User Guide - Windows File System *i*DataAgent

TABLE OF CONTENTS

Operation Window

Global Filters

SRM for Unix\Linux File System
Cost Analysis
Database Aging

Erase Backup Data

Uninstalling Components

Online Help Links

BEST PRACTICES

FAQS

BACKUP TROUBLESHOOTING

RESTORE TROUBLESHOOTING

1-TOUCH FOR WINDOWS - DEPLOYMENT

1-TOUCH FOR WINDOWS - CONFIGURATION

1-TOUCH FOR WINDOWS - RECOVERY

1-TOUCH FOR WINDOWS - TROUBLESHOOTING

1-TOUCH FOR WINDOWS - FAQS

ONEPASS AGENT - DEPLOYMENT

ONEPASS AGENT - CONFIGURATION

ONEPASS AGENT - ARCHIVE

ONEPASS AGENT - RECOVER

ONEPASS AGENT - ADVANCED CONFIGURATION

ONEPASS AGENT - ADVANCED ARCHIVE

ONEPASS AGENT - ADVANCED RECOVER

ONEPASS AGENT - TROUBLESHOOTING

ONEPASS AGENT - FAQS

DESKTOP BROWSE (ADMINISTRATOR) - INSTALL

DESKTOP BROWSE (ADMINISTRATOR) - SETUP

DESKTOP BROWSE (USER) - GETTING STARTED

DESKTOP BROWSE (USER) - RESTORE

DESKTOP BROWSE (USER) - ADVANCED OPTIONS

AGENTESS SRM

SRM FOR WINDOWS FILE SYSTEM - BASIC

SRM FOR WINDOWS FILE SYSTEM - ADVANCED

SRM FOR WINDOWS FILE SYSTEM - FILTERS

SRM FOR WINDOWS FILE SYSTEM - FILE LEVEL ANALYTICS

SRM FOR WINDOWS FILE SYSTEM - SUMMARIES

SRM FOR WINDOWS FILE SYSTEM - SRM ARCHIVER INTEGRATION

ONLINE HELP

Overview - Windows File System *i*DataAgent

<table>
<tr><td>

TABLE OF CONTENTS

</td><td>

WHERE TO GO NEXT

</td></tr>
</table>

Getting Started - Windows File System
Walks you through the process of installing and configuring the Windows File System *i*DataAgent.

INTRODUCTION

The Windows File System *i*DataAgent provides unified protection and recovery for the file system data residing on Windows clients. In addition to complete protection of file system data for disaster recovery, the Windows File System *i*DataAgent also provides more granular backup and recovery options that operate seamlessly with your data protection. Added options for deduplication, job management and reporting help ensure all your file system data is easily traceable and retrievable whenever the need arises.

KEY FEATURES

The Windows File System *i*DataAgent offers the following key features:

SIMPLIFIED DATA MANAGEMENT

The Windows File System *i*DataAgent enables easy management of all the Windows systems in your environment, by providing a singular approach to manage the data using the same unified console and infrastructure.

POINT-IN-TIME RECOVERY

In the event of a serious system failure, such as the breakdown of hardware, software, or operating systems, the Windows File System *i*DataAgent provides point-in-time recovery of files at any given time.

SYSTEM STATE

The Windows File System system state is made up of many components and services that are critical to recovery of the Windows operating system. The system state is backed up and restored as part of Windows File System *i*DataAgent backup and restore.

SNAPPROTECT BACKUP

SnapProtect™ backup enables you to create a point-in-time snapshot of the data to be used for various data protection operations. SnapProtect backup works in conjunction with software and hardware snapshot engines to provide snapshot functionality for data protection operations.

OFFICE COMMUNICATIONS SERVER

The Office Communications Server is made up of data, settings, and metadata that are critical to data protection operations residing in both the File System and SQL databases. In order to fully protect the Office Communications Server, both the OCS data and settings and the OCS metadata have to be backed up.
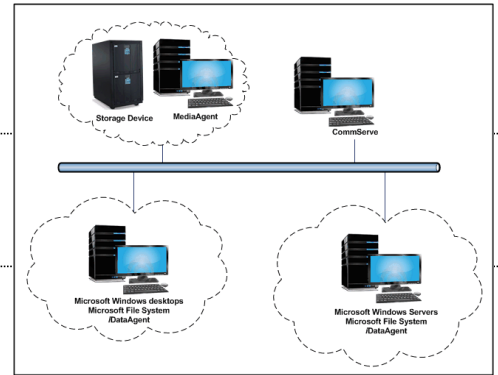
BACKUP AND RECOVERY FAILOVERS

In the event that a MediaAgent used for the backup or recovery operation fails, it is automatically resumed on alternate MediaAgents. In such cases, the backup or restore job will not restart from the beginning, but will resume from the point of failure. This is especially useful for backups and restores of large

amount of file system data.

In the event, that a network goes down, the backup and recovery jobs are resumed on alternate data paths. Similarly, in the event of a device failure, the jobs are automatically switched to alternate disk and tape drives.

EFFICIENT JOB MANAGEMENT AND REPORTING

You can view and verify the status of the backup and recovery operations from the Job Controller and Event Viewer windows within the CommCell Console. You can also track the status of the jobs using reports, which can be saved and easily distributed. Reports can be generated for different aspects of data management. You also have the flexibility to customize the reports to display only the required data and save them to any specified location in different formats. For example, you can create a backup job summary report to view at-a-glance the completed backup jobs. In addition, you can also schedule these reports to be generated and send them on email without user intervention.

BLOCK LEVEL DEDUPLICATION

Deduplication provides a smarter way of storing data by identifying and eliminating the duplicate items in a data protection operation.

Deduplication at the data block level compares blocks of data against each other. If an object (file, database, etc.) contains blocks of data that are identical to each other, then block level deduplication eliminates storing the redundant data and reduces the size of the object in storage. This way dramatically reduces the backup data copies on both the disk and tapes.

ADD-ON COMPONENTS

SRM FOR WINDOWS FILE SYSTEM

SRM is integrated with Windows File System iDataAgent to provide several advanced reporting capabilities for your backups. When enabled, backup jobs collect details on the file systems currently being used or not used, the memory and hardware resources consumed, storage usage, and granular file-level analytics.

SRM Reports include detailed information on the state of your file system data, including free space, used space, file count, file sizes, directory structure, and many other useful statistics.

In addition, **SRM Summaries** provide a graphical, real-time representation of usage information such as memory and CPU utilization. Optional file-level analytics provides even more granular details at the file-level for optimizing your storage resources.

SRM integration with Windows File System *i*DataAgent can be easily enabled with your backups to take advantage of these features.

1-TOUCH

1-Touch recovery helps to recover a crashed system in the least amount of time. By automatically rebuilding the operating system, you can recover systems with defective components such as inaccessible volumes or crashed disks. You don't need to reinstall the individual software packages or operating systems manually.

ONEPASS AGENT

The OnePass Agent is an integrated File System agent which backs up and archives the qualified data. It reclaims backup storage space when files and stubs are deleted on the primary storage.

DESKTOP BROWSE

Desktop Browse enables users to browse and restore data from a Web Browser, which provides the facility to access and restore data from anywhere.

TERMINOLOGY

The Windows File System documentation uses the following terminology:

CLIENT	The computer in which the *i*DataAgent is installed and contains the data to be secured.
BACKUPSET	A group of subclients which includes all of the data backed up by the *i*DataAgent.
SUBCLIENT	The Windows file system data to be backed up.

Back to Top

System Requirements - Microsoft Windows File System *i*DataAgent

| System Requirements | Supported Features |

The following requirements are for the Microsoft Windows File System *i*DataAgent:

OPERATING SYSTEM

WINDOWS 8

Microsoft Windows Client 8
Microsoft Windows Client 8.1

See Considerations for Microsoft Windows Server 2012, 2012 R2, and Windows 8 for more information.

WINDOWS SERVER 2012

Microsoft Windows Server 2012 Editions
Microsoft Windows Server 2012 R2 Editions

See Considerations for Microsoft Windows Server 2012, 2012 R2, and Windows 8 for more information.

WINDOWS 7

Microsoft Windows 7 32-bit and x64 Editions

WINDOWS SERVER 2008

Microsoft Windows Server 2008 Editions
Microsoft Windows Server 2008 R2 Editions

WINDOWS VISTA

Microsoft Windows Vista 32-bit and x64 Editions

WINDOWS SERVER 2003

Microsoft Windows Server 2003 32-bit and x64 Editions* with a minimum of Service Pack 1

* Special configuration considerations apply. See Installing 32-bit Components on a Microsoft Windows x64 Platform for more information.

WINDOWS XP

Microsoft Windows XP Home Editions with a minimum of Service Pack 3
Microsoft Windows XP Professional 32-bit and x64 Editions with a minimum of Service Pack 3

CLUSTER - SUPPORT

The software can be installed on a Cluster if clustering is supported by the above-mentioned operating systems.

For information on supported cluster types, see Clustering - Support.

HARD DRIVE

1.3 GB minimum of hard disk space for software/ 1.5 GB recommended

1 GB of additional hard disk space for log file growth

725 MB of temp space required for install or upgrade (where the temp folder resides)

MEMORY

32 MB RAM minimum required beyond the requirements of the operating system and running applications

PROCESSOR

All Windows-compatible processors supported

PERIPHERALS

DVD-ROM drive

Network Interface Card

MISCELLANEOUS

NETWORK

TCP/IP Services configured on the computer.

MICROSOFT VISUAL C++

Microsoft Visual C++ 2008 Redistributable Package is automatically installed. Note that Visual C++ 2008 Redistributable Package can co-exist with other versions of this software.

.NET FRAMEWORK

.NET Framework 2.0 is automatically installed. Note that .NET Framework 2.0 can co-exist with other versions of this software.

DISCLAIMER

Minor revisions and/or service packs that are released by application and operating system vendors are supported by our software but may not be individually listed in our System Requirements. We will provide information on any known caveat for the revisions and/or service packs. In some cases, these revisions and/or service packs affect the working of our software. Changes to the behavior of our software resulting from an application or operating system revision/service pack may be beyond our control. The older releases of our software may not support the platforms supported in the current release. However, we will make every effort to correct the behavior in the current or future releases when necessary. Please contact your Software Provider for any problem with a specific application or operating system.

Additional considerations regarding minimum requirements and End of Life policies from application and operating system vendors are also applicable

Getting Started - Windows File System Deployment

WHERE TO INSTALL

Install the software on a client computer that you want to protect and satisfies the minimum requirements specified in the System Requirements.

Follow the steps given below to install the Windows File System *i*DataAgent.

INSTALLATION

The software can be installed using one of the following methods:

METHOD 1: INTERACTIVE INSTALL

Use this procedure to directly install the software from the installation package or a network drive.

METHOD 2: INSTALL SOFTWARE FROM COMMCELL CONSOLE

Use this procedure to install remotely on a client computer.

BEFORE YOU BEGIN

Download Software Packages
Download the latest software package to perform the install.

System Requirements
Verify that the computer in which you wish to install the software satisfies the System Requirements.

METHOD 1: INTERACTIVE INSTALL

1. Run **Setup.exe** from the **Software Installation Package**.

2. Select the required language.

   Click **Next**.

3. Select the option to install software on this computer.

   The options that appear on this screen depend on the computer in which the software is being installed.

4. Select **I accept the terms in the license agreement**.

   Click **Next**.

5. Expand **Client Modules** | **Backup & Recovery** | **File System** and select **Windows File System** *i***DataAgent**

Click **Next**.

6. Click **YES** to install Microsoft .NET Framework package.

- This prompt is displayed only when Microsoft .NET Framework is not installed.
- Once the Microsoft .NET Framework is installed, the software automatically installs the Microsoft Visual J# 2.0 and Visual C++ redistributable packages.

7. If this computer and the CommServe is separated by a firewall, select the **Configure firewall services** option and then click **Next**.

For firewall options and configuration instructions, see Firewall Configuration and continue with the installation.

If firewall configuration is not required, click **Next**.

8. Enter the fully qualified domain name of the **CommServe Host Name**.

Click **Next**.

Do not use space and the following characters when specifying a new name for the CommServe Host Name:

\|`~!@#$%^&*()+=<>/?,[]{}:;'"

9. Click **Next**.

10. Select **Add programs to the Windows Firewall Exclusion List**, to add CommCell programs and services to the Windows Firewall Exclusion List.

Click **Next**.

This option enables CommCell operations across Windows firewall by adding CommCell programs and services to Windows firewall exclusion list.

It is recommended to select this option even if Windows firewall is disabled. This will allow the CommCell programs and services to function if the Windows firewall is enabled at a later time.

11. Verify the default location for software installation.

Click **Browse** to change the default location.

Click **Next**.

- Do not install the software to a mapped network drive.
- Do not use the following characters when specifying the destination path:

/ : * ? " < > | #

It is recommended that you use alphanumeric characters only.

12. Select a Client Group from the list.

Click **Next**.

This screen will be displayed if Client Groups are configured in the CommCell Console.

13. Click **Next**.

14. Click **Next**.

15. Select a **Storage Policy** from the drop-down list. Click **Next**.

Select the **Configure for Laptop or Desktop Backup** option to install **Backup Monitor** utility. This utility allows you to view the backup job summary from the client computer without opening the CommCell Console. See Monitor - Laptop User for more information.

If you do not have Storage Policy created, this message will be displayed.

Click **Next**.

You can create the Storage Policy later in step 19.

16. Click **Next**.

17. Click **Next**.

18. Click **Finish**.
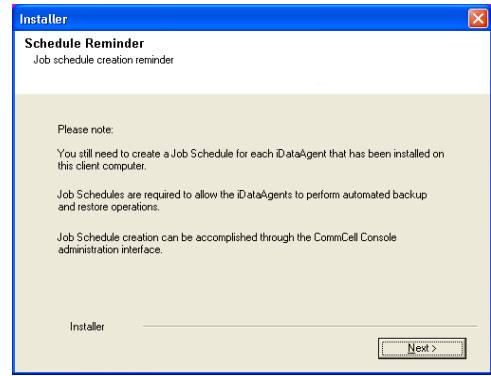
If you already have a storage policy selected in step 15, Click **Next** button available at the bottom of the page to continue.

If you do not have Storage Policy created, continue with the following step.

19. To create a storage policy, you must have configured a library in the CommCell.

- If you do not already have a library configured, go to Disk Library Creation.
- If you have a library configured, go to Storage Policy Creation.

DISK LIBRARY CREATION:

1. From the CommCell Console, click the **Backup Target** button on **EZ Operations Wizard**.

2. Click **Disc Library (For backup to disc)** and click **Next**.

3. Click **Use Local Disk**.

   Type the name of the folder in which the disc library must be located in the **Enter backup destination folder** box or click the **Browse** button to select the folder.

   Click **Next**.

   If you click the **Use Network Share** option you will be prompted for the credentials (user name and password) to access the share.

4. Click **Next**.

5. Click **Finish**.

This will create a library and Storage Policy. Click the **Next** button available at the bottom of the page to continue.

STORAGE POLICY CREATION:

1. From the CommCell Browser, navigate to **Policies**.

2. Right-click the **Storage Policies** and then click **New Storage Policy**.

3. Follow the prompts displayed in the Storage Policy Wizard. The required options are mentioned below:
   - Select the Storage Policy type as **Data Protection and Archiving** and click **Next**.
   - Enter the name in the **Storage Policy Name** box and click **Next**.
   - From the **Library** list, click the name of a disk library to which the primary copy should be associated and then click **Next**.

     Ensure that you select a library attached to a MediaAgent operating in the

current release.

○ From the **MediaAgent** list, click the name of a MediaAgent that will be used to create the primary copy and then click **Next**.

○ For the device streams and the retention criteria information, click **Next** to accept default values.

○ Select **Yes** to enable deduplication for the primary copy.

○ From the **MediaAgent** list, click the name of the MediaAgent that will be used to store the Deduplication store.

Type the name of the folder in which the deduplication database must be located in the Deduplication Store Location or click the Browse button to select the folder and then click **Next**.

○ Review the details and click **Finish** to create the Storage Policy.

This will create a storage policy. Click the `Next` button available at the bottom of the page to continue.
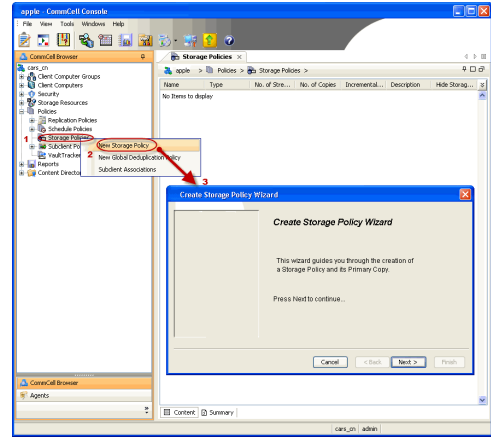
METHOD 2: INSTALL SOFTWARE FROM COMMCELL CONSOLE

1. From the CommCell Browser, select **Tools | Add/Remove Software | Install Software.**
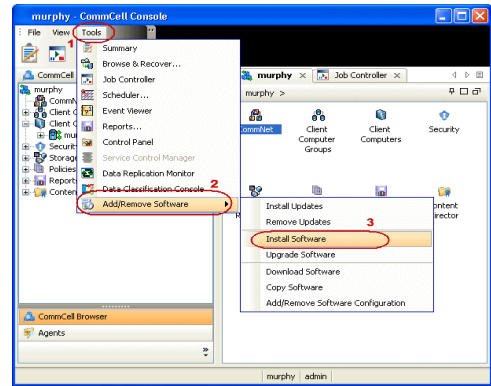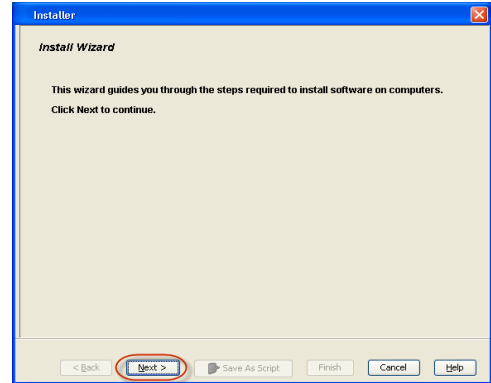
2. Click **Next**.

3. Select **Windows**.
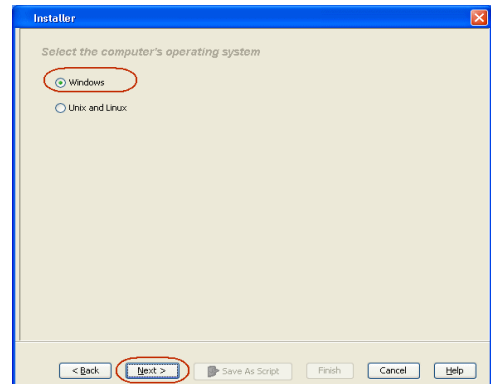
Click **Next**.

4. Select **Manually Select Computers**.

Click **Next**.

5. Enter the fully qualified domain name of the client computer.

For example: `apple.domain.company.com`

Click **Next**.

6. Click **Next**.

7. Specify **UserName** and **Password** that must be used to access the client computer.

Click **Next**.

8. Select **Windows File System** *i***DataAgent**.
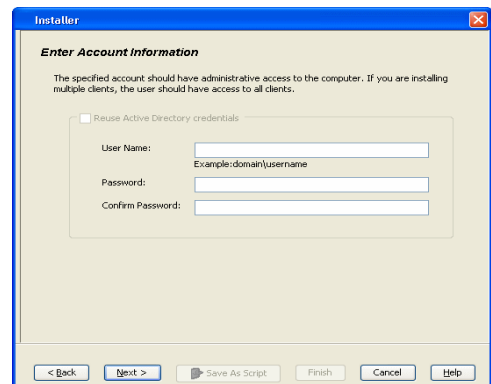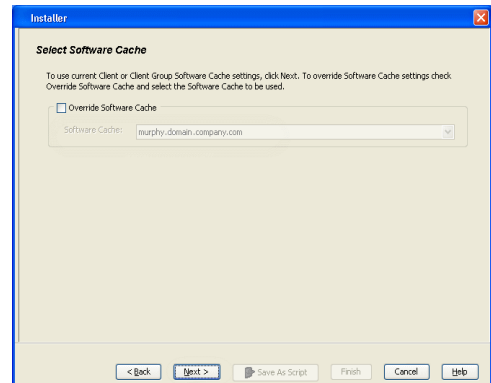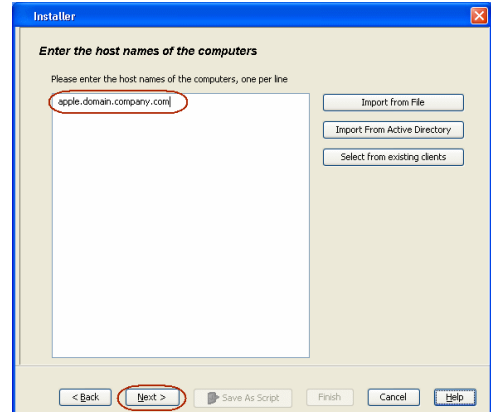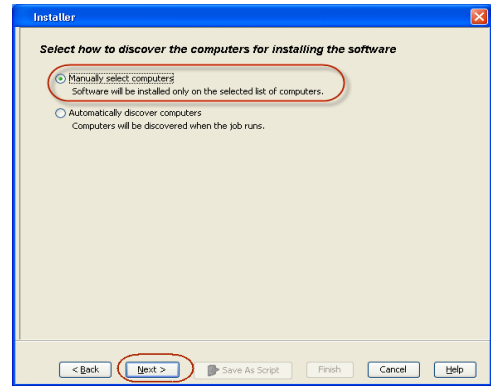
Click **Next**.

9.
- Select **Client Group** from **Available** and click **Add**.
- Select a **Storage Policy** from the drop-down list. Click **Next**.

    Select the **Configure for Laptop or Desktop Backup** option to install **Backup Monitor** utility. This utility allows you to view the backup job summary from the client computer without opening the CommCell Console. See Monitor - Laptop User for more information.
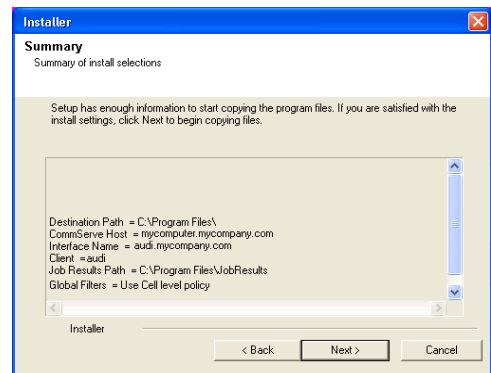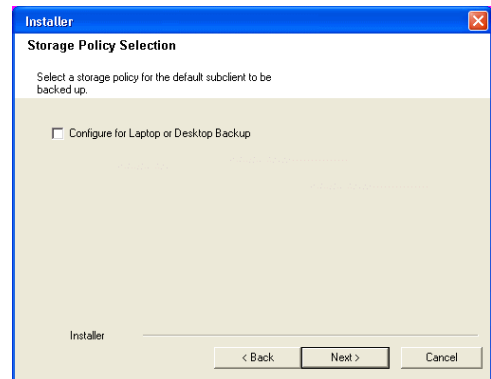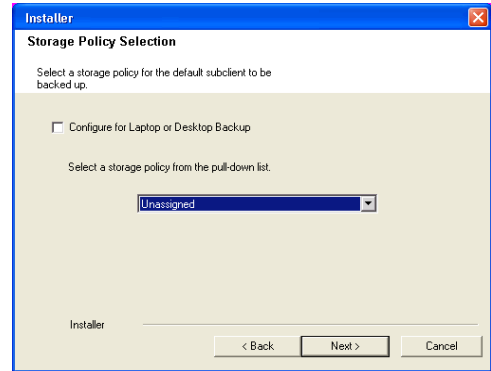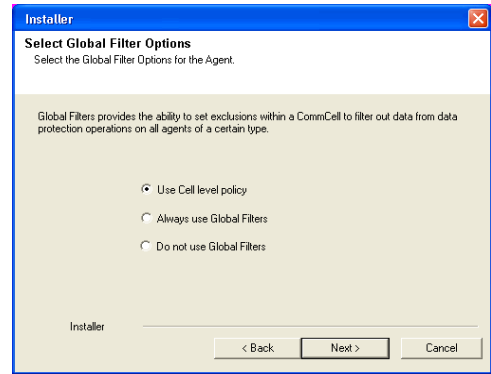

10. Click **Next**.

11. Select **Immediate**.
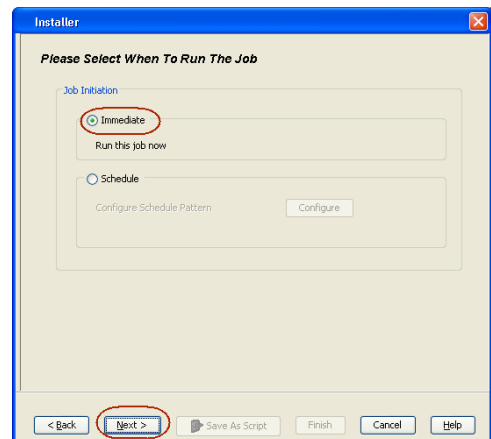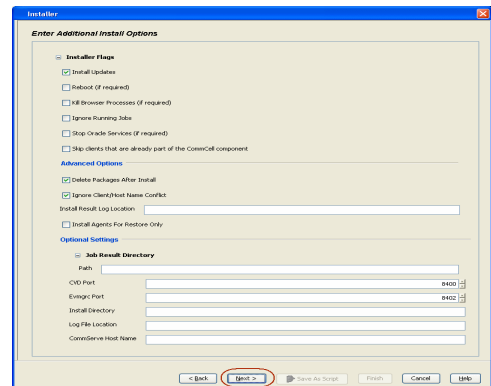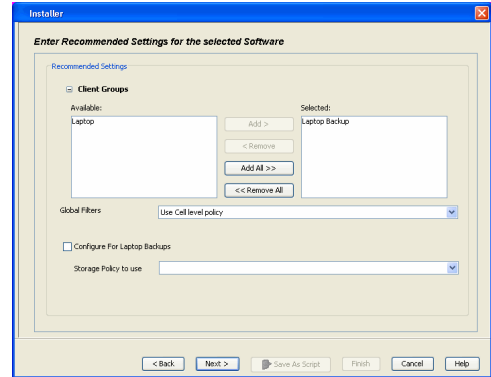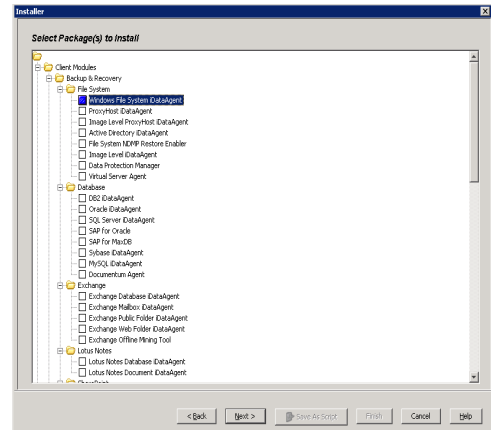
    Click **Next**.

12. Click **Finish**.

13. You can track the progress of the job from the **Job Controller** or **Event Viewer** window.
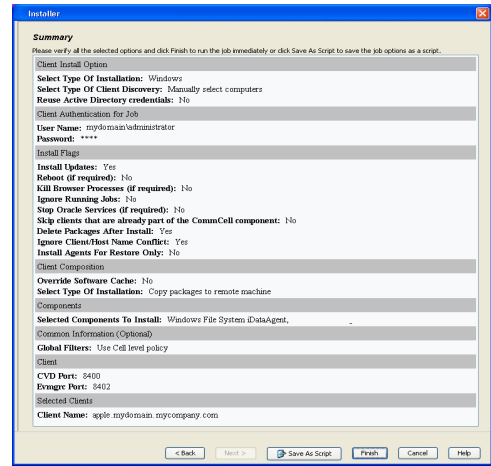
14. Once the job is complete, right-click the **CommServe** computer, click **View** and then click **Admin Job History**.
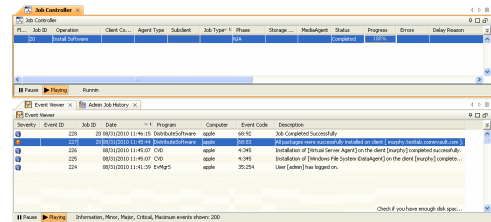
15. Select **Install/Upgrade/Remove Software**.

Click **OK**.
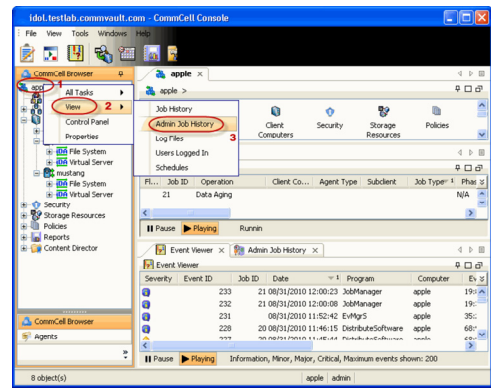
16. You can view the following details about the job by right-clicking the job:
- Items that succeeded during the job
- Items that failed during the job
- Details of the job
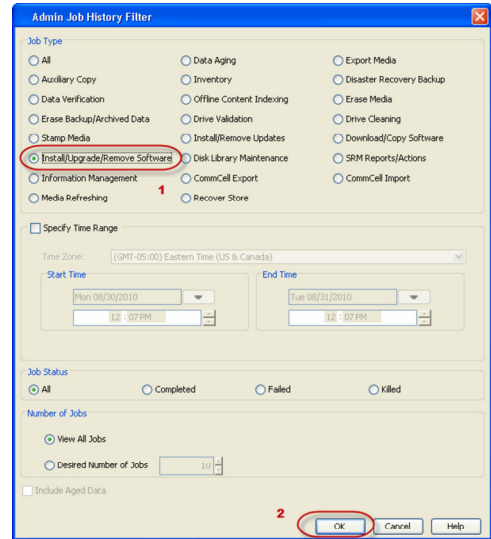
- Events of the job
- Log files of the job
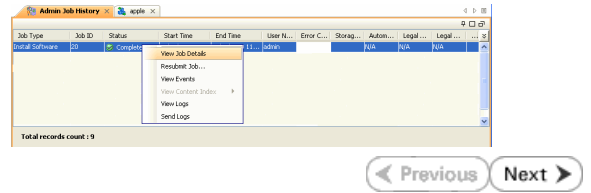
Getting Started - Windows File System *i*DataAgent Deployment on a Cluster

〈 Previous 〉 Next 〉

SKIP THIS PAGE IF YOU ARE NOT INSTALLING THIS AGENT ON A CLUSTER.

Click Next 〉 to continue with the deployment.

WHERE TO INSTALL

Install the software from the active node in the cluster group. Make sure the cluster group satisfies the minimum requirements specified in the System Requirements.

Follow the steps given below to install the Windows File System *i*DataAgent in a Clustered Environment.

BEFORE YOU BEGIN

Download Software Packages
Download the latest software package to perform the install.

System Requirements
Verify the cluster group which you wish to install the software satisfies the System Requirements.

1. Run **Setup.exe** from the **Software Installation Package**.

2. Select the required language.

   Click **Next**.

3. Select the option to install software on this computer.

   The options that appear on this screen depend on the computer in which the software is being installed.

4. Select **I accept the terms in the license agreement**.

   Click **Next**.

5. Select **Configure a Virtual Server**.
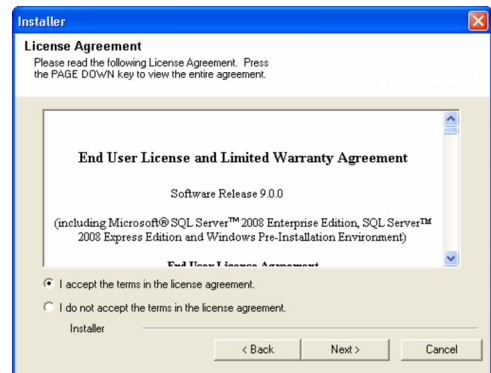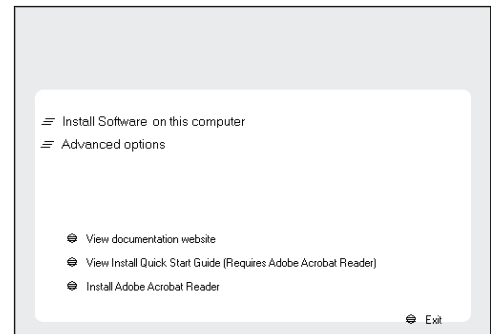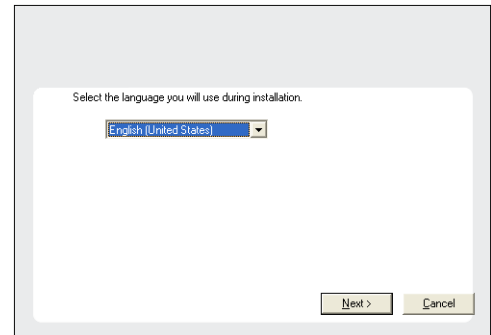
   Click **Next**.

6. Select the disk group in which the cluster group resides.

Click **Next**.
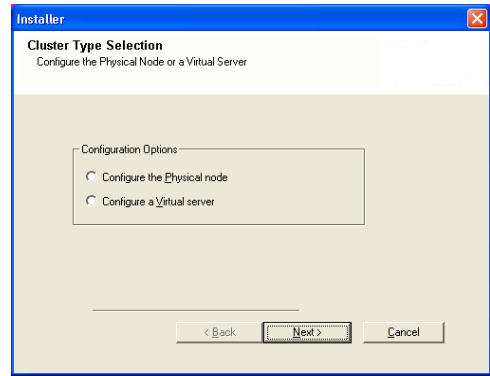
7. Expand **Client Modules** | **Backup & Recovery** | **File System** and select **Windows File System** *i***DataAgent**
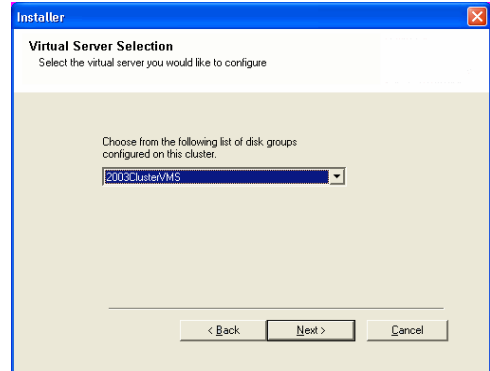
Click **Next**.

8. If this cluster group and the CommServe is separated by a firewall, select the **Configure firewall services** option and then click **Next**.

For firewall options and configuration instructions, see Firewall Configuration and continue with the installation.

If firewall configuration is not required, click **Next**.
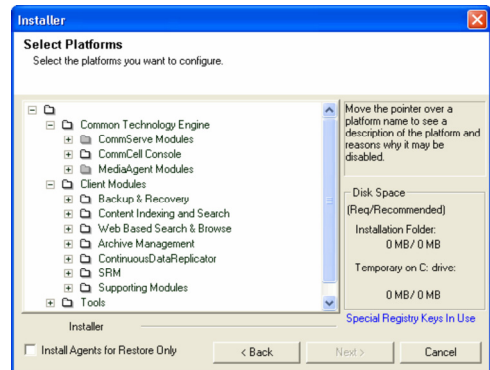
9. Enter the fully qualified domain name of the **CommServe Host Name**.
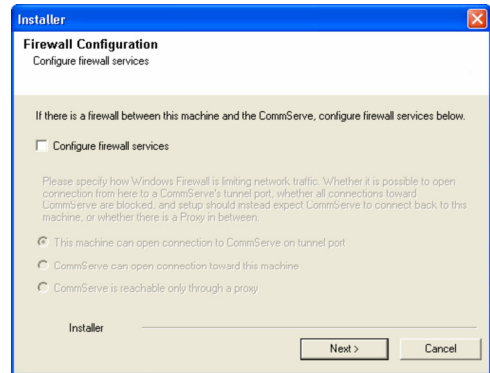
Click **Next**.

> Do not use space and the following characters when specifying a new name for the CommServe Host Name:
>
> \|`~!@#$%^&*()+=<>/?,[]{}:;'"

10. Verify the **Virtual Machine** name and click **Next**.

> The virtual machine is the name of the resource hosting the cluster group.

11. Select the name of the **Physical Machine** from drop-down list.

Click **Next.**

12. Select **Add programs to the Windows Firewall Exclusion List**, to add CommCell programs and services to the Windows Firewall Exclusion List.

Click **Next**.

> This option enables CommCell operations across Windows firewall by adding CommCell programs and services to Windows firewall exclusion list.
>
> It is recommended to select this option even if Windows firewall is disabled. This will allow the CommCell programs and services to function if the Windows firewall is enabled at a later time.

13. Type or **Browse** to specify the software installation path which must be located on local disk of your physical machine and then click **Next**.

- Do not install the software to a mapped network drive.
- Do not use the following characters when specifying the destination path:

  / : * ? " < > | #

> It is recommended that you use alphanumeric characters only.
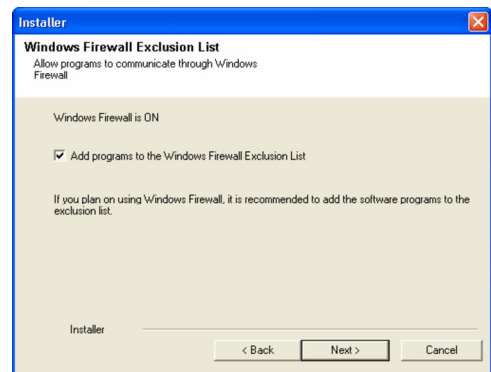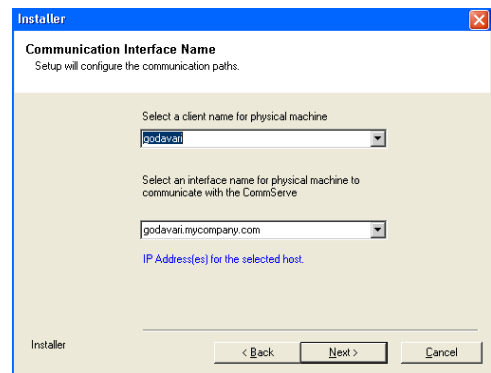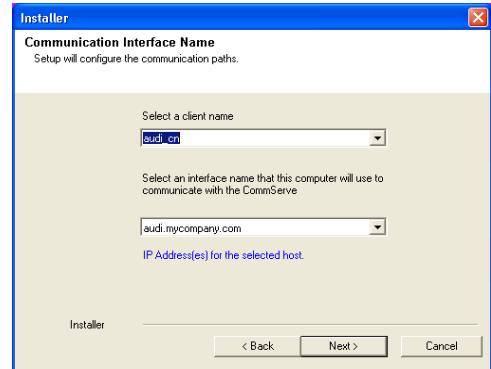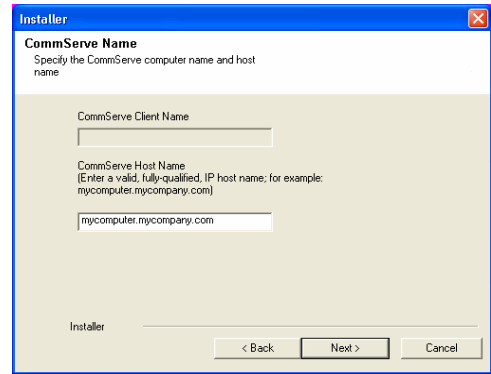
14. Verify the default location for Job Results Path.

Click **Browse** to change the default location.
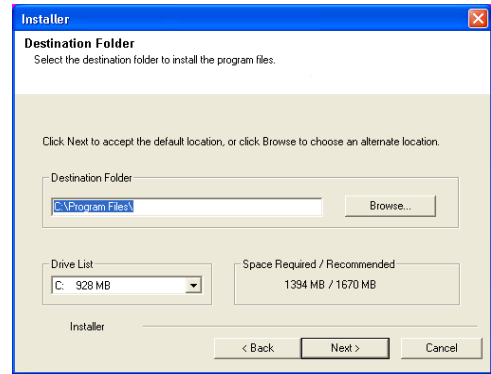
Click **Next**.

15. Select a Client Group from the list.

Click **Next**.

This screen will be displayed if Client Groups are configured in the CommCell Console.
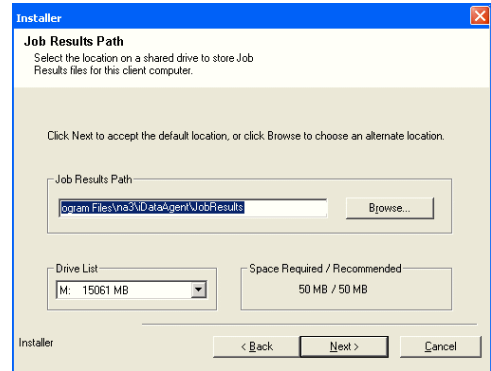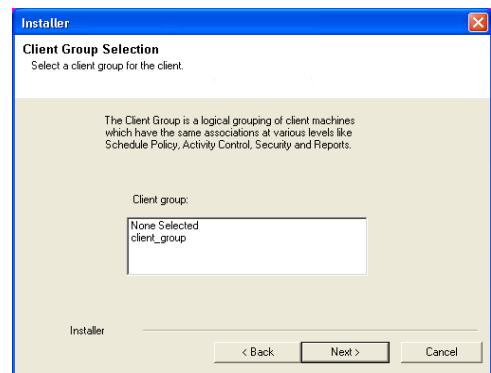
16. Click **Next**.
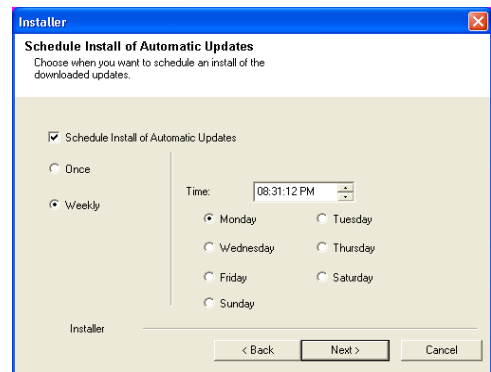
17. Click **Next**.

18. Select a **Storage Policy** from the drop-down list and click **Next**.

Select the **Configure for Laptop or Desktop Backup** option to install **Backup Monitor** utility. This utility allows you to view the backup job summary from the client computer without opening the CommCell Console. See Monitor - Laptop User for more information.

If you do not have Storage Policy created, this message will be displayed.

Click **OK**.

You can create the Storage Policy later in step 27.

19. Click **Next**.

20. To install the software on the remaining nodes of the cluster, click **Yes**.

To complete the install for this node only, click **No**.

21. Select cluster nodes from the **Preferred Nodes** list and click the arrow button to move them to the **Selected Nodes** list.

Once you complete your selections, click **Next**.

- The list of **Preferred Nodes** displays all the nodes found in the cluster; from this list you should only select cluster nodes configured to host this cluster group server.
- Do not select nodes that already have multiple instances installed.
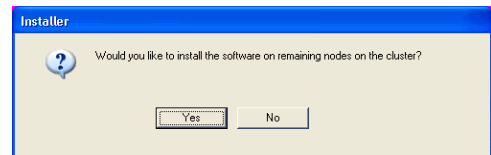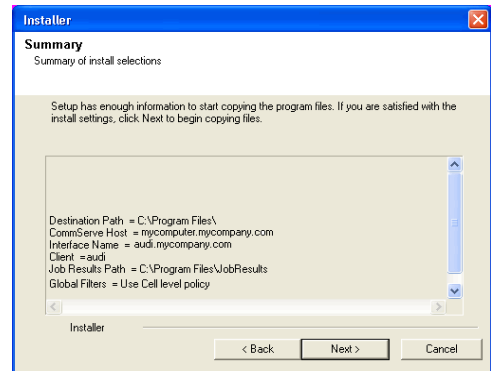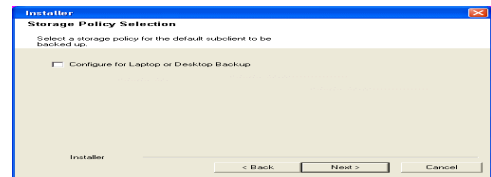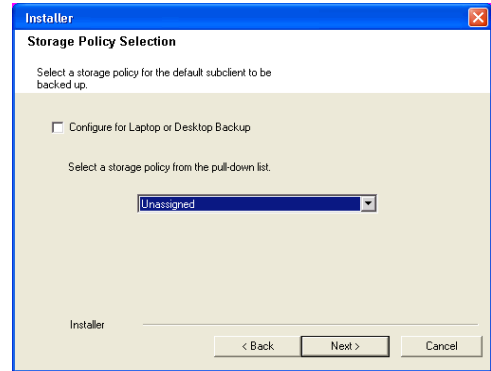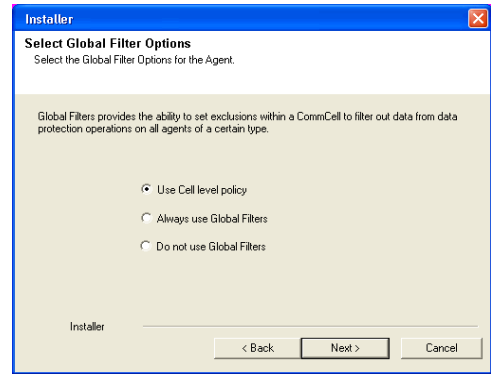
22. Specify **User Name** and **Password** for the **Domain Administrator account Information** to perform the remote install on the cluster nodes you selected in the previous step.

Click **Next**.
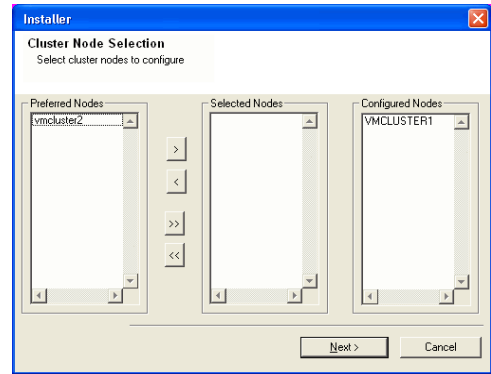
23. The progress of the remote install for the cluster nodes is displayed; the install can be interrupted if necessary.

Click **Stop** to prevent installation to any nodes after the current ones complete.

Click **Advanced Settings** to specify any of the following:

● Maximum number of nodes on which Setup can run simultaneously.
● Time allocated for Setup to begin executing on each node, after which the install attempt will fail.
● Time allocated for Setup to complete on each node, after which the install attempt will fail.

> If, during the remote install of a cluster node, setup fails to complete or is interrupted, you must perform a local install on that node. When you do, the install begins from where it left off, or from the beginning if necessary. For procedures, see Manually Installing the Software on a Passive Node.
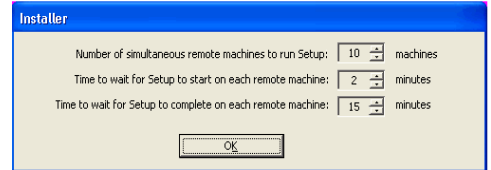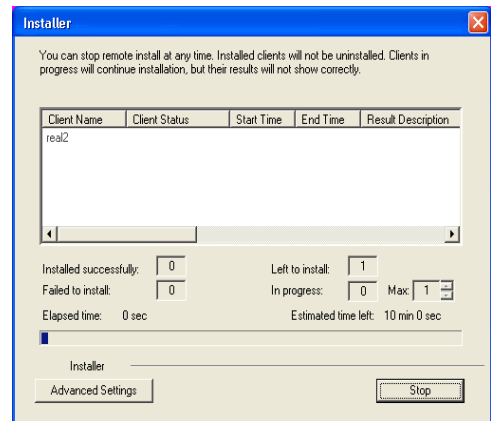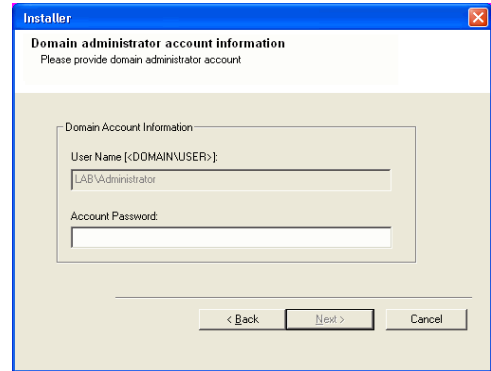
24. Read the summary for remote installation to verify that all selected nodes were installed successfully.

Click **Next**.

● If any node installation fails, you must manually install the software on that node once the current installation is complete. See Manually Installing the Software on a Passive Node for step-by-step instructions.
● The message displayed on your screen will reflect the status of the selected nodes, and may look different from the example.
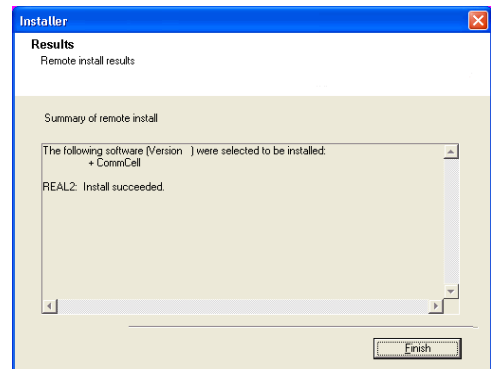
25. Click **Next**.

26. Click **Finish**.
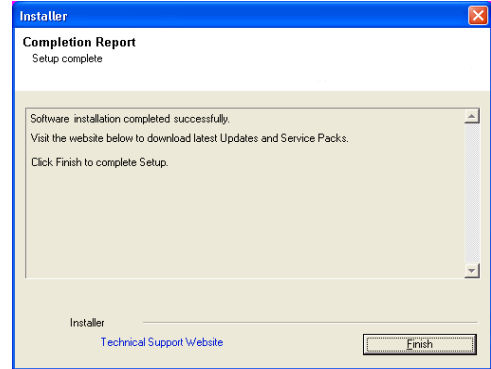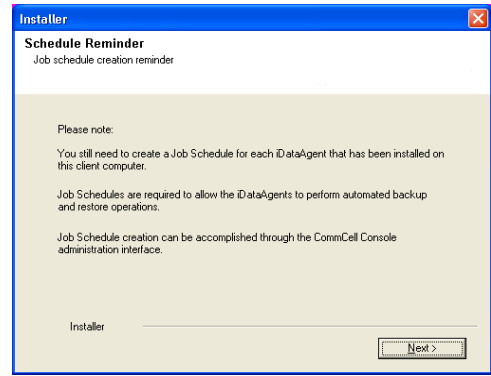
If you already have a storage policy selected in step 18, Click **Next** button available at the bottom of the page to proceed to the **Configuration** section.

If you do not have Storage Policy created, continue with the following step.

27. To create a storage policy, you must have configured a library in the CommCell.
- If you do not already have a library configured, go to Disk Library Creation.
- If you have a library configured, go to Storage Policy Creation.

DISK LIBRARY CREATION:

1. From the CommCell Console, click the **Backup Target** button on **EZ Operations Wizard**.

2. Click **Disc Library (For backup to disc)** and click **Next**.

3. Click **Use Local Disk**.

   Type the name of the folder in which the disc library must be located in the **Enter backup destination folder** box or click the **Browse** button to select the folder.

   Click **Next**.

   If you click the **Use Network Share** option you will be prompted for the credentials (user name and password) to access the share.

4. Click **Next**.

5. Click **Finish**.

This will create a library and Storage Policy. Click the **Next** button available at the bottom of the page to continue.

STORAGE POLICY CREATION:

1. From the CommCell Browser, navigate to **Policies**.

2. Right-click the **Storage Policies** and then click **New Storage Policy**.

3. Follow the prompts displayed in the Storage Policy Wizard. The required options are mentioned below:
   ○ Select the Storage Policy type as **Data Protection and Archiving** and click **Next**.
   ○ Enter the name in the **Storage Policy Name** box and click **Next**.
   ○ From the **Library** list, click the name of a disk library to which the primary copy should be associated and then click **Next**.

     Ensure that you select a library attached to a MediaAgent operating in the

current release.

○ From the **MediaAgent** list, click the name of a MediaAgent that will be used to create the primary copy and then click **Next**.

○ For the device streams and the retention criteria information, click **Next** to accept default values.

○ Select **Yes** to enable deduplication for the primary copy.

○ From the **MediaAgent** list, click the name of the MediaAgent that will be used to store the Deduplication store.

Type the name of the folder in which the deduplication database must be located in the Deduplication Store Location or click the Browse button to select the folder and then click **Next**.

○ Review the details and click **Finish** to create the Storage Policy.

Getting Started - Windows File System *i*DataAgent Deployment On A Non-Microsoft Cluster

SKIP THIS PAGE IF YOU ARE NOT INSTALLING THIS AGENT ON A NON-MICROSOFT CLUSTER.

Click Next ▶ to begin Configuration.

INSTALLATION	RELATED TOPICS
The software can be installed in one of the following Non-Microsoft Clustered environments:	**Download Software Packages** Download the latest software package to perform the install.
INSTALL WINDOWS FILE SYSTEM IDATAAGENT IN VERITAS CLUSTER ENVIRONMENT	**System Requirements** Verify that the computer in which you wish to install the software satisfies the System Requirements.
Use this procedure to install the software from the installation package or a network drive on a VERITAS Cluster environment.	**Firewall** Provides comprehensive information on firewall.
INSTALL WINDOWS FILE SYSTEM IDATAAGENT IN HP SCALABLE NAS/POLYSERVE CLUSTER ENVIRONMENT	
Use this procedure to install the software from the installation package or a network drive on a NAS/Polyserve Clustered environment.	

INSTALL WINDOWS FILE SYSTEM IDATAAGENT IN VERITAS CLUSTER ENVIRONMENT

WHERE TO INSTALL

Install the software in a VERITAS Clustered Environment, by locating the active node that is hosting the cluster resources and perform the installation from this node to the virtual node.

Follow the steps given below to install the Windows File System iDataAgent in a VERITAS Clustered environment

1. Create `bIgnoreClusterVMCheck` registry key to detect that the agent is being installed on a virtual node in a non-Microsoft cluster.

   To create the registry key, see the following steps:

   1. Start the Registry Editor (Regedit.exe or Redegt32.exe)

   2. Locate the directory under which you want to create a key, e.g., `HKEY_LOCAL_MACHINE\SOFTWARE\`.

   3. Right click the **SOFTWARE** and click **New** -> **Key**.

   4. Name the key as **GalaxyInstallerFlags**.

   5. Right click the **GalaxyInstallerFlags** and select **New -> DWORD** value, name it as `bIgnoreClusterVMCheck` and by double clicking the `bIgnoreClusterVMCheck` key modify the **Value** data to **1**.

2. Run **Setup.exe** from the **Software Installation Package**.

3. Select the required language.

   Click **Next**.

4. Select the option to install software on this computer.

   The options that appear on this screen depend on the computer in which the software is being installed.

5. Select **I accept the terms in the license agreement**.
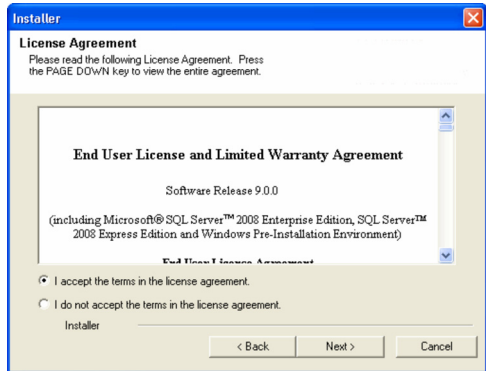
Click **Next**.

6. Select **Configure a Virtual Server**.

Click **Next**.
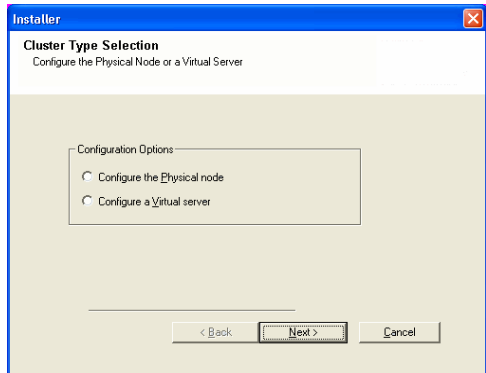
7.
- In the **disk groups** box, specify the host name of the Virtual Host created for backup, e.g., VirtualVeritasServe.
- In the **Communication Interface Name** box, specify the fully qualified domain name of the Virtual Host, e.g., VirtualVeritasServe.acme.com.
- Click **Next**.

8. Specify the hosts node in the **Preferred Nodes** and click **Add** to add in the Nodes on which **Virtual Group is configured to run**.

Specify the name of active node in **Current Owner Node** box.

Click **Next**.

9. Click **Yes** if it is the Active node.

NOTES

- If you click **No** the program will perform the passive install. Follow the steps described in Manually Installing the Software on a Passive Node.
- This screen may look different from the example shown.

10. Expand **Client Modules** | **Backup & Recovery** | **File System** and select **Windows File System *i*DataAgent**

Click **Next**.

11. If this computer and the CommServe is separated by a firewall, select the **Configure firewall services** option and then click **Next**.

For firewall options and configuration instructions, see Firewall Configuration and continue with the installation.

If firewall configuration is not required, click **Next**.

12. Enter the fully qualified domain name of the **CommServe Host Name**.

Click **Next**.

Do not use space and the following characters when specifying a new name for the CommServe Host Name:

\|`~!@#$%^&*()+=<>/?,[]{}:;'"

13. Click **Next**.

14. Select **Add programs to the Windows Firewall Exclusion List**, to add CommCell programs and services to the Windows Firewall Exclusion List.

Click **Next**.

> This option enables CommCell operations across Windows firewall by adding CommCell programs and services to Windows firewall exclusion list.
>
> It is recommended to select this option even if Windows firewall is disabled. This will allow the CommCell programs and services to function if the Windows firewall is enabled at a later time.

15. Verify the default location for software installation.

Click **Browse** to change the default location.

Click **Next**.

- Do not install the software to a mapped network drive.
- Do not use the following characters when specifying the destination path:

  / : * ? " < > | #

  It is recommended that you use alphanumeric characters only.
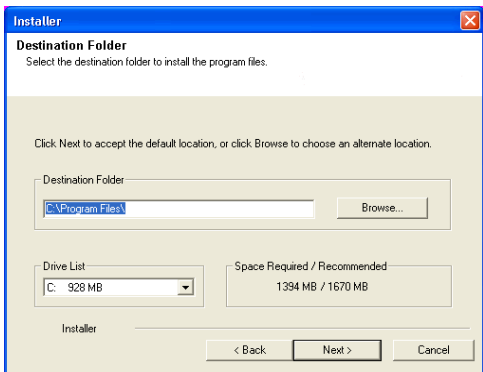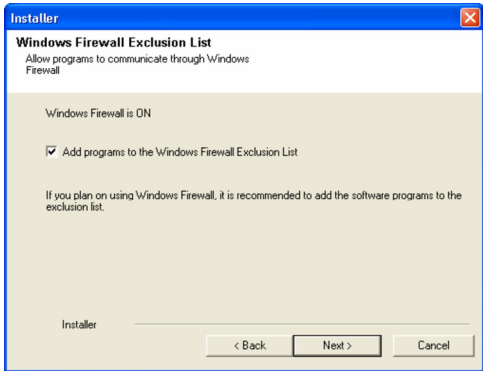
16. Select a Client Group from the list.

Click **Next**.

> This screen will be displayed if Client Groups are configured in the CommCell Console.
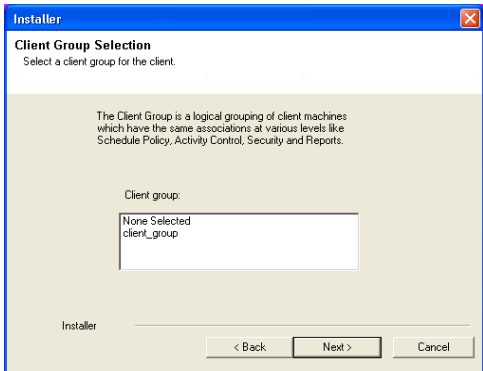
17. Click **Next**.

18. Click **Next**.
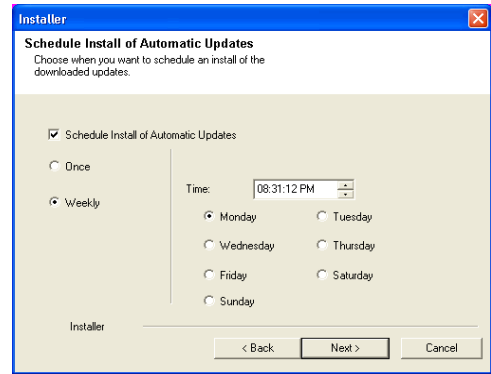
19. Select a **Storage Policy** from the drop-down list.
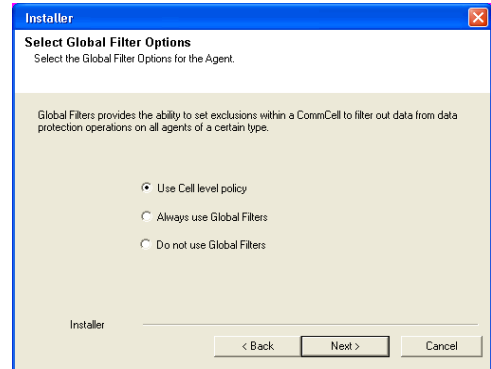
Click **Next**.

20. Click **Next**.
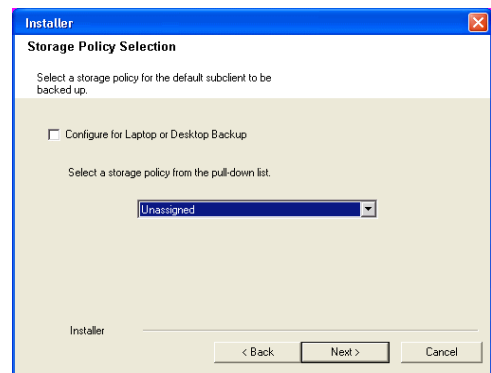
21. Click **OK** and manually configure the cluster resources.

See Configuring the VERITAS Cluster Resources for more information on configuring the cluster resources.
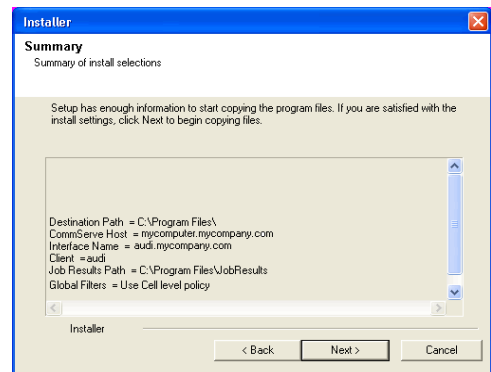
22. Click **Next**.
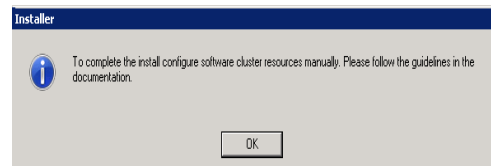
23. Click **Finish**.
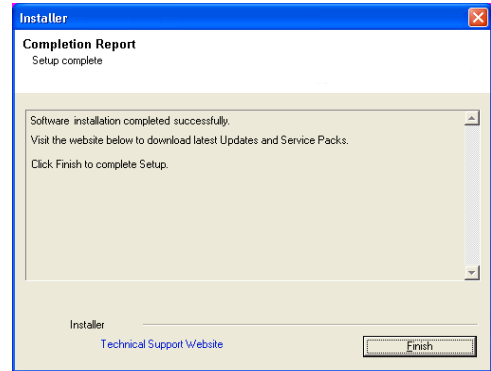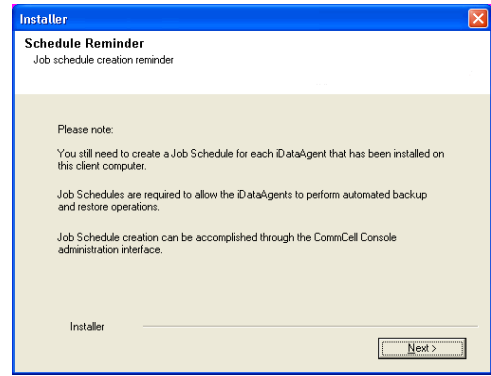
CONFIGURING VERITAS CLUSTER RESOURCES

In case of VERITAS Cluster you must manually install the software on all the available Nodes. For installs on the VERITAS Cluster, complete the following procedures for the agent. These procedures can be completed using the VERITAS Cluster Administrator.

CREATE THE CLUSTER RESOURCES FOR SERVICES

24. Once the physical nodes and the virtual machine are installed, services should be added as generic services.

Also, you may want to designate the services as "critical" if you want to cause the virtual machine to fail over if the associated service stops.

- In Windows Services, locate the services for each installed cluster (e.g., `Bull Calypso Cluster Plugin (penodevn1_netwo) (instance001)`) right-click and select **Properties**, and locate the service name in the **General** tab (e.g., `GxClusPlugin (penodevn1_netwo) (Instance001)`)

  The service name is case- and space-sensitive, so record it exactly as it appears.

- In Cluster Administrator, navigate to the appropriate Cluster group. Create a generic service resource for the cluster plugin service.
- If you want an automatic failover to occur, mark the resource as **Critical** and **Enabled**.
- Repeat this procedure for each client installed on the cluster.

25. Create Service Dependencies

- In Cluster Administrator, click **Resources**.
- Click **Link** and make the Cluster plugin resource dependent upon the Mount resource and the **Lanman** service.

26. Associate Services with the Current Active Node

- In Cluster Administrator, navigate to the appropriate **GenericService** group.
- Right-click the cluster plugin resource.
- From the short-cut menu, click **Online** and the name of the current active node.

INSTALL WINDOWS FILE SYSTEM IDATAAGENT IN HP SCALABLE NAS/POLYSERVE CLUSTER ENVIRONMENT

WHERE TO INSTALL

Install the software in HP Scalable NAS/Polyserve Cluster environment from the active host to virtual server.

The software must be installed on each passive node available to the virtual host. During install, you will be asked to provide the name of the active host for each passive host installation. See Manually Installing the Software on a Passive Node for step-by-step instructions.

Follow the steps given below to install the Windows File System iDataAgent in a HP Scalalable NAS/Polyserve Clustered environment:

1. Create `bIgnoreClusterVMCheck` registry key to detect that the agent is being installed on a virtual node in a non-Microsoft cluster.

To create the registry key, see the following steps:

1. Start the Registry Editor (Regedit.exe or Redegt32.exe)

2. Locate the directory under which you want to create a key, e.g., `HKEY_LOCAL_MACHINE\SOFTWARE\`.

3. Right click the **SOFTWARE** and click **New** -> **Key**.

4. Name the key as **GalaxyInstallerFlags**.

5. Right click the **GalaxyInstallerFlags** and select **New - > DWORD** value, name it as `bIgnoreClusterVMCheck` and by double clicking the `bIgnoreClusterVMCheck` key modify the **Value** data to **1**.

2.
- In the PolyServe Matrix Server, create a virtual host resource name that has an assigned TCP/IP address in the network.
- Provide a virtual host name (e.g., VirtualPolyServe.acme.com) and an Application name (e.g., VirtualPolyServe).
- Select all network Interfaces that will be available as hosts for the backup software services and click **OK**.

3. From the Virtual Hosts tab in the PolyServe Matrix Server dialog box, locate the primary node for the virtual server you are installing, and perform the installation from the active (primary) host to the virtual server.

4. Run **Setup.exe** from the **Software Installation Package**.

5. Select the required language.

Click **Next**.

6. Select the option to install software on this computer.

The options that appear on this screen depend on the computer in which the software is being installed.

7. Select **I accept the terms in the license agreement**.
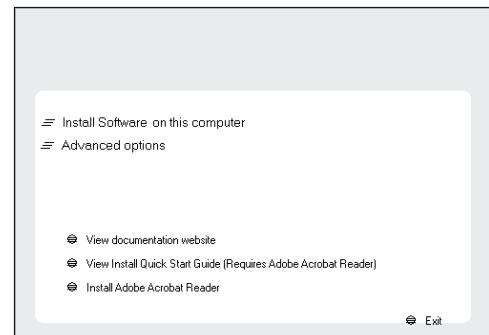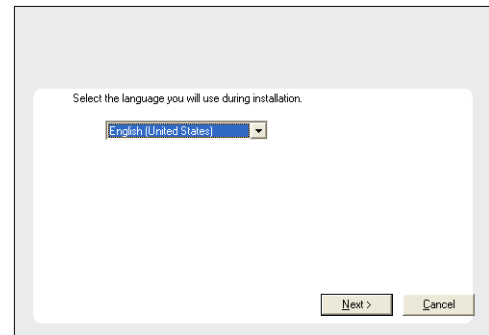
Click **Next**.

8. Select **Configure a Virtual Server**.

Click **Next**.

9.
- In the **disk groups** box, specify the host name of the Virtual Host created for backup, e.g., VirtualVeritasServe.
- In the **Communication Interface Name** box, specify the fully qualified domain name of the Virtual Host, e.g., VirtualVeritasServe.acme.com.
- Click **Next**.
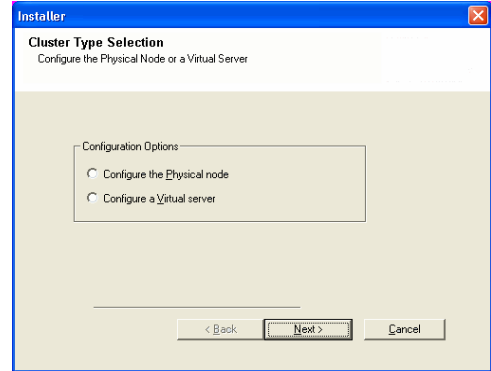
10. Specify the hosts node in the **Preferred Nodes** and click **Add** to add in the Nodes on which **Virtual Group is configured to run**.

Specify the name of active node in **Current Owner Node** box.

Click **Next**.
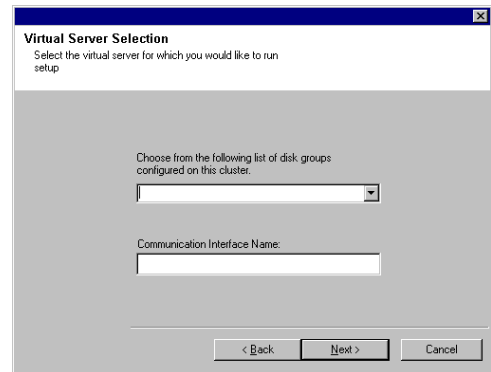
11. Click **Yes** if it is the Active node.

- If you click **No** the program will perform the passive install. Follow the steps described in Manually Installing the Software on a Passive Node.
- This screen may look different from the example shown.

12. Expand **Client Modules** | **Backup & Recovery** | **File System** and select **Windows File System** *i***DataAgent**

Click **Next**.

13. If this computer and the CommServe is separated by a firewall, select the **Configure firewall services** option and then click **Next**.

For firewall options and configuration instructions, see Firewall Configuration and continue with the installation.

If firewall configuration is not required, click **Next**.

14. Enter the fully qualified domain name of the **CommServe Host Name**.

Click **Next**.

> Do not use space and the following characters when specifying a new name for the CommServe Host Name:
>
> \|`~!@#$%^&*()+=<>/?,[]{}:;'"

15. Click **Next**.

NOTES

● The client name should be equivalent to the vhost name and the interface name equals the vhosts fully qualified domain name.

16. Select **Add programs to the Windows Firewall Exclusion List**, to add CommCell programs and services to the Windows Firewall Exclusion List.

Click **Next**.

> This option enables CommCell operations across Windows firewall by adding CommCell programs and services to Windows firewall exclusion list.
>
> It is recommended to select this option even if Windows firewall is disabled. This will allow the CommCell programs and services to function if the Windows firewall is enabled at a later time.
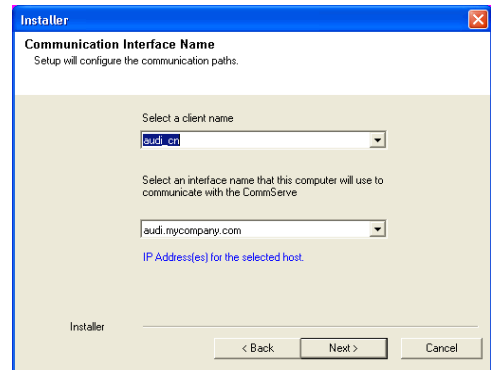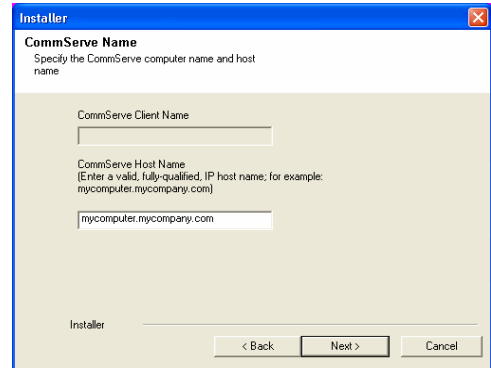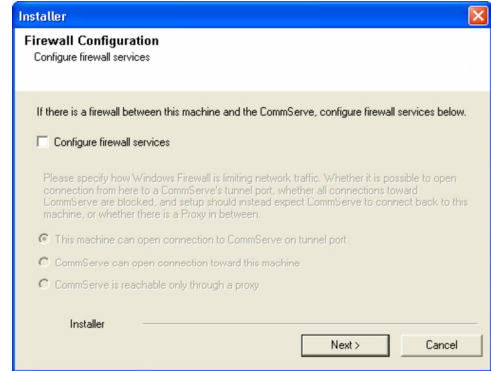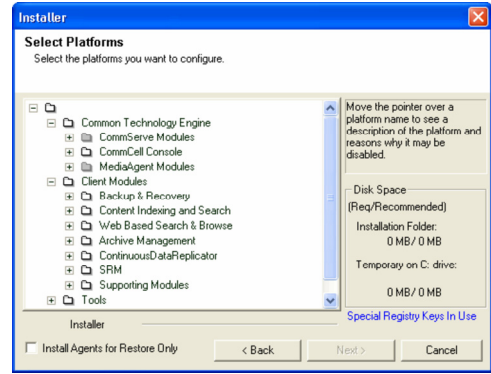
17. Verify the default location for software installation.

Click **Browse** to change the default location.

Click **Next**.

- Do not install the software to a mapped network drive.
- Do not use the following characters when specifying the destination path:

  / : * ? " < > | #

  It is recommended that you use alphanumeric characters only.

18. Select a Client Group from the list.

Click **Next**.

This screen will be displayed if Client Groups are configured in the CommCell Console.

19. Click **Next**.

20. Click **Next**.
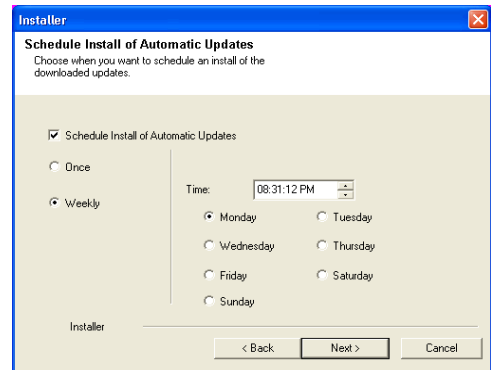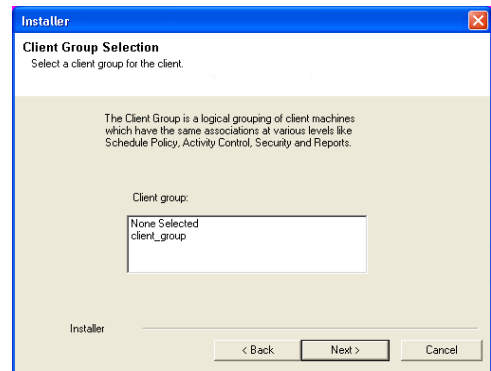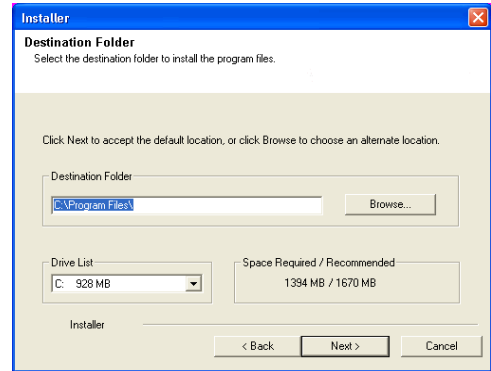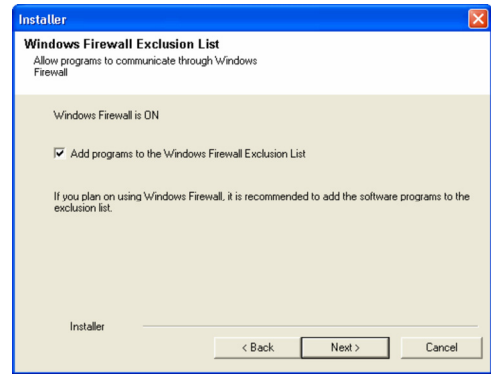
21. Select a **Storage Policy** from the drop-down list.
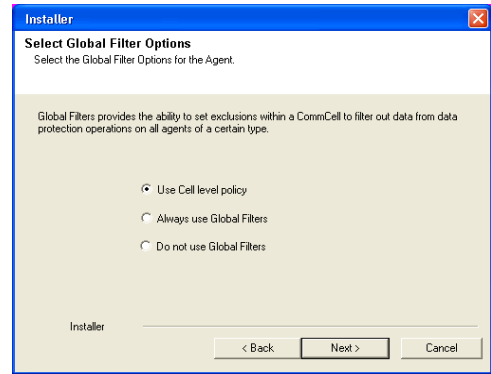
Click **Next**.

22. Click **Next**.
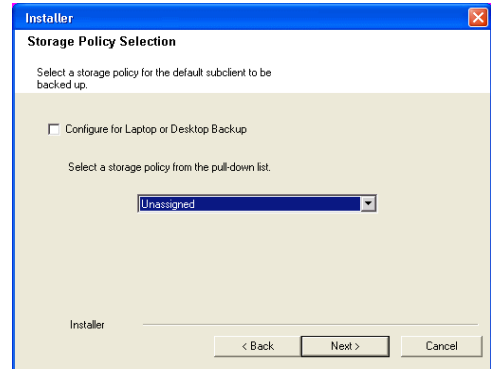
23. Click **OK** and manually configure the cluster resources.

See Configuring the HP Scalable NAS/Polyserve Cluster Resources for more information on configuring the cluster resources.
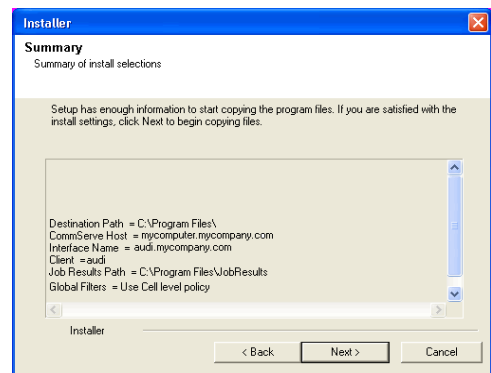
24. Click **Next**.
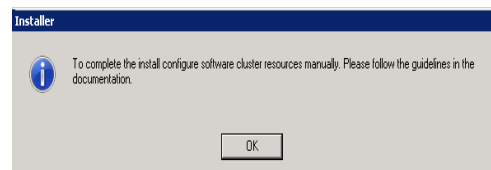
25. Click **Finish**.
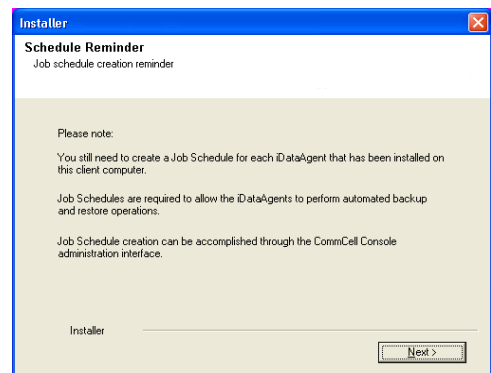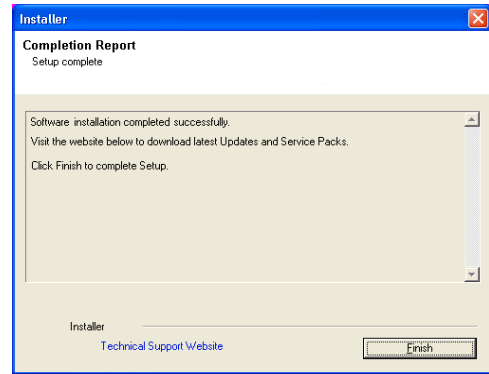
CONFIGURING HP SCALABLE NAS/POLYSERVE CLUSTER RESOURCES

For installs on the HP Scalable NAS/PolyServe Cluster, complete the following procedures for the agent.

26. Create and Use Scripts to Administer Virtual Machine Services.

You should create and use three scripts to administer virtual machine services:

- Probe script is used to reveal the state of the specified services. This is done using the `GxSCMCmd.exe` utility.
- Start script is used to start services.
- Stop script is used to stop services.

Create a probe script to have the status of both the Bull Calypso Communications Service (GxCVD) and the Bull Calypso Event Manager Service (GxEvMgrC) checked. In the probe script, include the `GxSCMCmd.exe` utility by name in the appropriate command. (This utility is available from the Resource Pack. See Tools and Utilities for more information.) Create a folder (e.g., `m:\GxSCMCmd`) on a shared disk that the virtual host you created has access to. Copy the `GxSCMCmd.exe` utility and the script files you created (`probe.bat`, `start.bat`, `stop.bat`) to this folder. The utility will return the state of the specified services: '0' if the services are running or '1' if services are stopped. For an error condition, '-1' is returned. Note that the service name includes the name of the client and the name of the instance. To avoid error in providing the vhost name and instance name in the path of scripts, copy the key name from here:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\GXClusPlugIn (vhostname) (Instance00x)`

> These examples provide sample script names, locations and virtual host name as suggested names not requirements.

The command syntax is:

GxSCMCmd.exe -IsRunning <list of service name>

For example, your probe script (e.g., `m:\GxSCMCmd\gxprobe.bat`) may appear as follows:

@echo off

if'%MX_ACTIVE_STATE%'='INACTIVE' exit 0

m:\GxSCMCmd\GxSCMCmd.exe -IsRunning "GxClusPlugIn (virtualpolyserve) (Instance001)"

if ERRORLEVEL 0 exit 0

exit 1

Be sure to copy the `GxSCMCmd.exe` utility to the shared disk resource. Also, be sure to include the probe script on the shared disk.

The stop and start scripts must also contain the registry entry for the virtual machine service names. Your start script (e.g., `m:\GxSCMCmd\gxstart.bat`) may appear as follows:

@echo off

C:\WINDOWS\system32\net.exe start "GxClusPlugIn (virtualpolyserve) (Instance001)"

exit 0

Your stop script (e.g., `m:\GxSCMCmd\gxstart.bat`) may appear as follows:

@echo off

C:\WINDOWS\system32\net.exe stop GxClusPlugIn (virtualpolyserve)

```
(Instance001)
```

exit 0

27. Add the Customer Service Monitor

Add the custom service monitor to the virtual host configuration in the PolyServe Matrix Server console.

1. Ensure that the virtual host name `<virtualpolyserve>` is online.

2. From the Services MMC snap-in, verify or manually start the cluster plugin service, "`Bull Calypso Cluster Plugin (virtualpolyserve) (Instance00x)`", on the active primary node for the Vhost `virtualpolyserve`

3. From the PolyServe Matrix Server, click the **Virtual Hosts** tab.

4. Right click **Virtual Host <**`virtualpolyserve`**>** and then **Add Service Monitor**.

5. For the **Monitor Type** field in the Add Service Monitor dialog box, click **CUSTOM**.

6. Assign a name to the service monitor by typing the name in the **Name** field.

7. In the **User probe script** field, type the path to the probe script that calls the GxSCMCmd.exe command (on the share disk)

8. Click **Advanced**.

9. From the Advanced Service Configuration dialog box, click the **Scripts** tab.

10. In the **Script pathname: Start** field, type the path to the start script (shared disk). In the corresponding **Timeout (seconds)** field, type a timeout value greater than 60 seconds.

11. In the **Script pathname: Stop** field, type the path to the stop script (shared disk). In the corresponding **Timeout (seconds)** field, type a timeout value greater than 60 seconds.

12. Click **OK** once, then again.

The monitor should now start, and the primary node should now be active. Failover will occur if services are disabled on the primary node, and services in such a case will move to a secondary node.

◀ Previous   Next ▶

Getting Started - Windows File System Configuration

CONFIGURATION

Once installed, follow the steps given below to assign a storage policy with the default subclient:

1.
- From the CommCell Browser, navigate to **Client Computers | <*Client*> | File System | defaultBackupSet**.
- Right-click the default subclient and then click **Properties**.
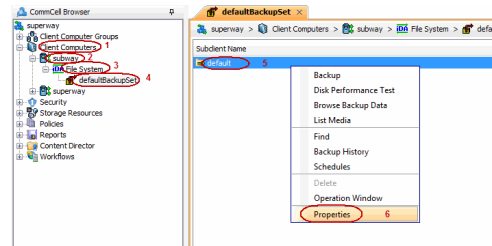
2.
- Click the **Storage Device** tab.
- In the **Storage Policy** box, select a Storage Policy name.
- Click **OK**.

Click **Next ▶** to continue.

If you do not have Storage Policy created, follow the step given below to create a storage policy.

3.
1. Click **Create Storage Policy**.
2. Follow the prompts displayed in the Storage Policy Wizard. The required options are mentioned below:
   ○ Select the Storage Policy type as **Data Protection and Archiving** and click **Next**.
   ○ Enter the name in the **Storage Policy Name** box and click **Next**.
   ○ From the **Library** list, click the name of a disk library to which the primary copy should be associated and then click **Next**.

   Ensure that you select a library attached to a MediaAgent operating in the current release.

   ○ From the **MediaAgent** list, click the name of a MediaAgent that will be used to create the primary copy and then click **Next**.
   ○ For the device streams and the retention criteria information, click **Next** to accept default values.
   ○ Select **Yes** to enable deduplication for the primary copy.
   ○ From the **MediaAgent** list, click the name of the MediaAgent that will be used to store the Deduplication store.

   Type the name of the folder in which the deduplication database must be located in the Deduplication Store Location or click the Browse button to select the folder and then click **Next**.

   ○ Review the details and click **Finish** to create the Storage Policy.

Getting Started - Windows File System Backup

PERFORM A BACKUP

Once the storage policy is configured, you are ready to perform your first backup.

WHAT GETS BACKED UP

COMPONENT	WHAT GETS BACKED UP
File System	File Allocation Table (FAT) file systems
	New Technology File Systems (NTFS)
	Transactional File Systems
	Distributed File System (DFS) data
File System Elements	Universal Naming Convention (UNC) Paths
	Mount Points
	Encrypted files
	Compressed Data
	Shared Volumes
	Share with Macintosh data
	Single Instance Storage
	Remote Storage Service
System State	System File Protection catalog and files
	Performance monitor configuration files
	Active Directory
	Registry
	Quotas
	SYSVOL (if this is a domain controller)
	Certificate Services database (if this is a certificate server)
	Cluster database (if this server is part of a cluster)
	COM+ database
	Terminal Server Licensing database
	RSM database
	WMI database
	DHCP
	WINS
	IIS
	UDDI (only with Windows Server 2003 using VSS)
	Disk quota information
	Event logs
	Content Indexing catalogs
	Network Policy Server (NPS)
	1-Touch Component
Office Communication Server (OCS)	OCS Data
	OCS Settings

WHAT DOES NOT GET BACKED UP

COMPONENT	WHAT DOES NOT GET BACKED UP
File System	Locked Files - Files that are locked by applications or system programs while they are in use.
Office Communication Server (OCS)	OCS Metadata - Use SQL Server iDataAgent to backup the OCS Metadata.
Resilient File System (ReFS) on Windows Server 2012	Change Journal and Data Classification scan methods are not supported on Resilient File System (ReFS) volumes - Use the classic scan to backup the data.
System State	Offline files will not get backed up if the client computer has UEFI.

Web Server on Windows Server 2012	Data from the Web Server will not get backed up.

The following section provides step-by-step instructions for performing your first backup:

1.
- From the CommCell Browser, navigate to **Client Computers | <*Client*> | File System | defaultBackupSet**.
- Right-click the default subclient and click **Backup**.

2.
- Click **Full** as backup type and then click **Immediate**.
- Click **OK**.
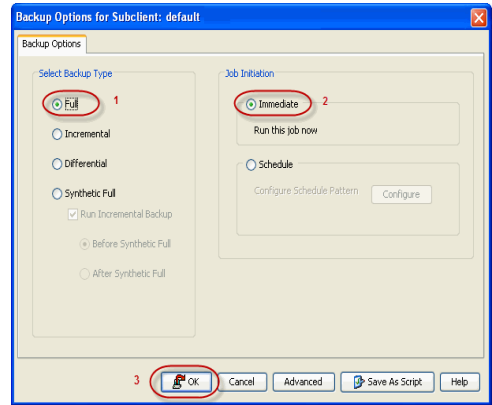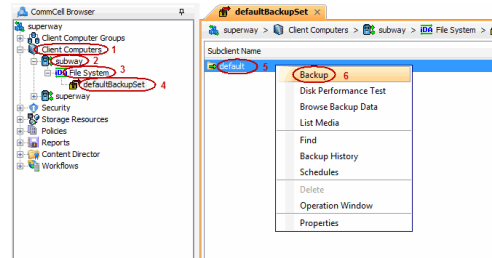
3. You can track the progress of the job from the **Job Controller** window of the CommCell console.
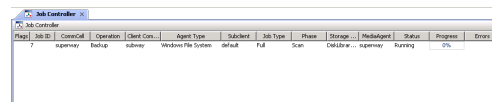
4. Once the job is complete, view the job details from the **Backup History**. Right-click the **Subclient** and select **Backup History**.
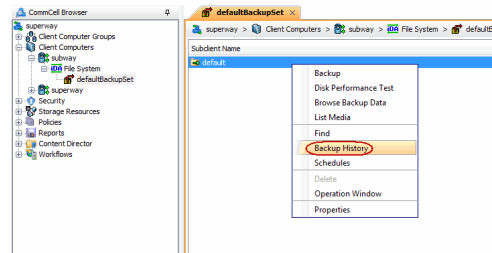
5. Click **OK**.
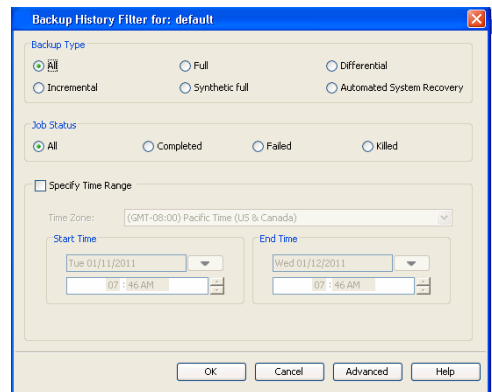
6. You can view the following details about the job by right-clicking the job:
- Items that failed during the job
- Items that succeeded during the job
- Details of the job
- Events of the job
- Log files of the job
- Media associated with the job
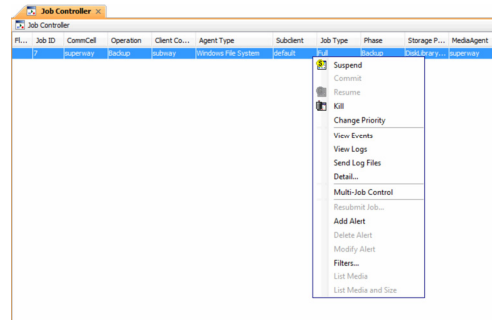
Getting Started - Windows File System Restore

Previous   Next
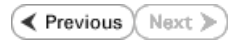
PERFORM A RESTORE

It is recommended that you perform a restore operation immediately after your first full backup to understand the process. The following section explains how restore the **Temp** folder to a new location.

1.
- From the CommCell Browser, navigate to **Client Computers| <*Client*> | File System | defaultBackupSet**
- Right-click the default subclient and then click **Browse Backup Data**.
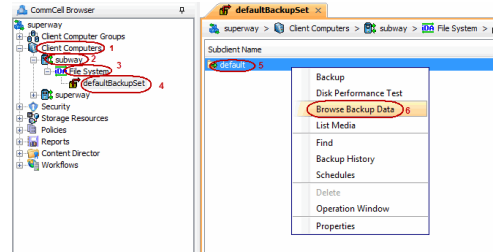
2.   Click **OK**.
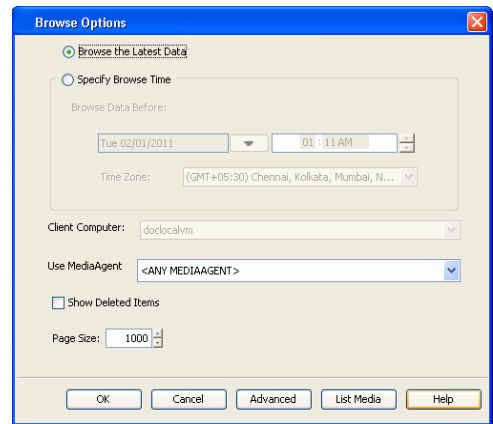
3.
- Expand the **defaultBackupSet** and navigate to **Windows** folder.
- Select the **Temp** folder.

  For the first restore job, select any folder with smaller data size.

- Click **Recover All Selected**.
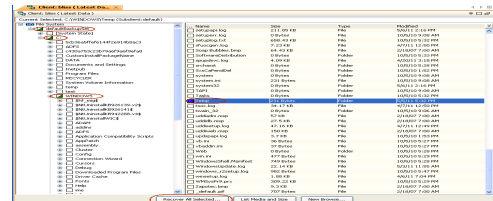
4.
- Clear the **Overwrite Files** and **Restore to same folder** options.
- Specify the destination path by clicking **Browse** button.

  This will ensure that the existing files are not overwritten.

- Click **OK**.

5.
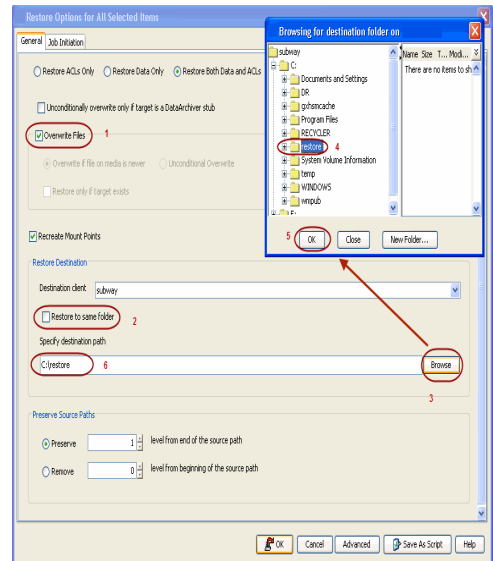
- Click the **Job Initiation** tab.
- Select **Immediate** to run the job immediately.
- Click **OK**.
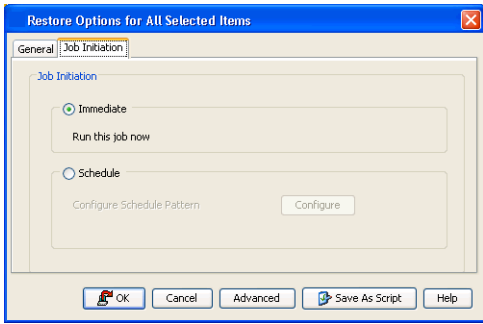
6. You can monitor the progress of the restore job in the **Job Controller** window of the CommCell Console.
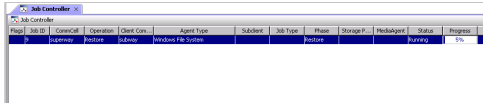
7. Once the restore job has completed, right-click the **defaultBackupSet** , point to **View** and then click **Restore History**.
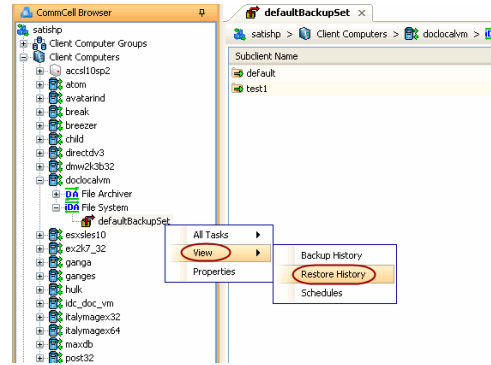
8. Click **OK**.
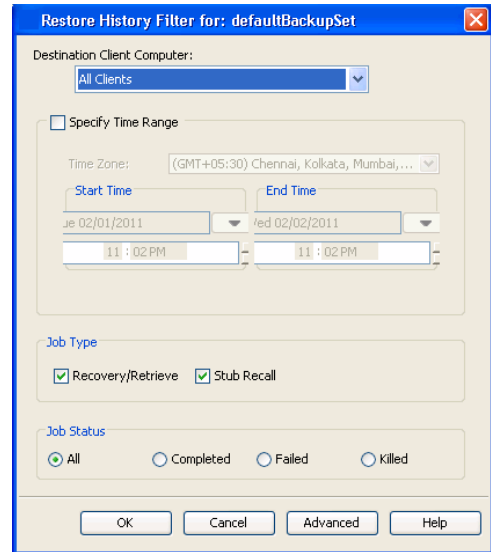
9. You can view the following details about the job by right-clicking the job:
   - View Restore Items

     You can view them as **Successful**, **Failed**, **Skipped** or **All**.

   - View Job Details
   - View Events of the restore job.
   - View Log files of the restore job
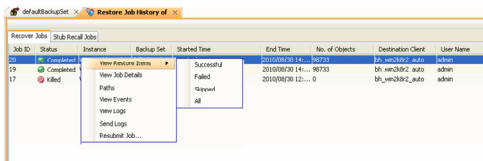
10. Once the File System is restored, verify that the restored files/folders are available in the restore destination provided during step 4.
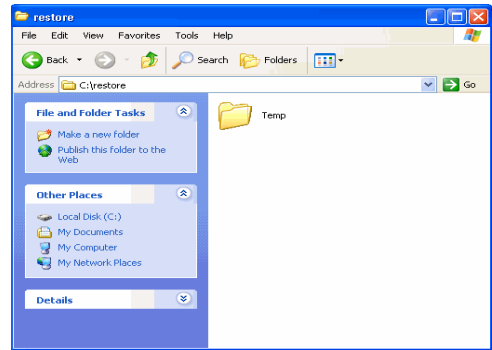
CONGRATULATIONS - YOU HAVE SUCCESSFULLY COMPLETED YOUR FIRST BACKUP AND RESTORE.

