent.
2. Open a command prompt and navigate to the location of the Agent Windows 6.82 .exe file. The default location for the file is C:\Program Files\EVault Software\Agent.
3. Run a command similar to this:

```
setup.exe /s /v" /qn"
```

2.10 Customizing a Silent Installation

To customize your silent Agent installation, you specify the properties on the command line. For example, to install the Agent in a different directory, you run this command:

```
setup.exe /s /v" SILENTINSTALLDIR=\"C:\Program Files\Acme Software\" /qn"
```

To install a different language, run a command similar to this:

```
setup.exe /s /v" /qn" /l"1036"
```

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

To install an Agent and register it with the Web Agent Console, run a command similar to this:

```
setup.exe /s /v" REGISTERWITHWEBCC=True AMPNWADDRESS=123.456.com
AMPUSERNAME=test@test.com AMPPASSWORD=LetMeIn3 /qn"
```

To install an Agent with the Agent Assistant, and then register the Agent with the Web Agent Console, run a command similar to this:

```
setup.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 an Agent and the SQL Plug-In:

```
setup.exe /s /v" FEATURESQL=On /qn"
```

This table lists the optional properties that you can specify when you silently install the Agent from the command line:

Property	Default Value	Description
ACCOUNTTYPE	LocalSystem	Possible values are LocalSystem, AutoCreate, and Custom.
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.
BCKHELPURL		If FEATUREMAESTRO is True, this field is required.
BCKLOGINURL		If FEATUREMAESTRO is True, this field is required.
EXTRACTMSI	False	Turns on/off extraction of the Microsoft Installer (MSI) package.
FEATURECLUSTER	Off	Turns on/off installation of the Cluster Plug-In.
FEATUREEXCHANGE	Off	Turns on/off installation of the Exchange 2003/2007 Plug-In.
FEATUREEXCHANGE2010	Off	Turns on/off installation of the Exchange 2010 Plug-In.
FEATUREMAESTRO	Off	Turns on/off installation of the Agent Assistant.
FEATUREORACLE	Off	Turns on/off installation of the Oracle Plug-In.
FEATURESHAREPOINT	Off	Turns on/off installation of the SharePoint Plug-In.
FEATURESQL	Off	Turns on/off installation of the SQL Plug-In.
KEEPAMPREGISTRATION	True	Set this property to True to retain the previous Web Agent Console registration.
MSIPATH	C:\	If EXTRACTMSI is True, this property denotes the location of the extracted MSI and MST files.
REGISTERWITHWEBCC	False	Turns on/off registration of the Agent with Web Agent Console.
SERVICEACCOUNTNAME		If ACCOUNTTYPE is Custom, this field is required.
SERVICEACCOUNTPASSWORD		If ACCOUNTTYPE is Custom, this field is required.
SILENTINSTALLDIR	C:\Program Files\EVault Software\	
TOTALUNINSTALL	False	If this property is False, uninstalling will only remove the program files.

2.11 Modifying an Agent Installation

To change the language of an Agent, uninstall the Agent program files and then re-install 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 software provider.
3. Click **Next**.
4. Select **Modify**.
5. Complete the **Agent InstallShield** wizard. For field descriptions, see Agent InstallShield Wizard Fields.
6. Click **Install**.

2.12 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 software provider.
3. Click **Next**.
4. Select **Repair**.
5. Complete the **Agent InstallShield** wizard. For field descriptions, see Agent InstallShield Wizard Fields.
6. Click **Install**.

2.13 Uninstalling an Agent

To uninstall the Agent under Windows:

1. Log on to the computer on which you want to uninstall the Agent.
2. Double-click the Agent Windows.exe file. To obtain the self-extracting installation file, contact your licensed software provider.
3. Click **Next**.
4. Select **Remove**.
5. Select **Total Uninstall**.
6. Click **Remove**.
7. Click **Finish**.

2.14 Silently Uninstalling an Agent

To silently uninstall an Agent:

1. Log on to the computer on which you want to uninstall the Agent.
2. Open a command prompt and run this command:

```
setup.exe /s /x /v"/qn TOTALUNINSTALL=True"
```

3 Upgrading the Agent

This section provides information and procedures for upgrading Agent 6.82 for Microsoft Windows. You can upgrade these Agent versions to Agent 6.82:

- Version 6.7x
- Version 6.6x
- Version 6.50
- Version 6.4x
- Version 5.6

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 version 6.8.

These conditions can cause your backups to reseed:

- If you upgrade older Agents with Jobs that were created and backed up with 4K 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 k blocks change to the newer 32 k blocks, causing a reseed on the next backup.
- Microsoft Exchange mailbox names in Agent 6.82 for Microsoft Windows use the same name as the Exchange System Manager Console. If the mailbox names are not identical, a reseed occurs.

3.1 Hardware and Software Requirements

The computer on which you install Agent 6.82 should meet the minimum hardware requirements for the operating system specified by Microsoft. In addition, a minimum of 100 MB of free disk space is required for the installation and operation of the Agent. More disk space might be required if your backups are large or you install plug-ins.

For the specific requirements for each operating system, see the Shipping Products Chart or the Release Notes.

3.2 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 Vault Console installed. See the Agent release notes for the specific requirements for each operating system.

3.3 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 software provider.
3. Click **Yes**.
4. Complete the **Agent InstallShield** wizard. For field descriptions, see Agent InstallShield 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.

3.4 Upgrading an Agent that Uses OTM

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

1. Log on to the computer on which you want to upgrade the Agent.
2. Upgrade the operating system to Windows 7 or Windows Server 2008 R2.
3. Double-click the Agent Windows 6.82 .exe file. To obtain the self-extracting installation file, contact your licensed software provider.
4. Click **Yes**.
5. Complete the **Agent InstallShield** wizard. For field descriptions, see Agent Wizard Fields.

6. 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.

3.5 Upgrading the Microsoft Exchange Server MAPI Plug-in

If you installed the Exchange 2003 plug-in on an Agent version 5.6, 6.0, or 6.1 you might need to replace or remove older Microsoft Exchange Server MDB mailbox names when you upgrade the Agent.

After an upgrade, mailbox names identified as **LegacyExchangeDN** do not match the newer Exchange System Manager Console (Active Directory) names. Before you upgrade the Agent, the MDB mailbox names start with a number. The upgraded Agent uses Active Directory names and the mailbox names start with a letter. As a result, the old mailboxes are not included with the Job parameters. The Upgrade log file lists the mailbox names that do not match. Edit the Job and change the mailbox name from a number to a letter.

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 software provider.
3. Click **Yes**.
4. Select **I want to proceed with the upgrade of this Agent**
5. Complete the **Agent InstallShield wizard**. For field descriptions, see Agent InstallShield Wizard Fields.
6. Click **Finish**.

4 Configuring the Agent

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

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

You use the Agent Console to manage and configure the Agent. You can use a single Agent Console 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 the Agent Console 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, or you are performing a bare-metal restore, you must re-register 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 the Agent Console.
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.

   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**.

4.3 Adding an Agent Group

To save time, you can use a text file to apply Agent information to multiple Agents. For more information about this process, see the Windows Agent Console Operations Guide.

To add an Agent group:

1. Open the Agent Console.
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**.

4.4 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 the Agent Console.

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**.

4.5 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 the Agent Console.
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**.

4.6 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 Agent Console 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 **Refresh**, or press **F5**. 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 f you want to see them all. Do not add a separator, such as a decimal point, or comma in the field.
Default Text Viewer	This is the viewer that is used to show logs (XML based), and other text based files

4.7 Setting Workspace Options

To set workspace options:

1. Open the Agent Console.
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**.

4.8 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.
Re-register 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.
User name	The user name used to access the Vault.
Password	The password used to access the Vault. This field is case sensitive.

4.9 Configuring a New Vault Connection

To configure a Vault connection:

1. Open the Agent Console.
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**.

4.10 Re-Registering an Agent

When you delete an Agent from a Vault, the Agent profile is deleted on 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 re-registration. You must re-register 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 SQL server.
- The domain, username, and password of the account used to back up a networked drive.

When a re-registration 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 re-registration 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.

4.11 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 back up.
Unicode: All files will be backed up. Some filenames will display improperly in the file	Includes all files in the back up.

selection screens.	
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 _, -, $ (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	Backup system files.
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.

4.12 Creating a Job

To create a Job:

1. Open the Windows Agent Console.
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**.

4.13 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 the Windows Agent Console.
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. Use a question mark (?) to select a file name, or Directory that matches a single character.
8. Click **OK**.
9. Click **OK**.

4.14 Wildcards in Directory Paths

Vault Console 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\<all the A's>, C:\Users\<all the B's> and so on until <all the Z's>. You want to be able to back up all these user directories. If you select "C:\Users" and select Recursive, you will get everything, in one backup. However, as more users are added, the backup takes longer. What you want to do is break the backup into separate backups, with each taking a part of the data. For instance, one takes all the A to E, another takes all the F to J, or whatever "balance" you decide.

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).

Of course, you can still filter further with"include only files matching this filter".

When you have finished selecting (and including) all the files and directories you want to be in this Backup Job, click **Yes** and you will be back at the Source screen, where you can click **Next** to continue the next step of the New Job Wizard. See the section on "Create a Job" above.

4.15 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*\.*.*

4.16 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\.*.*

4.17 Removing Files and Directories from a Job

To remove files or directories from a Job:

1. Open the Windows Agent Console.
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**.

4.18 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 back up. Typically, a system state backup includes these files:

- COM+ Class Registration Database
- Registry
- Boot Files
- Windows System Files
- Performance Counter

To back up system state files:

1. Open the Windows Agent Console.
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**.

4.19 Backing up System Files

System and state files are critical to the recovery of the operating system. Including system files with your back up 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 the service packs you install determine what files are included with the system files back up. Windows makes a dynamic list of these DLLs when you include them in your backup.

To back up system files:

1. Open the Windows Agent Console.
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**.

4.20 Additional Back up Options

When you create a new Job and you 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 complete a bare metal restore of a computer. This option is available when you create the Job and select Local Drive Only as the backup source type.
- **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 and provides a hierarchal storage and fast retrieval of IIS configuration properties for Web sites, 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 restoration of replicated data where the target is the primary Active Directory server.

4.21 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.

4.22 Scheduling a Job

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

1. Open the Windows Agent Console.
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 Manual Data Backup

This section provides information and procedures for running a manual, or ad-hoc backup.

5.1 About Seeding and Re-Seeding

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 re-seed.

With a re-seed, your backup takes longer to complete and a message about re-seeding is added to the log file.

5.2 Running an ad hoc Backup

To run an unscheduled or ad hoc backup:

1. Open the Windows Agent Console.
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**.

5.3 Viewing Process Information

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

5.4 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 the Windows Agent Console.
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**.

5.5 Viewing Log Files

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

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

5.6 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-2009 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-2009 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
```