If you want to further explore this Agent's features read the **Advanced** sections of this documentation.

Advanced - Windows File System Configuration

TABLE OF CONTENTS

UNDERSTANDING THE COMMCELL CONSOLE

Windows File System *i*DataAgent uses following main components to perform backup and restore operations from the CommCell Console.

Backup Set - collective information of all the data that needs to be backed up for the client.

Subclient - defines the data to be backed up.
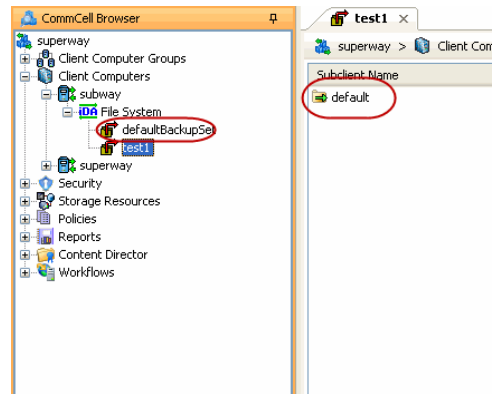
CREATING AN ON DEMAND BACKUP SET

On Demand backups allow content to be specified as an external input at the time of initiating a backup. Whereas traditional backups are performed using subclients, which contain fixed content configured prior to performing the operation, On Demand backups allow you to specify content each time you perform a backup.

Content for On Demand backups is defined through two entities:

- a **Content File**, which is a text file that defines the location of the data that you want to protect. Each Content File contains the fully qualified paths from the root directory to files, links, and devices to be backed up.

- a **Directive File**, which is a text file that defines where each Content File is located. The Directive File contains the fully qualified paths from the root directory to one or more Content Files. Only one Directive File is needed for a single On Demand backup.

Once these entities are defined, an On Demand Backup Set is then created. Backups run from this Backup Set will provide the facility to select the Content and Directive Files to be included.

FORMATTING CONTENT AND DIRECTIVE FILES

Content File entries should be in the following format with no filters, wildcards, or regular expressions included:

`\\client1\shares\ondemand_content\test1.txt`

`c:\data\datafile.txt`

Similarly, Directive File entries should be in the following format with no filters, wildcards, regular expressions, or blank lines:

`c:\temp\ContentFile1.txt`

CONFIGURING ON DEMAND BACKUPS

Create one or more Content Files defining the content to be backed up.

1. From the CommCell Browser, navigate to **Client Computers | <Client>.**

2. Right-click the **File System**, point to **All Tasks** and then click **New On Demand Backup Set**.

3. In the **New Backup Set Name** box, type a name (up to 32 characters).

4. Click **OK**.

Create a Directive File defining the locations of each Content File.

> Once an On Demand Backup Set has been created, it cannot be changed into a traditional backup set.
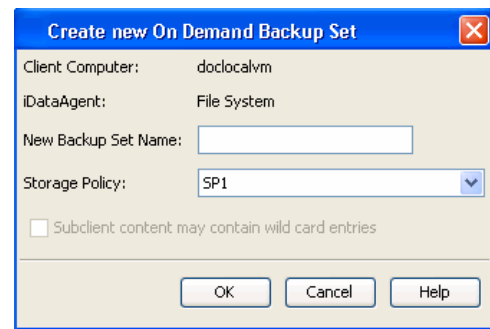
ADDING FILES AND FOLDERS WITH UNICODE CHARACTERS TO CONTENT FILES

If the path or the filename contains Unicode characters, the Content File must be converted to a format that can be used by the data protection operation. The Unicode Conversion utility must be used to convert the Content File to a format that can be provided as input.

1. Using a text editor, create a file that contains a list of files/folders with Unicode characters. Make sure to save the file as a Unicode text file.

2. From the Command Line, navigate to the *<software install folder>*/base folder and type the following:

   cvconvertunicode <source file> <destination file>

   Where:

   <source file> is the full path and name of the file created in Step 1.

   <destination file> is the full path and name of the destination file. The file will automatically be created by the utility.

3. Use the destination file as the content file to perform an On-Demand backup.

PREVENTING DUPLICATE BACKUPS OF FILES

On-Demand Backups explicitly backs up the files listed in the Content File. If the Content file has two entries for the file, the file can be backed up twice.

For example, consider a Content File that lists the following entries:

`/usr/`

`/usr/textfile`

In this scenario, a backup operation will back up the contents of all data residing in the textfile folder twice as the Content File already has the entry for the parent folder to be backed up.

It is recommended that Content Files do not include such duplicate entries. If you are not able to avoid duplicate entries, use the following steps to prevent the

duplication of data.

CONFIGURING CONTENT FILE TO EXCLUDE DUPLICATE ENTRIES

1. From the CommCell Browser, navigate to **Client Computers**.
2. Right-click the *<Client>* in which you want to add the registry key, and then click **Properties**.
3. Click the **Registry Key Settings** tab.
4. Click **Add**.
5. In the **Name** box, type `OnDemand_AutoExpandDir`.
6. In the **Location** list, type `HKEY_LOCAL_MACHINE\SOFTWARE\CommVault Systems\Galaxy\Instance<xxx>\`
7. In the **Type** list, select `REG_DWORD`.
8. In the **Value** field, type `0`.
9. Click **OK**.
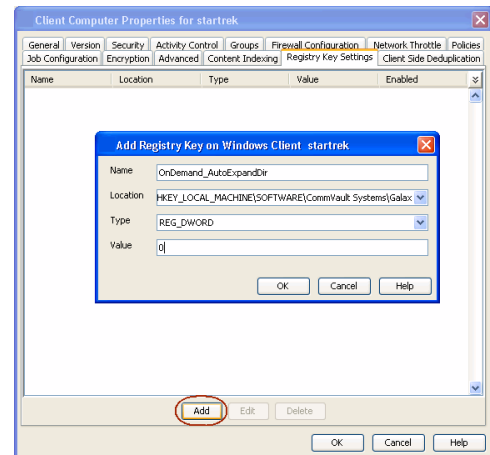
CREATING A SUBCLIENT TO BACKUP SPECIFIC FILES

You can create user defined subclient to manage and back up specific data files.

1. From the CommCell Browser, navigate to **Client Computers | *<Client>* | File System | Backup Set**.
2. Right-click the **Backup Set**, point to **All Tasks** and then click **New Subclient**.
3. In the **Subclient Name** box, type a name.
4. Click the **Storage Device** tab.
5. In the **Storage Policy** list, click a storage policy name.
6. Click the **Content** tab.
7. Click **Browse**.
8. Select the directory or file to be backed up and click **Add**.

    Repeat this step to include all the files and directories to be backed up.

    You can also select **Add Paths** and enter the paths of the directories or files to be backed up.
9. Click **Close**.
10. Click **OK**.
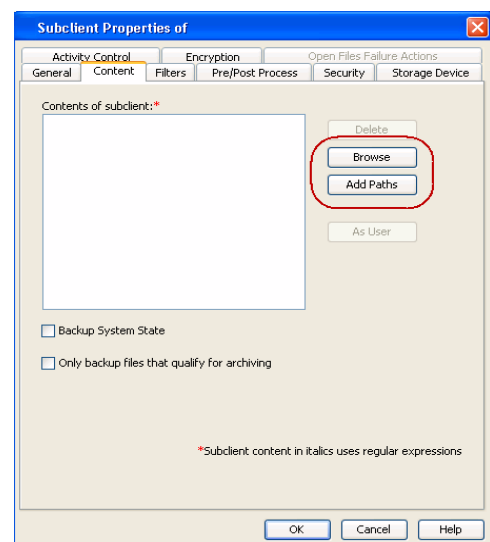
CREATING A SUBCLIENT TO BACKUP UNC PATHS

A UNC path describes the location of a volume, directory, or file. You can add UNC paths as a content in a subclient.

Before adding UNC paths as a content in a subclient, note the following:

*   If you use wildcards to define the content or filters in the same subclient that contains UNC paths, the UNC content will not get backed up.
*   Subclient content consisting of only UNC paths cannot use wildcards in contents or filters.
*   You cannot enter UNC path from a domain different than the client's domain.
*   You cannot perform multi-stream backups on a subclient whose content consists of UNC paths.

1. From the CommCell Browser, navigate to **Client Computers | *<Client>* | File System | Backup Set**.
2. Right-click the **Backup Set**, point to **All Tasks** and then click **New Subclient**.
3. In the **Subclient Name** box, type a name.
4. Click the **Storage Device** tab.
5. In the **Storage Policy** list, click a storage policy name.
6. Click the **Content** tab.

7. Click **Add Paths** and enter the UNC path of files and directories that you want to backup.

8. Click **As User** to provide user name and password required to access the UNC path.

9. Click **Close**.

10. Click **OK**.
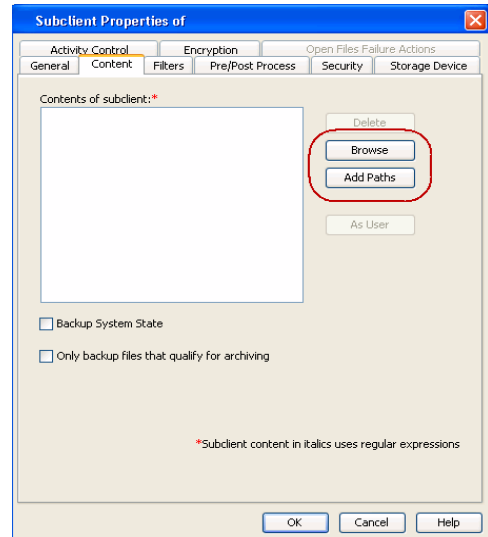
CONFIGURING THE DEFAULT SUBCLIENT FOR WILDCARD SUPPORT

You can use the wildcards to specify the content of a default subclient in any backup set. Note that you can use wildcards only in the default subclient. Hence, if you want to use wildcards to specify the pattern of files or directories as a subclient content, it is recommended to create a new backup set.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | File System | <User Defined Backup Set>**.

2. Right-click the **default** subclient in the right pane and then click **Properties**.

3. In the **Subclient Name** box, type a name.

4. Click the **Storage Device** tab.

5. In the **Storage Policy** list, select a storage policy.

6. Click the **Content** tab.

7. Click **Add Paths**.

8. Select the **Treat characters as regular expressions or wildcards** check box.

9. Enter the pattern of the directories or files to be backed up.

10. Click **OK**.

11. Click **OK**.
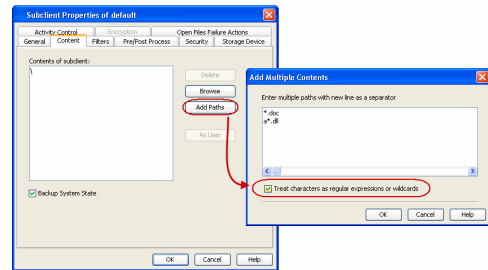
If you modified the content of a default subclient using wildcards, make sure to perform a full backup.

You can use the following wildcards for a default subclient:

WILDCARDS	DESCRIPTION	EXAMPLE
*	Any number of characters This wildcard is used in following scenarios: ● Back up all files of a specific extension ● Backup all files under a specific directory ● Backup all files of a specific extension where the file name starts with a specific pattern.	`*.doc` will backup all files with the extension `.doc` (e.g., status.doc, mission.doc) on all drives on the client computer. `C:\Test\*.doc` will backup all `.doc` files only in the `C:\Test\`directory `a*.dll` will backup all files with the extension `.dll` (e.g., `alsvc.dll, advdcc.dll`) on the client computer which have the name beginning with "a".
?	Any one character This wildcard is used in following scenarios: Backup all files (or folders) for which the name begins with a specific word and the last character of the word is variable.	`access?` will backup any folder on the C drive for which the name begins with-"access" followed by any one character such as `access1` or `access5`. However, `access12` or `access15` will not backup because the last two characters in the name are variable.
[ ]	Set of characters. You can combine this wildcard with *. If the default subclient is associated with a subclient policy and these wildcards are used in the subclient policy, then the wildcards will be treated as literal characters.	`C:\[a-m]*.doc` will backup any file with `.doc` extension on the C drive for which the name begins with the letters "a" through "m". `C:\[AEIOU]*.doc` will backup any file name that ends with `.doc` and begins with the letters `A, E, I, O, U`
[!]	The negation of a set of characters. You can use the wildcard in following scenario:	`C:\Windows\[!AEIOU]*.doc` would backup all `.doc` files in the `C:\Windows` directory that start with a letter other than A, E, I, O, or U.

	Back up all files in a directory except the files for which the name starts with any character from the specified set of characters. If the default subclient is associated with a subclient policy and these wildcards are used in the subclient policy, then the wildcards will be treated as literal characters.	
**	Any directory level.	`C:\**\move.cpp` - the file named move.cpp located at any directory level under the c: drive. (e.g., c:\info\com\move.cpp) `C:\sys*\**` - all directories starting with sys will be filtered.

CONFIGURING BACKUPS OF LOCKED FILES

Some applications and system programs lock certain files while in use (open). Files that are locked are skipped during the backup job. The Windows File System *i*DataAgent automatically attempts to obtain any skipped files in the next backup job.

CONFIGURING BACKUPS USING VSS

In some cases, it may be desirable to allow write operations on data being backed up to continue while the backup runs. Enabling VSS for backups provides this capability.

Microsoft Volume Shadow Service is the default, and only supported VSS software provider. The VSS software provider takes a snapshot of the source volume, database or file, which is then used to create backups or QR Volumes (when used with the Quick Recovery Agent).

VSS can be enabled for backups of local volumes in both clustered and non-clustered environments. VSS can be enabled only on the NTFS volumes and not on the FAT or FAT32 volumes. If the operating system fails to create a shadow copy of the data a traditional backup of the data will be performed, and a corresponding message will appear in the Event Viewer.

VSS is supported on all the Windows operating systems listed in the System Requirements, except Windows 2000. You cannot enable VSS on Windows 2000.

1. From the CommCell Console, navigate to **Client Computers | File System | Backup Set | Subclient.**

2. Right-click the subclient and click **Properties**.

3. Ensure that the **Use VSS** check box is selected.

4. Click **OK**.
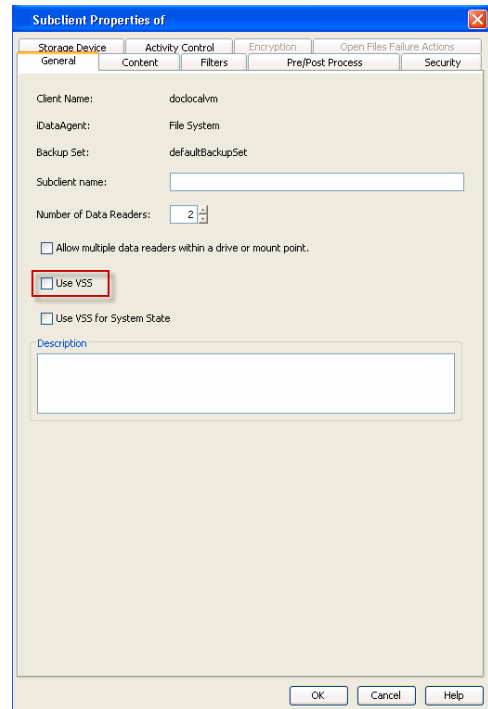
CONFIGURING BACKUPS USING QSNAP

For Windows XP clients, you can use QSnap to enable backup of mandatory locked files. Before you enable this option, install QSnap on the client. Follow the steps given below to use QSnap as a snap engine:

USING QSNAP TO BACKUP LOCKED FILES

Before you enable this option, install QSnap on the client. Follow the steps given below to use QSnap as a snap engine:

1. From the CommCell Browser, navigate to **Client Computers | <Client> | File**

System | Backupset.

2. Right-click the **<*Subclient*>** in the right pane and then click **Properties**.

3. Select **Use QSnap to handle backup of locked files.**

4. Click **OK**.
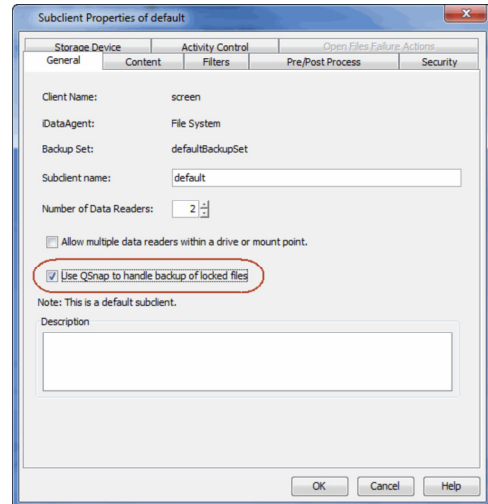
ENABLING BACKUP OF LOCKED FILES

You can ignore the file lock detection and backup the files with mandatory locks using the following steps:

1. From the CommCell Browser, navigate to **Client Computers.**

2. Right-click the <*Client*>, and then click **Properties**.

3. Click the **Registry Key Settings** tab.

4. Click **Add**.

5. In the **Name** field, type `nOverrideVSSSnapSelection`.

6. In the **Location** list, type `HKEY_LOCAL_MACHINE\SOFTWARE\CommVault Systems\Galaxy\Instance<xxx>\File System iDataAgent`.

7. In the **Type** list, select **REG_DWORD**.

8. In the **Value** field, type **1**.

9. Click **OK**.
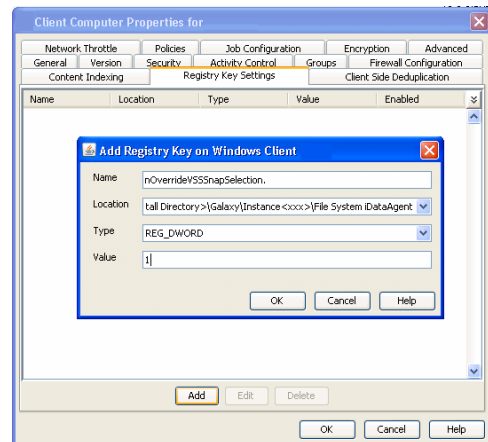
CONFIGURING SYSTEM STATE BACKUPS

By default, system state data is backed up along with file system data by the default subclient. System state data includes the following:

- System File Protection catalog and files
- Performance monitor configuration files
- Active Directory
- Quotas
- SYSVOL (if this is a domain controller)
- Certificate Services database (if this is a certificate server))
- Cluster database (if this server is part of a cluster)
- Registry
- COM+ database
- DHCP
- WINS
- IIS
- UDDI (only with Windows Server 2003 using VSS)
- Disk quota information
- Event logs
- RSM database
- WMI database

- Terminal Server Licensing database

- Content Indexing catalogs

- File Server Resource Manager (FSRM)

- Network Policy Server (NPS)

- Offline Files (only when the client computer does not have UEFI)

You can also create a separate subclient to back up the system state. Within any backup set, however, only one subclient can back up the system state. To back up System State data, the service user must be either an administrator or a backup operator. Also, system state backups require backup operator group permissions on the `HKLM\SYSTEM\SETUP` key to enable system-protected file backups.

1. In the CommCell browser, right-click the default backup set and select **New Subclient**.

2. Click the **Content** tab.

3. Select the **Backup System State** check box.

   Clear the **Backup System State** check box on the **Content** tab of the **defaultBackupSet**.

4. Click **OK**.

This subclient will be used to backup the system state. Additionally, system state data will be removed from all subsequent backups of the default subclient.

   By default, VSS will be used to perform system state backup.

   For Windows 2008, the **Use VSS for System State Backup** check box is not available. However, VSS will be used to perform the system state backup.
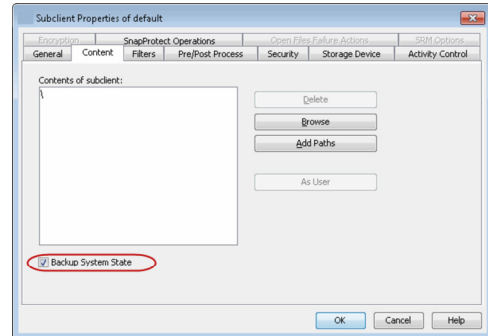
CONFIGURING BACKUP OF OFFICE COMMUNICATION SERVER (OCS)

The Office Communications Server is made up of data, settings, and metadata. OCS data and settings are backed up and restored using the OCS enabled Windows File System iDataAgent. You can perform the backup of following OCS versions:

- Live Communications Server 2005

- Office Communication Server 2007

- Office Communication Server 2007 R2

The OCS application stores its metadata in a SQL database. Use the SQL Server iDataAgent to backup and restore the OCS database that contains the OCS metadata.

The following sections describe how to include the OCS data and settings in the File System backup.

ENABLING OCS BACKUP

If you have Office Communications Server on multiple computers, you must install Windows File System iDataAgent and enable OCS backup on all servers.

Follow the steps given below to enable OCS backup using the Windows File System iDataAgent:

1. From the CommCell Console, navigate to **Client Computers**.

2. Right-click the **File System** and select **Properties**.

3. In the **General** tab of the **File System Properties** dialog box, select the **Enable Office Communication Server** Backup check box.

4. Click **OK**.
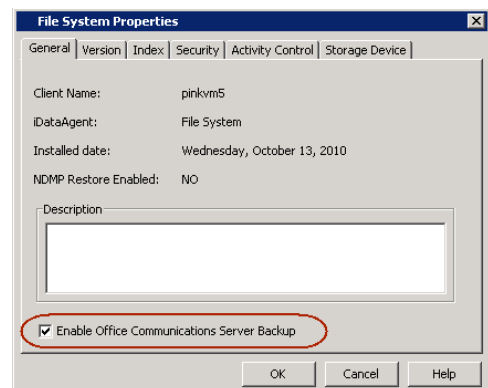
INCLUDING OCS DATA IN A SUBCLIENT

OCS data and settings can be backed up by any subclient of a Windows File System iDataAgent backup set, for which the OCS backup is enabled. Within a backup set, only one subclient can back up the OCS data and settings. The OCS data and settings is always backed up in full irrespective of the backup type selected for the subclient that includes the OCS.

Follow the steps given below to include the OCS data and settings in a subclient:

1. From the CommCell Console, navigate to **Client Computers | File System | Backupset**.

2. Right-click the subclient in the right pane and select **Properties**.

3. In the the **Subclient Properties** dialog box, click **Content**

4. On the Content tab, select the Backup Communication Server check box.

5. If the OCS credentials, displayed on the **Content** tab, are incorrect, click **Edit**.

6. Enter the credentials for **Office Communication Server**.

7. Click **OK** on the **Office Communication Server Credentials** dialog box.

8. Click **OK** on the **Subclient Properties** dialog box.
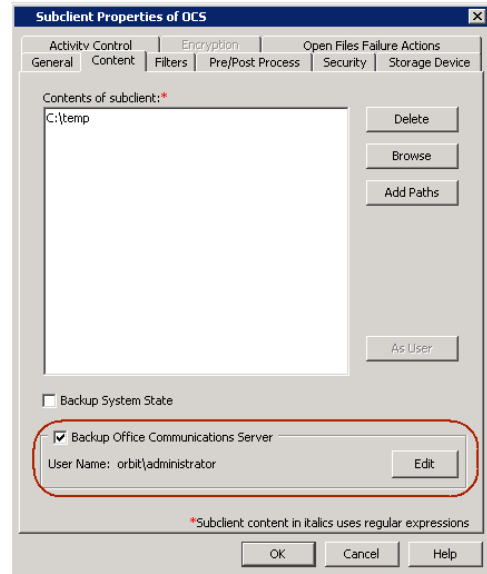
CONFIGURING FILTERS FOR BACKUPS

Prior to backups, you can set filters to prevent specific type of files from being backed up. Filters can also be used to exclude certain system-related files and database application files which consistently fail during a backup operation and are not integral to the operation of the system or application.

See Content, Filters, and Regular Expressions for comprehensive information on filtering data from backup.

FILTERING FILES FROM A BACKUP

Subclient-level backup filters are available for the File System *i*DataAgent to exclude specified directories and files from being backed up. Follow the steps given below to configure filters on a subclient:

1. From the CommCell Browser, navigate to **Client Computers | <*Client*> | File System | Backup Set**.

2. Right-click the **Subclient** in the right pane and then click **Properties**.

3. Click the **Filters** tab.

4. Under **Exclude these files/folders/patterns,** click **Browse.**

5. Click the file, folder, or directory that you want to exclude from backup operations and click **Add**.

6. Optionally, click **Add** under **Exclude these files/folders/patterns** and type the path to files and folders that you want to exclude. You can also enter patterns of files or folders using wild cards.

   You cannot enter Escape sequence to specify the path or file name.

7. Click **Close**.

8. Click **OK**.

Ensure that the subclient content does not have any UNC paths. The data from a UNC path will not get backed up if you are using wildcards in a subclient content. You can create another subclient to backup the UNC paths.
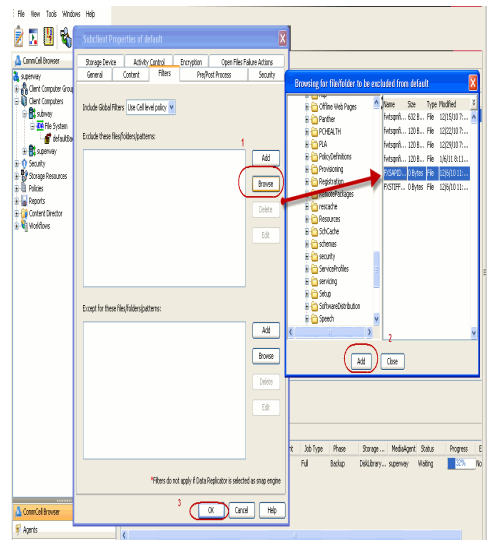
SUPPORTED WILDCARDS

You can use the following wildcards to specify the pattern of files as a filter.

WILDCARD	DEFINITION	EXAMPLE
*	Any number of characters. This wildcard is used in following scenarios: ● filter all files of a specific extension ● filter all files when the file name starts with a specific pattern	`C:\*.log` will filter all files with the .log extension on root of the C drive. If you want to filter files with the `.log` extension from a folder on the C drive, you must include the path to the folder in the filter. (e.g. `C:\Test\*.log`) `ntuser*` will filter all files for which the file name starts with the word `ntuser`.

?	Any one character	To filter files:
	This wildcard is used in following scenarios: Filter all files (or folders) for which the name begins with a specific word and the last character of the word is variable.	`C:\access?.doc` will filter any files with the extension .doc on the C drive for which the name begins with- `"access"` followed by any one character such as `access1.doc` or `access5.doc`. However, `access12.doc` or `access15.doc` will not be filtered because the last two characters in the name are variable. To filter folders: `C:\access?\**\*` will filter any on the C drive for which the name begins with- `"access"` followed by any one character such as `C:\access1` or `C:\access`5. However, `C:\access12` or `C:\access15` will not be filtered because the last two characters in the name are variable.
***	All files under a specific directory	`C:\Test\Data\**\*` will filter all files and subdirectories under and including `C:\Test\Data` `C:\**\Data\**\*` will filter all files and subdirectories below and including any directory called "Data" at any level in the C: volume `G:\Users\**\xpprofile\*.log` will filter all files with the .log extension from any `xpprofile` subdirectory under `Users` directory `G:\Users\**\xpprofile\ntuser*` will filter all filenames starting with `ntuser` from any `xpprofile` subdirectory under `Users` directory

FILTERING SYSTEM STATE COMPONENTS FROM A BACKUP

By default, the system state is backed up along with file system data by the default subclient of a Backup Set. A system state backup is always a full backup whether you select full, incremental, or differential backup for the subclient that includes the system state. You can, however, filter out some components from system state backup.

1. From the CommCell Console, navigate to **Client Computers | File System | Backup set**.
2. Right-click the **subclient** in the right pane and click **Properties**.
3. Click the **Filters** tab.
4. Click **Add** from the **Exclude these files/folders/patterns** group.
5. Enter the path within curly brackets. Following are the entries that can be made:
   - {System Protected Files}
   - {IIS}
   - {COM+ Database}
   - {Event Logs}
   - {One Touch Files}
   - {RSM}
   - {Terminal Services Licensing}
   - {Disk Quotas}
   - {Content Indexing Catalogs}
   - {WMI Database}
   - {DHCP}
   - {WINS}
   - {UDDI Database}
   - {Remote Storage Database}
   - {Certificate Services }
   - {Offline Files}
   - {Active Directory Application Mode}
   - {File Server Resource Manager}
   - {NPS Database}
6. Click **Add**.
7. Click **OK** to save your changes.
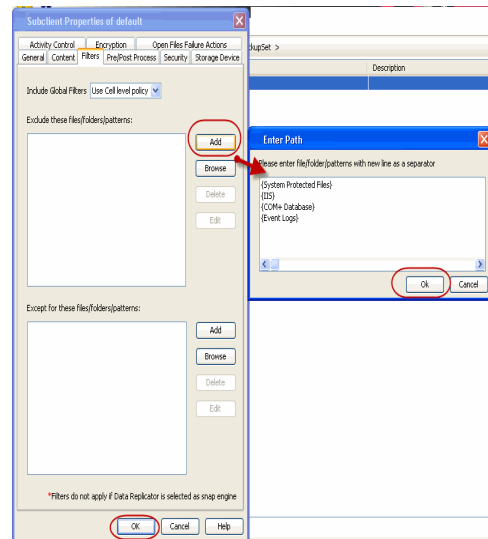
CONFIGURING EXCLUSIONS TO FILTERS

Once you set the filters, you can also provide exceptions for the filters. The files or folders added to the exception list will be included in the backup operations. For example, if you want to exclude from your back up operation all the files in the /Ops directory except the Maintenance file. You can add a subclient filter to exclude the /Ops directory from being backed up and also provide an exception to allow the Maintenance file to be backed up.

1. From the CommCell Browser, navigate to **Client Computers | <*Client*> | File System | Backup set**.

2. Right-click the **<*Subclient*>** in the right pane and click **Properties**.

3. Click the **Filters** tab.

4. Under **Except for these files/folders/patterns,** click **Browse.**

5. Click the file, folder, or directory that you want to include in the backups and then click **Add**.

6. Click **Close.**

7. Click **OK**.
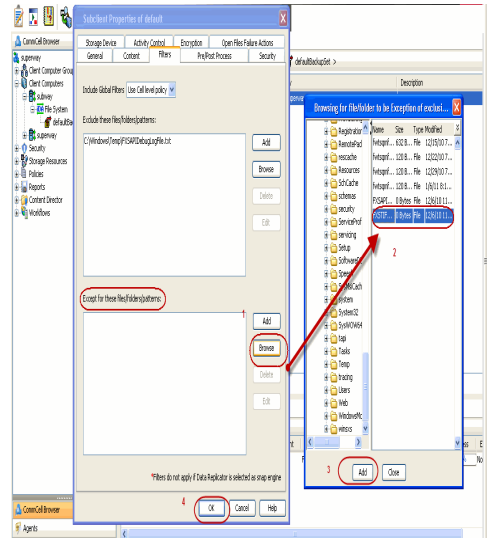
EXCLUDING COMMCELL CONSOLE DIRECTORIES

Software Installation, Index Cache, Job Control, and Job Results directories are by default included in the backups performed by the Windows File System iDataAgent. To exclude them from data protection operations follow the steps given below:

1. From the CommCell Browser, navigate to **Client Computers**.

2. Right-click the <*Client*>, and then click **Properties**.

3. Click the **Registry Key Settings** tab.

4. Click **Add**.

5. In the **Name** field, type `nFilterGalaxyDirectories`.

6. In the **Location** list, type `HKEY_LOCAL_MACHINE\SOFTWARE\CommVault Systems\Galaxy\Instance<xxx>\`.

7. In the **Type** list, select Reg_ DWORD.

8. In the **Value** field, type 1.

9. Click **OK**.
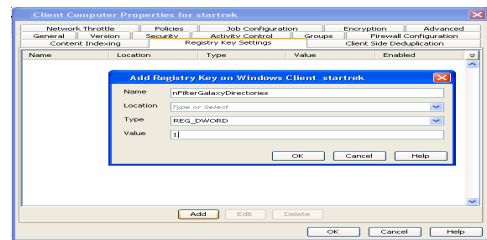
DELETING A FILTER

You can remove a filter by deleting it from the exclusion list.

1. From the CommCell Browser, navigate to **Client Computers | <*Client*> | File System | Backup set**.

2. Right-click the **<*Subclient*>** in the right pane, and then click **Properties**.

3. Click the **Filters** tab.

4. Under **Exclude these files/folders/patterns,** select the filter that you want to delete.

5. Click **Delete**.

6. Click **OK.**
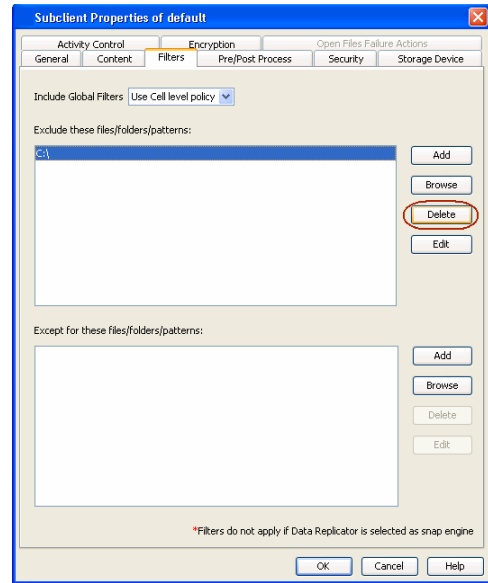
CONFIGURING THE SCAN METHOD FOR DETECTING CHANGED FILES

You can use one of the following scan methods to determine which files in a backup set have changed and/or have been backed up.

CONFIGURING CHANGE JOURNAL SCAN

Change Journal is selected as the default method for scanning files to determine which files have changed and/or have been backed up. When using this method of scanning the incremental backup will backup all the new or changed data since the last incremental or full backup, ignoring any differential backups performed prior to the current backup.

1. From the CommCell Console, navigate to **Client Computers | File System**.
2. Right-click the **File System | Backup set**
3. Right-click **Backup set** and click **Properties**.
4. Select **Use Change Journal**.
5. Click **OK**.
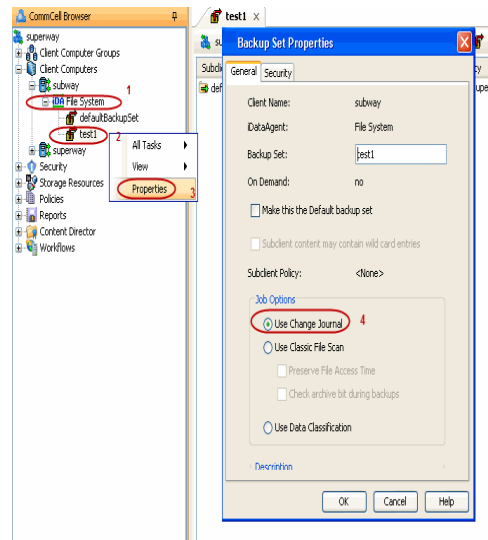
CONFIGURING CLASSIC FILE SCAN

There are some instances in which the Classic File Scan is always used, including but not limited to:

- When backing up FAT Volumes.
- When files or file level wildcards are used to define subclient content.

Follow the steps given below to configure Classic File Scan:

1. From the CommCell Console, navigate to **Client Computers | File System**.
2. Right-click the **File System | Backup set**
3. Right-click **Backup set** and click **Properties**.

4. Select **Use Classic File Scan**.

5. Select **Preserve File Access Time**.

6. Select **Check archive bit during backups**.

7. Click **OK**.
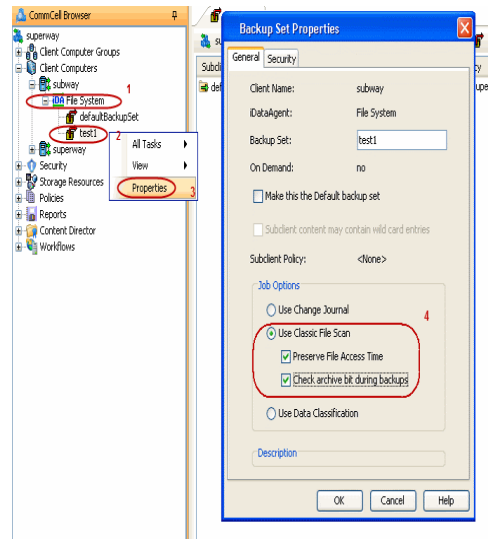
CONFIGURING DATA CLASSIFICATION SCAN

By default Change Journal Scan is selected as the method for scanning files to determine which files have changed and/or have been backed up. However, you can also select Data Classification as the preferred method of scanning the files, as this method is much faster as compared to the Classic File Scan.

Before selecting Data Classification as the scan method, consider the following:

● Use Data Classification for NTFS volumes but not for the FAT volumes.

● If the subclient content has any mount points, the Classic File scan method will be used automatically even if you select the Data Classification as the scan method.

1. From the CommCell Console, navigate to **<Client> | <Agent> | defaultBackupSet**.

2. Right-click the **defaultBackupSet** and select **Properties**.

3. Click **Use Data Classification**.

4. Click **OK** to enable the data classification.
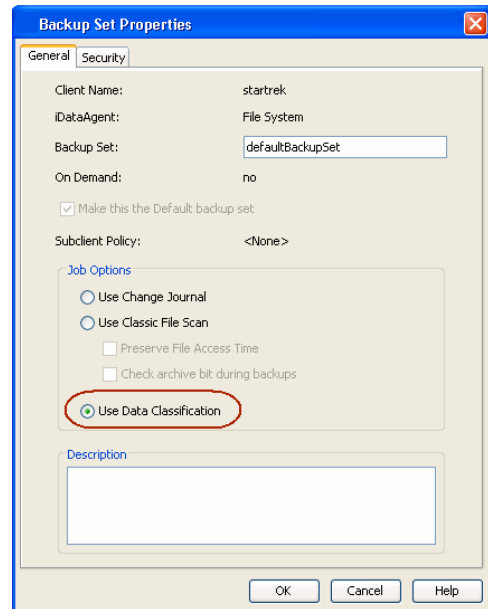
CONFIGURING MULTIPLE STREAMS FOR BACKUPS

File System Multi-Streaming employs multiple data streams per subclient for data protection operations. This enables the subclient's contents to be distributed to all the streams, transmitting them in parallel to the storage media. Hence a subclient whose data is secured using three data streams, utilizes more of the available network resources, and can complete in as little as one third the time that the same data would require using a single stream. You can allocate a maximum of 63 streams for a subclient.

Note that, you do not have to enable multi-streaming if you have multiple mount points pointing to the same physical drive. Do not use multiple streams if you have added UNC paths to the subclient content.

Before enabling multi streaming, ensure that you can use multi-streaming when you restore the data and create an auxiliary copy.

Follow the steps given below to configure multi-streaming.

1. From the CommCell Browser, navigate to **Client Computers | <*Client*> | File System | Backup Set**.

2. Right-click the **<*Subclient*>** in the right pane and click **Properties**.

3. In the **Number of Data Readers** box type or select the number of data streams.

4. Select the **Allow multiple data readers within a drive or mount point** checkbox.

5. Click the **Storage Device** tab.

6. In the **Storage Policy** list, click a storage policy name.

7. Click **OK**.

    The number of streams configured in the Storage Policy should be equal to, or greater than the specified **Number of Data Readers** .
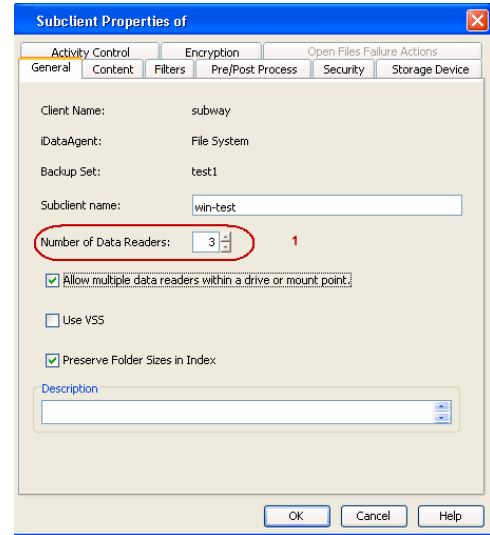
CONFIGURING PRE/POST PROCESSING FOR BACKUPS

The following sections provide the steps to configure pre/post scripts for backup operations. For additional information, see Pre/Post Process.

SETTING UP PRE/POST PROCESSES

You can add and modify Pre/Post processes for a subclient. These are batch files or shell scripts that you can run before or after certain job phases. For example, you can use an `echo` command to check the level of a backup. Similarly, you can include a `case` statement within a script to run specific operations based on the level of the backup job.

A **Save As Script** file can also be run as a pre/post process, if you include the absolute path of the associated input file in the script file.

1. From the CommCell Browser, navigate to **Client Computers | <*Client*> | File System | BackupSet.**

2. Right-click the **<*Subclient*>** in the right pane, and then click **Properties**.

3. Click the **Pre/Post Process** tab.

4. Depending on the process you want to set up, click the corresponding **Browse** button.

5. Select the process and then click **OK**.
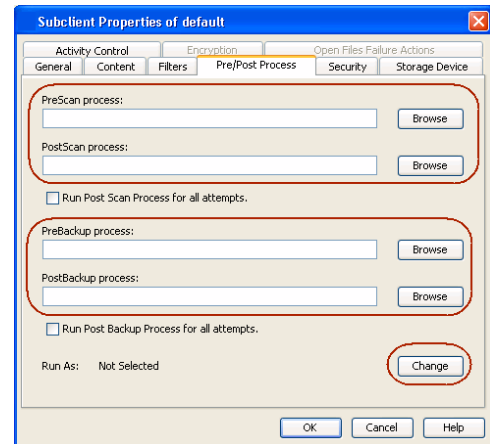
SETTING UP POST PROCESSES TO RUN DURING FAILURES

By default, a specified post process command is executed only on successful completion of the scan or backup operation or if the job is killed.

Use the following steps to run a post process even if the scan or backup operation did not complete successfully. For example, this may be useful to bring a database online or release a snapshot.

1. From the CommCell Browser, navigate to **Client Computers | <*Client*> | File System | BackupSet.**

2. Right-click the **<*Subclient*>** in the right pane, and then click **Properties**.

3. Click the **Pre/Post Process** tab.

4. Select the **Run Post Scan Process for all attempts** check box.

5. Select the **Run Post Backup Process for all attempts** check box.

6. Click **OK.**
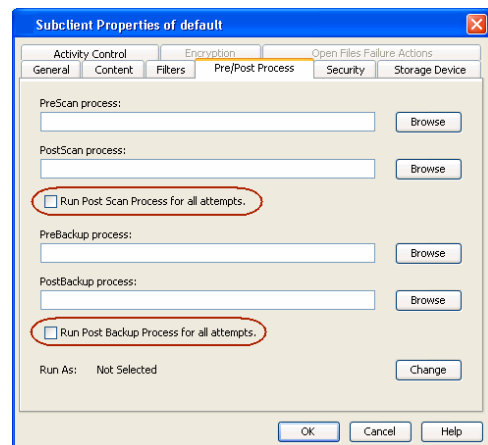
CONFIGURING USER ACCOUNTS

Users performing backups must be either an administrator or a backup operators. Backup operators (or Service Users) are designed to have full control to the registry and the install folder.

An administrator or a backup operator in a local group can back up any file and folder on the local computer to which the local group applies. An administrator or backup operator on a domain controller can back up any file and folder on any computer in the domain or any computer in a domain where a two-way trust relationship exists.

To back up files if you are not an administrator or a backup operator, you must be the owner of the files and folders you want to back up or have one or more of the following permissions for the files and folders you want to back up:

● Read

● Read and execute

● Modify

● Full Control

Users can be configured at the server and domain control levels to perform backups using the following procedures:

CONFIGURING WINDOWS USERS ON AN INDIVIDUAL SERVER

To add a user to the Backup Operators Group, perform the following steps on an individual server:

1. Navigate to **Start** | **Settings** | **Control Panel** | **Administrative Tools**.

2. Double-click **Computer Management**.

3. Navigate to **Local User and Groups** | **Users**.

4. Right-click the user who will be performing backups and click **Member of**.

5. Add the **Backup Operators** group to the User.

6. Click **OK**.

7. Log off and log in as the domain controller **Administrator** for the policies to take effect.

CONFIGURING WINDOWS USERS ON A DOMAIN CONTROLLER

To add a user to the Backup Operators Group, perform the following steps on the domain controller:

1. Create or prepare to manage a Windows user who will run the services.

2. Navigate to **Active Directory Users** | **Computers** | **Users**.

3. Right-click the user who will be performing backups and click **Member of**.

4. Add the **Backup Operators** group to the User.

5. Click **OK**.

6. Log off and log in as the domain controller **Administrator** for the policies to take effect.

CONFIGURING WINDOWS USERS FOR SPECIFIC FOLDERS

1. Right-click the folder to be backed up and select **Properties**.

2. Select the **Security tab**

3. Enable **Add Backup Operators** with full control rights.

4. Click **OK**.

CONFIGURING CREDENTIALS FOR UNC PATH CONTENT

You can define from the subclient level an account to be used when configuring a UNC Path as part of the subclient's content.

The user name and password that you use must have sufficient rights to access the share to which the UNC Path is pointing. Also, the user name and password must have the right to log on to the client machine that is running the backup, as well as rights to the logs on that computer.

To perform a backup or a restore operation using a UNC Path as either the content of the subclient or the destination for a restore, we recommend using an account that has administrative privileges. Also, the User Account that is used must be an account that already exists. If you choose to use an account that does not exist, it must be created.

Once you establish the account, you can modify the account. See Change Account for Configuring UNC Paths for step-by-step instructions.

1. From the CommCell Browser, right-click the **Subclient** and click **Properties.**

2. From the **Content** tab, type in the UNC path of the share that you want to add in the **Enter New Content** field and click **Add**.

   Repeat this step if you want to add more files and/or folders to the content.

3. Click **As User**.

4. Enter the appropriate user name and password.

5. Click **OK**.

CONFIGURING CREDENTIALS FOR RESTRICTED DRIVES OR DIRECTORIES

You can define a user or an account with permissions to restore data to either mapped/shared network drives or directories to which you have no write privileges.

1. From the CommCell Browser, right-click **File System,** click **All Tasks**, and then click **Browse and Restore**.

2. From the **Restore Options** dialog box, click **Advanced**.

3. Select **Impersonate Windows User**.

4. Enter the appropriate user name and password.

5. Click **OK** to save the settings.

CONFIGURING INDEX FOR BACKUPS

CREATING A NEW INDEX ON A FULL BACKUP

This option accelerates Full or On Demand backups and is enabled by default. Subsequently, when you perform a browse and restore operation, the default browse displays data up to the most recent full backup. To browse and restore older data you have to use the options to browse before or between specific dates.

When disabled, Full or On Demand backups may be slower. However, the default browse displays all data in the entire retention period; not just one full backup cycle.

Use the following steps to configure this option for all subclients. This option can also be set for the individual backups when initiating the job.

1. From the CommCell Browser, navigate to **Client Computers | <Client>**.

2. Right-click the **File System** on the right pane, and then click **Properties**.

3. Click the **Index** tab.

4. Select the **Create new index on Full Backup** check box.

5. Click **OK**.
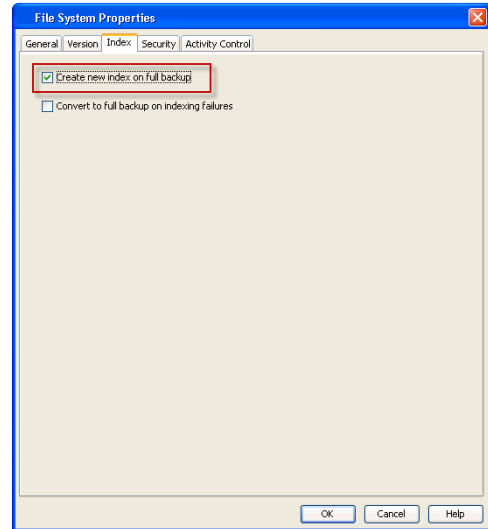
CONVERTING TO A FULL BACKUP ON INDEXING FAILURES

Use this option to ensure that the backup does not fail if the index is irretrievable. When disabled, the backup will fail if the index is irretrievable.

1. From the CommCell Browser, navigate to **Client Computers | <Client>**.
2. Right-click the **File System** on the right pane, and then click **Properties**.
3. Click the **Index** tab.
4. Select the **Convert to full backup on indexing failures** check box.
5. Click **OK**.
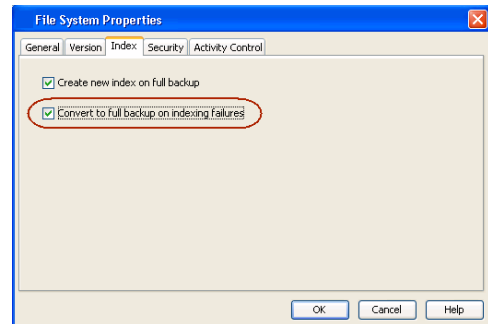
COMMAND LINE OPERATIONS

You can add, modify or delete several configurable properties for the File System *i*DataAgent from command line.

Command line configuration enables you to:

● configure the same properties across multiple clients simultaneously.
● reuse the same configurations for additional entities.

The following sections describe the available command line configurations:

LOG ON TO THE COMMSERVE

To run command line operations you must first login to the CommServe as follows:

● From Command prompt, navigate to <Software_Installation_Directory>/Base and run the following command:

```
qlogin -cs <commserve name> -u <user name>
```

● For example, to log on to CommServe 'server1' with username 'user1':

```
qlogin -cs server1 -u user1
```

CONFIGURE SUBCLIENTS

CREATE SUBCLIENT

1. Download the create_subclient_template.xml file and save it on the computer from where the command will be executed.
2. Execute the following command from the <Software_Installation_Directory>/Base folder after substituting the parameter values.

```
qoperation execute -af create_subclient_template.xml -appName 'File System' -clientName xxxxx -backupsetName xxxxx -
subclientName xxxxx -contentOperationType ADD -content/path 'xxxxx'
```

GET SUBCLIENT PROPERTIES

1. Download the get_subclient_properties_template.xml file and save it on the computer from where the command will be executed.

2. Execute the following command from the <Software_Installation_Directory>/Base folder after substituting the parameter values.

   ```
   qoperation execute -af get_subclient_properties_template.xml -appName 'File System' -clientName xxxxx -backupsetName
   xxxxx -subclientName xxxxx
   ```

MODIFY SUBCLIENT

1. Download the update_subclient_add_template.xml file and save it on the computer from where the command will be executed.

2. Execute the following command from the <Software_Installation_Directory>/Base folder after substituting the parameter values.

   ```
   qoperation execute -af update_subclient_add_template.xml -appName 'File System' -clientName xxxxx -backupsetName xxxxx
   -subclientName xxxxx -contentOperationType xxxxx -content/path 'xxxxx'
   ```

RENAMING A SUBCLIENT

1. Download the update_subclient_add_template.xml file and save it on the computer from where the command will be executed.

2. Execute the following command from the <Software_Installation_Directory>/Base folder after substituting the parameter values.

   ```
   qoperation execute -af update_subclient_add_template.xml -appName 'File System' -clientName xxxxx -backupSetName xxxxx
   -subclientName xxxxx -newName xxxxx
   ```

DELETE SUBCLIENT

1. Download the delete_subclient_template.xml file and save it on the computer from where the command will be executed.

2. Execute the following command from the <Software_Installation_Directory>/Base folder after substituting the parameter values.

   ```
   qoperation execute -af delete_subclient_template.xml -appName 'File System' -clientName xxxxx -backupsetName xxxxx -
   subclientName xxxxx
   ```

AVAILABLE PARAMETERS FOR SUBCLIENTS

The following table displays all the parameters you can use with the commands mentioned in the above sections. To add a parameter to your command, use the following syntax: (Some examples are provided at the end of the table.)

```
qoperation execute -af <template XML file> -<parameter name> <value>
```

PARAMETER	DESCRIPTION OF PARAMETER VALUES
clientName	Name of the client computer.
backupsetname	Name of the backup set. If the backup set name is not specified in the command query, the default backup set is used by default.
appName	Name of the application. In this case it would be 'File System'.
subclientname	Name of the subclient.
newName	New name of the subclient.
enableBackup	Option to enable/disable backup. Valid values are True/False.
encryptionFlag	Option to set the encryption points during backups. Valid values are: ● ENC_MEDIA_ONLY, to encrypt the backup data after transmission and prior to storage on the media. ● ENC_NETWORK_AND_MEDIA, to encrypt the backup data before transmission. The data is stored encrypted on the media. ● ENC_NETWORK_ONLY, to encrypt the backup data for transmission and then decrypt the data prior to storage on the media. ● ENC_NONE, to disable data encryption.
networkAgents	Number of Network Agents.
softwareCompression	Option to enable compression on the Client or MediaAgent computer. Valid values are: ● ON_CLIENT, to enable software compression on the client. ● ON_MEDIAAGENT, to enable software compression on the MediaAgent. ● OFF, to disable software compression.
throttleNetworkBandwidth	Enhancing backup performance by reducing network bandwidth overhead. Valid values are 0/1.
enableDeduplication	Option to enable deduplication on subclient. Valid values are True/False.
generateSignature	A component of deduplication performed on the client or MediaAgent computer. Valid values are: ● ON_CLIENT, to enable signature generation on the client. ● ON_MEDIA_AGENT, to enable signature generation on the MediaAgent. ● OFF, to disable signature generation.
storagePolicyName	Name of the Storage Policy to be associated for backup.

useGlobalFilters	Option to enable the use of global filters. Valid values are: • ON, to enable global filters for the subclient. • USE_CELL_LEVEL_POLICY, to enable the use of global filters if the **Use Global Filters on All Subclients** option is enabled on the Control Panel (Global Filters) dialog. If the option is disabled, USE_CELL_LEVEL_POLICY will disable global filters for the subclient. • OFF, to disable global filters.
useVSS	Option to enable/disable VSS for backing up the file system data. Valid values are True/False.
useVSSForSystemState	Option to enable/disable VSS for backing up the system state. Valid values are True/False.
backupSystemState	Option to enable/disable back up of the system state. Valid values are True/False.
postBackupCommand	Path to the post process script that will be run after the backup.
postScanCommand	Path to the post process script that will be run after the scan phase
preBackupCommand	Path to the pre process script that will be run before the backup.
preScanCommand	Path to the pre process script that will be run before the scan phase
runAs	Option to specify the user name who has permissions to run the pre/post process scripts. Valid values are: • USE_IMPERSONATION, to specify a user with enough privileges to run the scripts. When using this value, you also need to provide the user credentials: `-prepostUserName/userName <user name> -prepostUserName/password <password>` • USE_LOCAL_SYS_ADMIN, to use the administrator account to run the scripts.
content/path	Location of the content to be backed up. This parameter must be used along with the contentOperationType parameter, for example: `-contentOperationType <value> -content/path '<path value>'`
content/excludepath	Location of the content to be excluded from backup. This parameter must be used along with the contentOperationType parameter, for example: `-contentOperationType <value> -content/excludepath '<path value>'`
content/includepath	Location of the content to be included in the backup from the excluded list. This parameter must be used along with the contentOperationType parameter, for example: `-contentOperationType <value> -content/includepath '<path value>'`
contentOperationType	Modification type. Valid values are • ADD, to add content to the subclient • OVERWRITE, to overwrite contents to the subclient. • DELETE, to delete the contents from the subclient.

The following examples show how to add a parameter for a command:

Adding Content	To update the location for the subclient content, add the 'path' parameter to the following command: `qoperation execute -af update_subclient_add_template.xml -appName 'File System' -clientName client1 -backupSetName backupset1 -subclientName subclient1 -contentOperationType ADD -content/path '/etc'`
Setting a Storage Policy	To assign a storage policy to a subclient, add the 'storagePolicyName' parameter to the following command: `qoperation execute -af update_subclient_add_template.xml -appName 'File System' -clientName client1 -backupSetName backupset1 -subclientName subclient1 -storagePolicyName sp1`

For detailed information on the Subclient parameters see Subclient Properties.

LIST SCHEDULE POLICY ASSOCIATION

1. Download the sched_policy_association_template.xml file and save it on the computer from where the command will be executed.

2. Execute the following command from the <Software_Installation_Directory>/Base folder after substituting the parameter values.

   `qoperation execute –af sched_policy_association_template.xml –taskName mypolicy`

PARAMETER	DESCRIPTION OF PARAMETER VALUES
taskName	Name of the Schedule Policy to be associated.

CONFIGURING FOLDER SIZE FOR BACKUPS

You can use the **Show Folder Size** option to get a graphical representation of the space used by backed up data on a client. This can be done for each subclient for a given client. The graph gets refreshed every time a backup is run for the change in data. To use this option, you must enable SRM for a given client and run a Full Backup.

1. Enable SRM
   ○ From the CommCell Browser, right-click the File System

*i*DataAgent and select **Properties**.

○ Click **Enable SRM Feature** from the **General** tab.

○ Click **OK**.

2. Run a Backup

○ Right-click the subclient, and click **Backup** in the CommCell Browser.

○ Click **Full** as backup type and then click **Immediate**.

○ Click **OK**.

3. Show Folder Size

○ From the CommCell Browser, navigate to **Client Computers | <Client> | File System | defaultBackupSet**.

○ Right-click the subclient for which you want to display folder size information and click **Show Folder Size**.

○ Chart displaying the folder size of the backed up data will be displayed.
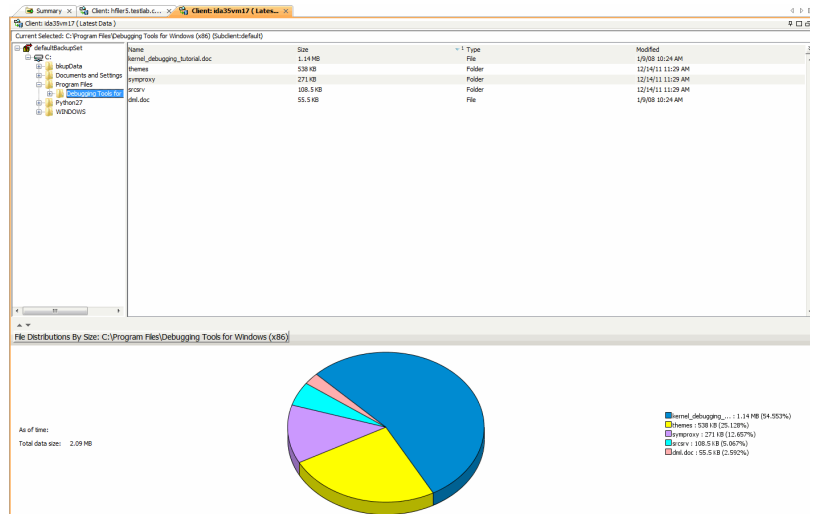
MODIFYING AN AGENT, BACKUP SET OR SUBCLIENT

The following table describes the properties that can configured from the agent, backup set and subclient levels.

OPTION	DESCRIPTION	RELATED TOPICS
Preserving the File Access Time	This option allows you to prevent the file access time from being changed as a result of running data protection operations on the client. When this option is selected, the file access time will be preserved. 1. From the CommCell Browser, right-click the backup set, and then click **Properties.** 2. Select the **Preserve File Access Time** check box. 3. Click **OK**.	
Change Storage Policies	You can modify the storage policies in any of the following situations: ● To include a different media for the backup operation. ● To use a storage policy with a different retention criteria. You can change the storage policies from the subclient level. 1. From the CommCell Browser, right-click the subclient. 2. Click **Properties**. 3. Click **Storage Device**. 4. Select the **Storage policy** from the drop-down menu. 5. Click **OK**.	Refer to Storage Policies.
Rename a Backup Set or Subclient	You can rename backup sets and subclients. Renaming BackupSet: 1. From the CommCell Bowser, navigate to **Client Computers	<Client>	File System**. 2. Right-click the **<Backup Set>**, and then click **Properties.** 3. In the **Backup Set** box, type a name. 4. Click **OK**. Renaming subclient: 1. From the CommCell Browser, navigate to **Client Computers	<Client>	File System	<Backup Set>**. 2. Right-click the **<user-defined Subclient>**, and then click **Properties.** 3. In the **Storage Policy** list, click a storage policy name. 4. Click **OK**.	
Data Transfer Options	You can efficiently configure the available resources for transferring data secured by data protection operations from the subclient level. This includes the following: ● Enable or disable **Data Compression** either on the client or the MediaAgent. ● Configure the transfer of data in the network using the options for **Network Bandwidth Throttling** and **Network Agents**. You can configure the data transfer options. 1. From the CommCell Browser, navigate to **Client Computers	<Client>	File System	BackupSet.**	Refer to Data Compression and Network Bandwidth Throttling.

	2. Right-click the *<Subclient>* in the right pane, and then click **Properties**.	
	3. Click the **Storage Device** tab**.**	
	4. Click the **Data Transfer Option** tab.	
	5. Choose the appropriate software compression option for this subclient.	
	6. Select the **Throttle Network Bandwidth** check box, and set the required bandwidth.	
	7. Click **OK.**	
View Data Paths	You can view the data paths associated with the primary storage policy copy of the selected storage policy or incremental storage policy. You can also modify the data paths including their priority from the subclient level. 1. From the CommCell Browser, navigate to **Client Computers	*<Client>*	File System	BackupSet.** 2. Right-click the *<Subclient>* in the right pane, and then click **Properties**. 3. Click the **Storage Device** tab**.** 4. In the **Storage Policy** list, click a storage policy name. 5. Click **Data Paths**.	
Configure Activity Control	You can enable backup and restore operations from the agent and subclient level. However, you can enable restore operations only from the agent level. 1. From the CommCell Browser, navigate to **Client Computers**	*<Client>* 2. Right-click the *<Client>* or *<Subclient>* in the right pane, and then click **Properties**. 3. Click the **Activity Control** tab and select or clear option(s) as desired. 4. Click **OK.**	Refer to Activity Control.
Configure User Security	You can configure user security from the agent or subclient level. You can perform the following functions: ● Identify the user groups to which this CommCell object is associated. ● Associate this object with a user group. ● Disassociate this object from a user group. 1. From the CommCell browser, right-click the subclient. 2. Click **Properties.** 3. Click **Security**. 4. Select the appropriate user groups to which you want to associate to the CommCell object from the **Available Groups** pane, and then move the user group to the **Associated Groups** pane. 5. Click **OK**.	Refer to User Administration and Security.
Enable/Disable Data Encryption	You can enable data encryption from the suclient level.Encryption must be enabled at the client level prior to configuring any instances residing on that client. 1. From the CommCell browser, right-click the subclient. 2. Click **Properties.** 3. Click **Encryption.** 4. Select the desired encryption. 5. Click **OK**.	Refer to Data Encryption.
View Software Version and Installed Updates	The **Version** tab, at the Agent level displays the software version and post-release service packs and updates installed for the component. 1. From the CommCell browser, right-click the agent. 2. Click **Properties**. 3. Click **Version.** 4. Click **OK.**	
CommCell Configuration Report	The CommCell Configuration Report provides the properties of the CommServe, MediaAgents, clients, agents, SRM agents, subclients, and storage policies within the CommCell based on the selected filter criteria. 1. From the CommCell Browser, double-click **Reports** icon. 2. Select **CommCell Configuration**. 3. Click **Run**.	Refer to CommCell Configuration.

DELETING AN AGENT,BACKUPSET OR SUBCLIENT

The following sections describe the steps involved in deleting an agent, archive set or subclient.

When you delete an instance or backupset, the associated data is logically deleted and you can no longer access the corresponding data from CommCell Console for recovery purposes.

Refer to the troubleshooting article on Recovering Data Associated with Deleted Clients and Storage Policies for information on how to recover data if you accidentally delete an entity.

DELETING AN AGENT

You need to uninstall or DeConfigure the agent software from the client computer before deleting from CommCell Browser. After you delete the client software, you can either leave the corresponding data intact for appropriate action or you can remove the data immediately. If you choose to remove the data immediately, you must delete the agent from the CommCell Browser. If you delete the agent, all of the agent's data is irretrievably lost.

● You cannot delete an agent while operations for that agent are running.

1. From the CommCell Browser, navigate to **Client Computers | <Client>**.

2. Right-click the **<Agent>**, and then click **Delete**.

3. A confirmation message is displayed with the following message:

   This operation will permanently delete the data backed up from this level and it cannot be restored.

4. Click **OK** to continue with the deletion operation., or click **No** to abort the deletion.

DELETING A BACKUPSET

Consider the following before deleting a Backup Set:

● You cannot delete a default Backup Set.

● Schedules associated with the Backup Set are also automatically deleted.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | <Agent>.**

2. Right-click the **<Backup Set>**, and then click **Delete**.

3. A confirmation message is displayed, asking if you want to delete the Backup Set.

   Click **No** to cancel the deletion and retain the Backupset, or click **Yes** to continue the deletion.

DELETING A SUBCLIENT

Consider the following before deleting a subclient:

● You cannot delete a default subclient.

● Schedules associated with the subclient are also automatically deleted.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | <Agent> | <Backup Set>.**

2. Right-click the **<subclient>** that you want to delete, and then click **Delete**.

3. A confirmation message is displayed, asking if you want to delete the subclient.

   Click **No** to cancel the deletion and retain the subclient, or click **Yes** to continue the deletion.

Back to Top

Advanced – Windows File System Backup

TABLE OF CONTENTS

FULL BACKUP

Full backups provide the most comprehensive protection of data.

1. From the CommCell Browser, navigate to **<*Client*>** | **File System** | **defaultBackupSet**.

2. Right click the <*Subclient*> and click **Backup**.

3. Select **Full** as backup type and **Immediate** to run the job immediately.

4. Click **OK**.

   You can track the progress of the job from the **Job Controller** or **Event Viewer** window. When the backup has completed, the Job Controller displays **Completed**.
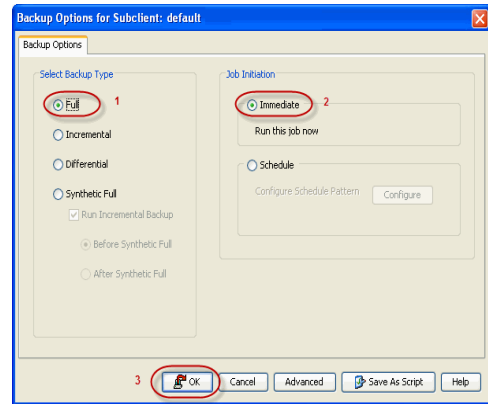
INCREMENTAL BACKUP

An incremental backup contains only data that is new or has changed since the last backup, regardless of the type. On average, incremental backups consume less media and use less resources than full backups.

The illustration on the right clarifies the nature of full and incremental backups.

Follow steps given below to perform an incremental backup:
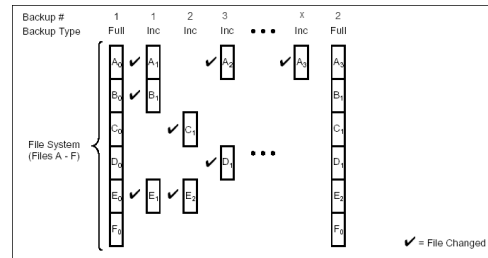
1. From the CommCell Browser, navigate to **<*Client*>** | **File System** | **defaultBackupSet.**

2. Right click the <*Subclient*> and click **Backup**.

3. Select **Incremental** as backup type and **Immediate** to run the job immediately.

4. Click **OK**.

   You can track the progress of the job from the **Job Controller**. When the backup has completed, the **Job Controller** displays **Completed**.
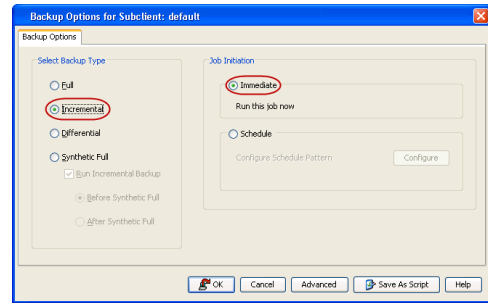
DIFFERENTIAL BACKUP

A differential backup contains only the data that is new or has changed since the last full backup. Like incremental backups, differential backups also consume less media and use less resources than full backups. Differential backups are cumulative. This means that each differential backup contains all changes accumulated since the last full backup. Each successive differential backup contains all the changes from the previous differential backup.

The illustration on the right demonstrates the nature of differential backups. For simplicity, assume there is a file system that contains six files as represented in the figure.

1. From the CommCell Browser, navigate to <*Client*> | **File System** | **defaultBackupSet.**

2. Right click the <*Subclient*> and click **Backup**.

3. Select **Differential** as a backup type and **Immediate** to run the job immediately.

4. Click **OK**.

   You can track the progress of the backup job from the **Job Controller**. When the backup has completed, the **Job Controller** displays **Completed**.
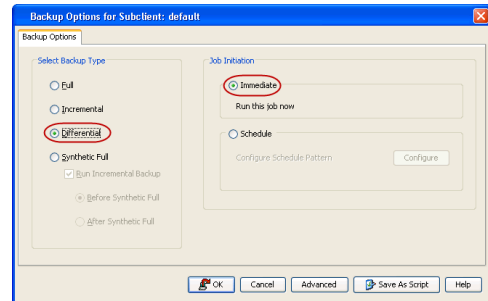
SYNTHETIC FULL BACKUP

A synthetic full backup is a synthesized backup, created from the most recent full backup and subsequent incremental and/or differential backups. The resulting synthetic full backup is identical to a full backup for the subclient.

Unlike full, incremental, and differential backups, a synthetic full backup does not actually transfer data from a client computer to the backup media. Therefore, they do not use any resources on the client computer.

Synthetic full backups are media-based; they read backup data from one media and simultaneously write (restore) the result to the new active media within the same media group. As a result, synthetic full backups require that at least two media drives for the same storage policy be available at the time the job is started. Synthetic full backups cannot be performed on subclients where the storage policy is associated with a stand-alone drive.

RUNNING SYNTHETIC FULL BACKUPS

Synthetic full backups can either be started manually or scheduled to occur at regular intervals. Do not concurrently run more than one synthetic full backup, especially synthetic full backups with multiple streams.

1. From the CommCell Console, navigate to <*Client*> | **File System** | **defaultBackupSet**.

2. Right click the <*Subclient*> and click **Backup**.

3. From the **Backup Options** window, select **Synthetic Full** for **Backup Type**.

4. Select **Immediate** for **Job Initiation**.

5. Click **OK**.

   You can track the progress of the backup job from the **Job Controller**. When the backup has completed, the **Job Controller** displays **Completed**.
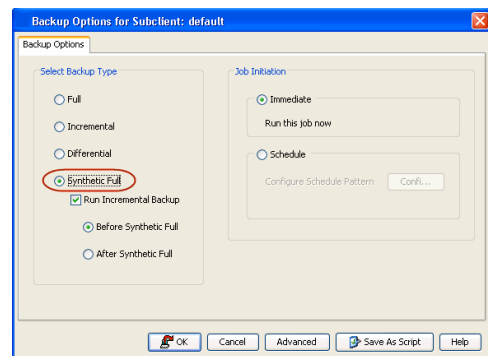
RUNNING AN INCREMENTAL BACKUP BEFORE OR AFTER A SYNTHETIC FULL BACKUP

An incremental backup can be run either before or after a synthetic full backup.

● Running an incremental backup before the synthetic full ensures that any new or recently changed data is included in the synthetic full.
● Running an incremental backup after the synthetic full ensures that any new or recently changed data since the backup that occurred prior to the synthetic full, but was not included in the synthetic full, is backed up by the incremental.

The sections below describe the steps to run an incremental backup before or after a synthetic full backup:

1. From the CommCell Console, navigate to **<Client>** | **File System** | **defaultBackupSet**.

2. Right click the **<Subclient>** and click **Backup**.

3. From the **Backup Options** window, select **Synthetic Full** for **Backup Type**.

4. Select **Run Incremental Backup** and then select **Before Synthetic Full** or **After Synthetic Full** options.

5. Select **Immediate** for **Job Initiation**.

6. Click **OK**.

   You can track the progress of the backup job from the **Job Controller**. When the backup has completed, the **Job Controller** displays **Completed**.
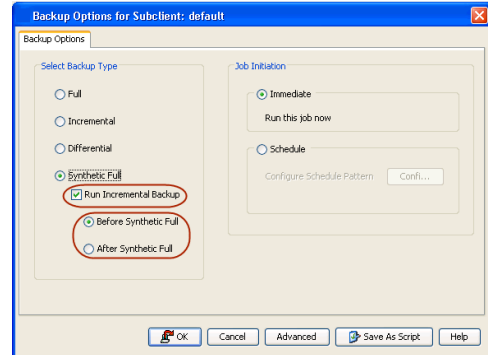
VERIFYING SYNTHETIC FULL BACKUPS

This option ensures that files that have not backed up by incremental jobs since the last full backup are backed up by the next incremental.

For example: If you perform the conventional full backup only once for a given subclient and then perform incremental (or differential) backups and periodic synthetic full backups. After the conventional full backup, a file is added to the subclient and the file has a time stamp older than the time of full backup. In such scenario, the file will never get backed up. Eventually, such files may be pruned and no backup of such files will be available.

The illustration on the right explains the necessity of verifying synthetic full backups.

In order to overcome this problem, it is recommended to verify the synthetic full backups job periodically as follows:

1. From the CommCell Console, navigate to **<Client>** | **File System** | **defaultBackupSet**.

2. Right click the **<Subclient>** and click **Backup**.

3. From the **Backup Options** dialog box, select **Synthetic Full**.

4. Click **Advanced**.

5. In the **Advanced Backup Options** dialog box, click the **Data** tab.

6. Select **Verify Synthetic Full**. Click **OK** to continue.

7. Click **OK**.

IGNORING ERRORS IN SYNTHETIC FULL BACKUPS

Errors encountered in synthetic full backups can be ignored, even if backup media is partially corrupted. Errors such as inability to read data (bad tape, files missing on disk media, etc.) will be ignored when this option is enabled.

1. From the CommCell Console, navigate to **<Client>** | **File System** | **defaultBackupSet**.

2. Right click the subclient and click **Backup**.

3. From the **Backup Options** dialog box, select **Synthetic Full**.

4. Click **Advanced**.

5. In the **Advanced Backup Options** dialog box, click the **Data** tab.

6. Select **Verify Synthetic Full** and then select **Ignore Error in Synthetic Full**.

7. Click **OK** to close the **Advanced Backup Options** dialog box.

8. Click **OK** .

ACCELERATED SYNTHETIC FULL BACKUPS (DASH FULL)

When a storage policy copy is deduplicated, synthetic full backups can be created in an accelerated mode to significantly reduce the copy duration. This is done by identifying and transferring the data signatures (instead of the data itself) to the target wherever possible.

Learn more...

BACKING UP MOUNT POINTS

Backups follow mount points by default, backing up both the configuration and the data on the mounted volume. You can use another subclient to backup the data on the mounted volume. In such case, you can exclude the data on the mounted volume from the default backup.

1. From the CommCell Console, navigate to **<Client>** | **File System** | **defaultBackupSet**.

2. Right click the default subclient and click **Backup**.

3. Select **Full** as backup type and **Immediate** to run the job immediately.

4. Click the **Advanced** button and select **Advanced Backup Options (Data)**

5. Select (or clear) **Follow mount points** to include (or exclude) the data on the mount points in the subclient.

6. Click **OK**.

   Depending upon your selection, the mount point data will be included or excluded in the subclient when you run the backup.
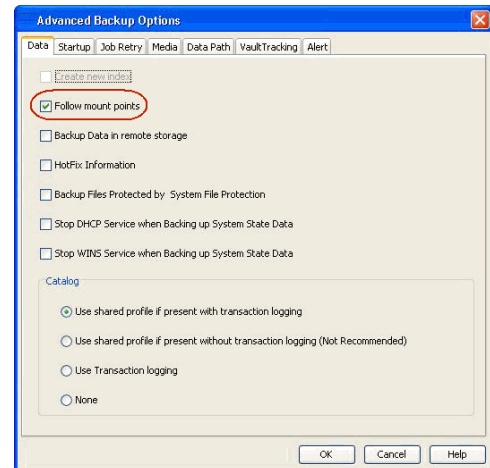
BACKING UP SYSTEM PROTECTED FILES

The system protected files are critical files that are installed as a part of windows operating system installation. For example, files with a .dll, .exe, .ocx, and .sys extension and some True Type fonts.

The system protected files are backed up by default via System State. Follow the steps given below to exclude these files from a backup.

1. From the CommCell Console, navigate to **<Client>** | **File System** | **defaultBackupSet**.

2. Right click the default subclient and click **Backup**.

3. Select **Full** as backup type and **Immediate** to run the job immediately.

4. Click the **Advanced** button and select **Advanced Backup Options (Data)**

5. Clear **Back up Files Protected by System File Protection** to exclude system protected files from the subclient.

6. Click **OK**.

   The system protected files will be excluded from the subclient when you run the backup.

   If you exclude the system protected files from the backup, you cannot use the backup for full system restore or system state restore.
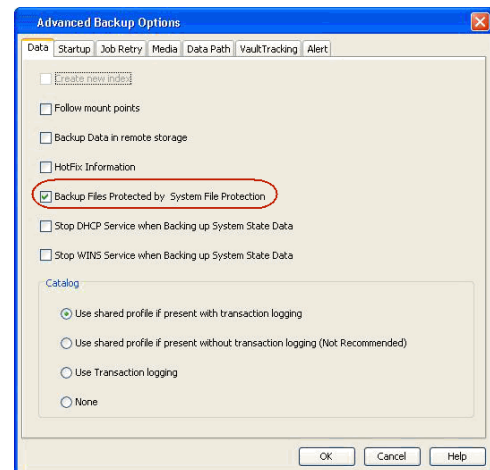
BACKING UP HOTFIX INFORMATION

The Hot Fix information is backed up by default. You can include or exclude the Hot Fix information from a subclient.

1. From the CommCell Console, navigate to **<Client>** | **File System** | **defaultBackupSet**.

2. Right click the default subclient and click **Backup**.

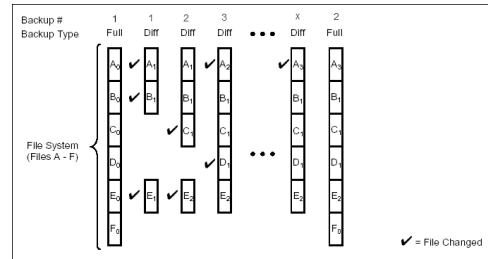3. Select **Full** as backup type and **Immediate** to run the job immediately.

4. Click the **Advanced** button and select **Advanced Backup Options (Data)**

5. Select (or clear) **HotFix Information** to include (or exclude) Hot Fix information from the subclient.

6. Click **OK**.

7. You can track the progress of the job from the **Job Controller**.

   Depending upon your selection, the Hot Fix information will be included or excluded from the subclient when you run the backup.
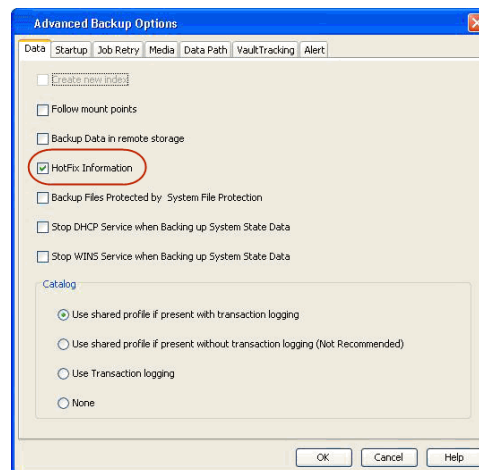
COMMAND LINE BACKUPS

You can perform backups of file system data from the command line interface.

Command line backups enable you to perform backup operation on multiple clients simultaneously. In order to run the backups from command line, you need an input xml file which contains the parameters for configuring the backup options. This input xml file can be obtained from one of the following ways:

● Download the input xml file template and save it on the computer from where the backup will be performed.

● Generate the input xml file from the CommCell Console and save it on the computer from where the backup will be performed.

LOG ON TO THE COMMSERVE

To run command line operations you must first login to the CommServe as follows:

● From Command prompt, navigate to <Software_Installation_Directory>/Base and run the following command:

  `qlogin -cs <commserve name> -u <user name>`

● For example, to log on to CommServe 'server1' with username 'user1':

  `qlogin -cs server1 -u user1`

PERFORM THE BACKUP

1. Download the backup_template.xml file and save it on the computer from where the command will be executed.

2. Execute the saved .xml script using qoperation execute command.

   `qoperation execute -af backup_template.xml -appName 'File System' -clientName xxxxx -backupsetName xxxxx -subclientName xxxxx -backupLevel FULL`

3. Verify the status of the job using the following command:

   `qlist job -j JOBID`

4. Once the job completes, logout from the CommServe using the qlogout command.

   `qlogout [-cs commserver] [-all] [-tf tokenfile] [-tk token] [-h]`

EXAMPLES

Performing a Full Backup	`qoperation execute -af backup_template.xml -appName 'File System' -clientName client1 -backupsetName backupset1 -subclientName subclient1 -backupLevel FULL`
Performing an Incremental Backup	`qoperation execute -af backup_template.xml -appName 'File System' -clientName client1 -backupsetName backupset1 -subclientName subclient1 -backupLevel INCREMENTAL`

GENERATE THE COMMAND LINE SCRIPT FROM THE COMMCELL CONSOLE

In addition to the parameters provided in the template xml file, if you want to include additional options for the backup, you can do so by selecting the required options from the CommCell Console and generate the command line xml script for the backup.

Follow the steps given below to generate a script which you can use to perform a backup from the command line interface:

1. From the CommCell Console, navigate to **<Client>** | **File System** | **defaultBackupSet**.

2. Right click the default subclient and click **Backup**.

3. Select the required backup options which you want to execute using the script.

4. Click **Save as Script**.
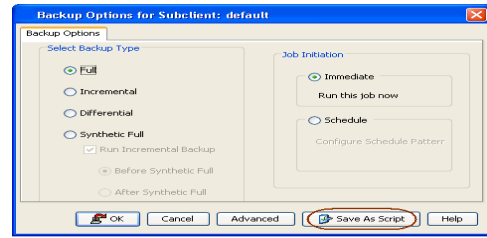
5. Enter the location where you want to save the script or click **Browse** and navigate to the location.

   The script will be saved as a .xml file and a .bat file is created.

   If a file with the same name already exists in the specified location, the .xml file will be created with a timestamp. However, the .bat file will overwrite the existing file.

6. Enter the username and password for the user account which you want to use to perform the backup.

   By default, the user account which you have used to login to CommCell console is used for performing the backup. However, if the user account does not have access to any application or database, click **Use a different account**.

7. Click **OK**.
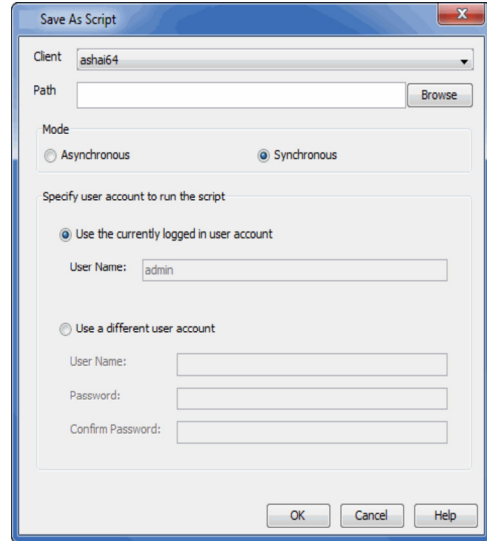
SCHEDULING A BACKUP

Follow the steps given below to schedule a data protection operation:

1.
   - From the CommCell Browser, navigate to **<Client>** | **File System** | **defaultBackupSet.**
   - Right-click the **Subclient** and click **Backup.**

2.
   - Select the **Backup type**.
   - Click **Schedule**.
   - Click the **Configure** button.
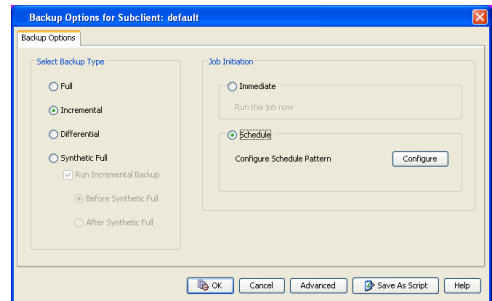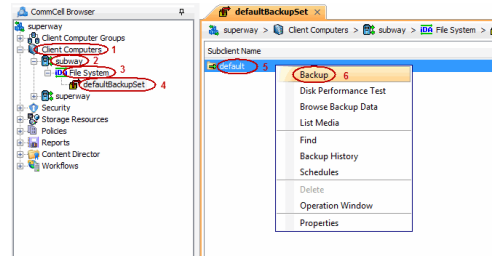
3. Select the appropriate scheduling options.

   For example, use the following steps to create a weekly schedule:

   - Type a name for the schedule in the **Schedule Name** box.
   - Click **Weekly**.
   - In the **Start Time** box type or select the schedule start time.
   - Click and select the days to run the schedule.
   - Click **OK**.

4. When the schedule is run, the **Job Controller** window will display the job as shown in the sample image.

5. Once the job is complete, you can view the job details from the **Backup History**.
    ● Right-click the **Subclient** and select **View Job Details**.

See Scheduling for a comprehensive information on scheduling jobs.

PERFORMING AN ON DEMAND BACKUP

1. From the CommCell Console, navigate to **<*Client*>** | **File System** | **<On Demand Backup Set>**.

2. Right click the subclient and click **Backup**.

3. Click **Browse**.

4. Navigate to the Directive file or Content file that you want to use.

5. Click **OK**.

6. Select **Immediate** to run the job immediately.

7. Click **OK**.

    You can track the progress of the job from the **Job Controller**.
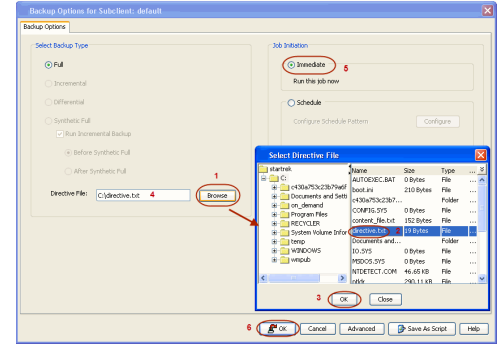
ADDITIONAL BACKUP OPTIONS FOR WINDOWS 2003

BACKING UP REMOTE STORAGE DATA

Remote Storage is used to extend disk space on your server without adding more hard disks. It automatically copies eligible files on your local volumes to a library of magnetic tapes or optical disks and monitors the amount of space that is available on your local volumes.

By default, when you back up the data in Remote Storage, the pointers to the remotely stored data and the data gets backed up. If you want to conserve disk space, you can backup only the pointers and exclude the actual data from the backup.

1. From the CommCell Console, navigate to **<*Client*>** | **File System** |**defaultBackupSet**.

2. Right click the subclient and click **Backup**.

3. Select **Full** as backup type and **Immediate** to run the job immediately.

4. Click the **Advanced** button and select **Advanced Backup Options (Data)**.

5. Select (or clear) **Backup data in Remote Storage** to include (or exclude) the

remote storage data from the subclient.

6. Click **OK**.

Depending upon your selection, the remote storage data will be included or excluded from the subclient when you run the backup.
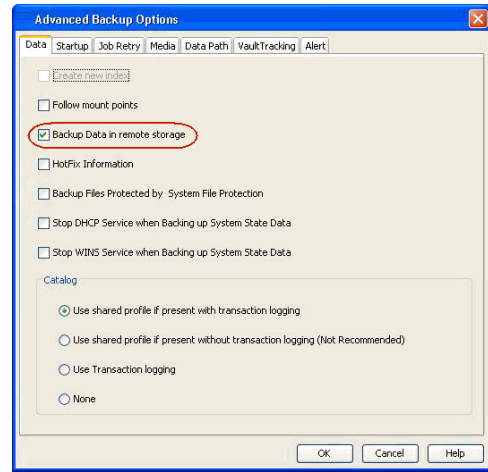
BACKING UP WINS AND DHCP SERVICES

You can backup the WINS and DHCP services during the system state backup. You must stop these services to include them in the system state backup.

1. From the CommCell Console, navigate to **<Client>** | **File System** | **defaultBackupSet**.

2. Right click the subclient and click **Backup**.

3. Select **Full** as backup type and **Immediate** to run the job immediately.

4. Click the **Advanced** button and select **Advanced Backup Options (Data)**.

5. Select (or clear) **Stop DHCP Service when Backing up System State Data** to include (or exclude) the DHCP services in the system state backup.

6. Select (or clear) **Stop WINS Service when Backing up System State Data** to include (or exclude) the WINS services in the system state backup.

7. Click **OK**.

Depending upon your selection, the WINS and DHCP services will be included or excluded from the subclient when you run the backup.
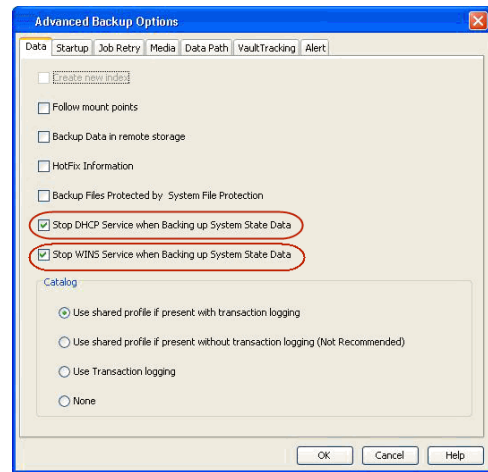
MANAGING JOBS

Jobs can be managed in a number of ways. See Job Management for a comprehensive information on managing jobs.

The following sections provide information on the different job management options available:

RESTARTING JOBS

Jobs that fail to complete successfully are automatically restarted based on the job restartability configuration set in the Control Panel. Keep in mind that changes made to this configuration will affect all jobs in the entire CommCell.

To Configure the job restartability for a specific job, you can modify the retry settings for the job. This will override the setting in the Control Panel. It is also possible to override the default CommServe configuration for individual jobs by configuring retry settings when initiating the job. This configuration, however, will apply only to the specific job.

Backup jobs for this Agent are resumed from the point-of-failure.

CONFIGURE JOB RESTARTABILITY AT THE COMMSERVE LEVEL

1. From the CommCell Browser, click **Control Panel** icon.

2. Select **Job Management.**

3. Click **Job Restarts** tab and select a **Job Type.**
    ○ Select **Restartable** to make the job restartable.
    ○ Change the value for **Max Restarts** to change the maximum number of times the

Job Manager will try to restart a job.

- ○ Change the value for **Restart Interval (Mins)** to change the time interval between attempts for the Job Manager to restart the job.

4. Click **OK.**

CONFIGURE JOB RESTARTABILITY FOR AN INDIVIDUAL JOB

1. From the CommCell Console, navigate to **<Client>** | **File System |** **<Backup Set>**.

2. Right-click the **Subclient** and select **Backup**

3. Click **Advanced.**

4. In the **Advanced Backup Options** dialog box, click the **Job Retry** tab.

5. Select **Enable Total Running Time** and specify the maximum elapsed time before a job can be restarted or killed.

   Select **Kill Running Jobs When Total Running Time Expires** to kill the job after reaching the maximum elapsed time.

6. Select **Enable Number Of Retries** and specify the number of retries.

7. Click **OK.**

CONTROLLING JOBS

The following controls are available for running jobs in the Job Controller window:

SUSPEND	Temporarily stops a job. A suspended job is not terminated; it can be restarted at a later time.
RESUME	Resumes a job and returns the status to Waiting, Pending, Queued, or Running. The status depends on the availability of resources, the state of the Operation Windows, or the Activity Control setting.
KILL	Terminates a job.

SUSPENDING A JOB

1. From the Job Controller of the CommCell Console, right-click the job and select **Suspend**.

2. The job status may change to **Suspend Pending** for a few moments while the operation completes. The job status then changes to **Suspended.**

RESUMING A JOB

1. From the Job Controller of the CommCell Console, right-click the job and select **Resume**.

2. As the Job Manager attempts to restart the job, the job status changes to **Waiting**, **Pending**, or **Running**.

KILLING A JOB

1. From the Job Controller of the CommCell Console, right-click the job and select **Kill**.

2. Click **Yes** when the confirmation prompt appears if you are sure you want to kill the job. The job status may change to **Kill Pending** for a few moments while the operation completes. Once completed, the job status will change to **Killed** and it will be removed from the Job Controller window after five minutes.

VIEWING LIST OF BACKED UP FILES IN A JOB

Use the `ListFilesForJob` utility to generate a list of files which are backed up during a specific job. Follow the steps give below to create a file which contains the list of files:

1. Open the Command Prompt and navigate to following location:

   `<Software_Installation_Directory>\calypso\Base\`

2. Enter the following command:

```
ListFilesForJob.exe -job <JOBID> -ma <MAName> [-vm <Instance>] [-flag <ArchiveBitFlag>] [-tmpdir <TMPDIRPATH>] [-o <OUTFILENAME>]
```

Where:

JobID	the job id of the job for which you are generating the list.
MAName	Name of the MediaAgent which is used to perform the backup job.
Instance	Name of the instance which you have used to install the Windows File System *i*DataAgent This is an optional argument. If you do not specify any value, the job in Instance001 will be used by default to generate the list of files.
ArchiveBitFlag	1 to set the Archive Bit 0 to reset the Archive Bit This is an optional argument. If you do not specify any value, the archive bit will not change and the file that contains the list of files can be deleted.
TMPDIRPATH	The directory in which you want to create the file. This argument is optional. If you do not specify any directory, the file will be created in the default temporary directory. The default temporary directory for the software is set using the dGALAXYTEMPDIR registry key. When you install Windows File System *i*DataAgent, the dGALAXYTEMPDIR registry key gets created at the following location: `HKEY_LOCAL_MACHINE\SOFTWARE\CommVault Systems\Galaxy\Instance<xxx>\Base`
OUTFILENAME	The name of the file in which you want to store the list

3. Navigate to the directory specified in `TMPDIRPATH` and open the `<OUTFILENAME>` file to view the list of files.

ADDITIONAL OPTIONS

The following table describes the available additional options to further refine your backup operations:

OPTION	DESCRIPTION	RELATED TOPICS
Startup Options	The Startup Options are used by the Job Manager to set priority for resource allocation. This is useful to give higher priority to certain jobs. You can set the priority as follows: 1. From the CommCell Browser, navigate to **Client Computers	<Client>	File System	Backup Set**. 2. Right-click the **Subclient** in the right pane and click **Backup**. 3. Click **Advanced** and click **Startup** tab. 4. Select the **Change Priority** checkbox. 5. Enter a priority number - 0 is the highest priority and 999 is the lowest priority. 6. Select the **Start up in suspended State** check box to start the job in a suspended state. 7. Click **OK**.	Refer to Job Priority and Priority Precedence.
Alerts	This option enables users or user groups to get automatic notification on the status of the data protection job. Follow the steps given below to set up the criteria to raise notifications/alerts: 1. From the CommCell Browser, navigate to **Client Computers	<Client>	File System	Backup Set**. 2. Right-click the **Subclient** in the right pane and click **Backup**. 3. Click **Advanced** and select the **Alert** tab. 4. Click **Add Alert.** 5. From the **Add Alert Wizard** dialog box, select the required threshold and notification criteria and click **Next**. 6. Select the required notification types and click **Next**. 7. Select the recipients and click **Next**. 8. Click **Finish**. 9. Click **OK**.	Refer to Alerts.
Command Line Backups	Command Line Interface enables you to perform backups or restore from the command line. The commands can be executed from the command line or can be integrated into scripts. You can also generate command line scripts for specific operations from the CommCell Browser using the **Save As Script** option.	Refer to Command Line Interface.
CommCell Readiness Report	The CommCell Readiness Report provides you with vital information, such as connectivity and readiness of the Client, MediaAgent and CommServe. It is useful to run this report before performing the data protection or recovery job. Follow the steps given below to generate the report: 1. From the **Tools** menu in the CommCell Console, click **Reports**. 2. Navigate to **Reports	CommServe	CommCell Readiness**.	Refer to CommCell Readiness Report.

	3. Click the **Client** tab and click the **Modify** button.	
	4. In the **Select Computers** dialog box, clear the **Include All Client Computers and All Client Groups** check box.	
	5. Select the client from the **Exclude** list.	
	6. Click the **Include >** button.	
	7. Click **OK**.	
	8. Click the **MediaAgent** tab.	
	9. Clear the **Include All MediaAgents** checkbox.	
	10. Select the MediaAgent from the **Exclude** list.	
	11. Click **Include >**.	
	12. Click **Run**.	
	The generated report is displayed.	
Backup Job Summary Report	The Backup Job Summary Report provides you with information about all the backup jobs that are run in last 24 hrs for a specific subclient. You can get information such as status, time, data size etc. for each backup job. It is useful to run this report after performing the backup. Follow the steps given below to generate the report:	Refer to Backup Job Summary Report.
	1. From the **Tools** menu in the CommCell Console, click **Reports**.	
	2. Navigate to **Reports | Jobs | Job Summary**.	
	3. Click **Data Management** on the **General tab** in the right pane.	
	4. Select the Computers tab.	
	5. Click **Subclient** and select the **Edit** tab.	
	6. Navigate to **Client Computers | <Client> | File System | Backup Set | Subclient**.	
	7. Click **Run**.	
Data Path Options	Data Protection operations use a default Library, MediaAgent, Drive Pool, and Drive as the Data Path. You can use this option to change the data path if the default data path is not available. Follow the steps given below to change the default data path:	Refer Change Data Path.
	1. From the CommCell Browser, navigate to **Client Computers | <Client> | File System | Backup Set**.	
	2. Right-click the **Subclient** in the right pane and click **Backup**.	
	3. Click **Advanced** and select the **Data Path** tab.	
	4. Select the **MediaAgent** and **Library**.	
	5. Select the **Drive Pool** and **Drive** for optical and tape libraries.	
	6. Click **OK**.	
Index Cache Server	Index Cache Server provides the facility to automatically continue data protection operations when there are job failures due to loss of connectivity to the index. You can configure the Index Cache Server as follows:	Refer to Index Cache Server for more information.
	1. From the CommCell Browser, navigate to **Storage Resources | MediaAgent**.	
	2. Right-click the <**MediaAgent**> and click **Properties**.	
	3. Click the **Catalog** tab and ensure that the **Index Cache Server** is configured.	
	4. From the CommCell Browser, navigate to **Client Computers | <Client> | File System | Backup Set**.	
	5. Right-click the **Subclient** in the right pane and click **Backup**.	
	6. Click **Advanced**.	
	7. Make sure that the **Use shared profile if present with transaction logging** option is selected.	
	8. Click **OK**.	
Create New Index	This option accelerates Full or On Demand backups and is enabled by default. When you perform a browse and restore operation, the default browse displays data up to the most recent full backup. To browse and restore older data you have to use the options to browse before or between specific dates.	Refer to Index.
	When disabled, Full or On Demand backups may be slower. However the default browse displays all data in the entire retention period; not just one full backup cycle. Use the following steps to configure this option for specific Full or On Demand backups. This option can also be configured for all subclients at the *i*DataAgent level.	
	1. From the CommCell Browser, navigate to **Client Computers | <Client> | File System | Backup Set**.	
	2. Right-click the **Subclient** in the right pane and click **Backup**.	
	3. Select **Full** as a backup type and click **Advanced**.	

	4. Select the **Create new index** check box**.**	
	5. Click **OK**.	
Start New Media	The Start New Media option enables you to start the data protection operation on a new media. This feature provides control over where the data physically resides.Use the following steps to start the data protection operation on a new media:	Refer to Start New Media.
	1. From the CommCell Browser, navigate to **Client Computers | <Client> | File System | Backup Set**.	
	2. Right-click the **Subclient** in the right pane and click **Backup**.	
	3. Click **Advanced** and select the **Media** tab.	
	4. Select the **Start New Media** check box.	
	5. Click **OK**.	
Mark Media Full	This option marks the media as full, two minutes after the successful completion of the data protection job. This option prevents another job from writing to this media. Follow the steps given below:	Refer to Export Media.
	1. From the CommCell Browser, navigate to **Client Computers | <Client> | File System | Backup Set**.	
	2. Right-click the **Subclient** in the right pane and click **Backup**.	
	3. Click **Advanced** and select **Media** tab.	
	4. Select the **Mark Media Full on Success** check box**.**	
	5. Click **OK**.	
Allow other Schedules to use Media Set	The Allow Other Schedules to use Media Set option allows jobs that are part of the schedule or schedule policy and using the specific storage policy to start a new media. It also prevents other jobs from writing to the same set of media.	Refer to Creating an Exportable Media Set.
	1. From the CommCell Browser, navigate to **Client Computers | <Client> | File System | Backup Set**.	
	2. Right-click the **Subclient** in the right pane and click **Backup**.	
	3. Click **Advanced** and select the **Media** tab.	
	4. Select the **Allow Other Schedules To Use Media Set** check box.	
	5. Click **OK**.	
Reserve Resources Before Scan	Media is reserved for a job when the job is ready to write data. You can use this option to reserve the media during the initial phase of the job. Follow the steps given below to reserve media:	
	1. From the CommCell Browser, navigate to **Client Computers | <Client> | File System | Backup Set**.	
	2. Right-click the **Subclient** in the right pane and click **Backup**.	
	3. Click **Advanced** and select the **Media** tab.	
	4. Select the **Reserve Resources before Scan** check box.	
	5. Click **OK**.	
Extended Data Retention	This option allows you to extend the expiration date of a specific job. This will override the default retention set at the corresponding storage policy copy. Follow the steps given below to extend the expiration date:	Refer to Extended Retention Rules.
	1. From the CommCell Browser, navigate to **Client Computers | <Client> | File System | Backup Set**.	
	2. Right-click the **Subclient** in the right pane and click **Backup**.	
	3. Click **Advanced** and select the **Media** tab.	
	4. Select one of the following options: ○ **Infinite** - Select this option to extend the expiration date by infinite number of days ○ **Number of day** - Select this option to specify the number of days to extend the expiration date and then enter the number of days.	
	5. Click **OK**.	
Vault Tracker	This feature provides the facility to manage media that is removed from a library and stored in offsite locations. Depending on your VaultTracker setup, select the required options. Use the following steps to access and select the VaultTracker options.	Refer to VaultTracker or VaultTracker Enterprise.
	1. From the CommCell Browser, navigate to **Client Computers | <Client> | File System | Backup Set**.	
	2. Right-click the **Subclient** in the right pane and click **Backup**.	
	3. Click **Advanced** and select the **VaultTracking** tab.	
	4. Select the required options.	
	5. Click **OK**.	

Browse Data - Windows File System

RELATED TOPICS

List Media
Provides comprehensive information on media management and prediction.

UNDERSTANDING THE BROWSE WINDOW

Browse provides an easy-to-use convenience to search and restore data.

You can open the browse window from client, agent, backup-set or subclient level. The sub levels displayed in the browse window is based on where you start the browse operation.

SELECTING OBJECTS FROM THE BROWSE WINDOW FOR RESTORE

The browse window displays objects and consists of two parts:

- The left pane displays the object tree at the selected level.

- The right pane displays the contents of the selected object.

Note that the window displays only the data that was obtained by a backup. Data that is excluded by a filter, or data which did not exist as of the specified browse time does not appear in the window.

Selections follow these rules:

- All selections are recursive.

- Clicking a box again causes the selection to be cleared.

- If you select an object in the left pane, then all of its contents are selected.

- You can select a specific object in the right pane.

Selection status is revealed by the selection icons as follows:

☐	Indicates that the object is not selected for restoration.
◩	Indicates that a portion of the object is selected for restoration. i.e., only some of the child object(s) within the selected object.
▨	Indicates that the entire object, including all of its child objects, are selected for restoration.

BROWSE DATA

The option to browse the backup data provides the facility to view and restore the data that was backed up. The following sections explain how to browse the backup data.

LATEST DATA

Follow the steps given below to view the latest data backed up by a backup set:

1. From the CommCell Browser, navigate to **Client Computers | *<Client>* | File System**

2. Right-click a Backup Set and click **All Tasks** | **Browse/Browse Backup Data**.

3. Click **OK**.
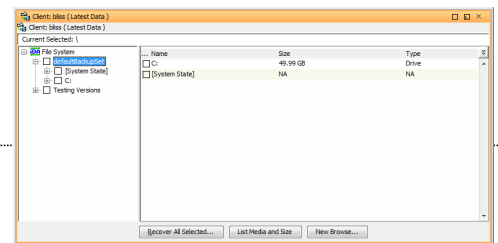
The latest data backed up by all the subclients is displayed in the **Client Browse** tab.

DATA BEFORE A SPECIFIED TIME

Follow the steps given below to browse the data backed up before specified time:

1. From the CommCell Browser, navigate to **Client Computers | <*Client*> | File System**

2. Right-click a Backup Set and click **All Tasks** | **Browse/Browse Backup Data**.

3. Select **Specify Browse Time**.

4. Select a date and time to **Browse Data Before** it.

5. Click **OK**.
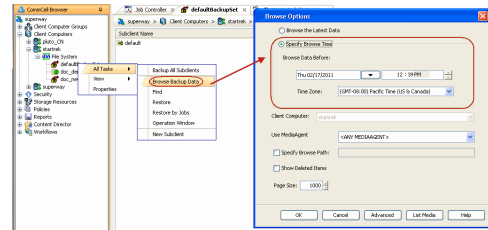
DATA BETWEEN A SPECIFIED TIME

Follow the steps given below to browse data between specified time:

1. From the CommCell Browser, navigate to **Client Computers | <*Client*> | File System**

2. Right-click a Backup Set and click **All Tasks** | **Browse/Browse Backup Data**.

3. Select **Specify Browse Time**.

4. Select a date and time to **Browse Data Before** it.

5. Click **Advanced**.

6. In the **Advanced Browse Options** dialog box, select **Exclude Data Before.**

7. Select the date and time to exclude the data before it from the browse operation.

8. Click **OK** in the **Advanced Browse Options** dialog box .

9. Click **OK** in the **Browse Options** dialog box.
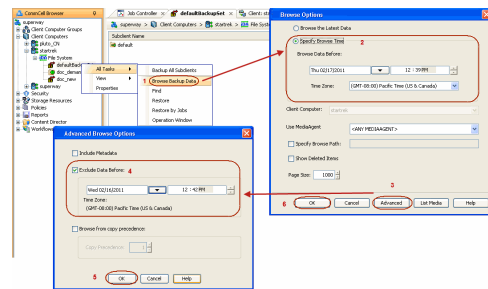
BROWSE FROM COPIES

By default, when a browse operation is requested, the software attempts to browse from the storage policy copy with the lowest copy precedence. If the data that you want to browse was already pruned from the primary copy, the software searches the other copies of the storage policy, starting from the copy with the lowest copy precedence to a copy with the highest copy precedence.

This feature is useful in the following conditions:

- The media containing protected data for a particular copy has been removed from the storage library, you can choose to browse from a copy whose media are inside the library.

- Allows browsing from a copy that accesses faster disk media rather than slower tape media.

- When media drives used by a particular copy are busy with another operation, this helps in browsing from a different copy to avoid resource conflicts.

1. From the CommCell Browser, navigate to **Client Computers | <*Client*> | File System**

2. Right-click a Backup Set and click **All Tasks** | **Browse/Browse Backup Data**.

3. From the **Browse Options** dialog box, click **Advanced**.

4. In the **Advanced Browse Options** dialog box select the **Browse from copy precedence** option.
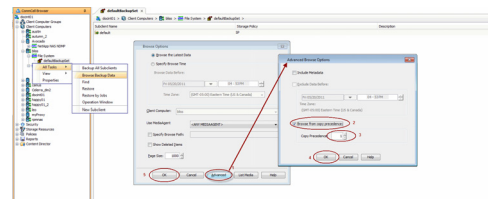
> If you specify a copy precedence number for a browse operation, the software searches only the storage policy copy with that precedence number in all storage policies used for securing the data. If data does not exist in the specified copy, the browse operation fails even if the data exists in another copy of the same storage policy.

5. Specify the precedence number in **Copy Precedence**.

6. Click **OK** in the **Advanced Browse Options** dialog box .

7. Click **OK** in the **Browse Options** dialog box.

LIST MEDIA

List media option is useful to predict media required to restore the index required to browse data. This is useful when the index is not available in the index cache.

The following section describes how to perform this operation.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | File System**.

2. Right-click the backup set for which you wish to list media, point to **All Tasks** and then click **Browse**.

3. From the **Browse Options** dialog box, if required, select the following options:
   o Click **Browse the Latest Data** to list media associated with the most recent data protection cycle.
   o Click **Specify Browse Time** to list media associated with data protection operations up to the specified date and time range. Use the **Browse Data Before** box to specify the end date and time.
   o Click **Advanced** and then click **Exclude Data Before** and then select the date and time from which you wish to list media associated with data protection operations.

   Note that you can use the **Specify Browse Time** and **Exclude Data Before** options to list media between a specified date and time range.

4. Click **List Media**.

5. From the **List Media** dialog box, click **List Media for restore within specified time range.**

6. Click **OK**.

   The appropriate media is listed in the **Media** dialog box.
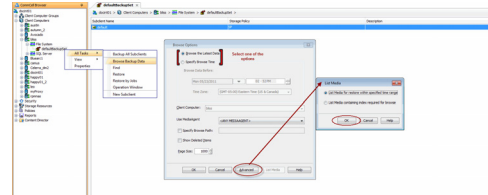
FULL BACKUP TRANSPARENT BROWSE

The browse searches described so far are confined to one full backup cycle, either the most recent (by default) or some previous cycle. Usually, this provides the desired results because generally you may want to restore either the latest version or the latest version as of some specified date.

If, however, you want to view all available versions that has not yet been pruned, then the browse cannot access data beyond it in a single operation.

Full backup transparent browses enable you to browse all the data within the entire retention period, not just one full backup cycle. When you use the **View All Versions** option, the browse operation displays all versions available in the backup.

By default, the Full Backup Transparent Browse is not enabled. Use the following steps to enable this option on a client before performing a backup:

1. From the CommCell Browser, navigate to **Client Computers | <Client>.**

2. Right-click the Agent and click **Properties**.

3. Click **Index** and then clear **Create new index on Full Backup**.

4. Click **OK**.
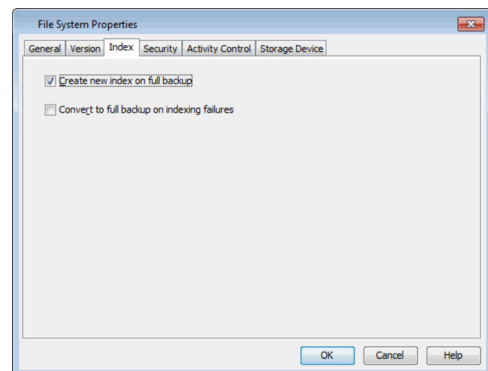
FIND A FILE OR DIRECTORY

Use Find to find a file or directory name or a name pattern. Find has the capability to browse multiple indexes which allows you to find beyond the last full backup (or new index) as long as the data resides on an index that exists within the retention period.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | File System**

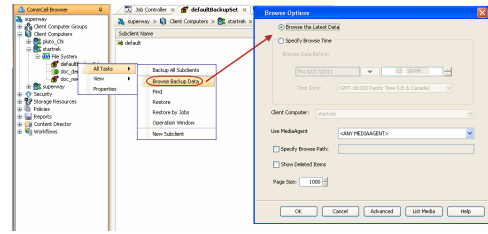2. Right-click a Backup Set and click **All Tasks** | **Browse/Browse Backup Data**.

3. Click **OK**. The latest data backed up by all the subclients is displayed in the **Client Browse** tab.

4. Right-click the selected content and click **Find**.

5. Enter the file name and the location of the file to be searched in the **Name/Pattern** and **Folder** fields and click **Search**.
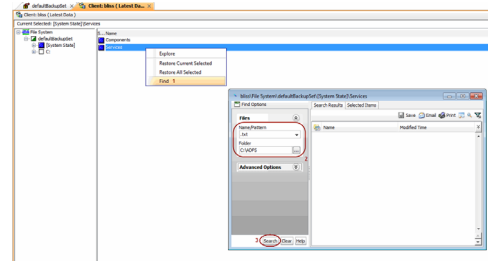
IMAGE/NO-IMAGE BROWSE

Image browse displays the structure of the entity as it existed as of some specified time. When you browse data in the image mode, the system by default returns the requested data based on the latest image available. The image browse can only restore the latest version. If the requested version was deleted before the most recent full backup, the default browse will not find the data.

The no-image browse is useful for retrieving data that may have been deleted at some unknown time. It is also useful to retrieve a previous backup version.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | File System**

2. Right-click a Backup Set and click **All Tasks** | **Browse/Browse Backup Data**.

3. From the **Browse Options** dialog box, select one of the following options:
   - Click and select the **Show Deleted Items** option to perform a no-image browse of the data.
   - Clear the **Show Deleted Items** option to perform an image browse of the data.

4. Click **OK**.
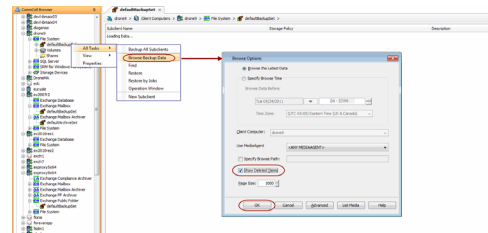
BROWSE MULTIPLE VERSIONS OF A FILE

By default, the system allows you to browse and recover previously backed up versions of data. This feature allows you to restore more than one version of the same file by restoring each version individually.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | File System**

2. Right-click a Backup Set and click **All Tasks** | **Browse/Browse Backup Data**.

3. Click **OK**.

4. From the **Browse Window**, right-click the file with multiple versions and then click **View All Versions**.

   The **All Version** dialog box displays the available versions for the file.
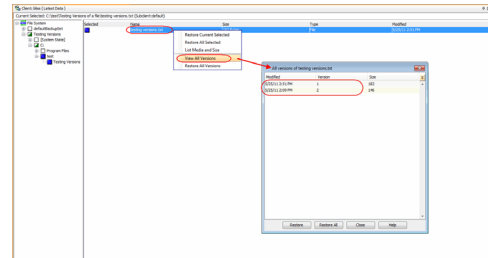
ESTABLISH THE PAGE SIZE FOR A BROWSE

The Page Size option allows you to specify the number of objects to be displayed in the browse window. You can browse through each page list by selecting the appropriate page number in the Browse window. This field reverts back to the default setting after use.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | File System**

2. Right-click a Backup Set and click **All Tasks** | **Browse/Browse Backup Data**.

3. From the **Browse Options** dialog box, enter a value for **Page Size**.

4. Click **OK**.
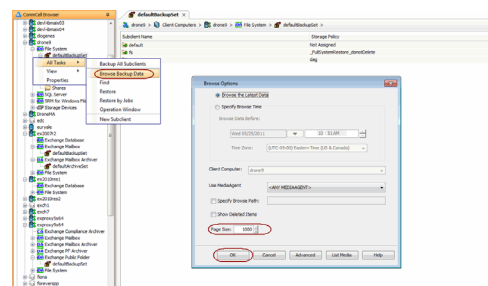
BROWSE USING A SPECIFIED PATH

The Browse Path option allows you to specify the starting point for the browse operation.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | File**

System

2. Right-click a Backup Set and click **All Tasks** | **Browse/Browse Backup Data**.

3. From the **Browse Options** dialog box, enter the browse path in **Specify Browse Path**.

4. Click **OK**.
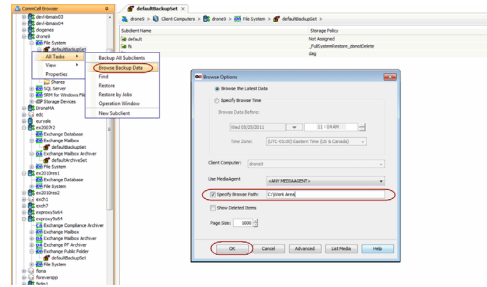
BROWSE USING MEDIA AGENT

Data can be restored from any compatible library and drive type in the CommCell. By default, the system automatically identifies and restores data from any configured library in the CommCell, even if the media is not available in the original library in which the data protection operation was performed. Use this procedure to Browse using a specific MediaAgent.

1. From the CommCell Browser, navigate to **Client Computers | <*Client*> | File System**

2. Right-click a Backup Set and click **All Tasks** | **Browse/Browse Backup Data**.

3. From the **Browse Options** dialog box, choose the **MediaAgent** that must be used to perform the browse.

4. Click **OK**.
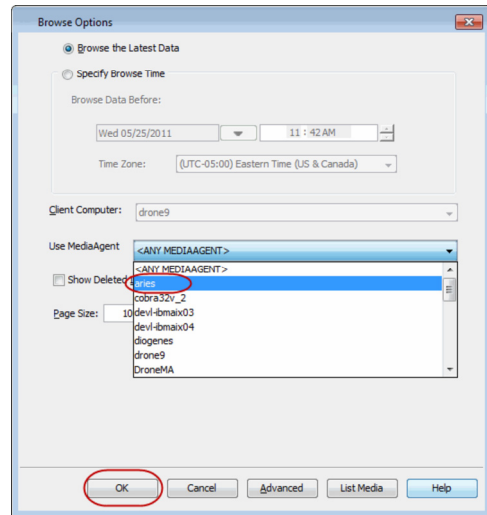
Advanced - Windows File System Restore

TABLE OF CONTENTS

PERFORM A DIRECT RESTORE

Perform a direct restore in the following scenarios:

- You know the path to the data that you want to restore. For example: `C:\info\com\move`
- The data that you want to restore is from a single volume. For example: `D:\`

If you want to restore data from multiple volumes, perform a browse and restore.

Follow the steps given below to perform a direct restore:

1.
- From the CommCell Browser, navigate to **Client Computers | <*Client*> | File System**.
- Right-click the **defaultBackupSet** and then click **All Tasks | Restore**.

2.
Enter the starting path of the data that you want to restore.

You can use wildcard characters to specify the patterns for files and folders to be included in the restore. For example: If you want to restore all the files starting with the word file, then specify `file*.*`

3.
- In the **Destination Client** list, select the name of the client computer.
- If you want to add more data for restore, click **Advanced**.

4.
- Click the **Path/Filters** tab.
- Click **Add** for **Source Item** list and enter the path of the data.

  If you want to use wildcard characters to specify a file name pattern, you must express complete paths (e.g. `C:\Test\*.dll`).

- Click **OK**.

4.
- Click the **Job Initiation** tab.
- Select **Immediate** from the **Job Initiation** tab.
- Click **OK**.
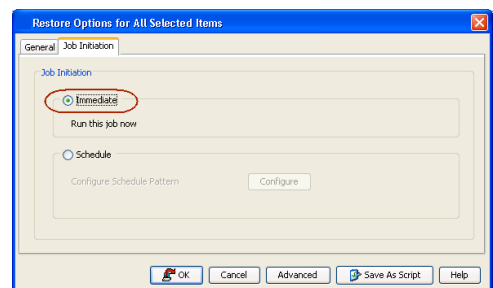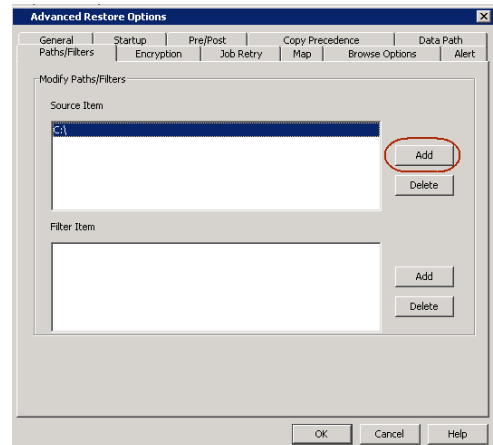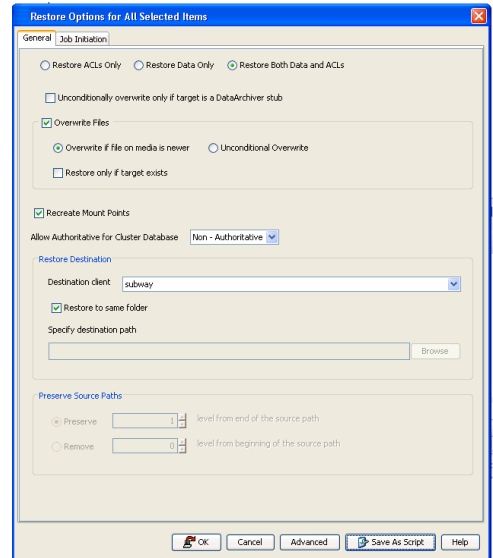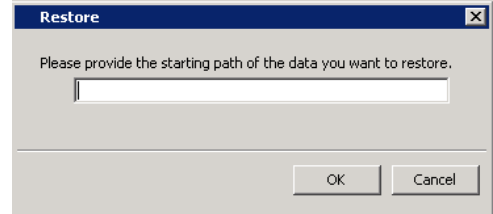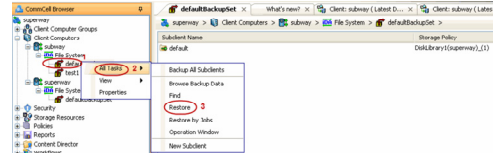
5.

You can track the progress of the job from the **Job Controller**.

RESTORING DATA USING REGULAR EXPRESSIONS

By default you can use wildcard characters to specify the patterns for files and folders to be included in the restore.

Use the following steps to define wildcard characters as regular expressions:

1. From the CommCell Browser, navigate to **Client Computers | <*Client*> | File System**.

2. Right-click the **defaultBackupSet** and then click **All Tasks | Restore**.

3. Enter the source path that contains regular expressions and/or wild cards.

4. In the **Restore Options for All Selected Items** dialog box, click **Advanced**.

5. Clear **Automatically Detect Regular Expressions** and click **OK**.

   This option is selected by default for direct restore operations. For Browse and Restore operations, the option cannot be enabled as you are selecting definitive paths to restore.

6. Click **OK**.
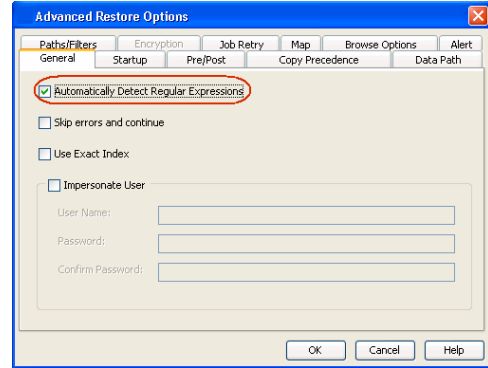
SUPPORTED WILDCARDS IN REGULAR EXPRESSIONS

If enabled, the following wildcards can be automatically detected in regular expressions when restoring data.

WILDCARD	DEFINITION	EXAMPLE
*	Any number of characters. This wildcard is used in following scenarios: ● filter all files of a specific extension ● filter all files when the file name starts with a specific pattern	`C:\*.log` will filter all files with the .log extension on root of the C drive. If you want to filter files with the `.log` extension from a folder on the C drive, you must include the path to the folder in the filter. (e.g. `C:\Test\*.log`) `ntuser*` will filter all files for which the file name starts with the word `ntuser`.
?	Any one character This wildcard is used in following scenarios: Filter all files (or folders) for which the name begins with a specific word and the last character of the word is variable.	To filter files: `C:\access?.doc` will filter any files with the extension .doc on the C drive for which the name begins with- "`access`" followed by any one character such as `access1.doc` or `access5.doc`. However, `access12.doc` or `access15.doc` will not be filtered because the last two characters in the name are variable. To filter folders: `C:\access?\**\*` will filter any on the C drive for which the name begins with- "`access`" followed by any one character such as `C:\access1` or `C:\access5`. However, `C:\access12` or `C:\access15` will not be filtered because the last two characters in the name are variable.
***	All files under a specific directory	`C:\Test\Data\**\*` will filter all files and subdirectories under and including `C:\Test\Data` `C:\**\Data\**\*` will filter all files and subdirectories below and including any directory called "Data" at any level in the C: volume `G:\Users\**\xpprofile\*.log` will filter all files with the .log extension from any `xpprofile` subdirectory under `Users` directory `G:\Users\**\xpprofile\ntuser*` will filter all filenames starting with `ntuser` from any `xpprofile` subdirectory under `Users` directory

REVIEWING THE SIZE DISTRIBUTION

Before restoring any drive, you can quickly review the data size distribution of various folders in that drive. Follow the steps given below to view the size

distribution:

1. From the CommCell Browser, navigate to **Client Computers | *<Client>* | File System**

2. Right-click a Backup Set and click **All Tasks** | **Browse/Browse Backup Data**.

3. Select the required options on the **Browse Options** dialog box and click **OK**.

4. Select the drive or folder that you want to restore.

5. Ensure that the **Show size distributions** check box is selected.

A pie chart of size distribution is displayed in the right pane of the CommCell Browser.
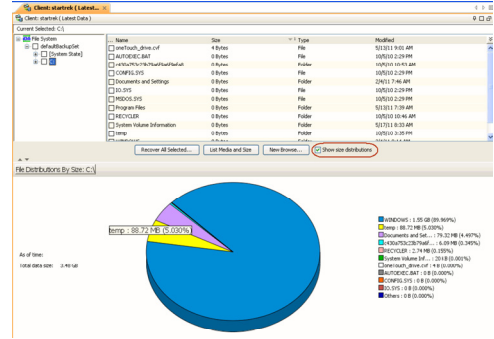
PERFORMING AN OUT-OF-PLACE RESTORE

You can restore the data to following locations:

- Different folder on the same computer from which the data was backed up
- Different computer

Keep in mind that the destination computer must reside in the same CommCell as the client whose data was backed up.

RESTORING TO DIFFERENT FOLDER ON THE SAME CLIENT

Follow the steps given below to restore data to a different folder on the same client from which data is backed up:

1. From the CommCell Browser, navigate to **Client Computers | *<Client>* | File System | *<Backup Set>*.**

2. Right-click the *<Subclient>* in the right pane and then click **Browse Backup Data**.

3. Click **OK**.

4. Select the data that you want to restore and click **Recover All Selected**.

5. Clear the **Restore to same folder** check box and click **Browse**.

6. Click **OK**.

7. Use the options in the **Preserve Source Paths** area to exclude folders (and its contents) from the source path.

   For Example: If the selected data is `Documents\Users\Memos\Sales`, and you want to restore data only from the `Sales` folder, set the **Preserve <n> level from end of source path** option to 1.

   If the selected data is `Documents\Users\Memos\Sales`, and you want to restore the data from `Memos` and `Sales` folders, set the **Remove <n> level from beginning of source path** option to 2.

8. Click **OK**.
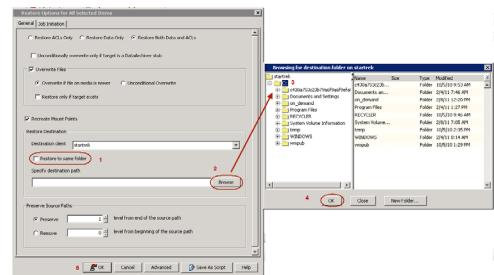
RESTORING TO A DIFFERENT CLIENT

Follow the steps given below to restore data to a different client:

1. From the CommCell Browser, navigate to **Client Computers | *<Client>* | File System | *<Backup Set>*.**

2. Right-click the *<Subclient>* in the right pane and then click **Browse Backup Data**.

3. Click **OK**.

4. Select the data that you want to restore and click **Recover All Selected**.

5. In the **Destination Client** list, select the client. You can select any client that is in the same CommCell as that of the client from which the data was backed up.

6. Click **OK**.

The data will be restored to a different client. The location of the data will remain same as the source client. If you restore a shared folder from one client computer to another client computer, the share status of the folder will be restored.
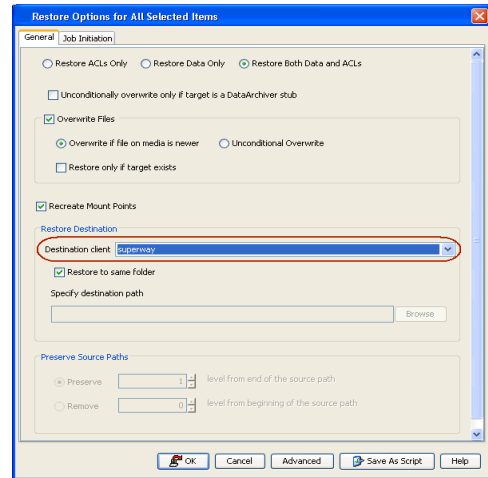
PERFORMING A CROSS-PLATFORM RESTORE

You can restore data to the following platforms:

● All supported versions of Windows

● All supported versions of Unix, Linux and Macintosh

   You cannot restore encrypted files from a windows client to the Unix client.

Follow the steps given below to perform a cross-platform restore:

1. From the CommCell Browser, navigate to **Client Computers | <*Client*> | File System | <*Backup Set*>**.

2. Right-click the **<*Subclient*>** in the right pane and then click **Browse Backup Data**.

3. Click **OK**.

4. Select the data that you want to restore and click **Recover All Selected**.

5. In the **Destination Client** list, select the client. You can select any client that is in the same CommCell as that of the client from which the data was backed up.

6. Clear the **Restore to same folder** check box and click **Browse**.

7. Select the destination folder and click **OK**.

8. Click **OK**.
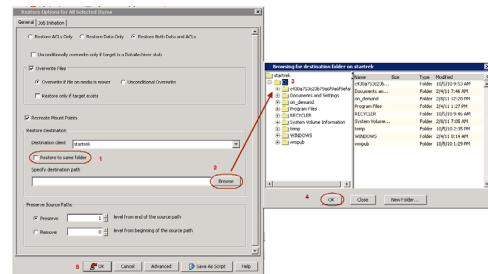
RESTORE TO A UNC PATH/ NFS-MOUNTED FILE SYSTEM

Follow the steps given below to restore data to a UNC path (Windows) or NFS-mounted file system (Unix).

1. From the CommCell Browser, navigate to **Client Computers | <*Client*> | File System | <*Backup Set*>**.

2. Right-click the **<*Subclient*>** in the right pane and then click **Browse Backup Data**.

3. Click **OK**.

4. Select the data that you want to restore and click **Recover All Selected**.

5. In the **Destination Client** list, select the computer that hosts the share or mounted file system.

6. Clear the **Restore to same folder** check box and enter the UNC path or the network share.

   For example: \\quark\restore\client_a\

7. When you are restoring to a UNC path (Windows), click the **Advanced**.

8. From the **General** tab of the **Advanced Restore Options** dialog box, select the **Impersonate User** option.

9. Enter a username and password that has all permissions for the folder to which the data will be restored. This user should be allowed to create files in the in the destination folder of the client where you are restoring the data.

10. Click **OK**.

11. Click **OK**.
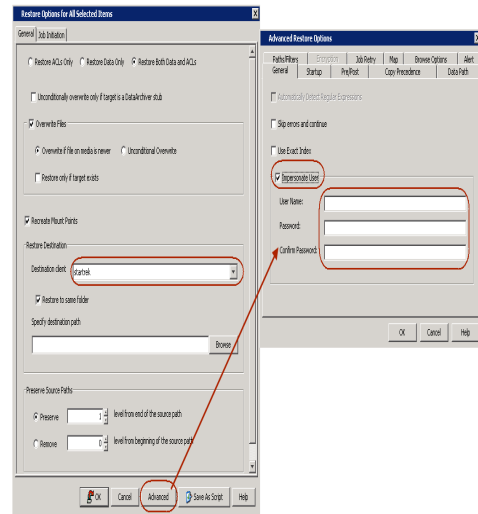
RENAMING FILES ON RESTORE

If you do not want to overwrite the existing files during restores, you can append a suffix to the filenames and restore them as new files. (This suffix is appended to the filename before the extension.)

Follow the steps given below to rename files during the restore:

1. From the CommCell Browser, navigate to **Client Computers | <*Client*> | File System | <*Backup Set*>**.

2. Right-click the **<*Subclient*>** in the right pane and then click **Browse Backup Data**.

3. Click **OK**.

4. Select the data that you want to restore and click **Recover All Selected**.

5. In the **Destination Client** list, select the client.

6. Click **Advanced**.

7. In the **Advanced Restore Options** dialog box, select the **Map** tab.

8. Enter the desired string that you want to append as a suffix to the filenames in **Rename all restore files with suffix** and click **OK**. For Example: Enter the string `temp` will rename `file.txt` to `filetemp.txt`.

9. Click **OK**.

10. Click **OK** to start the restore.
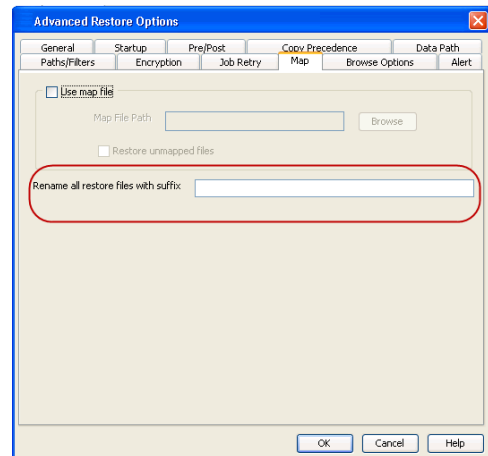
OVERWRITING DATA DURING RESTORES

By default, the data in the destination is overwritten when the restored version is newer than the one in the destination.

Use the following steps to overwrite data irrespective of the destination version:

1. From the CommCell Browser, navigate to **Client Computers | <*Client*> | File System | <*Backup Set*>**.

2. Right-click the **<*Subclient*>** in the right pane and then click **Browse Backup Data**.

3. Click **OK**.

4. Select the data that you want to restore and click **Recover All Selected**.

5. Ensure that the **Overwrite Files** check box is selected.

6. Click **Unconditional Overwrite**.

7. Click **OK**.
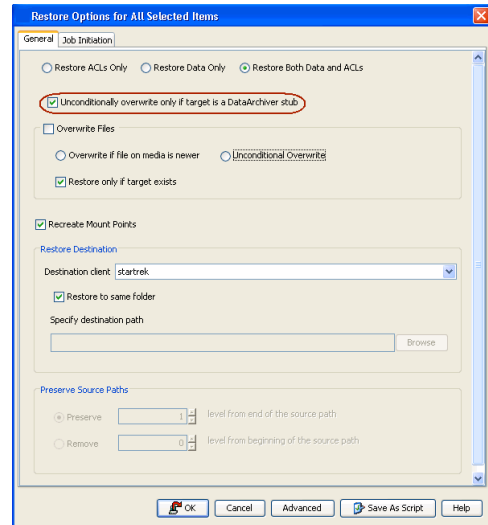
RESTORING DATA ONLY WHEN IT EXISTS ON THE DESTINATION

Follow the steps given below to restore the only data that already exists in the destination computer. This ensures any data removed from the destination computer is not reintroduced by the data recovery.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | File System | <Backup Set>**.

2. Right-click the **<Subclient>** in the right pane and then click **Browse Backup Data**.

3. Click **OK**.

4. Select the data that you want to restore and click **Recover All Selected**.

5. Ensure that the **Overwrite Files** check box is selected. (If it is not selected, only those files that do not exist on the destination will be restored.)

6. Select the **Restore only if target exists** check box.

7. Click **OK**.
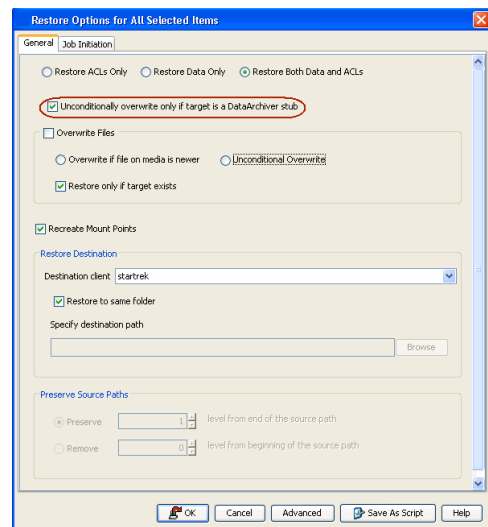
RESTORING BY JOBS

You can select a specific backup job for a restore. This method of restoring data is faster and useful in the following scenarios:

- To restore point-in-time data associated with a specific backup job
- To restore multiplexed data from the same client

RESTORING ALL THE DATA BACKED UP DURING A JOB

Following the steps to restore all the data data backed up during the selected job:

1. From the CommCell Browser, navigate to **Client Computers | <Client> | File System**.

2. Right-click the **<Backup Set>** and select **All Tasks | Restore by Jobs**.

3. Enter the **Start Time** and **End Time** and click **OK**. The list of backup jobs, completed in the specified time period is displayed.

4. Right click the job you wish to restore and select **Restore Selected Jobs.**

5. Click **OK**.
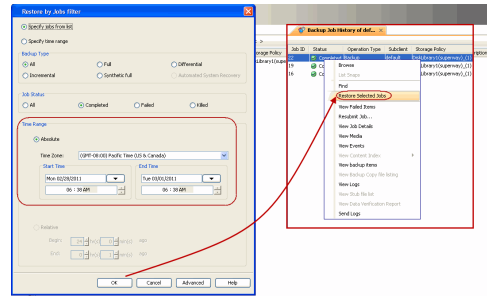
RESTORING SPECIFIC DATA BACKED UP DURING A JOB

You can restore specific files and folders from the data backed up during the selected job. Follow the steps given below to restore specific files and folders from the selected backup job:

1. From the CommCell Browser, navigate to **Client Computers | <Client> | File System**.

2. Right-click the **<Backup Set>** and select **All Tasks | Restore by Jobs**.

3. Enter the **Start Time** and **End Time** and click **OK**. The list of backup jobs, completed in the specified time period is displayed.

4. Right click the job you wish to restore and select **Browse**.

5. Click **OK** in the **Browse Options** dialog box.

6. Select data that you want to restore and click **Recover All Selected**.

7. Click **OK**.
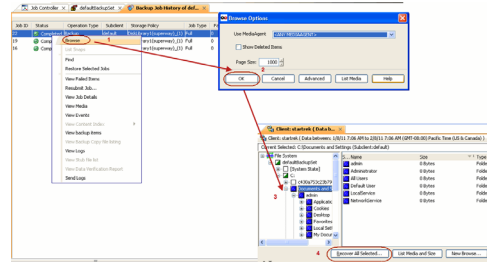
RESTORING FROM A FAILED OR KILLED JOB

You can restore from a failed or killed job. When restoring from a failed or killed job, the data backed up to the point of failure will be restored.

Failed or killed backup jobs are immediately aged regardless of their defined retention rules, therefore, these jobs can only be restored if the media is not yet overwritten. You can restore aged data from tape media but cannot restore from disk libraries.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | File System**.

2. Right-click the **<Backup Set>** and select **All Tasks | Restore by Jobs**.

3. Select **Failed** or **Killed** in the **Job Status** area of the **Restore by Jobs Filter** dialog box.

4. Enter the **Start Time** and **End Time** to specify the time period in which the job was failed or killed.

5. Click **Advanced.**

6. Select the **Include Aged Data** check box and click **OK**.

7. Click **OK** on the **Restore Jobs Filter** dialog box. The list of backup jobs, completed in the specified time period is displayed. The list also includes Failed or Killed jobs.

8. Right click the job you wish to restore and click **Restore Selected Jobs.**

9. Click **OK**.
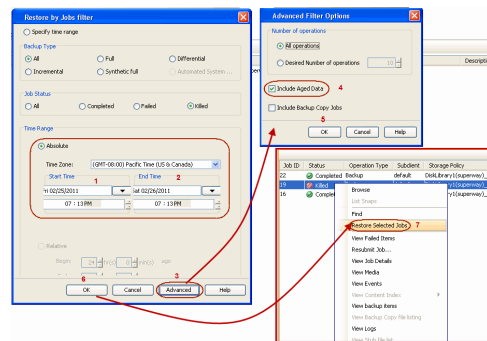
RESUBMITTING A RESTORE JOB

You can rerun a failed or completed restore job. This is useful when you want to use all the options and settings configured for the original job.

Follow the steps given below to rerun a restore job:

1. From the CommCell Browser, navigate to **Client Computers**.

2. Right-click the **<Client>** and click **View | Job History**.

3. Select **Data Recovery**.

4. Select the **Restore** check box and clear all other check boxes.

5. Right-click the restore job that you want to resubmit from the **Data Recovery Job History** tab and click **Resubmit Job**.

6. Click **OK** in the **Restore Options for All Selected Items** dialog box.
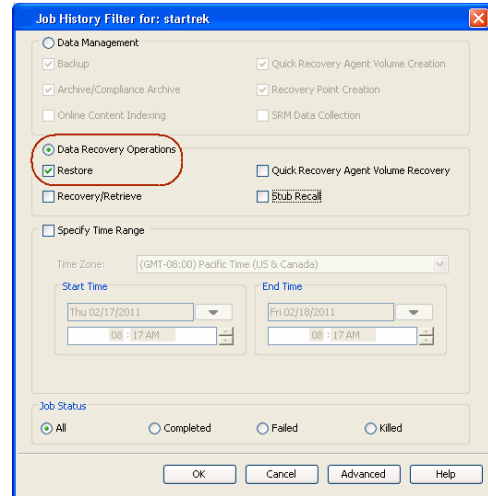
FILTERING DATA FROM RESTORES

During a restore operation, you can specify the files, directories, and file name patterns that you want to filter and exclude from restoring.

1. From the CommCell Browser, navigate to **Client Computers | <*Client*> | File System | <*Backup Set*>**.

2. Right-click the **<*Subclient*>** in the right pane and then click **Browse Backup Data**.

3. Click **OK**.

4. Select the data that you want to restore and click **Recover All Selected**.

5. In the **Recover Options for All Selected Items** dialog box, click **Advanced**.

6. Select the **Paths/Filters** tab.

7. If you want to remove any files or folders from restore operation, click **Add** for **Filter Item** list and enter the path of the data. Wildcard entries must be expressed as complete paths.

   You can also click **Delete** to remove existing source or filter items.

8. In the **Advanced Recover Options** dialog box, click **OK**.

9. In the **Recover Options for All Selected Items** dialog box, click **OK**.
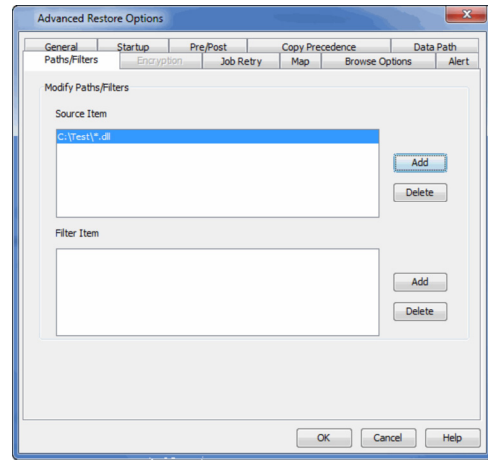
SUPPORTED WILDCARDS IN FILTERS

The following wildcards can be used in filters to include or exclude data when restoring data.

WILDCARD	DEFINITION	EXAMPLE
*	Any number of characters. This wildcard is used in following scenarios: ● filter all files of a specific extension ● filter all files when the file name starts with a specific pattern	`C:\*.log` will filter all files with the .log extension on root of the C drive. If you want to filter files with the `.log` extension from a folder on the C drive, you must include the path to the folder in the filter. (e.g. `C:\Test\*.log`) `ntuser*` will filter all files for which the file name starts with the word `ntuser`.
?	Any one character This wildcard is used in following scenarios: Filter all files (or folders) for which the name begins with a specific word and the last character of the word is variable.	To filter files: `C:\access?.doc` will filter any files with the extension .doc on the C drive for which the name begins with- "`access`" followed by any one character such as `access1.doc` or `access5.doc`. However, `access12.doc` or `access15.doc` will not be filtered because the last two characters in the name are variable. To filter folders: `C:\access?\**\*` will filter any on the C drive for which the name begins with- "`access`" followed by any one character such as `C:\access1` or `C:\access5`. However,

		C:\access12 or C:\access15 will not be filtered because the last two characters in the name are variable.
***	All files under a specific directory	C:\Test\Data*** will filter all files and subdirectories under and including C:\Test\Data C:**\Data*** will filter all files and subdirectories below and including any directory called "Data" at any level in the C: volume G:\Users**\xpprofile*.log will filter all files with the .log extension from any xpprofile subdirectory under Users directory G:\Users**\xpprofile\ntuser* will filter all filenames starting with ntuser from any xpprofile subdirectory under Users directory

RESTORING DATA USING A MAP FILE

You can restore individual files and folders to different locations using a map file containg a list of files to be restored, with their corresponding restore paths.

CREATING A MAP FILE

The map file is a text file in the CSV (Command Separated Value) format. Follow the steps given below to create a map file:

1. Create a text file on the client computer where you want to restore the data.

2. Add the mapping information in the file in the following format:

   "<source path>","<destination path>"

   o If the specified destination folder is not available, the necessary destination folder will be created during the restore.

The specified paths for both the source and destination should be absolute paths within the same client computer. (Computer names or UNC paths should not be used in the source and destination names.)

You can provide following information in a map file:

INFORMATION	EXAMPLE
File to File mapping	"C:\dir1\file1.txt","E:\dir2\file1.txt"
Folder to Folder mappings	"C:\dir2","E:\dir2"
Drive to Drive mappings	"C:\","E:\"
Renaming files/folder	"C:\dir4\file2.txt","F:\dir5\file3.txt"
Filtering files	"C:\dir5",""
File to File mapping with UNC path for source to UNC path for destination When restoring to/from an UNC path, prefix the path with "UNC-NT"	"UNC-NT_Filer\Share\source2","UNC-NT_Filer\Share\destination2"
File to File mapping using UNC path for source	"UNC-NT_Filer\Share\source2","E:\dir2"

ADDING FILES AND FOLDERS WITH UNICODE CHARACTERS TO A MAP FILE

If the path or the filename contains Unicode characters, the Map File must be converted to a format that can be used by the data protection operation. The Unicode Conversion utility must be used to convert the Map File to a format that can be provided as input.

1. Using a text editor, create a file that contains a list of files/folders with Unicode characters. Make sure to save the file as a Unicode text file.

2. From the Command Line, navigate to the <software install folder>/base folder and type the following:

   cvconvertunicode <source file> <destination file>

   Where:

   <source file> is the full path and name of the file created in Step 1.

   <destination file> is the full path and name of the destination file. The file will automatically be created by the utility.

3. Use the destination file as the Map File to perform the restore.

RESTORING USING A MAP FILE

Use the following procedure to restore a list of files and folders from a computer and each of these files have a different destination.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | File System | <Backup Set>**.

2. Right-click the *<Subclient>* in the right pane and then click **Browse Backup Data**.

3. Click **OK**.

4. Select the data that you want to restore and click **Recover All Selected**.

5. Click **Advanced**.

6. Select the **Map** tab.

7. Select the **Use map file** check box and click **Browse** to navigate to the map file.

8. Clear the **Restore unmapped file** check box.

9. In the **Advanced Recover Options** dialog box, click **OK**.

10. Click **OK** to start the restore.
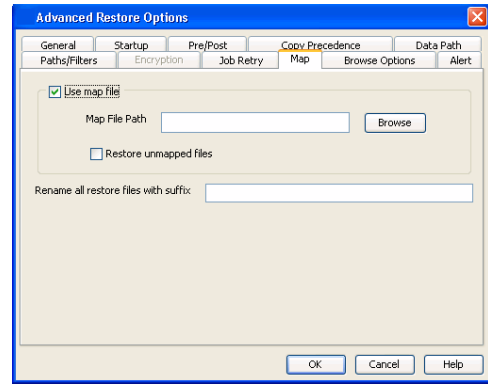
COMBINING BROWSE AND RESTORE WITH THE MAP FILE RESTORE

Use the following procedure to restore a set of files to a specified location with some files within that set to different destinations:

1. From the CommCell Browser, navigate to **Client Computers | *<Client>* | File System | *<Backup Set>*.**

2. Right-click the *<Subclient>* in the right pane and then click **Browse Backup Data**.

3. Click **OK**.

4. Select the data that you want to restore and click **Recover All Selected**.

5. Click **Advanced**.

6. Select the **Map** tab.

7. Select the **Use map file** check box and click **Browse** to navigate to the map file.

8. Select the **Restore unmapped file** check box.

9. In the **Advanced Recover Options** dialog box, click **OK**.

10. In the **Recover Options for All Selected Items** dialog box, click **OK**.

RESTORING DELETED FILES

Follow the steps given below to restore deleted files:

1. From the CommCell Browser, navigate to **Client Computers | *<Client>* | File System | *<Backup Set>*.**

2. Right-click the *<Subclient>* in the right pane and then click **Browse Backup Data**.

3. Click **OK**.

4. Select the data that you want to restore and click **Recover All Selected**.

5. Click **Advanced**.

6. Select the **Browse Options** tab**.**

7. Select the **Restore deleted items** check box and then select the **Specify Time Range** check box.

8. Select the time range to restore the files, deleted in that period of time.

9. In the **Advanced Recover Options** dialog box, click **OK**.

10. In the **Recover Options for All Selected Items** dialog box, click **OK**.

SETTING UP PRE-POST PROCESSES

You can run batch files or shell scripts before and/or after restore jobs. Follow the steps given below to setup a process before or after the restore job:

1. From the CommCell Browser, navigate to **Client Computers | *<Client>* | File System | *<Backup Set>*.**

2. Right-click the *<Subclient>* in the right pane and then click **Browse Backup Data**.

3. Click **OK**.

4. Select the data that you want to restore and click **Recover All Selected**.

5. Click **Advanced** and then click the **Pre/Post** tab.

6. If you want perform a process before the restore job, enter the path for the batch file in the **Pre Recovery Command** box or click **Browse** to select the batch file.

7. If you want perform a process after the restore job, enter the path for the batch file in the **Post Recovery Command** box or click **Browse** to select the batch file.

8. Select one of the following options:
   - ○ **Use Local Accounts** - Select this option if the local account has permissions to execute the processes on the destination client.
   - ○ **Impersonate User** - Select this option and enter the username and password, that has the permissions to execute the processes on the destination client.

9. Click **OK**.

10. Click **OK** to start the restore.
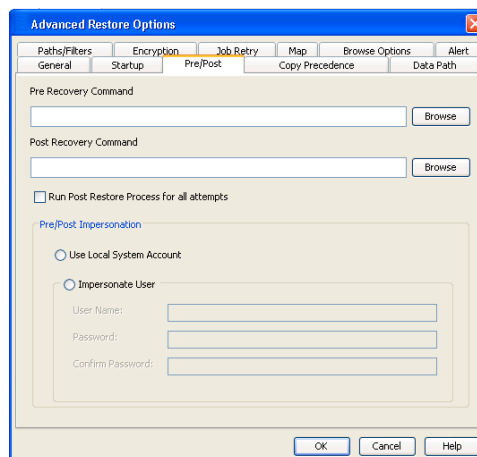
SETTING UP A PRE/POST PROCESS TO RUN AFTER EACH ATTEMPT

By default, a specified post process command is executed only on successful completion of the restore operation.
Use the following steps to run a post process even if the restore operation did not complete successfully. For example, this may be useful to bring a database online or release a snapshot.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | File System | <Backup Set>**.

2. Right-click the **<Subclient>** in the right pane and then click **Browse Backup Data**.
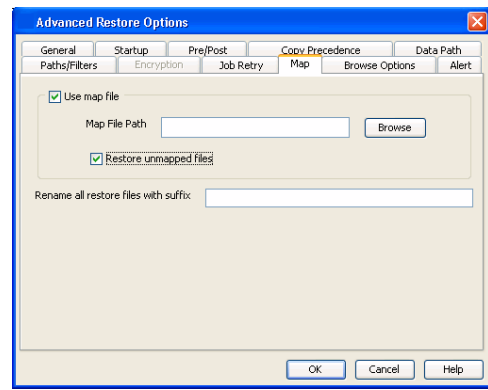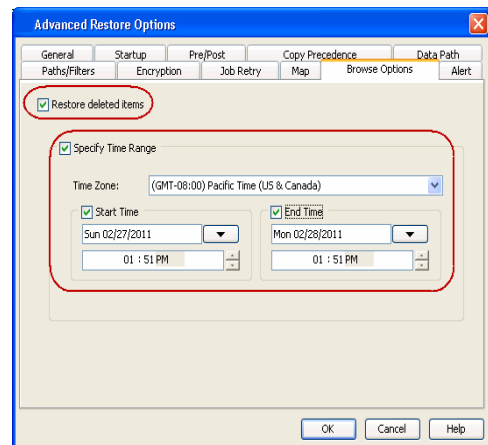
3. Click **OK**.

4. Select the data that you want to restore and click **Recover All Selected**.

5. Click **Advanced** and then click the **Pre/Post** tab.

6. Enter the path for the batch file in the **Post Recovery Command** box or click **Browse** to select the batch file.

7. Select the **Run Post Process for all attempts** check box.

8. Click **OK**.

9. Click **OK** to start the restore.
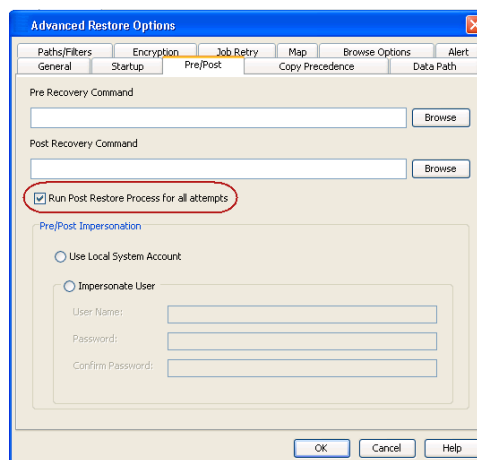
RESTORING THE FULL SYSTEM

You can restore any one or all of the following components during full system restore:

- File System
- System State
- Office Communications Server

Before performing a full system restore, make sure that the backup jobs are disabled for the client so that any scheduled backups for the client will not start until the full system backup is complete.

1. Open the CommCell Console.

2. From the CommCell Browser, right-click the **<Client>** and select **Properties**.

3. Click the **Activity Control** tab.

4. Clear the **Enable Data Management** check box. This will disable backup jobs for the client and any scheduled backup jobs for the client will not start during the full system restore.

5. Click **OK.**

6. From the CommCell Browser, navigate to **Client Computers| <Client> | File System**.

7. Right-click the **<Backupset>** that contains the system state data and all the drives and then click **Browse Backup Data**.

8. Select the required options from the **Browse Options** dialog box and click **OK**.

9. Select the **<BackupSet>** box from the **Client Browse** tab which contains system state data and all the drives.

10. Click **Recover All Selected**.

For more information on Full System Restore on a Non Domain Controller, see Full System Restore of Non-Domain Controller.

For more information on Full System Restore of a Domain Controller on Windows Server 2003 and 2008, see Full System Restore of a Domain Controller on Windows Server 2003 and Full System Restore of a Domain Controller on Windows Server 2008 respectively.

RESTORING THE SYSTEM STATE

System State components can be restored as follows:

SYSTEM STATE CATEGORY	COMPONENTS	TYPE OF RESTORE
COMPONENTS	System File Protection catalog and files Performance monitor configuration files Active Directory Quotas SYSVOL (if this is a domain controller) Certificate Services database (if this is a certificate server) Cluster database (if this server is part of a cluster) Registry COM+ database 1-Touch component	• You can do an in-place and out-of place restore of all components together. • Individual components can only be restored out-of-place. • 1-Touch component will be used to perform 1-Touch Recovery. You cannot perform the Direct Restore or Browse and Restore of 1-Touch component.
SERVICES	DHCP WINS Event logs Disk quota information RSM database WMI database Terminal Server Licensing database Content Indexing catalogs	• All services except Content Indexing Catalogs can be restored together or individually in place or out of place. • Content Indexing Catalog service will be included when you restore the entire system state but cannot be restored individually.

PREREQUISITES

• Install Microsoft .NET Framework 3.5 and 4 on the client computer. This is not required if the client computer has Windows 2003 or Windows XP.

• If you have excluded any critical system state component from the backup, you cannot use that backup for the system restore. Ensure that the following critical system state components are not excluded from the backup:

Registry

System Protected Files

Active Directory

Cluster DB

Sysvol (For 2000 or 2003 domain controllers level)

DFSR (Windows 2008 Domain controller level)

RESTORE THE SYSTEM STATE IN-PLACE

Before performing the system state restore ensure that the service user is a local administrator or services are running on a local system.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | File System | defaultBackupSet** .

2. Right-click the default subclient in the right pane and then click **Browse Backup Data**.

3. Click **OK** in the **Browse Options** dialog box.

4. Expand the items in the **defaultBackupSet** in the left pane of the **Client Browse**
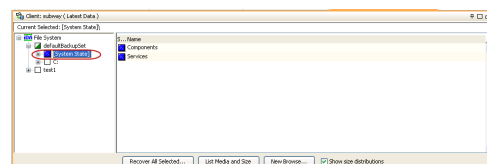
tab and click the **System State** box.

5. Click **Recover All Selected**.

6. Click **OK**.

RESTORE THE SYSTEM STATE OUT-OF-PLACE

You can perform an out-of-place restore of the following entities in system state:

- SYSVOL to restore deleted group policy objects (GPOs) back to the Active Directory server without having to do a full system restore.

- Registry hives. This can be helpful if the server has crashed and you need a version of the registry. Once these hives are restored, you can manually replace the hives that exist on your server. You can also load them into the registry to view the contents before replacing them on server.

- IIS metabase file to repair a IIS server using Microsoft procedures.

  These methods require advanced skills. Be sure to visit the Microsoft support website and look for articles that describe these methods in more detail.

1. From the CommCell Browser, navigate to **Client Computers |** *<Client>*.

2. Right-click the backup set that includes the system state, click **All Tasks** and then click **Browse Backup Data**.

3. Click **OK**.

4. Expand the items for the backup set in the left side of the **Client Browse** tab.

5. Click the **System State** box on the left.

6. Click **Recover All Selected**.

7. If you want to restore the data to another client, select the client from **Destination client** list. The source client and destination client must reside in the same CommCell.

8. Clear the **Restore to same folder** option.

9. Enter the destination path in the **Specify destination path** box.

   Optionally, click **Browse** to browse and select the path.

10. Click **OK**.
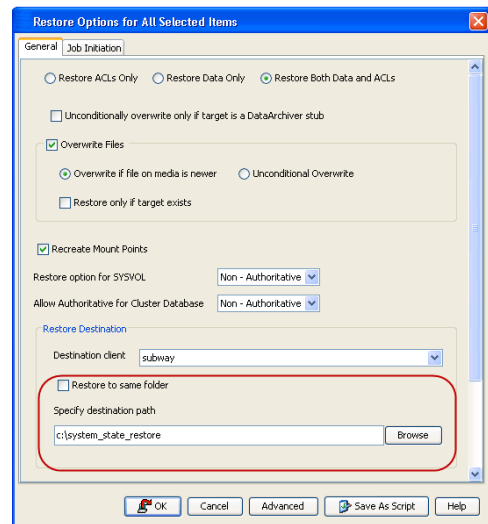
RESTORE SPECIFIC SYSTEM STATE OBJECTS

Follow the steps given below to restore individual system state components:

1. From the CommCell Browser, navigate to *<Client>*.

2. Right-click the backup set that includes the system state, click **All Tasks | Browse Backup Data**.

3. Click **OK**.

4. Expand the items for the backup set in the left side of the **Client Browse** tab.

5. In the left pane, expand **[System State]** to display the two main objects: Components, Services.

6. Select the Components and Services that you want to restore from the right pane of the **Client Browse** tab.

7. Click **Recover All Selected**.

8. If you want to restore the data to another client, select the client from the **Destination client** list. The source client and destination client must reside in the same CommCell.

9. Clear the **Restore to same folder** option.

10. Enter the destination path in the **Specify destination path** box.

    Optionally click the **Browse** button to browse and select the path.

11. Click **OK**.
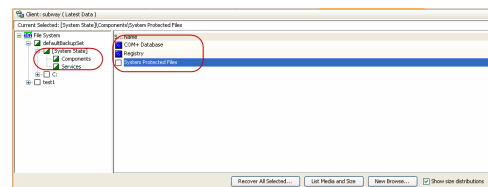
RESTORING OFFICE COMMUNICATIONS SERVER DATA (OCS)

Follow the steps given below to restore OCS Data and Settings:

1. From the CommCell Browser, navigate to **Client Computers | <*Client*> | File System | <Backup Set>** .

2. Right-click the subclient in the right pane and then click **Browse Backup Data**.

3. Click **OK** in the **Browse Options** dialog box.

4. Right-click the subclient, that contains the OCS data and settings, from the right pane and click **Browse Backup Data**.

5. Select the OCS data and settings to be restored and click **Recover all Selected.**

6. In the **Recover Options for All Selected Items** dialog box, select the client from the **Destination client** list and specify the **Destination path**.

7. Click **OK**.
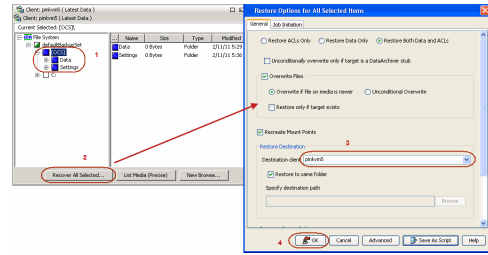
OCS metadata is backed up and restored with the SQL Server *i*DataAgent.

RESTORING ACLS

The ACLs are restored by default when you restore a data. You can choose to restore only the data or the ACLs.

RESTORING ONLY THE ACLS

You can restore only the ACLs and apply it to an existing data in the destination. Follow the steps given below to restore only the ACLs and apply it to the existing files in the destination:

1. From the CommCell Browser, navigate to **Client Computers | <*Client*> | File System | <Backup Set>**.

2. Right-click the **<Subclient>** in the right pane and then click **Browse Backup Data**.

3. Click **OK**.

4. Select the data that you want to restore and click **Recover All Selected**.

5. Select **Restore ACLs Only**.

6. Click **OK**.
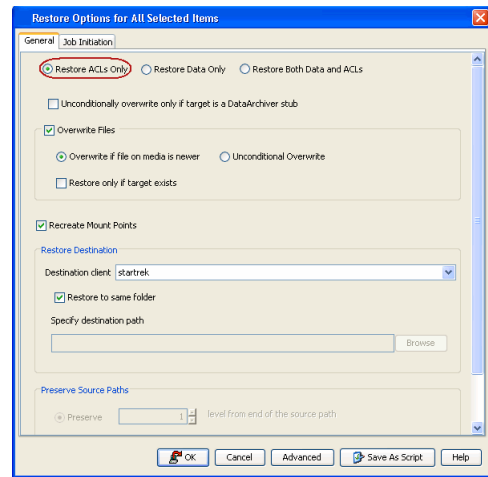
RESTORING ONLY THE DATA

You can restore only the data and inherit permissions from the parent directory in the destination. Follow the steps given below to restore only the data, without restoring the ACLs:

1. From the CommCell Browser, navigate to **Client Computers | <*Client*> | File System | <Backup Set>**.

2. Right-click the **<Subclient>** in the right pane and then click **Browse Backup Data**.

3. Click **OK**.

4. Select the data that you want to restore and click **Recover All Selected**.

5. Select **Restore Data Only**.

6. Click **OK**.
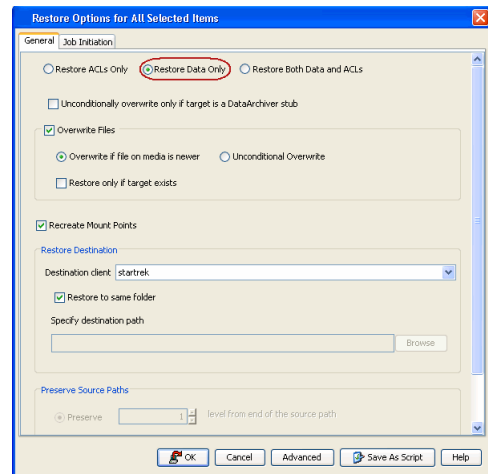
RESTORING VIRTUAL MACHINES

Data secured by the Windows File System iDataAgent can be restored to a virtual machine running Windows.

MICROSOFT VIRTUAL SERVER

To restore virtual machines on Microsoft Virtual Server using the Windows File System iDataAgent:

1. Shut down the virtual machine(s).

2. Remove the virtual machine(s) using the Virtual Server Web admin utility.

3. Remove the configuration files from the virtual machine directories.

4. Restore all files for each virtual machine backup to that machine's virtual machines configuration directory. (The directory with the machine DNS name can be restored in place.)

5. Using the Virtual Server Web admin utility, add a virtual machine. Use the full path for the `vmc` file of the machine you want to restore.

6. Select the option to **restore from saved state**.

The virtual machine(s) should restore and display as `running`.

MICROSOFT HYPER-V

To restore virtual machines on Microsoft Hyper-V using the Windows File System iDataAgent:

1. Shut down the virtual machine(s).

2. From the command prompt, run **net stop vmms**. You can also run this as a batch job in a PreRestore Process in the **Advanced Restore Option** dialog box.

3. Browse the backed up data and select the VM to be restored.

4. Run an in-place restore using the **Unconditional Overwrite** option.

5. From the command prompt, run **net start vmms**. You can also run this as a batch job in a PostRestore Process in the **Advanced Restore Option** dialog box.

6. Select the restored virtual machine in the Hyper-V Manager.

7. Select the **Start** option of the virtual machine.

The virtual machine(s) should restore and display as `running`.

LISTING MEDIA

Before restoring any file or folder, you can review all the media that is associated with the selected data. Use this option to ensure that the media required to restore the selected data is available. You can also predict the total size of the data that you want to restore. Follow the steps given below to display the media and the size:

See List Media comprehensive information on media management and prediction.

1. From the CommCell Browser, navigate to **Client Computers | <Client> | File System**

2. Right-click a Backup Set and click **All Tasks | Browse/Browse Backup Data**.

4. Click **OK**.

5. Select the data that you want to restore and click **List Media and Size**.

6. Click **OK**.

The media associated with the selected data is displayed. If required, you can recall the required media from the export location.
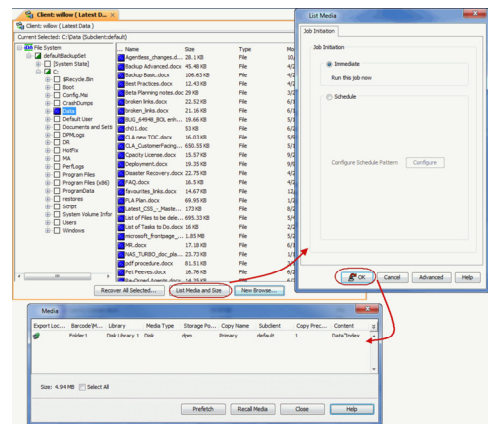
COMMAND LINE RESTORES

You can restore file system data from the command line interface.

Command line restores enable you to perform restore operations on multiple clients at the same time. It also allows you to reuse the command line scripts for additional restores.

When performing command line restores, note that backups taken from the CommCell Console can be restored using Command Line and vice versa. However, backups taken from a previous version of the CommCell Console can be restored only from the Command Line.

In order to run the restores from command line, you need an input xml file which contains the parameters for configuring the restore options. This input xml file can be obtained using one of the following ways:

● Download the input xml file template and save it on the computer from where the restore will be performed.

● Generate the input xml file from the CommCell Console and save it on the computer from where the restore will be performed.

LOG ON TO THE COMMSERVE

To run command line operations you must first login to the CommServe as follows:

● From Command prompt, navigate to <Software_Installation_Directory>/Base and run the following command:

```
qlogin -cs <commserve name> -u <user name>
```

● For example, to log on to CommServe 'server1' with username 'user1':

```
qlogin -cs server1 -u user1
```

PERFORM THE RESTORE

1. Download the restore_template.xml file and save it on the computer from where the command will be executed.

2. Execute the saved xml script using qoperation execute command.

   ```
   qoperation execute -af restore_template.xml -appName 'File System' -clientName xxxxx -backupsetName xxxxx -destPath
   'xxxxx' -sourceItem 'xxxxx'
   ```

3. Verify the status of the job using the following command:

   ```
   qlist job -j JOBID
   ```

4. Once the job completes, logout from the CommServe using the qlogout command.

   ```
   qlogout [-cs commserver] [-all] [-tf tokenfile] [-tk token] [-h]
   ```

EXAMPLES

Restoring from a Current Backup	qoperation execute -af restore_template.xml -appName 'File System' -clientName client1 -backupsetName backupset1 -destPath 'C:\temp' -sourceItem 'C:\test'
Restoring Files to a Point in Time (date)	qoperation execute -af restore_template.xml -appName 'File System' -clientName client1 -backupsetName backupset1 -destPath 'C:\temp' -sourceItem 'C:\test' -toTimeValue 2011-11-28
Restoring Files to a Point in Time (date and time)	qoperation execute -af restore_template.xml -appName 'File System' -clientName client1 -backupsetName backupset1 -destPath 'C:\temp' -sourceItem 'C:\test' -toTimeValue 2011-11-28 15:40:00
Restoring by Jobs	qoperation execute -af restore_by_job_template.xml -jobids 52 -sourceItem 2:52 -striplevel 1 where: ● jobids is the backup job ID ● sourceItem is the CommCell D and the backup job ID separated by a colon (':'). By default, the CommCell ID is 2. ● striplevel is the number of folder levels to exclude from the source path. This parameter is optional. For example, if you have a directory structure (source path) as /a/b/c and you select strip level 2, the data will be restored from folder c, while folders a and b are excluded. Ensure that the strip level is always less than the source path level.

GENERATE THE COMMAND LINE SCRIPT FROM THE COMMCELL CONSOLE

In addition to the parameters provided in the template xml file, if you want to include additional options for the restore, you can do so by selecting the required options from the CommCell Console and generate the command line xml script for the restore operation.

Follow the steps given below to generate a script which you can use to perform a restore from the command line interface:

1. From the CommCell Browser, navigate to **Client Computers | <Client> | File System | <Backup Set>**.

2. Right-click the **<Subclient>** in the right pane and then click **Browse Backup Data**.

3. Click **OK**.

4. In the right pane of the Browse window, select the data that you want to restore and click **Recover All Selected**.

5. Select the required restore options which you want to execute using the script.

6. Click **Save as Script**.
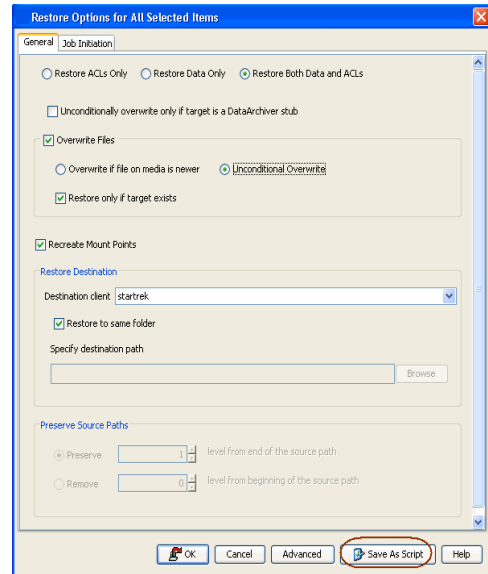
7. Enter the location where you want to save the script or click **Browse** and navigate to the location.

   The script will be saved as a .xml file and a .bat file is created.

   If a file with the same name already exists in the specified location, the .xml file will be created with a timestamp. However, the .bat file will overwrite the existing file.

8. Enter the username and password for the user account which you want to use to perform the restore.

   By default, the user account which you have used to login to CommCell console is used for performing the restore. However, if the user account does not have access to application and database, click **Use a different account**.

9. Click **OK**.
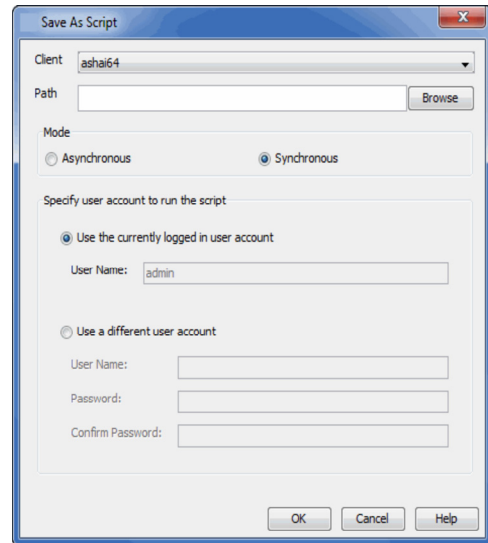
SCHEDULING A RESTORE

Follow the steps given below to schedule a restore job:

1.
- From the CommCell Console, navigate to **Client Computers** | **<client> | File System**.
- Right-click an backupset and click **All Tasks** | **Browse Backup Data**.
- Click **OK**.

2.
- Select a file to restore.
- Click **Recover All Selected**.
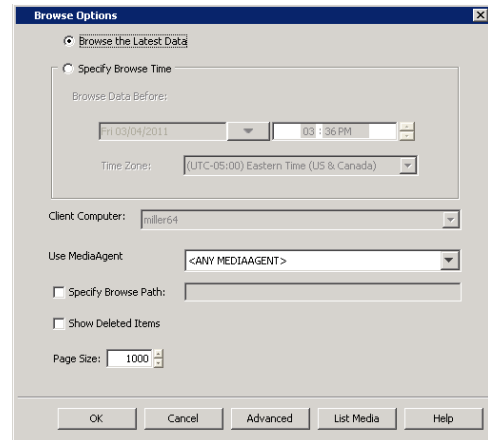
3. Select the name of the client computer from the **Destination Client** list.

Click **OK**.
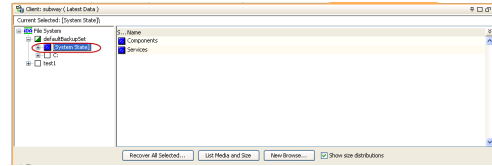
4.
- Click **Job Initiation** tab and click **Schedule**.
- Click **Configure**.
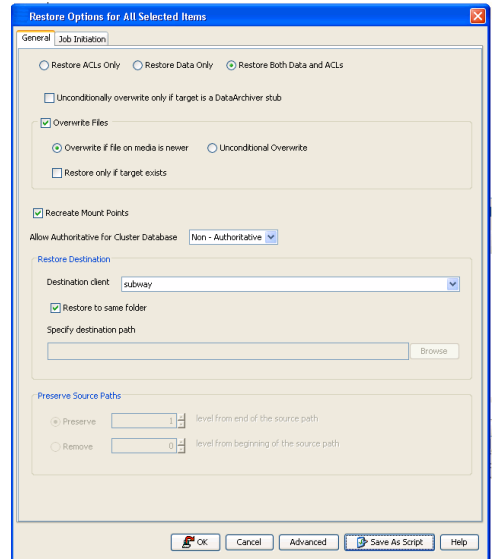
5. Select the appropriate scheduling options. For example:
- Click **Weekly**.
- Check the days you want the run the restore job.
- Change the Start Time to 9:00 PM
- Click **OK** to close the Schedule Details dialog
- Click **OK** to close the Restore Options dialog

The restore job will execute as per the schedule.
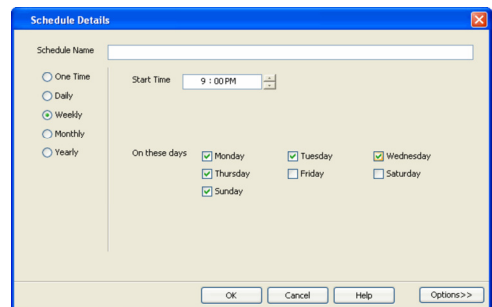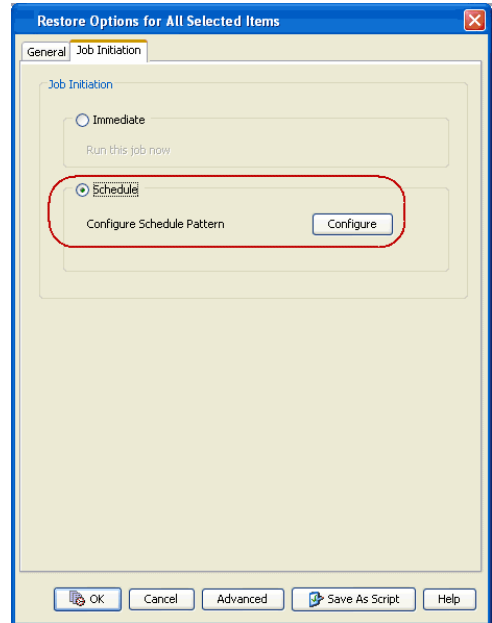
See Scheduling for a comprehensive information on scheduling jobs.

MANAGING RESTORE JOBS

Once you initiate the restore operation, a restore job is generated in the Job Controller. Jobs can be managed in a number of ways. See Job Management for a comprehensive information on managing jobs.

The following sections provide information on the different job management options available:

RESTARTING JOBS

Jobs that fail to complete successfully are automatically restarted based on the job restartability configuration set in the Control Panel. Keep in mind that changes made to this configuration will affect all jobs in the entire CommCell.

To Configure the job restartability for a specific job, you can modify the retry settings for the job. This will override the setting in the Control Panel. It is also possible to override the default CommServe configuration for individual jobs by configuring retry settings when initiating the job. This configuration, however, will apply only to the specific job.

> Backup jobs for this Agent are resumed from the point-of-failure.

CONFIGURE JOB RESTARTABILITY AT THE COMMSERVE LEVEL

1. From the CommCell Browser, click **Control Panel** icon.

2. Select **Job Management.**

3. Click **Job Restarts** tab and select a **Job Type.**
   - Select **Restartable** to make the job restartable.
   - Change the value for **Max Restarts** to change the maximum number of times the Job Manager will try to restart a job.
   - Change the value for **Restart Interval (Mins)** to change the time interval between attempts for the Job Manager to restart the job.

4. Click **OK.**

CONFIGURE JOB RESTARTABILITY FOR AN INDIVIDUAL JOB

1. From the CommCell Browser, navigate to **Client Computers | <Client> | File System | <Backup Set>**.

2. Right-click the **<Subclient>** in the right pane and then click **Browse Backup Data**.

3. Click **OK**.

4. Select the data that you want to restore and click **Recover All Selected**.

5. Click **Advanced** and select the **Job Retry** tab

6. Select **Enable Total Running Time** and specify the maximum elapsed time before a job can be restarted or killed

   Select **Kill Running Jobs When Total Running Time Expires** to kill the job after reaching the maximum elapsed time.

7. Select **Enable Number Of Retries** and specify the number of retries.

8. Click **OK.**

CONTROLLING JOBS

The following controls are available for running jobs in the Job Controller window:

SUSPEND	Temporarily stops a job. A suspended job is not terminated; it can be restarted at a later time.
RESUME	Resumes a job and returns the status to Waiting, Pending, Queued, or Running. The status depends on the availability of resources, the state of the Operation Windows, or the Activity Control setting.
KILL	Terminates a job.

SUSPENDING A JOB

1. From the Job Controller of the CommCell Console, right-click the job and select **Suspend**.

2. The job status may change to **Suspend Pending** for a few moments while the operation completes. The job status then changes to **Suspended.**

RESUMING A JOB

1. From the Job Controller of the CommCell Console, right-click the job and select **Resume**.

2. As the Job Manager attempts to restart the job, the job status changes to **Waiting**, **Pending**, or **Running**.

KILLING A JOB

1. From the Job Controller of the CommCell Console, right-click the job and select **Kill**.

2. Click **Yes** when the confirmation prompt appears if you are sure you want to kill the job. The job status may change to **Kill Pending** for a few moments while the operation completes. Once completed, the job status will change to **Killed** and it will be removed from the Job Controller window after five minutes.

ADDITIONAL RESTORE OPTIONS

The following table describes the available additional options to further refine your restore operations:

OPTION	DESCRIPTION	RELATED TOPIC
Skip Errors and Continue	This option enables you to to continue the restore job regardless of media errors and create a file that lists the full path names of the files that failed to get restored. Follow the steps given below to set this option: 1. From the CommCell Browser, click **Client Computers** | **File System**. 2. Right-click the <**Backup set**> that contains the data you want to restore, point to **All Tasks** and then click **Browse Backup Data**. 3. In the **Browse Options** dialog box, click **OK**. 4. In the **Client Browse** tab, select the data to be restored and click **Recover all Selected.** 5. In the **Restore Options for All Selected Items** dialog box, click **Advanced**. 6. In the **Advanced Restore Options** dialog box, click **General**. 7. On the **General** tab, select the **Skip errors and continue** check box. 8. Click **OK**.	
Use Exact index	This option enables you to use the index associated with the data protection operation performed at a specific time or the latest index. By default, the system uses the index associated with the most recent data protection operation when your Browse the data. This option allows you to associate the media with the most recent index available in the CommCell. Follow the steps give below to use exact index: 1. From the CommCell Browser, click **Client Computers** | **File System**. 2. Right-click the <**Backup set**> that contains the data you want to restore, point to **All Tasks** and then click **Browse Backup Data**. 3. In the **Browse Options** dialog box, click **OK**. 4. In the **Client Browse** tab, select the data to be restored and click **Recover all Selected.** 5. In the **Restore Options for All Selected Items** dialog box, click **Advanced**. 6. In the **Advanced Restore Options** dialog box, click **General**. 7. On the **General** tab, select the **Use Exact Index** check box. 8. Click **OK**.	
Startup Options	The Startup Options are used by the Job Manager to set priority for resource allocation. This is useful to give higher priority to certain jobs. You can set the priority as follows: 1. From the CommCell Browser, click **Client Computers** | **File System**. 2. Right-click the <**Backup set**> that contains the data you want to restore, point to **All Tasks** and then click **Browse Backup Data**. 3. In the **Browse Options** dialog box, click **OK**. 4. In the **Client Browse** tab, select the data to be restored and click **Recover all Selected.** 5. In the **Restore Options for All Selected Items** dialog box, click **Advanced**. 6. In the **Advanced Restore Options** dialog box, click **Startup**. 7. On the **Startup** tab, select **Change Priority**.	Refer to Job Priority and Priority Precedence.

	8. Enter a priority number - 0 is the highest priority and 999 is the lowest priority.	
	9. Select the **Start up in suspended State** check box to start the job in a suspended state.	
	10. Click **OK**.	
Copy Precedence	By default, the system retrieves data from the storage policy copy with the lowest copy precedence. If the data was pruned from the primary copy, the system automatically retrieves data from the other copies of the storage policy in the lowest copy precedence to highest copy precedence order. Once the data is found, it is retrieved, and no further copies are checked.	Refer to Recovering Data From Copies.
	You can retrieve data from a specific storage policy copy (Synchronous Copy or Selective Copy). If data does not exist in the specified copy, the data retrieve operation fails even if the data exists in another copy of the same storage policy. Follow the steps given below to retrieve the data from a a specific storage policy copy:	
	1. From the CommCell Browser, click **Client Computers**	**File System**.	
	2. Right-click the <**Backup set**> that contains the data you want to restore, point to **All Tasks** and then click **Browse Backup Data**.	
	3. In the **Browse Options** dialog box, click **OK**.	
	4. In the **Client Browse** tab, select the data to be restored and click **Recover all Selected.**	
	5. In the **Restore Options for All Selected Items** dialog box, click **Advanced**.	
	6. In the **Advanced Restore Options** dialog box, click **Copy Precedence**.	
	7. On the **Copy Precedence** tab, select the **Restore from copy precedence** check box.	
	8. Enter the copy precedence number.	
	9. Click **OK**.	
Data Path Options	The data recovery operations use a default Library, MediaAgent, Drive Pool, and Drive as the Data Path. You can use this option to change the data path if the default data path is not available. Follow the steps given below to change the default data path:	Refer to Change Data Path.
	1. From the CommCell Browser, click **Client Computers**	**File System**.	
	2. Right-click the <**Backup set**> that contains the data you want to restore, point to **All Tasks** and then click **Browse Backup Data**.	
	3. In the **Browse Options** dialog box, click **OK**.	
	4. In the **Client Browse** tab, select the data to be restored and click **Recover all Selected.**	
	5. In the **Restore Options for All Selected Items** dialog box, click **Advanced**.	
	6. In the **Advanced Restore Options** dialog box, click **Data Path**.	
	7. On the **Data Path** tab, select the **MediaAgent** and **Library**.	
	8. Select the **Drive Pool** and **Drive** for optical and tape libraries.	
	9. Select the name of the **Proxy** server if you wish to restore using a proxy server.	
	You can select the Proxy server only when you are restoring from a snapshot. This option is not available for a regular restore.	
	10. Click **OK**.	
Encryption	If the client's data is encrypted with a pass phrase, you must enter the pass-phrase to start the data recovery operation. Follow the steps given below to enter the pass-phrase:	Refer to Data Encryption.
	1. From the CommCell Browser, click **Client Computers**	**File System**.	
	2. Right-click the <**Backup set**> that contains the data you want to restore, point to **All Tasks** and then click **Browse Backup Data**.	
	3. In the **Browse Options** dialog box, click **OK**.	
	4. In the **Client Browse** tab, select the data to be restored and click **Recover all Selected.**	
	5. In the **Restore Options for All Selected Items** dialog box, click **Advanced**.	
	6. In the **Advanced Restore Options** dialog box, click **Encryption**.	
	7. Enter the Pass Phrase.	
	8. Click **OK**.	
Alerts	This option enables users or user groups to get automatic notification on the status of the data recovery job. Follow the steps given below to set up the criteria to raise notifications/alerts:	Refer to Alert.
	1. From the CommCell Browser, click **Client Computers**	**File System**.	
	2. Right-click the <**Backup set**> that contains the data you want to restore, point to **All Tasks** and then click **Browse Backup Data**.	

	3. In the **Browse Options** dialog box, click **OK**. 4. In the **Client Browse** tab, select the data to be restored and click **Recover all Selected.** 5. In the **Restore Options for All Selected Items** dialog box, click **Advanced**. 6. In the **Advanced Restore Options** dialog box, click **Alerts**. 7. Click **Add Alert.** 8. From the **Add Alert Wizard** dialog box, select the required threshold and notification criteria and click **Next**. 9. Select the required notification types and click **Next**. 10. Select the recipients and click **Next**. 11. Click **Finish**. 12. Click **OK**.	
Command Line Restores	Command Line Interface enables you to perform backups or restore from the command line. The commands can be executed from the command line or can be integrated into scripts. You can also generate command line scripts for specific operations from the CommCell Browser using the **Save As Script** option.	Refer to Command Line Interface.
CommCell Readiness Report	The CommCell Readiness Report provides you with vital information, such as connectivity and readiness of the Client, MediaAgent and CommServe. It is useful to run this report before performing the data protection or recovery job. Follow the steps given below to generate the report: 1. From the **Tools** menu in the CommCell Console, click **Reports**. 2. Navigate to **Reports | CommServe | CommCell Readiness**. 3. Click the **Client** tab and click the **Modify** button. 4. In the **Select Computers** dialog box, clear the **Include All Client Computers and All Client Groups** check box. 5. Select the client from the **Exclude** list. 6. Click the **Include >** button. 7. Click **OK**. 8. Click the **MediaAgent** tab. 9. Clear the **Include All MediaAgents** checkbox. 10. Select the MediaAgent from the **Exclude** list. 11. Click **Include >**. 12. Click **Run**. The generated report is displayed.	Refer to CommCell Readiness Report.
Restore Job Summary Report	The Restore Job Summary Report provides you with information about all the data recovery jobs that are run in last 24 hours for a specific client and agent. You can get information such as failure reason, failed objects, job options etc. It is useful to run this report after performing the restore. Follow the steps given below to generate the report: 1. From the **Tools** menu in the CommCell Console, click **Reports**. 2. Navigate to **Reports | Jobs | Job Summary**. 3. Click **Data Recovery** on the **General tab** in the right pane. 4. On the **Computers** tab, select the client and the agent for which you want to run the report. 5. Click **Run**.	Refer to Restore Job Summary Report.

Data Aging - Microsoft Windows File System *i*DataAgent

TABLE OF CONTENTS

Getting Started

**Extended Retention Rules**

GETTING STARTED

Data Aging is the process of removing old data from secondary storage to allow the associated media to be reused for future backups.

By default, all backup data is retained infinitely. However, you should change the retention of your data based on your needs. Note that if you continue to have infinite retention, you will also need infinite storage capacity.

1. From the CommCell Browser, navigate to **Policies | Storage Policies**.
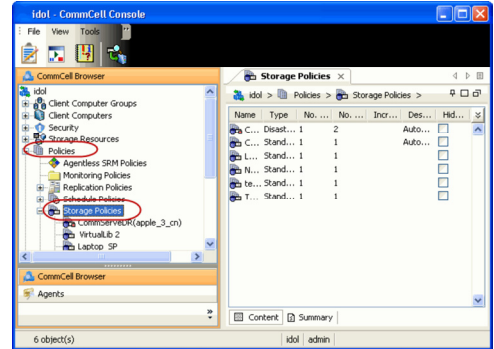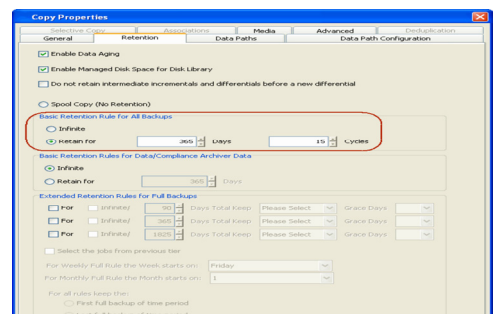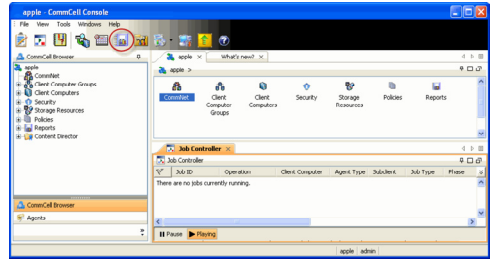
2. Highlight the **Storage Policy**.
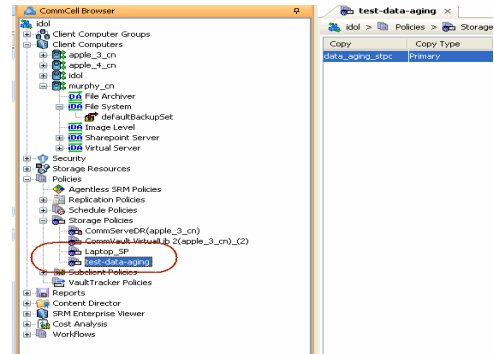
3. From the right pane, right-click the **Storage Policy Copy** and click the **Properties**.
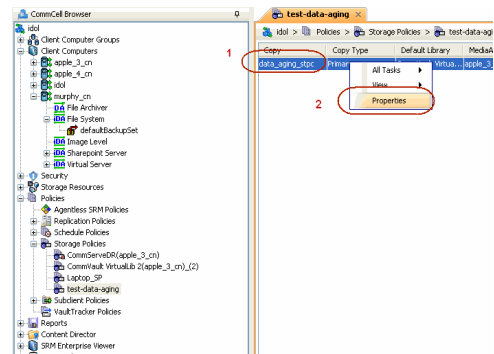
4.
- Click the **Retention** tab.
- Click the **Retain For** in the **Basic Retention Rules for All Backups** area.
- Enter number of days to retain the data.
- Enter number of cycles to retain the data.
- Click **OK**.

5.

From the CommCell Browser, click the **Reports** icon.

6.

Expand Reports and select **Data Retention Forecast and Compliance.**
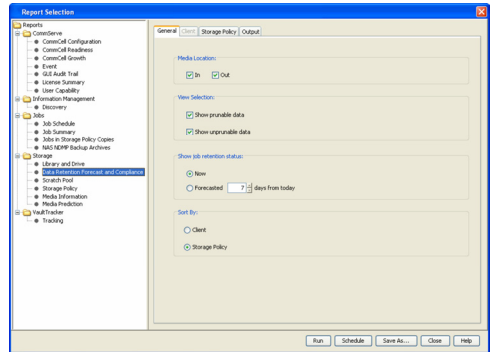
7.

Click **Run**.
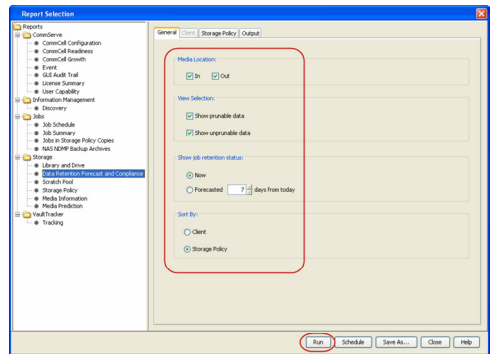
8.

The report will display the data to be pruned when a data aging job is run.

> To ensure only data intended for aging is actually aged, it is important to identify the data that will be aged based on the retention rules you have configured. Hence, ensure this report includes only the data you intend to age.
>
> If necessary, fine-tune your rules so that only the intended data is aged.
>
> Once you run a data aging job, the data will be lost.

Data Retention Forecast and Compliance Report
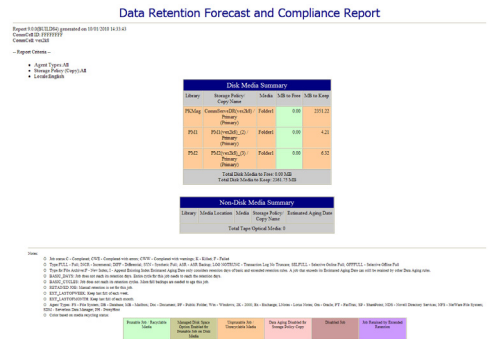
9.

From the CommCell Console, right click the CommServe icon and click **All Tasks | Data Aging**.
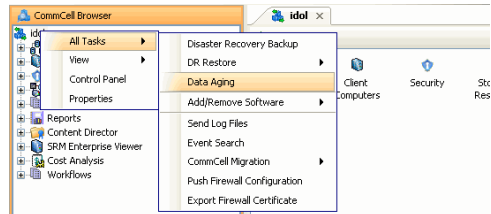
10.

Select **Immediate** in the Job Initiation section and click **OK**.
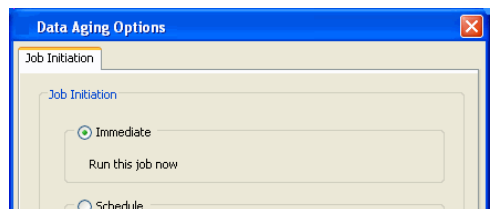
11. You can track the progress of the job from the **Job Controller** window. When the job has completed, the Job Controller displays **Completed**.

Make sure that the job completes successfully. If the job did not complete successfully, re-run the job.
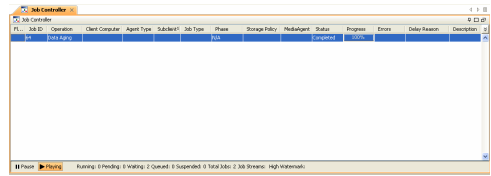
EXTENDED RETENTION RULES

Extended retention rules allow you to keep specific full (or synthetic full) backups for longer periods of time.

Extended retention rules can be used in the following circumstances:

● If you have a single drive tape library

● If you want to create a hierarchical retention scheme (grandfather-father-son tape rotation)

In all other cases, it is recommended that the Auxiliary Copy feature be used for extended storage as it actually creates another physical copy of the data, thereby reducing the risk of data loss due to media failure.

UNDERSTANDING EXTENDED RETENTION RULES

Extended retention allows you to retain a specific full (or synthetic full) backup for an additional period of time. For example, you may want to retain your monthly full backups for 90 days.

Extended retention rules allow you to define three additional "extended" retention periods for full (or synthetic full) backups. For example:

● You may want to retain your weekly full backups for 30 days.

● You may want to retain your monthly full backup for 90 days.

● You may want to retain your yearly full backup for 365 days.

A backup job will be selected for extended retention based on its start time. For example: If a backup job starts at 11:55 pm on August 31st and ends at 1 am on September 1st, then it will be selected as the last full backup for the month of August and will be picked up for extended retention.

SETTING UP EXTENDED RETENTION RULES

Use the following steps for setting up the extended retention rules:

1. Right-click the storage policy copy and click **Properties**.

2. Click the **Retention** tab.

3. Set the basic retention rules by clicking **Retain for** and entering the number of days and cycles appropriate for your organization.

4. Set the extended retention rules as follows:

   Click the **For** button.

   Enter the number of **Days Total** to retain the backup.

   Click the **Keep** drop-down list, and select the desired backup criteria (e.g., Monthly Full).

   Click the **Grace Days** drop-down list and select the number of days (e.g., 2).