6 Restoring Data

This section provides information and procedures for restoring data.

You can run multiple restores at a time. Each restore starts a new process that you can monitor.

6.1 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 **from** and **to** 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.
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.

6.2 Restoring a Safeset

Restoring a safeset allows you to recover a single file or a complete directory.

To restore a safeset:

1. Open the Windows Agent Console.
2. Expand an Agent in the left pane.
3. Right-click a Job and select **Restore**.
4. Complete the fields in the **Restore** wizard. For field descriptions, see Restore Wizard Fields.
5. Click **Finish**.
6. Click **Close** to close the **Process Information** dialog.

6.3 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 Server Side Includes (SSI) file on the CD or DVD must correspond to the safeset number that you specify in the **safeset** field.

To restore data from a CD or DVD:

1. Open the Windows Agent Console.
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.

6.4 Viewing Restore Log Files

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

1. Open the Windows Agent Console.
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.

6.5 Restoring Data from Another Computer

To restore data from another computer:

1. Open the Windows Agent Console.
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.
5. Complete the fields in the **Restore** wizard. For field descriptions, see Restore Wizard Fields.
6. Click **Finish**.
7. Click **Close** to close the **Process Information** dialog.

6.6 Creating a Bare Metal Restore Backup

You can use a bare metal restore (BMR) to apply a complete backup to a new computer. You use the System Restore application to complete a BMR. See the System Restore User Guide for more information.

To prepare the Agent for a bare metal restore, you select the Bare Metal Restore option in the Job Properties dialog. When you select the Bare Metal Restore option, the information necessary for a System Restore is added to the backup. When you select Bare Metal Restore, you cannot select System State. Volumes containing System State information are automatically included in the backup. In addition, a BMR backup performs regular file and folder backups and restores of the entire disk.

The Bare Metal Restore option is available when you create the Job and select Local Drive Only as the backup source type.

To create a Bare Metal Restore Backup:

1. Open the Windows Agent Console.
2. Create a new Job and select **Bare Metal Restore** as the files and directory backup option. See Creating a Job.

   To include data files from other volumes in the backup, select **Data Files**. Click **Options** to add or remove data files from the system volume. If you remove a system file that is required for the System Restore, it is automatically included in the backup.

6.7 Migrating an Existing Job to Bare Metal Restore Job

You can change an existing local system Job to a bare metal restore Job. When you change a Job to a bare metal restore, these options are disabled:

- System State
- RSM Database
- Event Logs
- Terminal Services Licenses

Selecting the Bare Metal Restore option does not alter existing job file selections. However, file exclusions that are required to complete the bare metal restore are ignored.

When you select the Bare Metal Restore option, the Job uses a System Restore license on the Vault console when you save the Job. If a bare metal restore license is not available, a warning message appears, but the Job is saved. Clearing the Bare Metal Restore option does not release the bare metal restore license on the Director.

To migrate an existing Job to a bare metal restore Job:

1. Open the Windows Agent Console.
2. Right-click a Job in the left pane and select **Properties**.
3. Click the **Source** tab.
4. Select **Bare Metal Restore** in the top pane.

   To include data files from other volumes in the backup, select **Data Files**. Click **Options** to add or remove data files from the system volume. If you remove a system file that is required for the System Restore, it is automatically included in the backup.
5. Click **OK**.

7 Working with the Cluster Plug-In

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

You use the Cluster Support plug-in to redirect the workload from a failed computer to another computer in a cluster. The existing configuration is automatically applied to the server after a failover. Single Copy Cluster (SCC), LCR, CCR, and SCR are supported.

Clusters do not guard against loss of a user data.

An Agent must be installed on every computer in a cluster and each Agent must have a separate license. Every Agent must be registered to a Vault. When a failure occurs, you must manually re-start Jobs.

When using the Agent and the Cluster plug-in in a virtual environment, these parameters apply:

- A user uses an IP or a domain name to connect to an Agent with a Cluster plug-in and a proper license on a virtual server or a local machine.
- The virtual server Agent backs up virtual server shared data without re-seeding, or in case of a failover.
- Jobs on a shared drive on a virtual server can be used by all Agents in the cluster.
- Virtual server backup scheduling is managed by node Agents without schedule overlapping. The configuration files are located on the virtual server drive.
- You must enter the licenses for the Cluster plug-ins on the virtual server.
- When you first configure an Agent on a virtual server, you will be prompted for a location on a drive that is accessible to the virtual servers. After a failover, the Agent configuration is available to all servers owned by the virtual server.
- In the Windows Agent Console, different icons are used to identify a regular local Agent and a virtual server Agent.

7.1 Installing and Configuring the Cluster Plug-in

To use the Cluster plug-in failover features, you must create the backup Job from the Virtual Node.