5. Repeat Step 4 to configure additional extended retention.

6. Click **OK**.
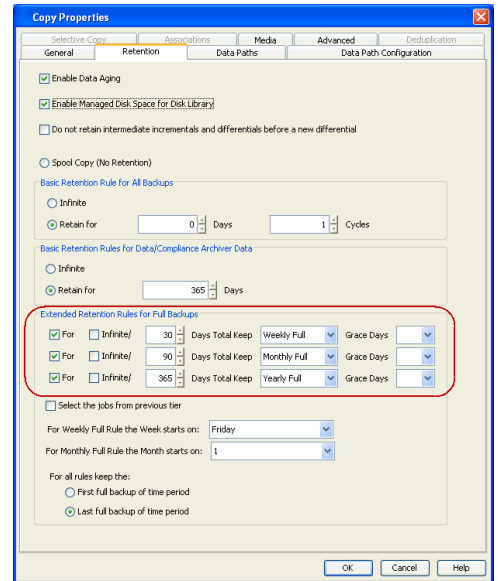
ADVANCED TOPICS

Data Aging - Advanced
Provides comprehensive information on additional Data Aging capabilities.

Disaster Recovery - Windows File System

TABLE OF CONTENTS

PLANNING FOR A DISASTER RECOVERY

Before you begin a disaster recovery, make sure to do the following:

● Perform regular backups of the Windows file system or schedule the backups to run at regular intervals.

● Install Microsoft .NET Framework 3.5 and 4 on the client computer. This is not required if the client computer has Windows 2003 or Windows XP.

● On a Windows 2003 Server, restore to the same platform that you used for performing the backup. For example, You cannot do a full system restore on an x64 platform if you are using a 32-bit iDataAgent for backup.

● If you have excluded any critical system state component from the backup, you cannot use that backup for the system restore. Ensure that the following critical system state components are not excluded from the backup:

Registry

System Protected Files

Active Directory

Cluster DB

Sysvol (For 2000 or 2003 domain controllers level)

DFSR (Windows 2008 Domain controller level)

CREATING A CHECKLIST

If the operating system of your client is corrupted, you need to re-build the operating system.

During the rebuild you will be prompted for the following system information. Since the computer will be down during the operating system rebuild, you may not be able to access necessary information about the system. It is important to record such information before a disaster occurs.

SYSTEM INFORMATION	HOW TO GET IT
Windows Operating System	Use Windows installation discs, CD, required service packs (SPs) and Hot fixes to install the Windows Operating System.
Windows File System iDataAgent	Use Windows File System iDataAgent installation disc to install the Windows File System iDataAgent.
Drives	Use the Disk Management utility to record the volumes and sizes of the hard drives in the system, which are needed to recreate the disk configuration in case of hard drive failure. Hard drives must be configured before restoring System State or file system data.
Computer name	Use the same computer name and avoid changing other configuration settings.
Network Interface Card configuration and settings	1. Click **Start	Programs	Accessories	System Information**. 2. In the **System Information** dialog box, click **Components	Network |Adapter**. 3. Note down the Network Adapter and Drivers information.
TCP/IP Settings	On the command prompt give following commands:

	• `hostname` - Note down the fully qualified network name
	• `ipconfig` - Note down the IP address, Subnet mask, TCP/IP domain name for the network, IP address of the domain name server (DNS) settings.
Video settings	Note down the video settings if the resolution and color depth are important.
Domain information	Note down the domain in which this computer resides.
Domain password	Note down this information if you are restoring a domain controller.
Local admin password	Note down this information to log on to the computer once it is restored.

WHAT GETS RESTORED

You can restore any one or all of the following components during full system restore:

- File System
- System State
- Office Communications Server

WHAT DOES NOT GET RESTORED

By default, the Calypso files and registry entries are excluded from the restore. After the full system restore, when you install Calypso, all the latest patches will be available.

If the backup contains all the latest patches, create the nDisableGalaxyMerge registry key and set the value to 1 to restore the registry entries for Calypso.

FULL SYSTEM RESTORE OF A NON-DOMAIN CONTROLLER

1. Rebuild the system hardware if necessary.

2. Configure hardware devices such as disk arrays and ensure connectivity to all drives.

3. Using the instructions provided with the software, install Windows operating system and include any previously installed Service Packs and Hot Fixes.

   Do not install IIS Services. These services will be restored automatically during the restore.

4. Format and partition the hard drives to match their previous configurations.

   When recreating partitions, you can Browse the backup data to determine the previous size of the partitions. When you browse the backup set, each drive letter will have its size noted in the Browse window.

5. If the client was installed with a fully qualified domain name, perform the following tasks, otherwise, skip to the next step.
   - Change the Computer name to the fully qualified domain name to avoid a naming resolution conflict when the client is restored.
   - Add the IP address and the fully qualified domain name and a short name of the Client, MediaAgent and CommServe to the host file of the client in the following format:

     `<ip address> <fully qualified domain name> <short name>`

     Until the DNS server is restored, there is no domain name resolution and the client will be unable to communicate with the CommServe and MediaAgent computers unless this information is added to the host file.

     Similarly, add the CommServe, MediaAgent and Client names and their IP addresses to the Host file of the MediaAgent, and CommServe when restoring a Domain Name Server.

6. Enable and configure TCP/IP support.

7. Configure the Network Interface Card(s).

   Ensure that the Network Interface Card used is the first card listed in the network binding order when restoring a client with multiple Network Interface Cards.

8. Run the following command to verify network communications between the client computer and the CommServe:

   ping `<CommServe name>`

9. Run the following command to verify network communications between the client computer and the MediaAgent:

   ping <MediaAgent name>

10. Install the Windows File System *i*DataAgent all applicable updates on the default install partition of the client computer.

11. Open the CommCell Console.

12. From the CommCell Browser, right-click the **<Client>** and select **Properties**.

13. Click the **Activity Control** tab.

14. Clear the **Enable Data Management** check box. This will disable backup jobs for the client and any scheduled backup jobs for the client will not start during the full system restore.

15. Click **OK.**

16. From the CommCell Browser, navigate to **Client Computers| <*Client*> | File System**.

17. Right-click the <***Backupset***> that contains the system state data and all the drives and then click **Browse Backup Data**.

18. Select the required options from the **Browse Options** dialog box and click **OK**.

19. Select the <***BackupSet***> box from the **Client Browse** tab which contains system state data and all the drives.

20. Click **Recover All Selected**.

21. Select the required options from the **Restore Options** dialog box and click **OK**.

    If the hardware of the destination computer is drastically different than the hardware of the source computer, do not select **Unconditional Overwrite** option.

22. Click **Compare** to view the Service Pack information of source and destination computer.

23. Note down the service packs that are not installed on the destination computer and click **Close**.

    The **Include Hotfix** check box will be available for the source computer if you have chosen the **Include Hotfix Information** option during the backup.

24. Click **No** if the source computer and the destination computer has different service packs. Install the required service packs and hot fixes on the destination computer.

    Click **Yes** if all the service packs on the source and destination computer are same. The full system restore starts.

25. Click **OK** to restart the computer.

26. Re-install any agents that were previously installed on the restored client computer.

27. Enable the backup jobs for the client by selecting the **Enable Data Management** check box from the **Activity Control** tab of the **Client Properties** dialog box.

    On a Windows Server 2008, select **Configure Refresh** from the **Server Manager** main page and update Features and Roles as they are not updated during a restart.

RESTORING TEAMING NETWORK ADAPTERS

If you are using teaming network adapters, follow the steps given below:

1. Uninstall the teaming software.

2. Restart the computer.

3. Install the teaming software.

FULL SYSTEM RESTORE OF A DOMAIN CONTROLLER ON WINDOWS SERVER 2003

1. Rebuild the system hardware if necessary.

2. Configure hardware devices such as disk arrays and ensure connectivity to all drives.

3. Using the instructions provided with the software, install Windows operating system and include any previously installed Service Packs and Hot Fixes.

    Do not install IIS Services. These services will be restored automatically during the restore.

    Do not include the server in the domain. Keep it in the workgroup.

4. Format and partition the hard drives to match their previous configurations.

    When recreating partitions, you can Browse the backup data to determine the previous size of the partitions. When you browse the backup set, each drive letter will have its size noted in the Browse window.

5. If the client was installed with a fully qualified domain name, perform the following tasks, otherwise, skip to the next step.

   ○ Change the Computer name to the fully qualified domain name to avoid a naming resolution conflict when the client is restored.

   ○ Add the IP address and the fully qualified domain name and a short name of the Client, MediaAgent and CommServe to the host file of the client in the following format:
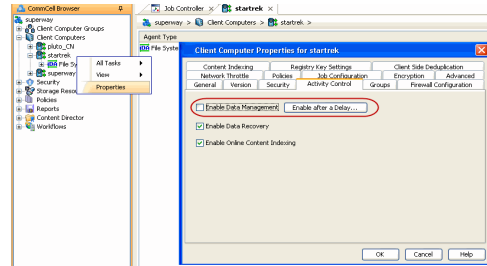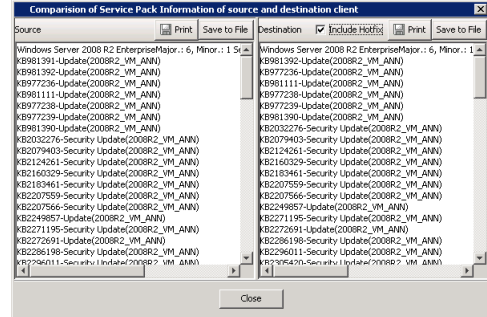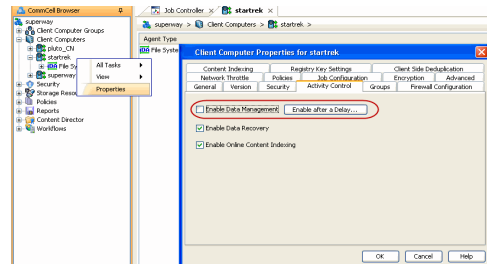
   `<ip address> <fully qualified domain name> <short name>`

   Until the DNS server is restored, there is no domain name resolution and the client will be unable to communicate with the CommServe and MediaAgent computers unless this information is added to the host file.

   Similarly, add the CommServe, MediaAgent and Client names and their IP addresses to the Host file of the MediaAgent, and CommServe when restoring a Domain Name Server.

6. Enable and configure TCP/IP support.

7. Configure the Network Interface Card(s).

   Ensure that the Network Interface Card used is the first card listed in the network binding order when restoring a client with multiple Network Interface Cards.

8. Run the following command to verify network communications between the client computer and the CommServe:

   ping `<CommServe name>`

9. Run the following command to verify network communications between the client computer and the MediaAgent:

   ping <MediaAgent name>

10. Install the Windows File System iDataAgent all applicable updates on the default install partition of the client computer.

    Restart the computer in Directory Services mode after installing Windows File System iDataAgent.
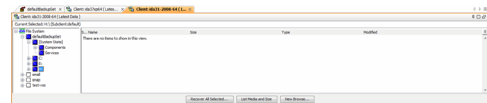
11. Open the CommCell Console.

12. From the CommCell Browser, right-click the **<Client>** and select **Properties**.

13. Click the **Activity Control** tab.

14. Clear the **Enable Data Management** check box. This will disable backup jobs for the client and any scheduled backup jobs for the client will not start during the full system restore.
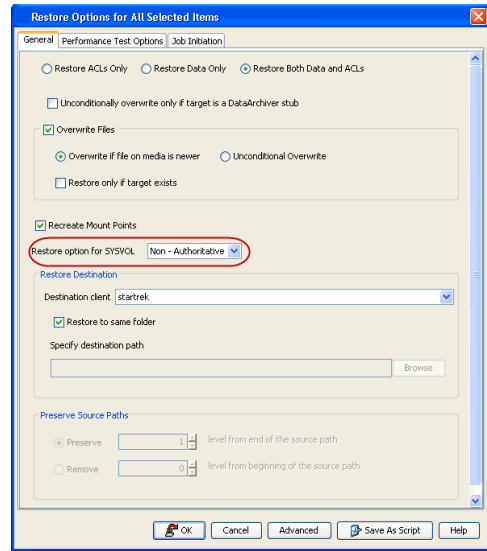
15. Click **OK.**

16. From the CommCell Browser, navigate to **Client Computers| <Client>** | **File System**.

17. Right-click the **<Backupset>** that contains the system state data and all the drives and then click **Browse Backup Data**.

18. Select the required options from the **Browse Options** dialog box and click **OK**.

19. Select the **<BackupSet>** box from the **Client Browse** tab which contains system state data and all the drives.

20. Click **Recover All Selected**.

21. Select one of the following from the **Restore option for SYSVOL** list:

    ○ **Primary** - Select this option when you are restoring for a standalone domain controller or the first domain controller restored in the network

    ○ **Non-Authoritative** - Select this option to restore the domain controller without replicating any changes to the other domain controllers on the network

    ○ **Authoritative** - Select this option to restore the domain controller and also replicate any changes to the other domain controllers on the network. You must run the **ntdsutil** to replicate the changes to the other domain controllers.
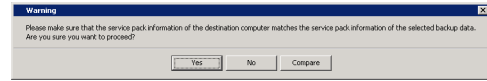
    If the hardware of the destination computer is drastically different than the hardware of the source computer, do not select **Unconditional Overwrite** option.

    Select the other required options and click **OK**.

22. Click **Compare** to view the Service Pack information of source and destination computer.

23. Note down the service packs that are not installed on the destination computer and click **Close**.

    The **Include Hotfix** check box will be available for the source computer if you have chosen the **Include Hotfix Information** option during the backup.
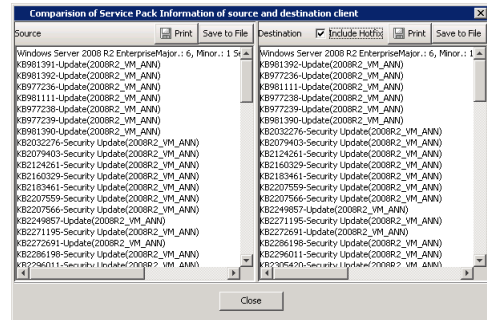
24. Click **No** if the source computer and the destination computer has different service packs. Install the required service packs and hot fixes on the destination computer.

    Click **Yes** if all the service packs on the source and destination computer are same. The full system restore starts.

25. Click **OK** to restart the computer.

26. Re-install any agents that were previously installed on the restored client computer.

27. Enable the backup jobs for the client by selecting the **Enable Data Management** check box from the **Activity Control** tab of the **Client Properties** dialog box.

REPLICATING ACTIVE DIRECTORY DATA TO ALL THE DOMAIN CONTROLLERS IN A DOMAIN

The system performs a non-authoritative restore of the Active Directory by default, ensuring that any Active Directory data that has changed since the last backup is not replicated to other domain controllers. However, you can force an authoritative restore of the Active Directory and replicate all the restored data to all the remaining domain controllers in the domain by running the `ntdsutil`.

It is recommended that you review all Microsoft instructions and methods before replicating the data to all domain controllers.

Follow the steps given below to run the `ntdsutil` :

1. Perform the Authoritative full system restore of a domain controller.

2. Restart the computer in the Directory Services mode.

3. From the Command Prompt, type `ntdsutil`.

4. At the `ntdsutil` prompt, type `Authoritative Restore`.

5. At the Authoritative Restore prompt, type `Restore Database`.

6. Click **Yes** to confirm this operation.

7. Type `quit` to exit the Authoritative Restore prompt.

8. Type `exit` to end the ntdsutil session.

9. Type `exit` to exit the command prompt.

10. Restart the computer in normal mode and wait for replication to complete.

If you are performing an Authoritative restore of the SYSVOL without performing the full system restore, you must run the `ntdsutil`. When you run this utility, the policies and scripts will be accessible from Active Directory Users and Computers.

FULL SYSTEM RESTORE OF A DOMAIN CONTROLLER ON WINDOWS SERVER 2008

1. Rebuild the system hardware if necessary.

2. Configure hardware devices such as disk arrays and ensure connectivity to all drives.

3. Using the instructions provided with the software, install Windows operating system and include any previously installed Service Packs and Hot Fixes.

   Do not install IIS Services. These services will be restored automatically during the restore.

   Do not include the server in the domain. Keep it in the workgroup.

4. Format and partition the hard drives to match their previous configurations.

   When recreating partitions, you can Browse the backup data to determine the previous size of the partitions. When you browse the backup set, each drive letter will have its size noted in the Browse window.

5. If the client was installed with a fully qualified domain name, perform the following tasks, otherwise, skip to the next step.
   - Change the Computer name to the fully qualified domain name to avoid a naming resolution conflict when the client is restored.
   - Add the IP address and the fully qualified domain name and a short name of the Client, MediaAgent and CommServe to the host file of the client in the following format:

     `<ip address> <fully qualified domain name> <short name>`

     Until the DNS server is restored, there is no domain name resolution and the client will be unable to communicate with the CommServe and MediaAgent computers unless this information is added to the host file.

     Similarly, add the CommServe, MediaAgent and Client names and their IP addresses to the Host file of the MediaAgent, and CommServe when restoring a Domain Name Server.

6. Enable and configure TCP/IP support.

7. Configure the Network Interface Card(s).

   Ensure that the Network Interface Card used is the first card listed in the network binding order when restoring a client with multiple Network Interface Cards.

8. Run the following command to verify network communications between the client computer and the CommServe:

   ping `<CommServe name>`
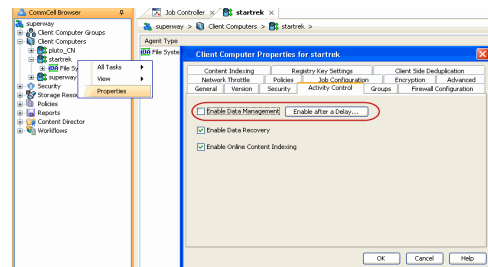
9. Run the following command to verify network communications between the client computer and the MediaAgent:

   ping `<MediaAgent name>`

10. Install the Windows File System iDataAgent all applicable updates on the default install partition of the client computer.

    Restart the computer in Directory Services mode after installing Windows File System iDataAgent.

11. Open the CommCell Console.

12. From the CommCell Browser, right-click the **<Client>** and select **Properties**.

13. Click the **Activity Control** tab.

14. Clear the **Enable Data Management** check box. This will disable backup jobs for the client and any scheduled backup jobs for the client will not start during the full system restore.

15. Click **OK.**

16. From the CommCell Browser, navigate to **Client Computers| <Client>** | **File System**.

17. Right-click the **<Backupset>** that contains the system state data and all the drives and then click **Browse Backup Data**.

18. Select the required options from the **Browse Options** dialog box and click **OK**.

19. Select the **<BackupSet>** box from the **Client Browse** tab which contains system state data and all the drives.
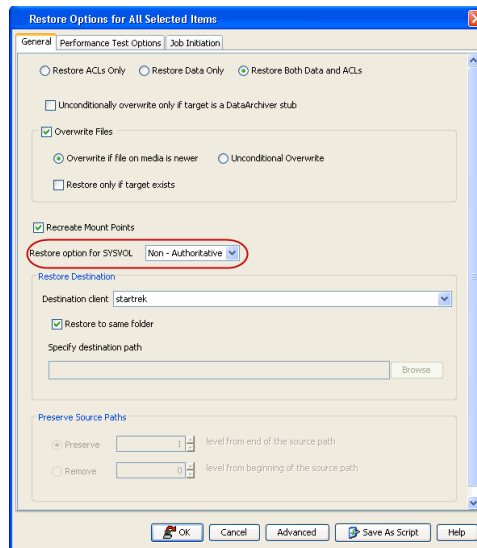
20. Click **Recover All Selected**.

21. Select one of the following from the **Restore option for SYSVOL** list:
    - **Primary** - Select this option when you are restoring for a standalone domain controller or the first domain controller restored in the network
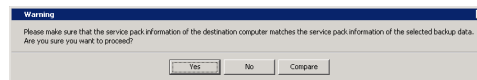
○ **Non-Authoritative** - Select this option to restore the domain controller without replicating any changes to the other domain controllers on the network

○ **Authoritative** - Select this option to restore the domain controller and also replicate any changes to the other domain controllers on the network. You must run the **ntdsutil** to replicate the changes to the other domain controllers.

If the hardware of the destination computer is drastically different than the hardware of the source computer, do not select **Unconditional Overwrite** option.

Select the other required options and click **OK**.

22. Click **Compare** to view the Service Pack information of source and destination computer.
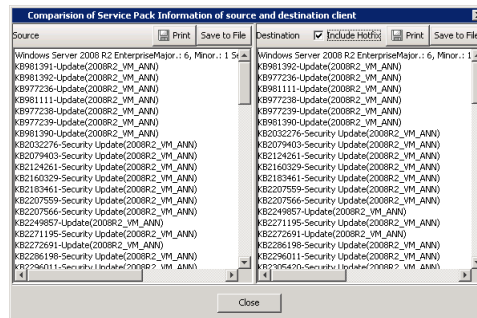
23. Note down the service packs that are not installed on the destination computer and click **Close**.

The **Include Hotfix** check box will be available for the source computer if you have chosen the **Include Hotfix Information** option during the backup.

24. Click **No** if the source computer and the destination computer has different service packs. Install the required service packs and hot fixes on the destination computer.

Click **Yes** if all the service packs on the source and destination computer are same. The full system restore starts.

25. Click **OK** to restart the computer.

26. Re-install any agents that were previously installed on the restored client computer.

27. Enable the backup jobs for the client by selecting the **Enable Data Management** check box from the **Activity Control** tab of the **Client Properties** dialog box.

28. Select **Configure Refresh** from the **Server Manager** main page and update Features and Roles as they are not updated during a restart.

REPLICATING ACTIVE DIRECTORY DATA TO ALL THE DOMAIN CONTROLLERS IN A DOMAIN

The system performs a non-authoritative restore of the Active Directory by default, ensuring that any Active Directory data that has changed since the last backup is not replicated to other domain controllers. However, you can force an authoritative restore of the Active Directory and replicate all the restored data to all the remaining domain controllers in the domain by running the ntdsutil.

It is recommended that you review all Microsoft instructions and methods before replicating the data to all domain controllers.

Follow the steps given below to run the ntdsutil :

1. Perform the Authoritative full system restore of a domain controller.

2. Restart the computer in the Directory Services mode.

3. From the Command Prompt, type ntdsutil.

4. At the ntdsutil prompt, type Activate instance NTDS.

5. At the ntdsutil prompt, type Authoritative Restore.

6. At the Authoritative Restore prompt, type Restore Subtree DistinguishedName.

where DistinguishedName is the name of the subtree that is to be marked authoritative.

For example: Restore subtree DC=DomainName,DC=COM will restore domainname.com.

7. Click **Yes** to continue.

The restore process will complete and a message confirming the creation of one text and 2 LDAP Data Interchange Format (LDIF) files will be displayed.

8. Restart the computer in normal mode and allow time for replication to complete.

9. To run an LDIF file to recover back-links, type the following command at the command prompt.

   `ldifde -i -k -f FileName` (where the `FileName` is the name of the LDIF file)

10. Repeat step 5 and 6 for each additional domain.

RESTORING A CLUSTER ON WINDOWS SERVER 2003

NON-AUTHORITATIVE RESTORE

Performed a non-authoritative restore in the following scenarios:

● Single node in a cluster fails completely (no boot) and the shared disks are still functional

● Complete loss of all nodes and storage

PREREQUISITES

● If you are restoring a cluster node running SQL or Exchange servers, see the Microsoft disaster recovery documentation for restoring SQL and Exchange servers before restoring the node.

● When you are recovering primary node, turn off all cluster nodes except the primary node to be recovered.

Follow the steps given below to perform the Full System Restore of a Primary Node or Passive node:

1. Rebuild the system hardware if necessary.

2. Configure hardware devices such as disk arrays and ensure connectivity to all drives.

   Configure all disk array devices with access to the shared array

3. Using the instructions provided with the software, install Windows operating system and include any previously installed Service Packs and Hot Fixes.

   Do not install IIS Services. These services will be restored automatically during the restore.

   Do not include the server in the domain. Keep it in the workgroup.

4. Format and partition the hard drives to match their previous configurations.

   > When recreating partitions, you can Browse the backup data to determine the previous size of the partitions. When you browse the backup set, each drive letter will have its size noted in the Browse window.

5. If the client was installed with a fully qualified domain name, perform the following tasks, otherwise, skip to the next step.
   ○ Change the Computer name to the fully qualified domain name to avoid a naming resolution conflict when the client is restored.
   ○ Add the IP address and the fully qualified domain name and a short name of the Client, MediaAgent and CommServe to the host file of the client in the following format:
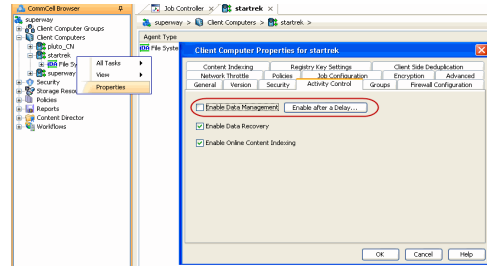
   `<ip address> <fully qualified domain name> <short name>`

   Until the DNS server is restored, there is no domain name resolution and the client will be unable to communicate with the CommServe and MediaAgent computers unless this information is added to the host file.

   Similarly, add the CommServe, MediaAgent and Client names and their IP addresses to the Host file of the MediaAgent, and CommServe when restoring a Domain Name Server.

6. Enable and configure TCP/IP support.

7. Configure the Network Interface Card(s).

   Ensure that the Network Interface Card used is the first card listed in the network binding order when restoring a client with multiple Network Interface Cards.

   Bind the public Network Interface Card before the Private network interface card.

8. Run the following command to verify network communications between the client computer and the CommServe:

   ping `<CommServe name>`

9. Run the following command to verify network communications between the client computer and the MediaAgent:

   ping <MediaAgent name>

10. Install the Windows File System *i*DataAgent all applicable updates on the default install partition of the client computer.

11. Open the CommCell Console.

12. From the CommCell Browser, right-click the **<Client>** and select **Properties**.

13. Click the **Activity Control** tab.

14. Clear the **Enable Data Management** check box. This will disable backup jobs for the client and any scheduled backup jobs for the client will not start during the full system restore.
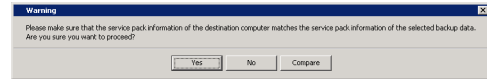
15. Click **OK.**

16. From the CommCell Browser, navigate to **Client Computers| <*Client*> | File System**.

17. Right-click the <***Backupset***> that contains the system state data and all the drives and then click **Browse Backup Data**.

18. Select the required options from the **Browse Options** dialog box and click **OK**.

19. Select the <***BackupSet***> box from the **Client Browse** tab which contains system state data and all the drives.

20. Click **Recover All Selected**.

21. Select the required options from the **Restore Options** dialog box and click **OK**.

   If the hardware of the destination computer is drastically different than the hardware of the source computer, do not select **Unconditional Overwrite** option.

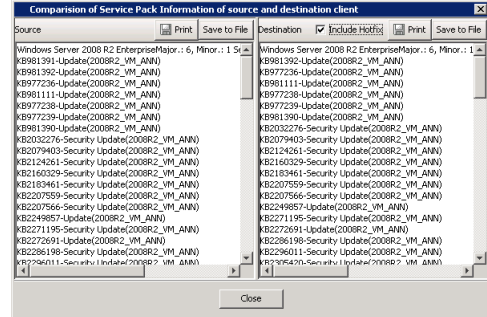22. Click **Compare** to view the Service Pack information of source and destination computer.

23. Note down the service packs that are not installed on the destination computer and click **Close**.

   The **Include Hotfix** check box will be available for the source computer if you have chosen the **Include Hotfix Information** option during the backup.

24. Click **No** if the source computer and the destination computer has different service packs. Install the required service packs and hot fixes on the destination computer.

   Click **Yes** if all the service packs on the source and destination computer are same. The full system restore starts.

25. Click **OK** to restart the computer.

26. Re-install any agents that were previously installed on the restored client computer.

27. Enable the backup jobs for the client by selecting the **Enable Data Management** check box from the **Activity Control** tab of the **Client Properties** dialog box.

28. Restore Program files for the virtual server. Use one of the following methods to restore the program files:
    - Restoring program files when registry keys are merged during the restore.
    - Restoring program files when registry keys are not merged during the restore.

AUTHORITATIVE RESTORE

Perform the authoritative restore when all the cluster nodes are running and you want to restore the cluster database and restart the cluster services on all the nodes.

Follow the steps given below to perform the Full System Restore of a node that has the cluster database:

1. Rebuild the system hardware if necessary.

2. Configure hardware devices such as disk arrays and ensure connectivity to all drives.

   Configure all disk array devices with access to the shared array

3. Using the instructions provided with the software, install Windows operating system and include any previously installed Service Packs and Hot Fixes.

   Do not install IIS Services. These services will be restored automatically during the restore.

   Do not include the server in the domain. Keep it in the workgroup.

4. Format and partition the hard drives to match their previous configurations.

   When recreating partitions, you can Browse the backup data to determine the previous size of the partitions. When you browse the backup set, each drive letter will have its size noted in the Browse window.

5. If the client was installed with a fully qualified domain name, perform the following tasks, otherwise, skip to the next step.

   ○ Change the Computer name to the fully qualified domain name to avoid a naming resolution conflict when the client is restored.

   ○ Add the IP address and the fully qualified domain name and a short name of the Client, MediaAgent and CommServe to the host file of the client in the following format:

   `<ip address> <fully qualified domain name> <short name>`

   Until the DNS server is restored, there is no domain name resolution and the client will be unable to communicate with the CommServe and MediaAgent computers unless this information is added to the host file.

   Similarly, add the CommServe, MediaAgent and Client names and their IP addresses to the Host file of the MediaAgent, and CommServe when restoring a Domain Name Server.

6. Enable and configure TCP/IP support.

7. Configure the Network Interface Card(s).

   Ensure that the Network Interface Card used is the first card listed in the network binding order when restoring a client with multiple Network Interface Cards.

   Bind the public Network Interface Card before the Private network interface card.

8. Run the following command to verify network communications between the client computer and the CommServe:
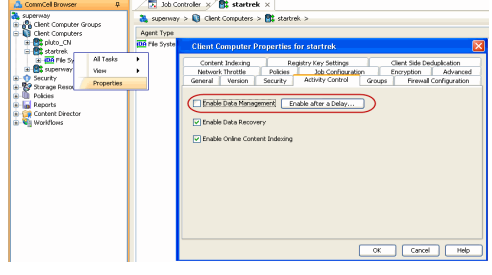
   ping `<CommServe name>`

9. Run the following command to verify network communications between the client computer and the MediaAgent:
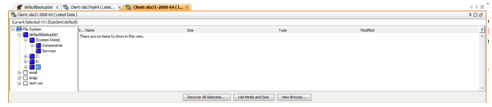
   ping `<MediaAgent name>`

10. Install the Windows File System *i*DataAgent all applicable updates on the default install partition of the client computer.

11. Open the CommCell Console.

12. From the CommCell Browser, right-click the *<Client>* and select **Properties**.

13. Click the **Activity Control** tab.

14. Clear the **Enable Data Management** check box. This will disable backup jobs for the client and any scheduled backup jobs for the client will not start during the full system restore.
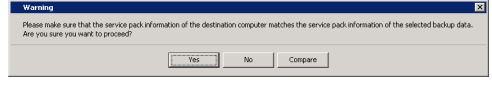
15. Click **OK.**

16. From the CommCell Browser, navigate to **Client Computers| *<Client>* | File System**.

17. Right-click the *<Backupset>* that contains the system state data and all the drives and then click **Browse Backup Data**.

18. Select the required options from the **Browse Options** dialog box and click **OK**.

19. Select the *<BackupSet>* box from the **Client Browse** tab which contains system state data and all the drives.

20. Click **Recover All Selected**.

21. Select the required options from the **Restore Options** dialog box and click **OK**.

    If the hardware of the destination computer is drastically different than the hardware of the source computer, do not select **Unconditional Overwrite** option.

22. Click **Compare** to view the Service Pack information of source and destination computer.

23. Note down the service packs that are not installed on the destination computer and click **Close**.
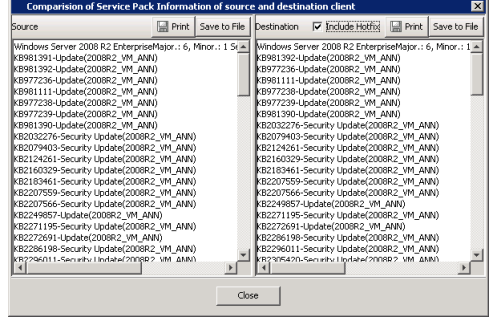
    The **Include Hotfix** check box will be available for the source computer if you have chosen the **Include Hotfix Information** option during the backup.

24. Click **No** if the source computer and the destination computer has different service packs. Install the required service packs and hot fixes on the destination computer.

    Click **Yes** if all the service packs on the source and destination computer are same. The full system restore starts.

25. Click **OK** to restart the computer.

26. Re-install any agents that were previously installed on the restored client computer.

27. Enable the backup jobs for the client by selecting the **Enable Data Management** check box from the **Activity Control** tab of the **Client Properties** dialog box.

28. Restore Program files for the virtual server. Use one of the following methods to restore the program files:

    ○ Restoring program files when registry keys are merged during the restore.

    ○ Restoring program files when registry keys are not merged during the restore.

29. Enter `Y (yes)` for the following message:

    `Full iDataAgent Restore job completed. Do you want to reboot?`

30. Enter Y (yes) for the following message:

    `New Hardware found. Windows has finished installing new devices.... Do you want to restart your computer now?`

31. Restart the computer.

32. After the computer restarts, from a command prompt, navigate to `<Install Directory>\base` folder and enter the following command :

    `authorutil.exe -cluster`

    This command will stop the cluster services on all the nodes, replicate the cluster database information on all the nodes and then restart the services.

RESTORING PROGRAM FILES FOR VIRTUAL SERVER WHEN REGISTRY KEYS ARE MERGED

If the registry key nDisableGalaxyMerge is enabled before starting the full restore of primary node, the registry keys on a primary node are merged during the full system restore. As a result, the following resources are restored during the full system restore:

● The CommVault Communications Service (GxCVD)

● CommVault Client Event Manager (GxEvMgrC) cluster

The program files are required to start and run these resources. Perform one of the following steps to restore program files for a virtual server to the physical node that owns the virtual disk:

● Select all the virtual disk data and restore it.

● Restore only the program files in order to get the services started. Then restore the rest of the data using the virtual server's File System iDataAgent.

RESTORING PROGRAM FILES FOR VIRTUAL SERVER WHEN REGISTRY KEYS ARE NOT MERGED

If you haven't enabled the registry key nDisableGalaxyMerge before starting the full restore of primary node, the registry keys on a primary node are not merged during the Full System Restore. Follow the steps given below to restore program files on a virtual server:

1. Uninstall all *i*DataAgents from the virtual server.

2. Re-install File System *i*DataAgent and all other required *i*DataAgents on the virtual server

3. Restore the virtual server's data using the File System *i*DataAgent.

RESTORING THE CLUSTER ON WINDOWS SERVER 2008

RESTORING CLUSTER SERVICES

On a Windows Server 2008 computers, the cluster services will be restored automatically in any of the following scenarios:
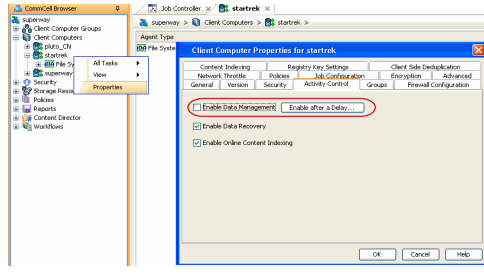
SITUATION	CORRECTIVE ACTION
Cluster files on witness disk/Quorum Disk) are corrupt	● Files in the `\Cluster` directory will be re-created. ● Cluster configuration will be 'pushed' to the Witness Disk
Cluster database (ClusDB) on a single node is missing or corrupt	Healthy nodes will be contacted and an updated ClusDB will be downloaded.
Complete loss of Witness Disk/LUN occurs	● If using Disk Only quorum model you need to use /ForceQuorum recovery switch. ● Use Cluster Quorum Wizard to change quorum disk designation.

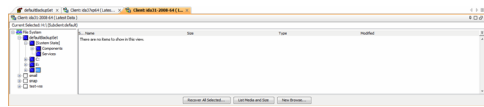### AUTHORITATIVE RESTORE OF CLUSTER ON WINDOWS SERVER 2008

Perform the Authoritative Restore of cluster on Windows 2008 if you alter the cluster configuration or delete a large number of resources. You can perform the authoritative restore only if all cluster nodes and services are running. Follow the steps given below to revert to the original cluster configuration:

1. Open the CommCell Console.

2. From the CommCell Browser, right-click the *<Client>* and select **Properties**.

3. Click the **Activity Control** tab.

4. Clear the **Enable Data Management** check box. This will disable backup jobs for the client and any scheduled backup jobs for the client will not start during the full system restore.
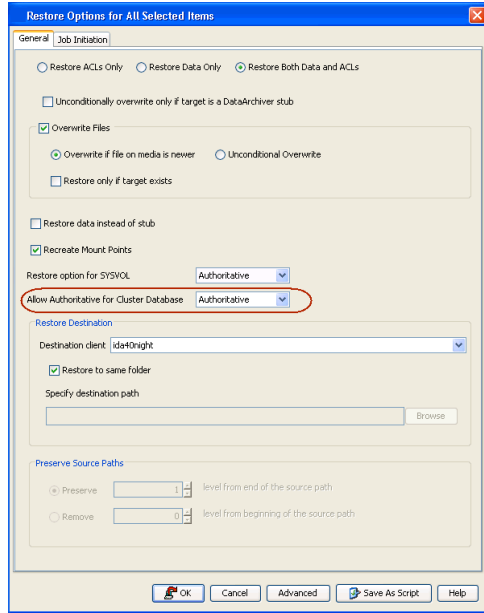
5. Click **OK.**

6. From the CommCell Browser, navigate to **Client Computers| <***Client***> | File System**.

7. Right-click the <***Backupset***> that contains the system state data and all the drives and then click **Browse Backup Data**.

8. Select the required options from the **Browse Options** dialog box and click **OK**.

9. Select the <***BackupSet***> box from the **Client Browse** tab which contains system state data and all the drives.

10. Click **Recover All Selected**.

11. Select the required options from the **Restore Options** dialog box and click **OK**.

   If the hardware of the destination computer is drastically different than the hardware of the source computer, do not select **Unconditional Overwrite** option.
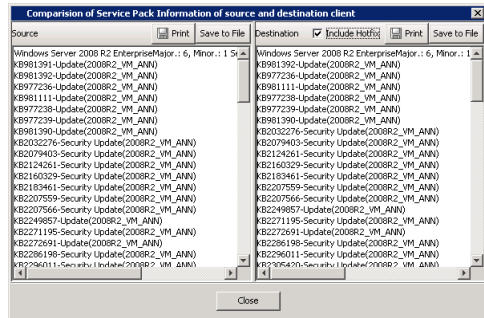
12. Select **Authoritative** from the **Allow Authoritative for Cluster Database** list.

13. Select the other required restore options and click **OK**.

14. Click **Compare** to view the Service Pack information of source and destination computer.

15. Note down the service packs that are not installed on the destination computer and click **Close**.

   The **Include Hotfix** check box will be available for the source computer if you have chosen the **Include Hotfix Information** option during the backup.

16. Click **No** if the source computer and the destination computer has different service packs. Install the required service packs and hot fixes on the destination computer.

   Click **Yes** if all the service packs on the source and destination computer are same. The full system restore starts.

17. Click **OK** to restart the computer.

18. Re-install any agents that were previously installed on the restored client computer.

19. Enable the backup jobs for the client by selecting the **Enable Data Management** check box from the **Activity Control** tab of the **Client Properties** dialog box.

20. Select **Configure Refresh** from the **Server Manager** main page and update Features and Roles as they are not updated during a restart.

19. Ensure that the cluster services are stopped on all the other nodes of the cluster. If required, stop the cluster services on all the other nodes.

20. Enter `Y (yes)` for the following message:

    ```
    Full iDataAgent Restore job completed. Do you want to reboot?
    ```

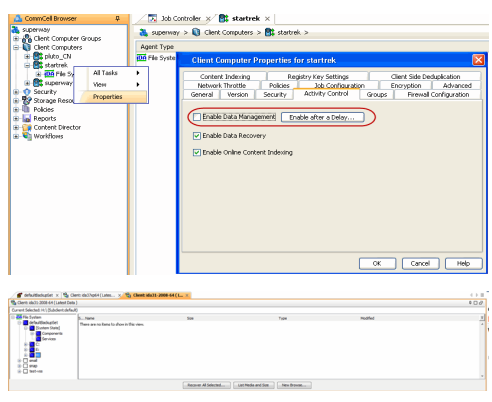21. Start the services on all the other nodes in the clusters.

NON-AUTHORITATIVE RESTORE OF CLUSTER ON WINDOWS SERVER 2008

Performed a non-authoritative restore in the following scenarios:

- Single node in a cluster fails completely (no boot) and the shared disks are still functional

- Complete loss of all nodes and storage

Follow the steps given below to perform the non-authoritative restore

1. Open the CommCell Console.

2. From the CommCell Browser, right-click the **<Client>** and select **Properties**.

3. Click the **Activity Control** tab.

4. Clear the **Enable Data Management** check box. This will disable backup jobs for the client and any scheduled backup jobs for the client will not start during the full system restore.

5. Click **OK.**

6. From the CommCell Browser, navigate to **Client Computers| <Client>** | **File System**.

7. Right-click the **<Backupset>** that contains the system state data and all the drives and then click **Browse Backup Data**.

8. Select the required options from the **Browse Options** dialog box and click **OK**.

9. Select the **<BackupSet>** box from the **Client Browse** tab which contains system state data and all the drives.

10. Click **Recover All Selected**.

11. Select the required options from the **Restore Options** dialog box and click **OK**.
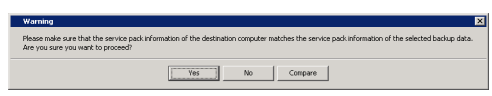
    If the hardware of the destination computer is drastically different than the hardware of the source computer, do not select **Unconditional Overwrite** option.

12. Select **Non-Authoritative** from the **Allow Authoritative for Cluster Database** list.

13. Select the other required restore options and click **OK**.

14. Click **Compare** to view the Service Pack information of source and destination computer.
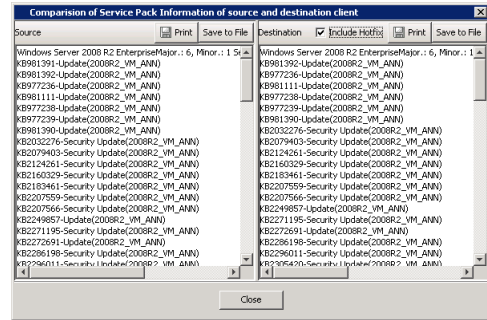
15. Note down the service packs that are not installed on the destination computer and click **Close**.

    The **Include Hotfix** check box will be available for the source computer if you have

chosen the **Include Hotfix Information** option during the backup.

16. Click **No** if the source computer and the destination computer has different service packs. Install the required service packs and hot fixes on the destination computer.

    Click **Yes** if all the service packs on the source and destination computer are same. The full system restore starts.

17. Click **OK** to restart the computer.

18. Re-install any agents that were previously installed on the restored client computer.

19. Enable the backup jobs for the client by selecting the **Enable Data Management** check box from the **Activity Control** tab of the **Client Properties** dialog box.

20. Enter `Y (yes)` for the following message:

    ```
    Full iDataAgent Restore job completed. Do you want to reboot?
    ```

21. Select **Configure Refresh** from the **Server Manager** main page and update Features and Roles as they are not updated during a restart.

Best Practices - Windows File System *i*DataAgent

ELIMINATING BACKUP FAILURES

You can use filters to exclude items which consistently fail and that are not integral to the operation of the system or applications. Some items fail because they are locked by the operating system or application and cannot be opened at the time of the data protection operation. This often occurs with certain system-related files and database application files. Also, keep in mind that you will need to run a full backup after adding failed files to the filter in order to remove them.

RE-CONFIGURING DEFAULT SUBCLIENT CONTENT

We recommend that you do not re-configure the content of a default subclient because this would disable its capability to serve as a catch-all entity for client data. As a result, some data will not get backed up or scanned.

RESTORE BY JOB

Avoid running restores by jobs for jobs associated with the default backup set, if you do not want to restore the operating system files or directories. The entire content of the backed up client will be restored and the client where you are restoring might run out of space.

RESTORING TO A REBUILT OR NEW COMPUTER

If you are restoring to a different computer, perform the following checks to make sure the target computer is similar to the source computer:

● Make sure the target computer has the same fully qualified network name as the original.

● Try to match the general hardware configuration (i.e., IDE, SCSI) of the original computer.

● Match the local disk drive configuration as closely as possible to that of the client being restored.

● Make sure the computer's disk(s) can accommodate the quantity of data being restored.

● If possible, use the same network interface card (NIC) as that of the client being restored.

The CommCell Console requires 256 colors to run. When you open the CommCell Console on a rebuilt computer, you may need to install the correct video driver to increase the color depth of the client computer or run the console from another computer.

RESTORING TO A COMPUTER WITH DIFFERENT HARDWARE CONFIGURATION

If you are performing a full system restore to a computer with a different hardware configuration (mass storage device, network interface card, video card, etc.), do not restore the system state data. Restoring system state data includes restoration of the hardware entries in the registry.

REPLICATING ACTIVE DIRECTORIES TO OTHER DOMAIN CONTROLLERS

The Active Directory uses a Tombstone mechanism to delete objects from its directory on Windows 2000 and Server 2003 clients. When an Active Directory object is deleted from a domain controller, it is initially marked as *tombstoned* and is not fully removed from the directory. During Active Directory replication, the tombstone attribute is replicated to the other domain controllers, temporarily deleting the object from all the domain controllers. Once the tombstone lifetime is reached, the object is permanently removed from the directory. The Active Directory Tombstone has a default lifetime setting of 60 days.

When performing restore operations, you must consider the Active Directory tombstone lifetime. Restoring from a backup that was secured more than a lifetime before the restore may result in Active Directory inconsistencies. The restored domain controller may have objects that are not replicated on the other domain controllers. These objects will not be deleted automatically, as the corresponding tombstones on the other servers have already been deleted. Therefore, when you restore from a backup that is older than the tombstone lifetime, you may have to manually delete each unreplicated object on the restored computer in order to resolve inconsistencies.

INSTALLING WINDOWS DURING FULL SYSTEM RESTORE

Windows must be installed in the same directory as that of the original computer; otherwise, full system restores will not work. For machines that have been upgraded to Server 2003 from Windows 2000, Windows must be installed in the WINNT directory.

CREATING A SUBCLIENT TO BACKUP LOCKED FILES

When you are have enabled VSS for a default subclient, the Locked database files are backed up in an inconsistent state and some system protected data will get backed up.

For example, you may have an Exchange database installed on the client. The Exchange database should not be backed up by the Windows File System *i*DataAgent because it will not be able to restore the database. Furthermore, this will increase your media usage. It is recommended to use the Exchange Database *i*DataAgent to backup the Exchange database.

If you have locked files that you would like to back up using VSS, it is recommended that you create a subclient for them and enable VSS on that subclient.

If you want to enable VSS on the default subclient then it is recommended to filter the data from other *i*DataAgents (For example: Excahnge *i*DataAgent or SQL

*i*DataAgent) from the default subclient.

SYSTEM STATE RESTORE FOR WINDOWS SERVER 2008

The system state restore for Windows Server 2008 may take a long time to complete. All editions of Windows Server 2008 treat more files are System Protected files as compared to any other Windows operating systems. Large System Protected Files backups can require additional disk space for recovery while the files are being moved.

It is recommended to keep at least 10-15GB free space on the following drives:

- The drive where job results folder is located
- The drive where Windows is installed

RESTORE FROM DEDUPLICATED VOLUMES ON WINDOWS SERVER 2012

Windows Server 2012 has a deduplication feature that can be enabled. Data from deduplicated volumes will be backed up in its original state (uncompressed). Therefore, during a restore, ensure that you have enough storage space on the volume to restore the full data size. In addition, make sure that a minimum service pack level of SP9b is installed on the client prior to backing up deduplicated volumes on Windows Server 2012.

Frequently Asked Questions - Windows File System

TABLE OF CONTENTS

General

Scan Methods

VSS

Wildcards

GENERAL

HOW DO I BACKUP THE QUORUM DATA IN A CLUSTER SETTING?

The Windows File System *i*DataAgent on a physical node of the cluster includes the quorum data during a system state backup. It is essential for quorum data to be backed up, as it includes recovery logs as well as cluster configuration and state data. To back up the quorum data on a regular basis, you must ensure that a data protection operation is scheduled for a Windows File System *i*DataAgent subclient on the physical nodes, with the Backup System State option selected; a system state backup will automatically include quorum data.

WHY ARE MY SNAPSHOTS MISSING FROM THE BACKUP?

When backing up a snapshot of a client computer, ensure that the operating system of the backup server is either same or higher version than the client computer.

I DO NOT SEE THE NEWLY ADDED DATA IN THE BACKED UP FILES?

It is recommended to perform a full backup after changing or adding and subclient content to ensure that the newly added or modified data is completely backed up.

WHY DOES MY BACKUP AND RECOVERY DISPLAY INCONSISTENT DATA?

Ensure that the volume, network or the user quota for an object are not set lower than the amount already used.

DO I NEED TO INSTALL QSNAP WHILE PERFORMING THE FULL SYSTEM RESTORE?

Depending upon the backup from which you are restoring the system, install the QSnap either before the full system restore or after the full system restore. The following table explains the scenarios to reinstall the QSnap:

BACKUP	INSTALL QSNAP
QSnap Enabled Backup	Install QSnap before performing the full system restore.
QSnap was installed on the source computer after the backup was performed.	• Install the Windows File System *i*DataAgent and then perform the full system restore. Then install QSnap after the client is restored and has rebooted. • If you are not rebuilding the operating system, uninstall QSnap, restore the registry, and then reinstall QSnap.

HOW TO RESTORE BACK-LINKS FOR AUTHORITATIVELY RESTORED OBJECTS?

If you have authoritatively restored objects that have back-links in another domain, you need to create LDAP Data Interchange Format (LDIF) file and then run the LDIF file on any domain controller in the same domain. Do not run the LDIF file on the same domain controller where you created the file. For more information on how to create and run the LDIF file, refer to http://technet.microsoft.com/en-us/library/cc778643(WS.10).aspx.

HOW TO BACKUP THE SOURCE DATA FOR A DIRECTORY JUNCTION POINT?

By default, the directory junction point gets backed up but the source data (data linked to junction point) is not backed up. This prevents undesired backup and restore of system created directory junction points. To back up the source data of a junction point that is not part of a subclient contents, the source data must be explicitly added to a subclient's content.

WHEN DOES A NON-FULL BACKUP AUTOMATICALLY GET CONVERTED TO A FULL BACKUP?

A non-full backup is automatically converted to a full backup in the following situations:

● First backup of the subclient.

● Re-associating a subclient to another storage policy.

● Promote a secondary storage policy copy that is not synchronized with a primary copy (for all the subclients of a storage policy).

● If a backup job within the most recent backup cycle is pruned or disabled from a primary copy.

- Adding a new content path to the subclient.
- If you switch from a SnapProtect backup to a traditional backup or vice versa.
- CommCell Migration operation.

DO WE STAGE COMPONENTS IN THE JOB RESULTS FOLDER DURING THE SYSTEM STATE RESTORE?

During the system state restore some components are staged in the job results folder and then get deleted once the restore of that component is complete. If a file needs to be moved during reboot, the file will not be deleted from the job results folder until the computer reboots.

BACKUP OPERATION IS SLOW. HOW DO I TROUBLESHOOT THE SLOWNESS?

You can view the log files of an active backup job and use performance counters in the logs to check the performance bottle necks. For more information about how to View the Log Files of an Active Job. A log has following IDs

- `File Open Time` - Time taken to open a file
- `Disk Read Time` - Time taken to read the file from a disk
- `Pipeline Allocation time and Pipeline Write Time` - Time taken to write data on a media and time taken to transfer data over network.

A log displays time take by each of this process. For example, a log snippet may look as follows:

```
ID=File Open time, Bytes Read = 0, Total time = 0.011359, Average = 0.011359, Samples = 1

ID=Disk Read time, Bytes Read = 20, Total time = 0.013465, Average = 0.001417, Samples = 1

ID=Pipeline Allocation time, Bytes Read = 0, Total time = 0.000010, Average = 0.000010, Samples = 1

ID=Pipeline Write time, Bytes Read = 1160, Total time = 0.000004, Average = 282.587336, Samples = 1
```

The time value is in seconds. The highest "Total time" indicates that the majority of the time is spent in that operation. Generally it is the Disk Read Time.

If the time taken by Disk Read operation is high, the disk is the bottle neck. You can use Disk Read utility to verify the disk read performance.

If multiple reads are enabled on the disk, ensure that the hardware supports multiple reads. Enabling multiple reads degrades the performance if the hardware does not support. On the other hand if you have Raid disks or disks that allow multiple simultaneous reads, allowing multiple reads can improve the backup performance.

Slowness can be because of either the network or the media. For troubleshooting this slowness, you can use the testport, DiskRead and tapetest utilities. If the media is a tape, use tapetest utility. If the media is a disk, use DiskReadWrite utility in the write mode. For more information about all the utilities, refer to Tools and Utilities.

CAN I BACKUP THE DATA WHICH IS ENCRYPTED USING THE MCAFEE ENDPOINT ENCRYPTION?

Yes. You can perform the backup and restore of the data which is encrypted using the McAfee Endpoint Encryption.

SCAN METHODS

HOW DOES THE DATA CLASSIFICATION SCAN ENHANCE THE SCANNING CAPABILITIES OF AN IDATAAGENT?

When you enable the Data Classification Scan for a File System, a meta database is created. The meta database contains information about the files in the associated volume. The Data Classification service constantly updates the databases to track file additions, volume additions, content update to files, etc. Journals from the FSF driver are used to keep track of the updates to each meta database.

WHAT IS THE DEFAULT LOCATION OF THE META DATABASE?

On each volume, the meta database is created at the following location:

`System Volume Information\Bull Calypso \Data Classification`

It is named as `dc_<instance_number>.db`

For example: On the C drive, it would be `C:\System Volume Information\Bull Calypso \Data Classification\dc_<instance_number>.db`

You cannot relocate the database.

HOW TO TURN OFF THE DATA CLASSIFICATION SCAN?

Use the ServiceEnabled registry key to enable or disable the data classification monitoring threads for all volumes on a client computer.

If you want to disable data classification for selected volumes, use the VolumeFilters registry key to provide the list of volumes.

HOW MUCH HARD DISK SPACE IS CONSUMED BY THE METADATA DATABASE?

The meta databases created by Data Classification usually consume about 5% of the total space on the hard disk. Depending on the type of data and folder layout, the metafiles may consume additional space.

VSS

HOW MUCH DISK SPACE IS REQUIRED ON A VOLUME FOR THE VSS SHADOW COPY?

During a VSS backup, the free space needed on a volume for the shadow copy is related to the duration of the backup and the amount of changes being made to the data objects (files, databases) that are being backed up. VSS snapshots capture and copy disk blocks that are being changed by other processes while the backup for a particular object is running. If the backup runs longer, or there is a lot of disk activity (files or databases being changed). This causes VSS to copy more data blocks and therefore, use more disk space.

CAN I USE VSS TO BACKUP FILES ON CLUSTERED VIRTUAL SERVERS?

For Clustered Virtual Servers, use of VSS controls the backup method for file system data only, not system state components; system state data is backed up by the physical node(s), not by the virtual server(s). Note that the physical cluster node will automatically filter all shared disk resources, and the virtual server will automatically filter all physical disk resources from backup operations.

WHY DOES THE DIFFERENTIAL OR INCREMENTAL BACKUP BECOMES A FULL BACKUP WHEN VSS IS ENABLED?

If you use **Classic File** scan and the select the **Check archive bit during backups** option, then all backups by VSS on subclients will be converted to full backups. If you want to perform incremental or differential backup, you must use the **Change Journal** scan. If you want to use **Classic File** scan, do not select the **Check archive bit during backups** option.

WHEN I AM PERFORMING BACKUP OF A DATA, WHAT HAPPENS TO THE SYSTEM STATE COMPONENT?

When you want to backup only data, ensure that the the **Backup System State** check box is not selected on the **Content** tab of the **Subclient Properties** dialog box. Now when you perform the backup for any such subclient, the VSS will filter any system state component from the backup data. VSS will be used for this operation even when **Use VSS** option is not selected on the **General** tab of the of the **Subclient Properties** dialog box.

WILDCARDS

CAN I USE WILDCARDS TO SPECIFY A PATTERN OF FILE NAMES AS A CONTENT OF A SUBCLIENT?

You can use wildcards to specify a pattern of file names only in the default subclient. For more information, refer to Configuring The Default Subclient for Wildcard Support.

If a subclient contents has brackets which are treated as wildcards, e.g. [!ensure] and [?ensure], ensure that the default subclient is not associated to a subclient policy. If the contents is defined in a subclient policy, it will only be treated as literal path.

A SUBCLIENT IS CREATED IN 8.0 VERSION OF WINDOWS FILE SYSTEM *I*DATAAGENT AND IT CONTAINS WILDCARDS. CAN I USE THE SAME SUBCLIENT IN THE CURRENT VERSION OF WINDOWS FILE SYSTEM *I*DATAAGENT ?

In a user defined subclient, you can use the wildcards only in the last level of the path. For example: c:\temp** or c:\temp*.doc. Therefore, if you want to use a subclient created in 8.0 version of Windows File System *i*DataAgent, ensure that the wildcards are present only in the last level of the path.

If you have included a mount point or an UNC path in the subclient, ensure that the wildcards are not present in the path.

Troubleshooting - Windows File System Agents Backup

| Backup | Restore |

The following section provides information on some of the troubleshooting scenarios related to backup:

BACKUP FAILURE WHILE BACKING UP LARGE FILES OR SYSTEM VOLUMES

CAUSE

When backing up large files and/or system volumes, the Windows memory pool resources may run low and the backup may fail with errors reported in the Windows Event Viewer and the *i*DataAgent logs.

SOLUTION

Review the Microsoft documentation for increasing the maximum memory pool usage and paged memory pool size.

BACKUP GOES TO PENDING STATE WHILE BACKING UP AN UNFORMATTED VOLUME AND MOUNT POINTS

SYMPTOM

The Event Viewer displays following message: `Cannot scan <path>`

SOLUTION

Add the NSkipDirErrors Registry Key and set the value at 1 (or any value other than 0)

BACKUP GOES TO PENDING STATE FOR POLYSERVE (NON-MICROSOFT CLUSTERS)

SYMPTOM

The backup job for a Polyserve goes to pending state

SOLUTION

Exclude the following folders from the backup and anti-virus scan:

For backup	c:\program files\polyserve\matrixserver\conf\mounts
For anti virus scans	c:\program files\polyserve\matrixserver\conf
	`<Calypso install directory>`/Base

During Disaster Recovery, open up the Polyserve Configuration Utility and export the configuration to the node that was rebuilt. This will ensure complete synchronization prior to introducing a rebuilt node again into the matrix.

BACKUP OF SUBCLIENT THAT CONTAINS ONLY FILES AND NO FOLDERS

CAUSE

When a subclient contains only files and no folders, the backup can fail if you select Data Classification as the scan method.

SOLUTION

When a subclient contains only files and no folders, always use Classic File Scan as the scan method.

COMPLETED WITH ONE OR MORE ERRORS

Backup jobs from Windows File System *i*DataAgent will be displayed as "Completed w/ one or more errors" in the Job History in the following cases:

For subclient containing only system state backup:

- Fails to backup critical component - the job status is failed
- Fails to backup non-critical component - the job status is completed w/ one or more errors

For subclient containing system state backup along with File system data:

- Failure to backup critical component - marks the job as completed w/ one or more errors, so the data can continue to backup.
- Failure to backup non-critical component - marks the job as completed w/ one or more errors

Troubleshooting - Windows File System Agents Restore

| Backup | Restore |

ERROR MESSAGES DURING BROWSE OPERATION

When you are browsing the backup data, one of the following error condition can occur:

SYMPTOM

Failure to connect the MediaAgent

SOLUTION

Check the connectivity between MediaAgent and the client computer. Add the client host name and IP address in the host file on the MediaAgent.

SYMPTOM

Index Cache Inaccessible

SOLUTION

Check the connectivity between MediaAgent and the client computer. Add the client host name and IP address in the host file on the MediaAgent.

FILES PREVENTED FROM OVERWRITING

CAUSE

When a file is in use by the operating system or open with exclusive read access by an application, the file is locked and cannot be overwritten.

SOLUTION

The system automatically restores the file with another file name within the same directory and records the instance in the Windows registry. These are restored automatically at the time when the computer is restarted.

These files can be viewed from the Restore Job Summary Report They have a "Needs Reboot" tag attached to it. They can be viewed in the **Restore History** from the CommCell Console. In order to view these files you need to select the **Failed Objects** check box in **Job Summary Selection** tab. These files are displayed as Skipped files.

CLUSTER SERVICES ARE NOT STARTED AUTOMATICALLY DURING DISASTER RECOVERY

CAUSE

If the cluster disks were repartitioned, a failure message may appear because the disk GUIDs for the quorum may have been changed.

SOLUTION

If the cluster service does not start, or if you see Event ID 1034 in the System Event Log, reference the KB 305793 and KB 280425 Microsoft Knowledge Base articles on http://support.microsoft.com/ to get the cluster service back online.

If the cluster service does not start automatically, start it manually in the service control manager.

RECOVERING DATA ASSOCIATED WITH DELETED CLIENTS AND STORAGE POLICIES

The following procedure describes the steps involved in recovering data associated with the following entities:

● Deleted Storage Policy
● Deleted Client, Agent, Backup Set or Instance

BEFORE YOU BEGIN

This procedure can be performed when the following are available:

● You have a Disaster Recovery Backup which contains information on the entity that you are trying to restore. For example, if you wish to recover a storage policy (and the data associated with the storage policy) that was accidentally deleted, you must have a copy of the disaster recovery backup which was performed before deleting the storage policy.

- Media containing the data you wish to recover is available and not overwritten.

- If a CommCell Migration license was available in the CommServe when the disaster recovery backup was performed, no additional licenses are required. If not, obtain the following licenses:

  - IP Address Change license

  - CommCell Migration license

  See License Administration for more details.

- A standby computer, which will be used temporarily to build a CommServe.

RECOVERING DELETED DATA

1. Locate the latest Disaster Recovery Backup which contains the information on the entity (Storage Policy, Client, Agent, Backup Set or Instance) that you are trying to restore.

   - You can check the Phase 1 destination for the DR Set or use Restore by Jobs for CommServe DR Data to restore the data.

   - If the job was pruned and you know the media containing the Disaster Recovery Backup, you can move the media in the **Overwrite Protect Media** Pool. See Accessing Aged Data for more information. You can then restore the appropriate DR Set associated with the job as described in Restore by Jobs for CommServe DR Data.

   - If the job is pruned and you do not know the media containing the Disaster Recovery Backup, you can do one of the following:

     If you regularly run and have copies of the Data on Media and Aging Forecast report you can check them to see if the appropriate media is available.

2. On a standby computer, install the CommServe software. For more information on installing the CommServe, see CommServe Deployment.

3. Restore the CommServe database using the CommServe Disaster Recovery Tool from the Disaster Recovery Backup described in Step 1. (See Restore a Disaster Recovery Backup for step-by-step instructions.)

4. Verify and ensure that the **Bull Calypso Client Event Manager Bull Calypso Communications Service (EvMgrS)** is running.

5. If you did not have a CommCell Migration license available in the CommServe when the disaster recovery backup was performed, apply the IP Address Change license and the CommCell Migration license on the standby CommServe. See Activate Licenses for step-by-step instructions.

6. Export the data associated with the affected clients from the standby CommServe as described in Export Data from the Source CommCell.

   When you start the Command Line Interface to capture data, use the name of the standby CommServe in the –
   `commcell` argument.

7. Import the exported data to the main CommServe as described in Import Data on the Destination CommCell.

   This will bring back the entity in the CommServe database and the entity will now be visible in the CommCell Browser. (Press F5 to refresh the CommCell Browser if the entity is not displayed after a successful merge.)

8. If you have additional data that was backed up after the disaster recovery backup and before the deletion of the entity, use the procedure described in Import Metadata from a Tape or Optical Media to obtain the necessary information.

9. You can now browse and restore the data from the appropriate entity.

   As a precaution, mark media (tape and optical media) associated with the source CommCell as READ ONLY before performing a data recovery operation in the destination CommCell.

ERROR DURING THE FULL SYSTEM RESTORE OF WINDOWS VISTA OR WINDOWS SERVER 2003

SYMPTOM

During the Disaster Recovery of Windows Vista or Windows Server 2003, you may get the following error:

```
An unauthorized change was made to Windows
```

SOLUTION

When rebuilding an entire computer, it is required that the Windows service pack and hotfixes in the backup are also applied on the target computer. The service pack on the target must always match the backup prior to a restore. To restore the hotfix from the backups, select the **Overwrite Files** check box on the **Restore Options** dialog box and then select the **Unconditional Overwrite** option.

Select this option if the source computer had Internet Explorer 8.0 and the target computer has Internet Explorer 7.0.

AN UNAUTHORIZED CHANGE WAS MADE TO WINDOWS. YOU MUST RETYPE YOUR WINDOWS SERVICE PRODUCT KEY TO ACTIVATE THE LICENSE.

SYMPTOM

During the Disaster Recovery of Windows Vista or Windows Server 2003, you may get the following error:

```
An unauthorized change was made to Windows. You must retype your Windows Service Product Key to activate the license.
```

SOLUTION

If the Windows product license key is not activated on the target computer prior to a full restore, you will receive the following message, and you will be required to provide the product license key after the restore. Refer to the check list that you have creating while planning for disaster recovery.

FILES ON THE SINGLE INSTANCE STORAGE LINKED VOLUMES APPEAR CORRUPTED AFTER RESTORE

SYMPTOM

After the full system restore, the SIS-linked files are not be accessible, and they appear to be corrupted. The name and size of a SIS-linked file appear as normal. However, the file is a zero-length file and it does not have access to the data it should contain.

SOLUTION

Before starting the restore, ensure the following

- The source and target drive letter are the same.
- The SIS/Groveler are running and attached to the volume to which you are restoring data.

For more information on How to restore a volume that is managed by Single Instance Storage, refer the KB 263027 Microsoft Knowledge Base article on http://support.microsoft.com/.

COMPLETED WITH ONE OR MORE ERRORS

Restore jobs from Windows File System iDataAgent will be displayed as "Completed w/ one or more errors" in the Job History in the following cases:

For subclient containing only system state restore:

- Fails to restore critical component - the job status is failed
- Fails to restore non-critical component - the job status is completed w/ one or more errors

For subclient containing system state restore along with File system data:

- Failure to restore critical component - marks the job as completed w/ one or more errors, so the data can be recovered.
- Failure to restore non-critical component - marks the job as completed w/ one or more errors

UPDATING FEATURES AND ROLES ON WINDOWS SERVER 2008

On Windows Server 2008, when you perform the Full System Restore, the Features and Roles do not get updated.

Select **Configure Refresh** from the **Server Manager** main page and update Features and Roles as they are not updated during a restart.

BSoD ERROR AFTER A FULL SYSTEM RESTORE OPERATION

SYMPTOM

After the full system restore, the computer reboots with a BSoD error screen.

RESOLUTION

Make sure that the following are not filtered while performing the full system restore operation:

1. *:\drivers*
2. *:\win*\inf*

DISTRIBUTED COMPONENT OBJECT MODEL (DCOM) COMPONENT APPEARS DISABLED AFTER A RESTORE OPERATION

SYMPTOM

Distributed Component Object Model (DCOM) component appears disabled after a restore operation is performed on the client computer.

SOLUTION

Run the following command from the command prompt on the client computer after the restore operation is complete:

```
%windir%\system32\msdtc.exe -resetLog
```

SYSTEM STATE RESTORE FAILS

SYMPTOM

If you back up certain system protected files in a cluster shared drive and the drive is no longer available, then the System State restore fails.

SOLUTION

Create the nIgnoreNonexistingClusterDrivePathErrors additional setting to skip the files that belong to the cluster shared drive. The restore operation then completes successfully for other files.

Deployment - 1-Touch for Windows

| Deployment | Configuration | Recovery | Troubleshooting | FAQ |

◀ Previous   Next ▶

TABLE OF CONTENTS

1-Touch Recovery allows you to recover the entire computer system without installing the Operating system or any other software.

Perform the following to enable 1-Touch Recovery:

Install 1-Touch Server Software

Setup a Remote Software Cache
  Configure a Remote Software Cache For 1-Touch Server
  Download and Install Software Updates on 1-Touch Server
  Apply Updates in 1-Touch Server Cache to 1-Touch Live CD Boot image

Install Windows File System iDataAgent on the Client Computer

BEFORE YOU BEGIN

Download Software Packages
  Download the latest software package to perform the install.

Software Installation Discs
  The software package is also available on the software installation discs.

System Requirements for 1-Touch Server and Client
  Verify that the computer in which you wish to install the 1-Touch Software satisfies the System Requirements.

Overview
  Provides comprehensive information about 1-Touch feature

INSTALL THE 1-TOUCH SERVER SOFTWARE

Install 1-Touch Server software on the computer that satisfies the minimum system requirements. This computer is referred as the 1-Touch Server.

1. Run **Setup.exe** from the **Software Installation Disc** on the computer that satisfies the minimum system requirements.

2. Select the required language.
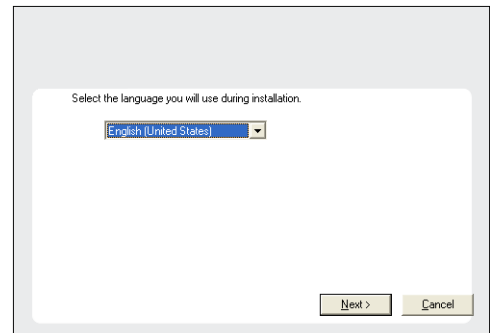
    Click **Next**.

3. Select the option to install software on this computer.
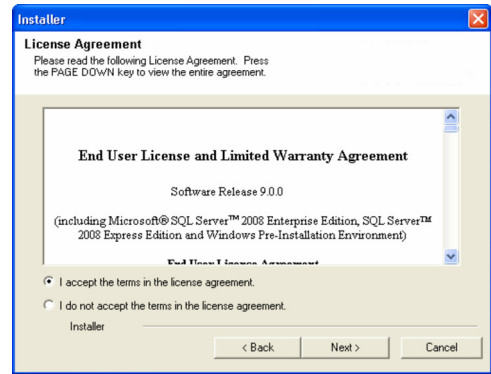
    NOTES

    ● The options that appear on this screen depend on the computer in which the software is being installed.
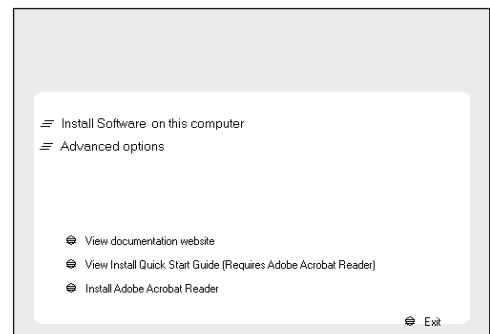
4. Select **I accept the terms in the license agreement**.

    Click **Next**.

5. Expand **Client Modules** | **Backup & Recovery** | **File System** and select **1-Touch Server**.

Click **Next**.

6. If this computer and the CommServe is separated by a firewall, select the **Configure firewall services** option and then click **Next**.

For firewall options and configuration instructions, see Firewall Configuration and continue with the installation.

If firewall configuration is not required, click **Next**.
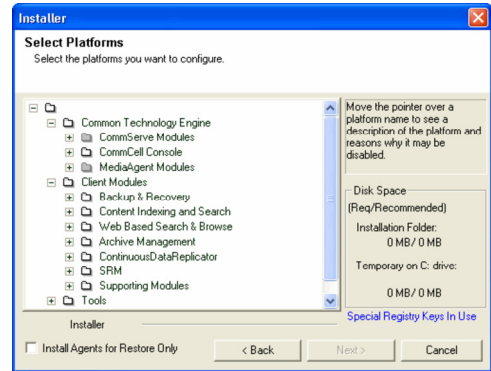
7. Enter the fully qualified domain name of the **CommServe Host Name**.

Click **Next**.

> Do not use space and the following characters when specifying a new name for the CommServe Host Name:
>
> \|`~!@#$%^&*()+=<>/?,[]{}:;'"
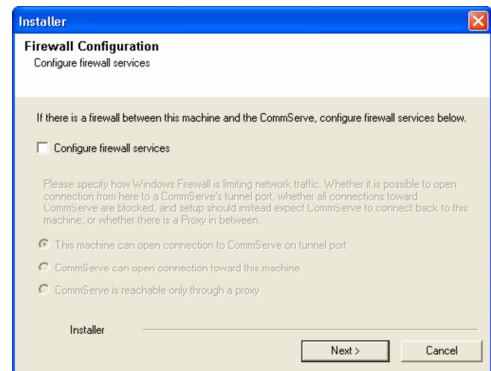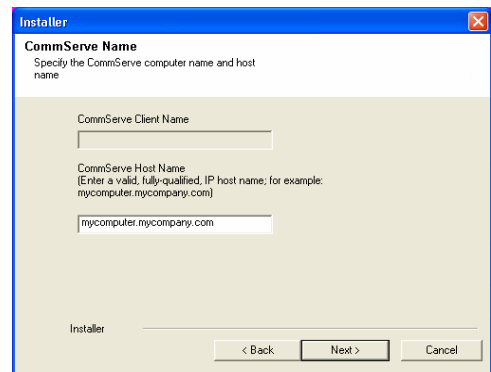
8. Click **Next**.

9. Select **Add programs to the Windows Firewall Exclusion List**, to add CommCell programs and services to the Windows Firewall Exclusion List.

Click **Next**.

This option enables CommCell operations across Windows firewall by adding CommCell programs and services to Windows firewall exclusion list.

It is recommended to select this option even if Windows firewall is disabled. This will allow the CommCell programs and services to function if the Windows firewall is enabled at a later time.

10. Verify the default location for software installation.

Click **Browse** to change the default location.

Click **Next**.

- Do not install the software to a mapped network drive.
- Do not use the following characters when specifying the destination path:

  / : * ? " < > | #
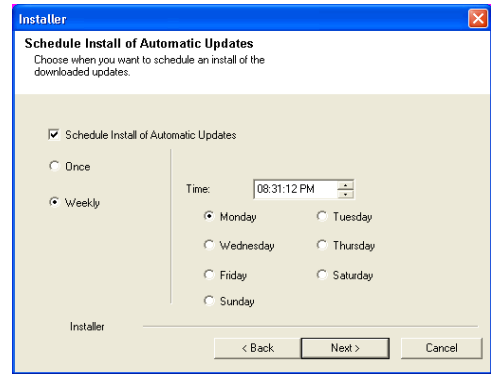
  It is recommended that you use alphanumeric characters only.

11. Click **Next**.
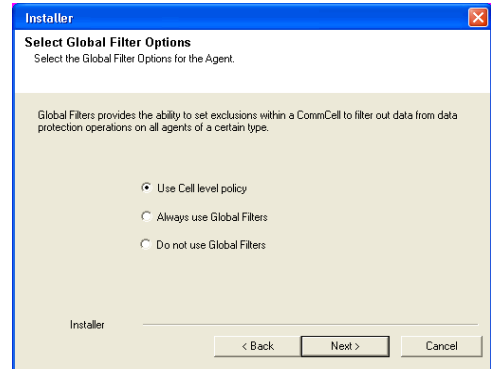
12. Click **Next**.
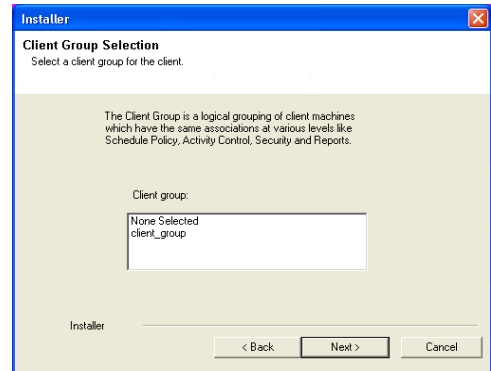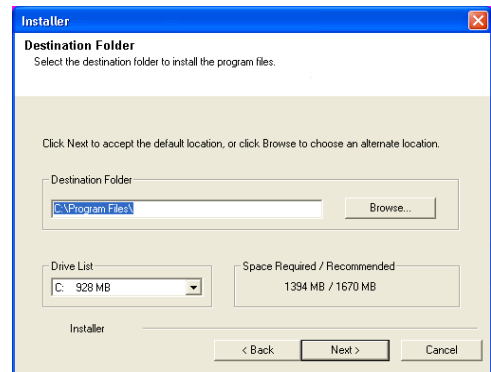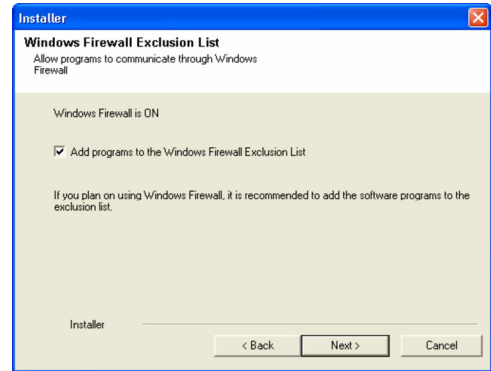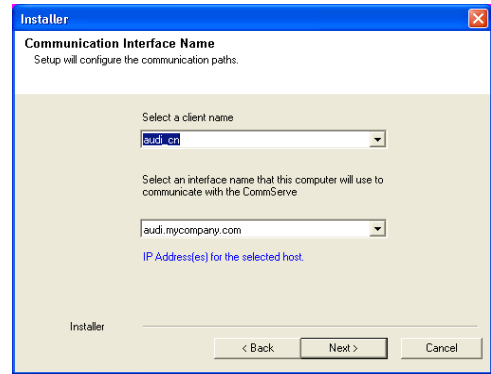
13. Click **Next**.

14. Select a **Storage Policy**.

Click **Next**.

If you do not have Storage Policy created, this message will be displayed.

Click **OK**.

You can create the Storage Policy later in step 20.

15. Enter the path for 1-Touch Server distribution folder.

Click **Next**.

NOTES

This folder will contain the following:

- Client Files share - It will contain client files and folders selected for recovery.
- Image share - It will contain the files, required to deploy the File System *i*DataAgent. It will also contain a `Boot_image` folder with **1touchBoot.iso** for burning a bootable CD-ROM
- WINDIST folder- It will contain shares housing the Microsoft Windows Distribution folders
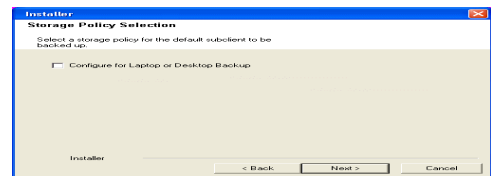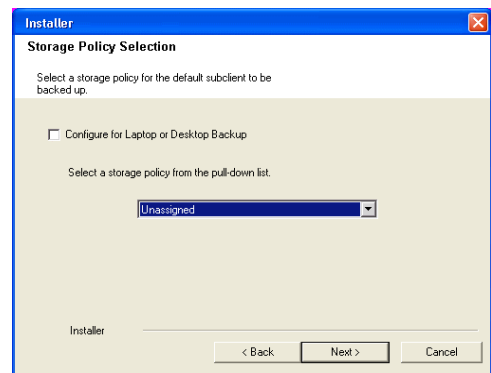
16. Click **Next**.
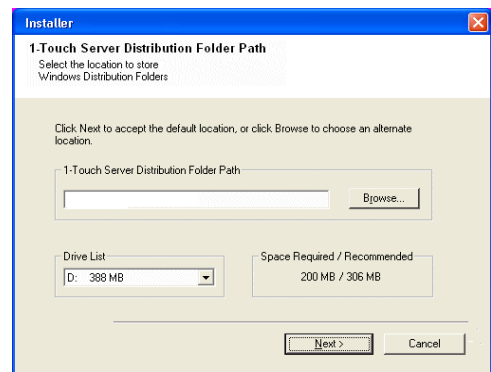
17. Click **Next**.
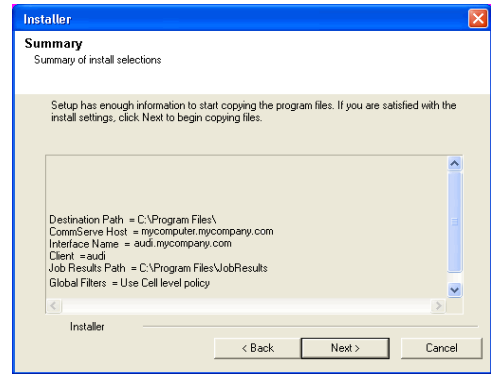
18. Select **Do not launch 1-Touch Options now. I will prepare the 1-Touch Server at a later time**.

Click **Next**.
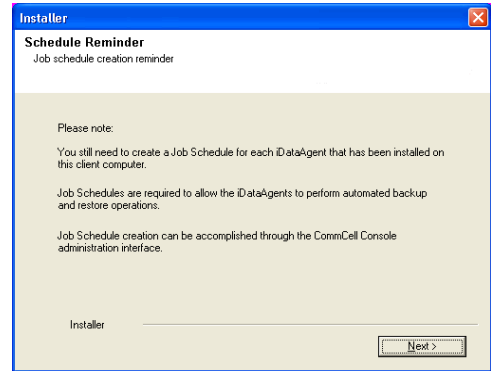
19. Click **Finish**.
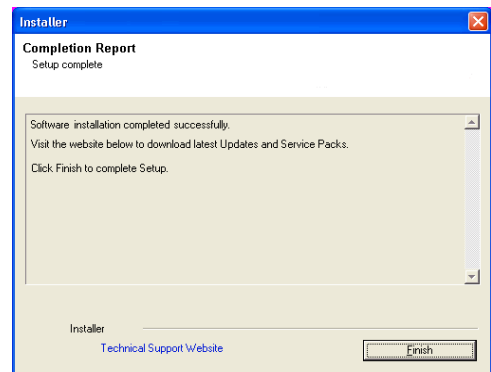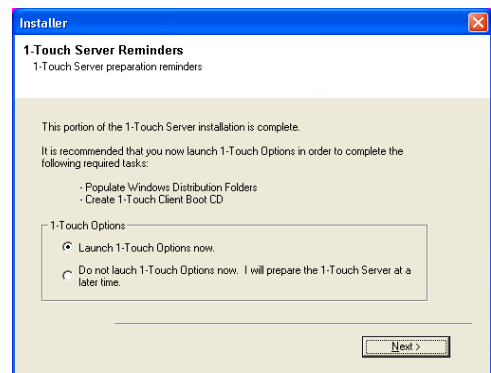
If you already have a storage policy selected in step 14, click the **Next** button available on the bottom of the page to proceed to the **Configuration** section.

If you do not have Storage Policy created, continue with the following step.

20. Create a Storage Policy:

1. From the CommCell Browser, navigate to **Policies**.

2. Right-click the **Storage Policies** and then click **New Storage Policy**.

3. Follow the prompts displayed in the Storage Policy Wizard. The required options

are mentioned below:

○ Select the Storage Policy type as **Data Protection and Archiving** and click **Next**.

○ Enter the name in the **Storage Policy Name** box and click **Next**.

○ From the **Library** list, click the name of a disk library to which the primary copy should be associated and then click **Next**.

Ensure that you select a library attached to a MediaAgent operating in the current release.

○ From the **MediaAgent** list, click the name of a MediaAgent that will be used to create the primary copy and then click **Next**.

○ For the device streams and the retention criteria information, click **Next** to accept default values.

○ Select **Yes** to enable deduplication for the primary copy.

○ From the **MediaAgent** list, click the name of the MediaAgent that will be used to store the Deduplication store.

Type the name of the folder in which the deduplication database must be located in the Deduplication Store Location or click the Browse button to select the folder and then click **Next**.

○ Review the details and click **Finish** to create the Storage Policy.

SETUP A REMOTE SOFTWARE CACHE

The 1-Touch server will be used to create the 1-Touch Live CD required for 1-Touch recovery. The 1-Touch Live CD boots the client computer and and installs Bull Calypso on the client computer during 1-Touch recovery. You must download and install all the latest updates for Bull Calypso and WinPE on the 1-Touch server.

CONFIGURE A REMOTE CACHE FOR 1-TOUCH SERVER

When the 1-Touch Server software is not installed on a CommServe, you must configure a remote cache for the 1-Touch server. A remote cache will store all the updates for 1-Touch Server software, Windows File System *i*DataAgent and WinPE. You can skip this configuration if 1-Touch server is installed on the CommServe.

1. From the CommCell Console, right click the CommServe computer and click **All Tasks | Add/Remove Software | Add/Remove Software Configuration**.
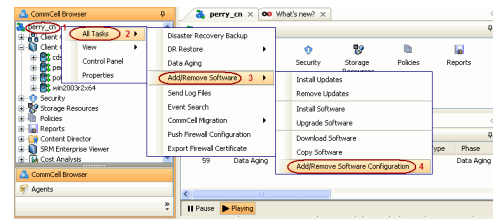
2.
- Select **Remote Software Cache** tab
- Click **Add**.
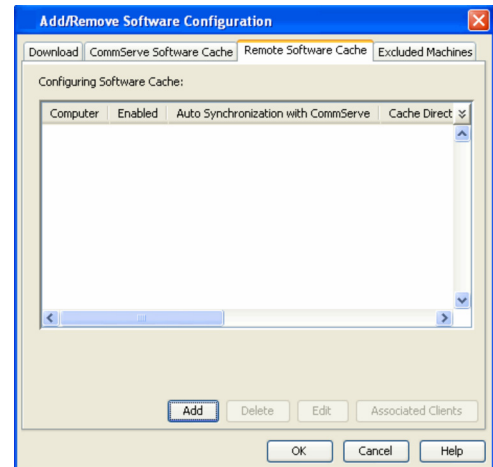
3.
- Select the client **Computer**.
- Click **Enable Remote Software Cache**.
- Enter the path to **Cache Directory**.
- Click **OK**.
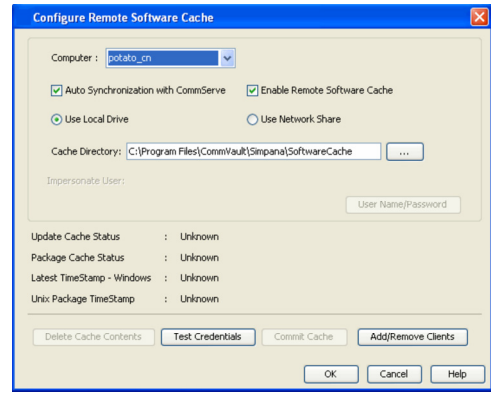
DOWNLOAD AND INSTALL UPDATES ON 1-TOUCH SERVER

Before creating the 1-Touch Live CD, download all the software updates for 1-Touch Server software, Windows File System *i*DataAgent and WinPE.

1.   From the CommCell Browser, right-click on the CommServe computer node, and click **All Tasks -> Add/Remove Software -> Download Software**.
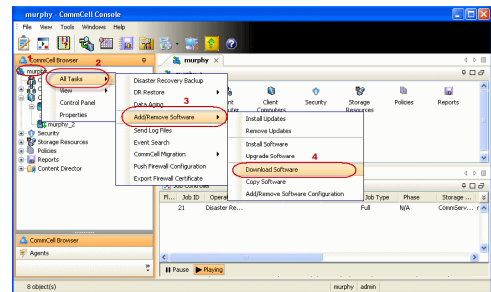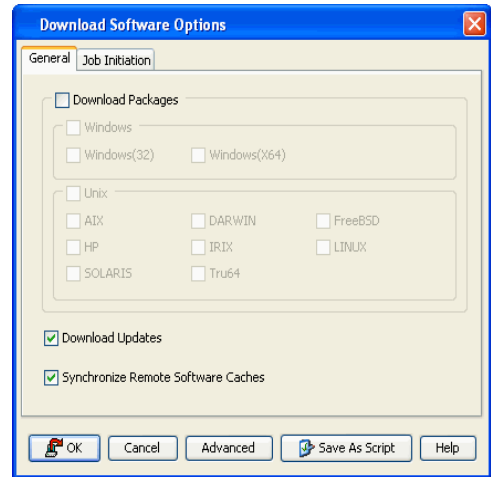
2.   Click **OK**.

3.
- Click **Job Initiation** tab.

  By default **Immediate** option is selected.
- Click **OK**.
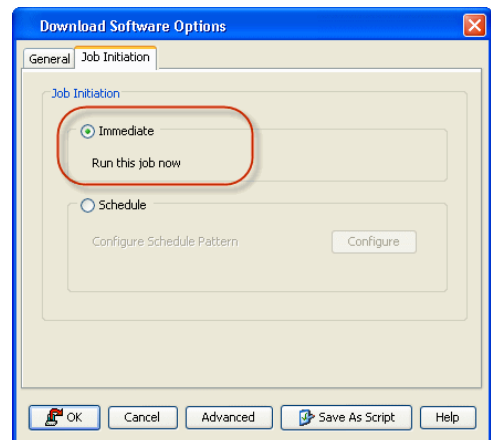
4. You can track the progress of the job from the **Job Controller** window. The software updates are stored automatically in the CommServe Cache and 1-Touch Server cache.
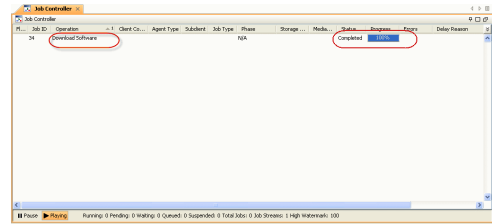
5. From the CommCell Browser, right-click on the 1-Touch Server computer node, and click **All Tasks -> Add/Remove Software -> Install Updates**

6.
- Click **Job Initiation** tab.
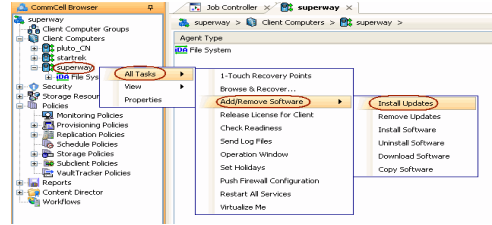
  By default **Immediate** option is selected.

- Click **OK**.
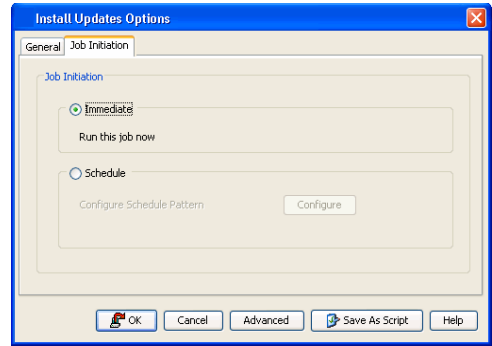
APPLY UPDATES IN 1-TOUCH SERVER CACHE TO 1-TOUCH LIVE CD BOOT IMAGE

Follow the steps given below to mount the **1-Touch Live** CD and apply the software updates to the ISO:

1.
- From the CommCell Console, navigate to **<Client Computers> | < 1-Touch Server>.**
- Right-click and click **All Tasks | Add/Remove Software | Copy Software**.
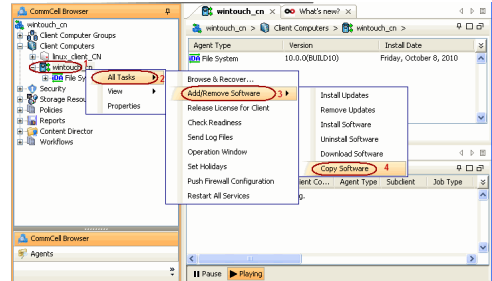
2.
- Select **Copy and Update One Touch Cache**.
- Click **OK**.

  All the software updates are copied to 1-Touch server cache and then integrated with 1-Touch ISO for each type of processor.
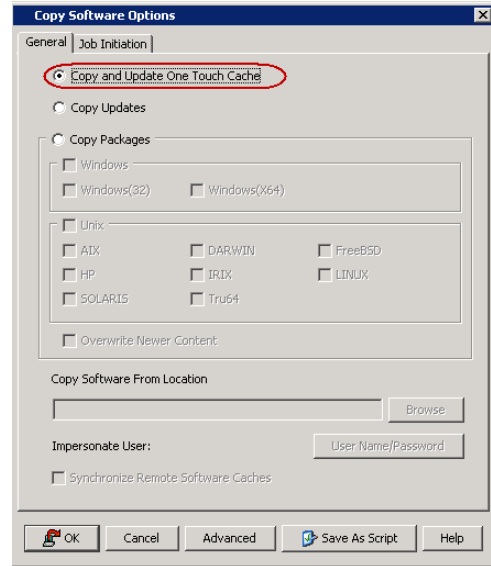
INSTALL WINDOWS FILE SYSTEM *i*DATAAGENT ON THE CLIENT COMPUTER

Install Windows File System *i*DataAgent on the computers that satisfies the minimum system requirements. The computer is referred as the 1-Touch Client.

The software can be installed using one of the following methods:
- Method 1: Interactive Install - to install directly on client computer.
- Method 2: Install Software from CommCell Console - to install remotely on a client computer.

INTERACTIVE INSTALL

1. Run **Setup.exe** from the **Software Installation Disc** on the computer that satisfies the minimum system requirements.

2. Select the required language.

Click **Next**.

3. Select the option to install software on this computer.

NOTES

- The options that appear on this screen depend on the computer in which the software is being installed.

4. Select **I accept the terms in the license agreement**.

Click **Next**.

5. Expand **Client Modules** | **Backup & Recovery** | **File System** and select **Windows File System** *i***DataAgent**.

Click **Next**.

6. Click **YES** to install Microsoft .NET Framework package.

● This prompt is displayed only when Microsoft .NET Framework is not installed.
● Once the Microsoft .NET Framework is installed, the software automatically installs the Microsoft Visual J# 2.0 and Visual C++ redistributable packages.

7. If this computer and the CommServe is separated by a firewall, select the **Configure firewall services** option and then click **Next**.

For firewall options and configuration instructions, see Firewall Configuration and continue with the installation.

If firewall configuration is not required, click **Next**.

You cannot perform 1-Touch restore and VirtualizeMe operations if you configure firewall between CommServe and the client computer.

8. Enter the fully qualified domain name of the **CommServe Host Name**.

Click **Next**.

Do not use space and the following characters when specifying a new name for the CommServe Host Name:

\|`~!@#$%^&*()+=<>/?,[]{}:;'"

9. Click **Next**.

10.   Select **Add programs to the Windows Firewall Exclusion List**, to add CommCell programs and services to the Windows Firewall Exclusion List.

Click **Next**.

This option enables CommCell operations across Windows firewall by adding CommCell programs and services to Windows firewall exclusion list.

It is recommended to select this option even if Windows firewall is disabled. This will allow the CommCell programs and services to function if the Windows firewall is enabled at a later time.

11.   Verify the default location for software installation.

Click **Browse** to change the default location.

Click **Next**.

● Do not install the software to a mapped network drive.
● Do not use the following characters when specifying the destination path:

/ : * ? " < > | #

It is recommended that you use alphanumeric characters only.

12.   Select a Client Group from the list.

Click **Next**.

This screen will be displayed if Client Groups are configured in the CommCell Console.

13.   Click **Next**.

14. Click **Next**.

15. Select a **Storage Policy**.
    Click **Next**.

    If you do not have Storage Policy created, this message will be displayed.
    Click **OK**.

    You can create the Storage Policy later in step 19.

16. Click **Next**.
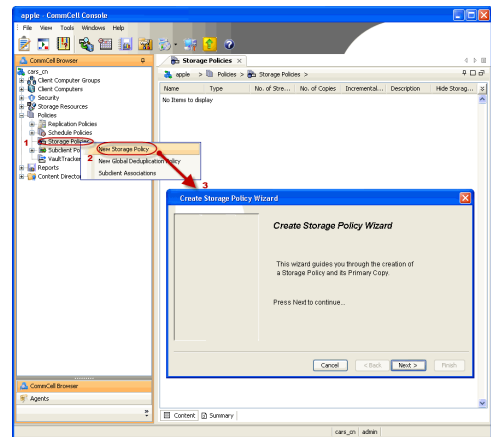

17. Click **Next**.

18. Click **Finish**.

If you already have a storage policy selected in step 15, click the **Next** button available on the bottom of the page to proceed to the **Configuration** section.

If you do not have Storage Policy created, continue with the following step.

19. Create a Storage Policy:

1. From the CommCell Browser, navigate to **Policies**.

2. Right-click the **Storage Policies** and then click **New Storage Policy**.

3. Follow the prompts displayed in the Storage Policy Wizard. The required options are mentioned below:

○ Select the Storage Policy type as **Data Protection and Archiving** and click **Next**.

○ Enter the name in the **Storage Policy Name** box and click **Next**.

○ From the **Library** list, click the name of a disk library to which the primary copy should be associated and then click **Next**.

Ensure that you select a library attached to a MediaAgent operating in the current release.

○ From the **MediaAgent** list, click the name of a MediaAgent that will be used to create the primary copy and then click **Next**.

○ For the device streams and the retention criteria information, click **Next** to accept default values.

○ Select **Yes** to enable deduplication for the primary copy.

○ From the **MediaAgent** list, click the name of the MediaAgent that will be used to store the Deduplication store.

Type the name of the folder in which the deduplication database must be located in the Deduplication Store Location or click the Browse button to select the folder and then click **Next**.

○ Review the details and click **Finish** to create the Storage Policy.
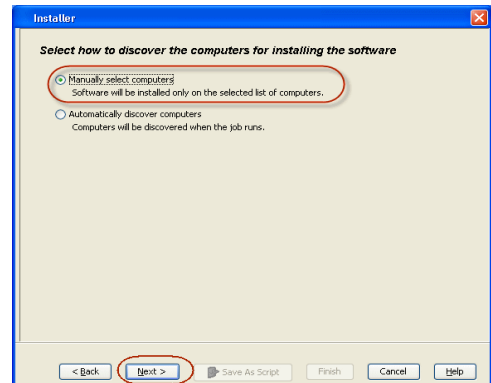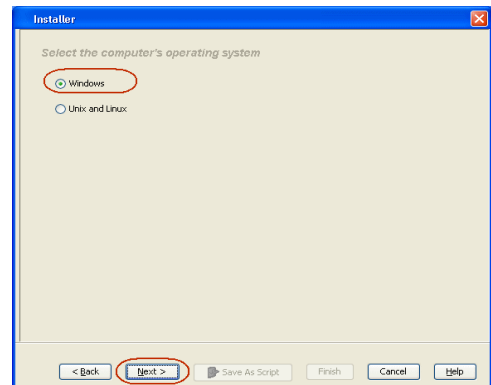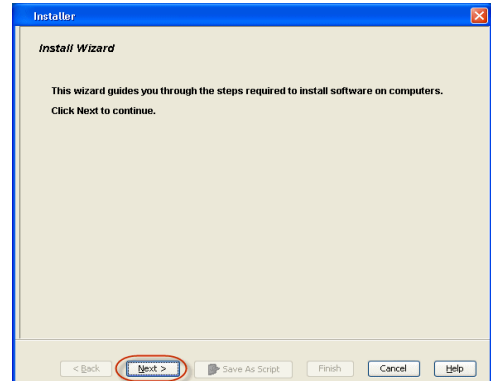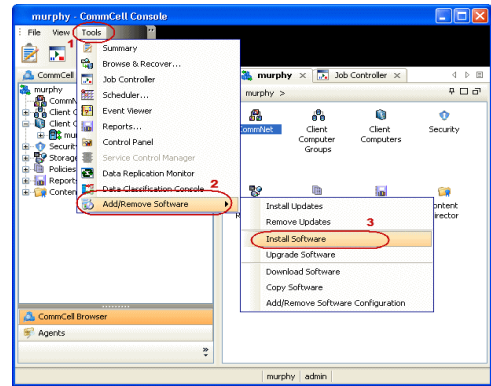

METHOD 2: INSTALL SOFTWARE FROM COMMCELL CONSOLE

1. From the CommCell Browser, select **Tools** | **Add/Remove Software** | **Install Software.**
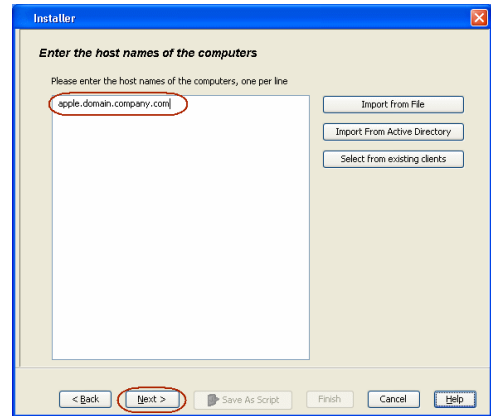
2. Click **Next**.

3. Select **Windows**.

    Click **Next**.

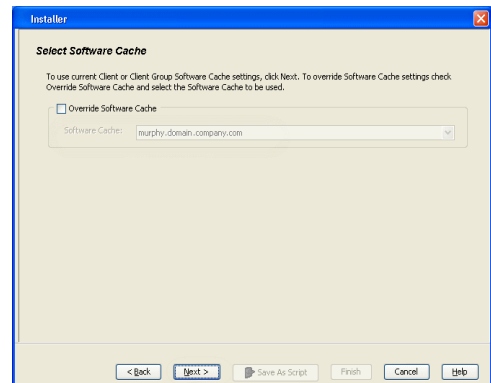4. Select **Manually Select Computers**.

    Click **Next**.

5. Enter the fully qualified domain name of the computer in which you wish to install.

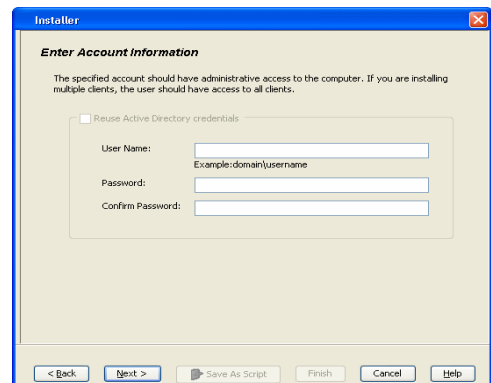   For example: `apple.domain.company.com`
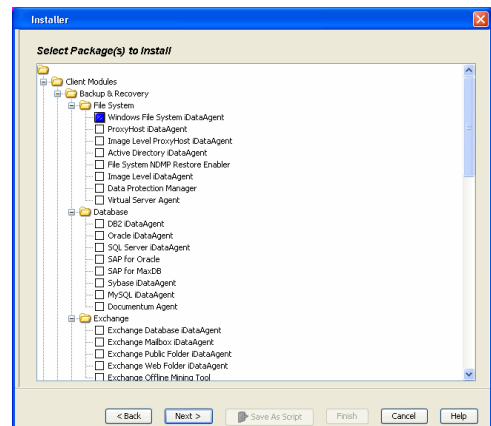
    Click **Next**.

6. Click **Next**.

7. Specify **UserName** and **Password**.
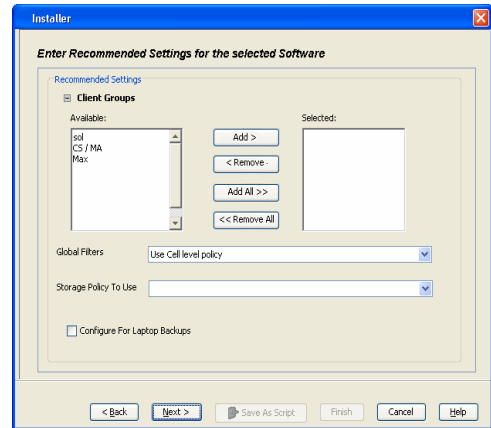
Click **Next**.

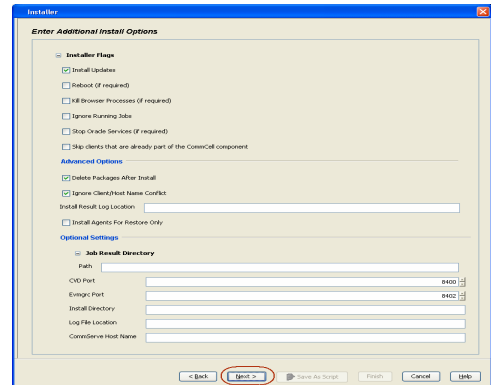**8.** Select **Windows File System iDataAgent**.
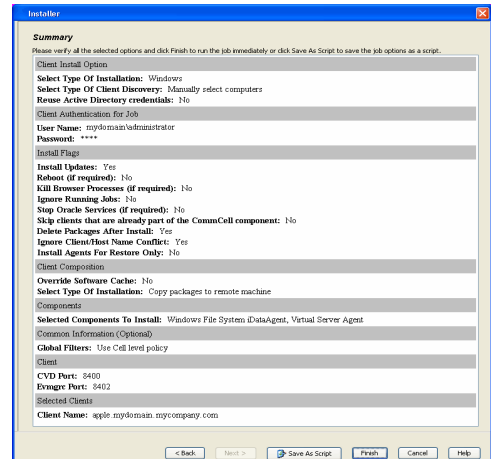
Click **Next**.

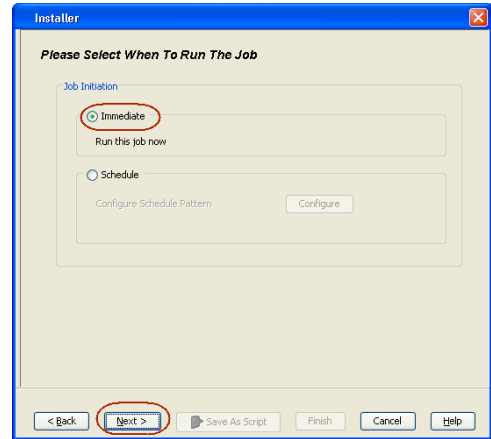
9. Click **Next**.

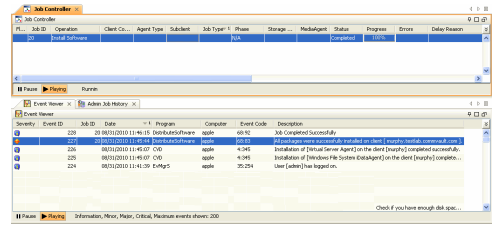**10.** Click **Next**.

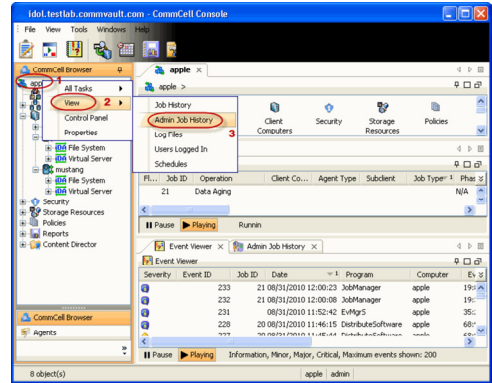**11.** Select **Immediate**.

Click **Next**.

12. Click **Finish**.

13. You can track the progress of the job from the **Job Controller** or **Event Viewer** window.

14. Once the job is complete, right-click the **CommServe** computer, click **View** and then click **Admin Job History**.

15. Select **Install/Upgrade/Remove Software**.

Click **OK**.

16. You can view the following details about the job by right-clicking the job:
- Items that succeeded during the job
- Items that failed during the job
- Details of the job
- Events of the job
- Log files of the job

Configuration - 1-Touch for Windows
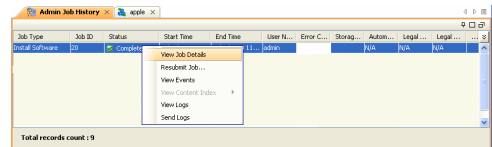
| Deployment | Configuration | Recovery | Troubleshooting | FAQ |

◀ Previous   Next ▶

TABLE OF CONTENTS

Basic Configuration

Configuration for Online Restore

Additional Options

BASIC CONFIGURATION

ENABLE 1-TOUCH BACKUP

The windows system state backup includes all the information required for 1-Touch recovery. Follow the steps given below to ensure that the system state data is included in a subclient:

1.
- From the CommCell Console, navigate to **<Client>** | **File System *i*DataAgent** | **defaultBackupSet**.
- Right-click the default subclient, and click **Properties**.
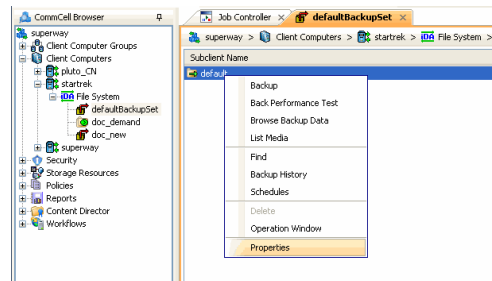
2.
- Click the **General** tab.
- Ensure that **Use VSS for System State** check box is selected.
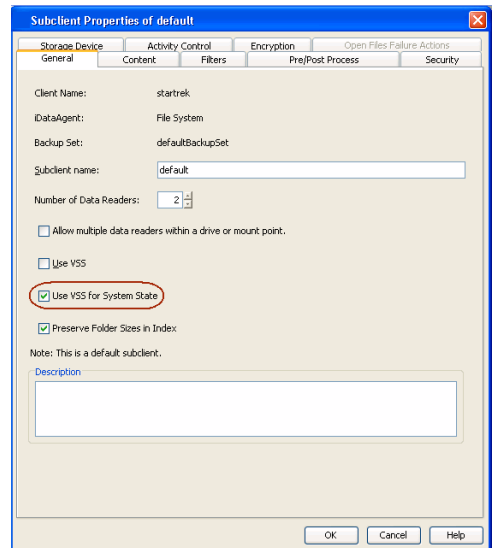
3.
- Click the **Content** tab.
- Ensure that the **Backup System State** check box is selected.
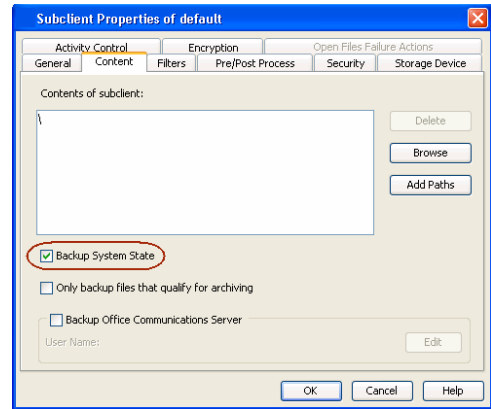
You can use any subclient to backup the system state data. However, if you want to perform the non interactive restore, use the default subclient to back up the system state data.

PERFORM A BACKUP OF 1-TOUCH CLIENT

Before recovering a client, ensure that you have run at least one full backup for the subclient that contains the system state data.

> If you are performing backup of a Windows 7 client, ensure that the Administrator account is enabled. You cannot perform the Offline restore if administrator account is not enabled while performing the backup.

Follow the steps given below to perform a full backup:
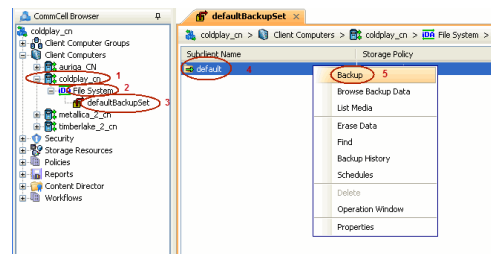
1.	• From the CommCell Console, navigate to **<Client>** | **File System iDataAgent** | **defaultBackupSet**. • Right-click the subclient, and click **Backup**.	
2.	• Select **Full**. • Select **Immediate**. • Click **OK**.	
3.	You can track the progress of the backup job from the **Job Controller** window. When the backup job has completed, the **Job Controller** displays the status as `Completed`.	
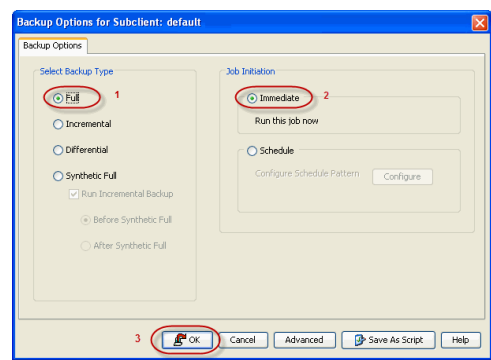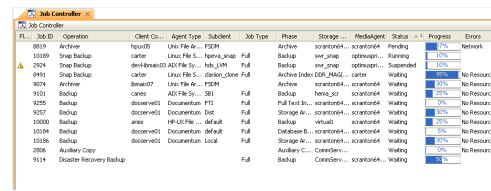
CREATE A CHECKLIST

If you want to perform an Online Restore or an Interactive Restore, ensure that you have all the required client information before starting the a restore. Create a checklist that contains the following client information:

REQUIRED INFORMATION	HOW TO FIND IT
CommCell Credentials	

	1. Invoke the CommCell Console on the client computer 2. Note down the username and password to login to CommServe from CommCell Console.
Windows Credentials	1. Login to 1-Touch server. 2. Note down username and password.
Network Adapters and Drivers	1. Click **Start | Programs | Accessories | System Information**. 2. In the **System Information** dialog box, click **Components | Network |Adapter**. 3. Note down the Network Adapter and Drivers information.
Mass Storage Drivers	1. Click **Start | Programs | Accessories | System Information**. 2. In the **System Information** dialog box, click **Software Environment | System Drivers**. 3. Note down the driver information.
CommServe Host Name	1. From the CommCell Console, navigate to **<Client>.** 2. Right click the **<Client>** and click **Properties**. 3. Select **General** tab. 4. Note down the **CommServe HostName**.
CommServe IP Address	1. Login to CommServe using the administrator login and password. 2. Invoke the Command Prompt. 3. Type `ipconfig`
Windows License Key	Refer to the License document. Note down the string of 25 letters on the license document.

CONFIGURATION FOR ONLINE RESTORE

If you are not planning to perform an online restore, skip the following steps and go to **Recovery** section. Follow the steps given below before starting an Online restore:

MANAGE WINDOWS DISTRIBUTION SHARES, SERVICE PACKS, AND HOT FIXES

Check if all the required Windows Distribution Shares are available on the 1-Touch Server. Also, ensure that all the service packs and hot fixes are integrated with the distribution share.

If required, you can add the Windows Distribution Shares. You will need the installation CD and the License Key for the appropriate version of the Windows operating system.

1. Login to 1-Touch Server.
2. Click **Start \| Programs \| Bull Calypso \| Calypso \| 1-Touch**.
3. Click **Windows Distribution Manager**.
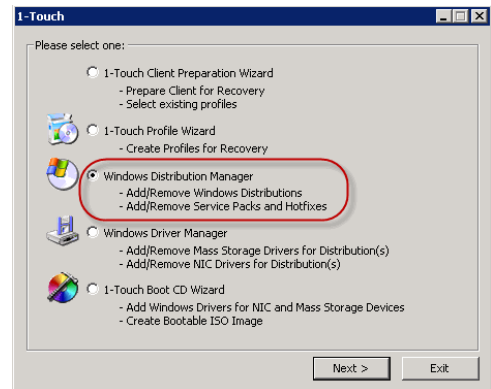
4. Click **Add**.

5.

- Select the **Product Version**.
- Enter the **Folder name to create** a new windows distribution share.
- Enter the **Number of source folders, CDs, DVDs to import from**.
- Enter **Source Location**.
- Enter the **User** name and **Password**.
- Enter the **License Key**.
- Click **Add**.

This distribution share will be available for selection in the **1-Touch Client Preparation Wizard**.

6.

- Review the Hotfixes and service packs change log.
- Select the unrequired Hotfixes and service packs from the list and click **Remove**.
- Click **Update** to apply Windows Updates to a Windows Distribution Share.

7.

- Browse to the appropriate Hotfixes or service packs from the list
- Click the Windows Distributions to which you want to apply these Hotfixes or service packs.
- Click **Apply**.
- Click **Done.**

  - Removing a Hotfix or service pack from the list of available Hotfixes does not remove the Hotfix from the Windows Distribution to which it has been applied.
  - Once a service pack or Hotfix is applied/slipstreamed to a Windows Distribution, it cannot be removed.
  - The option to integrate, or slipstream, Security Updates and Service Packs into Windows distribution shares supports Update.exe 5.4.15.0 or any later version.
  - When integrating Updates in your distribution shares, be sure to integrate the Service Pack first.
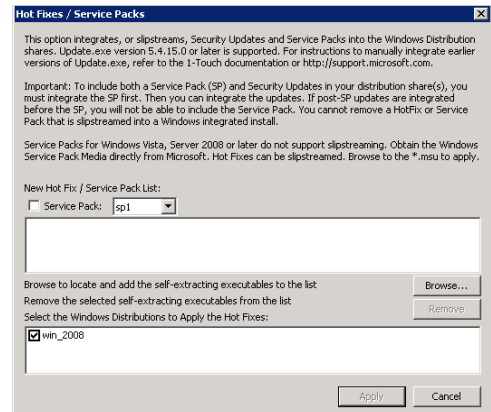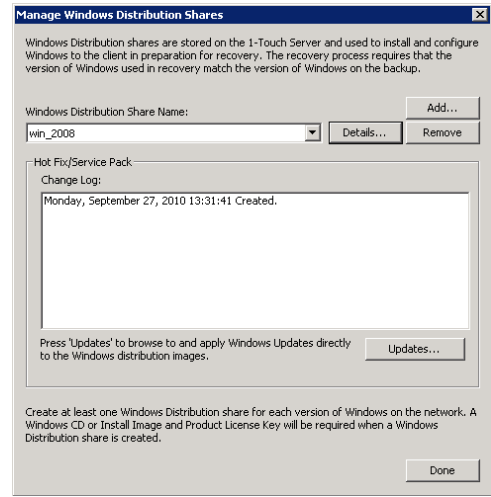
MANAGE WINDOWS DRIVERS

Check if all the required mass storage and network adapter drivers are available on 1-Touch Server. Add the required drivers.

1. Login to 1-Touch Server.

2. Click **Start | Programs | Bull Calypso | Calypso | 1-Touch**
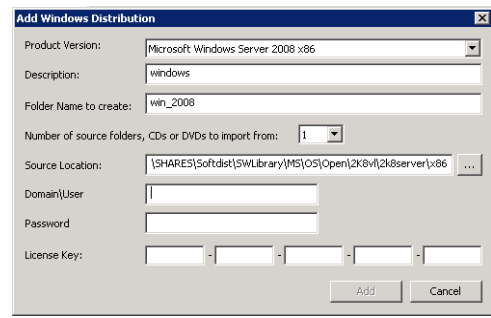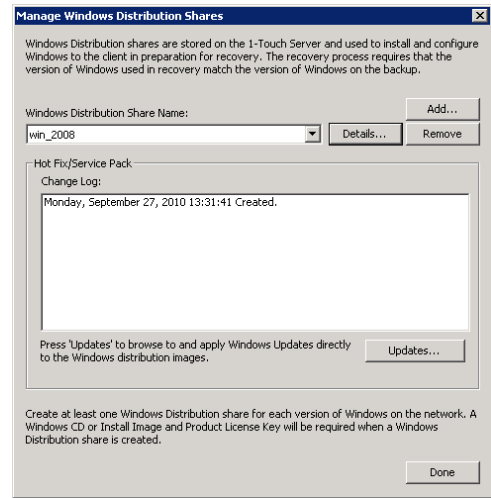
3. Click **Windows Driver Manager**.
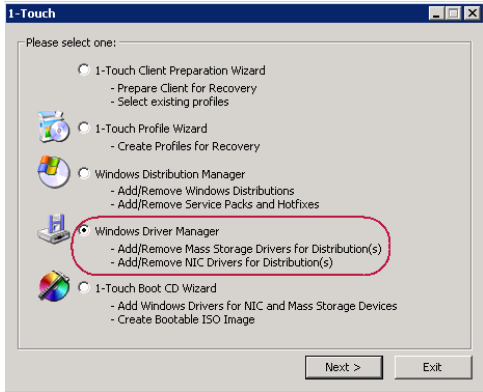
4.
- Select the **Driver Type**.
- Select the **OS Family**.
- Review the list of available drivers for the selected operating system.
- Click **Add** to add any additional drivers.
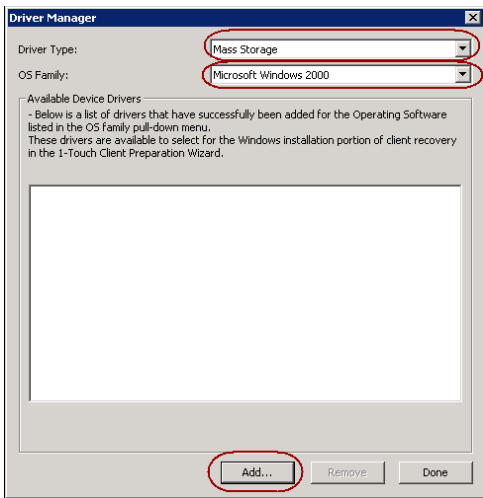
- Select the **Driver Type** from the list.
- Browse to the **Location** where drivers are stored.
- **Select Driver** from the list of available drivers.
- Select a **Processor Type** from the list.
- Select the **OS Family**.
- Click **OK.**

  These drivers will be available for selection in the **1-Touch Client Preparation Wizard.**
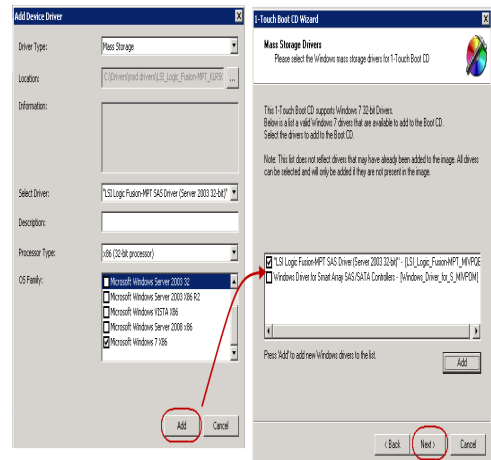
- If third-party mass storage drivers are needed, use standard vendor-supplied Windows drivers.
- You can use the RIS version or the native version of the Mass Storage Driver for 1-Touch Recovery.
- The drivers must be compatible to Windows version on the client that is being recovered.

CREATE AN ANSWER FILE

When you have all drivers and windows distribution shares ready on the 1-Touch server, create an answer file. You can also create an answer file after you boot

the client.

1. Login to 1-Touch Server.

2. Click **Start | Programs | Bull Calypso | Calypso | 1-Touch**.

3.
   - Select **1-Touch Client Preparation Wizard**.
   - Click **Next**.
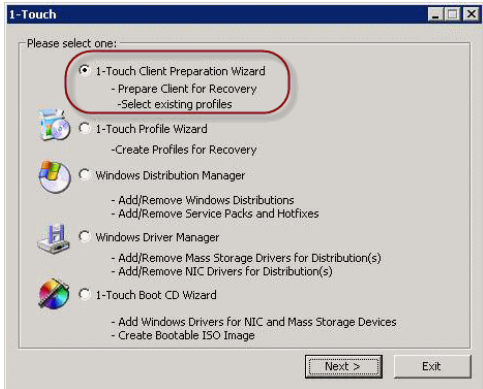
4. Click **Next**.
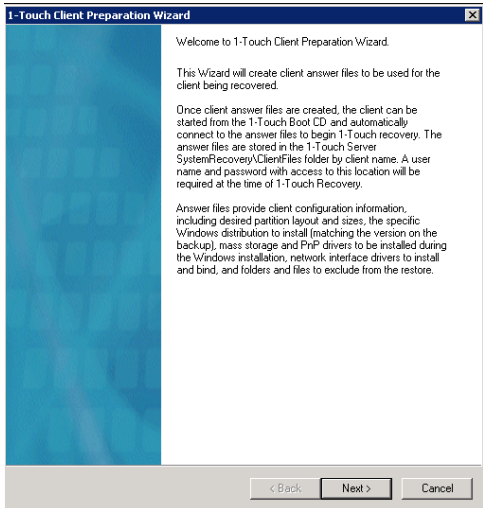
5.
   - Enter **CommCell User Name**.
   - Enter **CommCell Password**.
   - Select the client for which you want to create the answer file.
   - Click **Next**.
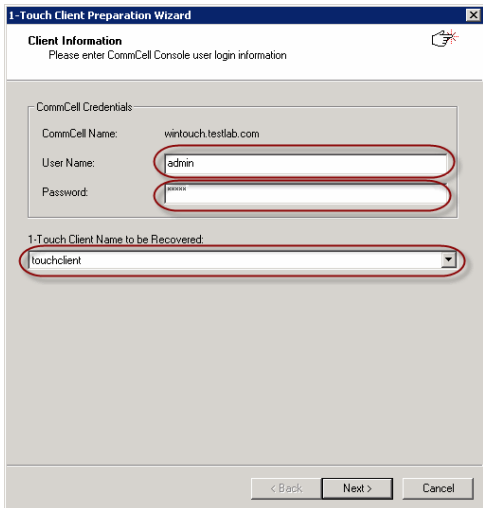
6. Click **Next**.

7. Enter the Windows User name and Password for 1-Touch Server.

Do not use the following characters in the password: { , | , } , ~.

If the password contains any of these characters, create a new user and enter the new User Name and Password.

8. Click **Next**.

9.
- Select Windows Distribution **Share Name** from the list of available shares.
- Click **Next**.
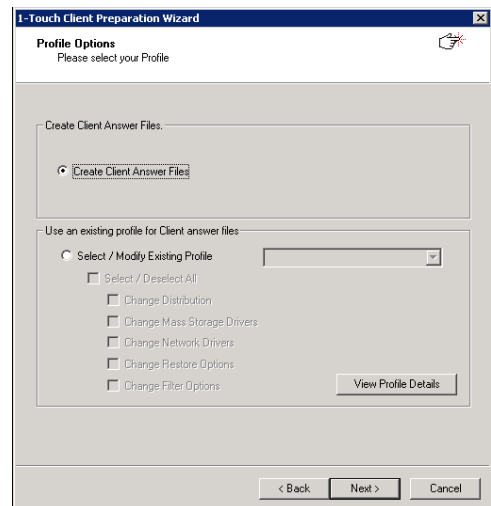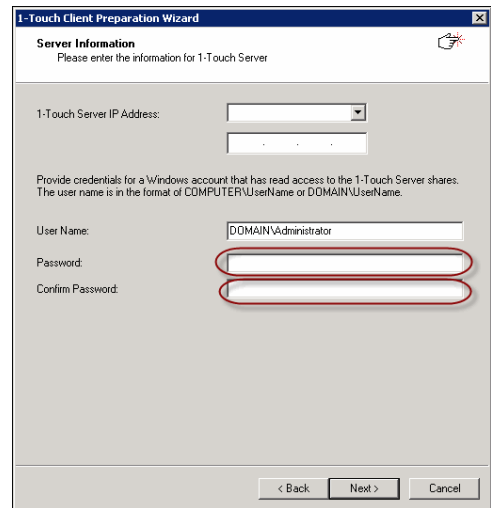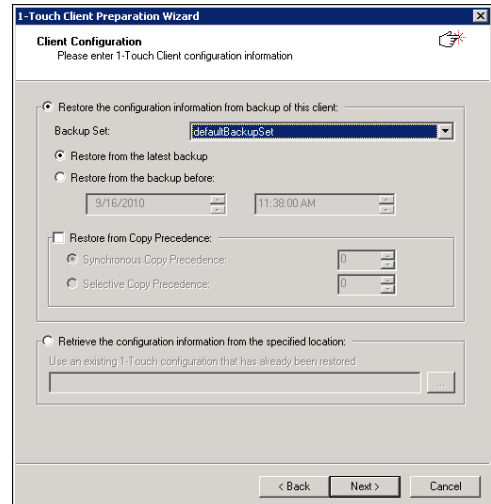
10.
- **Select the primary mass storage driver** from the list.
- Select all the mass storage drivers necessary for installing the operating system.

    If you are performing Cross Hardware Restore, select the mass storage drivers for the computer where you are recovering.

- Click **Next**.

11.
- Select **PnP Drivers for the Client**. The PnP Drivers will be used while installing the operating system.
- Click **Next**.

12. Click **Next**.

Select **Dissimilar Disk Mapping** if the computer where you are performing the restore has different disk configuration from the client that was backed up.

If the client computer has iSCSI disk, select the **Configure and restore iSCSI** disks check box.
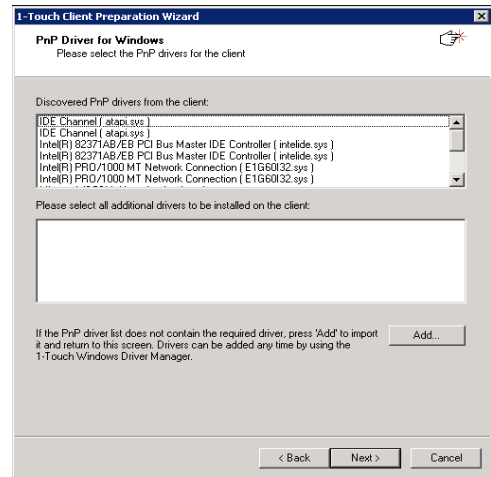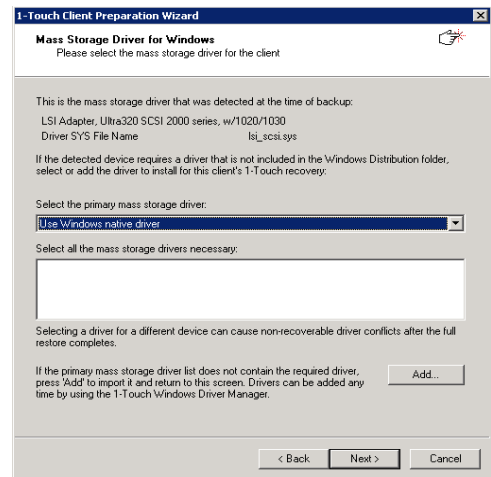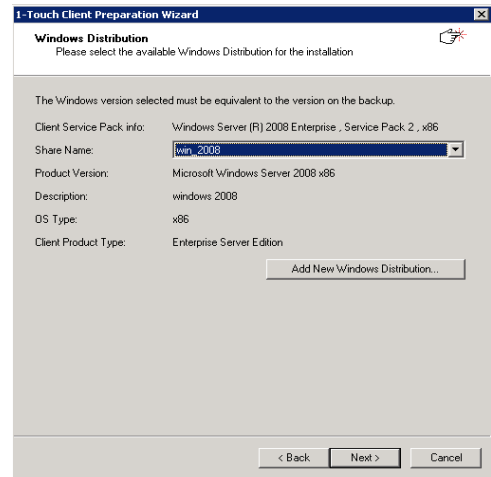
13.
- If you want to exclude any folder or driver from the full system restore, enter the path of the folder or driver and click **Add**.
- Click **Next**.
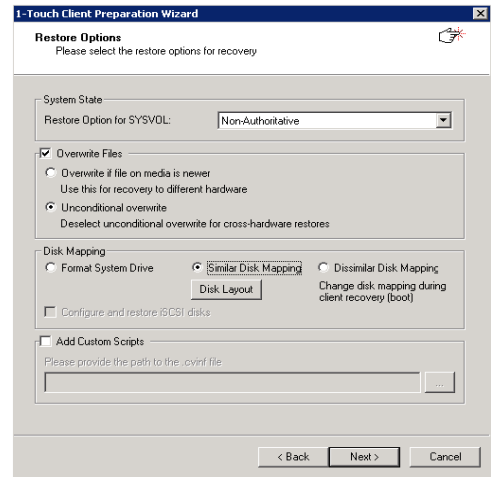
14.
- Select the **Network Adapter to Bind**.
- Click **Next**.
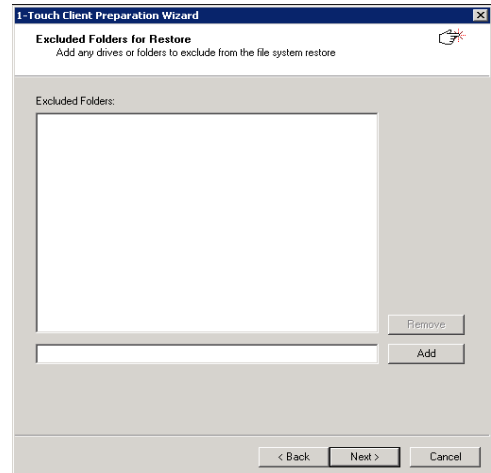
15.
- Click **Next**.
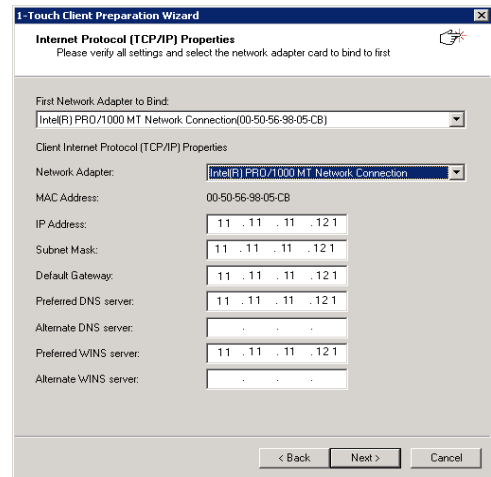
16.
- Review the summary of the client answer file.
- Click **Done** to save the answer file.
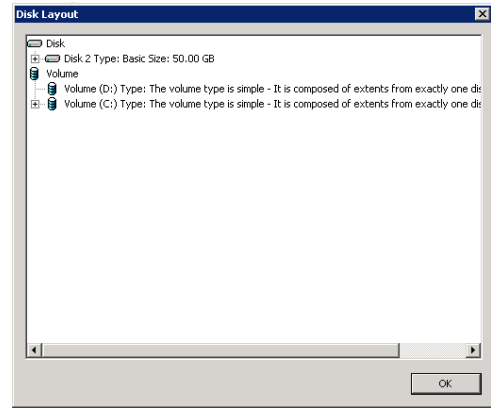
17.
- Enter the name of a Client Profile
- Click **Save** to save the client preparation as a client profile.
- Click **Done** to save the client preparation as a client answer file. It is saved on the 1-Touch server in the `SystemRecovery\Client Files` folder.
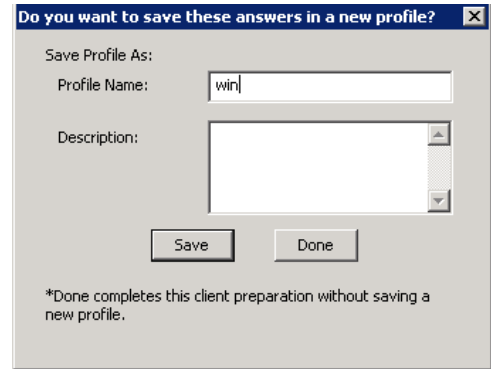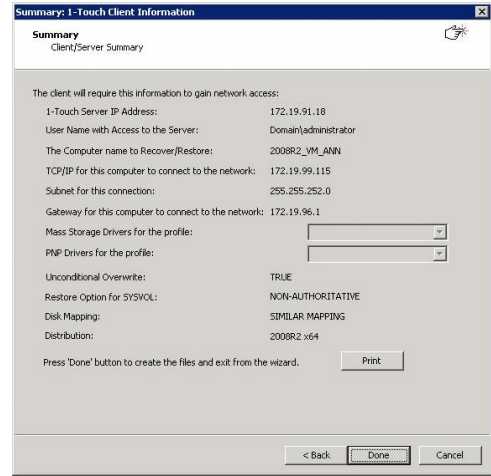
ADDITIONAL OPTIONS

CREATING AN ANSWER FILE FOR ISCSI DISKS RESTORE

If the client computer is using iSCSI disks, follow the steps given below while creating an answer file:

1. Ensure that you have selected the **Configure and restore iSCSI** disks check box while creating the answer file for the client.

3.   If you are restoring Windows 2003 computer, provide the following details:

- Location of the iSCSI Initiator Installation File.
- User name and password for the location where iSCSI Initiator Installation File is stored.

You must perform an Online Restore if you are restoring a client that has iSCSI disks. Foe more information, refer Online Restore.

Recovery - 1-Touch for Windows

| Deployment | Configuration | Recovery | Troubleshooting | FAQ |

◀ Previous   Next ▶

TABLE OF CONTENTS

PREREQUISITES

● Users must have CommCell administrative privileges to perform 1-Touch recovery.

● Disable authentication for Agent installation using the following steps:

  1. Log on to the CommServe.

  2. Right-click the <***CommServe***> and click the **Security** tab.

  3. Disable **Require Authentication for Agent Installation** check box.

  4. Click **OK**.

CREATE A LIVE CD

A Live CD will be required to boot the client. You can create a Live CD image using 1-Touch Wizard on 1-Touch server. Before creating a Live CD image, consider the following prerequisites:

● All the software updates for 1-Touch Server software, Windows File System *i*DataAgent and WinPE are downloaded to remote cache on 1-Touch server and applied to 1-Touch Live CD. For more information refer to Download and Install Updates on 1-Touch Server.

Follow the steps given below to create a Live CD:

1. Login to 1-Touch Server.

2. Click **Start | Programs |Bull Calypso | Calypso | 1-Touch**.

3. Click **1-Touch Boot CD Wizard**.
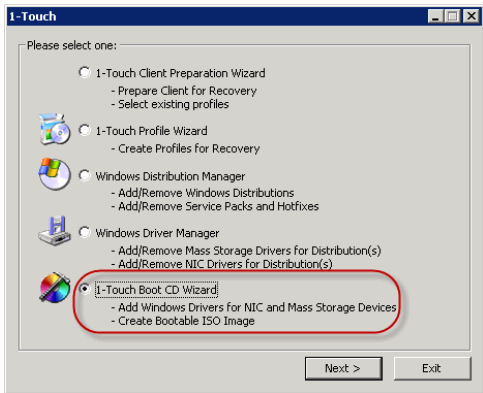
4. Click **Next**.
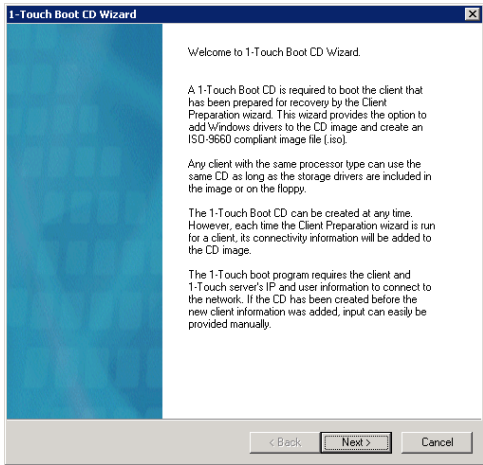
5. Select the processor type from the list. The processor type must match with the processor of the computer where you are restoring the client.
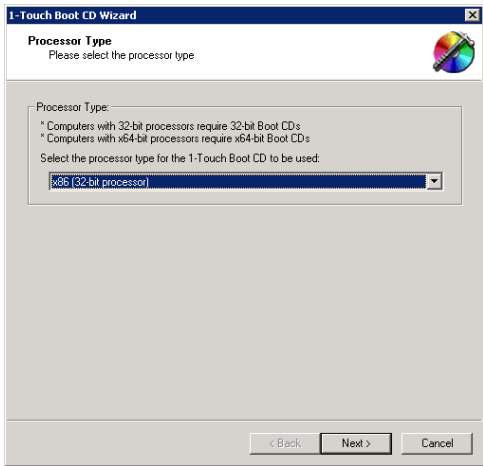
6. By default Mass Storage Drivers for Windows 7 WINPE are automatically added to the boot CD. The mass storage drivers are required by the Boot CD to connect to primary mass storage device. Click **Next** and go to step 8.

If you want to add any additional drivers to the boot CD, click **Add** and continue to next step.

7. Skip this step if you do not want to add any Mass Storage Drivers to the list.

- Select **Mass Storage** from the **Driver Type** list.
- Browse to the **Location** where .oem files are stored and select the required file.
- Select a **Processor Type** from the list.
- In the **OS Family** list, select **Windows 7**.
- Click **Add**.
- The list of **Mass Storage Drivers** displays the newly added driver.
- Select the drivers from the list which you want to add to the boot CD. You can select multiple drivers.
- Click **Next**.
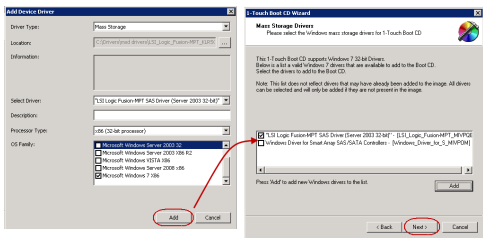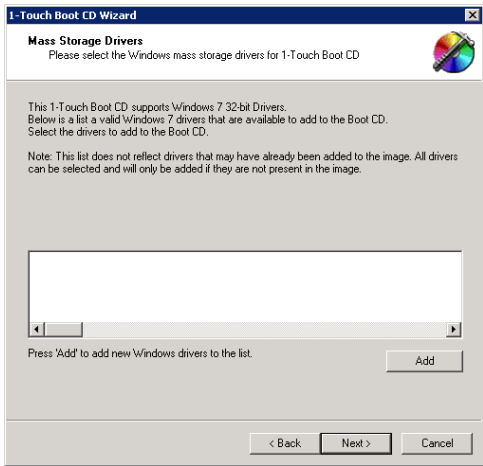
8. By default NIC Drivers for Windows 7 WINPE are automatically added to the boot CD. The NIC drivers are required by the ISO to connect with the network. Click **Next** and go to step 10.

> If you want to add any additional drivers to the list, click **Add** and continue to next step.
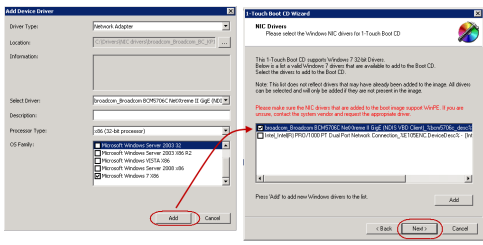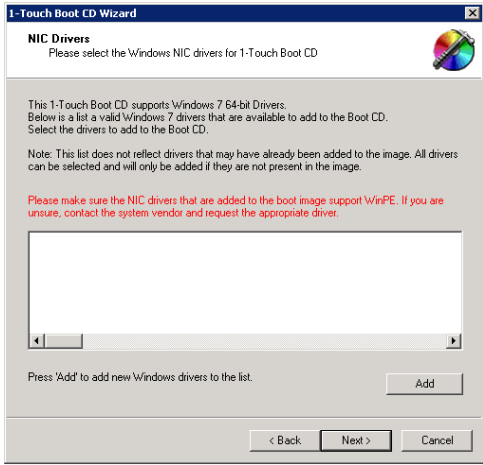
9. Skip this step if you do not want to add any NIC Drivers.

- Select **Network Adapter** from the **Driver Type** list.
- Browse to the **Location** where .inf files are stored and select the required file.
- **Select Driver** from the list of available drivers.
- Select a **Processor Type** from the list.
- In the **OS Family** list, select **Windows 7**.
- Click **Add**.
- The list of **NIC Drivers** displays the newly added driver.
- Select the drivers from the list which you want to add to the boot CD. You can select multiple drivers.
- Click **Next**.

10.
- Enter the location to save the ISO image.
- Click **Done**.
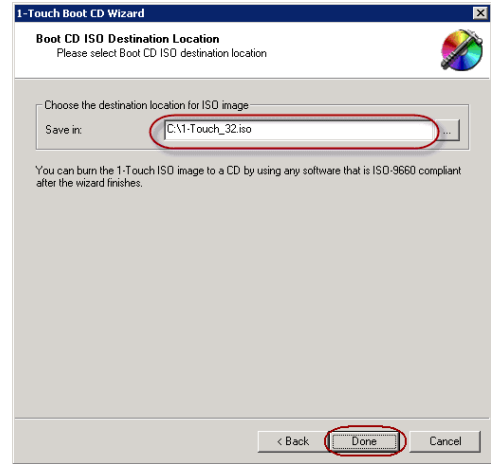
11.   Create a **Live CD** using the ISO.

    1-Touch clients may have different types of operating systems and processors. You must create a Live CD for each type of processor. Ensure that you have all the latest software updates included in the **Live CD**. Learn more....

Back to Top

SIMILAR DISK RESTORE

When you are restoring to a computer which has the same hardware and disk configuration as that of the backed up computer, use one of the following methods to perform the restore:

OFFLINE NON-INTERACTIVE RESTORE

Use this method when you do not want to provide the client information during the restore. When you backup the client, the client information is stored as a client configuration.

This is a offline recovery method to restore the operating system. It does not require connection with 1-Touch Server.

1.   Create a 1-Touch Live CD.

2.
    - From the CommCell Console, navigate to **<Client>**
    - Right-click the **<Client>** and click **All Tasks | 1-Touch Recovery Point**

3.
    - Select the most recent client configuration to create a response file.

        A new client configuration is generated when you make any changes in the client network configuration and then perform a full backup.

    - Click **Export Config**.

4.
- Enter the credentials used to login to CommCell Console.
- Click **OK**.

5. Save the response file as `onetouchresponse.xml`.

By default, the response file is saved in the `My documents` folder on the computer that is running the CommCell Console.

6. Copy the response file to a USB drive or a removable disk or a network location.

7. Connect the USB drive or the removable disk to the client that you want recover.

If you want to use a network location to access the response file during the restore, follow the steps given in Accessing the Response File From an UNC Path During a Non-Interactive Restore.

8. Use the 1-Touch **Live CD** to boot the client.

9.
- Select the language from the list
- Click **OK**.

10. Click **OK** to start the full system restore.

10.
- Click **OK**.
- Remove the **Live CD** and restart the computer.

OFFLINE INTERACTIVE RESTORE

Use this method when you want to specify the client configuration information during the restore.

This is a offline recovery method to restore the operating system. It does not require connection with 1-Touch Server.

1. Create 1-Touch Live CD

   Use the 1-Touch **Live CD** to boot the client.

2.
- Select the language from the list
- Click **OK**.

3. Click **Next**.

4. Click **Yes** if all disk devices are detected.

5.
- Enter **CommServe Host Name**.
- Enter **CommServe IP address**.
- Select the Network Connection from the **Connection** drop-down combo box.
- Click **Get Clients**.
- Select client **Host Name** from the list.
- Click **Next**.

6.
- Review network information for CommServe and restored client.
- Click **Next**.

7.
- Enter **CommCell User Name**.
- Enter **CommCell Password**. Enter the credentials that are used to login to CommCell from the client.
- Click **Next**.

8. Click **Next**.

9. Click **Next**.

    If you want to exclude any folder or driver from the full system restore, enter the path of the folder or driver and click **Add**.

10. Click **Next**.

11.   Click **Next**.
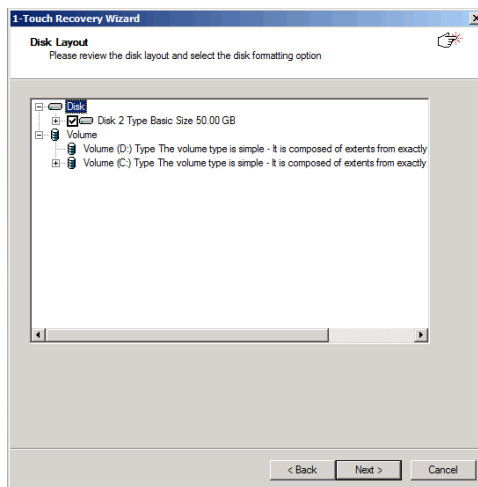
12.   Click **OK**.

The TCP/IP Properties of the client captured during the backup are displayed. If the target computer has different IP, change the TCP/IP Properties or click **Use DHCP** to use DHCP instead of static IP address.

The full system restore starts.
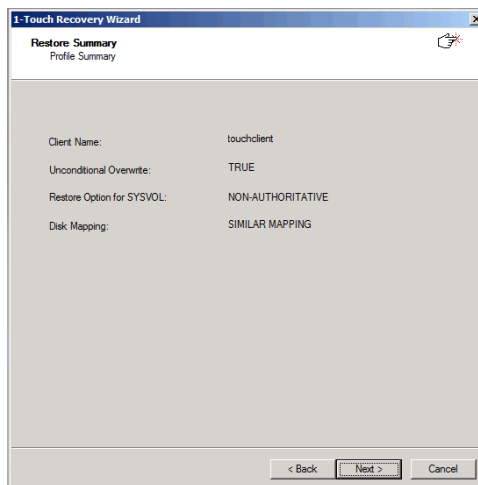
13.
- Click **OK**.
- Click **Finish**.
- Remove the **Live CD** and restart the computer.

After you click **Finish**, the computer may reboot one or more times.

ONLINE RESTORE

Perform the Online Restore to reinstall the operating system on the client. The Windows Distribution Shares and Drivers available on 1-Touch Server are used to reinstall the operating system.

1. Login to 1-Touch Server and create Answer File for the 1-Touch Client. For more information, go to Creating an Answer File.

2. Create 1-Touch Live CD.

   Use 1-Touch **Live CD** to boot the client.

3.
   - Select the language from the list
   - Click **OK**.

4. Click **Next**.

5. Click **Yes** if all disk devices are detected.

6.
   - Select **Online Restore**.
   - Enter the **Client Name**.

     If the client answer file is not created on 1-Touch Server, select **Create Client Answer files for 1-Touch Recovery** and follow the steps described in Creating an Answer File.

   - Click **Next**.

7.
- Enter **IP Address** of the **1-Touch Server** where the client answer file is available.
- Enter the **User name** and **Password** for the 1-Touch Server.
- Click **Next**.

8. Click **Next**.

8. Reboot the computer after the windows installation completes.

During the Windows installation process of a 1-Touch Recovery, the Windows Administrator password is set as 1Touch. Upon completion of the 1-Touch Recovery, the Administrator's original password will be restored from the backup.

After the windows installation completes, the computer may reboot one or more times.
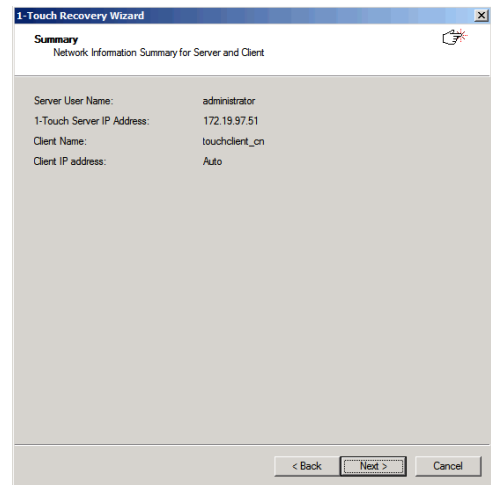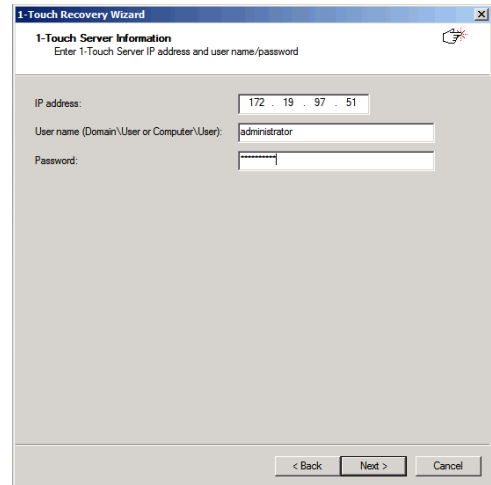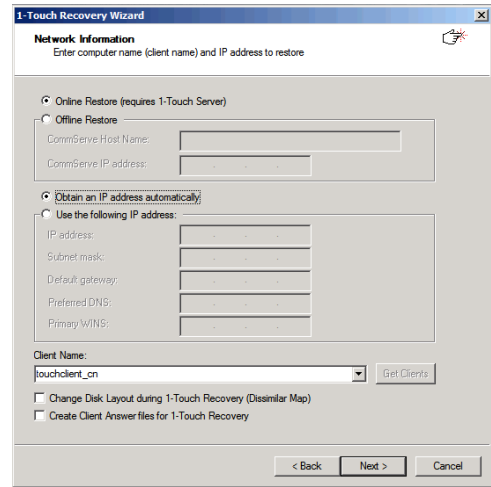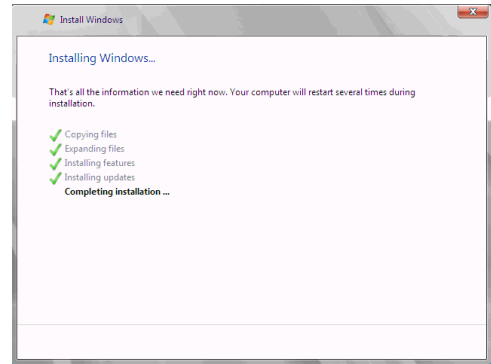
Back to Top

DISSIMILAR DISK RESTORE

Perform a Dissimilar Disk Restore, when the computer where you are restoring, satisfies the following criteria:

● The hardware configuration of the computer is same as backed up computer

● The disk configuration of the computer is different than the backed up computer

Use one of the following methods to perform the restore.

OFFLINE NON INTERACTIVE RESTORE

Use this method when you do not want to provide the client information during the restore. When you backup the client, the client information is stored as a client configuration.
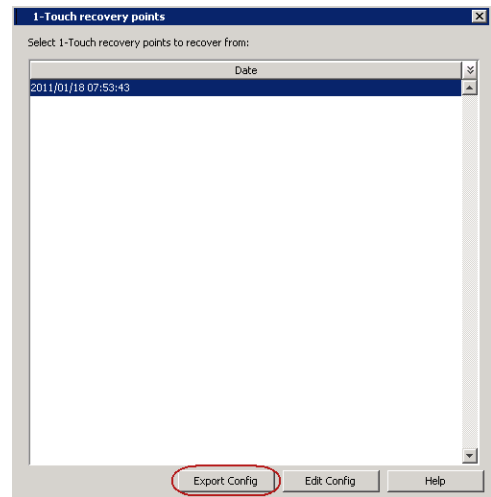
This is a offline recovery method to restore the operating system. It does not require connection with 1-Touch Server.

1. Create a 1-Touch Live CD.

2.
● From the CommCell Console, navigate to **<Client>**
● Right-click the **<Client>** and click **All Tasks | 1-Touch Recovery Point**

3.
● Select the most recent client configuration to create a response file.

A new client configuration is generated when you make any changes in the client network configuration and then perform a full backup.

● Click **Export Config**.

4.
● Enter the credentials used to login to CommCell Console.
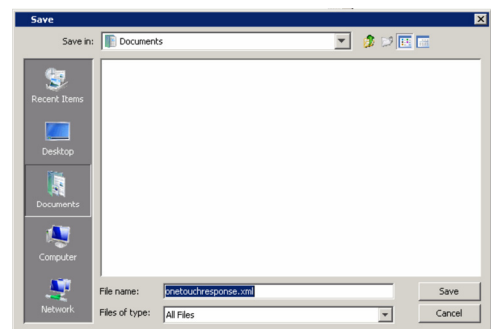
- Click **OK**.

5. Save the response file as `onetouchresponse.xml`.

By default, the response file is saved in the `My documents` folder on the computer that is running the CommCell Console.
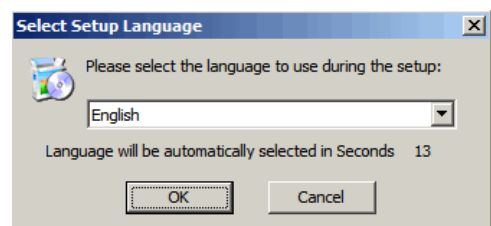
6. Copy the response file to a USB drive or a removable disk or a network location.

7. Connect the USB drive or the removable disk to the client that you want recover.

If you want to use a network location to access the response file during the restore, follow the steps given in Accessing the Response File From an UNC Path During a Non-Interactive Restore.
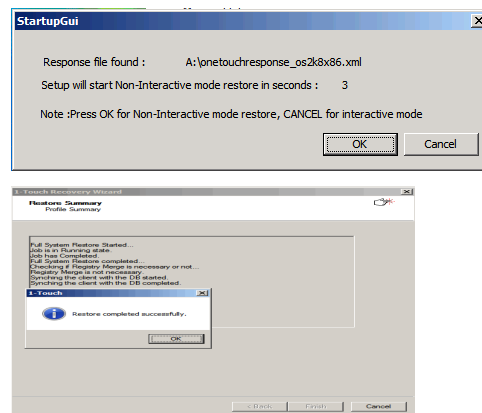
8. Use the 1-Touch **Live CD** to boot the client.

9.
- Select the language from the list
- Click **OK**.

10. Click **OK** to start the full system restore.

11.
- Review the **Source Disk Layout** and **Destination Disk Layout**.
- Right-click a disk from **Destination Disk Layout** and select the disk type that you want to assign to the destination disk.
- Click **OK** to start the disk initialization process.

12. Click **Yes**.
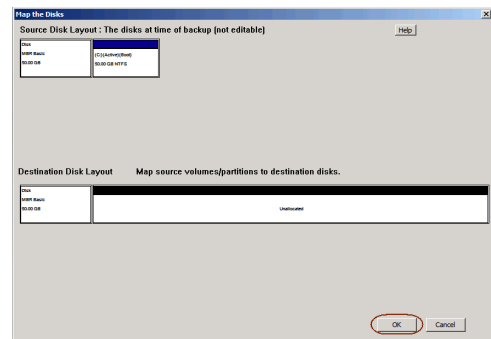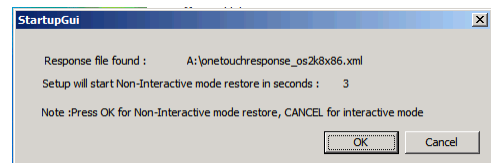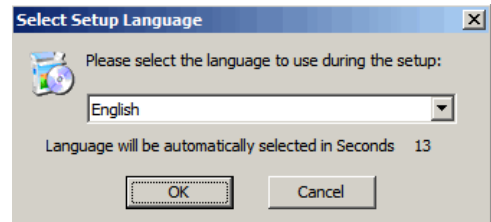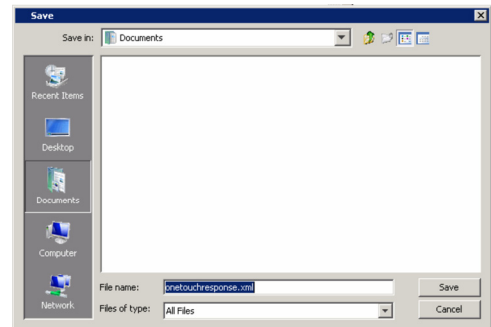
13.
- Repeat the steps 11 and 12 to clean all the required disks from the **Destination Disk Layout**.
- Click **Done** after all disks are initialized.

14.
- Right-click the disk from the **Source Disk Layout** that you want to map with a destination disk.
- Select **Map**.

15.
- Select a destination disk from the the **Available Disk List** to map with the selected source disk .
- Select the Partition **Type**.
- Select the **File system**.
- Click **Perform quick format** if you want to format the selected disk.
- Click **Enable file and folder compression** to enable the file system compression for the selected disk.
- Enter the Volume **Size**.
- Select a **Drive Letter** to assign it to the selected volume.
- Click **OK**.

16.
- Review the **Destination Disk Layout**.
- Click **OK** to start full system restore.

17.
- Click **OK**.
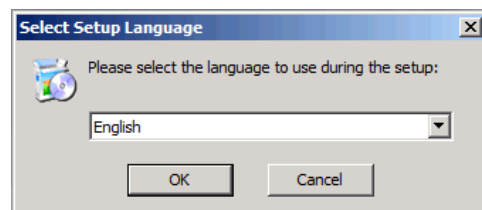- Remove the **Live CD** and restart the computer.
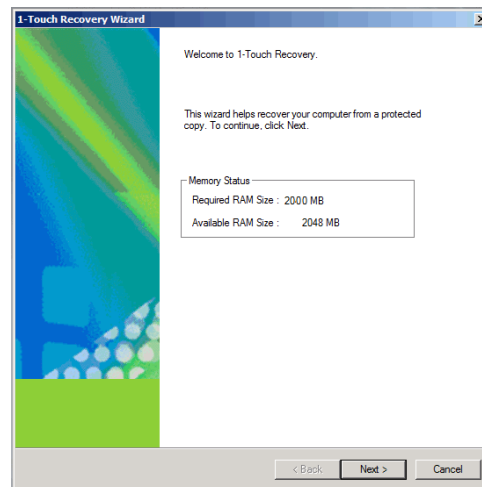
OFFLINE INTERACTIVE RESTORE

Use this method when you want to specify the client configuration information during the restore.

This is a offline recovery method to restore the operating system. It does not require connection with 1-Touch Server.

1.   Create 1-Touch Live CD

      Use the 1-Touch **Live CD** to boot the client.

2.
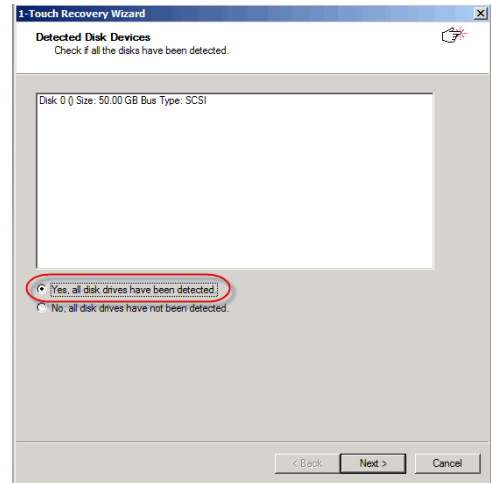- Select the language from the list
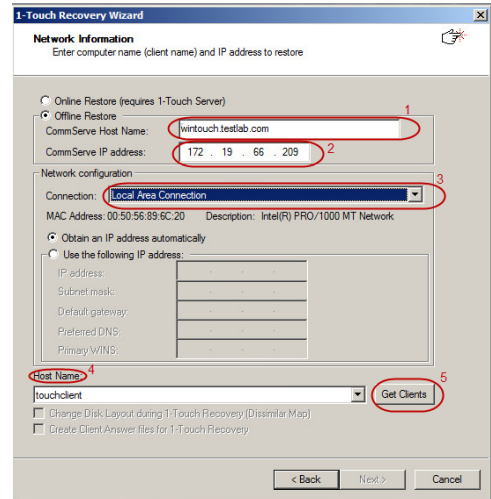- Click **OK**.

3.   Click **Next**.

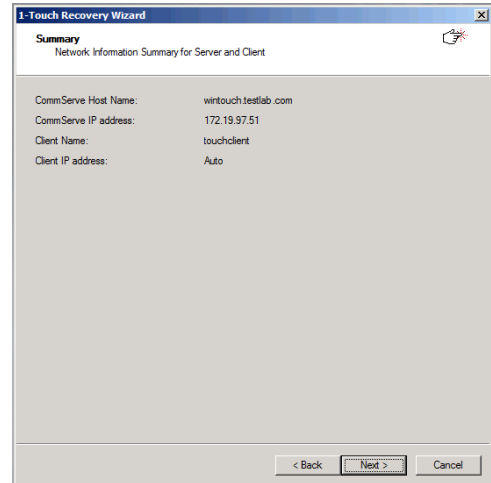**4.**   Click **Yes** if all disk devices are detected.

5.
- Enter **CommServe Host Name**.
- Enter **CommServe IP address**.
- Select the Network Connection from the **Connection** drop-down combo box.

- Click **Get Clients**.
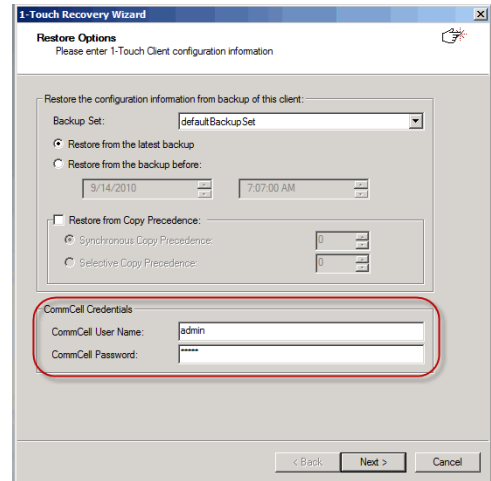- Select client **Host Name** from the list.
- Click **Next**.

6.
- Review network information for CommServe and restored client.
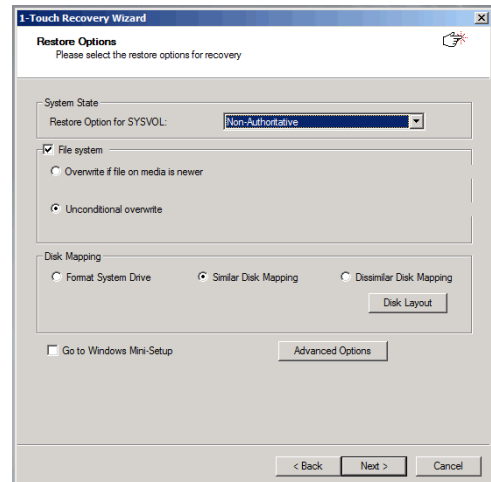- Click **Next**.
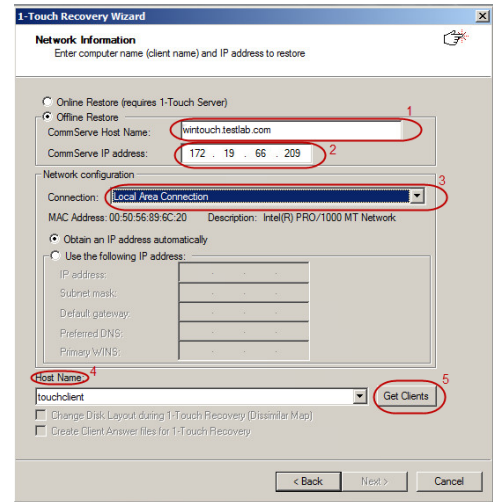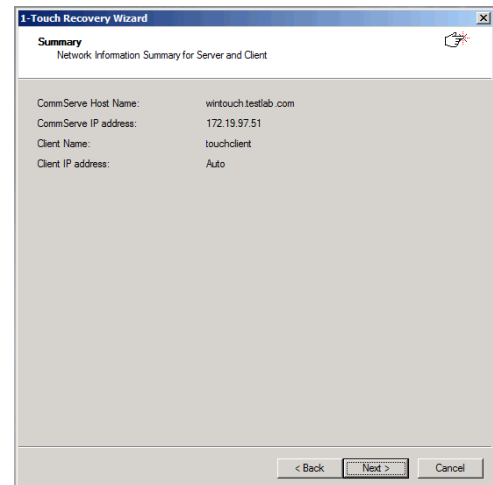
7.
- Enter **CommCell User Name**.
- Enter **CommCell Password**. Enter the credentials that are used to login to CommCell from the client.
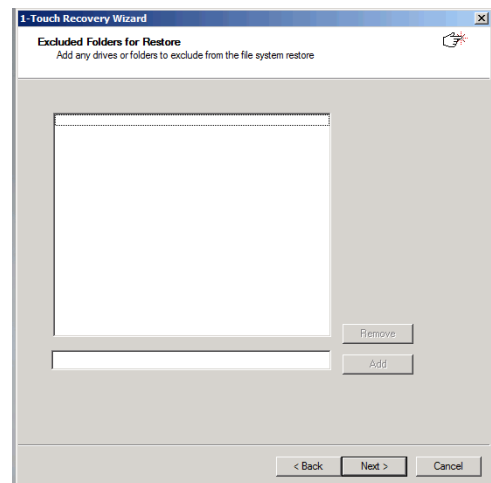- Click **Next**.
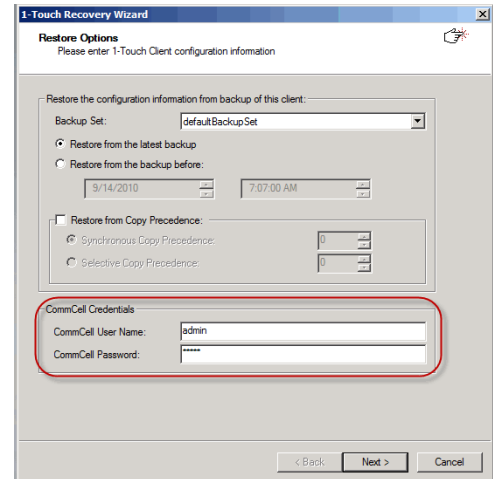
8.
- Ensure that **Dissimilar Disk Mapping** is selected.
- Click **Next**.
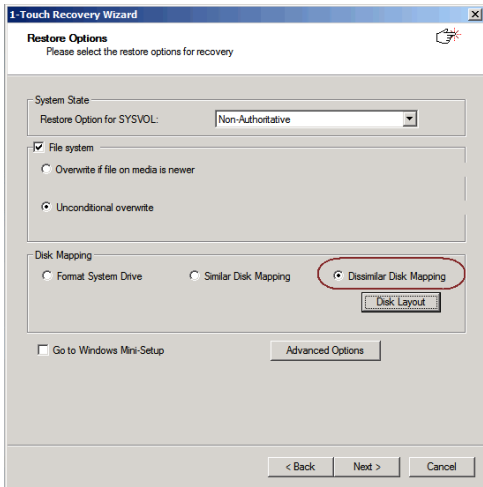
9.   Click **Next**.

        If you want to exclude any folder or driver from the full system restore, enter the path of the folder or driver and click **Add**.
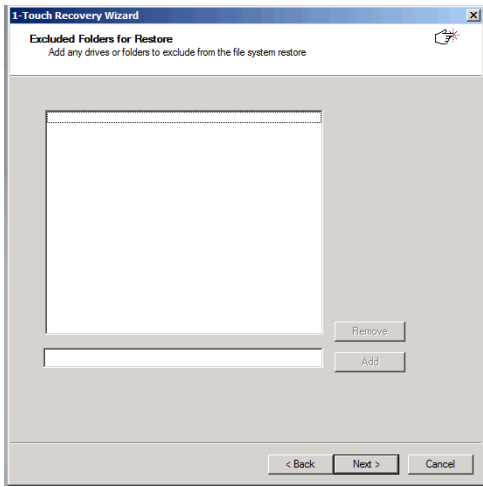

10.
- Review the **Source Disk Layout** and **Destination Disk Layout**.
- Right-click a disk from **Destination Disk Layout** and select the disk type that you want to assign to the destination disk.
- Click **OK** to start the disk initialization process.
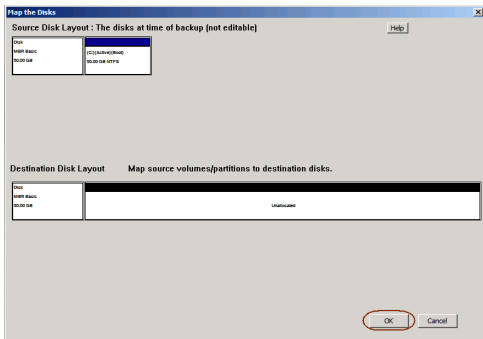
11.   Click **Yes**.
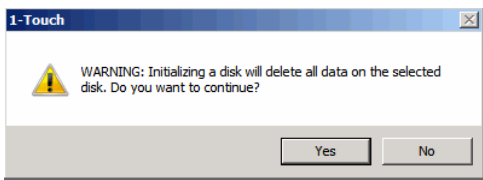
12.
- Repeat the steps 9 and 10 to clean all the required disks from the **Destination Disk Layout**.
- Click **Done** after all disks are initialized.

13.
- Right-click the disk from the **Source Disk Layout** that you want to map with a destination disk.
- Select **Map**.

14.
- Select a destination disk from the the **Available Disk List** to map with the selected source disk .
- Select the Partition **Type**.
- Select the **File system**.
- Click **Perform quick format** if you want to format the selected disk.
- Click **Enable file and folder compression** to enable the file system compression for the selected disk.
- Enter the Volume **Size**.
- Select a **Drive Letter** to assign it to the selected volume.
- Click **OK**.

15.
- Review the **Destination Disk Layout**.
- Click **OK** to start full system restore.
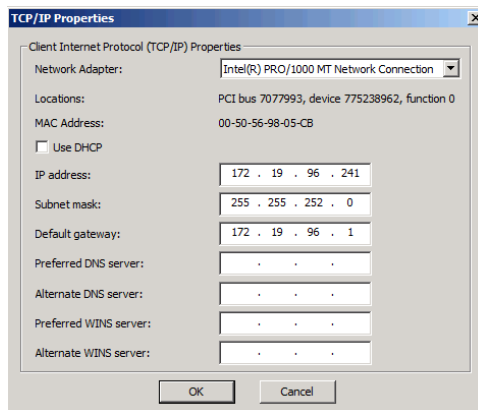

16. Click **OK**.

The TCP/IP Properties of the client captured during the backup are displayed. If the target computer has different IP, change the TCP/IP Properties or click **Use DHCP** to use DHCP instead of static IP address.

The full system restore starts.

17.
- Click **OK**.
- Remove the **Live CD** and restart the computer.
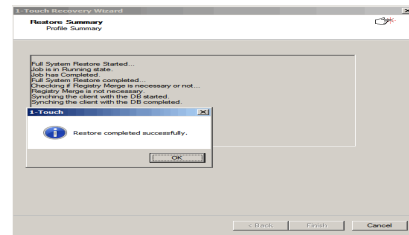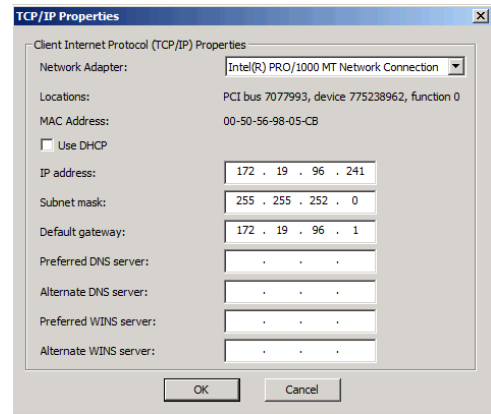
ONLINE RESTORE

Perform the Online Restore to reinstall the operating system on the client. The Windows Distribution Shares and Drivers available on 1-Touch Server are used to reinstall the operating system.
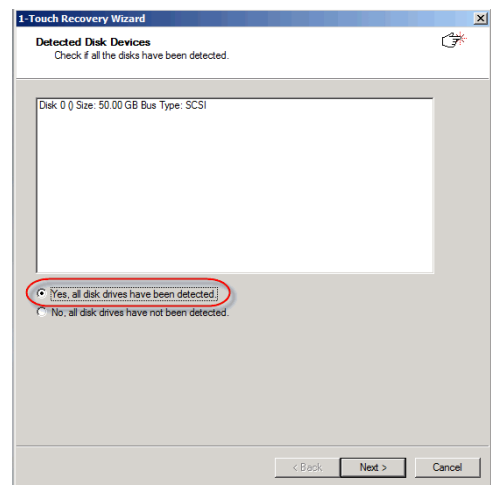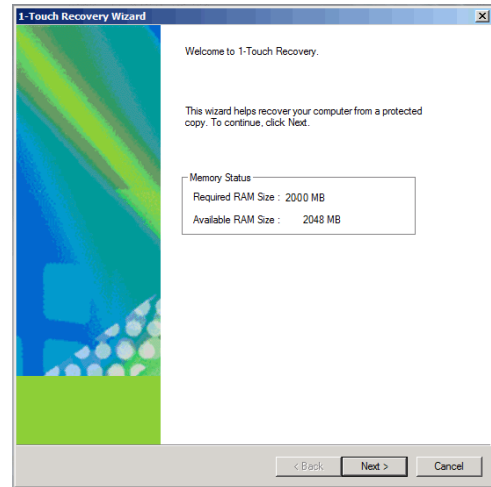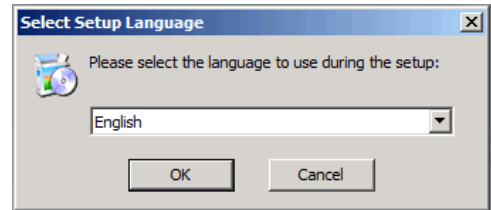
Ensure that you have selected **Dissimilar Disk Mapping** Restore Option while creating the answer file.

1. Login to 1-Touch Server and create Answer File for the 1-Touch Client. For more information, go to Creating an Answer File.

2. Create 1-Touch Live CD.

Use 1-Touch **Live CD** to boot the client.

3.
- Select the language from the list
- Click **OK**.

4. Click **Next**.

**5.** Click **Yes** if all disk devices are detected.

6.
- Select **Online Restore**.
- Enter the **Client Name**.

  If the client answer file is not created on 1-Touch Server, select **Create Client Answer files for 1-Touch Recovery** and follow the steps described in Creating an Answer File.

- Click **Next**.

7.
- Enter **IP Address** of the **1-Touch Server** where the client answer file is available.
- Enter the **User name** and **Password** for the 1-Touch Server.
- Click **Next**.

8. Click **Next**.

9.
- Review the **Source Disk Layout** and **Destination Disk Layout**.
- Right-click a disk from **Destination Disk Layout** and select the disk type that you want to assign to the destination disk.
- Click **OK** to start the disk initialization process.
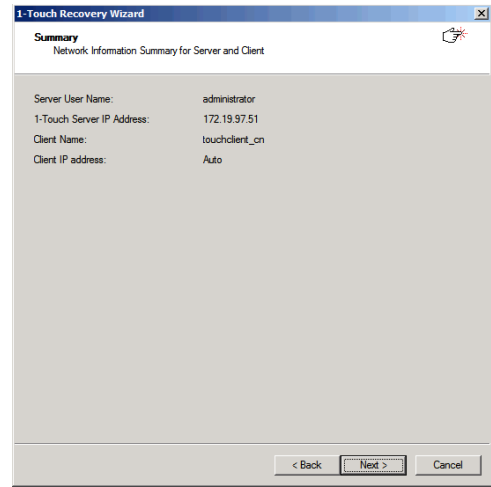
10. Click **Yes**.
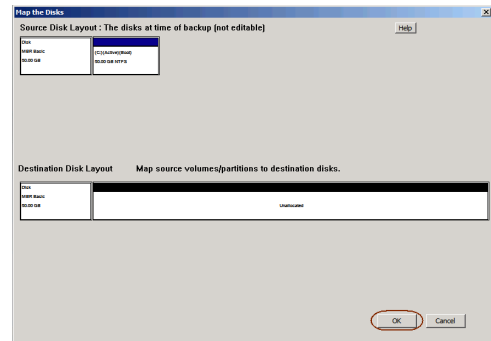
11.
- Repeat steps 9 and 10 to clean all the required disks from the **Destination Disk Layout**.
- Click **Done** to start the disk cleaning.

12.
- Right-click the disk from the **Source Disk Layout** that you want to map with a destination disk.
- Select **Map**.

13.
- Select a destination disk from the the **Available Disk List** to map with the

selected source disk .

- Select the Partition **Type**.
- Select the **File system**.
- Click **Perform quick format** if you want to format the selected disk.
- Click **Enable file and folder compression** to enable the file system compression for the selected disk.
- Enter the Volume **Size**.
- Select a **Drive Letter** to assign it to the selected volume.
- Click **OK**.

14.
- Review the **Destination Disk Layout**.
- Click **OK** to start recovery of the destination disk.

15. Reboot the computer after the windows installation completes.

After the windows installation completes, the computer may reboot one or more times.

During the Windows installation process of a 1-Touch Recovery, the Windows Administrator password is set as 1Touch. Upon completion of the 1-Touch Recovery, the Administrator's original password will be restored from the backup.
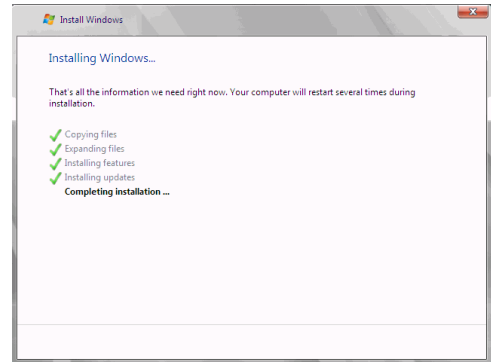
Back to Top

CROSS HARDWARE SIMILAR DISK RESTORE

When a target system has different hardware than the backed up system, perform the Cross Hardware restore. If the backed up system is still running the Calypso services, stop the services before performing the cross hardware restore.
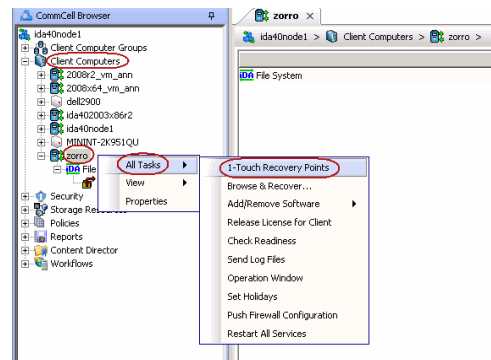
Use one of the following methods to perform the restore.

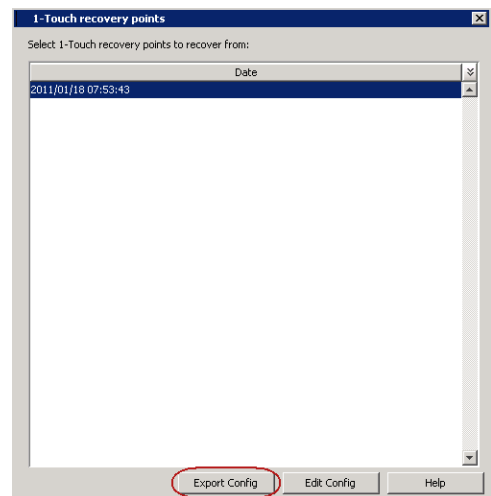### OFFLINE NON INTERACTIVE RESTORE

Use this method when you do not want to provide the client information during the restore. When you backup the client, the client information is stored as a client configuration.

This is a offline recovery method to restore the operating system. It does not require connection with 1-Touch Server.

PREREQUISITES

Copy all the required Mass Storage Drivers and NIC Drivers to a network location. For example: If the target system requires `Adaptec Ultra160` mass storage driver, then copy the `driver.inf` for `Adaptec Ultra160` to a network location.

1. Create a 1-Touch Live CD.

2.
- From the CommCell Console, navigate to **<Client>**

- Right-click the **<Client>** and click **All Tasks | 1-Touch Recovery Point**

3.
- Select the most recent client configuration to create a response file.

  A new client configuration is generated when you make any changes in the client network configuration and then perform a full backup.

- Click **Export Config**.

4.
- Enter the credentials used to login to CommCell Console.
- Click **OK**.

5. Save the response file as `onetouchresponse.xml`.

By default, the response file is saved in the `My documents` folder on the computer that is running the CommCell Console.

6. Copy the response file to a USB drive or a removable disk or a network location.

7. Connect the USB drive or the removable disk to the client that you want recover.

If you want to use a network location to access the response file during the restore, follow the steps given in Accessing the Response File From an UNC Path During a Non-Interactive Restore.

8. Use the 1-Touch **Live CD** to boot the client.

9.
- Select the language from the list
- Click **OK**.

10. Click **OK** to start the full system restore.

11.
- Enter a UNC path to the `.inf` file for the mass storage drivers.

  The third party Mass Storage drivers are required to locate the boot disk when restarting the computer. You must provide the path to `.inf` file for the mass storage drivers.

- You can provide the path to `.inf` file for the NIC drivers now or you can provide it after the system restarts.
- It is recommended that you install the latest hardware drivers after the restore completes.

12. Enter the password to access the network location where drivers are stored.

13.
- Select file(s) required to install the drivers.
- Click **Open**.

14. Click **OK**.

15.
- Enter the valid license key for the restored Windows Operating System. Refer to the check list in the Configuration section.
- Click **OK**.

16.
- Click **OK**.
- Remove the **Live CD** and restart the computer.

OFFLINE INTERACTIVE RESTORE

Use this method when you want to specify the client configuration information during the restore.

This is a offline recovery method to restore the operating system. It does not require connection with 1-Touch Server.

PREREQUISITES

Copy all the required Mass Storage Drivers and NIC Drivers to a network location. For example: If the target system requires `Adaptec Ultra160` mass storage driver, then copy the `driver.inf` for `Adaptec Ultra160` to a network location.

1. Create 1-Touch Live CD

Use the 1-Touch **Live CD** to boot the client.

2.
- Select the language from the list
- Click **OK**.

3. Click **Next**.

4. Click **Yes** if all disk devices are detected.

5.
- Enter **CommServe Host Name**.
- Enter **CommServe IP address**.
- Select the Network Connection from the **Connection** drop-down combo box.
- Click **Get Clients**.
- Select client **Host Name** from the list.
- Click **Next**.

6.
- Review network information for CommServe and restored client.
- Click **Next**.

7.
- Enter **CommCell User Name**.
- Enter **CommCell Password**. Enter the credentials that are used to login to CommCell from the client.
- Click **Next**.

8.
- Ensure that the **Go to Windows Mini-Setup** is selected. This option is selected by default when the restored computer has different mouse, keyboard, disk configuration, network interface card, or processor than that of the backed up computer.

  The mini-setup wizard runs after the restore. This wizard configures network settings and installs the required drivers. You need to provide the credentials for the domain in which you want to add the restored computer.

- Click **Advanced Options**.
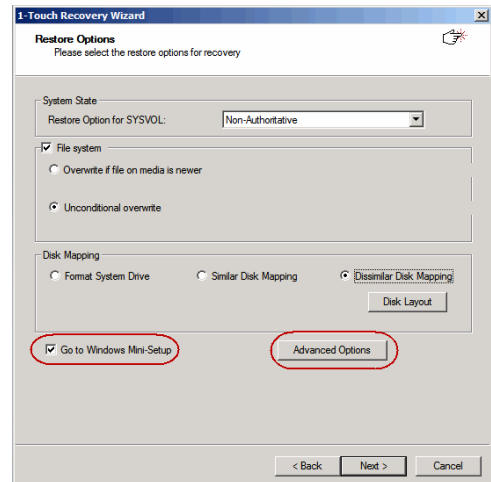
9.
- Enter the **Username** and **Password** for the domain in which you want to add the restored computer.

- Ensure that the **Reboot After Restore is completed** is selected.

- Click **OK**.

    Select the **Increase logging level** option if you want to increase the logging level of windows and **Calypso** logs. The increased logging level gives you more information for troubleshooting.

    After the restore, you may want to review the system state for troubleshooting. Do not select the **Reboot After Restore is completed** option if you want to review the system state.

10.   Click **Next**.
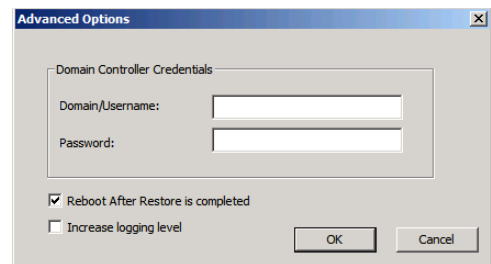
11. Click **OK**.

     The TCP/IP Properties of the client captured during the backup are displayed. If the target computer has different IP, change the TCP/IP Properties or click **Use DHCP** to use DHCP instead of static IP address.

     The full system restore starts.

12. ● Enter a UNC path to the `.inf` file for the mass storage drivers.

     The third party Mass Storage drivers are required to locate the boot disk when restarting the computer. You must provide the path to `.inf` file for the mass storage drivers.

     ● You can provide the path to `.inf` file for the NIC drivers now or you can provide it after the system restarts.

     ● It is recommended that you install the latest hardware drivers after the restore completes.

13. ● Enter the valid license key for the restored Windows Operating System. Refer to the check list in the Configuration section.

     ● Click **OK**.

14. Click **OK**.

     Windows Mini-Setup Wizard configures the network settings and installs required drivers. This process may take few minutes. The computer may reboot one or more times.
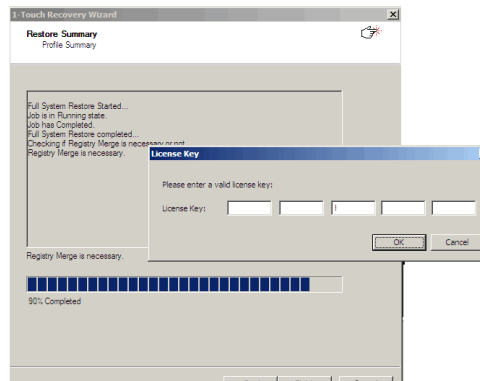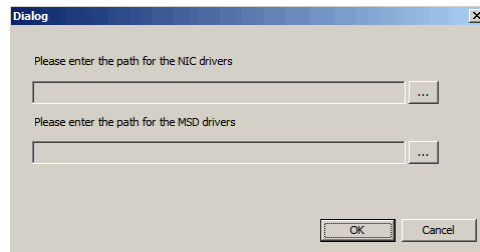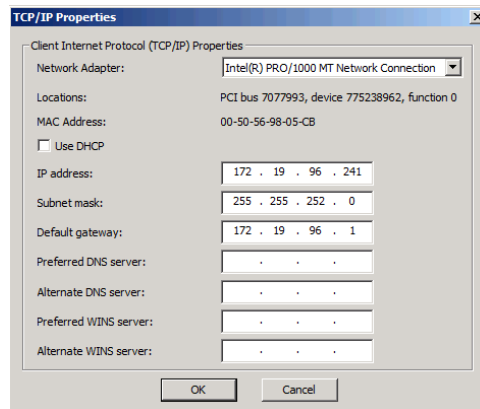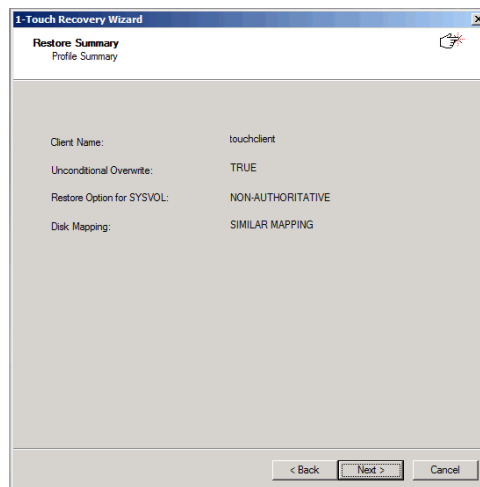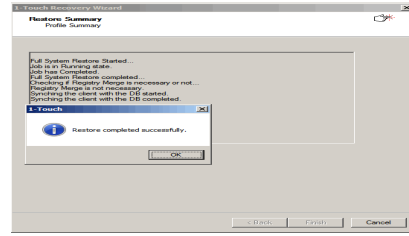
ONLINE RESTORE

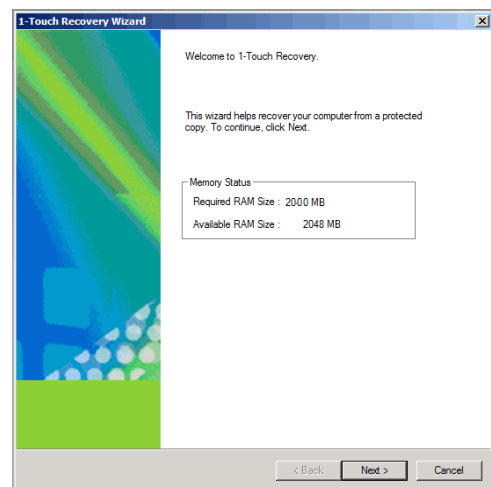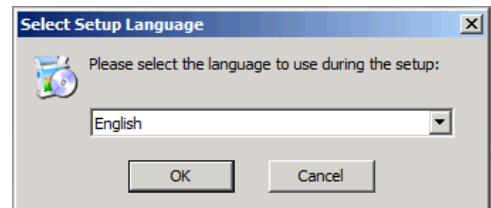Perform the Online Restore to reinstall the operating system on the client. The Windows Distribution Shares and Drivers available on 1-Touch Server are used to reinstall the operating system.

PREREQUISITES

Make sure that the required mass storage and NIC drivers are included in the answer file.

1. Login to 1-Touch Server and create Answer File for the 1-Touch Client. For more information, go to Creating an Answer File.

2. Create 1-Touch Live CD.

   Use 1-Touch **Live CD** to boot the client.

3.
   - Select the language from the list
   - Click **OK**.

4. Click **Next**.

5. Click **Yes** if all disk devices are detected.

6.

- Select **Online Restore**.
- Enter the **Client Name**.

  If the client answer file is not created on 1-Touch Server, select **Create Client Answer files for 1-Touch Recovery** and follow the steps described in Creating an Answer File.

- Click **Next**.

7.

- Enter **IP Address** of the **1-Touch Server** where the client answer file is available.
- Enter the **User name** and **Password** for the 1-Touch Server.
- Click **Next**.

8. Click **Next**.

7. Check the TCP/IP and Display Adapter configurations. Use the Client Checklist to check the configuration.

    If they are incorrect, perform the following steps:

    ● Re-install the appropriate Network Interface Card drivers.
    ● Uninstall the Network Adapters and Display Adapters using the Hardware Uninstall Wizard or Windows Device Manager.
    ● Restart the computer.
    ● Reconfigure the TCP/IP and Display Adapter settings.
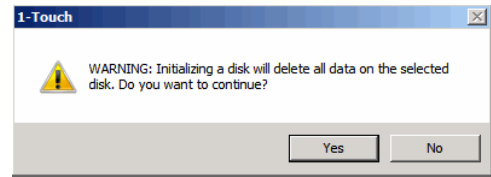

9. ● Reboot the computer after the windows installation completes.

    During the Windows installation process of a 1-Touch Recovery, the Windows Administrator password is set as 1Touch. Upon completion of the 1-Touch Recovery, the Administrator's original password will be restored from the backup.

    After the windows installation completes, the computer may reboot one or more times.
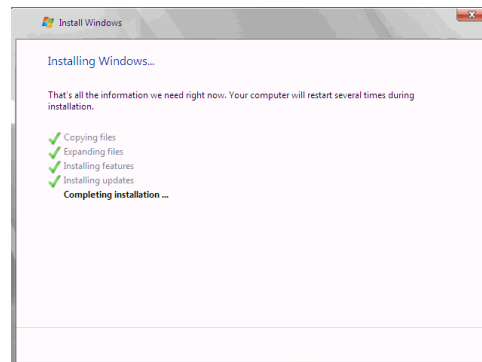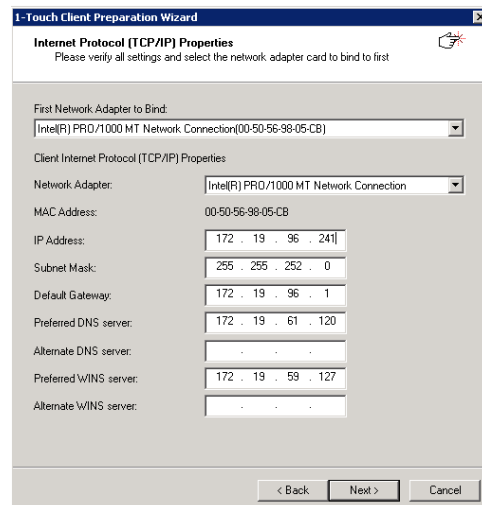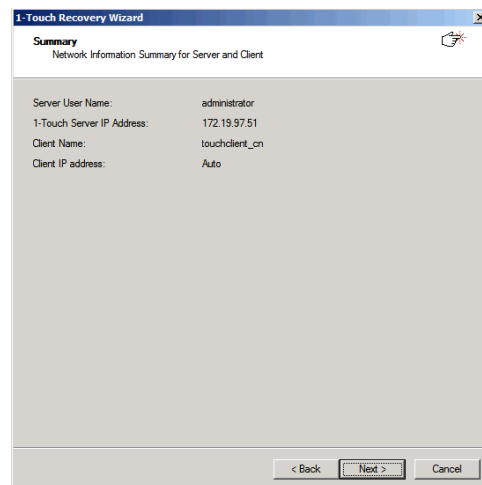
Back to Top

CROSS HARDWARE DISSIMILAR DISK RESTORE

When a target system has different hardware and the different disk configuration than the backed up system, perform the Cross Hardware Dissimilar Disk restore. If the backed up system is still running the Calypso services, stop the services before performing the cross hardware restore.

Use one of the following methods to perform the restore.

OFFLINE NON INTERACTIVE RESTORE

Use this method when you do not want to provide the client information during the restore. When you backup the client, the client information is stored as a client configuration.

This is a offline recovery method to restore the operating system. It does not require connection with 1-Touch Server.

PREREQUISITE

Copy all the required Mass Storage Drivers and NIC Drivers to a network location. For example: If the target system requires `Adaptec Ultra160` mass storage driver, then copy the `driver.inf` for `Adaptec Ultra160` to a network location.

1. Create a 1-Touch Live CD.

2.
- From the CommCell Console, navigate to **<Client>**
- Right-click the **<Client>** and click **All Tasks | 1-Touch Recovery Point**

3.
- Select the most recent client configuration to create a response file.

  A new client configuration is generated when you make any changes in the client network configuration and then perform a full backup.

- Click **Export Config**.