If you create a new Exchange Server Job from an SQL Server Virtual node, the Exchange Server is available in the Backup Source Type list. However, you cannot back up the Exchange Server from this location. You can only back up the SQL Server with a SQL Server Job on the SQL Server Virtual node.

If you create a new SQL Server Job from an Exchange Virtual node, the SQL Server is available in the Backup Source Type list. However, you cannot back up the SQL Server from

this location. You can only back up the Exchange Server with an Exchange Job on the Exchange Virtual node.

To install and configure the Cluster plug-in:

1. Install the Agents and plug-ins on the physical nodes.
2. Configure the Cluster, SQL, and Exchange 2003/2007 plug-ins on the physical nodes.
3. Create a new Agent for your Exchange or SQL cluster on the virtual node using the IP address or host name.
4. On the Agent, double-click the Global file.
5. Select a drive letter for your SQL or Exchange Cluster. Click **OK**.
6. Enter your Vault connection information. Click **OK**.

8 Working with the Command Line Interface

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

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

8.1 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	Re-synchronizes 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	

8.2 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>	Is safeset encryption password (case sensitive).
/ASSIST[=YES]	Requests operator assistance, if necessary.
/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 all the Job-specific files and the root of the Job data sub-directories.

8.3 Backup Command Options

The following qualifiers apply to all Backup commands:

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

8.4 Restore Command Options

These qualifiers apply to all restore commands:

Qualifier	Description
/CREATESUBDIRS[=YES]	Creates all necessary sub-directories.
/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.

8.5 Sync Command Options

This qualifier applies to the synchronize command (synch):

Qualifier	Description
/SOURCE=<source>	The name of the server to re-synchronize from. By default, the Backup destination is used.

8.6 Inventory Command Options

The following qualifier applies to the INVENTORY command:

Qualifier	Description
/OUTPUT	

8.7 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	

8.8 Forcereseed Option

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

Before the delta is recreated, the backup is forced to reseed if the backup detected that the required DTA file was missing or corrupt. With the delta recreation feature, 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 will only apply to CLI. The UI will not be affected. In case of a failure in rebuilding a delta file, this is an alternative approach to rebuild the delta file by reseeding. 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, any 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, any delta information cannot be recreated.

In these cases, it will report errors in the restore log that the DTA recreation failed, on the version 5 files. The restore itself will still function 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, then the delta information can be recreated.)

When performing a Backup to a non-Vault location (i.e. Local backup), delta recreation information is included by default. To suppress this behavior, run the backup via the Command Line Interface with:

```
/FORCEDELTAREC=No
```

8.9 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.

8.10 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.

8.11 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, sub-directories are created under the data directory for each Job, with the same name as the Job.

Local catalog files, Delta information files, and other related files would be stored in the Job-specific sub-directory.

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.

8.12 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
```

8.13 Global Job Settings

Setting	Description
Data_directory	Specifies the location of all the Job-specific files and the root of the Job data sub-directories.
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.
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.

8.14 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 sub-directories. 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.
Backup.enc_type	The encryption type. These are the options: • NONE • DES • TRIPLEDES • BLOWFISH • AES
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 sub-directory.
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"). **NOTE** 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. tape9: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 sub-directories.
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.
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.create_subdirs	Creates sub-directories.
Restore.use_orig_dirs	Restores data to the original directories.
Restore.destination	The location to restore to. For example: • \.*.* Restores to original locations and creates sub-directories • c:\.*.* Restores to C:, creating sub-directories • c:\temp*.* Restores to c:\temp, without creating sub-directories
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.

8.15 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 Agent Console application to execute immediate functions, such as backup and restore.

8.16 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.

8.17 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 that is specific to your operating system.

8.18 How Simultaneous Scheduled Backups are Processed

The position of the scheduled entries in the Schedule.cfg file relative to each other determines which entry takes precedence. For example, the 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 with the same command (backup, restore, synchronize) and Jobname are automatically rescheduled if they conflict.

8.19 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 the Windows Agent Console.

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 Agent Console 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.