4.
- Enter the credentials used to login to CommCell Console.
- Click **OK**.

5. Save the response file as `onetouchresponse.xml`.

By default, the response file is saved in the `My documents` folder on the computer that is running the CommCell Console.

6. Copy the response file to a USB drive or a removable disk or a network location.

7. Connect the USB drive or the removable disk to the client that you want recover.

    If you want to use a network location to access the response file during the restore, follow the steps given in Accessing the Response File From an UNC Path During a Non-Interactive Restore.

8. Use the 1-Touch **Live CD** to boot the client.

9. - Select the language from the list
    - Click **OK**.

10. Click **OK** to start the full system restore.

10. - Review the **Source Disk Layout** and **Destination Disk Layout**.
    - Right-click a disk from **Destination Disk Layout** and select the disk type that you want to assign to the destination disk.

11. Click **Yes**.

12. - Repeat steps 10 and 11 to clean all the required disks from the **Destination Disk Layout**.
    - Click **Done** after all disks are initialized.

13. - Right-click the disk from the **Source Disk Layout** that you want to map with a destination disk.
    - Select **Map**.

14.
- Select a destination disk from the the **Available Disk List** to map with the selected source disk .
- Select the Partition **Type**.
- Select the **File system**.
- Click **Perform quick format** if you want to format the selected disk.
- Click **Enable file and folder compression** to enable the file system compression for the selected disk.
- Enter the Volume **Size**.
- Select a **Drive Letter** to assign it to the selected volume.
- Click **OK**.

15.
- Review the **Destination Disk Layout**.
- Click **OK** to start recovery of the destination disk.

16.
- Enter a UNC path to the `.inf` file for the mass storage drivers.

  The third party Mass Storage drivers are required to locate the boot disk when restarting the computer. You must provide the path to `.inf` file for the mass storage drivers.
- You can provide the path to `.inf` file for the NIC drivers now or you can provide it after the system restarts.
- It is recommended that you install the latest hardware drivers after the restore completes.
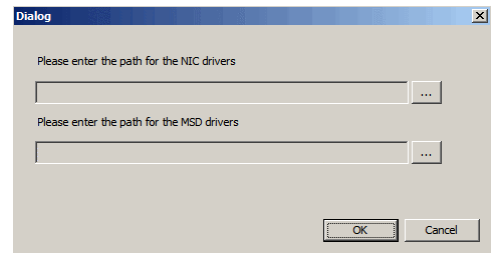
17. Enter the password to access the network location where drivers are stored.
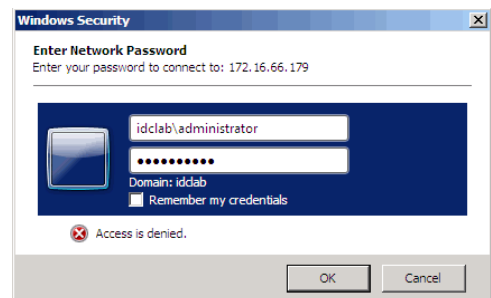
18.
- Select file(s) to install the drivers.

- Click **Open**.

19.   Click **OK**.

20.
- Enter the valid license key for the restored Windows Operating System. Refer to the check list in the Configuration section.
- Click **OK**.

21.
- Click **OK**.
- Remove the **Live CD** and restart the computer.

OFFLINE INTERACTIVE RESTORE

Use this method when you want to specify the client configuration information during the restore.

This is a offline recovery method to restore the operating system. It does not require connection with 1-Touch Server.

PREREQUISITE

Copy all the required Mass Storage Drivers and NIC Drivers to a network location. For example: If the target system requires `Adaptec Ultra160` mass storage driver, then copy the `driver.inf` for `Adaptec Ultra160` to a network location.

1.   Create 1-Touch Live CD

Use the 1-Touch **Live CD** to boot the client.

2.
- Select the language from the list
- Click **OK**.

3. Click **Next**.

4. Click **Yes** if all disk devices are detected.

5.
- Enter **CommServe Host Name**.
- Enter **CommServe IP address**.
- Select the Network Connection from the **Connection** drop-down combo box.
- Click **Get Clients**.
- Select client **Host Name** from the list.
- Click **Next**.

6.
- Review network information for CommServe and restored client.

● Click **Next**.

7.
● Enter **CommCell User Name**.

● Enter **CommCell Password**. Enter the credentials that are used to login to CommCell from the client.

● Click **Next**.

8.
● Ensure that the **Go to Windows Mini-Setup** check box is selected. This option is selected by default when the restored computer has different mouse, keyboard, disk configuration, network interface card, or processor than that of the backed up computer.

The mini-setup wizard runs after the Offline Restore. This wizard configures network settings and installs the required drivers. You need to provide the credentials for the domain in which you want to add the restored computer.

● Ensure that the **Dissimilar Disk** Mapping is seleced.

● Click **Advanced Options**.

9.
● Enter the **Username** and **Password** for the domain in which you want to add the restored computer.

● Ensure that the **Reboot After Restore is completed** is selected.

● Click **OK**.

Select the **Increase logging level** option if you want to increase the logging ilevel of windows and **Calypso** logs. The increased logging level gives you more information for troubleshooting.

After the restore, you may want to review the system state for troubleshooting. Do not select the **Reboot After Restore is completed** option if you want to review the system state.

10. Click **Next**.

If you want to exclude any folder or driver from the full system restore, enter the path of the folder or driver and click **Add**.

11.
- Review the **Source Disk Layout** and **Destination Disk Layout**.
- Right-click a disk from **Destination Disk Layout** to initialize the disk and select the disk type that you want to assign to the destination disk.

12. Click **Yes**.

13.
- Repeat steps 11 and 12 to clean all the required disks from the **Destination Disk Layout**.
- Click **Done** after all disks are initialized.

14.
- Right-click the disk from the **Source Disk Layout** that you want to map with a destination disk.
- Select **Map**.

15.

- Select a destination disk from the the **Available Disk List** to map with the selected source disk .
- Select the Partition **Type**.
- Select the **File system**.
- Click **Perform quick format** if you want to format the selected disk.
- Click **Enable file and folder compression** to enable the file system compression for the selected disk.
- Enter the Volume **Size**.
- Select a **Drive Letter** to assign it to the selected volume.
- Click **OK**.

16.

- Review the **Destination Disk Layout**.
- Click **OK** to start recovery of the destination disk.

17. Click **OK**.

The TCP/IP Properties of the client captured during the backup are displayed. If the target computer has different IP, change the TCP/IP Properties or click **Use DHCP** to use DHCP instead of static IP address.
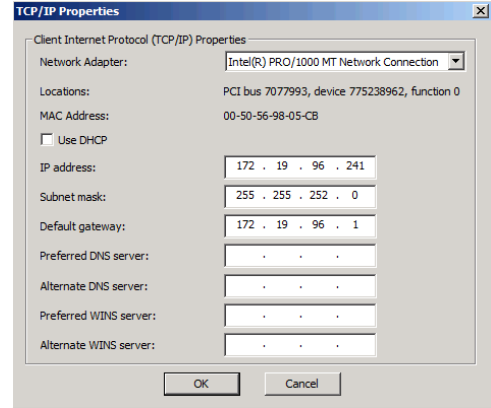
The full system restore starts.

18.

- Enter a UNC path to the `.inf` file for the mass storage drivers.

  The third party Mass Storage drivers are required to locate the boot disk when restarting the computer. You must provide the path to `.inf` file for the mass storage drivers.

- You can provide the path to `.inf` file for the NIC drivers now or you can provide it after the system restarts.

● It is recommended that you install the latest hardware drivers after the restore completes.

19.
● Enter the valid license key for the restored Windows Operating System. Refer to the check list in the Configuration section.

● Click **OK**.

20.
● Click **OK**.
● Remove the **Live CD** and restart the computer.
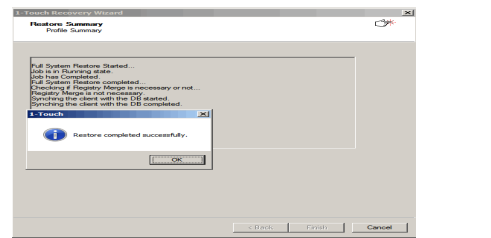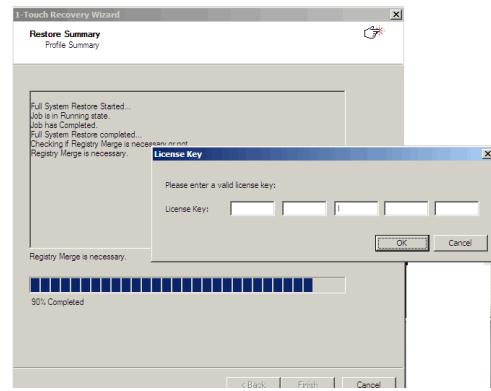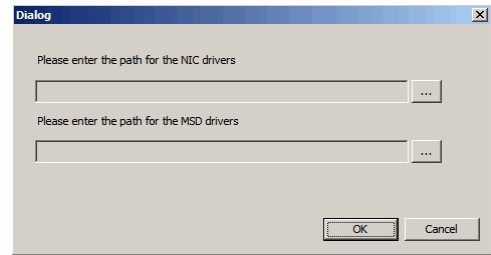
ONLINE RESTORE

Perform the Online Restore to reinstall the operating system on the client. The Windows Distribution Shares and Drivers available on 1-Touch Server are used to reinstall the operating system.

PREREQUISITE

Make sure that the Dissimilar Disk Restore Option is selected and all the required mass storage and NIC drivers are selected while creating the answer file.

1. Login to 1-Touch Server and create Answer File for the 1-Touch Client. For more information, go to Creating an Answer File.

2. Create 1-Touch Live CD.

Use 1-Touch **Live CD** to boot the client.

3.
● Select the language from the list
● Click **OK**.

4. Click **Next**.

5. Click **Yes** if all disk devices are detected.

6.
- Select **Online Restore**.
- Enter the **Client Name**.

  If the client answer file is not created on 1-Touch Server, select **Create Client Answer files for 1-Touch Recovery** and follow the steps described in Creating an Answer File.

- Click **Next**.

7.
- Enter **IP Address** of the **1-Touch Server** where the client answer file is available.
- Enter the **User name** and **Password** for the 1-Touch Server.
- Click **Next**.

8. Click **Next**.

9. Check the TCP/IP and Display Adapter configurations. Use the Client Checklist to check the configuration.

If they are incorrect, perform the following steps:

- Re-install the appropriate Network Interface Card drivers.
- Uninstall the Network Adapters and Display Adapters using the Hardware Uninstall Wizard or Windows Device Manager.
- Restart the computer.
- Reconfigure the TCP/IP and Display Adapter settings.

10.
- Review the **Source Disk Layout** and **Destination Disk Layout**.
- Right-click a disk from **Destination Disk Layout** and select the disk type that you want to assign to the destination disk.

11. Click **Yes**.

12.
- Repeat steps 10 and 11 to clean all the required disks from the **Destination Disk Layout**.
- Click **Done** to start the disk cleaning.

12.
- Right-click the disk from the **Source Disk Layout** that you want to map with a destination disk.
- Select **Map**.

13.
- Select a destination disk from the the the **Available Disk List** to map with the selected source disk .
- Select the Partition **Type**.
- Select the **File system**.
- Click **Perform quick format** if you want to format the selected disk.
- Click **Enable file and folder compression** to enable the file system compression for the selected disk.
- Enter the Volume **Size**.
- Select a **Drive Letter** to assign it to the selected volume.
- Click **OK**.

14.
- Review the **Destination Disk Layout**.
- Click **OK** to start recovery of the destination disk.

15.
- Reboot the computer after the windows installation completes.

During the Windows installation process of a 1-Touch Recovery, the Windows Administrator password is set as 1Touch. Upon completion of the 1-Touch Recovery, the Administrator's original password will be restored from the backup.

After the windows installation completes, the computer may reboot one or more times.

ADDITIONAL OPTIONS

ACCESSING THE RESPONSE FILE FROM AN UNC PATH DURING AN OFFLINE NON-INTERACTIVE RESTORE

You can access the recovery response file from a network location during the non-interactive restore. Follow the steps give below to perform the non-interactive restore when the recovery response file is stored in a network location:

1. Boot the client using the 1-Touch Live CD.

2.
- Select the language from the list
- Click **OK**.

3. Click **OK**.

A temporary DHCP IP will be assigned automatically to the client that you are recovering.

4. If the temporary DHCP IP is not assigned automatically, you have to provide the Static IP, Subnet Mask Default Gateway, Primary DNS and WINS.

5. Enter the UNC path of the location where the response file is located and click **OK**.

The permanent IP address of the client will be the IP address that is stored in the
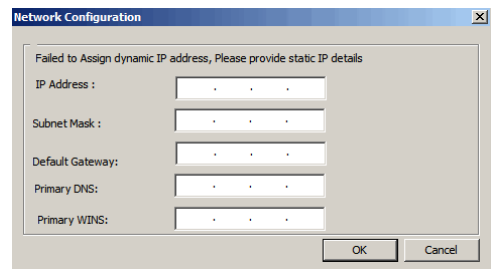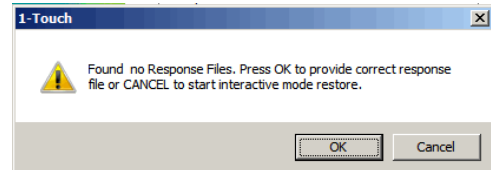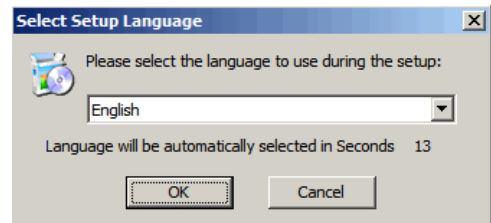
response file.

10. Click **OK** to start the full system restore.

....
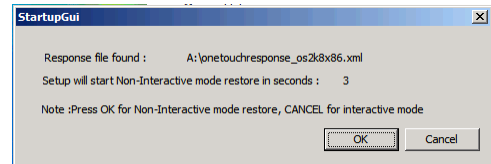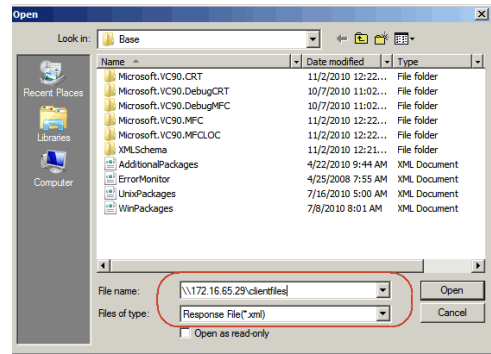
CHANGINGTHE CLIENT CONFIGURATION DURING AN OFFLINE NON-INTERACTIVE RESTORE

During a non-interactive restore, follow the steps given below to change the client configuration:

1.
   - From the CommCell Console, navigate to **<Client>**
   - Right-click the **<Client>** and click **All Tasks | 1-Touch Recovery Point**
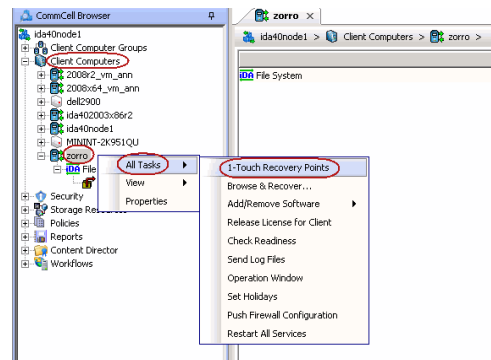
2.
   - Select a client configuration.
   - Click **Edit Config**.
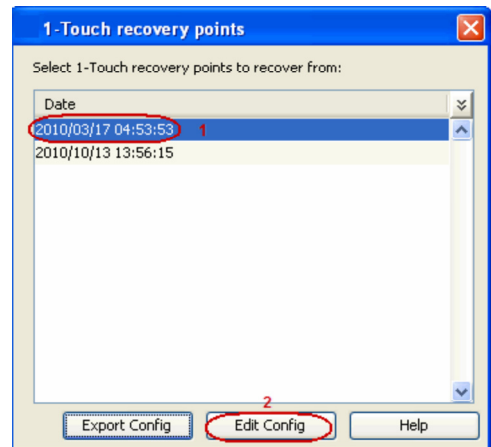
3.
   - Enter the CommServe IP address.
   - Enter the hostname and IP address of the MediaAgent that is used to backup the client.
   - Click **Change** and enter the CommCell Console credentials.
   - Click Change and enter the **Domain Login** Credentials.
   - Click **OK**.

4.
- Click **DNS** tab.
- Enter domain name server suffix for the network where client will be recovered.

5.
- Click **Network Config** tab.
- Select an interface to change the network configuration of the client.
- Click **Edit**.

6.
- Enter the IP address and network details of the network where client will be recovered.
- Click **OK**.

7. Click **OK** to save the updated client configuration.
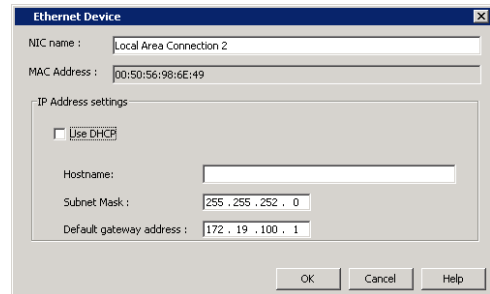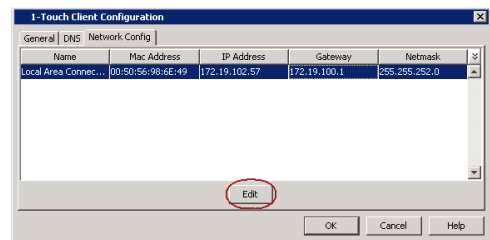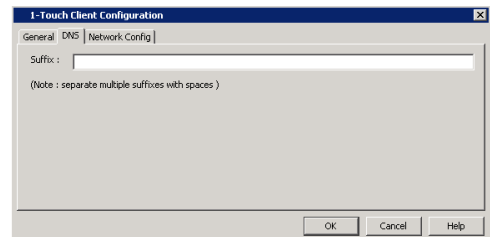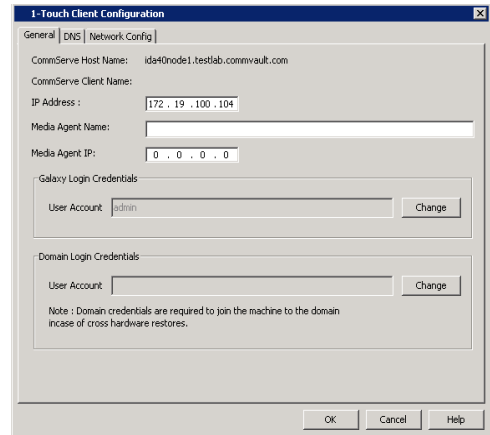
USING AN USB DRIVE INSTEAD OF LIVE CD

You can use an USB drive to boot the client. Follow the steps given below to create an USB drive for booting the client:

1. Connect the USB drive with the computer where you have stored the 1-Touch ISO image.

2. Open the Command Prompt and enter the following commands:

   ```
   DISKPART
   ```

   ```
   lis disk
   ```

3. Identify the disk number of the USB drive that you want to use to boot the client and enter the following commands:

   ```
   sel <disk number>
   ```

   ```
   clean
   ```

   ```
   create partition primary
   ```

   ```
   select partition 1
   ```

```
active

format fs=ntfs quick

assign

exit
```

4. Copy the `bootsect.exe` from Boot folder of Win7 distribution to one of the following location:

   ○ For Windows X64 clients: `SystemRecovery\Images\Windows x64\BOOT_IMAGE\ISO\boot`

   ○ For Windows 32-bit clients: `SystemRecovery\Images\Windows 32\BOOT_IMAGE\ISO\boot`

5. Using the command prompt, navigate to the above location and enter following command:

   `BOOTSECT.EXE/NT60 <assigned drive letter for USB drive>:`

6. Copy the content in ISO folder (`SystemRecovery\Images\Windows 32-bit\BOOT_IMAGE\ISO`) to USB Drive.

7. Connect the USB drive to the client that you want to boot.

8. Change the BIOS Settings on the client to boot from the USB drive.

CLUSTER RECOVERY

If all nodes the cluster are down, offline recovery is not supported for the first or primary node recovery. Perform the **Online Restore** to recover the first node in a cluster. Once the cluster starts, remaining nodes can be recovered using offline or online recovery process.

Perform the 1-Touch recovery of the Windows Server 2003 and 2008 cluster as follows:

1. Perform the **Online Restore** of the active node. The active node is the the node that has the quorum disk. The cluster services become available when the quorum disk is restored.

2. Perform the Interactive or Non-Interactive Restore to recover the passive nodes in the cluster.

   ● If the restored node shows unavailable in the cluster, evict and add the restored node.
   ● Do not perform the authoritative restore when you are performing Offline Restore.
   ● After you complete the Online or Offline Restore, do not start the authoritative restore before performing a full backup.
   ● For Windows Server 2003, start the command prompt, go to the `<install directory>\base` folder and enter the following command:

      authorutil.exe -cluster

RESTORE PROGRAM FILES FOR THE VIRTUAL SERVER

The cluster uses the following resources:

● Bull Calypso Communications Service
● Bull Calypso Client Event Manager

The program files required to start and run these resources must be restored to the virtual server's disk. You will need to restore the data to each virtual server using the Full System Restore of the Microsoft Windows File System *i*DataAgent restore. For more information, go to Restore Program Files for Virtual Server.

CONFIGURING WINS AND DNS DURING INTERACTIVE RESTORE

When the client computer and CommServe are in the same domain, DNS will be used for name resolution between client computer and CommServe.

WINS will be used for name resolution in the following scenarios:

● CommServe and Client computer are in different networks.
● CommServe is registered in a workgroup

During the Interactive Restore, you can configure the WINS as follows:

1. In the 1-Touch Client Recovery wizard, select **Offline Restore**.
2. Enter **CommSeve Host Name** and **IP Address**.
3. Select the Network Connection from the **Connection** drop-down combo box.
4. Select **Use the following IP address**.
5. Enter **IP address**, **Subnet mask**, **Default gateway**.
6. Enter the **DNS** in which CommServe is registered**.**
7. Enter the **Primary WINS**.
8. Click **Get Clients** to connect with CommServe and get the list of clients.
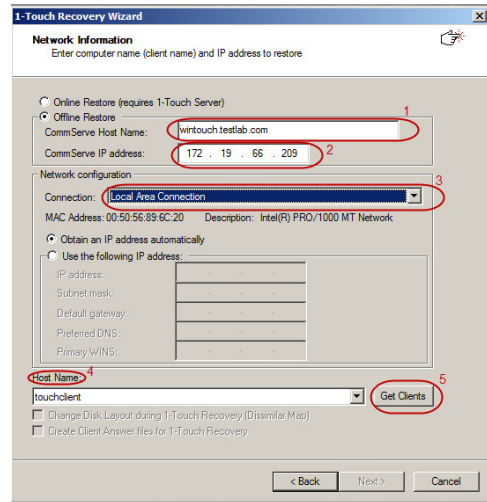
RESTORE THE TEAMING NETWORK ADAPTERS

To restore the teaming network adapter:

1. Uninstall the teaming software.

2. Restart the computer.

3. Install the teaming software to restore the teaming net.

Back to Top
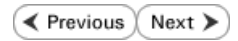
Troubleshooting - 1-Touch for Windows

| Deployment | Configuration | Recovery | Troubleshooting | FAQ |

◀ Previous | Next ▶

The following section provides information on some of the troubleshooting scenarios related to 1-Touch Recovery:

SYMPTOM/ERROR	SOLUTION
A full system restore of a Microsoft Windows 2008 Server requires the administrator to provide the product license key. This message will appear on the Windows login screen after a full system recovery from a backup that contained an activated product key: `An unauthorized change was made to Windows. You must retype your Windows Server Product Key to activate the license.`	Provide the activated product key again in order to log in to the recovered client.
When you attempt to integrate a service pack into a Windows Distribution folder for a processor type, X64, IA64, etc. that does not match the version of the 1-Touch Server, the following message will appear: `update.exe is valid, but is for a machine type other than the current machine`	1. Copy the Windows folder, CD-ROM or DVD to a directory. For example, from the Windows CD-ROM, **copy *.* C:\winXP.** 2. Download, copy and extract the Windows Service Pack executable to the same directory. For example: **copy xpsp2.exe c:\winXPSP2 c:\winXPSP2 \xpsp2.exe /u /x:C:\winXPSP2**. This will extract the i386 folder into `C:\winXPSP2` 3. Update/integrate the Windows Directory with the Service Pack. For example: **cd winXPSP2\UPDATES c:\winXPSP2 \UPDATES\update.exe /s:C:\winXP** The slipstreamed service pack distribution can now be imported to the 1-Touch Server using the Windows Distribution.
For Windows 2000, the system state restore fails.	If Hotfix KB828741 is in the backup, it must be applied to the target. Slipstream this fix into the Windows 2000 Distribution folder. Refer to KB828741 or Microsoft Security Bulletin MS04-012, "Cumulative Update for Microsoft RPC/DCOM (828741)" at http://www.microsoft.com/technet/security/bulletin/ms04-012.mspx.
Failure during Windows Server 2003 Cluster Recovery	When the cluster disks are repartitioned, a failure message may appear because the disk GUIDs for the quorum have been changed. 1. View the System Event Log. 2. If you see Event ID 1034 in the System Event Log, refer to the KB 305793 and KB 280425 in the Microsoft Knowledge Base articles on http://support.microsoft.com/.
Windows Installation Fails for Systems using HP OEM NIC	For Systems using the HP OEM NIC, when boot the client using the 1-Touch Live CD, a pop-up will indicate that the network interface cards found in the computer are different from those found at backup time. This error message appears, if the backup has captured the team virtual MAC address that was set by teaming. It is a software-generated MAC address and not an actual address. 1. Verify or provide the correct MAC address to the NICs found in the computer. This will update the Windows `unattend.txt` file. Copy the updated `%1-Touch Server% \ClientFiles\%ClientName%\unattend.txt` file to the `%1-Touch Server%\ClientFiles\% ClientName%\$OEM$\OnetouchTmp` folder. 2. Perform the Online Restore.

`During the mini setup stage the following error message appears:`
 	
`Windows could not complete the installation. To install Windows on this computer, restart the installation.`
	1. Open Command Prompt
	
	2. Navigate to `%systemdrive%\Windows\Panther`.
	
	3. Open `diagerr.xml` file.
	
	4. Ensure that the `diagerr.xml` file displays the following error message:
	
	5. `EnableLocalUserAccount: Unable to enable local account [Administrator]; status = 0x8c5`
	
	6. Perform the administrator backup of the client.
	
	The mini-setup fails during the offline restore because only the administrator can run the mini-setup.
	
	7. Perform the offline restore.

During the installation of Windows 2003, the following error appears: Error loading operating system.	Update the BIOS of the target computer OR 1. Start the Windows Distribution Manager on the 1-Touch Server. 2. Apply the following Microsoft Hotfix:

	WindowsServer2003-KB931761-x86-ENU.exe
Windows Management Instrumentation (WMI) Service are not recovered after an Interactive or Non-interactive restore.	The WMI services cannot be restored using the Interactive or Non-interactive restore method if the VSS is not enabled before performing the system state backup. For more information about enabling VSS for system state backup, refer to Configuring System State Backups. To restore WMI services, browse the default subclient and select WMI from the System State. For more information about Browse and Restore method, refer to Getting Started - Windows File System Restore.
Interactive Restore fails if you manually reboot the client after the Calypso install.	After the Calypso install, the client IP address is added to the CommServe database and when you initiate the Interactive Restore with the same IP address and hostname, the restore fails. Follow the steps given below before starting the interactive restore: 1. From the CommCell Browser, navigate to **Client Computers**. 2. Identify and right-click the client and select **All Tasks | Release License**. 3. Right-click the client and select **All Tasks | Delete**. 4. Start the Interactive Restore.
When you performing an online restore for a client that has Calypso 8.0 version, you may get the following error: `Qlogin: Error 9x103: Invalid Login/Password. Logon Failed.`	When you are recovering the 8.0 client, you must provide the CommCell Console username and password in the answer file. The single signon feature is not available for 8.0 clients and the user account credentials of the domain cannot be used during the Online Restore. Follow the steps given below to avoid this error: 1. Before starting the recovery of an 8.0 client, create a CommCell user account with an administrative privileges. 2. From the 1-Touch Server, create an answer file for the client and enter the CommCell username and password. 3. Perform the Online Restore using the modified answer file.
During the Offline Restore the CommCell Console displays the following message: `Please check the Windows Server service. Windows share permissions will not be backed up or restored. [[2114] The Server service is not started.`	This message appears because Windows in not running on the target computer. The Share permissions will be restored automatically during the Offline Restore. You can ignore this error message.
Distributed Component Object Model (DCOM) component appears disabled after the 1-Touch restore of the client computer.	Run the following command from the command prompt on the client computer after 1-Touch restore is complete: `%windir%\system32\msdtc.exe -resetLog`

Microsoft Distributed Transaction Coordinator (DTC) Service does not start after 1-Touch Recovery.	Follow the steps given below to restart the Microsoft Distributed Transaction Coordinator (DTC) Service:
	
	1. Navigate to the following folder:
	`%SystemRoot%\System32\Dtclog`
	If the `Dtclog` folder does not exist, create the folder.
	
	2. Check if a `Msdtc.log` file exists and ename it to `Msdtc.old`.
	
	3. Create a new `Msdtc.log` file using Notepad and save it at the following location:
	`%SystemRoot%\System32\Dtclog`
	
	4. Open the command prompt and enter the following command:
	`msdtc -resetlog`

1-Touch Client does not reboot automatically after the full system restore.	If the client computer has 2 disks, the disk drive numbers may not correspond as expected during the full system restore. As a result, the system disk will be restored as a second disk and client computer fails to reboot. For more information about issues in disk enumeration, refer to http://support.microsoft.com/kb/937251. Change the order of the disks from the BIOS Settings after the restore completes.
Full System Restore goes to pending state during 1-Touch Recovery of Windows XP SP2.	If the 1-Touch client has Windows XP Service Pack 2 (SP2) installed on it, Windows Firewall is turned on by default. A full iDataAgent Restore job will go to a pending state if the client firewall is turned on. When the job state goes to pending perform the following: 1. On the command line, type CTRL+C and press Enter. 2. Turn off the firewall on the client. 3. Resume the job from the CommCell Console. The restore operation will recover the firewall settings from the backup data. You can view the firewall settings on the client computer: 1. Click **Start** and then click **Control Panel**. 2. In the **Control Panel**, click **Windows Security Center** and then click **Windows Firewall**.
Windows File System iDataAgent install fails during the Online Restore	The Online Restore process installs the Windows File System iDataAgent software in silent mode, and a silent mode install of this iDataAgent supports only the defined default port numbers. If the Windows File System iDataAgent software was installed on the client using port numbers other than the default port numbers (8400, 8402), the silent install of this iDataAgent may fail.

	If this occurs, install the Windows File System iDataAgent software and run fullida.bat on the client to continue with the recovery. The `fullida.bat` is located in `C:\onetouchtemp\` folder on the client computer.
While creating Live CD, you may get following error: `Could not contact server, AttachPreInstall failed.`	This error appears because the network card without an IP has got more priority in the 1-Touch server. Follow the steps given below to change the priority of the NIC card: 1. Click **Start | Run.** 2. Type `ncpa.cpl` and then click **OK**. You can see the available connections in the LAN and High-Speed Internet section of the Network Connections window. 3. On the **Advanced** menu, click **Advanced Settings**, and then click the **Adapters and Bindings** tab. 4. In the **Connections** area, select the connection that you want to move higher in the list. 5. Use the arrow buttons to move the connection.
1-Touch Restore Fails with the following Error: `Windows returned no error string for error 8004240f`	You will get this error when a new partition cannot be created on the unused space on a disk. Ensure that the specified partition size is smaller than the current partition size. You can manually decrease the size during disk creation by selecting the **Dissimilar Disk Mapping** option. For more information refer to following links: ● Dissimilar Disk Mapping - Dissimilar Disk Restore ● VDS Errors - http://msdn.microsoft.com/en-us/library/dd208031.aspx

◀ Previous   Next ▶

Frequently Asked Questions - 1-Touch Windows

| Deployment | Configuration | Recovery | Troubleshooting | FAQ |

◀ Previous   Next ▶

CAN I CONVERT A CLIENT COMPUTER INTO A VIRTUAL MACHINE?

Yes. When a CommServe is connected to an ESX server, you can convert convert a physical machine (computer) into a virtual machine using the 1-Touch backup data. You can also modify the hardware and network configuration of the client while converting it into a virtual machine. For more information, refer to Virtualize Me - Getting Started.

CAN I CONVERT A VIRTUAL MACHINE INTO A PHYSICAL MACHINE?

Yes. Follow the steps given below to convert a virtual machine into a physical machine:

1. Ensure that you have enabled 1-Touch backup on the virtual machine and you have performed atleast one full backup.

2. Create a response file for the virtual machine and perform the Non-Interactive Restore using the response file.

   For more information about creating response file for a Windows machine, refer to Non-Interactive Restore.

   For more information about creating response file for a Linux machine, refer to Non-Interactive Restore.

   During Non interactive restore, copy the response file on a USB drive and connect the USB drive to a physical machine.

HOW TO ADD 1-TOUCH ISO IMAGE TO A PXE SERVER

1. Create the 1-Touch ISO image using the **1-Touch Boot CD Wizard**.

2. Configure the PXE Server and add the 1-TOUCH ISO image to it.

3. Use a remote monitoring console to start the client and select a PXE boot.

4. Change the CMOS boot sequence to boot from the hard disk.

5. Perform the Offline or Online Restore.

6. Once the restore completes, set the CMOS back to PXE or the preferred boot method.

HOW TO ADD THE BROADCOM NETXTREME II DRIVER TO AN ANSWER FILE

1. Gather the following Broadcom Netxtreme II NIC drivers:
   - `bxnd52x.sys` (for the Windows install)
   - `bxvbdx.sys` (for the Windows install)
   - `b06nd51x.sys` (for the 1-Touch boot CD and RIS Driver)

2. Add any Mass Storage Drivers needed for the Windows installation to the answer file. For example: `percsas.sys` or `mraid32.sys`.

3. Add the following NIC Drivers to the answer file:
   - `BXBVD.INF`
   - `BXND.INF`

4. Create a batch file with the following contents for the NetxTremeII driver:

   c:\onetouchtmp\netset c:\onetouchtmp\unattend.txt

   When you run this batch file, NetxTremeII driver will be able to set static IP addresses during installation

5. Create a master batch file that contains the following batch file names and paths:

   Master.bat:

   Call "C:\OneTouchTmp\netxtremeII2.bat"

   Call "C:\OneTouchTmp\mapshare.bat"

   Call "C:\OneTouchTmp\afterBoot.bat"

6. Add the name and path of the master batch file in the `unattend.txt` file located at `Clientfiles\%clientname%`. The contents of the `unattend.txt` file will look as follows:

   [GuiRunOnce]

   Command0="C:\OneTouchTmp\MASTER.bat"

7. Copy the following files to `Clientfiles\%clientname%\$OEM$\$1\OneTouchTmp`:

    ○ `netXtremeII2.bat`

    ○ `netset.exe` (provided by Microsoft)

    ○ `unattend.txt` (from `Clientfiles\%clientname%`)

8. Add NetXtreme II RIS driver (B06ND.INF) to the 1-Touch ISO image.

   When you are importing the RIS driver to the Boot CD Image, remove any Broadcom non-RIS drivers from the image. Otherwise, the non-RIS driver will be found at the boot and it will not connect.

HOW CAN I MANUALLY ADD SOFTWARE UPDATES TO 1-TOUCH SERVER CACHE?

1. Login to 1-Touch Server.

2. Navigate to `<software_install_directory>/Base/`

3. Double-click `CopyToCache.exe`.

4. Enter or **Browse** to the location where updates are available.

5. Select **Copy to Cache** to copy the updates to CommServe Updates Cache

6. Select **Copy to 1-Touch** to copy the updates to 1-Touch Server Updates Cache.

7. Click **Copy** to start the copying process.
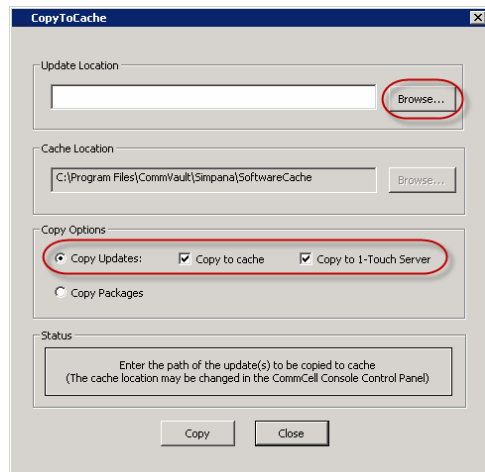
AFTER PERFORMING 1-TOUCH BACKUP, I UPGRADED THE CALYPSO VERSION. CAN I USE THE BACKUP PERFORMED BEFORE THE UPGRADE FOR 1-TOUCH RECOVERY?

If the Calypso version or update level on the client computer is different from that for the Calypso software on the backup date, then consider the following before performing the 1-Touch recovery:

- Online Restore –You must exclude the Calypso folder while performing the Online Restore. This will prevent any older versions of the binaries from being restored.

- Interactive Restore – You must perform the backup on the client computer after the upgrade and then perform the Interactive Restore.

CAN I USE CLIENT PREPARATION WIZARD TO ADD SERVICE PACKS TO WINDOWS VISTA AND WINDOWS 2008?

No. You cannot add service packs to Windows Vista and Windows 2008 using Client Preparation Wizard. For unsupported deployment scenarios, Microsoft KB recommends to obtain the Windows Service Pack media directly from Microsoft. Refer to http://support.microsoft.com/default.aspx/kb/951035/

CAN I INSTALL WINDOWS ON ANY DRIVE OF THE CLIENT COMPUTER?

1-Touch recovery may fail if the client computer has following configurations:

- Windows XP or Windows 2003 is installed on a drive other than the C drive.

- Drive letters up to and including Windows drive are not in order. For example:

  `C:, E:\Windows; D:`

  `C:, F:, G:\Windows`

- Drive letters up to and including the Windows (boot) drive are in order, but one letter is assigned to the installation disk drive. For example:

  `C:, D:(Installation Disk); E:\Windows\`

- Drive letters up to and including the Windows (boot) drive are in order, but Windows is installed on a disk other than the first disk that is controlled by a second disk controller. For example:

  `d1 controller1 C:, D:, E:,`

  `d2 controller2 F:\Windows`

A maximum of 19 partitions per computer can be used. Also, drive letters W:, X:, Y:, and Z: must not be assigned within the computer.

CAN I PERFORM 1-TOUCH RECOVERY OF A WINDOWS XP CLIENT WHICH HAS DYNAMIC DISKS?

You can perform the 1-Touch recovery of the Windows XP client if the system disk is not a dynamic disk. If the system drive is on a dynamic disk, perform one of the following:

● Select Recreate all disks option during 1-Touch Recovery. This option will recreate and restore the disk type as basic. All simple volumes on the disk will be created as basic partitions.

● Select Dissimilar Disk Mapping option during 1-Touch Recovery. Initialize the disk and map the partitions and disk as basic. The data will restore to a basic disk.

After the 1-Touch recovery is complete, the data is restored and the computer is restarted, use Disk Manager in Windows to manually convert the basic disk to dynamic. Basic partitions will be converted to simple once the disk is converted from basic to dynamic.

1-Touch recovery is not supported if the dynamic system disk has additional RAID volumes on the system disk. RAID volumes must be mapped as basic partitions after converting system disks to dynamic disks.

CAN I SELECT FORMAT SYSTEM DRIVE OPTION DURING ONLINE OR INTERACTIVE RESTORE?

You can select the **Format System Drive** option during the Online or Interactive Restore. Before selection this option, ensure that Calypso is installed on the system drive. If Calypso is installed on any drive other than the system drive, select the **Similar Disk Mapping** or **Dissimilar Disk Mapping** option.

CAN I PERFORM 1-TOUCH RECOVERY IF THE CLIENT AND THE COMMSERVE ARE SEPARATED BY A FIREWALL?

No. You cannot perform 1-Touch Recovery (Interactive, Non-Interactive, or Online Restore) when firewall is configured between the client and the CommServe.

CAN I PERFORM 1-TOUCH RECOVERY IF THERE IS A PORT RESTRICTION BETWEEN THE CLIENT AND THE MEDIAAGENT?

No. You cannot perform 1-Touch Recovery (Interactive, Non-Interactive, or Online Restore) when there is a port restriction between the client computer and the MediaAgent.

CAN I PERFORM 1-TOUCH RECOVERY OF A CLIENT COMPUTER WITH UEFI?

No. 1-Touch Recovery is not supported if the client computer is configured with UEFI or EFI BIOS.

CAN I PERFORM 1-TOUCH RECOVERY OF THE DATA WHICH IS ENCRYPTED USING THE MCAFEE ENDPOINT ENCRYPTION?

No. If the data on a client computer is is encrypted using the McAfee Endpoint Encryption, 1-Touch recovery is not supported.

WHICH SUBCLIENT CAN BE USED TO PERFORM THE BACKUP OF THE MACHINE?

If you want to perform the non-interactive restore, you must use default subclient in the default backupset to perform the 1-Touch or system state backup of the client computer. Any other subclient or backup set is not supported for Non-Interactive Restore.

◀ Previous Next ▶

Deployment - OnePass Agent for Windows File System

Install   **Configuration**   **Data Movement**   **Recover**   ◀ Previous   Next ▶

The OnePass Agent is integrated with Windows File System *i*DataAgent as a method to archive files which have been backed up. Only files which meet a predetermined user defined set of rules become candidates for archiving. Follow the steps given below to install the OnePass Agent for Windows File System.

INSTALLATION

The software can be installed using one of the following methods. Ensure you have the following before performing the install:

● Software version Service Pack 12.

METHOD 1: INTERACTIVE INSTALL

Use this procedure to install directly on client computer.

METHOD 2: INSTALL SOFTWARE FROM COMMCELL CONSOLE

Use this procedure to install remotely on a client computer.

BEFORE YOU BEGIN

Download Software Packages
Download the latest software package to perform the install.

System Requirements
Verify that the computer in which you wish to install the software satisfies the System Requirements.

METHOD 1: INTERACTIVE INSTALL

1. Run **Setup.exe** from the **Software Installation Disc** on a client computer that satisfies the minimum System Requirements.

2. Select the required language.

   Click **Next**.

3. Select the option to install software on this computer.

   The options that appear on this screen depend on the computer in which the software is being installed.

4. Click **Next**.

5. Click **OK**.
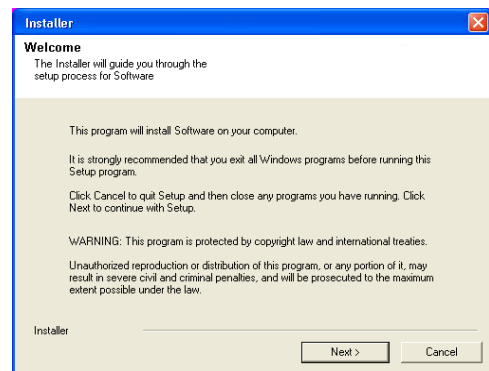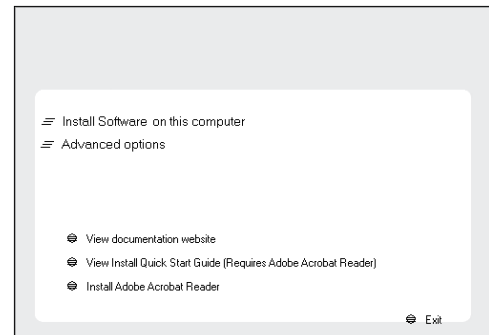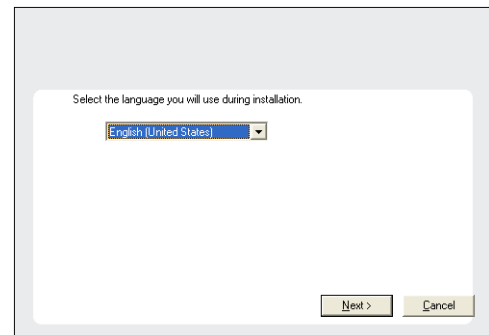
6. Select **I accept the terms in the license agreement**.
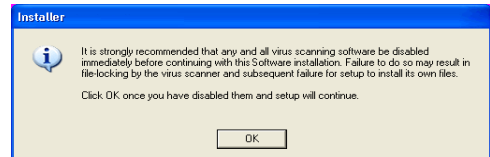
Click **Next**.

7. Expand **Client Modules** | **Backup & Recovery** | **File System** and select **Windows File System *i*DataAgent**.

Expand **Client Modules** | **Archive Management** and select **Driver for File Archiver**.

Click **Next**.

8. Click **YES** to install Microsoft .NET Framework package.

- This prompt is displayed only when Microsoft .NET Framework is not installed.
- Once the Microsoft .NET Framework is installed, the software automatically installs the Microsoft Visual J# 2.0 and Visual C++ redistributable packages.

9. If this computer and the CommServe is separated by a firewall, select the **Configure firewall services** option and then click **Next**.

For firewall options and configuration instructions, see Firewall Configuration and continue with the installation.

If firewall configuration is not required, click **Next**.
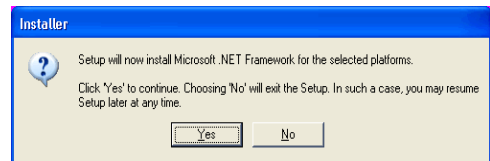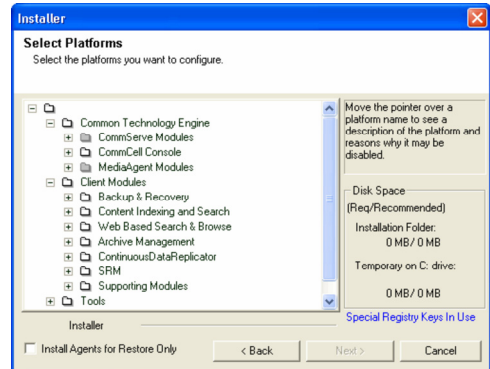
10. Enter the fully qualified domain name of the **CommServe Host Name**.

Click **Next**.

Do not use space and the following characters when specifying a new name for the CommServe Host Name:

\|`~!@#$%^&*()+=<>/?,[]{}:;'"
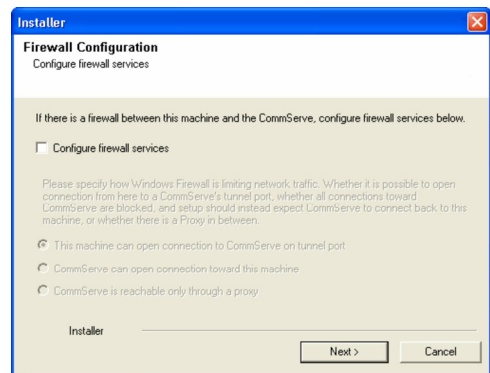
11. Click **Next**.
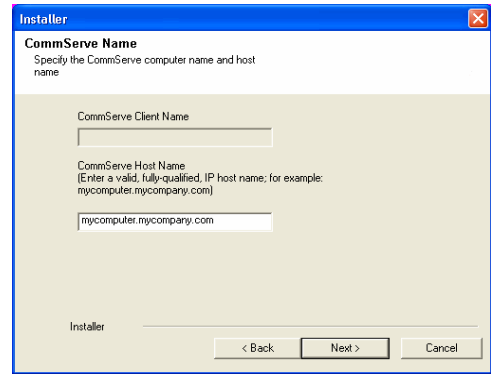
12. Select **Add programs to the Windows Firewall Exclusion List**, to add CommCell programs and services to the Windows Firewall Exclusion List.

Click **Next**.

> This option enables CommCell operations across Windows firewall by adding CommCell programs and services to Windows firewall exclusion list.
>
> It is recommended to select this option even if Windows firewall is disabled. This will allow the CommCell programs and services to function if the Windows firewall is enabled at a later time.
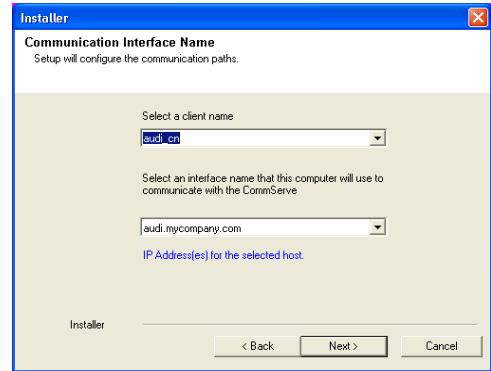
13. Click **Next**.
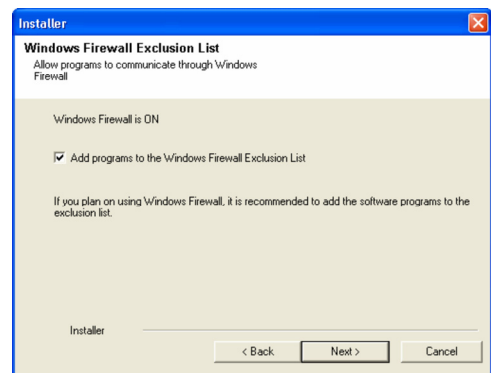
14. Verify the default location for software installation.

Click **Browse** to change the default location.

Click **Next**.

- Do not install the software to a mapped network drive.
- Do not use the following characters when specifying the destination path:

  / : * ? " < > | #
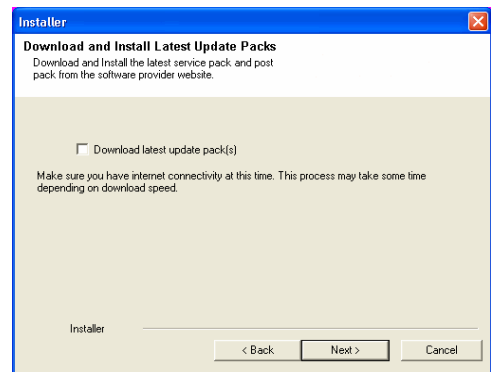
It is recommended that you use alphanumeric characters only.

15. Select a Client Group from the list.

Click **Next**.

This screen will be displayed if Client Groups are configured in the CommCell Console.

16. Click **Next**.

17. Click **Next**.

18. Select a **Storage Policy**.
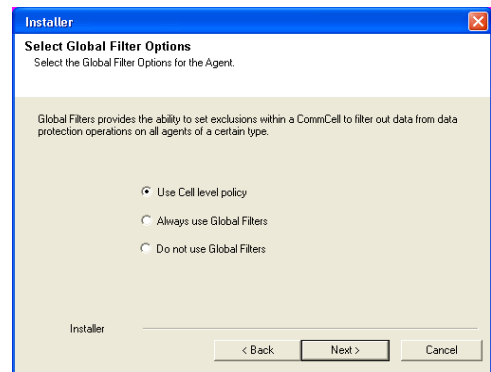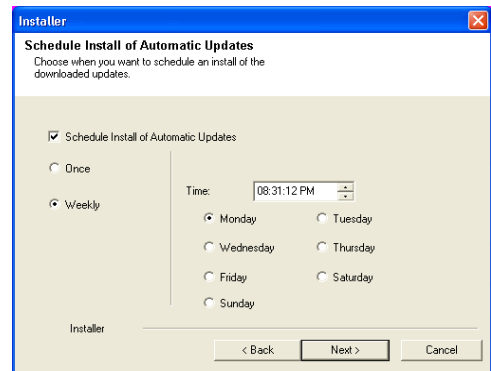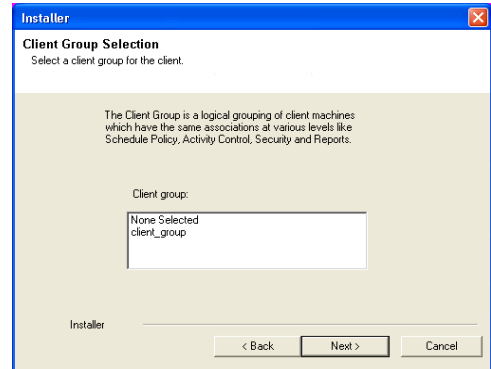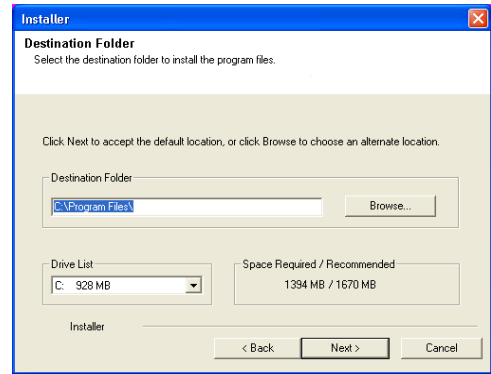
Click **Next**.

If you do not have Storage Policy created, this message will be displayed. Click **OK**.

19. Click **Next**.
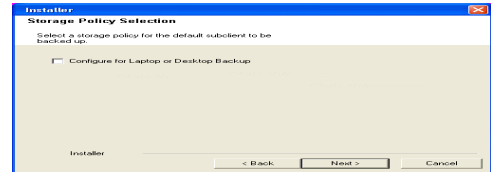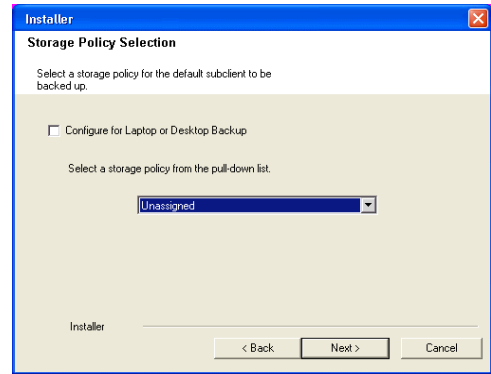
20. Click **Next**.
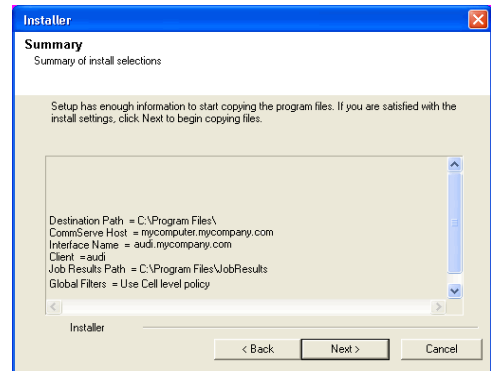
21. Click **Finish**.
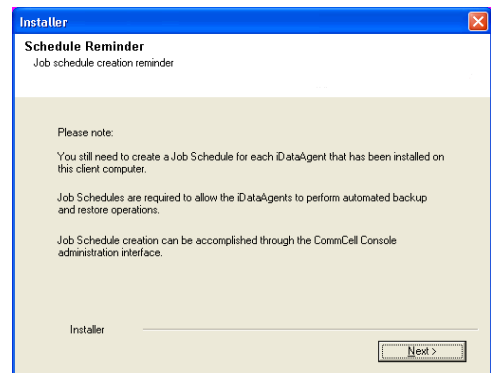
22. Install software version Service Pack 12 or higher.
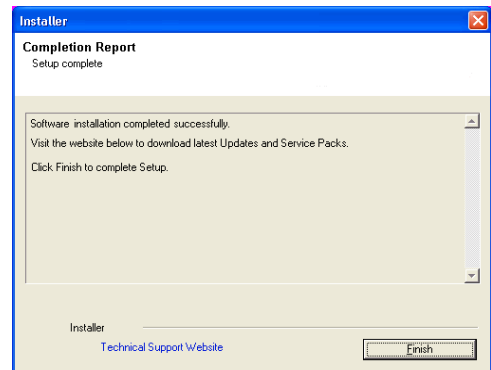
See Updates and Service Packs for more information on installing the latest service pack.

METHOD 2: INSTALL SOFTWARE FROM COMMCELL CONSOLE

1. From the CommCell Browser, select **Tools** | **Add/Remove Software** | **Install Software.**
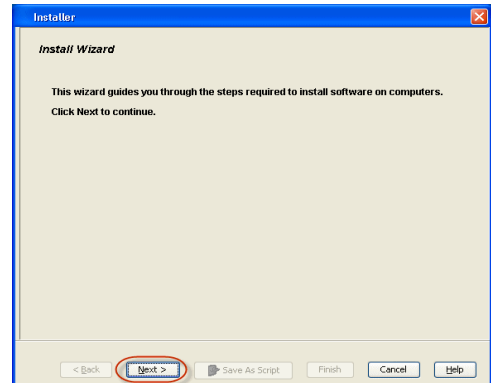
2. Click **Next**.

3. Select **Windows**.
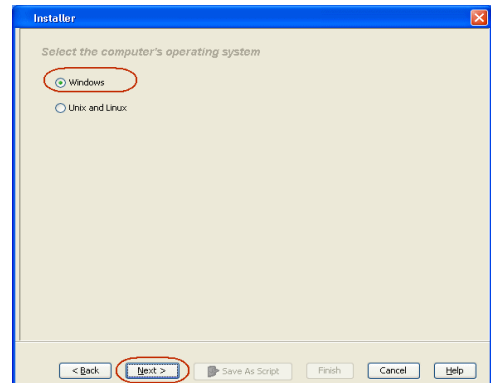
Click **Next**.

4. Select **Manually Select Computers**.
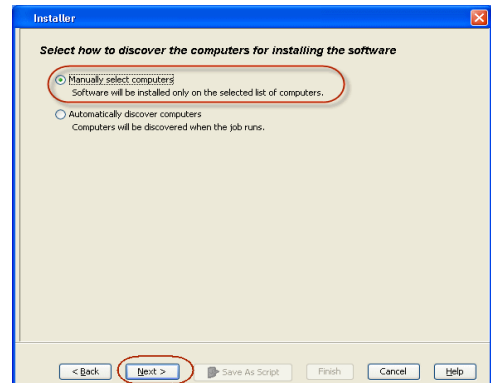
Click **Next**.

5. Enter the fully qualified domain name of the computer in which you wish to install.

For example: `apple.domain.company.com`

Click **Next**.
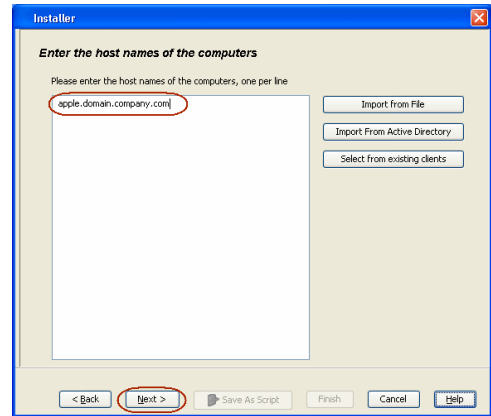
6. Click **Next**.

7. Specify **UserName** and **Password**.
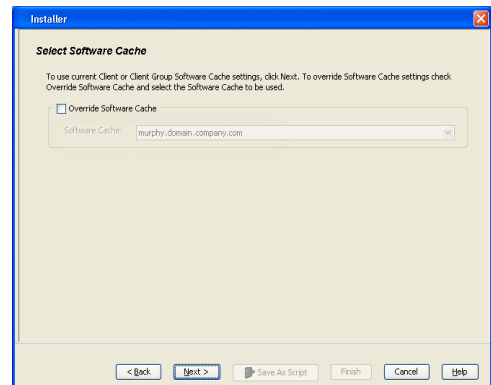
Click **Next**.

8. Select **Windows File System iDataAgent** and **Driver for File Archiver**.
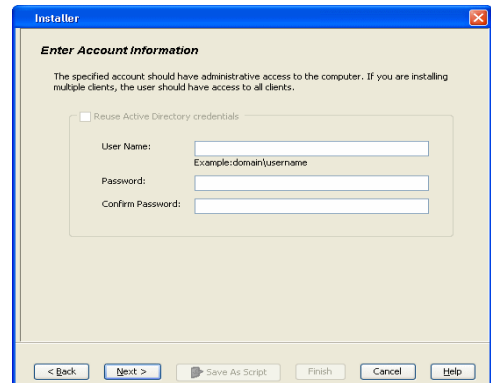
Click **Next**.

9. Click **Next**.
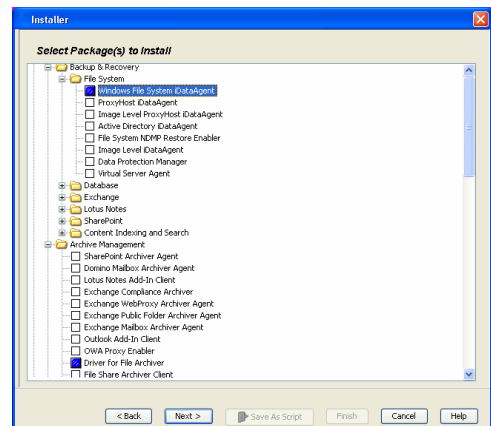
Client Groups will be displayed if Client Groups are configured in the CommCell Console.

10. Select **Reboot**.

Click **Next**.
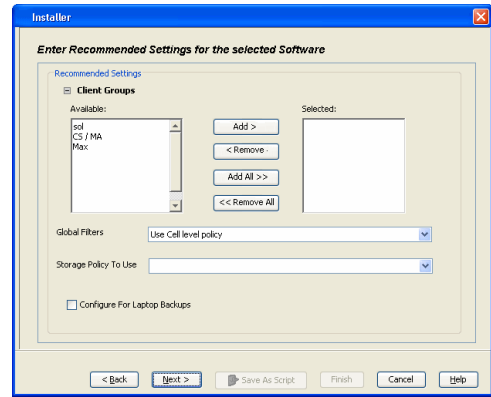
11. Select **Immediate**.

Click **Next**.
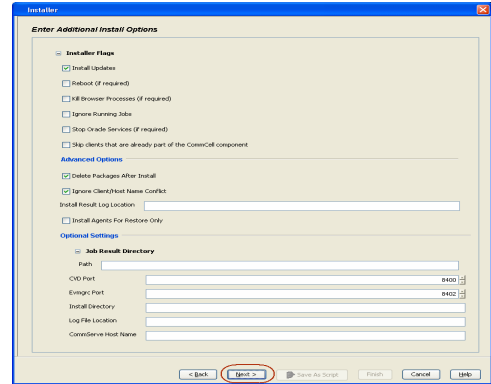
13. Click **Finish**.
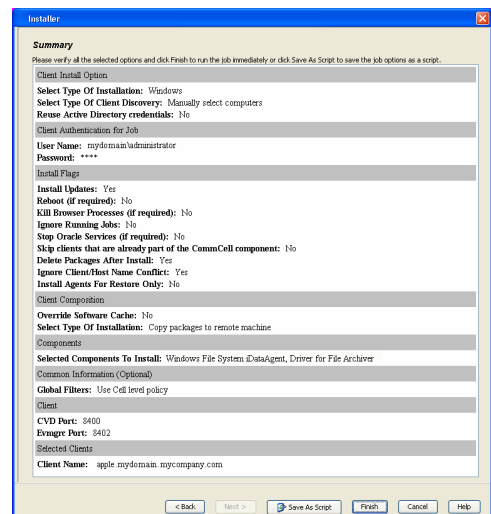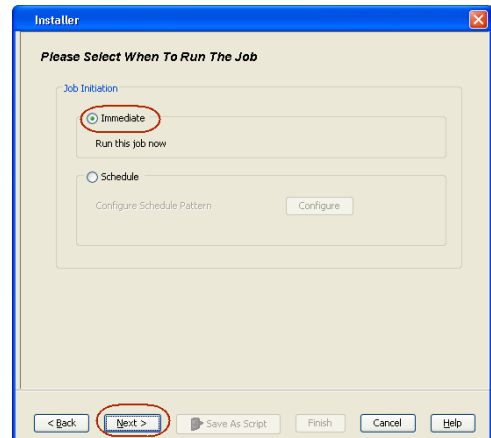
14. You can track the progress of the job from the **Job Controller** or **Event Viewer** window.
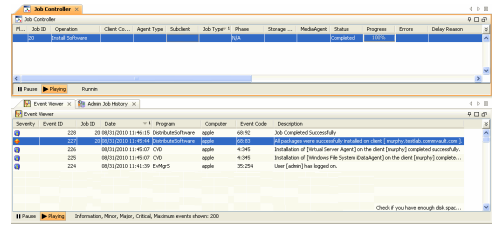
15. Once the job is complete, right-click the **CommServe** computer, click **View** and then click **Admin Job History**.
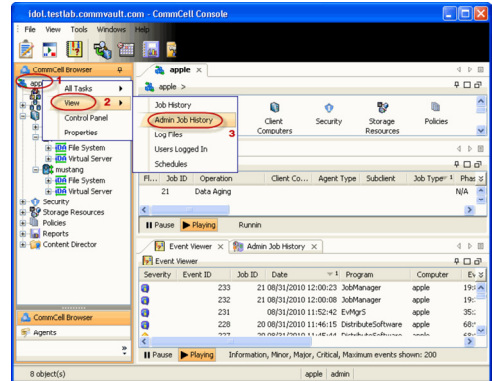
16. Select **Install/Upgrade/Remove Software**.

Click **OK**.
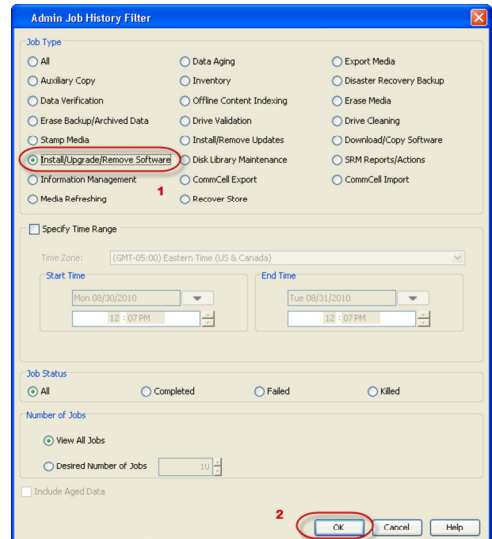
17. You can view the following details about the job by right-clicking the job:
- Items that succeeded during the job
- Items that failed during the job
- Details of the job
- Events of the job
- Log files of the job

18. Install software version Service Pack 12 or higher.
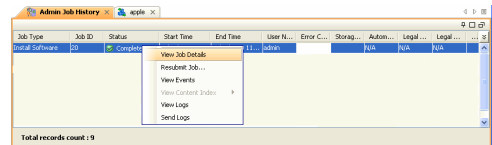
See Updates and Service Packs for more information on installing the latest service pack.

Configuration - OnePass Agent for Windows File System

| Install | Configuration | Data Movement | Recover |

◀ Previous   Next ▶

Once the Windows File System *i*DataAgent is installed, the OnePass Agent can be enabled by following the steps given below:

1.

- From the CommCell Console, navigate to **Client Computers | File System**.
- Right-click the **File System | Properties**.
- Select **Enable for Archiving.**
- Select **Enable SRM.**
- Click **OK**.

2.
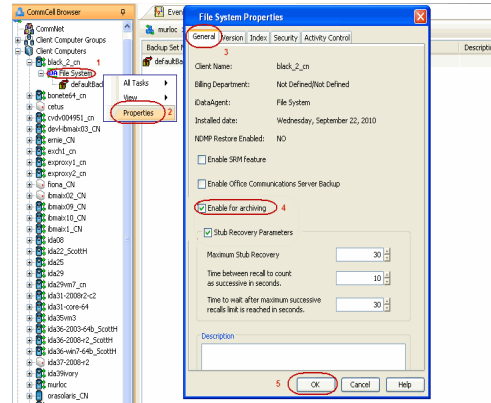
- From the CommCell Console, navigate to the **Subclient**.
- Right-click the subclient and select **Properties**.
- Click the **Rules** tab and select **Enable Stubbing**.
- To archive your files immediately, set the rules accordingly based on the file access time, modified time or file size.
- Click **OK**.

3.
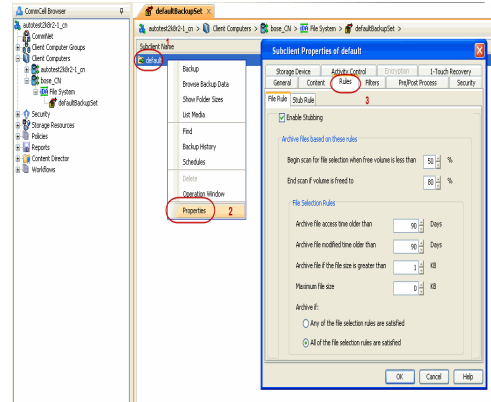
- Click the **Storage Device** tab.
- Select the **Storage Policy** from the drop down list.
- Click **Ok**.

   If you do not have a Storage Policy created, follow the steps given below to create a Storage Policy.
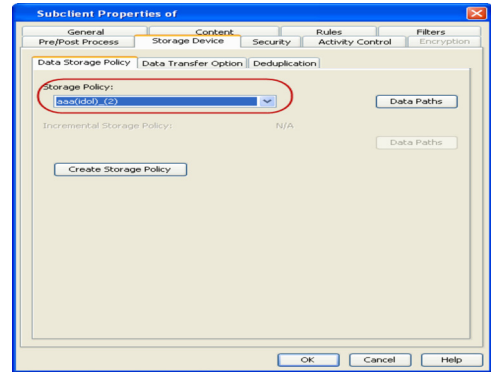
4.

1. Click **Create Storage Policy**.

2. Follow the prompts displayed in the Storage Policy Wizard. The required options are mentioned below:
   - Select the Storage Policy type as `Data Protection and Archiving`.
   - Select `No` to allow legal hold to use the policy.
   - Specify the name of the Storage Policy.
   - Specify the name of the primary copy. The primary copy is automatically created along with the Storage Policy.
   - Select `No` for use of an existing global deduplication policy.
   - Specify name of the default library to which the Primary Copy should be associated. This must be a disk library. Ensure that you select a library attached to a MediaAgent operating in the current release.
   - Select the MediaAgent.
   - Verify the device streams and the retention criteria information.
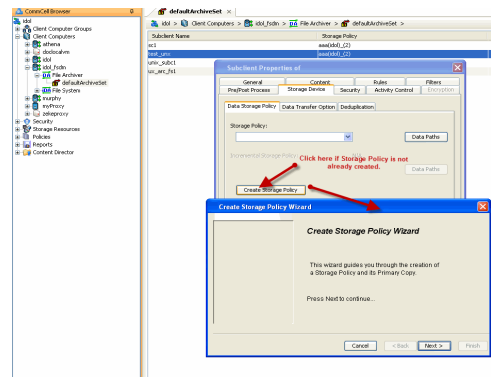
- Select `Yes` to enable deduplication for the primary copy. Select the Enable Client Side Deduplication option.
- Name of the Deduplication Store, MediaAgent hosting the Deduplication Store, and the location of the Deduplication Store.
- Review the details and click **Finish** to create the Storage Policy. The primary copy is also created.

3. Return to Step 3 to associate the Storage Policy to the subclient.

Data Movement - OnePass Agent for Windows File System

| Install | Configuration | Data Movement | Recover | ◀ Previous | Next ▶ |

PERFORM A BACKUP

After you have enabled the archiving option, perform a full backup to archive the backed up files.

WHAT GETS ARCHIVED	WHAT DOES NOT GET ARCHIVED
Local Volumes	Encrypted Files
Local Files and Folders	Files with extensions `*.dll`, `*.bat`, `*.exe`, `*.cur`, `*.ico`, and `*.lnk`
Mount points to volumes	Sparse Files
	The following Bull software folders cannot be archived: ● Install directory ● Job Results directory ● Log files directory ● Index cache directory
	Alias mount points to drive letter volumes.
	`/etc` system directory
	Files residing in the SIS Common store (Windows Single Instance Storage)
	Files from Resilient File System (ReFS) volumes on Windows Server 2012 computers

WHAT DOES NOT GET ARCHIVED

The following file types/objects are automatically filtered out of archive operations by the system, and cannot be archived.

● Install folder

● Job Results folder

● Index cache folder

● Log files folder

● Windows system32 folder

● Alias mount points to drive letter volumes*

● Unix data residing on a Windows NFS share

● Files with attributes of encrypted or sparse

● Files with attributes of hidden and system

Files Excluded from archiving (stubbing)

● *.dll

● *.bat

● *.exe

● *.cur

● *.ico

● *.lnk

The following section provides step-by-step instructions for performing your first backup:

1.
   ● From the CommCell Console, navigate to **Client Computers** | **File System**
   ● Right-click the **Subclient** and click **Backup**.
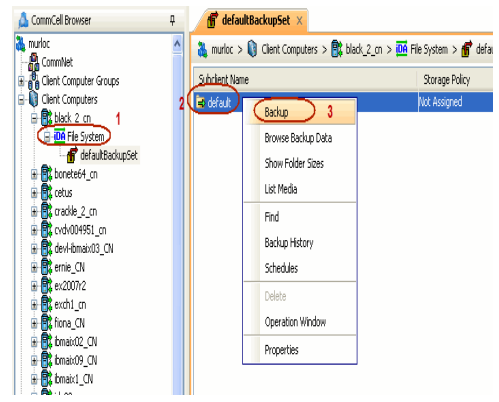
2.
   ● Select **Full** as backup type and **Immediate** to run the job immediately.

- Click **OK**.

3.   You can track the progress of the job from the **Job Controller** or **Event Viewer** window of the CommCell console.

4.   Once the backup process is completed, files that meet the stubbing rules are stubbed.

- **Stubs** are placeholders of the original data after it has been migrated to the secondary storage.
- Stubs replace the backed up files in the location of the file.
- After stubbing, the size of the files on the disk reduces.

5.   Once job is complete, view the details of job from the **Backup History**. Right-click the subclient and select **Backup History**.

Click **OK**.

6.
- You can view a list of the files archived during the backup.
- Right-click the job.
- Click **View Stub File List**.
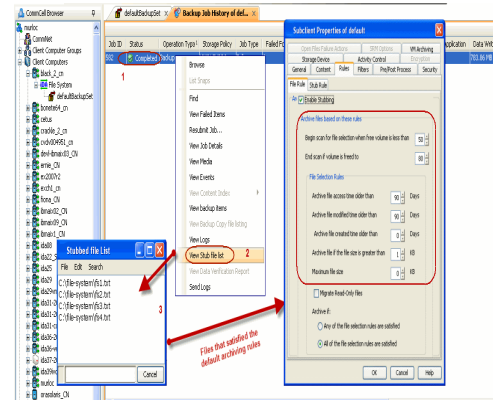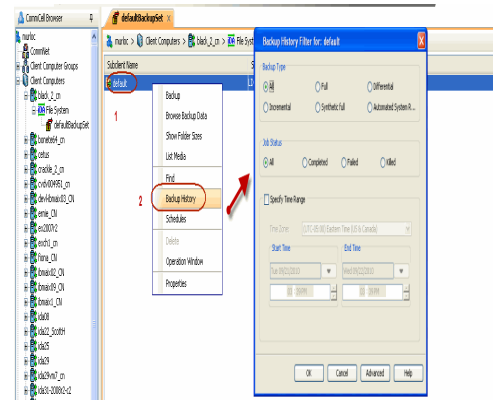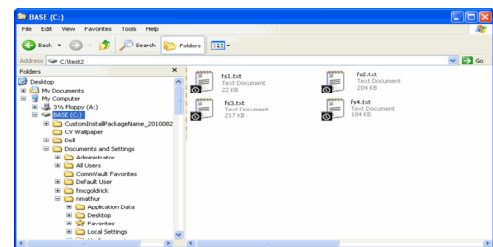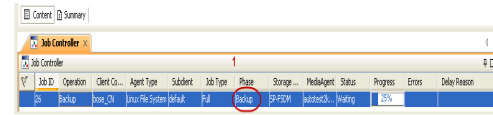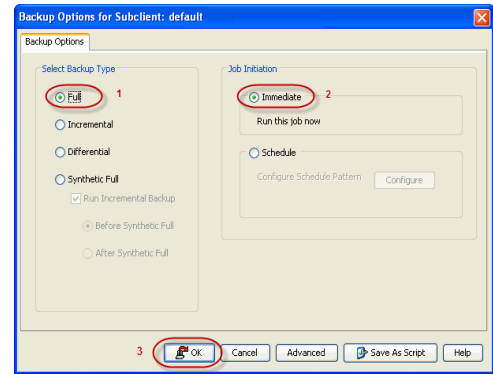
Recover Data - OnePass Agent for Windows File System

| Install | Configuration | Data Movement | Recover |

◀ Previous Next ▶

RECOVER STUBS

Use the following method to recover stubs of a file or multiple files.

1. To perform stub recovery of a file or multiple files, perform an action that executes an open and read on an archived file to initiate the recovery operation.

It might take a few minutes for the recovered file to show up once the stub is double-clicked.
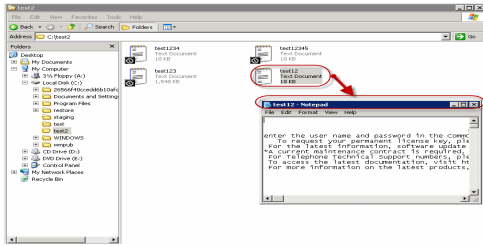
2.
- You can view the details of job from the **Restore History**.
- Right-click the **Backup Set** and select **View | Restore History**.
- Click **OK**.
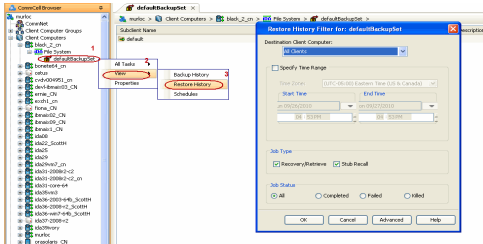
3. Right-click the job and select **View Job Details**.
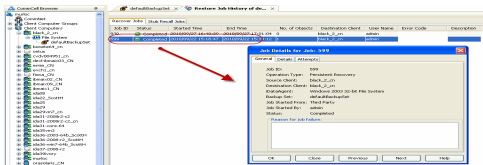
4. The stub gets replaced by the file in the location.

BROWSE AND RESTORE FROM COMMCELL CONSOLE

Use the following method to restore deleted files. Deleted stubs that are not yet aged, can also be recovered by performing a Browse and Restore.

1.
- From the CommCell Console, navigate to **<Client>** | **File System**
- Right-click the backup set that contains the data you want to restore and click **All Tasks** | **Browse Backup Data**
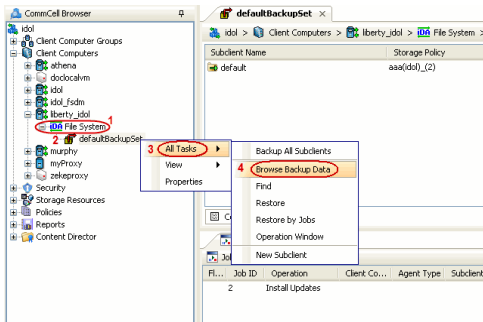
2. Click **OK**.

3.
- Select the folder level under the backup set. Its entire contents will be automatically selected in the right pane.
- Click **Recover All Selected**.

4. Click **OK**.

If you wish to restore the backed up data which may be stubbed, select **Restore data instead of stub**.

5. You can monitor the progress of the restore job in the **Job Controller** or **Event Viewer** window of the CommCell Console.

6.
- Once job is complete, view the details of job from the **Restore History**.
- Right-click the **BackupSet** and select **View | Restore History**.
- Click **OK**.
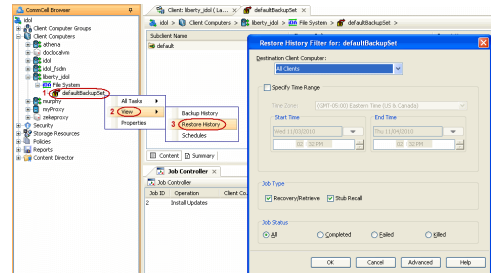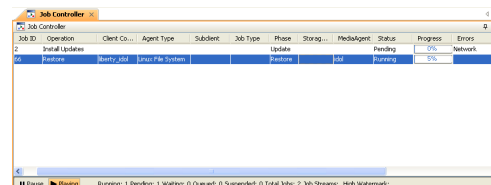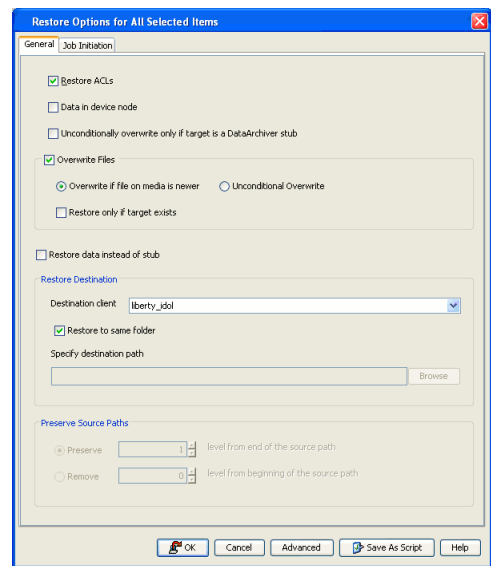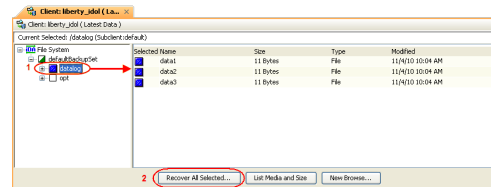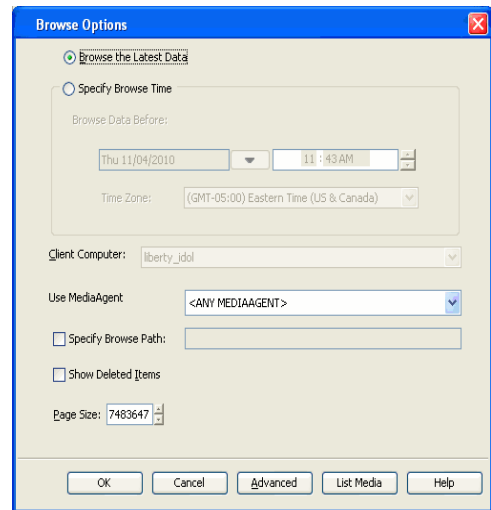
7.   Right-click the job and select **View Job Details**.
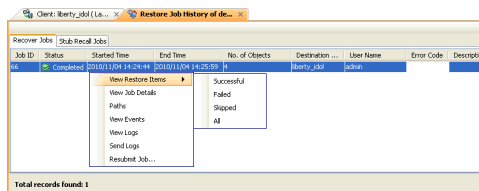
CONGRATULATIONS - YOU HAVE SUCCESSFULLY COMPLETED YOUR FIRST ARCHIVE AND STUB RECOVERY.

If you want to further explore this feature read the **Advanced Options** section of this documentation.
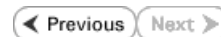
Advanced Configuration - OnePass Agent for Windows File System

TABLE OF CONTENTS

User Defined Subclient

Archiving Rules
  File System Size
  File Access Time
  File Modified Time
  File Size
  Based on File Attribute

Configuring Stub Rules

Pruning Archived Data for Space Reclamation
  Example 1
  Example 2

Configuring Filters
  Filtering Files from Archiving
  Configuring Exclusion to Filters

Configuring Stub Recalls on PolyServe File Systems
  Setting up the Backupset
  Setting up the Subclient
  Configuring Stub Recalls

USER DEFINED SUBCLIENT

The default subclient has the root directory as the subclient content. Therefore a backup and the archive job run on the default subclient results in backing up the entire root directory. In order to run a backup and archive of selective data files, a user defined subclient with specific content can be created.

Follow the steps given below create a user defined subclient:

1.
- From the CommCell Browser, navigate to **<Client> | File System | Default Backup Set**.
- Right-click **Default Backup Set | All Tasks**
- Click **New Subclient**.
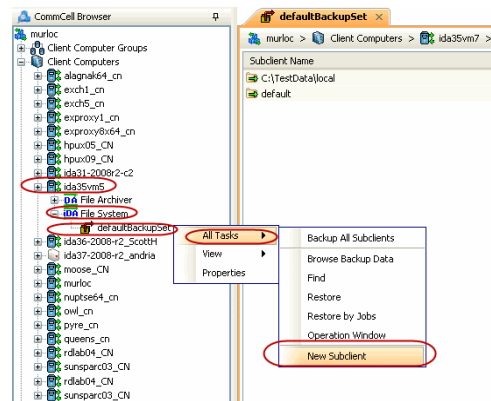
2. Enter **Subclient Name**.
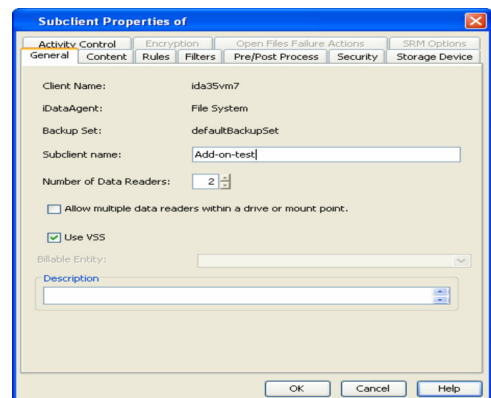
3.
- Click the **Content** tab.
- **Browse** to the folder that has files to be backed up.

- Select the folder and click **Add.**
- Click **Close**.
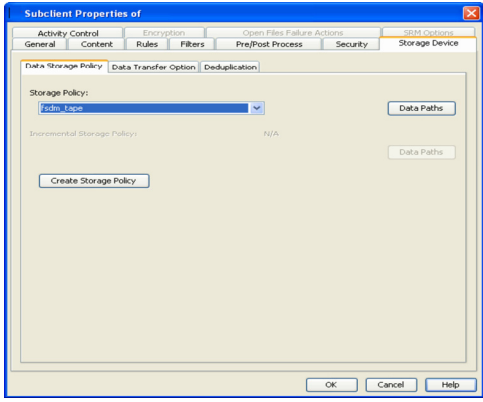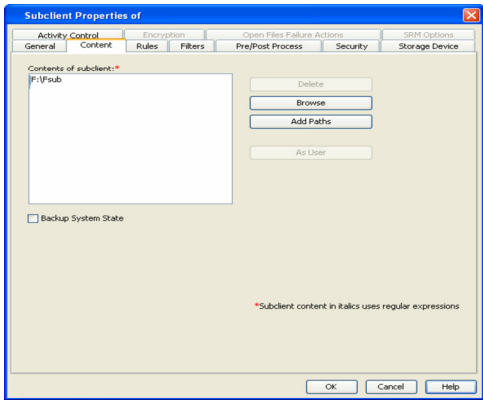
4.
- Click the **Storage Device** tab.
- Select the **Storage Policy** from the drop down list.
- Click **OK**.

ARCHIVING RULES

Archiving rules specify the criteria for the type of data to be archived. You can configure these rules on a requirement basis.

FILE SYSTEM SIZE

The backed up files can be stubbed based on the available free space on the volume. During a backup job if the free space on the volume is less than this value, files matching the remaining rules will become candidates for stubbing.

1. From the CommCell Console, navigate to **Client Computers** | **File System**.
2. Right-click the **Subclient** and click **Properties**
3. Select **Rules** tab.
4. Enter the low watermark value for the volume in **Begin scan for file selection when free volume is less than n%**.
5. Enter the high watermark value for the volume in **End scan if volume is freed to n%**.
6. Click **OK**.
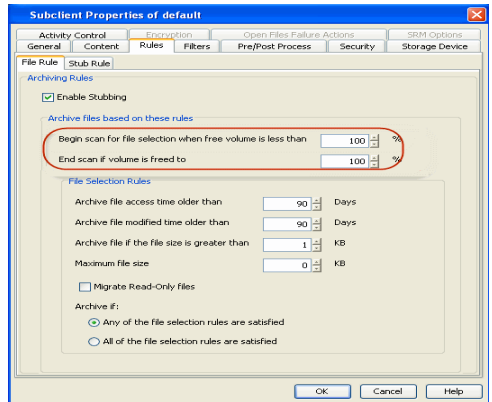
FILE ACCESS TIME

This configuration will stub files based on the last accessed date of each file within the volume or folder/directory. In case it is older than the number of days specified, the files will get stubbed.

1. From the CommCell Console, navigate to **Client Computers** | **File System**.
2. Right-click the **Subclient** and click **Properties**.
3. Select **Rules** tab.

4. Enter the number of days elapsed since the file was last accessed **Archive file access time older than *n* Days**.

5. Select **Any one of the file selection rules are satisfied**.

6. Click **OK**.
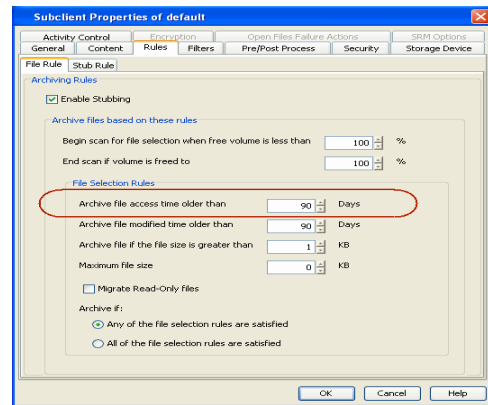
FILE ACCESS TIME FOR WINDOWS VISTA AND WINDOWS SERVER 2008

For Windows Vista, Windows Server 2008 and newer versions of Windows operating system, by default the access time is not updated for any files and folders. If you want to archive files based on access time, perform the following:

1. Enable the operating system to update last access time for all files and folders. For more information, refer to http://technet.microsoft.com/en-us/library/cc758569(v=ws.10).

2. Right-click the **Subclient** and click **Properties**.

3. Click the **Advanced Options** tab.

   Select **Recursive Scan** option and select the **Preserve File Access Time** check box.

   Or, if you want to use other scan types, make sure that the **Use VSS** check box has been selected in the **General** tab.

4. Select **Rules** tab.

5. Enter the number of days elapsed since the file was last accessed **Archive file access time older than *n* Days**.

6. Select **Any one of the file selection rules are satisfied**.

7. Click **OK**.

FILE MODIFIED TIME

This configuration will stub files based on the last modified date of each file within the volume or folder/directory.

1. From the CommCell Console, navigate to **Client Computers | File System**.

2. Right-click the **Subclient** and click **Properties**.

3. Select **Rules** tab.

4. Enter the number of days elapsed since the file was last modified **Archive file modified time older than *n* Days**.

5. Select **Any one of the file selection rules are satisfied**.

6. Click **OK**.
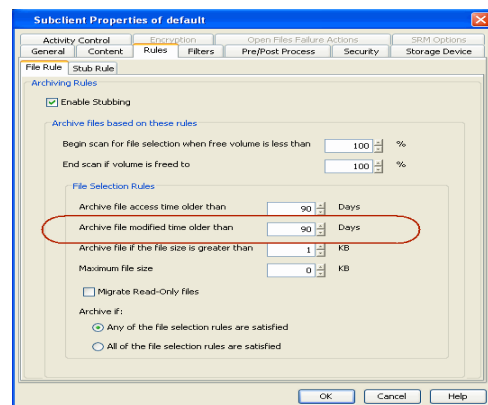
FILE SIZE

This configuration will stub files based on the file size. If a file size within a scanned volume or folder/directory is in between the two limit values set, it will get stubbed. Follow the steps given below to stub files based on their size:

1. From the CommCell Console, navigate to **Client Computers | File System**.

2. Right-click the **Subclient** and click **Properties**.

3. Select **Rules** tab.

4. Enter the minimum file size in **Archive file if size is greater than *n* KB**.

5. Enter the maximum file size in **Maximum file size**.

   These options can be used individually or in combination to specify a range.

6. Select **All of the file selection rules are satisfied**.

7. Click **OK**.

For Example:

To archive files more than 5KB but less than 20KB:

● Enter 5 KB in **Archive file if size is greater than *n* KB**.
● Enter 20 KB in **Maximum file size**.
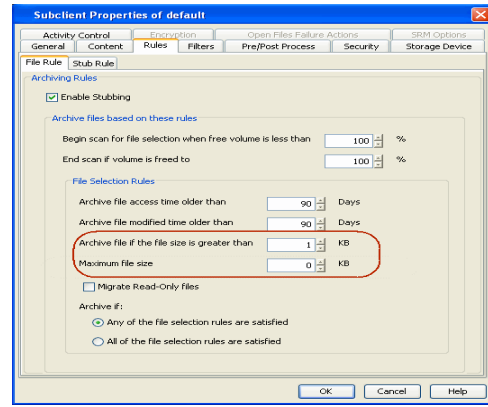
BASED ON FILE ATTRIBUTE

You can also archive the files that have the Read Only attribute set on them.

1. From the CommCell Console, navigate to **Client Computers | File System**.

2. In the right pane right-click the **Subclient** and click **Properties**.

3. Select the **Rules** tab.

4. Select **Enable all Rules**.

5. Select **Migrate Read-Only Files**.

6. Select **Any one of the file selection rules are satisfied**.

7. Click **OK**.
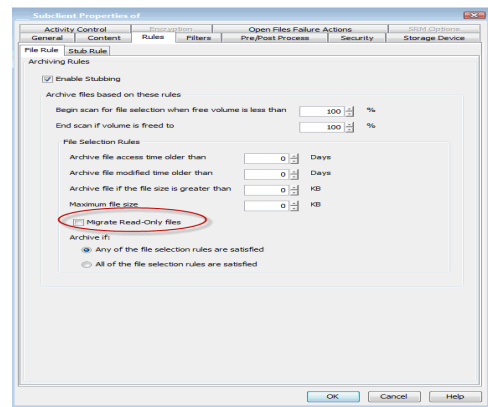
CONFIGURING STUB RULES

By default, the stubs are deleted 730 days from the day of stubbing when you enable the **Prune archived items** option. However, you can set the number of days after which the stubs will be pruned using the following steps:

1. From the CommCell Console, navigate to **Client Computers | File System**.

2. In the right pane right-click the **Subclient** and click **Properties**.

3. Click the **Rules** tab.

4. Select the **Stub Rule** tab and make sure that the **Prune archived items** checkbox is enabled.

5. You can enter the number of days after which the stubs will be pruned.

6. Click **OK**.
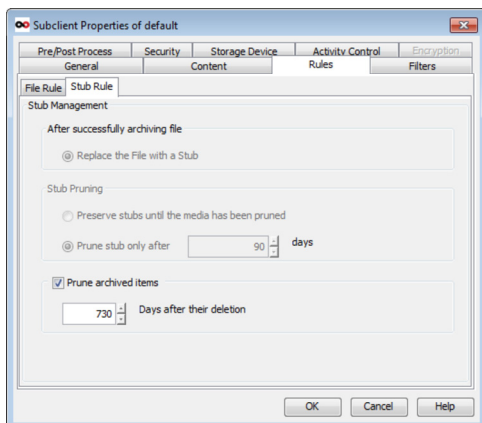
PRUNING ARCHIVED DATA FOR SPACE RECLAMATION

Archived data is pruned and secondary storage space is reclaimed based on the stub retention setting and the storage policy cycle - based retention criteria. . Running a synthetic full backup can reduce space on the secondary storage for deleted stubs that meet the expiration criteria. Running data-aging can reclaim space on the secondary storage by pruning the expired backup jobs. The following sections describe two scenarios for space reclamation:

EXAMPLE 1

By default stub retention is set to 730 days from the Stub Rules tab and the Storage Policy retention is set for 2 cycles and 15 days. The following procedure demonstrates the reduction in the secondary storage usage using stub retention rules:

1.
- Run a few backup jobs. This will lead to stub generation of the data meeting the defined archiving rules. The subsequent incremental backup will backup these stubs.
- Delete a few stubs.
- Perform an incremental backup operation. The time-interval between this incremental backup and the subsequent synthetic full will be calculated as the number of days specified in the retention criteria. The deleted stubs meeting the retention criteria will get expired. For example, if a user has set 20 days for pruning archived items, the deleted stubs will expire after 20 days of initiating this incremental backup.
- Run synthetic full backup with **Check for Deleted Stub** option selected in the advanced tab. The expired stubs and the corresponding data would not get backed up in this operation.
- From the backup job history, verify the backup file list. Ensure that the deleted stubs and their corresponding data are no longer included in the synthetic full backup image.
- Note that space on secondary storage has been freed up by pruning of expired stubs and their corresponding data by running a synthetic full backup.

2. The following procedure demonstrates the reclamation of secondary storage space:
- Run backup jobs to generate 2 backup cycles.
- Wait for the last job of the first cycle to expire (based on the Storage Policy retention, which is 15 days by default).
- Run a Synthetic full backup. This is considered as a third backup cycle and therefore the stubs that meet the retention criteria in the first backup cycle will get pruned.
- Running the synthetic full job will start the third backup cycle and will render the first cycle prune-able.
- Run a data aging job. Notice that the secondary storage space occupied by the first backup cycle has been reclaimed as the stubs have been pruned freeing up space.
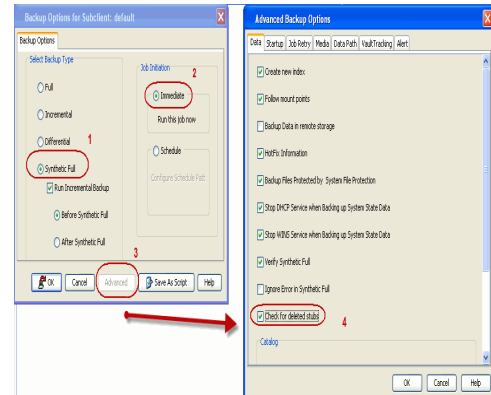
EXAMPLE 2

In order to reclaim space on secondary storage by completely pruning the backup cycles use the following steps:

Pre-requisites

- Stub retention has been set to n days from Subclient properties Stub Rule tab.
- Storage Policy retention has been set to x cycles and y days.
- A few backup cycles have been completed.

1. Change the stub retention to a minimum of 1 day from Subclient properties **Stub Rule** tab..
2. Change the storage policy retention setting to 2 cycles and 15 days.
3. Delete the unwanted stubs.
4. Perform incremental backups twice to generate two backup cycles.
5. Wait for the deleted stubs pertaining to last backup job in the first backup cycle to expire.
6. Run synthetic full backup with **Check for Deleted Stub** option selected in the advanced tab.

   Note that the synthetic full backup will be considered as the third backup cycle and it will render the stubs in the first cycle prunable.
7. Running the synthetic full backup will start a new backup cycle. Due to the change in storage policy retention all the previous backup have expired.
8. Run a data aging job. All jobs from the first backup cycle will be pruned.

   Note that space on secondary storage has been freed up as all the unwanted stubs and their corresponding data have been pruned.

CONFIGURING FILTERS

Prior to archiving the files, you can set filters to prevent specific type of files from being archived. Filters can also be used to exclude certain system-related files and database application files which consistently fail during a archive operation and are not integral to the operation of the system or application.

FILTERING FILES FROM ARCHIVING

You can manually set filters on selected file types, folders or files to be excluded from archiving. For example if you specify *.txt in the filters then all the text files will be excluded from being archived.

1. From the CommCell Console, navigate to **Client Computers** | **File System**.

2. In the right pane right-click the **Subclient** and click **Properties**.

3. Click the **Filters** tab.

4. Click **Add** from the **Exclude these files/folders/patterns** group.

5. Enter the complete path of the file, folder, or directory that you want to exclude from the archiving operations

   or

   Click the **Browse** and expand the file system of the client computer. Click the file, folder, or directory that you want to exclude from the archiving operations and then click **Add**.

6. Click **OK** to save your changes.
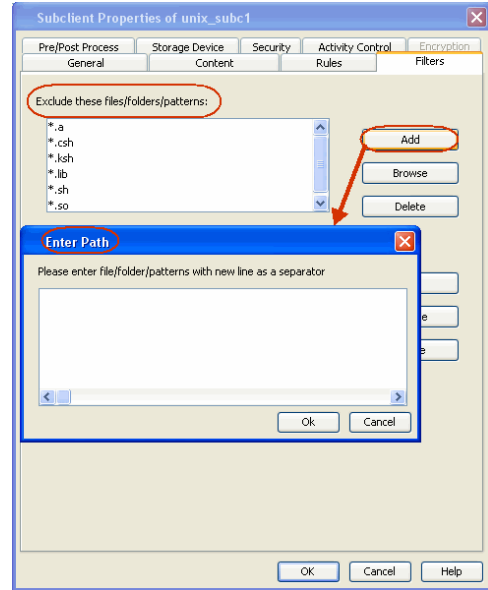
CONFIGURING EXCLUSION TO FILTERS

When excluding files from archiving, you can also provide exceptions to the data that you are excluding. For example, if you want to exclude all the files in the `My Documents` folder except the `Downloads` sub-folder, you can add a subclient filter to exclude the `My Documents` directory from being archived and also add a corresponding subclient filter to allow the `Downloads` sub-folder to be archived.

1. From the CommCell Console, navigate to **Client Computers** | **File System**.

2. In the right pane right-click the **Subclient** and click **Properties**.

3. Click the **Filters** tab.

4. Click **Add** from the **Include these files/folder/patters:** group.

5. Enter the complete path of the file, folder, or directory that you want to be included in the archiving operation.

   or

   Click the **Browse** and expand the file system of the client computer. Click the file, folder, or directory that you want to be included in the archiving operation. and then click **Add**.

6. Click **OK**.
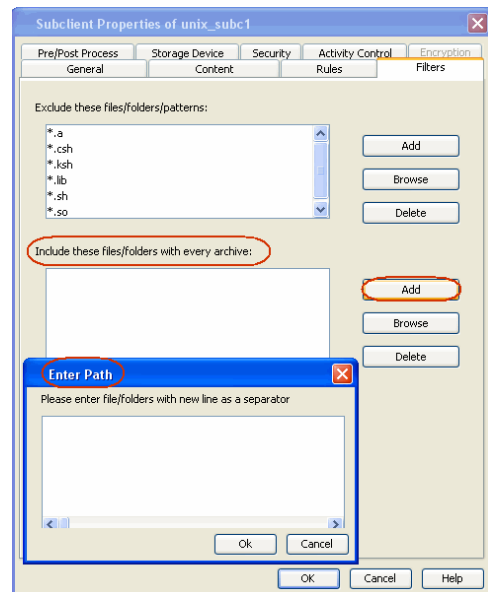
CONFIGURING STUB RECALLS ON POLYSERVE FILE SYSTEMS

Use the following steps to recall stubs from the PolyServe cluster:

1. Make sure that the OnePass Agent is installed on the physical nodes of Polyserve cluster.

2. Make sure that the **Use Classic File Scan** option is enabled in the backupset as described in Setting up the Backupset.

3. Make sure that the **Use VSS** option is not selected from the subclient used to perform the PolyServe cluster backup as described in Setting up the Subclient.

4. To perform stub recall, add the EnableThirdPartyFS registry key on the physical nodes of PolyServe cluster as described in Configuring Stub Recalls.

SETTING UP THE BACKUPSET

1. From the CommCell Console, navigate to **Client** | **File System** | **defaultBackupSet**.

2. Right click *<BackupSet>* and make sure that the **Use Classic File Scan** option is selected.

3. Click **OK**.
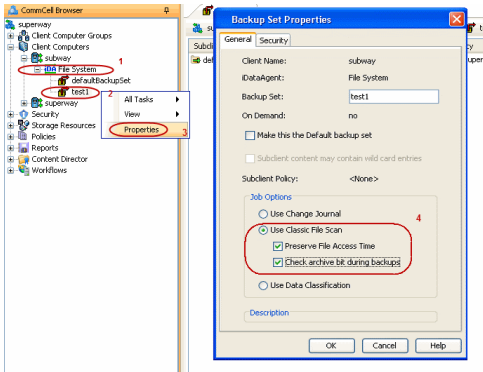
SETTING UP THE SUBCLIENT

1. Right-click the subclient used to perform backup and point to **Properties**.

2. Make sure that the **Use VSS** option is cleared.

3. Click **OK**.
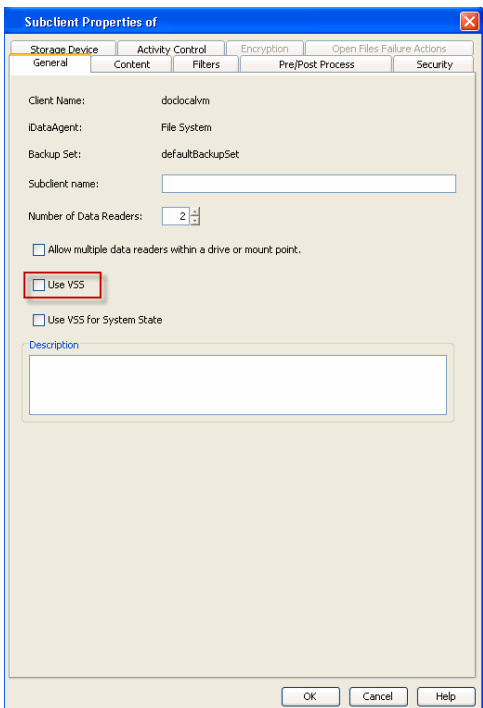
CONFIGURING STUB RECALLS FOR POLYSERVE CLUSTER

In order to recall the stubs that reside on the PolyServe File System, you need to add the EnableThirdPartyFS registry key on the physical nodes Use the following steps to enable the registry key:

1. Click **Start**, click **Run**, type **regedit**, and then click **OK**.

2. Navigate to the following directory:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\cvmhsm\Parameters`

3. Right click the `Parameters` and select **New -> DWORD** value, name it as `EnableThirdPartyFS`.

4. Double-click the `EnableThirdPartyFS` key and modify the **Value data** to 1 to enable the recall of stubs on a PolyServe File System**.**

5. Click **OK**.

6. Restart the machine for the changes to get applied.

Back to Top

Advanced Data Movement - OnePass Agent for Windows File System

TABLE OF CONTENTS

Scheduling an Archive Job

Check for Deleted/Moved Stubs

Long Term Data Retention

SCHEDULING AN ARCHIVE JOB

1.
   - From the CommCell Console, navigate to **Client Computers** | **File System | Backupset**
   - Right-click the **Subclient** in the left pane and click **Backup**.

     The OnePass agent does not support Differential backup and a selection of Differential backup will lead to job failure.

2.
   - Click **Schedule** to schedule the backup job for a specific time.
   - Click Configure to set the schedule for the backup job. The Schedule Details dialog displays.
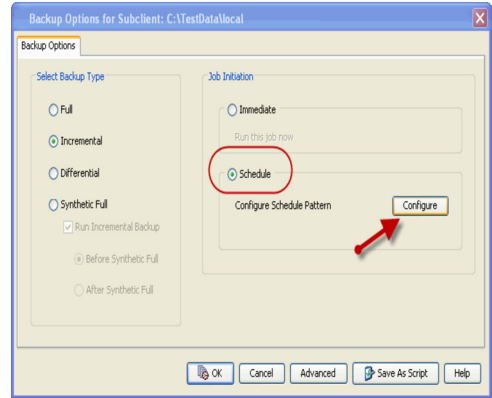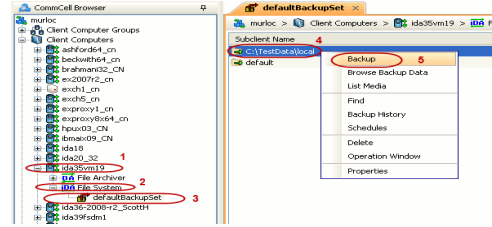
3. Select the appropriate scheduling options. For example:
   - Click **Weekly**.
   - Check the days you want the run the archive job.
   - Change the Start Time to 9:00 PM
   - Click **OK** to close the Schedule Details dialog
   - Click **OK** to close the Backup Options dialog

   The backup job will execute as per the schedule.
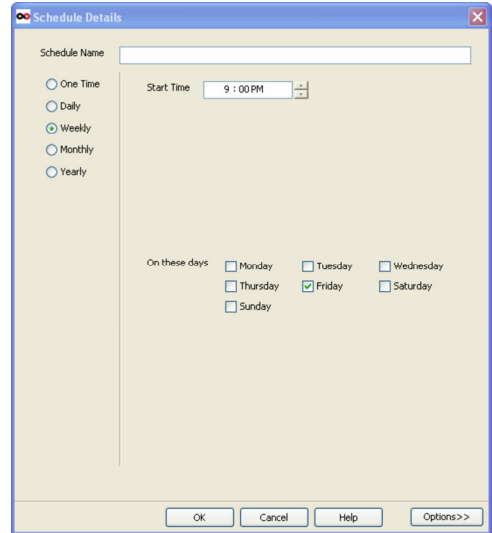
CHECK FOR DELETED/MOVED STUBS

You can run a check for deleted or moved stubs on your client computer. The client computer is scanned for moved/deleted stubs during a synthetic full backup if the **Check for deleted stubs** option is selected in the advanced tab.

We recommend you to enable this option only when the stubs are moved from one location to another. Enabling this option makes synthetic full

backups slower.

Follow the steps given below to run this scan:

1. From the CommCell Console, navigate to **Client Computers** | **File System**.

2. Right-click the **Subclient** and click **Backup**.

3. From the **Backup Options** dialog box, select **Synthetic Full** as the backup type and **Immediately** as the **Job Initiation** option.

4. Click **Advanced**.

5. Select **Check for deleted stubs**.

6. Click **OK**.

7. You can track the progress of the backup job from the **Job Controller** window.
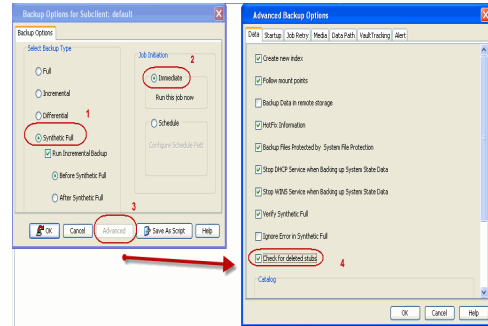
LONG TERM DATA RETENTION

Once the backed up data has been archived it can be transferred and retained for long term on cost effective media also by using the following:

CLOUD STORAGE

- Cloud Storage enables you to configure and use online storage devices — cloud storage devices — as storage targets.

- It reduces the need to maintain hardware resources such as tape or disk storage devices at onsite locations.

- It also provides the ability to easily increase your storage capacity as and when it is required.

- It also provides centralized data access, better failover capabilities and reduces the day-to-day storage administration tasks.

For more details, see Cloud Storage.

AUXILIARY COPY

- An auxiliary copy operation allows you to create secondary copies of data associated with data protection operations, independent of the original copy.

- The auxiliary copy operation can be useful for creating additional standby copies of data.

- The primary and secondary copies use different media and often use different libraries, depending on the configuration.

- In case the primary copy become inoperative, you can promote a synchronous copy to become the primary copy. This allows you to continue data protection and data recovery operations without interruptions.

For details, see Auxiliary Copy.

Advanced Recover Data - OnePass Agent for Windows File System

ACCESSING STUBS WITHOUT TRIGGERING A RECALL

COPYING STUBS

When stubs are copied across drives or on mount points on the same drive it may trigger a stub recall. To copy stubs from one location to another without triggering a recall, follow the steps given below:

1. Access the command prompt on the computer, where File System *i*DataAgent is installed.

2. Navigate to the <Windows File System *i*DataAgent>\Base> folder

3. Run the GXHSMUtility utility.

    Usage: `GXHSMUtility [-stubonly] <file_src> <file_dest>`

MOVING STUBS

When stubs are moved across drives it may trigger a stub recall. To move stubs from one location to another without triggering a recall, follow the steps given below:

1. Access the command prompt on the computer, where File System *i*DataAgent is installed.

2. Navigate to the <Windows File System *i*DataAgent>\Base> folder

3. Run the GXHSMUtility utility.

    Usage: `GXHSMUtility [-m] <file_src> <file_dest>`

SCHEDULING A RESTORE

1.
  - From the CommCell Console, navigate to **Client Computers** | **File System**.
  - Right-click the backup set and click **All Tasks** | **Browse**.
  - Click **OK**.

2.
  - Select data to restore.
  - Click **Recover All Selected**.
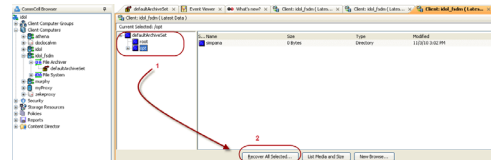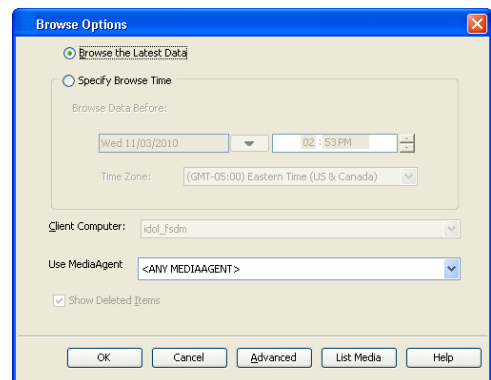
3.
- Click **Job Initiation** tab and click **Schedule**.
- Click **Configure**.
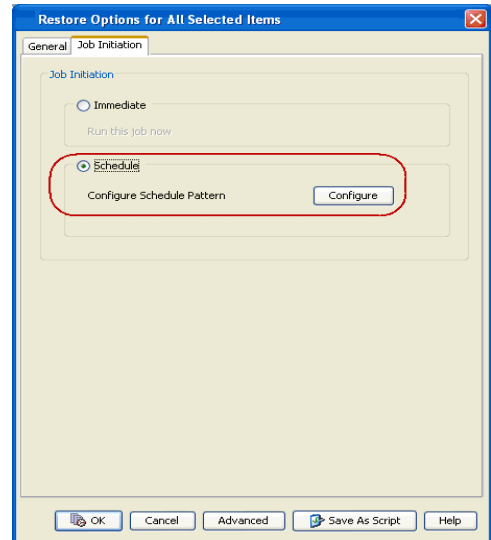
4. Select the appropriate scheduling options. For example:
- Click **Weekly**.
- Check the days you want the run the restore job.
- Change the Start Time to 9:00 PM
- Click **OK** to close the Schedule Details dialog
- Click **OK** to close the Restore Options dialog

The restore job will execute as per the schedule.
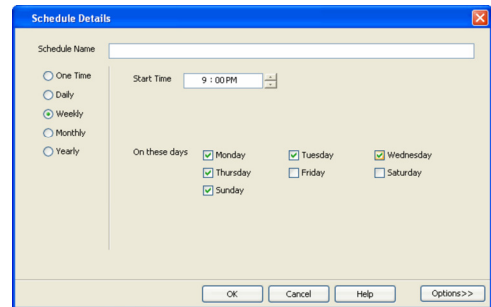
RESTORE DESTINATIONS

By default, the OnePass Agent restores data to the client computer from which it originated; this is referred to as an in-place restore. You can also restore the data to another client computer in the CommCell. The following section enumerates the types of restore destinations that are supported by the OnePass Agent.

IN-PLACE RESTORE

When restoring data, the OnePass Agent provides the facility to restore the data to the same path/destination on the client computer from which the data originated; this is referred to as an in-place restore.

1. From the CommCell Console, perform a **Browse and Restore** operation.

2. When browsing the data, select data that was initially backed up and click **Recover All Selected**.

3. Click **OK**.

4. Select the **Destination Client** that was the original computer from which the data originated.

5. Depending on the data selected to restore, choose one of more of the options (e.g., **Restore ACLs**).

6. Click **OK**.

OUT-OF-PLACE RESTORE

All restore levels provide the facility to restore data to a different directory on the client computer from which the data originated; this is referred to as an out-of-place restore to a different path/destination. You can also restore data to a different client computer in the CommCell using the same path/destination.

> When you perform an out-of-place restore, the restored data assumes the rights (i.e., permissions) of the parent directory.

1. From the CommCell Console, perform a **Browse and Restore** operation.

2. When browsing the data, select data that was initially backed up and click **Recover All Selected**.

3. Click **OK**.

4. Select the **Destination Client** that is a different computer from which the data originated.

5. Depending on the data selected to restore, choose one of more of the options (e.g., **Restore ACLs**).

6. Click **OK**.

RESTORE BY JOBS

The Restore By Jobs feature provides the facility to select a specific backup job to be restored. This method of restoring data is considerably faster as it reads continuously on the tape and retrieves the data and does not depend on the indexing subsystem to get the seek offsets on the media.

This feature can be used to restore point-in-time data associated with a specific backup job, such as full, incremental, differential, etc.

Consider the following when restoring by jobs:

- Run a restore by jobs whenever you want to restore the entire contents of the job.
- Avoid running restores by jobs for jobs associated with the default subclient. If you do this, the entire contents of the machine will be restored. As such, this may cause problems (e.g., the machine might run out of space) or produce undesirable results (e.g., you might end up restoring operating system files or directories that you really do not want to restore).
- Avoid modifying the contents of any associated subclients since this may result in the retrieval of older data.

Use the following steps to restore data by jobs.

1. From the CommCell Browser, right-click the level whose data you want to browse, click **View** and then click the **Backup History**.

2. From the **Backup History Filter** window, select the filter options, if any, that you want to apply and click **OK**.
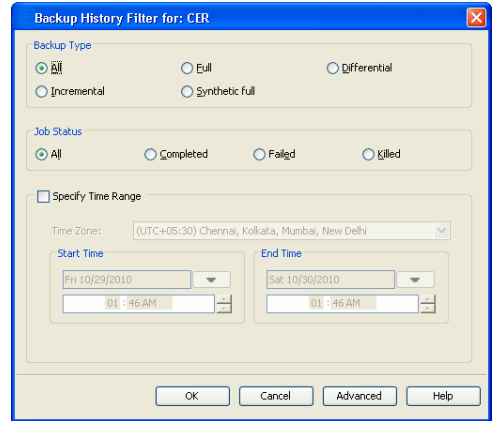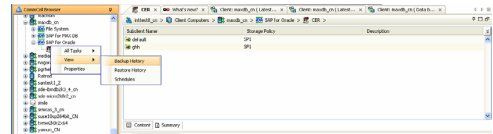
3. From the Backup Job History window, right-click the backup job that need to be restored and select **Browse**.

4. From the **Browse Options** dialog box, click **OK** to execute the browse using the **Browse the Latest Data** option.

5. From the **Browse** window, select the instance node in the left pane and then select the required data and logs in the right pane, and click the **Recover All Selected** button at the bottom of the window.

6. Select the desired restore options and click **OK**.
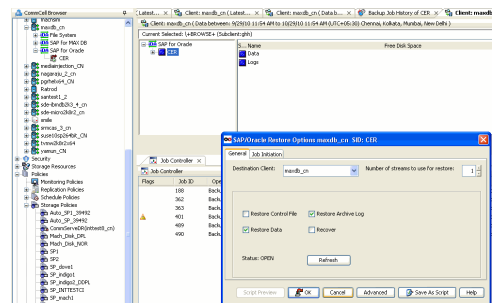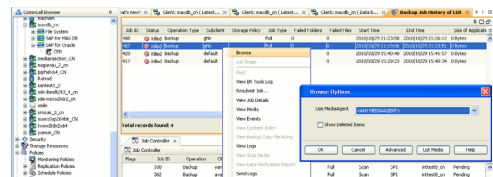
LISTING MEDIA

List media option is useful to predict media required for the following operations:

- To restore data associated with a specific backup set, subclient or instance
- To restore the index required to browse data associated with a specific backup set or subclient
- To restore a specific file (or specific files and folders)
- To restore data associated with a specific job

The list media operation can be performed for instances, backup sets, and subclients. The following sections describe each of these methods.

The List Media feature can also be used in a number of other capacities. Refer to the List Media documentation for a complete overview of this feature.

LISTING MEDIA FOR A SUBCLIENT

1. From the CommCell Browser, right-click the subclient for which you wish to list media and then click **List Media**.
2. From the **List Media** dialog box choose one of the following options:
   o Click **Media For the Latest Data** to list media associated with the most recent data protection cycle.
   o Click **Specify Time Range** to list media associated with data protection operations up to the specified date and time range.

   Use the **Data Before** box to specify the end date and time.

   o Click **Advanced** and then click **Exclude Data Before** to list media associated with data protection operations after the specified date and time.

   Note that you can use the **Specify Browse Time** and **Exclude Data Before** options to list media between a specified date and time range.
3. Click **OK**.

   The appropriate media is listed in the **Media** dialog box.

LISTING MEDIA FOR A BACKUP SET

1. From the CommCell Browser, right-click the backup set for which you wish to list media, click **All Tasks** and then click **Browse**.
2. From the **Browse Options** dialog box, if required, select the following options:
   o Click **Browse the Latest Data** to list media associated with the most recent data protection cycle.
   o Click **Specify Browse Time** to list media associated with data protection operations up to the specified date and time range.

   Use the **Browse Data Before** box to specify the end date and time.

   o Click **Advanced** and then click **Exclude Data Before** and then select the date and time from which you wish to list media associated with data protection operations.

   Note that you can use the **Specify Browse Time** and **Exclude Data Before** options to list media between a specified date and time range.
3. Click **List Media**.
4. From the **List Media** dialog box, click **List Media for restore within specified time range** and click **OK**.

   The appropriate media is listed in the **Media** dialog box.

RECALLING STUBS FROM POLYSERVE CLUSTER

In order to recall the stubs that reside on the PolyServe File System, you need to add the EnableThirdPartyFS registry key on the physical nodes Use the following steps to enable the registry key:

1. Click **Start**, click **Run**, type **regedit**, and then click **OK**.
2. Navigate to the following directory:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\cvmhsm\Parameters`
3. Right click the `Parameters` and select **New -> DWORD** value, name it as `EnableThirdPartyFS`.
4. Double-click the `EnableThirdPartyFS` key and modify the **Value data** to 1 to enable the recall of stubs on a PolyServe File System**.**
5. Click **OK**.
6. Restart the machine for the changes to get applied.

Troubleshooting - OnePass Agent for Windows File System

The following section provides information on some of the troubleshooting scenarios

BACKUP OF SUBCLIENTS USING ONEPASS AGENT WILL FAIL IF THE STORAGE POLICY IT WAS USING BEFORE RUNNING A NEW SYNTHETIC FULL BACKUP IS DELETED.

By default the OnePass Agent uses a synthetic full forever incremental design. If you want to change the storage policy being used, you should re-assign the policy, run a new synthetic full (this will get the data from the older policy). The older storage policy should only be deleted after running the new synthetic full.

If the older storage policy is accidentally deleted before running a synthetic full backup, follow the steps given below to allow for new backups to run:

1. Create a new backup set.

2. Configure subclient with the same content path as that of the old subclient.

3. Associate the new subclient to the new storage policy.

4. Run a backup.

    The first backup will be full, but all subsequent backups will be incremental.

ARCHIVE JOB MAY FREEZE

PROBLEM CAUSE

Archive job may freeze during the scan phase. For the frozen job to continue and complete successfully, restart GXHSMService.exe.

SOLUTION

If you are using Symantec Endpoint Protection 12, we recommend you to upgrade your version to 12.1.2 (RU2 MP1) (12.1.2100.2093) to resolve this issue.

INCREMENTAL BACKUPS GOING TO A PENDING STATE WITH THE "NO ARCHIVE DATA" ERROR MESSAGE

This message will be displayed if the full backup associated with the subclient is deleted.

It is recommended to create a new subclient, assign the same content and run full and incremental backups.

SYNTHETIC FULL BACKUPS FAILING WITH "NO INCREMENTAL JOB RAN" ERROR MESSAGE

This message will be displayed if you run a synthetic full backup after deleting the most recent synthetic full with no 'new' incremental backups in-between.

Re-run the synthetic full backup and the error will message will not be displayed again.

RECALL FAILS WITH ACCESS DENIED ERROR

PROBLEM CAUSE

When you double click a stub to perform a recall, the recall operation fails with the message **Access Denied**. You will receive an error in the CommCell Console which says **Recall abort due to exported media. Afile-Data=[*number*].**

This happens because the Archiver Services perform a pre-check to see if the required media is available in the library.

SOLUTION

Import the required media into the library. We recommend you to have a latest backup cycle available always so that the stubs can be recalled from that cycle. Backup operations performed on disk libraries enable faster recalls as they are not bound by the read and seek rules binding to the tape drives.

FILE RECALLS FROM SERVER MESSAGE BLOCK(SMB) PROTOCOL CAUSE SERVER TO LOCK UP

SYMPTOM

The following error occurs in **CVD.log** on the server that hosts the file archive share:

```
[CVD ] slSendMsg: send() failed. socket=10612 SndSize = 8192 Error = [1][10054][An existing connection was forcibly closed
by the remote host.]
```

```
[NET_WRITER ] Critical Network Error:: rc = 10054 ABORTING pipeline
```

CAUSE

When you perform a file recall on a computer that uses Vista, Windows 7, Windows 2008, or Windows 2008 R2 operating system, the server might lock up. This issue occurs because the Server Message Block (SMB) worker thread that handles SMB 2.x requests is not available. Therefore, the SMB worker thread does not respond to file share requests.

When two computers communicate with each other through the SMB protocol, the connection is controlled by the highest version of the SMB that is supported by both of the operating systems on the two computers. The recall process works correctly if the computer where the file share is hosted and the computer where the recall process is triggered have Windows 2003, 2003 R2, or XP operating system. These computers recall the file correctly because they use SMB 1.0.

PREREQUISITES

- CommServe and MediaAgent must be at the same or higher service pack level than the client servers in the CommCell.
- While updating Service Pack updates make sure that the CommServe computer and MediaAgent are updated prior to client servers.

RESOLUTION

After you install the Microsoft hot fix, make sure that you set the specific registry keys on the servers that perform the file recalls to match their resource allocation to the client computers resource allocation. If you do not set these registry keys, any activity between a server and an SMB 1.0 protocol that uses UNC, CIFS, or NFS automatically uses the lowest setting on the two servers.

ON THE DATA ARCHIVER AGENT COMPUTER

This procedure applies to Data Archiver Agent computers that use SMB 2.x protocol and use Vista or later versions of operating system.

1. Install Microsoft hot fix available in Microsoft KB article 2492806.

   Before you edit the registry, make sure that you follow Microsoft's standards for registry backup, editing and restore operations available in Microsoft KB article 322756.

2. Create **MaxThreadsPerQueue** registry key in the following location to override the operating system defaults.

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\MaxThreadsPerQueue

   Change the DWORD Decimal Value to 1024.

3. Create **MaxMpxCt** registry key in the following location to override the operating system defaults.

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\MaxMpxCt

   Change the DWORD Decimal Value to 125.

   For more information, refer to Change registry settings to maximize server service performance.

4. Restart the client computer for the settings to take effect.

ON THE WINDOWS CLIENT COMPUTER

This procedure applies to Windows client computers that use SMB 2.x protocol and use Vista or later versions of operating system.

1. Install Microsoft hot fix available in Microsoft KB article 2492806.

   Before you edit the registry, make sure that you follow Microsoft's standards for registry backup, editing and restore operations available in Microsoft KB article 322756.

2. Create **FileInfoCacheEntriesMax** registry key in the following location to override the operating system defaults.

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanWorkstation\Parameters\FileInfoCacheEntriesMax

   Change the DWORD Decimal Value to 1024.

3. Create **MaxCmds** registry key in the following location to override the operating system defaults.

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\MaxCmds

   Change the DWORD Decimal Value to 125. For more information, refer to Change registry settings to maximize server service performance.

4. Restart the client computer for the settings to take effect.

ON THE DATA ARCHIVER AGENT COMPUTER

This procedure applies to Data Archiver Agent computers that use SMB 1.0 protocol and operate on Windows Server 2003, 2003 R2, or Windows XP.

1. Create **MaxThreadsPerQueue** registry key in the following location to override the operating system defaults.

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\MaxThreadsPerQueue

Change the DWORD Decimal Value to 1024.

2. Create **MaxWorkItems** registry key in the following location to override the operating system defaults.

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\MaxWorkItems

   Change the DWORD Decimal Value to 500.

3. Create **MaxMpxCt** registry key in the following location to override the operating system defaults.

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\MaxMpxCt

   Change the DWORD Decimal Value to 125.

4. Restart the client computer for the settings to take effect.

ON THE WINDOWS CLIENT COMPUTER

This procedure applies to Windows client computers that use SMB 1.0 protocol and operate on Windows Server 2003, 2003 R2, or Windows XP.

1. Create **MaxCmds** registry key in the following location to override the operating system defaults.

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\MaxCmds

   Change the DWORD Decimal Value to 125. For more information, refer to Change registry settings to maximize server service performance.

2. Restart the client computer for the settings to take effect.

ADDITIONAL INFORMATION

- For more information on SMB protocol on Windows 2008 and 2008 R2, see List of currently available hot fixes for the File Services technologies in Windows Server 2008 and in Windows Server 2008 R2.

- For more information on SMB 2.0 and how to use the performance tuning guidelines to improve the performance Tuning Guidelines to improve the performance of client computers, see

  ○ New Networking Features in Windows Server 2008 and Windows Vista (Locate section Server Message Block 2.0)

  ○ Performance Tuning Guidelines for Windows Server 2008 (SMB 2.0 information starts on Page 47)

  ○ Performance Tuning Guidelines for Windows Server 2008 R2 (SMB 2.1 information starts on Page 56)

  ○ Performance Tuning Guidelines a Windows HPC Cluster for Parallel Applications

- For more information on adjustment of registry keys, see Microsoft KB article 898468.

- For additional information on modifying registry keys, see the following articles:

  ○ Tuning the Servers for UNC Content (IIS 6.0)

  ○ Registry Settings that can be Modified to Improve Operating System Performance

  ○ How to troubleshoot Event ID 2021 and Event ID 2022

- Microsoft has a tool to test SMB performance. For more information on these tools, see FSCT test results detail the performance of Windows Server 2008 R2 File Server configurations and File Server Capacity Tool (FSCT) 1.0 available for download.

- For more information on SMB 3.0, see Updated Links on Windows Server 2012 File Server and SMB 3.0 and Updated Links on Windows Server 2012 R2 File Server and SMB 3.0.

UNABLE TO RECALL ADOBE PDF FILES

SYMPTOM

When file recall is initiated for a PDF file on a DFS volume, the Adobe reader cannot open the file and displays the following error:

```
There was an error opening this document. Access denied.
```

RESOLUTION

This issue occurs because the application opens by default in protected mode, with the introduction of Adobe reader 10.x.x.

To resolve this issue, de-select the **Enable Protected Mode at startup** option in the **Preferences** dialog box.
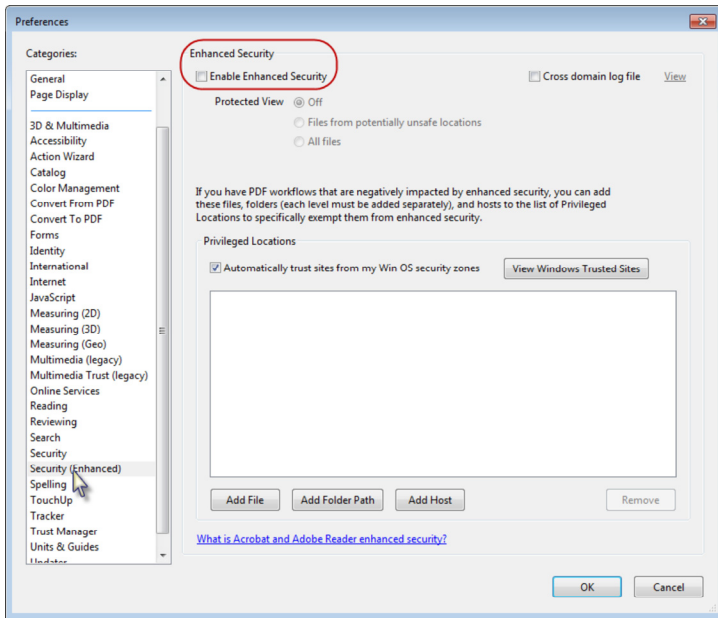
UNABLE TO RECALL ARCHIVED DATA

PROBLEM CAUSE

When you try to perform a recall of a restored stub, the recall operation may fail. This happens when you perform a synthetic full backup with the **Create new index** option not enabled in the **Advanced Backup Options** dialog box.

SOLUTION

Make sure that the **Create new index** option is enabled in the **Advanced Backup options** dialog box before performing a synthetic full backup.
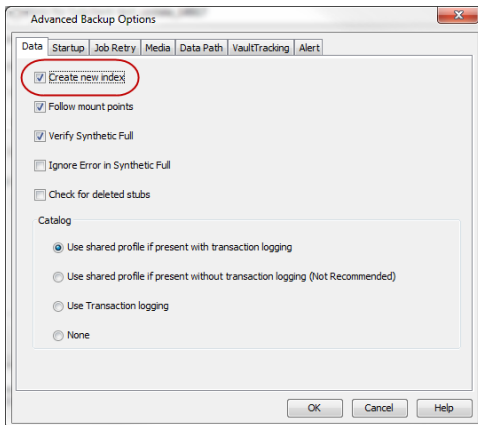
Frequently Asked Questions - OnePass Agent for Windows File System

I AM UNABLE TO SEE THE RULES TAB IN THE SUBCLIENT PROPERTIES DIALOG BOX

Select the **Enable for Archiving** option in the File System Agent properties dialog box, the OnePass mode gets enabled. Now right-click the subclient and select properties. The **Rules** tab will be visible with **File Rule** and **Stub Rule** tabs.

AFTER MY FIRST FULL BACKUP ALL SUBSEQUENT BACKUPS ARE RUNNING ON INCREMENTAL MODE

Once the OnePass mode is enabled, after the first full backup, all subsequent backups will be incremental by default. An incremental backup contains only data that is new or has changed since the last backup.

ONCE THE ONEPASS AGENT IS ENABLED, CAN I RUN FULL BACKUPS EVEN AFTER THE FIRST FULL BACKUP?

No. Once the OnePass Agent mode is enabled, after the first full backup, full backups will be converted into incremental backups followed by a synthetic full in these scenarios.

- Full backup job initiated manually by a user.
- Full backup job scheduled using a Schedule Policy.
- Full backup job scheduled using a Scheduler.

WHY ARE THE DIFFERENTIAL BACKUPS FAILING?

The OnePass agent does not support Differential backup. Therefore a selection of differential backup will result in backup job failure.

HOW DO I RECOVER DELETED STUBS?

Deleted stubs can be recovered using the following methods:

Case 1: If the stubs that were deleted have not yet reached the expiration date set at **Prune archived items** from the **Subclient Properties (Rules)** tab, you can recover the stubs by performing a Browse and Restore operation from the latest synthetic full backup. To restore data, navigate to the location the stubs are restored and perform a stub recovery.

Case 2: If stubs are deleted and aged, but data is still available in the media, you can restore them by performing the method described in Recovering Pruned and Deleted data.

HOW DO I EXTEND MY STUB PRUNING SETTING?

Follow the steps given below to extend and reset your stub pruning setting.

- From the CommCell Console, navigate to **Client Computers** | **File System**.
- Right-click the **Subclient** and click **Properties**.
- Select **Rules|Stub Rule**.
- Select **Prune archived items** to extend the retention days.
- Click **OK**.

HOW DO I RECALL STUBS THAT RESIDE ON THE POLYSERVE FILE SYSTEM?

Use the following steps to recall stubs from the PolyServe cluster:

1. Make sure that the OnePass Agent is installed on the physical nodes of Polyserve cluster.

2. Make sure that the **Use Classic File Scan** option is enabled in the backupset as described in Setting up the Backupset.

3. Make sure that the **Use VSS** option is not selected from the subclient used to perform the PolyServe cluster backup as described in Setting up the Subclient.

4. To perform stub recall, add the EnableThirdPartyFS registry key on the physical nodes of PolyServe cluster as described in Configuring Stub Recalls.

WHY AM I UNABLE TO ARCHIVE DATA?

Your data will get archived only if the **Enable for Archiving** checkbox is selected and your license is available.

- From the CommCell Console, navigate to **Client Computers | File System**.
- Right-click **File System | Properties**.
- Select **Enable for Archiving**, if it is not already selected.

WILL MY SYSTEM FILES GET ARCHIVED IF I BACKUP MY ROOT VOLUME?

No, backing up your root volume will not archive the system files. During backup of your entire client machine, system files are automatically excluded.

HOW DO I ADD THE ONEPASS IF I HAVE WINDOWS FILE SYSTEM *I*DATAAGENT ALREADY INSTALLED?

If the Windows File System *i*DataAgent is already installed, install the Driver for File Archiver. To install the Driver for File Archiver, follow the same steps as with installing the Windows File System iDataAgent with Archiving Enabled. Internally, the system will install only the driver.
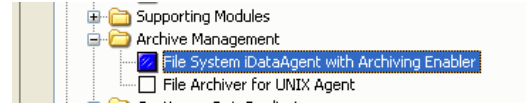
WHY ARE THE RECALLS SLOW?

The recall process may become slow when old data is not aged off. Therefore it is recommended to schedule Synthetic Full backups at regular intervals so that the archived items are aged off based on their retention criteria.

CAN I PERFORM A SYNTHETIC FULL BACKUP WITHOUT CREATING A NEW INDEX?

No. You should not perform a synthetic full backup without creating a new index. By default, the **Create new index** option is enabled in the **Advanced Backup Options (Data)** dialog box.

IS DISTRIBUTED FILE SYSTEM REPLICATION (DFSR) SERVICE COMPATIBLE WITH STUB RECALL?

Distributed File System Replication (DFSR) is not compatible with stub recall. This is due to a Microsoft known issue.

For more information, see Microsoft article DFSR Reparse Point Support.

Contact Microsoft if you still experience issues related to archiving or stub recall.

Desktop Browse - Windows File System (Administrator)

This feature/product/platform is deprecated in this release. See Deprecated Features, Products, and Platforms for more information.

It is recommended to use Laptop Backup to browse file system data.

Install | **Setup**

◀ Previous | Next ▶

Desktop Browse enables users to browse data from an user-friendly Web interface from any remote location. To enable Desktop Browse operations, you need to first install the Web Search Server and the Web Search Client. The Web Search Server and Web Search Client can be installed on the same computer or on different computers.

Ensure you have the following before performing the install:

- Software version or higher.

INSTALLING THE WEB SEARCH SERVER AND WEB SEARCH CLIENT

1. Ensure that the IIS is installed on the CommServe computer before installing the Web Search Server and Web Search Client.

2. Run **Setup.exe** from Software Installation Discs on the **CommServe** computer.

3. Select the required language.
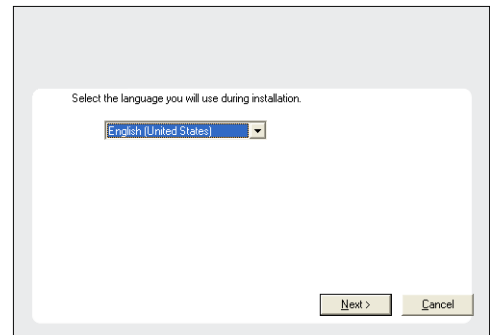
   Click **Next**.

4. Select the option to install software on this computer.

   NOTES

   - The options that appear on this screen depend on the computer in which the software is being installed.
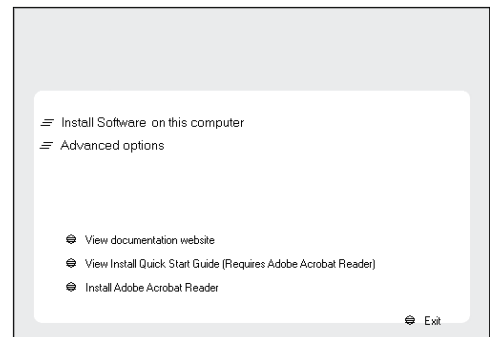
5. Click **Next**.
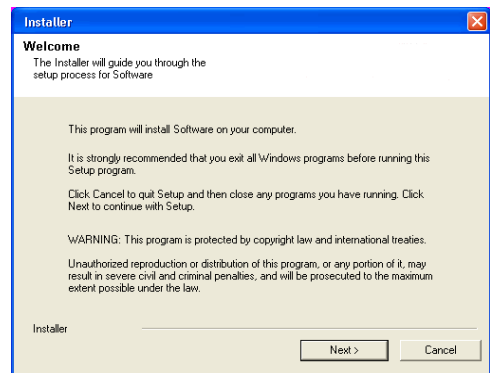
6. Click **OK**.

7. Select **I accept the terms in the license agreement**.

    Click **Next**.

8. Expand **Client Modules** | **Web Search Server & Browse** and select **Web Search Server** and **Web Search Client**.

    Click **Next**.

9. Click **Yes**.

10. Click **Yes**.

11. Specify the SQL Server System Administrator password.

    NOTES

    ● This is the password for the administrator's account created by SQL during the installation.

    Click **Next**.

12. Modify **Apache Tomcat Server port number** to **82**.
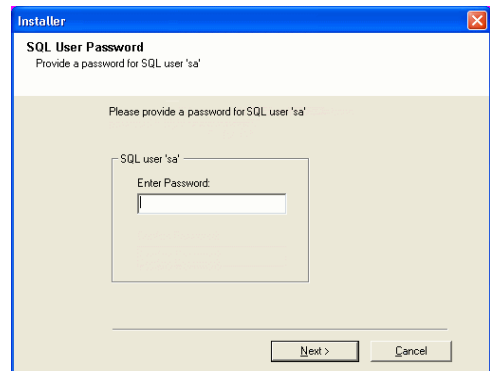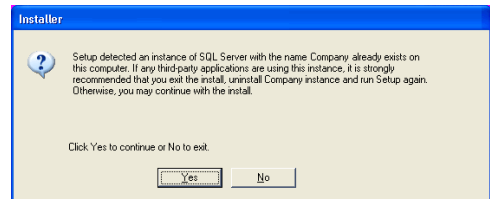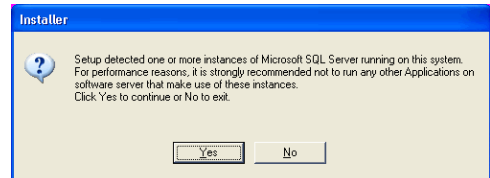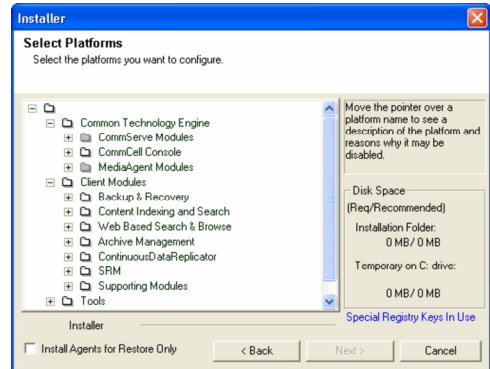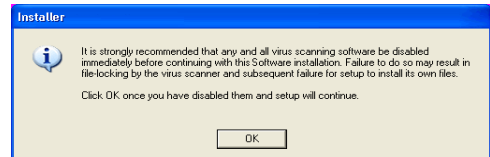
Click **Next**.

NOTES:

- Ensure that these port numbers are different and are not already used by any other services or application.

13. Click **Next**.

14. Select **Add programs to the Windows Firewall Exclusion List**, to add CommCell programs and services to the Windows Firewall Exclusion List.

Click **Next**.

    This option enables CommCell operations across Windows firewall by adding CommCell programs and services to Windows firewall exclusion list.

    It is recommended to select this option even if Windows firewall is disabled. This will allow the CommCell programs and services to function if the Windows firewall is enabled at a later time.

15. Enter the Web Search Server database installation path.

Click **Browse** to modify the default location.

Click **Next**.

16. Click **Next**.
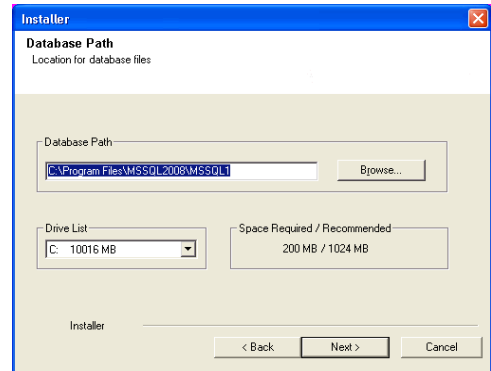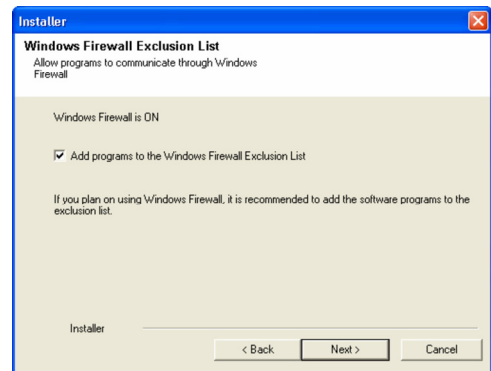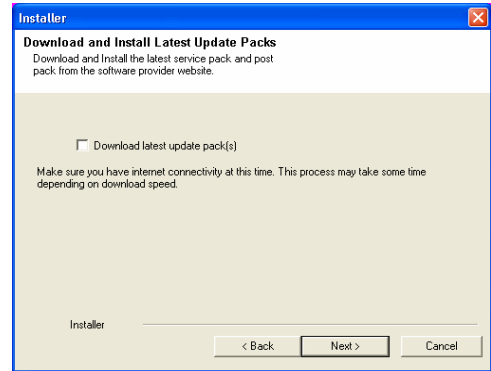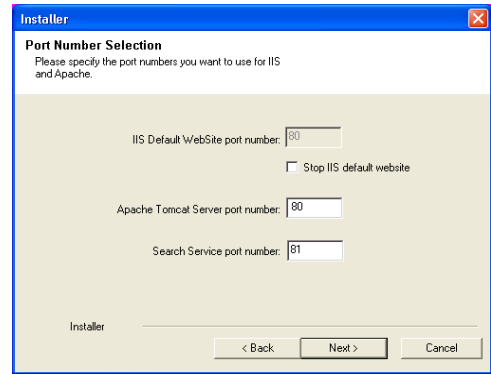
17. Click **Yes**.

18. Click **OK**.

19. Click **Next**.

20. Click **Next**.

21. Click **Reboot** to finish the installation.
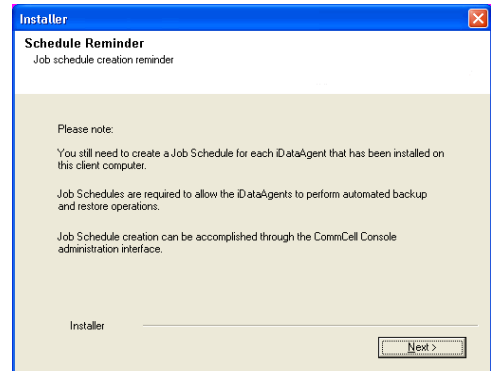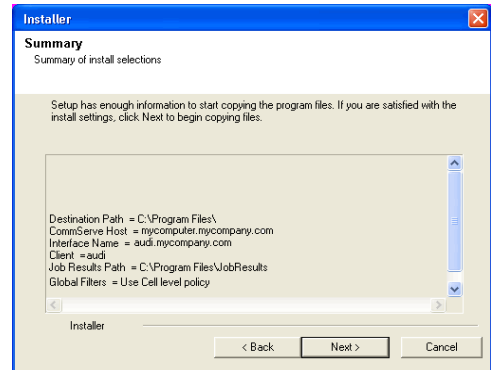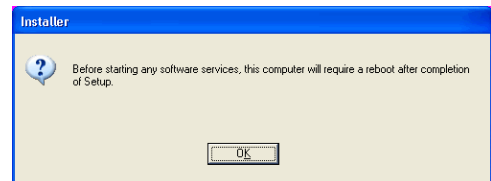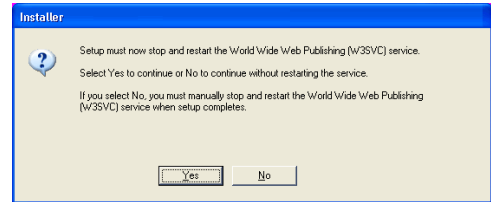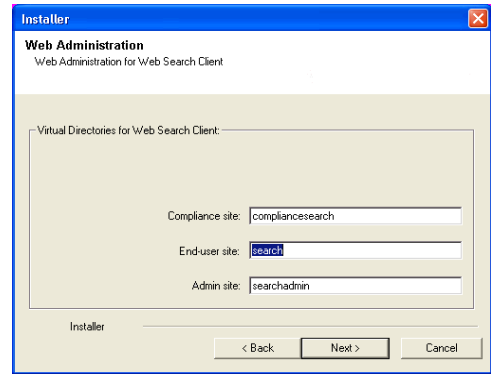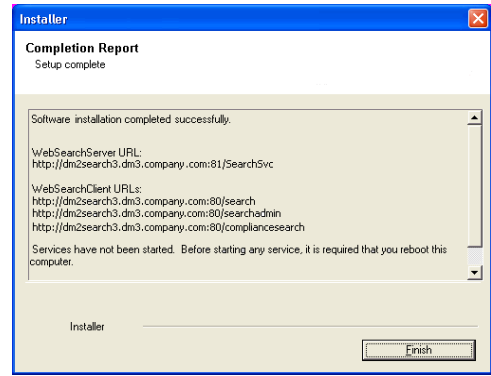
Desktop Browse - Windows File System (Administrator)

Install | **Setup**

Once the Web Search Server and Web Search Client are installed, perform the following configurations:

SETTING UP PERMISSIONS FOR END USERS

1. Obtain the domain name and fully qualified domain name of the Active Directory server.

2. Ensure that LDAP is configured on the AD server:
- From the Active Directory Server, select **Start | Run**.
- Type **ldp** on the **Run** dialog box and click **OK**.
- Click the **Connections** menu option, and select **Connect**.
- From the **Connect** dialog box, enter the following information:
  - ○ **Server**: Enter the name of the external domain server, e.g., computer.domain.com.
  - ○ **Port**: Enter 636 as the port number for the external domain server.
  - ○ **SSL**: Mark this checkbox to check for the proper certificate.
- Click **OK**. If properly configured for LDAP, the external domain server details will be displayed in the LDP windowpane. If not configured for use with LDAP, an error message will appear indicating that a connection cannot be made using this feature.

3. From the CommCell Browser, expand the **Security** node, right-click **Name Servers | Add New Domain** and click **Active Directory**.

4.
- Enter the domain name in **NetBIOS Name** text box, e.g., mydomain.
- Enter the Fully Qualified Domain Name (FQDN), e.g., mydomain.mycompany.com in the **Domain Name** text box.

5.
- Click **Edit** to enter the user account information for the domain.
- Type **Username** and **Password** in **Enter User Account Information**.
- Click **OK**.

6.
- Select **Use Secure LDAP** to enable the secure Lightweight Directory Access Protocol (LDAP) with the external domain.
- Click **OK**.

7. Once you have registered the Domain Controller, restart the IIS services on the Web Search Server.
- From your **CommServe** computer, click the **Start** button on the Windows task bar and then click **Administrative Tools**.
- Click **Services**.
- In the **Services** window, select and right-click **IIS Admin Service** and click **Restart**.
- **Restart Other Services** dialog will be displayed, click **Yes**.

8. From the CommCell Browser, expand the **Security** node, right-click **CommCell User Groups** and select **New User Group.**

9.
- Type the user group name in **Name** text box.
- Type a description on the user group in **Description** box.
- Click **Capabilities** tab.

10.
- Press **Ctrl** key and select the following capabilities:
  - ○ Browse
  - ○ End user search
- Click **>** to move the selected capabilities to the **Assigned Capabilities** list box.
- Click **Associated Entities** tab.

11.
- Expand **Client Computers** node and select the client computers to be browsed.
- Click **OK**.

12. Ensure that the specific external user group in which the user belongs has Group Scope defined as `Global` on the Active Directory Domain:
- Navigate to **Start | Administrative Tools | Active Directory Users and Computers**.
- Right-click the external group and select **Properties**.
- Select **Group** from **Group Scope** and click **OK**.

13.

From the CommCell Browser, navigate to **Security | Name Server |<Domain Name>**, right-click **External Groups** and select **Add New Group**.

14.

- Click **Browse**.
- Select the <**external user group name**> in which the user belongs.

15.

- Select the **CommCell User Group** to associate with the specified external user group.
- Click **OK**.

16. From the CommCell Browser, right-click to **<Client Computer>** on which Web
     Search Server is installed and click **Properties**.

17. Click **Search Server URLs** tab.

     Make a note of **End User Url** to provide the URL to the user to browse and recover
     the data.

SETTING UP PERMISSIONS FOR COMPLIANCE USERS

1. Obtain the domain name and fully qualified domain name of the Active Directory
    server.

2. Ensure that LDAP is configured on the AD server:
    - From the Active Directory Server, select **Start | Run**.
    - Type **ldp** on the **Run** dialog box and click **OK**.
    - Click the **Connections** menu option, and select **Connect**.
    - From the **Connect** dialog box, enter the following information:
      ○ **Server**: Enter the name of the external domain server, e.g.,
        `computer.domain.com.`
      ○ **Port**: Enter 636 as the port number for the external domain server.
      ○ **SSL**: Mark this checkbox to check for the proper certificate.
    - Click **OK**. If properly configured for LDAP, the external domain server details will
      be displayed in the LDP windowpane. If not configured for use with LDAP, an error

message will appear indicating that a connection cannot be made using this feature.

3. From the CommCell Browser, expand the **Security** node, right-click **Name Servers** | **Add New Domain** and click **Active Directory**.

4.
- Enter the domain name in **NetBIOS Name** text box, e.g., `mydomain`.
- Enter the Fully Qualified Domain Name (FQDN), e.g., `mydomain.mycompany.com` in the **Domain Name** text box.

5.
- Click **Edit** to enter the user account information for the domain.
- Type **Username** and **Password** in **Enter User Account Information**.
- Click **OK**.

6.
- Select **Use Secure LDAP** to enable the secure Lightweight Directory Access Protocol (LDAP) with the external domain.
- Click **OK**.

7. Once you have registered the Domain Controller, restart the IIS services on the Web Search Server.
- From your **CommServe** computer, click the **Start** button on the Windows task bar and then click **Administrative Tools**.
- Click **Services**.
- In the **Services** window, select and right-click **IIS Admin Service** and click **Restart**.
- **Restart Other Services** dialog will be displayed, click **Yes**.

8. From the CommCell Browser, expand the **Security** node, right-click **CommCell User Groups** and select **New User Group.**

9.
- Type the user group name in **Name** text box.
- Type a description on the user group in **Description** box.
- Click **Capabilities** tab.

10.
- Press **Ctrl** key and select the following capabilities:
  - ○ Browse
  - ○ Compliance Search
  - ○ Legal Hold Management
  - ○ Annotation Management
  - ○ Tag Management
  - ○ ERM Management
- Click **>** to move the selected capabilities to the **Assigned Capabilities** list box.
- Click **Associated Entities** tab.

11.
- Expand **Client Computers** node and select the client computers to be browsed.
- Click **OK**.

12. Ensure that the specific external user group in which the user belongs has Group Scope defined as `Global`on the Active Directory Domain:
- Navigate to **Start | Administrative Tools | Active Directory Users and Computers**.
- Right-click the external group and select **Properties**.
- Select **Group** from **Group Scope** and click **OK**.

13.

From the CommCell Browser, navigate to **Security | Name Server |<Domain Name>**, right-click **External Groups** and select **Add New Group**.

14.

- Click **Browse**.
- Select the <**external user group name**> in which the user belongs.

15.

- Select the **CommCell User Group** to associate with the specified external user group.
- Click **OK**.

16. From the CommCell Browser, right-click to **<Client Computer>** on which Web Search Server is installed and click **Properties**.

17. Click **Search Server URLs** tab.

Make a note of **End User Url** to provide the URL to the user to browse and recover the data.

ENABLING SECURED ACCESS FOR WEB SEARCH CLIENT

Use the following steps to enable secured access on the Web search client. This will allow you to access the Web Console using https instead of http.

INSTALL JAVA WITH ALL THE UPDATES

1. Stop the Tomcat services

2. If UAC is enabled, disable it.

3. Download and install the latest version of JAVA with all the updates on the Web client computer.

4. Open the command prompt window on the Web client computer, and execute the following command to verify if JAVA has been properly installed on the Web client computer:

   `C:\java -version`

   If you find that JAVA with the latest updates has not been installed, uninstall JAVA that you have installed and reinstall it again with all the updates.

Navigate to the command prompt on the Web client computer, and run the command specified in step 4 to verify if JAVA has been installed successfully.

Skip this step if the updates are installed successfully.

5. Start Tomcat services. If the Tomcat fails to start, point the JVM manually to Tomcat using the following steps:

   ○ Open the command prompt window on the Web client computer, navigate to `<PRODUCT_INSTALL_PATH>\Apache\bin` folder and execute the following command:

   `C:\<PRODUCT_INSTALL_PATH>\Apache\bin>tomcat6w.exe //ES//GxTomcatInstance001`

   where, `Instance001` is the instance installed on the WebClient computer.

   ○ On the Tomcat Services Instance properties dialog box, click the **Java** tab, and clear the **Use default** check box.

   ○ Restart Tomcat services

CONFIGURE SSL ON THE TOMCAT SERVER

Use the following steps for configuring SSL (Secure Socket layer) on the Tomcat Server:

1. Navigate to command prompt and run the following command:

   `C:\Program Files\Java\jre6\bin>keytool -genkey -alias cvtomcat -keyalg RSA -keystore "C:\Program Files\company\product\Apache\cert\keystore"`

2. Backup the server.xml file located in <product_install_path>\Apache\conf before making any changes to it.

3. In order to setup a JAVA JSSE connector to support SSL, search for the following entry in the server.xml:

   `<Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" />`

   Modify the above entry as following:

   `<Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="off" />`

4. Add the following entry to the `server.xml` file:

   `<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol" SSLEnabled="true" maxThreads="150" scheme="https" secure="true" clientAuth="false" keystoreFile="C:/Program Files/CommVault/Simpana/Apache/cert/keystore" keystorePass="mnoettomcat" sslProtocol="TLS" />`

5. Save the `server.xml` file, and restart the Tomcat services.

◀ Previous   Next ▶

Desktop Browse - Windows File System (User)

This feature/product/platform is deprecated in this release. See Deprecated Features, Products, and Platforms for more information.

It is recommended to use Laptop Backup to browse file system data.

Getting Started	Restore	Advanced Options

◀ Previous   Next ▶

Desktop Browse enables users to browse and restore data using a web browser from any remote location without the need for installing the software.

LOGGING TO WEB CONSOLE

1. Open the supported Web Browser and type the Web Console URL in the address line. For example, `http://amber.domain.company.com/<web_alias_name>`
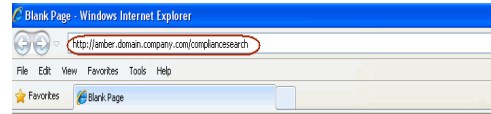
2.
   - Type the login credentials to access the Web Console.
   - Click **Login**.
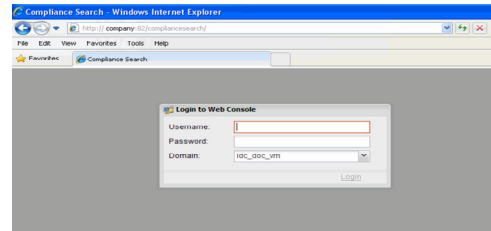
BROWSING AND RESTORING DATA

1. From the Web Console, click **Browse** on the left pane.

2. Double-click the **<CommServe computer name>**.
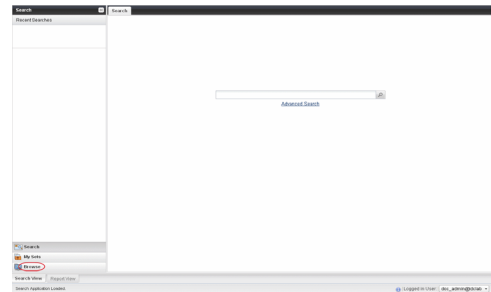
3. Double-click **Files**.
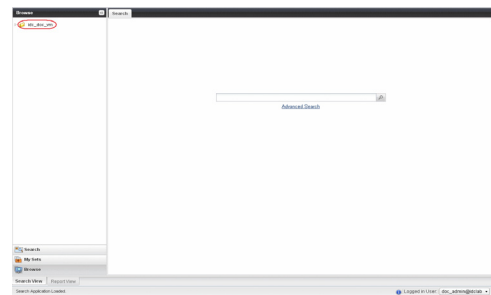
4.
- Double-click the specific <**client computer name**>.
- Select **Recent**.

5. Navigate to the file to be restored on the right pane**.**

6. Right-click the file and select **Retrieve.**

The file is copied to the **MyReviewSet** folder under **MySets | ReviewSet** node in the Web Console.

7. Right-click the file and select **Download Item**.

8.
- Click **Save** from the **File Download** dialog.
- Specify the location where the file needs to be downloaded in the Web Browser's download dialog box.
- Click **Save**.
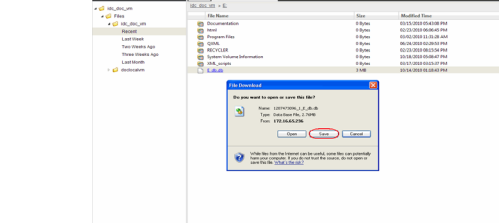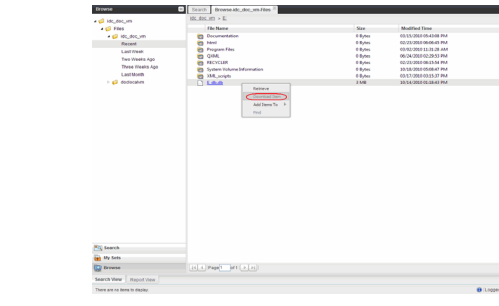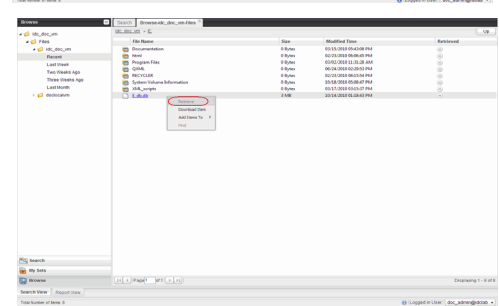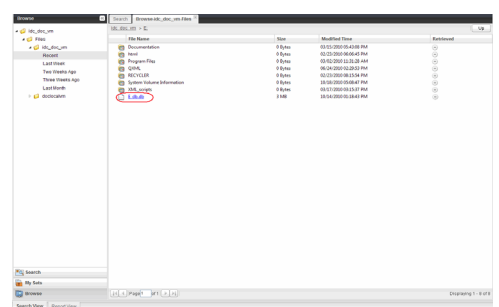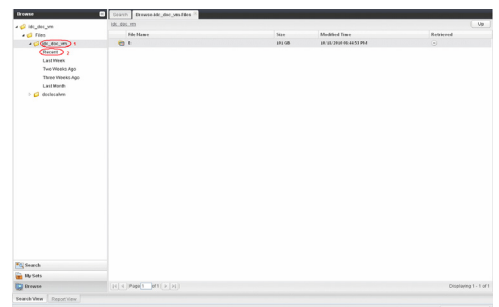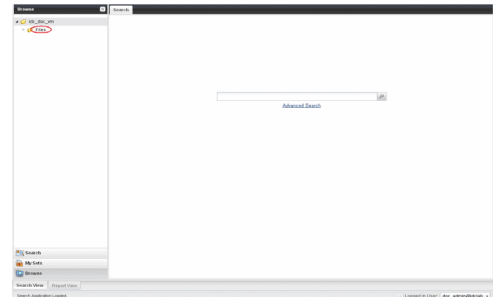
Desktop Browse - Windows File System (User)

| Getting Started | Restore | Advanced Options |

◀ Previous Next ▶

TABLE OF CONTENTS

RESTORING DATA FROM A SPECIFIC TIME RANGE

You can also browse and restore data that was backed up some time earlier or within a specific time range.

1. From the Web Console, click **Browse** on the left pane.

2. Double-click the **<CommServe computer name>**.

3. Double-click **Files**.

4. Double-click the specific **<client computer name>** and select one of the following options:
   - **Last Week**
   - **Two Weeks Ago**
   - **Three Weeks Ago**
   - **Last Month**.

5. Right-click the **<client computer name>** and select **Browse By Time**.

6. Select the time range in the **Before** drop down boxes.

7. Click **After** and specify the time range.

8. Click **OK**.

9. Navigate to the file to be restored on the right pane**.**

10. Right-click the file and select **Restore.** The file is copied to the **MyReviewSet** folder under **MySets | ReviewSet** node in the Web Console.

11. Right-click the file and select **Download Item**.

12. Click **Save** from the **File Download** dialog.

13. Specify the location where the file needs to be downloaded in the Web Browser's download dialog box and click **Save**.
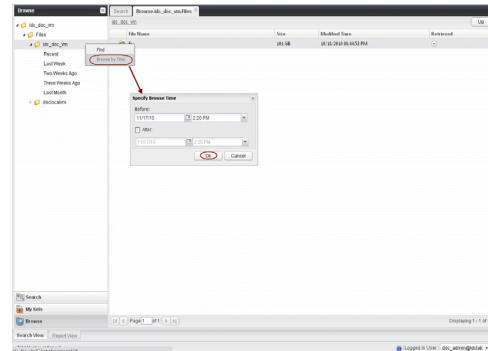
RESTORING DATA TO A SPECIFIC CLIENT COMPUTER

You can restore data to a specific destination computer.

1. From the Web Console, click **Browse** on the left pane.

2. Double-click the **<CommServe computer name>**.

3. Double-click **Files**.

4. Double-click the specific **<client computer name>** and select one of the following options:
   - **Last Week**
   - **Two Weeks Ago**
   - **Three Weeks Ago**
   - **Last Month**.

5. Right-click the **<client computer name>** and select **Browse By Time**.

6. Select the time range in the **Before** drop down boxes.

7. Click **After** and specify the time range.

8. Click **OK**.

9. Navigate to the file to be restored on the right pane**.**

10. Right-click the file and select **Restore To Client.**
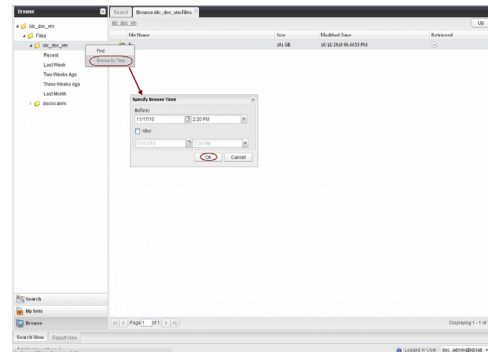
11. Select the **Destination Computer** from the drop-down box.
   - ○ Uncheck the **Restore to the same folder** check box
   - ○ Type the destination path to restore the file to a specific folder in the computer.

12. Click **OK**. The file will be restored to the specified destination computer.

FINDING DATA WITH A SPECIFIC PATTERN

You can use **Find** option to search and locate files with a specific file name or file name pattern.

Follow the steps given below to find and locate files with a specific file name or file name pattern:

1. From the Web Console, click **Browse** on the left pane.

2. Double-click the **<CommServe computer name>**.

3. Double-click **Files**.

4. Right-click the **<Client computer name>** and select **Find**.

5. Type the file name or wildcard pattern criteria in the **File/Pattern** text box from the **Find Options** dialog box.

6. Click **OK**.
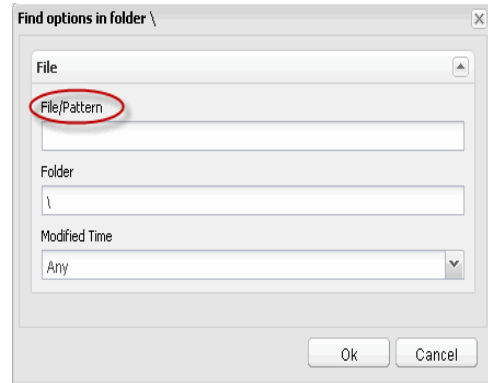
FINDING DATA WITHIN A SPECIFIC FOLDER

You can find and locate a folder with a specific folder name.

Follow the steps given below to find and locate a folder with a specific name.

1. From the Web Console, click **Browse** on the left pane.

2. Double-click the **<CommServe computer name>**.

3. Double-click **Files**.

4. Right-click the **<Client computer name>** and select **Find**.

5. Type the folder name in which the file resides in the **Folder** text box from the **Find Options** dialog box.

6. Click **OK**.
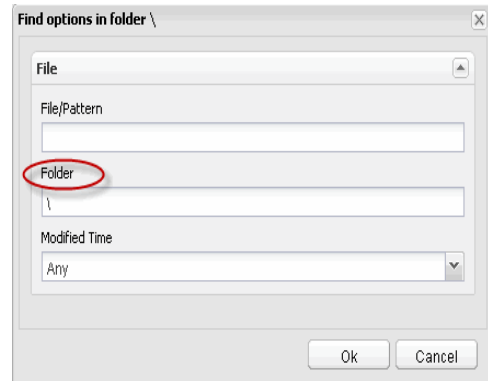
FINDING DATA WITH A SPECIFIC MODIFIED TIME

You can find and locate a file based on the time range (such as Today, Yesterday, etc) when the files were modified.

Follow the steps given below to find and locate files based on the modified time.

1. From the Web Console, click **Browse** on the left pane.

2. Double-click the **<CommServe computer name>**.

3. Double-click **Files**.

4. Right-click the **<Client computer name>** and select **Find**.

5. Click the **Modified Time** drop-down box and select the time range (such as Any, Today, Yesterday, This Week, etc.) when the files were modified.

6. Click **OK**.
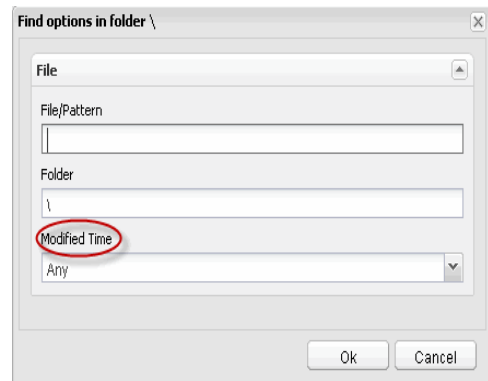
Desktop Browse - Windows File System (User)

Getting Started | Restore | Advanced Options

◀ Previous | Next ▶

TABLE OF CONTENTS

RETAINING A FILE FOR LONG TERM

Compliance users can retain specific files for a longer term by moving them to a Legal Hold container.

1. From the Web Console, click **MySets** on the left pane.

2. Double-click **Review Set** and click the <**Review Set Name**>.

3. Right-click the file, navigate to **Add Item To** | **Legal Holds** and select <**Legal Hold Name**>.
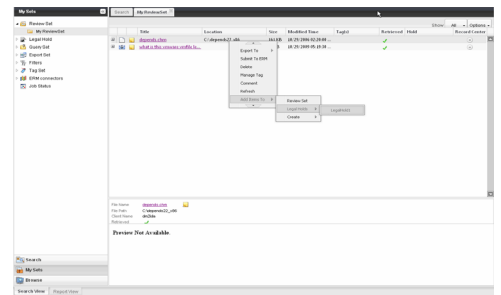
MOVING A FILE TO A RECORDS MANAGEMENT SITE

Compliance users can move files to a Records Management Site (eg., Microsoft SharePoint Site) using an ERM Connector.

1. From the Web Console, click **MySets** on the left pane.

2. Double-click **Review Set** and click the <**Review Set Name**>.

3. Right-click the file, and select **Submit To ERM**.

4. Click **ERM Connector Name** drop-down box and select the <**ERM Connector name**>.

5. Click **OK**.
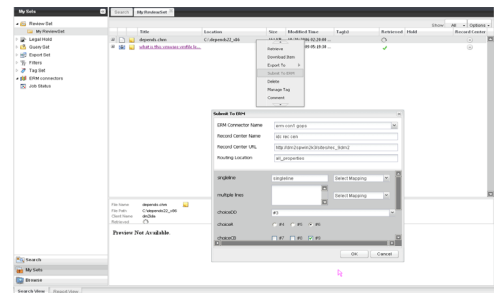
ADDING COMMENTS TO A FILE

1. From the Web Console, click **MySets** on the left pane.

2. Double-click **Review Set** and click the <**Review Set Name**>.

3. Right-click the file and select **Comment**.

4. Type the statement for comments and click **Comment**.

5. Click **Close** to exit the Comment window.
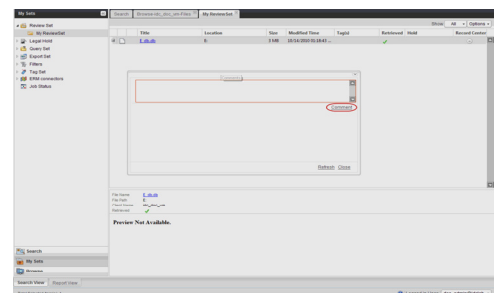
ADDING REVIEW TAGS TO A FILE

Compliance users can apply review tags to a file to facilitate easy search based on tags at a later point of time.

1. From the Web Console, click **MySets** on the left pane.

2. Double-click **Review Set** and click the **<Review Set Name>**.

3. Right-click the file and select **Manage Tags**.

4. On the **Manage Tag(s)** window, select the tag to apply.

5. Click **Apply Tags**.

GROUPING FILES BY FOLDER PATH

1. From the Web Browser, click **My Sets** on the left pane.

2. Double-click **Review Set**, and then click the desired **<Review Set name>**/**<Legal Hold Set Name>**.

3. On the **Group By** menu, click **Folder Path**.
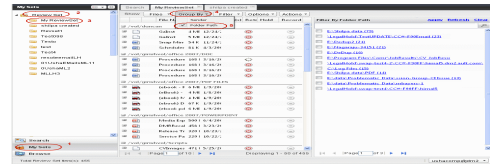
FILTERING FILES BY FOLDER PATH

1. From the Web Browser, click **My Sets** on the left pane.

2. Double-click **Review Set**, and then click the desired **<Review Set Name>**/**<Legal Hold Set Name>**

3. On the **Filter** menu, click **Folder Path**.

4. On the right pane, select the folder path.

5. Click **Apply**.
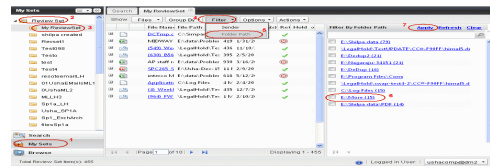
You can click the **Clear** button on the right pane to clear all the selected folder paths. To clear a specific selected folder path, click the cross-mark symbol corresponding to the selected folder path on the right pane.

DOWNLOADING A FILE

1. From the Web Console, click **MySets** on the left pane.

2. Double-click **Review Set** and click the **<Review Set Name>**.

3. Right-click the file and select **Download Item**.

4. Specify the location where the file needs to be downloaded in the Web Browser's download dialog box.
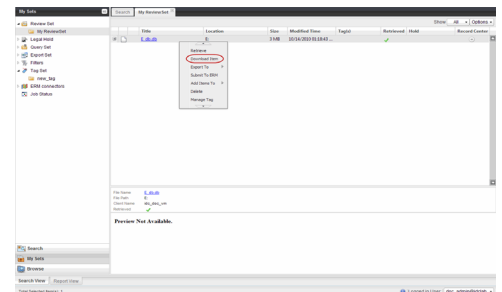
DOWNLOADING MULTIPLE FILES

In order to download multiple files, you can export the selected files/folder to a compressed file format (CAB format) and then download the CAB file to your computer.

1. From the Web Console, click **MySets** on the left pane.

2. Double-click **Review Set** and click the **<Review Set Name>**.

3. Right-click the file and select **Export To** | **CAB**.

4. Specify the **Download Name.**

5. Select the **Select Export** Set.

6. Click **OK**. The selected file(s) are moved to the selected **Export Set** with the given name.

7. Click **MySets | Export Set**.

8. Click the Export Set which contains the CAB file.

9. Right-click the CAB file and select **Download**.

10. Click **Save** from the **File Download** dialog box.
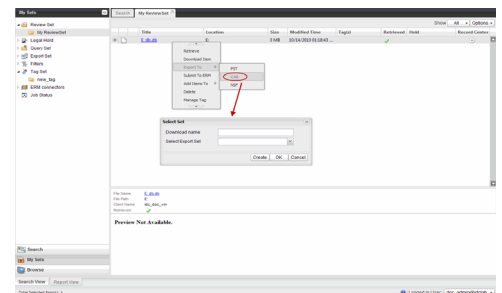
11. Navigate to the location where you want to download the file.

12. Click **OK**.

SAVING FILE PROPERTIES

You can save the properties of all the files in a reviewset as an XML file to you local computer.

1. From the Web Console, click **MySets** on the left pane.

2. Double-click **Review Set.**

3. Right-click the <**Review Set Name**> and select **Save to XML**.

4. Click **Save** from the File Download dialog.

5. Navigate to the location where you want to save the file.

6. Click **OK**.
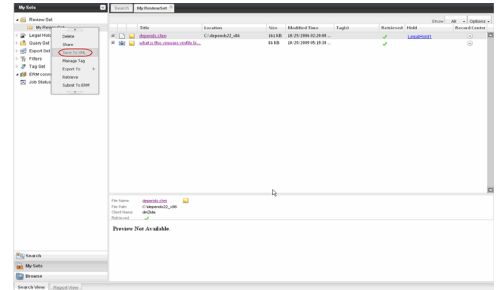
SHARING FILES TO OTHER USERS

You can share and assign access permissions to all the files in your Review Set folder to selected users.

1. From the Web Console, click **MySets** on the left pane.

2. Double-click **Review Set** and click the <**Review Set Name**>.

3. Right-click the review set and select **Shares**.

4. Click **Add**.

5. Select the user/user groups from the **Select User or Group** window.

6. Click **OK.**

7. Select **Allow** check box to assign the respective privileges.

8. Click **OK**.
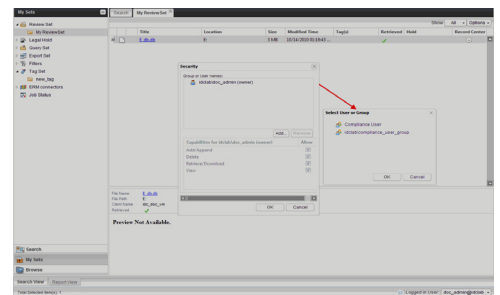
SHARING BROWSE RESULTS TO OTHER USERS

When browsing data, you can share the browse results with other users.

1. From the Web Console, click **Browse**.

2. Navigate to the client computer to be browsed.

3. Copy the URL of the browse result page from the browser's address bar and email to other users.

When the recipient users open the URL, they can directly view the browse result page as soon as they login to the Web Console.

◀ Previous   Next ▶
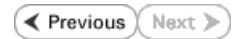
Agentless SRM

Topics | How To | Support | Related Topics

Overview

Pre-Requisites

Configuration

Reports supported by Agentless SRM

Summaries displayed for Agentless SRM

Considerations

Registry Keys for Agentless SRM

OVERVIEW

Agentless SRM is a compact version of Storage Resource Management (SRM) where a Windows Proxy Agent collects data from remote computers (i.e., managed clients) and operates without having to install Agent software on the managed clients.

The Agentless SRM setup allows for the running of Discovery level jobs and the generation of reports. It requires installing a single SRM File System Agent or Windows File System *i*DataAgent (with SRM Enabled) that can manage one or more remote clients (i.e., managed clients). This SRM Windows File System Agent or Windows File System *i*DataAgent (with SRM Enabled) acts a Windows Proxy agent to gather statistics and run discovery level jobs on the Managed Clients. The Agentless SRM setup is easy to configure as only one SRM File System Agent or Windows File System *i*DataAgent (with SRM Enabled) is required to be installed on a computer that acts as a Proxy and Data Collection can be performed on all the client machines managed by this Windows Proxy Agent without requiring to install the actual software on the managed clients.

The reports available for Agentless clients illustrate some of the basic data representation of the usage patterns of file systems, thus helping plan for growth. The reports can be customized by specifying filter criteria like Client Selection, Column selection, Report Options, Filters, Get SQL Query, etc. to generate a variety of charts and graphs.

Specific summaries are displayed for all the clients. When you select an Agentless SRM entity from the CommCell Console, its summary information appears in the main window.

Note the following terminologies used in this feature:

- Windows Proxy Agent is used to refer to a client computer that has the SRM File System Agent or Windows File System *i*DataAgent (with SRM Enabled) installed.
- Managed Client is used for computers managed by the Windows Proxy Agent.

The Windows Proxy Agent will perform Data Collection operations on the managed clients.

PRE-REQUISITES

WMI AND SSH

- On the Managed Clients running Windows, the Windows Management Instrumentation (WMI) service should be running.

  For more information on configuring WMI service across firewall, refer to http://msdn.microsoft.com/en-us/library/aa389286(VS.85).aspx.

- On the Managed Clients running Unix, Secure Shell (SSH) needs to be installed and running.

LICENSING

Agentless SRM does not requires any license. However you would require a license for the SRM Windows File System Agent that acts as the Windows Proxy Agent, this license is consumed when you install the Agent.

CONFIGURATION

Agentless Data Collection is a process that involves the following configuration settings:

INSTALL THE SOFTWARE ON WINDOWS PROXY AGENT

The SRM File System Agent or Windows File System *i*DataAgent (with SRM Enabled) needs to be installed on the Windows Proxy Agent. Deployment provides several methods to deploy SRM File System Agent or Windows File System *i*DataAgent (with SRM Enabled) - choose an appropriate method. See Deployment for step by step instruction on installing the Agent.

SETTING UP AGENTLESS SRM POLICY

Managed clients need to be configured/set up from the Windows Proxy Agent. This can be done automatically or manually using the Agentless SRM Policy. Setting up Client Computers using the Agentless SRM policy also creates a new Agentless Client Group.

For step-by-step instructions, see Create Agentless SRM Policy.

Refer to the sections below to determine which method better suits your requirements.

1. Manually enter client computer names

Setting up managed clients by manually entering the client name indicates that you will identify the computers that should be detected for Data Collection operations. This method is useful when it is required to setup one or two computers or groups of computers that must be managed, as it requires typing in the client names one in each line.

For step-by-step instructions, see Enter client names for Agentless SRM Policies.

2. Manual Setup of Client Computers

Setting up managed clients using the manual method indicates that you will identify the computers that should be detected for Data Collection operations. Using the manual method is useful when it is required to setup small or large number of computers or groups of computers that must be managed. If you need to manage all computers in a domain or multiple domains, use **Auto Setup of Client Computers** method.

Identifying the computers for selection can be done in three ways:

- List them individually

  This can be done using their fully qualified domain name

- Retrieve the list from an existing text file

  This file must list the client names as the fully qualified domain name, one in each line.

- Select the computers using Active Directory

  This can be done by selecting the client computers from within a specified domain by using the Active Directory Import feature. Optionally you could use **LDAP Filters** to perform a wildcard character search within the Active Directory to bring up desired results .

  E.g. he following query string will search for all objects of type "computer" with a name that begins with "dev".

  ```
  &(objectCategory=computer)(name=dev*))
  ```

For step-by-step instructions, see Setup Managed Clients on Windows Manually and Setup Managed Clients on UNIX Manually.

3. Auto Setup of Client Computers

Setting up managed clients using the auto discovery method indicates that you will identify a domain or multiple domains, which comprises the computers that should be detected for Data Collection operations. Using the auto discovery method is useful when it is required to setup all the computers within an entire domain. If you need to manage specific computers, use the **Manual Setup of Client Computers** method. You cannot select specific computers using this method.

For step-by-step instructions, see Setup Managed Clients on Windows Automatically and Setup Managed Clients on UNIX Automatically.

PERFORM DATA COLLECTION

Data Collection must be performed from the Windows Proxy Agent on all the managed clients before generating the reports. For Data Collection, a Managed Client must be attached to one Windows Proxy Agent - a single managed client cannot be attached to more than one Windows Proxy Agent. Data collection jobs can only be run from the Proxy Agent and not from managed clients. The maximum number of data collection jobs that can be run on the Windows Proxy Agent is 50.

Clients that are unreachable or which do not have WMI or SSH enabled at the time of Data Collection will not be available in client selection column at the time of report generation.

The following Data Collection Options are available for each Agentless Policy:

- Process Information
- Services Information
- Storage Information
- Quotas

- Software Information

It is recommended that you schedule the Data Collection operation on all the Managed Clients on a periodic basis in order to generate up-to-date reports. For step-by-step instructions, see Schedule Agentless SRM policies.

REPORTS SUPPORTED BY AGENTLESS SRM

Using SRM Agentless Data Collection, Discovery level jobs can be run and reports can be generated for the managed clients. Reports allow easy viewing and analyzing of data related to various aspects of different entities in an enterprise. Many pre-configured reports are available for the Agentless SRM Data Collection jobs for clients running on Windows and Unix operating systems that provide information about the resources of the client computers, each tailored to a particular aspect of resource management. Filter criteria can be specified to generate to a variety of customized charts and graphs. The following reports are available for clients running on Windows and Unix operating systems:

WINDOWS CLIENTS

For Managed Clients running on Windows operating system, a set of pre-configured reports and customizable reports are available. For the list of reports available for Agentless Data Collection for Windows clients see, SRM Windows File System Agent Reports and SRM for Windows File System - Reports.

UNIX CLIENTS

For Managed Clients running on UNIX operating system, a set of pre-configured reports and customizable reports are available. For the list of reports available for Agentless Data Collection for UNIX clients see, SRM UNIX File System Agent Reports.

SUMMARIES DISPLAYED FOR AGENTLESS SRM

Summaries for Agentless SRM clients displays status information including the resource, memory, and CPU usage, etc. Summary can be available in the images as in bar graphs and pie charts to provide a succinct snapshot of the statistical information or tables showing various columns. While viewing summary, data rows in tables can be sorted by any one of the columns listed in that summary. The following summaries are available at different levels for clients running on Windows and Unix operating systems:

WINDOWS CLIENTS

For Managed Clients running on Windows operating system, the following summaries are available:

CLIENTS

Summary information at the client level shows statistical data for the following:

- **Software Instances**

  The summary information for software instances displays details like Package, version and vendor name of all instances of the installed software.

- **Process Information**

  The summary information for processes displays details like Image Name, PID, Session ID, CPU Time, CPU Usage, Memory Usage, User Name, etc for each process that runs on the client.

- **Services**

  The summary information for services displays details like Name, State, Startup Type, and Log on information for each service that exists on the client.

VOLUMES

Summary information at the volumes level display charts for **File Count** and **File System Capacity** along with tables displaying details like Volume, Total Space, Used Space, Free Space, Percent Free, Percent Used, Type for the available volumes. Each Volume also displays Properties like Type, Mount Point, Used Space, Free Space, Capacity, etc. along with any Physical Devices if available.

1. From the CommCell Console, select the Client Computer Group with Agentless clients and select the client. Expand **SRM** and select **SRM Agent for Windows File System**.
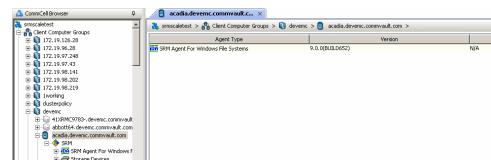
2. Select **Volume**.

3. The associated **Volume Summary** will appear in the main window.
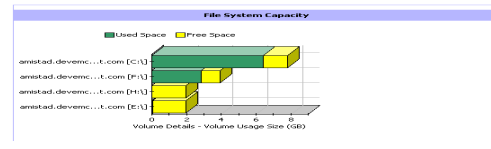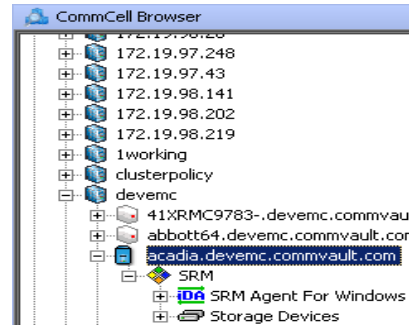
SHARES

Summary information include tables displaying Table Name, Path Name, and Protocol for the selected share.

STORAGE DEVICES

Summary information at the storage devices level include charts for **Allocated Vs Unallocated space per disk.** Each Physical Drive in turn displays charts for **Partition Capacity.** Physical properties like Name, Interface, Manufacturer, Block, Count , etc. are also displayed at this level.

1. From the CommCell Console, select the Client Computer Group with Agentless clients and select the client. Expand **SRM** and select **SRM Agent for Windows File System**.

2. Select **Storage Devices**.
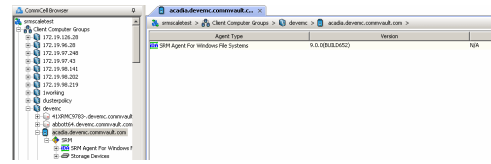
3. The associated **Storage Devices Summary** will appear in the main window.

UNIX CLIENTS

For Managed Clients running on UNIX operating system, the following summaries are available:

CLIENTS

Summary information at the client level shows graphs for the following:

- **CPU Utilization History**
- **Memory Utilization History**

The summary information also displays **Process Information** showing details like CPU Time, CPU Usage, Memory Usage, User Name, etc for each process that runs on the client.

VOLUME GROUP

Summary information at the Volume Group level Charts include charts for **Current Capacity by Volume Group.** This chart displays detail like Name, Volume

Group Manager, Capacity, Allocated Space, Unallocated Space, Access Mode, Logical Volume Count, Physical Volume Count, Physical Extent Count for the selected volume group.

1. From the CommCell Console, select the Client Computer Group with Agentless clients and select the client. Expand **SRM** and select **UNIX File System**.

2. Select **Volume Groups**.
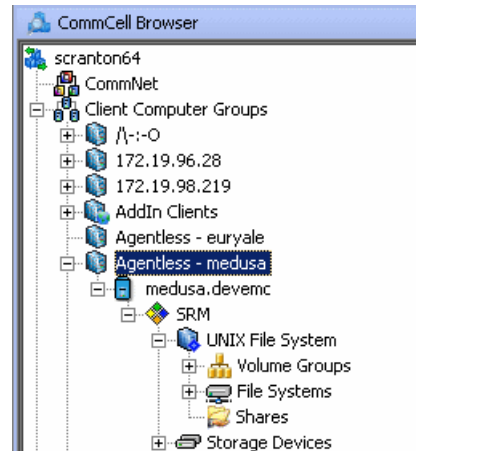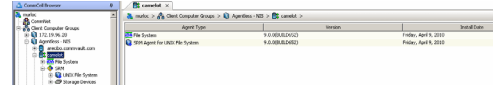
3. The associated **Volume Group Summary** will appear in the main window.
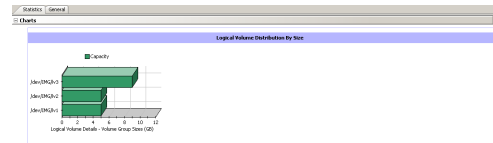
FILE SYSTEMS

Summary information at the File systems level include charts for **File Count** and **File System Capacity.** The **File System Capacity** chart displays detail like Name, Type, Mount Point, Used Space, Free Space, Capacity, Percent Used and Percent Free for the selected volume group.

1. From the CommCell Console, select the Client Computer Group with Agentless clients and select the client. Expand **SRM** and select **UNIX File System**.

2. Select **File Systems**.
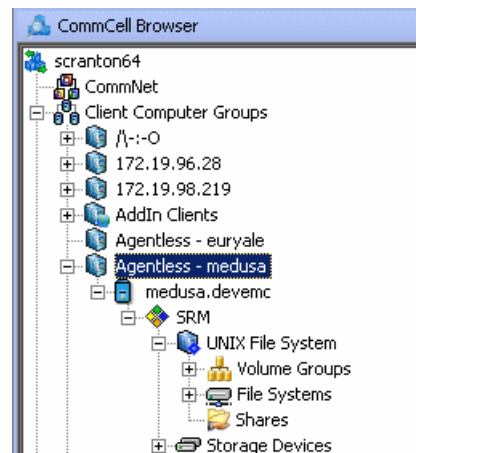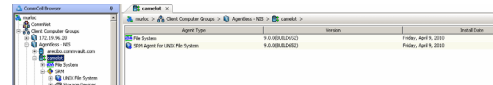
    You may also expand File Systems node and alternatively select any File System to view its summary.

3. The associated **File Systems Summary** will appear in the main window.
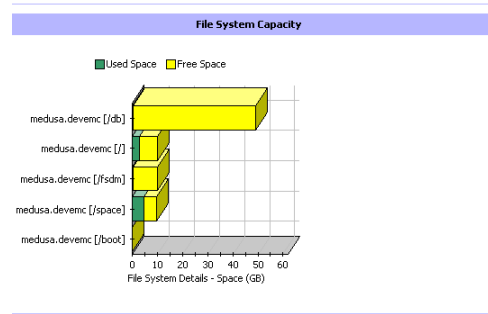
SHARES

Summary information include tables displaying Name, Path, Used Space and Billable Entity for the selected share.

STORAGE DEVICES

Summary information at the Storage Devices level display charts for **Allocated** vs. **Unallocated space per disk** and **Partition Capacity**. The Charts show details like Name, Interface, Serial Number (S/N), Manufacturer, Block Count, Block Size etc for the selected Storage Device.

1.	From the CommCell Console, select the Client Computer Group with Agentless clients and select the client. Expand **SRM** and select **UNIX File System**.

2.	Select **Storage Devices**.

> You may also expand Storage Devices node and alternatively select any storage device to view its summary.
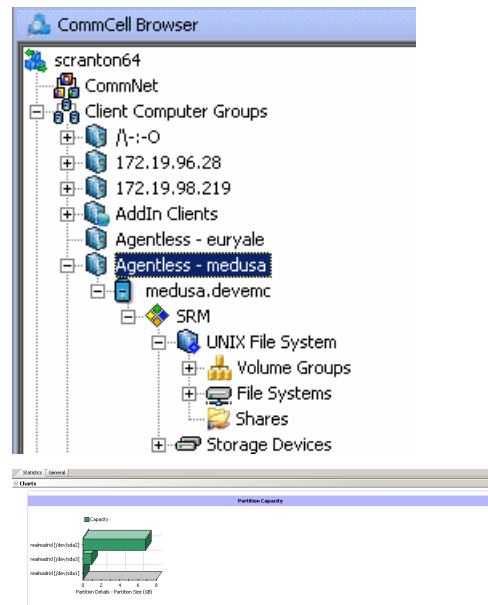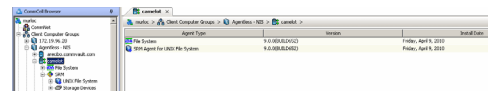
3.	The associated **Storage Devices Summary** will appear in the main window.

CONSIDERATIONS

The following important factors must be considered:

- For Agentless SRM jobs, the job details dialog displays the job completion in phases as Discover, Configure, Scan and Data Collection. The job is said to be complete if all the 4 phases complete successfully else the **Admin Job History (Attempts)** tab displays the completed and pending phases.

REGISTRY KEYS FOR AGENTLESS SRM

The default number of managed clients that can be discovered simultaneously in 10.

You can configure the `nSRMACLDCMaxThreads` registry key to increase the number of simultaneous discoveries of managed clients. Configure this Registry Key under the SRM folder.

Back to Top

SRM for Windows File System - Reports

| Basic | Advanced | Filters | Summaries | SRM Archiver Integration | FAQ |

TABLE OF CONTENTS

OVERVIEW

Managing storage resources is a critical job for any organization, which can be challenging because these resources are distributed across the network. SRM Windows File System reports provide a sleek, versatile, and easy-to-use reporting framework that enables you to easily and effectively choose, view, and analyze vital data. Customized reporting is available through the selection of filter criteria e.g., individual columns, specific clients, specific client computer groups, report options, and SQL Queries, a SRM Windows File System report helps you to:

● Assess used and free storage space to provide improved capacity planning.

● Track historical storage utilization for performance trending and proactively anticipate future resource needs.

CONFIGURATION

If SRM feature is enabled, SRM reports can be generated for all backup data as soon as the first full backup job has completed. Be sure to perform the following before generating reports:

OPTION	DESCRIPTION
Enable SRM for all backups	SRM can be enabled from the Agent levels for the *i*DataAgent. When Enable SRM is selected at the Agent level, SRM options get enabled for all subclients. 1. From the CommCell Browser, right-click the *i*DataAgent for which you want to enable SRM feature and select **Properties**. 2. **Enable SRM** must be selected from the **General** tab. A Discovery and Analysis Data Collection job is automatically set when you enable SRM. 3. Then confirm your selection by clicking **OK**.

Run a Backup	A full backup contains all the data that comprises a subclient's contents. If a client computer has multiple agents installed, then the subclients of each agent require a full backup in order to secure all of the data on that client. If a new subclient is added, a full backup is required on all subclients in order to maintain file level detail integrity.
	
	1. To perform a full backup, right-click the subclient, and click **Backup** in the CommCell Browser.
	
	  One of the following options must be selected from the Backup Options dialog box:
	
	  ○ Backup Type:
	    Select **Full**.
	  ○ Backup Schedule:
	    Select **Immediate** if you want to run the backup now.
	  ○ Granular Recovery:
	    Select **Enable Granular Recovery** if you intend to restore individual files and folders from a disk or volume-level backup.
	
	2. Then confirm your changes by clicking **OK**.
	
	You can track the progress of the backup job from the Job Controller window. When the backup has completed, the Job Controller displays Completed.
	
	After performing a first full backup you may select any other backup type for performing Data Collection operations.

GENERATE SRM REPORTS

The sections below discuss running, scheduling, and saving a report.

RUNNING A REPORT

You can choose to run a report so that you view it immediately. Alternatively, to view it at a later point in time you can schedule it or save it as a template to a file. When running a report, you can choose an out-of the box template or generate a more customized report by picking and choosing individual columns from a category.

TO RUN A SRM REPORT IMMEDIATELY:

1. From the CommCell Browser, click **Reports**, and then click **SRM Report Manager**.

2. Expand the applicable tree to view your agent. Then click a template to display the **Options** window.

3. Click the **Client Selection** tab and select the client computers or client computer group. This is a required step.

4. Click **Column Selection** tab.

For an out-of-the-box template, the columns are displayed here. To change the columns, select a category and click **Add** or **Remove** to move the columns between the **Available** and **Selected** boxes. Clicking **Remove All** will remove all previously selected filters for the reports.

5. Click **Run** to generate the report immediately and view the results.
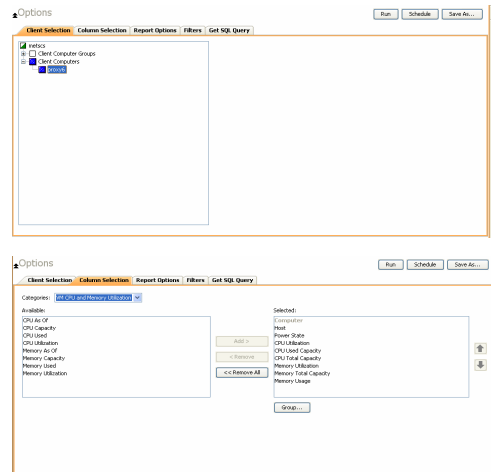
SCHEDULING A REPORT

Scheduling allows you to run a report on a user-defined schedule, send it in a different language or format, and configure notifications for specified recipients when the report has run. Reports can be scheduled so that they follow a backup schedule in order to guarantee up-to-date reporting. Scheduling a report involves these tasks:

● Specify a daily, weekly, monthly, yearly, or even one time basis schedule. When scheduling, patterns can be applied to the report so it runs on a specific time, repeated every so many days, or run for a particular number of times.

● Scheduled reports support different languages and formats. Default language is English and default output is HTML. You can even save the report to local drive or a network share.

● When scheduled reports are run, notifications can be sent in the form of an email or page, SNMP trap, RSS feed, or Event Viewer message to inform email recipients, computers, or a script that a report has run and is now available.

TO SCHEDULE A SRM REPORT:

1. From the CommCell Browser, click **Reports**, and then click **SRM Report Manager**.

2. Expand the applicable tree to view your agent. Then click a template to display the **Options** window.

3. Click the **Client Selection** tab and select the client computers or client computer group. This is a required step.

4. Click **Column Selection** tab.

For an out-of-the-box template, the columns are displayed here. To change the columns, select a category and click **Add** or **Remove** to move the columns between the Available and Selected boxes. Clicking **Remove All** will remove all previously selected filters for the reports.

5. Click **Schedule** to generate and schedule the report on a daily, weekly, monthly, yearly, or even one time basis.

Optionally, click **Report Options** to repeat sending the report every so many days, or run it for a particular number of times.

Click **Next**.

6. Select the report output options, such as:
- **Format** - select **MHTML**, **EXCEL**, or **PDF**.
- Specify a path in **Destination Path** if you want to save the report to a local drive or network share.

Click **Next**.

7. Configure the notifications for the scheduled report, such as:
- Select the **E-Mail/Pager** tab and click **Select [E-Mail/Pager] for notification**. Click either **Use default message** or add more tokens by selecting **Add Token**.
- Select the **SNMP** tab and click **Select [SNMP] for notification**. Click either **Use default message** or add more tokens by selecting **Add Token**. The SNMP Enabler software must be installed on the CommServe. See SNMP Enablers for more information.
- Select the **Event Viewer** tab and click **Select [Event Viewer] for notification**. Click either **Use default message** or add more tokens by selecting **Add Token**.
- Select the **Run Command** tab and click **Select [Run Command] for notification**. Click either **Run on CommCell** or **Run on Client**. Specify a path in **Command Script Location** and optionally specify arguments for the script in **Arguments**.
- Click **Run Data Archiver** tab to write files and directories of the report to a text file.
- Click **RSS Feeds** tab and click **Select [RSS Feeds] for notification**. Click either **Use default message** or add more tokens by selecting **Add Token**. Specify a feed location in **Select/Enter the FeedLocation** field.

Click **Next**.

Refer to the **Actions** documentation for more comprehensive information.

8. In this dialog, select the recipients for the scheduled report.

Use the **Add>** or **<Remove** buttons to specify CommCell users as the notification recipients.

Or, enter one or more email addresses in the **Email to Recipients** field. Separate multiple addresses with commas.

Click **Next**.
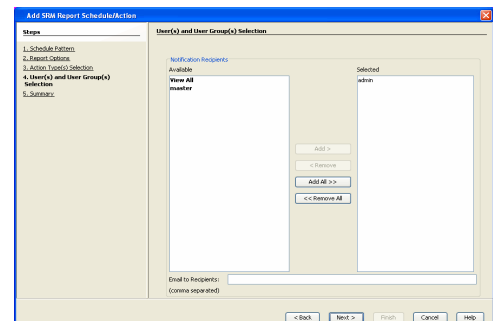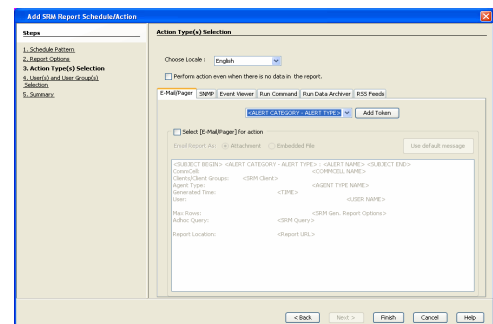
9.   Review the summary and if satisfied, click **Finish**.
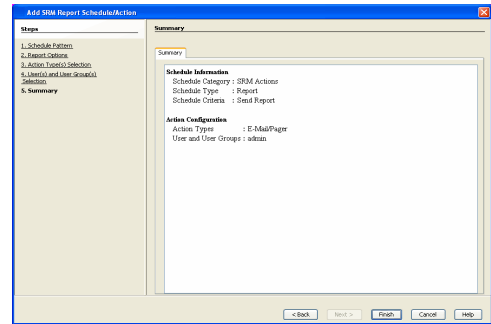
SAVING A REPORT

Saving a report allows you to save the filter criteria and schedule information, including notifications, to a template so it can be used to generate a report at a later date. All report templates are saved under **My Reports**.

TO SAVE A SRM REPORT TO A TEMPLATE:

1.   Create a report and optionally specify scheduling criteria as explained in Scheduling a Report. Advanced criteria such as Filters will also be saved in the report template.

2.   In the right-hand corner, click **Save As...** and enter a name for the report and click **OK**.

3.   The report template is saved under **My Reports**.

SEND A NOTIFICATION WHEN A SRM REPORT HAS RUN

Configuring notifications is a step when scheduling a report. For example, when scheduled reports are run, an email notification can be sent to inform the recipient that a report has run and is now available. The recipient can be either a CommCell user, a CommCell user group, a domain or external user (e.g., yahoo, gmail, etc.), or a pager address. For a comprehensive description of all notification types, refer to Actions.

TO SEND AN EMAIL NOTIFICATION WHEN A SCHEDULED REPORT HAS RUN:

1.   From the CommCell Browser, click **Reports**, and then click **SRM Report Manager**.

2.   Click **Applications** or **Enterprise**. Then click a template to display the **Filters** window.

3.   Configure the report by specifying clients and columns, report options, and optionally, ad hoc queries. Refer to Options, Report Options, and Filters respectively.

5.   Click **Schedule** to generate and schedule the report on a daily, weekly, monthly, yearly, or even one time basis.

       Optionally, click **Options** to repeat sending the report every so many days, or run it for a particular number of times.

       Click **Next**.

6. In this dialog, select the report output options, such as:

- **Format** - select **HTML**, **EXCEL**, or **PDF**.

- In **Locale**, select a report language. See Languages - Support for the list of supported languages.

- Specify a path in **Destination Path** if you want to save the report to a local drive or network share.

  > TIFF is no longer a supported output format. SRM supports saving Reports in these formats: HTML, EXCEL, and PDF.

  Click **Next**.

7. In this dialog, configure the **E-Mail/Pager** notification for the scheduled report as follows:

- Click **Select [E-Mail/Pager] for notification**.

- Either accept default format or add more tokens by selecting a token from the pulldown menu and clicking **Add Token**. The tokens are explained in Alert Tokens. Click **Use default message** to revert back to original default format.

  Click **Next**.

8. In the **User(s) and User Group(s) Selection** dialog, specify the recipients to whom the notification will be sent as follows:

- To add or remove CommCell users or a CommCell user group, select a user in the **Available** or **Selected** boxes and click **Add>** or **<Remove**.

- To specify a domain or external user (e.g., yahoo, gmail, etc.) or a pager address, enter the email address in **Email to Recipients** field. Separate multiple addresses with a comma.

9. Review the summary and if satisfied, click **Finish**.

GETTING STARTED WITH WINDOWS FILE SYSTEM REPORTS

The following illustrates a few possibilities of how Windows File System reports can be generated and used. For more information that explains the reports comprehensively and how to generate reports using all possible features, refer to Advanced page.

CAPACITY BY FILE SYSTEM

Use this report to display total, free and used space on the basis of File System.

TO VIEW THIS REPORT:

1. From the CommCell Browser, expand **Reports** and then click **SRM Report Manager**.

2. Expand **File Systems** | **Windows** | **Storage**.

3. Click the **Capacity by File System** template and select the client computers in the **Client Selection** tab.

4. Click **Run**.

    A statistics of file system capacity comprising of but not limited to total space, used space, free space, etc. for clients and client computer groups is displayed in chart and table formats.
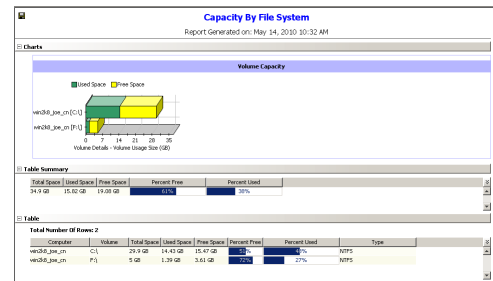
CURRENT FILE SYSTEM USAGE

Use this report to display details about files, directories, file size, depth, file count etc. for File System.

1. From the CommCell Browser, click **Reports**, and then click **SRM Report Manager**.
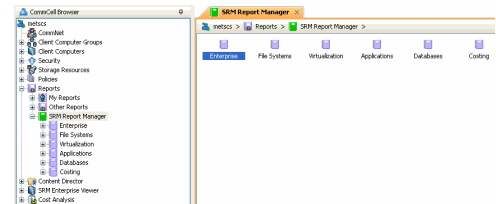
2. Expand **File Systems** | **Windows** | **Storage**.
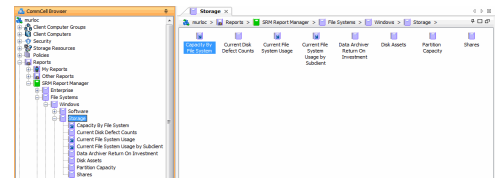
3. Click the **Current File System Usage** template and select the client computers in the **Client Selection** tab.
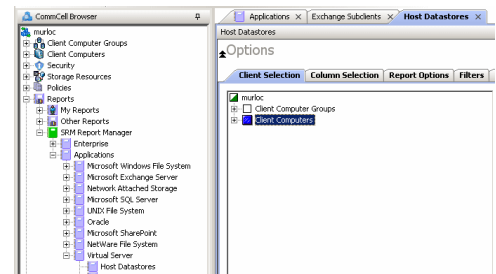
4. Click **Run**.

    A statistics of Current File System usage on the basis of files, directories, file size, depth, file count etc. is displayed in chart and table formats.
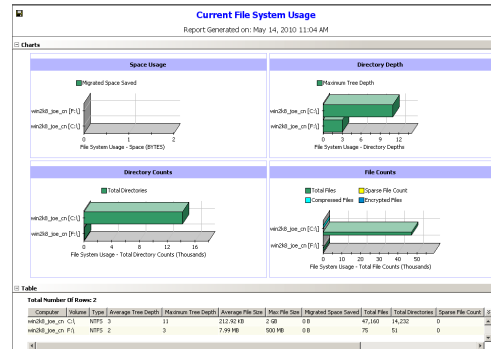
CURRENT FILE SYSTEM USAGE BY SUBCLIENT

Use this report to view details about files, directories, file size, depth, file count etc. on the basis of subclient of a file system.

TO VIEW THIS REPORT:

1. From the CommCell Browser, click **Reports**, and then click **SRM Report Manager**.
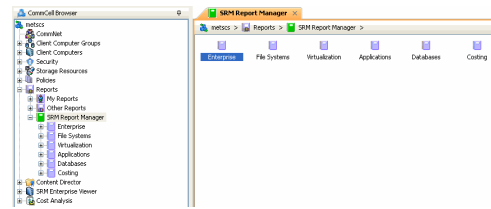
2. Expand **File Systems** | **Windows** | **Storage**.
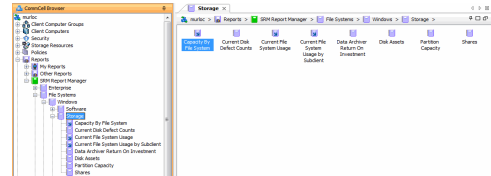
3. Click the **Current File System Usage by Subclient** template and select the client computers in the **Client Selection** tab.
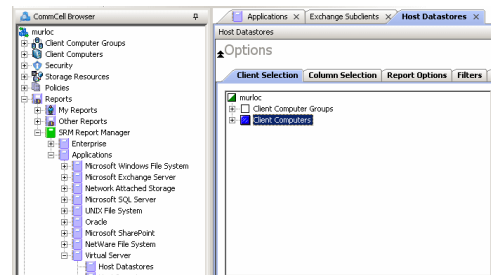
4. Click **Run**.

    Details such as files, directories, file size, depth, file count etc. on the basis of subclient of a file system are displayed in chart and table format.
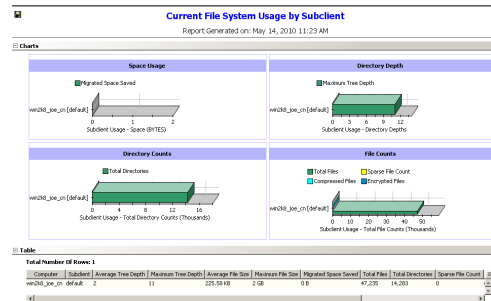
Back to Top

SRM for Windows File System - Reports

| Basic | Advanced | Filters | Summaries | SRM Archiver Integration | FAQ |

TABLE OF CONTENTS

OVERVIEW

SRM reporting provides a sleek, versatile, and easy-to-use reporting framework that enables you to easily and effectively choose, view, and analyze vital data. Enterprise and application-based reports can be rapidly generated with out-of-the-box templates or customized with filter criteria. Reports can be run immediately or scheduled to run daily, weekly, monthly, etc.

In essence, SRM Windows File System reports provide these features:

- Templates of predefined columns are provided so that a report can be generated quickly. The columns are preselected but can be adjusted as needed.

- Filter criteria. Reports can be customized according to particular criteria, such as client or client group, the columns to display in the report, etc.

- Report options control how the data is displayed in a report or chart. You can control the data size units, number of rows to display in an entire report or before a page break, sorting order, etc.

- Advanced features, such as Ad hoc SQL queries is another type of filter criteria that can also be applied to further refine the report.

- When scheduled, reports can be saved and shared in various formats (HTML, Excel, PDF) or in different languages.

- Notifications. When scheduled reports are run, notifications can be sent in the form of an email or page, SNMP trap, RSS feed, Event Viewer message to inform email recipients, computers, or a script that a report has run and is now available.

- Cost Analysis reports are available to provide Cost History and Usage History information (e.g., Cost History by Application, Usage History by Application). Data for these reports are compiled at regular intervals by a background process on the SRM Server.

The following sections describe the SRM Windows File System reporting features in more detail.

REPORT FEATURES

The following features are provided by SRM Reports.

OPTIONS

Out-of-the box templates provide pre-selected columns and can be run immediately after selecting clients or client computer groups. To generate a customized report, you can start with a template and then alter the pre-selected columns by adding or removing the columns. Note that when selecting clients, SRM data collection must be enabled and a full backup needs to have run for the Agent in order to have up-to-date information presented in the report.

> Pay particular attention when specifying filter criteria. Selecting criteria judiciously will aid in generating a useful report. Otherwise, the report may be too cumbersome and cluttered.

TO FILTER A SRM REPORT:

1. From the CommCell Browser, click **Reports**, and then click **SRM Report Manager**.

2. Expand the applicable tree to view your agent. Then select your agent and click a template to display the **Options** window.

3. Click the **Client Selection** tab and select the client computers or client computer group. This is a required step.
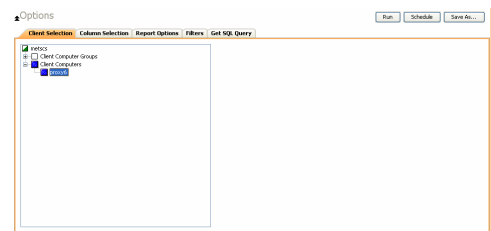
4. Click **Column Selection** tab.

   For an out-of-the-box template, the columns are displayed here. To change the columns, select a category and click **Add** or **Remove** to move the columns between the **Available** and **Selected** boxes. Clicking **Remove All** will remove all previously selected filters for the reports.

   The columns that can be selected are listed in **Available Columns**.

REPORT OPTIONS

The report options control how data is presented in the report. Either accept the defaults or modify the options as described below.

TO SPECIFY REPORT OPTIONS OF A SRM REPORT:

1. From the CommCell Browser, click **Reports**, and then click **SRM Report Manager**.

2. Expand the applicable tree to view your agent. Then select your agent and click a template to display the **Options** window.

3. Click the **Report Options** tab and click the **General tab** to modify these options:
   - Determine the **Data Size Unit** in the table section of the report and when building ad hoc queries. You can elect to have them converted for you automatically by selecting **Convert data size automatically** or you can specify the unit (e.g., Bytes, KB, MB, GB, MB, TB, PB). Default is GB.
   - Either accept the default number of 100 rows to display in the entire report or enter a new number in Limit number of rows to output.
   - Specify the number of rows to display in the report before breaking the page. Either accept the default of 100 or enter a new number in Number of rows per page.
   - For the columns selected, use the up and down arrows to move the sorting order of the columns in Set Sorting Order of Rows to Return. Also specify if you want ascending (ASC) or descending (DESC) order. For example, moving a column to the Top of the sorting order will filter the data base on that order first, followed by the rest of the columns. Select OFF to not include the column in the sort.

4. Click the **Report Options** tab and click the **Chart Options tab** to modify these options:
   - If you want to switch the X/Y Axes in the charts, click **Switch X/Y Axis**.
   - Select the columns in **Values** and **Labels** that should be displayed in the chart. To preserve charting space, only the first 25 characters for a label are visible in the report. To see the entire label, hover over the label with the mouse.
   - Specify the **Data Size Units in Chart** (e.g., BYTES, KB, MB, GB, MB, TB, PB) that you want displayed in the charts.
   - Enter the e **Maximum Number of Bar Points Per Chart** you want displayed, or click **Draw all Bar Points** to have all possible bar points drawn. Default is **10**.
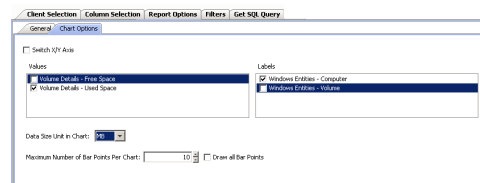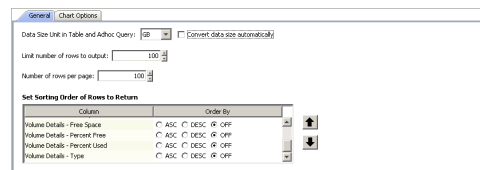
FILTERS

For the columns selected, Filters can also be applied to further refine the data in the report.

Selecting the **Get Query** tab will display the SQL query in long notation that will be used to get the data and generate the report. The query that is displayed is Read-only and can be used in a third-party SQL application, such as SQL Server Management Studio.

ACTIONS

Configuring notifications is a step when scheduling a report. When scheduled reports are run, notifications can be sent in the form of an email or page, SNMP trap, RSS feed, Event Viewer message to inform email recipients, computers, or a script that a report has run and is now available. The possible notifications are explained in the sections below.

E-MAIL/PAGER ADDRESS

A notification can be sent to email or pager recipients when a scheduled report has run. The recipient can be either a CommCell user, a CommCell user group, a domain or external user (e.g., yahoo, gmail, etc.), or a pager address.

A notification can be e-mailed or sent to a pager to a selected list of recipients when a scheduled report has run. The recipients can be either a CommCell user, a CommCell user group, a domain or external user (e.g., yahoo, gmail, etc.), or a pager address.

TO CONFIGURE AN EMAIL/PAGER NOTIFICATION WHEN A SCHEDULED REPORT HAS RUN:

1. From the CommCell Browser, click **Reports**, and then click **SRM Report Manager**.

2. Expand the applicable tree to view your agent. Then select your agent and click a template to display the **Options** window.

3. Configure the report by specifying clients and columns, report options, and optionally, ad hoc queries.

5. Click **Schedule** to generate and schedule the report on a daily, weekly, monthly, yearly, or even one time basis.

Optionally, click **Report Options** to repeat sending the report every so many days, or run it for a particular number of times.

Click **Next**.

6. In this dialog, select the report output options, such as:

- **Format** - select **MHTML**, **EXCEL**, or **PDF**.
- Specify a path in **Destination Path** if you want to save the report to a local drive or network share.

Click **Next**.

7. In this dialog, configure the **E-Mail/Pager** notification for the scheduled report as follows:

- Click **Select [E-Mail/Pager] for notification**.
- Either accept default format or add more tokens by selecting a token from the pulldown menu and clicking **Add Token**. The tokens are explained in Alert Tokens. Click **Use default message** to revert back to original default format.

Click **Next**.

8. In the **User(s) and User Group(s) Selection** dialog, specify the recipients to whom the notification will be sent as follows:

- To add or remove CommCell users or a CommCell user group, select a user in the **Available** or **Selected** boxes and click **Add>** or **<Remove**.
- To specify a domain or external user (e.g., yahoo, gmail, etc.) or a pager address, enter the email address in **Email to Recipients** field. Separate multiple addresses with a comma.

9. Review the summary and if satisfied, click **Finish**.

SNMP TRAPS

A notification can be sent by a CommServe, using the SNMP protocol, to other computers in the form of SNMP traps when a scheduled report has run. This notification type requires that the SNMP Enabler software must be installed on the CommServe computer. See SNMP Enablers for more information.

TO CONFIGURE AN SNMP TRAP NOTIFICATION WHEN A SCHEDULED REPORT HAS RUN:

1. From the CommCell Browser, click **Reports**, and then click **SRM Report Manager**.

2. Expand the applicable tree to view your agent. Then select your agent and click a template to display the **Options** window.

3. Configure the report by specifying clients and columns, report options, and optionally, ad hoc queries.

4. Click **Schedule** to generate and schedule the report on a daily, weekly, monthly, yearly, or even one time basis.

    Optionally, click **Report Options** to repeat sending the report every so many days, or run it for a particular number of times.

    Click **Next**.

5. In this dialog, select the report output options, such as:
    ● **Format** - select **MHTML**, **EXCEL**, or **PDF**.
    ● Specify a path in **Destination Path** if you want to save the report to a local drive or network share.

    Click **Next**.

6. Click the **SNMP** tab and configure this notification type as follows:
    ● Click **Select [SNMP] for notification**.
    ● Either accept default format or add more tokens by selecting a token from the pulldown menu and clicking **Add Token**. The tokens are explained in Alert Tokens. Click **Use default message** to revert back to original default format.

    Click **Next**.

7. Review the summary and if satisfied, click **Finish**.
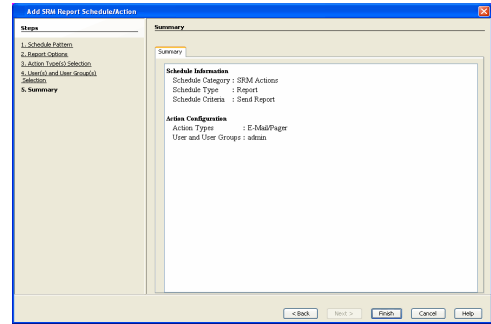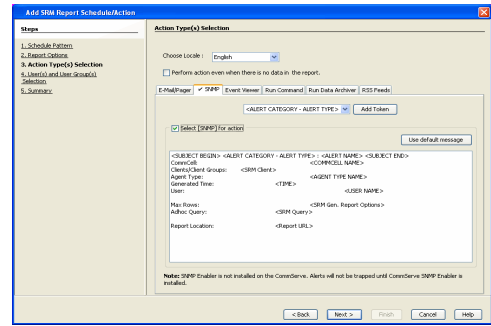
EVENT VIEWER

A message can be sent to the Event Viewer on the CommServe when a report is run or scheduled.

TO CONFIGURE AN EVENT VIEWER NOTIFICATION WHEN A SCHEDULED REPORT HAS RUN:

1. From the CommCell Browser, click **Reports**, and then click **SRM Report Manager**.

2. Expand the applicable tree to view your agent. Then select your agent and click a template to display the **Options** window.

3. Configure the report by specifying clients and columns, report options, and optionally, ad hoc queries.

4. Click **Schedule** to generate and schedule the report on a daily, weekly, monthly, yearly, or even one time basis.

Optionally, click **Report Options** to repeat sending the report every so many days, or run it for a particular number of times.

Click **Next**.

5. In this dialog, select the report output options, such as:
- **Format** - select **MHTML**, **EXCEL**, or **PDF**.
- Specify a path in **Destination Path** if you want to save the report to a local drive or network share.

Click **Next**.

6.   Click the **Event Viewer** tab and configure this notification type as follows:

- Click **Select [Event Viewer] for notification**.
- Either accept default format or add more tokens by selecting a token from the pulldown menu and clicking **Add Token**. The tokens are explained in Alert Tokens. Click **Use default message** to revert back to original default format.

Click **Next**.
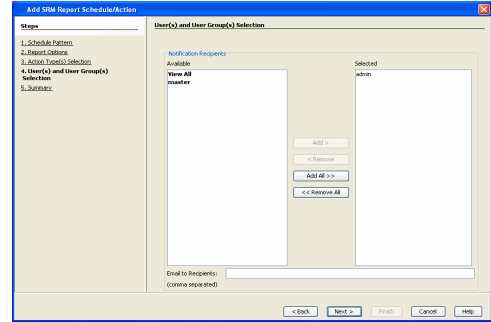
7.   Review the summary and if satisfied, click **Finish**.
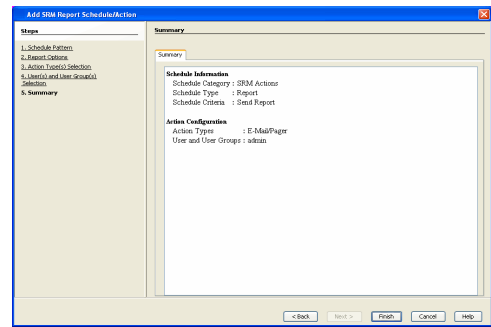
RUNNING A SCRIPT

A notification can be sent to a script when a scheduled report has run. Once receiving the notification, the script can be specified to run on the CommCell or a client computer. Arguments can be specified for the script as well. You can also select an option to read and archive a list of files and directories of a report if a supported Archiver Agent is installed on the client computer and an On Demand Archive Set is configured with SRM enabled.

TO CONFIGURE A NOTIFICATION TO RUN A SCRIPT WHEN A SCHEDULED REPORT HAS RUN:

1.   From the CommCell Browser, click **Reports**, and then click **SRM Report Manager**.

2.   Expand the applicable tree to view your agent. Then select your agent and click a template to display the **Options** window.

3.   Configure the report by specifying clients and columns, report options, and optionally, ad hoc queries.

4.   Click **Schedule** to generate and schedule the report on a daily, weekly, monthly, yearly, or even one time basis.

Optionally, click **Report Options** to repeat sending the report every so many days, or run it for a particular number of times.

Click **Next**.

5. In this dialog, select the report output options, such as:

- **Format** - select **MHTML**, **EXCEL**, or **PDF**.
- Specify a path in **Destination Path** if you want to save the report to a local drive or network share.

Click **Next**.

6. Click the **Run Command** tab and configure this notification type as follows:

- Click **Select [Run Command] for notification**.
- Select either **Run on CommCell** or **Run on Client** to specify where to run the script.
- Click either **Use Local Drive** or **Use Network Share** to specify the location of the script.
- Click **Change...** if you need to provide user account credentials so the script has the correct permissions to run. Specify a Windows User Account with the appropriate privileges to access the scripts directory. User impersonation requires that the specified user have write permissions to the scripts directory; otherwise, the user impersonation account may not take effect. This is especially true if the associated computer is not part of a domain and if the user is not a domain user.
- Click **Browse** or enter a path where the script is located in **Command Script Location**.
- Click **Browse** or enter in arguments in **Arguments** to be passed to the script while running.

Click **Next**.
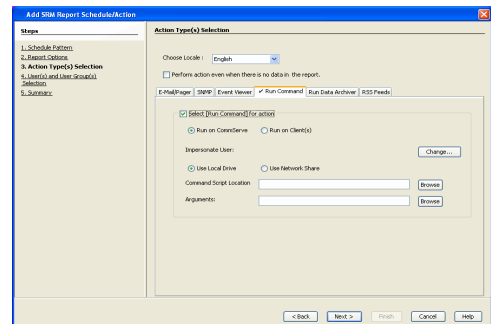
7. Review the summary and if satisfied, click **Finish**.
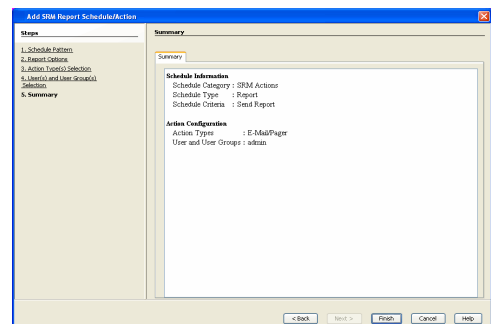
RUN DATA ARCHIVER

A notification can be sent to run a Data Archiver operation when a scheduled report has run. You can select an option to read and archive a list of files and directories of a report if a supported Archiver Agent is installed on the client computer and an On Demand Archive Set is configured with SRM enabled. For the Data Archiver schedule to run successfully, archive rights on the client computer are required.

**TO CONFIGURE A NOTIFICATION TO RUN A DATA ARCHIVER OPERATION WHEN A SCHEDULED REPORT HAS RUN:**

1. From the CommCell Browser, click **Reports**, and then click **SRM Report Manager**.

2. Expand the applicable tree to view your agent. Then select your agent and click a template to display the **Options** window.

3. Configure the report by specifying clients and columns, report options, and optionally,

ad hoc queries.

4. Click **Schedule** to generate and schedule the report on a daily, weekly, monthly, yearly, or even one time basis.

Optionally, click **Report Options** to repeat sending the report every so many days, or run it for a particular number of times.

Click **Next**.

5. In this dialog, select the report output options, such as:
   - **Format** - select **MHTML**, **EXCEL**, or **PDF**.
   - Specify a path in **Destination Path** if you want to save the report to a local drive or network share.

Click **Next**.

6. Click the **Run Data Archiver** tab and configure this notification type by selecting **Run Data Archiver** if a supported Archiver Agent is installed on the client computer and an On Demand Archive Set is configured with SRM enabled. In this case, the list of files and directories of the report will be read and an archive operation will be performed on the default subclient of the archive set.

Click **Next**.
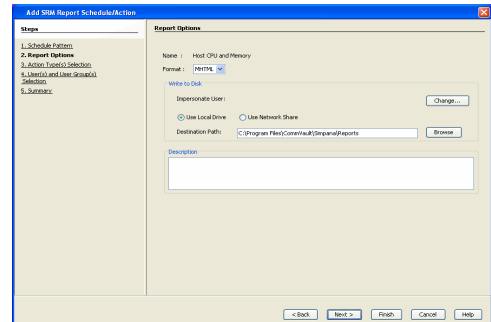
7. Review the summary and if satisfied, click **Finish**.
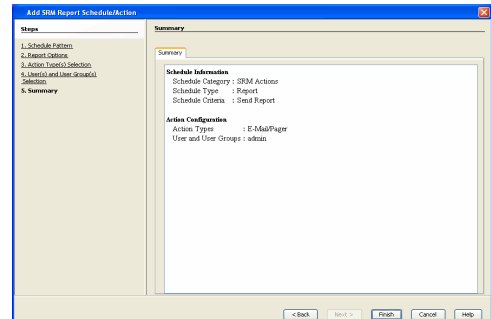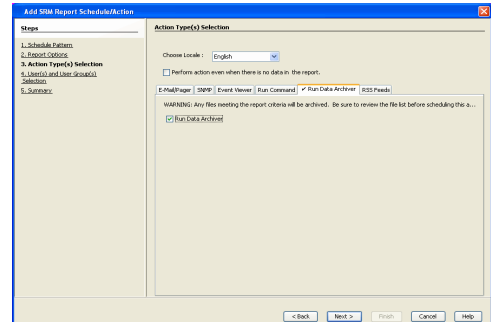
RSS FEEDS

A notification can be sent in a Really Simple Syndication (RSS) feed when a scheduled report has run. The RSS feed can be automatically integrated with your Web Browser.

TO CONFIGURE A RSS FEED NOTIFICATION WHEN A SCHEDULED REPORT HAS RUN:

1. From the CommCell Browser, click **Reports**, and then click **SRM Report Manager**.

2. Expand the applicable tree to view your agent. Then select your agent and click a template to display the **Options** window.

3. Configure the report by specifying clients and columns, report options, and optionally, ad hoc queries.

4. Click **Schedule** to generate and schedule the report on a daily, weekly, monthly, yearly, or even one time basis.

    Optionally, click **Report Options** to repeat sending the report every so many days, or run it for a particular number of times.

    Click **Next**.

5. In this dialog, select the report output options, such as:
    - **Format** - select **MHTML**, **EXCEL**, or **PDF**.
    - Specify a path in **Destination Path** if you want to save the report to a local drive or network share.

    Click **Next**.

6. Click the **RSS Feeds** tab and configure this notification type as follows:
    - Click **Select [RSS Feeds] for notification**.
    - Either accept default format or add more tokens by selecting a token from the pulldown menu and clicking **Add Token**. The tokens are explained in Alert Tokens. Click **Use default message** to revert back to original default format.
    - Specify the feed location in **Select/Enter the Feed Location** field.

    Click **Next**.
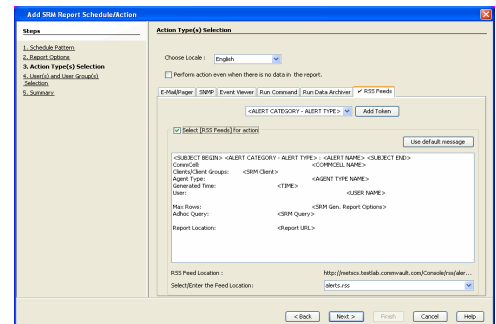
7. Review the summary and if satisfied, click **Finish**.
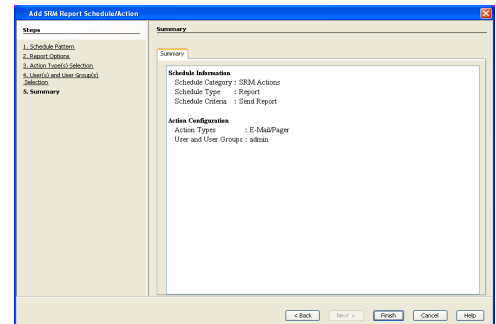
FORECASTING

Forecasting is prediction of data usage in future, based on the usage pattern in the past. Since Prediction allows visualizing data usage in future, it helps make business decisions accordingly. Prediction is available on history reports and it can be done based on Daily/weekly/Monthly data. In the graphs, prediction lines are shown as thin lines while the actual usage is shown as thick lines.

COPY CHART

When viewing a report in the CommCell Console, you can copy any chart to the clipboard in `.bmp` format by right-clicking the chart and selecting **Copy Chart**. This allows you to easily copy a chart into other applications. Note that the Copy Charts function is not compatible with Microsoft WordPad.

CATEGORIES AND COLUMNS

Reports can be used as initial templates or customized by adding or removing columns in the templates or specifying additional Filter Criteria. The following reports support File level Drill Down:

- Capacity by File System
- Current File System Usage
- Current File System Usage by Subclient

The table below lists the available report templates and the categories and columns that can be selected to configure a customized report. The table also shows the job types that are supported by each report.

Category/Column	Description	SRM Windows File System Agent		
		Discovery Job	**Discovery and Analysis Job**	**Agentless SRM**
Client Properties	Displays aspects of the client computer on which the SRM Windows File System Agent is installed.			
Available Memory		X		
Available Memory Percentage		X		
CPU Utilization		X		
Free Disk Percentage		X		
Free Disk Space		X		
Hostname		X		
Memory		X		
Operating System		X		
OS Vendor		X		
OS Version		X		
Processors		X		
Service Pack		X		
SP Version		X		
Time Zone		X		
Total Disk Space		X		
Used Disk Percentage		X		
Used Disk Space		X		
Used Memory		X		
Used Memory Percentage		X		
Data Archive Return on Investment	Displays the disk space saved and the cost saved by using an Archiver Agent.			
Archived File Size			X	
Archived Space Saved			X	
Billable Entity			X	
Cost Saved			X	

	Description				
Stub File Size			X		
Total Cost			X		
Total File Size			X		
Disk Details	Displays aspects of physical disks (e.g., capacity, partitions, space, etc.).				
Allocated Space		X	X	X	
Block Size		X	X	X	
Blocks		X	X	X	
Capacity		X	X	X	
Grown Defects		X	X		
Manufacturer		X	X		
Model		X	X	X	
Partitions		X	X	X	
Primary Defects		X	X	X	
Serial Number		X	X		
Total Defects		X	X	X	
Unallocated Space		X	X	X	
Disk History	Displays how physical disks have been used for a given time period. Useful for trending purposes and to identify disks that are likely to fail soon.				
As Of		X	X		
Grown Defects		X	X		
Primary Defects		X	X		
Total Defects		X	X		
File by Extensions	Displays aspects of each file per extension that is used and the number of files that include each file extension.				
Average File Size		X	X		
Extension		X	X		
Files		X	X		
Max File Size		X	X		
Total File Size		X	X		
File Level Analytic	Displays deeper analysis of files. Selecting **Analysis Job** is required when running data collection job.				
Access Time	Displays last time file was used, e.g., `11/11/2009 17:14`.				
Computer	Displays name of the local host, e.g., `client1`.				
Creation Time	Displays the time the file was originated, e.g., `1/19/2008 4:33`.				
Depth	Displays the number of directories away from the root directory, e.g., `6`.				
Directory	Displays the full path for a directory or file, e.g., `C:\\Windows\\System32\\drivers\\etc`.				
Directory Count	Displays the number of directories within a directory, e.g., `8`.				
Disk	Displays the physical disk, e.g., `\\.\PHYSICALDRIVE0`.				
Extension Name	Displays the extension associated with the file, e.g., `TXT`.				

File	Displays actual name of the file, e.g., `hosts`.			
File Count	Displays the number of files in a directory, e.g., `32`.			
Modification Time	Displays the last changed time, e.g., `9/18/2006 17:37`.			
Partition	Displays the location of the directory/file on the physical disk, e.g., `\\?\Volume{40c1a42b-ce5d-11de-aa5e-806e6f6e6963}\-5cddc2d7)`, `Partition_1, Disk_0`			
Size	Displays the file or directory size (0 MB for directory), e.g., `90.19MB`			
Subclient	Displays the subclient name, e.g., `default`.			
Type	Displays either the directory or file type, e.g., `Directory`.			
User Group Name	Displays the group to which the owner of the file(s) belong, e.g., `Engineering`.			
User Name	Displays the domain\owner of the file, e.g., `BUILTIN\\Administrators`.			
Volume	Displays the drive letter, e.g., `C:\`.			
File Level Analytic Directories	Displays deeper analysis of files. Selecting **Analysis Job** is required when running data collection job.			
Computer				
Directory				
Directory Depth				
Directory File Count				
Directory Name				
Directory Size				
Group Name				
Sub-directory Count				
Total Directories				
Total Files				
User Name				
Volume				
File Level Analytic Files	Displays deeper analysis of files. Selecting **Analysis Job** is required when running data collection job.			
Access Time				
Computer				
Creation Time				
Directory Path				
Extension Name				
File				
Is Stub File				
Modification Time				
Size				
Stub File Space Saved				
User Group Name				
User Group Name				
Volume				
	Displays aspects of files that are shared in the			

File Shares	network.			
Allocated Space		**X**	**X**	**X**
Free Space		**X**	**X**	**X**
Owner		**X**	**X**	**X**
Path Name		**X**	**X**	**X**
Protocol		**X**	**X**	**X**
Share Name		**X**	**X**	**X**
File System File Distribution by Access Time	Displays file statistics and average size of files, total file size, and type by access time.			
Average File Size			**X**	
Files			**X**	
Total File Size			**X**	
Type			**X**	
File System File Distribution by Modification Time	Displays file statistics and average size of files, total file size, and type by modification time.			
Average File Size			**X**	
Files			**X**	
Total File Size			**X**	
Type			**X**	
File System File Distribution by Size	Displays file statistics and average size of files, total file size, and type by size.			
Average File Size			**X**	
Files			**X**	
Total File Size			**X**	
Type			**X**	
File System File Distribution by Type	Displays file statistics and average size of files, total file size, and type by type.			
Average File Size			**X**	
Files			**X**	
Total File Size			**X**	
Type			**X**	
File System Usage	Displays file statistics and how the files are stored and organized in the file system.			
Average File Size			**X**	
Average Files per Directory			**X**	
Average Tree Depth			**X**	
Compressed Files			**X**	
Directories			**X**	
Encrypted Files			**X**	
Files			**X**	
Max File Size			**X**	
Maximum Tree Depth			**X**	
Migrated Space Saved			**X**	
Sparse File Count			**X**	
File System Usage History	Displays overall file system statistics. Useful for trending purposes.			
As Of		**X**	**X**	**X**

Percent Used		**X**	**X**	**X**
Used Space		**X**	**X**	**X**
Installed Software	Summarizes software installed on Windows File System clients in the SRM cell. Useful for troubleshooting installation or licensing problems.			
Package		**X**	**X**	**X**
Vendor		**X**	**X**	**X**
Version		**X**	**X**	**X**
Largest Files	Displays properties of largest files (e.g., name, owner, size).			
Largest File Accessed		**X**	**X**	**X**
Largest File Created		**X**	**X**	**X**
Largest File Group		**X**	**X**	**X**
Largest File Modified		**X**	**X**	
Largest File Name		**X**	**X**	
Largest File Owner		**X**	**X**	
Largest File Size		**X**	**X**	
Least Recently Used Files	Displays properties of least recently used files (e.g., name, owner, size).			
Least Recently Used File Accessed		**X**	**X**	**X**
Least Recently Used File Created		**X**	**X**	**X**
Least Recently Used File Group		**X**	**X**	**X**
Least Recently Used File Modified		**X**	**X**	
Least Recently Used File Name		**X**	**X**	
Least Recently Used File Owner		**X**	**X**	
Least Recently Used File Size		**X**	**X**	
Microsoft Exchange PST File	Displays aspects of PST (personal storage) files created by Microsoft Outlook.			
Accessed			**X**	
Created			**X**	
Group			**X**	
Modified			**X**	
Name			**X**	
Owner			**X**	
Size			**X**	
Oldest Files	Displays properties of oldest files (e.g., name, owner, size).			
Oldest File Accessed		**X**	**X**	**X**
Oldest File Created		**X**	**X**	**X**
Oldest File Group		**X**	**X**	**X**
Oldest File Modified		**X**	**X**	
Oldest File Name		**X**	**X**	
Oldest File Owner		**X**	**X**	
Oldest File Size		**X**	**X**	
Partition Details	Summarizes aspects of each partition of the file system.			
Blocks		**X**	**X**	**X**
Capacity		**X**	**X**	**X**

Type		**X**	**X**	**X**
Process Information	Displays aspects of the client computer on which the SRM Windows File System Agent is installed.			
Base Priority		**X**		
CPU Time		**X**		
CPU Usage		**X**		
GDI Objects		**X**		
Handles		**X**		
Image Name		**X**		
IO Other		**X**		
IO Other Bytes		**X**		
IO Read Bytes		**X**		
IO Reads		**X**		
IO Write Bytes		**X**		
IO Writes		**X**		
Memory Usage		**X**		
Memory Usage Delta		**X**		
Non-paged Pool		**X**		
Page Faults		**X**		
Page Faults Delta		**X**		
Paged Pool		**X**		
Peak memory Usage		**X**		
PID		**X**		
Session ID		**X**		
Threads		**X**		
User Name		**X**		
User Objects		**X**		
Virtual Memory Size		**X**		
Prohibited Files	Displays aspects of files that are not allowed (or forbidden) in the Windows file system.			
Accessed			**X**	
Created			**X**	
Group			**X**	
Modified			**X**	
Name			**X**	
Owner			**X**	
Size			**X**	
Services	Displays service names running on the client computer and their current state.			
Log On		**X**		
Name		**X**		
Startup Type		**X**		
State		**X**		
Software Activity	Displays activity such as when software packages was installed or removed and details of the software package.			
Date		**X**	**X**	**X**

			X	
Package Name		X	X	X
Type		X	X	X
Vendor Name		X	X	X
Version		X	X	X
Software Instances			X	
Instances		X	X	X
Name		X	X	X
Vendor		X	X	X
Subclient File Distribution by Access Time	Displays file statistics and average size of files per subclient, such as total file size, and type by access time.			
Average File Size			X	
Files			X	
Total File Size			X	
Type			X	
Subclient File Distribution by Modification Time	Displays file statistics and average size of files per subclient, such as total file size, and type by modification time.			
Average File Size			X	
Files			X	
Total File Size			X	
Type			X	
Subclient File Distribution by Size	Displays file statistics and average size of files per subclient, such as total file size, and type by size.			
Average File Size			X	
Files			X	
Total File Size			X	
Type			X	
Subclient File Distribution by Type	Displays file statistics and average size of files per subclient, such as total file size, and type by type.			
Average File Size			X	
Files			X	
Total File Size			X	
Type			X	
Version		X	X	X
Subclient Usage	Displays Calypso subclient (the logical entity that uniquely defines a unit of data on a client computer) information.			
Average File Size			X	
Average Files per Directory			X	
Average Tree Depth			X	
Compressed Files			X	
Directories			X	
Encrypted Files			X	
Files			X	
Maximum File Size			X	
Maximum Tree Depth			X	

Migrated Space Saved			**X**	
Sparse File Count			**X**	
Total File System Usage by User	Displays file information by individual user. Useful to identify the major consumers of storage for capacity management and planning purposes.			
Average File Size			**X**	
Files			**X**	
Max File Size			**X**	
Name			**X**	
Total File Size			**X**	
User Group Violations	Displays disk space violations per user to help enforce corporate storage usage policies.			
Disk Space Hard Limit		**X**	**X**	**X**
Disk Space Soft Limit		**X**	**X**	**X**
User Group Name		**X**	**X**	**X**
Violation Used Disk Space		**X**	**X**	**X**
User Usage	Displays a summary of files used and their size (average, maximum, total) per user name.			
Average File Size			**X**	
Files			**X**	
Maximum File Size			**X**	
Total File Size			**X**	
User Name			**X**	
User Violations	Displays quota violations per user to help enforce corporate storage usage policies. FSRM columns report Windows 2008 R2 File System Resource Manager (FSRM) information.			
Block Count Hard Limit		**X**	**X**	**X**
Block Count Soft Limit		**X**	**X**	**X**
FSRM Quota Path		**X**	**X**	**X**
FSRM Quota Type		**X**	**X**	**X**
FSRM Space Limit		**X**	**X**	**X**
FSRM Template		**X**	**X**	**X**
FSRM Used Block Count		**X**	**X**	**X**
Used Block Count		**X**	**X**	**X**
User Name		**X**	**X**	**X**
Volume Details	Displays aspects of each volume (a single accessible storage area with a single file system) to help identify heavy disk consumers for capacity management and planning purposes.			
Free Space		**X**	**X**	**X**
Percent Free		**X**	**X**	**X**
Percent Used		**X**	**X**	**X**
Total Space		**X**	**X**	**X**
Type		**X**	**X**	**X**
Used Space		**X**	**X**	**X**
Windows Entities	Displays overall aspects per each computer selected (e.g., computer name, host group, etc.).			
Client Computer Group		**X**	**X**	**X**

Computer		**x**	**x**	**x**
Disk		**x**	**x**	**x**
Partition		**x**	**x**	**x**
Subclient			**x**	
Volume		**x**	**x**	**x**

COST HISTORY AND USAGE HISTORY REPORTS

Data for the Cost History and Usage History reports (e.g., Cost History by Application, Usage History by Application) is compiled at regular intervals by a background process on the SRM Server. The default interval is one week, which means the Cost History reports will show one data point per week, no matter how often data collection is scheduled for them; thus, data collection for these reports should be synchronized to the summary interval. You can configure the interval by selecting **SRM Options** in the **Control Panel**.

For a newly installed SRM Server, no data will appear in these reports until either the default interval, or a user-specified interval has elapsed from the time of installation, at which time the first summary process will run, and data will be available for these reports.

TO RUN A COST ANALYSIS REPORT:

1. From the CommCell Browser, click **Reports**, and then click **SRM Report Manager**.

2. Click **Enterprise**. Then click **Cost Analysis** to display several out-of-the-box templates. Click on a template to get started.

3. For an out-of-the-box template, the columns are displayed here. To change the columns, select a category and click **Add** or **Remove** to move the columns between the **Available** and **Selected** boxes. Clicking **Remove All** will remove all previously selected filters for the reports.

4. Optionally, click the **Report Options** tab and specify options as explained in Report Options.

5. Optionally, click the **Adhoc Query** tab and configure an ad hoc query as explained in Ad Hoc SQL Query.
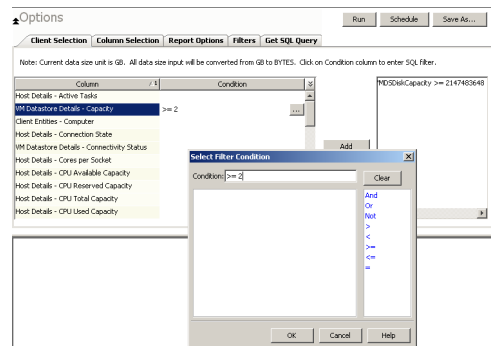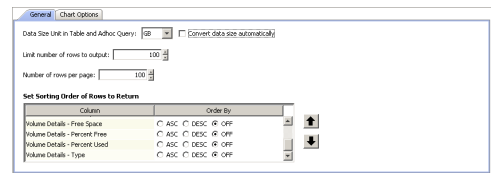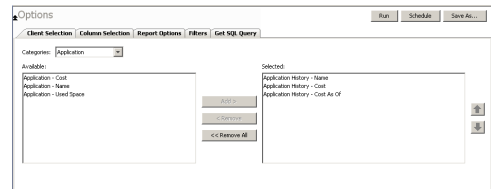
6. Click **Run** to generate the report immediately and view the results.

Back to Top

SRM for Windows File System - Reports

| Basic | Advanced | Filters | Summaries | SRM Archiver Integration | FAQ |

TABLE OF CONTENTS

Overview

Generate a Report with Filters

Examples of Queries used in filters
  Operators Explained

OVERVIEW

Customized queries can be applied as additional reporting filters to retrieve specific SRM information from the clients and client groups in your CommCell. These queries are extremely useful if the provided report filters (clients, columns) do not provide the necessary data required for your environment. For example, you could apply SQL query filters to the `Allocated Space` column to display disks of a certain size, such as 2 GB. This ad hoc query further refines and filters the data to facilitate management of your storage infrastructure.

More examples of why you may want to use filters for SQL queries include:

- You wish to generate a list of users who consume more than 10 MB of disk space.
- You want so see how much space is consumed by Exchange mailboxes on particular clients.
- You need to see a list of volumes on a NAS filer that exceed 5 TB of space.

Since the query will run against the CommServe database to retrieve the requested SRM data, which can be easily configured from the CommCell Console when specifying filter criteria of an SRM report. Any SQL query that is supported by a SQL Server can be used in Filters for SRM reporting. If desired, once the conditions have been defined, you can retrieve the full SQL query for use in third-party applications.

GENERATE A REPORT WITH FILTERS

Filters in the form of SQL queries can be defined during the configuration of an SRM report. You can add a SQL query to the report to filter additional data for a specified column. To configure a report with filters, you must complete the following:

1. Select the type of SRM report you wish to generate. An SRM report can be selected from the SRM Report Manager node.
2. Determine which client(s) and client computer group(s) from which you wish to collect data.
3. Determine and select the type of data to collect for the report (filtering).
4. Define the conditions for the SQL query. Queries that include strings are case-sensitive.
5. Generate the report.
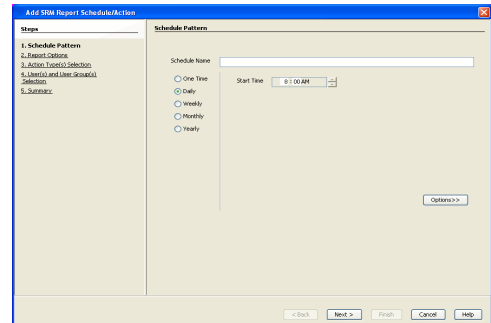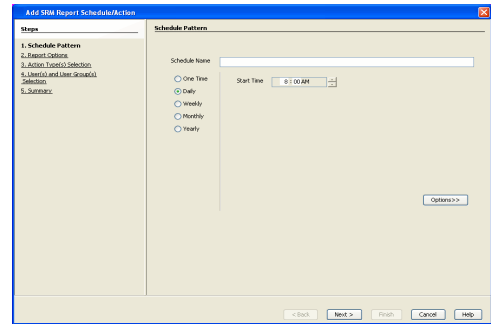
TO GENERATE A REPORT WITH FILTERS:

1. From the CommCell Browser, click **Reports**, and then click **SRM Report Manager**.

2. Expand the applicable tree to view your agent. Then select your agent and click a template to display the **Options** window.

3. Click the **Client Selection** tab and select the client computers or client computer group. This is a required step.
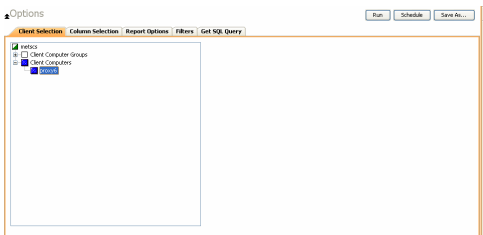
4. Click **Column Selection** tab.

   Select a category and **Add** or **Remove** columns between the Available and Selected boxes. The categories and columns differ for each type of report. Clicking **Remove All** will remove all previously selected filters for the reports.
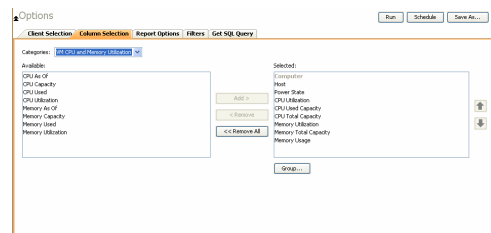
5. Click the **Report Options** tab to configure settings in the report. Click the **General** tab to:

- Set the time range of the report.
- Enable forecasting by clicking **Include Trending** and specifying default trending interval and number of data points on which the trending interval is based.
- Enter the **Maximum number of Bar Points per chart** or select **Draw All Bar Points**.
- Either accept the default of 100 rows or increase or decrease the rows to display in the report by specifying a number in the **Limit number of rows to output** field.
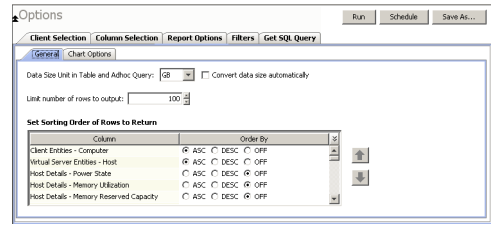
Click the **Advanced** tab to:

- Set the **Data Size Unit** to **GB** for the tables.
- Set the Sorting order of the columns in either ascending or descending order or no sorting order.

6. Select **Filters** tab to run real-time SQL queries can also be applied to the data to provide further filtering.

- Select a column in which you want to specify a condition (e.g., **VM Datastore Details - Capacity**) and click the **Conditions** field of Free Space and then click the ellipsis ⋯ button.
- In the **Select Filter Condition** dialog box, double-click the operator and in the **Condition** field, enter the values of the condition, such as **>2** and click **OK**.
- Click **Add**.
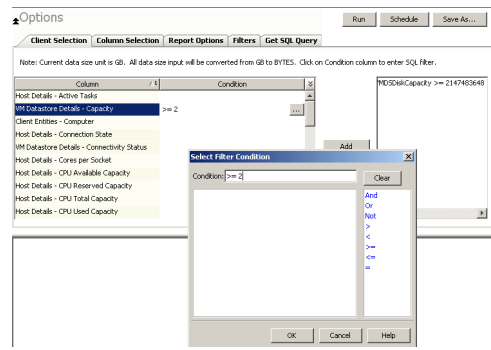
See Examples of Queries used in filters for an explanation of the operators.

7.
- The full SQL query can be generated if necessary after adding the condition and selecting the **Get SQL Query** tab.
- The query that is displayed is Read-only and can be used in a third-party application, such as SQL Server Management Studio and used there to collect and report data.
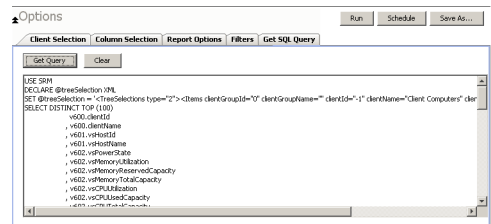
8. Generate or save the report with one of these options:

- Click **Run** to generate the report immediately and view the results in the CommCell Console.
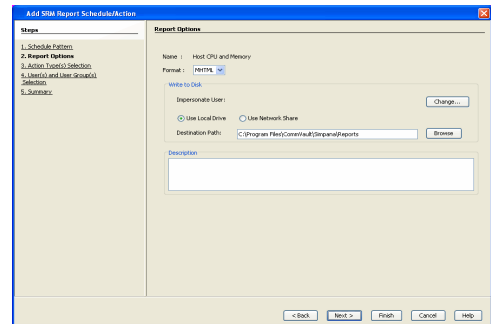- Click **Schedule** to generate and schedule the report on a daily, weekly, monthly, yearly, or even one time basis. Specify the report language (see Languages - Support for the list of languages supported in Reports), format (HTML, EXCEL, PDF), and location. Optionally, notifications can be configured so the report can be emailed, sent to an SNMP trap, or RSS feed, etc.

  When scheduling, patterns can also be applied to the report so it runs on a specific time, repeated every so many days, or run for a particular number of times. Some reports allow enabling Forecasting by specifying default trending interval and number of data points on which the trending interval is based.

- Click **Save As...** to save the report filter criteria, schedule information, notifications to a template so it can be used to generate a report at a later date. All report templates are saved under **My Reports**.

EXAMPLES OF QUERIES USED IN FILTERS

The sections below explain the operators than can be used in a SQL query as well as real-world examples describing why and how to specify the condition and build the query.

OPERATORS EXPLAINED

The following explains the operators that can be used in filters using SQL queries. Examples for each are provided. Queries that include strings are case-sensitive.

OPERATOR	DESCRIPTION	EXAMPLE
And	Is a binary operator that operates on two *operands* (data that is manipulated by the operator). Works with both numeric and string queries. Displays a result if both operands are TRUE and no result is displayed if either is FALSE.	Display a computer group that starts with B and ends with M (e.g., Birmingham). 1. Select `Client Computer Group` column.

		2. Enter this query: `Starts With B And Ends With M`
Or	Is a binary operator that operates on two *operands* (data that is manipulated by the operator). Works with both numeric and string queries. Displays a result if either operand is TRUE and no result is displayed if both are FALSE.	Display a computer that starts with B or starts with M (e.g., Birmingham, Milwaukee). 1. Select `Computer` column. 2. Enter this query: `Starts With B Or Starts With M`
Not	An operation on logical values that changes true to false, and false to true. The NOT operator inverts the result of a comparison expression or a logical expression. The specified condition must be false in order to view a result. Example: Display a computer that does not have less that < 4 GB of used space. Therefore, only computers with 4 or more GB of used space will be displayed.	Display a computer that does not have less that < 4 GB of used space. 1.Click **Report Options** tab and set data size unit to GB. 2. Select `Used Space` column. 3. Enter this query: `Not < 4`
Like	The LIKE operator is used in character string comparisons with pattern matching. It can contain the special wild-card pattern matching characters percent -- '%' and underscore -- '_'. Underscore matches any *single* character. Percent matches zero or more characters.	Display a computer that contains `eng` characters in its name to identify computers in the engineering department. 1. Select `Computer` column. 2. Enter this query: `%eng%`
Starts With	The Starts With operator is used in character string comparisons with pattern matching.	All names of computers in the engineering department use the convention of `eng_`. Display all computers that start with E to list computers in the engineering department. 1. Select `Computer` column. 2. Enter this query: `Starts With E`
Ends With	The Ends With operator is used in character string comparisons with pattern matching.	All names of computers in the System Test department use the convention of `system_test`. Display a computer that ends with T to list computers in the system_test department. 1. Select `Computer` column. 2. Enter this query: `Ends With T`
> (Greater Than)	A comparison operator that tests whether two expressions are the same. Works with only numeric queries.	Display file sizes that are larger than 2 GB. 1. Click **Report Options** tab and set data size unit to GB. 2. Select `Maximum Size` column. 3. Enter this query: `> 2`
< (Less Than)	A comparison operator that tests whether two expressions are the same. Works with only numeric queries.	Display file sizes that are less than 4 GB. 1. Click **Report Options** tab and set data size unit to GB. 2. Select `Maximum Size` column. 3. Enter this query: `< 4`
>= (Greater Than or Equal To)	A comparison operator that tests whether two expressions are the same. Works with only numeric queries.	Display file sizes that are greater than or equal to 2 TB. 1. Click **Report Options** tab and set data size unit to TB. 2. Select `Maximum Size` column. 3. Enter this query: `>= 2`
<=(Less Than or Equal To)	A comparison operator that tests whether two expressions are the same. Works with only numeric queries.	Display computers with less than or equal to 1 GB free space.

		1. Click **Report Options** tab and set data size unit to GB. 2. Select `Free Space` column. 3. Enter this query: `<= 1`
= (Equal)	The equals comparison operator compares two values for equality. Works with both numeric and string queries.	Display files that are located in the /usr/bin directory. 1. Select `Path` column. 2. Enter this query: `=/usr/bin`

RULES TO FOLLOW

When constructing a filter using SQL query, adhere to these rules:

- Queries that include strings are case-sensitive.

- When a string has a space, enclose it with double quotes. For example, enter "`Program Files`".

Back to Top

SRM for Windows File System - Summaries

| Basic | Advanced | Filters | Summaries | SRM Archiver Integration | FAQ |

TABLE OF CONTENTS

OVERVIEW

SRM Windows File System Agent Summaries provide a concise view of the status of SRM Windows File System entities in the CommCell Console. The status information includes the resource, memory, and CPU usage, as well as other resource-related information. Summary information is provided as images in the form of bar graphs and pie charts to provide a succinct snapshot of the statistical information. While viewing summary, data rows in tables can be sorted by any one of the columns listed in that summary.

When you select a SRM Windows File System entity from the CommCell Console, its summary information appears in the main window. Each section can be expanded or collapsed as desired.

REAL-TIME MONITORING

Critical information that rapidly changes is automatically collected and updated every 15 minutes by the Bull Calypso Communications Service.

All information of a summary, such as CPU Utilization, Memory Utilization, etc. is collected and updated by this Service.

If necessary, you can modify the number of minutes between collections using the nREFRESH_INTERVAL_MINUTES registry key, however it is not recommended as it alters the rate of data collection, which may impact performance.

The following section describes the available summary types of SRM Windows File System Agent:

SOFTWARE INSTANCES/PROCESS INFORMATION/SERVICES

Summary information at the client level shows statistical data for the following:

- **Software Instances**

  The summary information for software instances displays details like Package, version and vendor name of all instances of the installed software.

- **Process Information**

  The summary information for processes displays details like Image Name, PID, Session ID, CPU Time, CPU Usage, Memory Usage, User Name, etc for each process that runs on the client.

- **Services**

  The summary information for services displays details like Name, State, Startup Type, and Log on information for each service that exists on the client.

FILE SYSTEM USAGE

Summary at the defaultBackupSet level or the subclient level display charts and tables for **File System Usage by Subclient.** This tables displays details like Name, Average Tree Depth, Maximum File Size, Sparse File Count, Compressed Files, etc for the defaultBackupSet.

1. From the CommCell Console, select the Client Computer with SRM Windows File System Agent for which you want to view summaries.
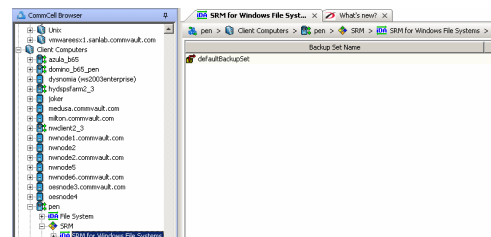
2. Expand **SRM** and select **SRM Agent for Windows File System**, then select

defaultBackupSet/Subclient.

3. The associated **defaultBackupSet** or **Subclient Summary** will appear in the main window.
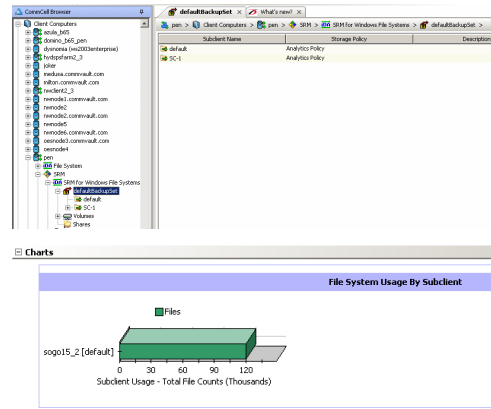
DISTRIBUTION

At the user defined or default Subclient level **Properties** showing physical information including name, state (enabled or disabled) last modification time and last analysis times, etc. are displayed along with Charts. The SRM Windows File System Agent at this level displays charts for **File Distribution by Size**, **File Distribution by Type**, **File Distribution by Access Time** and **File Distribution by Modification Time**.

1. From the CommCell Console, select the Client Computer with SRM Windows File System Agent for which you want to view summaries.

2. Expand **SRM** and select **SRM Agent for Windows File System**, then select **Subclients**.

3. The associated **Subclient Summary** will appear in the main window.
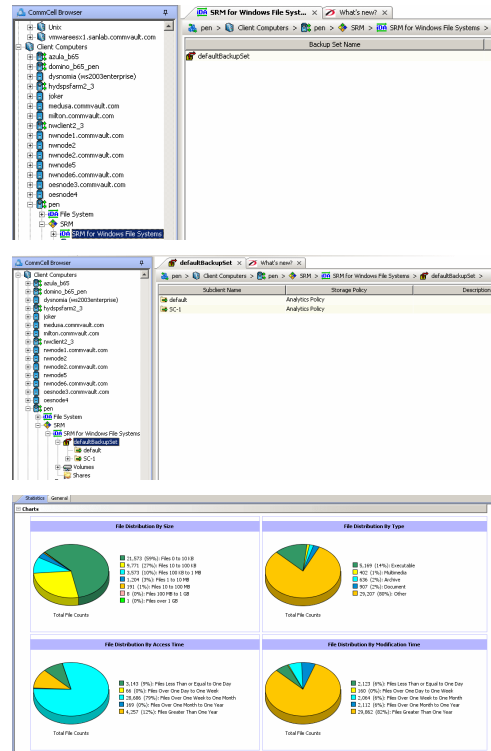
VOLUMES

Summary information at the Volumes level include charts for **File Count** and **File System Capacity.**

Each volume in turn displays charts for **File System Usage by Size**, **File System Usage by Type**, **File System Usage by Access Time**, **File System Usage by Modification Time** and **File System Usage History**. Advisories with severity level, the time stamp, and a brief description are also displayed along with charts at this level.

1. From the CommCell Console, select the Client Computer with SRM Windows File System Agent for which you want to view summaries.

2. Expand **SRM** and select **SRM Agent for Windows File System**, then select **Volume**.

3. The associated **Volume Summary** will appear in the main window.
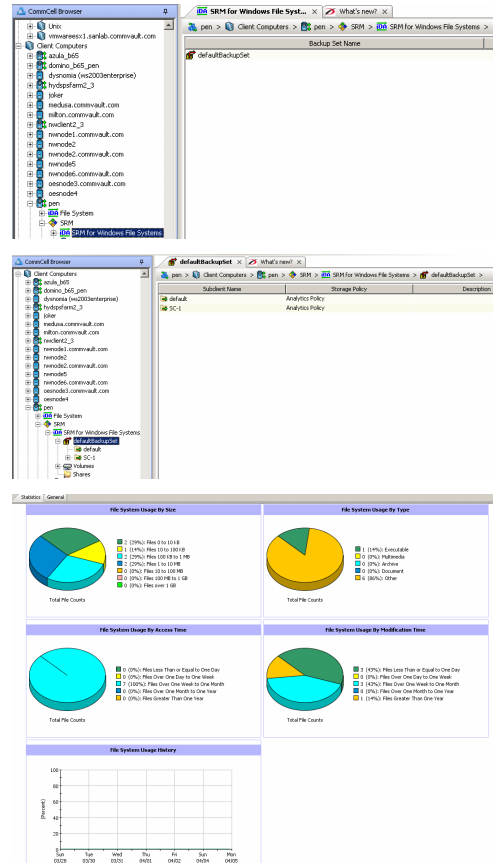
SHARES

Summary information include tables displaying Table Name, Path Name, Used Space and Protocol for the selected share.

STORAGE DEVICES

Summary information at the Storage Devices level include charts for **Allocated Vs Unallocated space per disk.** Each Physical Drive in turn displays charts for **Partition Capacity.** Physical properties like Name, Interface, Manufacturer, Block, Count , etc. are also displayed at this level.

1. From the CommCell Console, select the Client Computer with SRM Windows File System Agent for which you want to view summaries.

2. Expand **SRM** and select **Storage Devices**.

3. The associated **Storage Devices Summary** will appear in the main window.
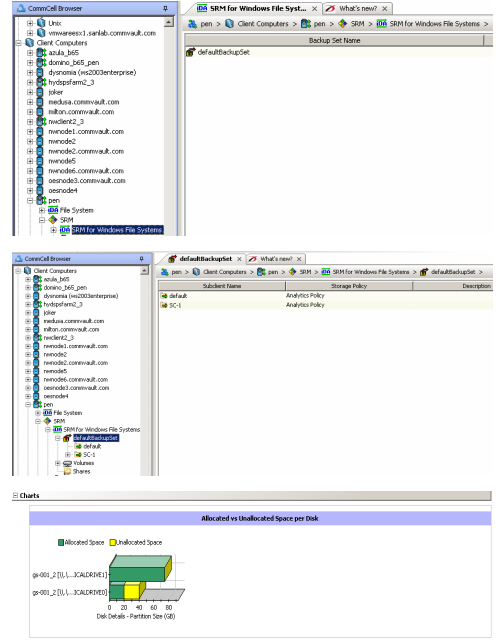
Back to Top

SRM for Windows File System - Reports

| Basic | Advanced | Filters | Summaries | SRM Archiver Integration | FAQ |

TABLE OF CONTENTS

Overview

Prerequisites

Configuration
  Archive Files Using SRM Reports
  Recover Archived Files

OVERVIEW

Archiver Integration with SRM is a powerful feature that allows you to define some very specific rules for archiving specific files and directories. It combines the powerful SRM Reporting capability with Schedule Actions to initiate archive operations. **Run Data Archiver** is one of the actions available when scheduling SRM Reports that can be used for Archiving specific data. This can further be set using Filters to select only the files that need to be sent for Archiving.

SRM Archiver Integration provide the following features:

- Specific files can be targeted for archiving
- Archive operations can be scheduled on a periodic basis
- Filters can be applied to further refine the file lists to be submitted for archiving
- Saves space for more recent files
- Helps segregating and later retrieving files of a particular type or from a particular time stamp

PREREQUISITES

1. The following Agents must be installed before Archiver operations can be run using SRM Reports Notification:

    - SRM Windows File System Agent - File Level Analytics must be selected for the subclient and a Data Collection job must be run.
    - File Archiver for Windows Agent - an On Demand Archive set must also be configured on the Agent.

2. The User initiating this job must have archive rights on the client computer.

CONFIGURATION

ARCHIVE FILES USING SRM REPORTS

1.
    Locate the correct client computer node that has both Windows File System
    *i*DataAgent and File Archiver for Windows Agent installed in the CommCell Browser.

2.
    In the File Archiver for Windows Agent, create a Local File System Instance.

    Right-click the File Archiver agent; select **All Tasks** > **Create Instance** > **Local File System.**
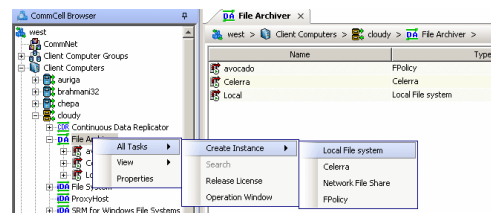
3. Create an On Demand Archive set within a Local File System Instance.

    Right-click the Agent and click **All Tasks** and then click **New On Demand Archive Set**.
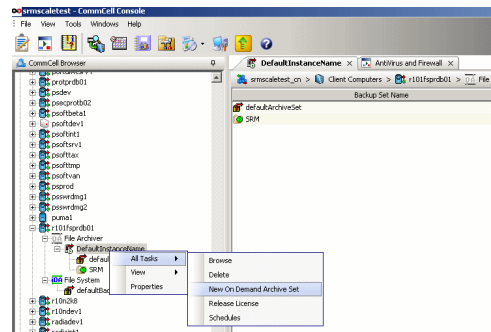
4. From the **Create New On Demand Archive Set** dialog box, enter a **New Archive Set Name** (up to 32 characters) of the archive set that you want to create and associate a storage policy with the default subclient by selecting one from the Storage Policies drop-down list.
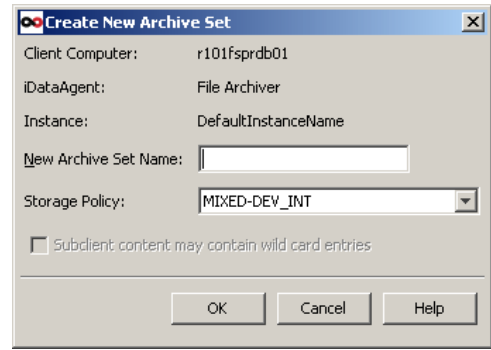
5. Right click the subclient and click **Properties**, from the **General** tab of the Subclient Properties dialog box select **Use content file provided by SRM**. When done, click **OK** to continue.
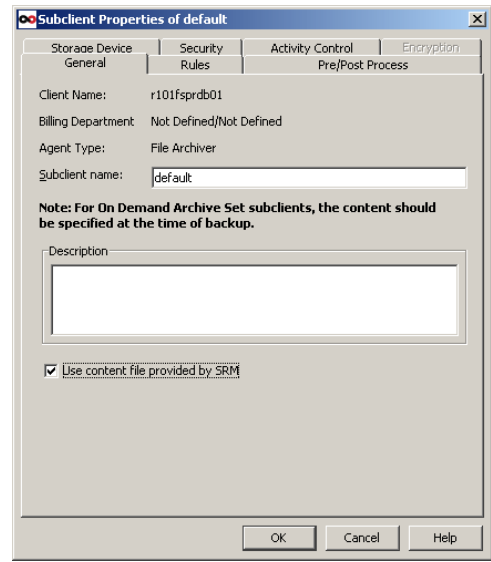
6. In the Windows File System *i*DataAgent, enable SRM and File Level Analytics and run a full backup.

Right-click the Agent and select Properties.

From the **General** tab, select **Enable SRM feature** and click **OK**.
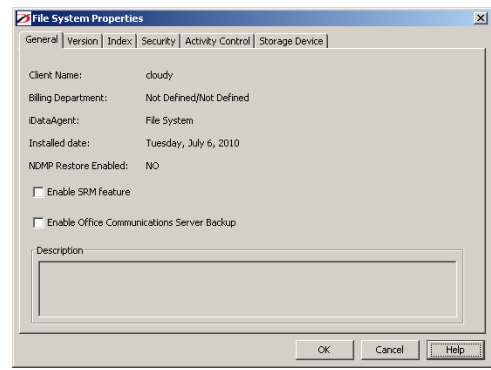
Navigate to the Subclient level and select **Subclient Properties** by right clicking the Subclient.

In the **SRM Options** tab **Discovery** is automatically selected. For detailed reporting with file level details select **Discovery and Analysis** with **File Level Analytics** then click **OK**.

> File Level Analytics increases the rate at which the SRM database grows, use additional filtering options provided in this dialog to further narrow the scope and match the files that meet your specific archive requirements.

7. Right-click the subclient, and click **Backup**.

    From the Backup Options select backup type as **Full**.

    From job Initiation, select **Immediate** and confirm your changes by selecting **OK**.
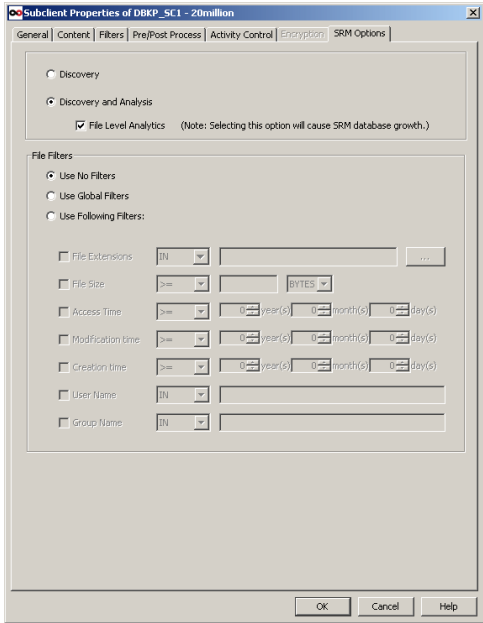
8. From the CommCell Browser, expand **Reports**, and then click **SRM Report Manager**.

    For creating SRM Report Action you must have permissions to perform data protection/management operations on the clients selected.
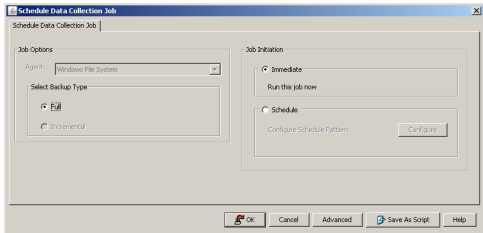
9. Expand **File Systems>Windows>File Level Analytics** and select one of the following templates to display the Filters window.

    ● **File Level Analytics Directories** - selecting this template will archive all files within a directory.
    ● **File Level Analytics Files** - selecting this template will archive selected files.
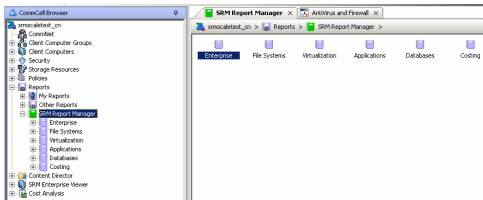
10. Click the **Client Selection** tab and select the client computers that have both the Windows File System *i*DataAgent and File Archiver for Windows Agent installed and configured.
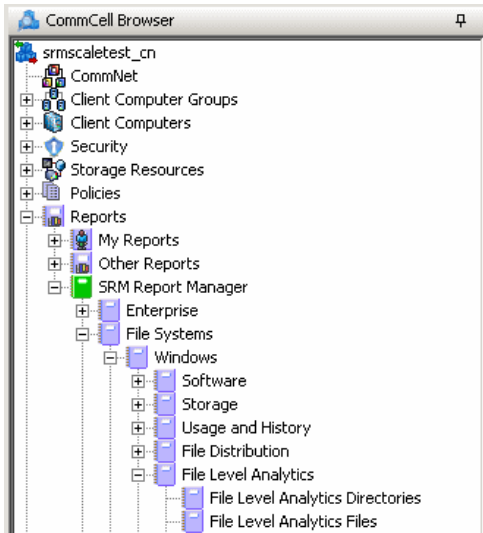
11. Click **Column Selection** tab. For the selected template, the columns are displayed here. To change the columns, select a category and click **Add** or **Remove** to move the columns between the **Available** and **Selected** boxes.
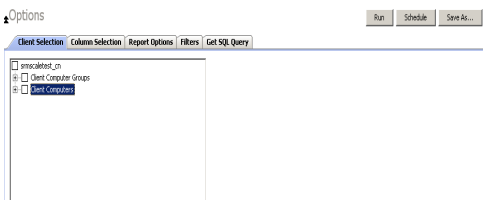
12. Click the **Report Options** tab and select the **General or Advanced tab** to modify any options.
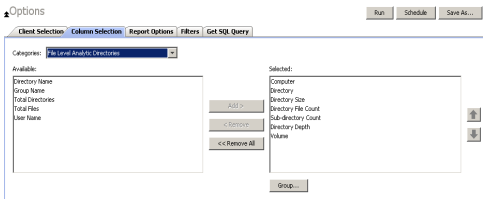
13. Click the **Filters** tab to apply a SQL Query to further refine the data in the report e.g.

```
Modification Time < '06/01/2007'

Size > 1024
```
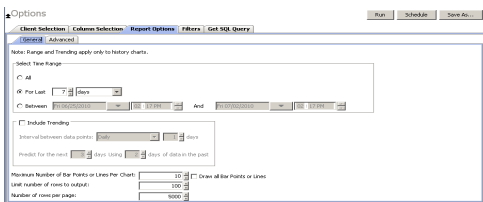

14. Select the **Get SQL Query** tab to display this query in long notation (that will be used to get the data and generate the report).
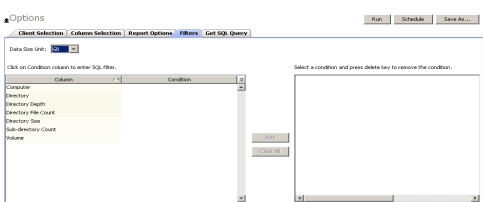
> Run the report and review the file list before scheduling them for archiving to make sure you are satisfied with the selections.

15. Click **Schedule** to generate and schedule the report on a daily, weekly, monthly, yearly, or even one time basis.

Optionally, click **Options** to repeat sending the report every so many days, or run it for a particular number of times.
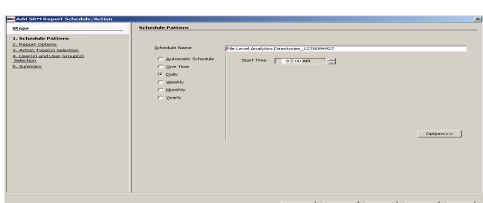
Click **Next**.

16. In **Report Options - Format**, select **MHTML**, **EXCEL**, or **PDF**. Specify a path in **Destination Path** if you want to save the report to a local drive or network share and click **Next**.
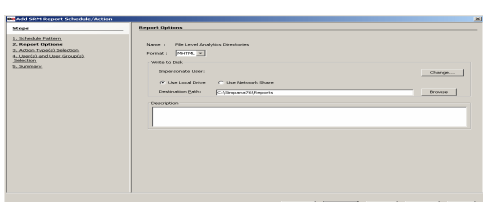
17. In **Action Type(s) Selection** dialog, configure the Run Data Archiver as an Action for the scheduled report by selecting **Run Data Archiver** option.
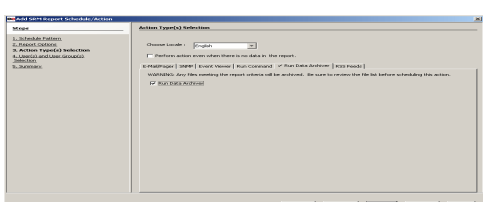
Review your selection and click **Finish**.

18. If scheduled, the **SRM Archiver** activity can be **Run Immediately** from within **CommCell Console** using **Scheduler**.

19. **SRM Report** operation will complete followed by the **Archiver** operation.

20. To view files that have been archived follow steps above for configuring the File Level Analytics reports and include **Is Stub File** and **Stub File Space Saved** columns before running the report.

21. In addition stubbed files can be viewed in Windows explorer with archive icon and Offline attribute.
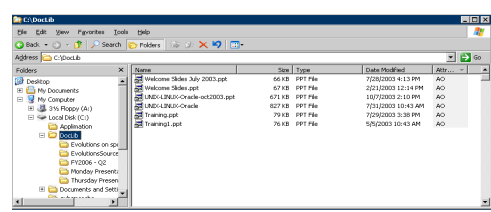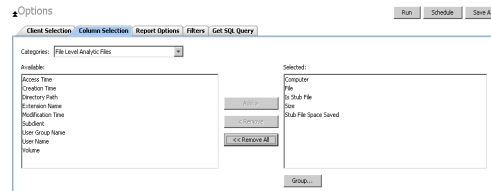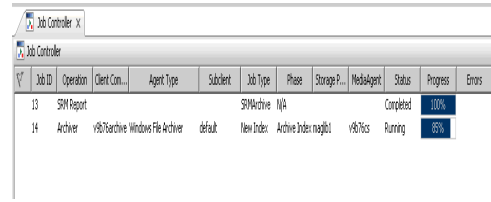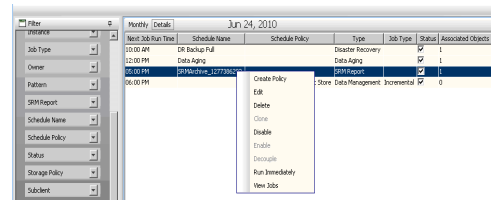
RECOVER ARCHIVED FILES

1. To recover files from within the CommCell Console, right click on the **OnDemand Archive Set** and select **View > Archiving History**.

From the **Archive History Filter,** choose the **Job Status** and set required values in **Specify Time Range** section then click **OK**.
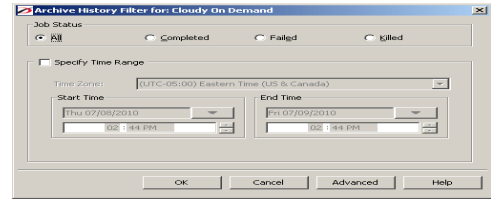
2. From the Archive Job History of OnDemand Archive Set right-click the job(s) from which you need to recover archived files and select **Browse.**

From the **Browse Options** dialog select defaults or make changes as needed and click **OK**.
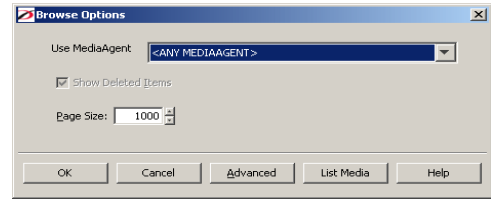
3. From the Client section select any/all files to recover, and click on **Recover All Selected**.
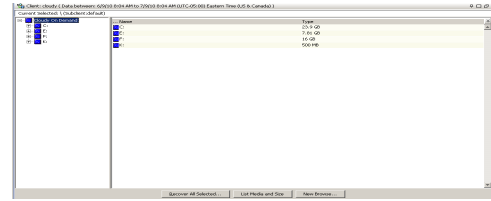
4. The Recover Options dialog pops up, accept the defaults or make necessary changes in this dialog and click **OK** when done.

In the Job Controller tab the Recovery job will run through completion.
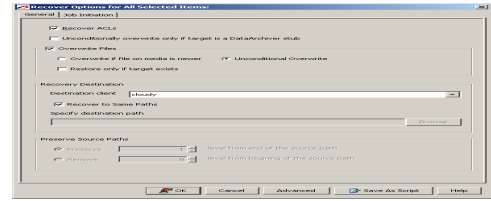
Agent Properties (General)

Use the Agent Properties (General) tab to obtain or provide general and/or user account information for the agent. Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent for which the information is being displayed.

Client (Computer, Name)

Displays the name of the client computer or application server.

Billing Department

Displays the name of the billing department, when the Agent is associated with a billing department. For more information on Billing and Costing See the *CommNet Books Online*.

*i*DataAgent/Agent (Type)

Displays the identity of the agent that is installed on the client computer or application server.

Installed (date)

Displays the date on which the agent was installed or upgraded on the client computer or application server.

Auto Discover Instances

If selected during installation, this option will also be selected at the Agent level after the install is complete. When selected, instances are automatically discovered every 24 hours; or whenever the Communications Service (GxCVD) service is restarted. The default every 24 hours timing can be overridden with the nAutoDiscoverSQLInstanceTimeout registry key.

> For Express installations, an option does not appear during installation but instances are automatically discovered. By default, this option is automatically selected at the Agent level.

Manage Content Automatically

When selected, SQL databases that were automatically discovered but later deleted from an application (e.g., SQL Server) will be automatically deleted from the content of the default subclient when the next backup is run. This alleviates having to delete the databases manually. Databases that are manually added and later deleted from an application are not automatically removed from the subclient when the next backup runs and the backup job will complete with errors. By default, this is selected after client install or upgrade.

Enable Instance Discovery

When selected, instances are automatically discovered every 168 hours (one week) by default or whenever the Communications Service (GxCVD) service is restarted. The default 168 hour (one week) timing can be overridden with the nORACLEINSTANCEDISCOVERYINTERVAL registry key.

Stub Recovery Parameters

Specifies whether to enable recall throttling for stub recovery jobs. Selecting this option will allow you to control the number of stub recovery jobs that can be run based on the limits set below. When these options are disabled in the CommCell Console, the system will apply any legacy registry key settings corresponding to these options, where applicable.

> It is recommended not to recall more stubs than the limit specified under the Maximum Stub Recovery for Celerra Proxy as it does not detect failure and the data is lost.

- **Maximum Stub Recovery**

  Use this space to specify the upper limit for the number of stubs to be recovered for this agent.

- **Time between recall to count as successive in seconds**

  Use this space to specify the number of seconds for a recall to be considered as successive.

- **Time to wait after maximum successive recalls limit is reached in seconds**

  Use this space to specify the number of seconds that this agent must wait before additional stub recovery jobs can begin after the upper limit has been reached.

Erase Archive Data when Stub is Deleted

In the text box, specify the path where deleted stubs will be monitored for deletion when an Erase Data job is run. This could be the entire machine (indicated by a \), a particular drive (C:\), a particular folder (C:\deleted_data), or a UNC path (\\filer\directory). Multiple locations could also be specified, separated by the ; delimiter.

> - The path that is configured here will be applicable for all instances of the File Archiver for Windows Agent.
> - For **Local File System** instances, a folder can be created to contain the stubs to be hard-deleted (SHIFT_DELETE). This folder would then be part of the path that is specified (e.g., (C:\deleted_data). This would alleviate specifying entire volumes. From the volumes, you can then move the stubs (cut+paste) to the specified deletion folder. To move stubs across volumes, you must use the GxhsmUtility tool in the Resource Pack.

- For **Celerra** and **FPolicy** instances, a folder cannot be created to contain the stubs to be deleted. You can instead restrict the deletion to certain folders by specifying a subclient path or a path that is a parent to the subclient path.
- The path that is configured here is only used when an Erase Data job is run.
- If you delete stubs within the path that is specified and the subclient that includes the path is deleted, the data will not be erased.
- For **FPolicy** instances, the user must either specify "\" or a specific deletion folder path. If the intended deletion folder path is \\<filer_name>\<volume_name>\<folder_name>, the deletion folder specification needs to be:

  \\<fully_qualified_filer_name>\ONTAP_ADMIN$\vol\<volume_name>\<folder_name>;\\<short_filer_name>\ONTAP_ADMIN$\vol\<volume_name>\<folder_name>. Otherwise, the data will not be erased.

- For local data archived by a **Local File System** instance, the stubs must be permanently deleted with a hard-delete (SHIFT+DELETE). Stubs that are removed with a soft-delete (DELETE or right-click and DELETE) will not be erased.

NDS Tree Name

Displays the name of the NDS tree that this agent can access.

NDMP Properties

Click to access the **NDMP Server Properties** screen.

NDMP Restore Enabled

Specifies whether the NDMP Restore Enabler was installed with the *i*DataAgent.

- **YES** indicates that the enabler is installed and the client is an available destination for the restore of data from a Network Attached Storage (NAS) client.
- **NO** indicates that the enabler is not installed and the client is not an available destination for the restore of data from a NAS client.

QSnap Maximum Cache Size (in MB)

Specifies the maximum cache size for QSnap. See **Books Online** for more information on QSnap, before changing the maximum cache size.

QSnap Minimum Cache Size (in MB)

Specifies the minimum cache size for QSnap. See the **Books Online** for more information on QSnap, before changing the minimum cache size.

User Account

Displays the user account used by the system to log in to or access the (the tree of the) server during various jobs (including backups, browses, restores, etc.). For NAS NDMP, displays the NDMP account used by the system to connect to the NAS data server.

Administrative Group Account

Displays the SharePoint Administrator Account that has required rights to create and modify SharePoint databases. This account will be used for data protection and recovery operations.

SSO Account

Displays the SSO Administrator account for the single sign-on service on this SharePoint Server.

Change Account

Click to specify a different account as the **User Account**.

SharePoint Server Name

Displays the name of the SharePoint Server that is installed on the client computer. You can use this space to modify this server name if the name displayed is incorrect (e.g., not the same as the Client name or Host name).

Index Backup/Restore path

The UNC path for a shared network folder to temporarily store the site index during backup and restore. There should be enough space available on the share for the index to be temporarily stored.

For a SharePoint All-in-One Server, the Index path must be local, not a UNC path.

If topology manager is locked during backup/restore, force its release

Specifies whether the system should release the lock for the topology manager and therefore allow jobs to complete without interruption. This option is selected by default for new installations.

SQL Databases hosted on a remote SQL Server

Specifies whether the SharePoint Server is part of a SharePoint Server Farm and whether the SQL Databases are hosted on a remote SQL Server. If selected, the SQL Databases must be backed up using the SQL Server *i*DataAgent.

Authenticate Active Directory Domain Controller

Specifies whether to use or change the user account to authenticate against the Active Directory domain controller to look up group membership for the specified user (per the following fields)

Domain Name

Use this space to enter the domain name for this user.

User Name

Use this space to enter the name of the user for the account discussed for the preceding field.

For CDR, displays the user account to be used for the creation of ONTAP snapshots.

Password

Use this space to enter the password for this user.

Confirm Password

Retype the password.

Description

Use this field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.

Enable Offline Mining

Select this option to enable browse and restore of offline data.

Enable Office Communication Server Backup

Select this option to enable OCS backup feature for a client with Windows File System *i*DataAgent. This feature provides the ability to perform data protection operations for data associated with the Office Communications Server.

Enable SRM feature

Select this option to Enable SRM Options.

Enable for Archiving

Select this option to enable archiving for the agent. Once selected a license will be consumed.

Back to Top

Version

Use this dialog box to view the software version and verify the update status. Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent for which the information is being displayed.

Software Install Directory

Displays the directory path in which the software is currently installed on the client or MediaAgent computer.

Crypto Library Version

Displays the current version of the Crypto Library module.

Version Information

Displays the software component version (CommServe, MediaAgent, Client or Agent) installed on the computer.

Update Status

Displays the update status for each client computer. The possible values and their descriptions are:

- **Unknown**

  The software is not able to determine if the client computer meets the baseline level of updates due to an error or an uninstalled client still showing in the CommCell console.

- **Has Diagnostic**

  One or more diagnostic updates have been installed on the client computer.

- **Up To Date**

  The updates in the client computer match the baseline.

- **Needs Update**

  The client computer must be updated to meet the baseline level of updates.

- **Ahead of Cache**

  The client computer exceeds the baseline level of updates in the CommServe Cache directory.

Package

Displays the name of the packages installed on the client.

Status

Displays the update status for each package. The possible values are: *Unknown*, *Has Diagnostic, Up To Date*, *Needs Update*, and *Ahead of Cache*. (Refer to previous section for a description of these values.)

Updates

Displays the name of the updates.

Update Information

Specifies the options for installing the updates.

This information is displayed only in the case of remote clients and/or remote MediaAgents. (A client/MediaAgent that is not installed on the CommServe computer)

- **Cache Source**

  This information is only displayed for client computers.

  - **CommServe**

    If selected, the selected client receives its updates from the CommServe computer.

  - **Software Cache**

    If selected, the selected client receives its updates from the specified Client designated as Software Cache computer.

- **Store Updates Locally**

  When selected, indicates that the update packages must be saved on the local computer, before they are installed. Use the space to type the location on the local computer in which the updates must be stored, or click the **Browse** button to select the location on the local computer.

  If this option is selected, make sure that there is adequate space for installing the necessary updates. Also note that the system automatically deletes the update packages once they are installed.
  (You cannot specify a different folder to serve as the temporary cache location for NetWare clients; this field is disabled.)

Agent Properties (Index)

Use this tab to establish the parameters for creating new index during backups by the agent.

Create new index on full backup

Specifies whether the system will create a new index with each full backup. If cleared, all backups build upon the index from the previous backup.

Convert to full backup on indexing failures

Specifies whether the system will create a new index if the index is irretrievable and whether, for agents that support non-full backup types, the system will convert the backup to a full backup.   If cleared, the backup will fail if the index is irretrievable.

Security

Use this dialog box to:

- Identify the user groups to which this CommCell object is associated.
- Associate this object with a user group.
- Disassociate this object from a user group.

Available Groups

Displays the names of the user groups that are not associated with this CommCell object.

Associated Groups

Displays the names of user groups that are associated with this CommCell object.

Automatically add New Users to the "View All" Group (CommServe Level Only)

Specifies that all new users will automatically be added to the `View All` user group. This group allows users to view all CommCell objects, regardless of the associations of the other user groups they belong to.

Require Authentication for Agent Installation (CommServe Level Only)

Enable this option to prompt users for authentication for any agent installation on the CommCell.

Client Owners

Specify a user to allow CommCell user access to this client computer through CommCell Console and allow permission to run Web Console browse and restore operations on this client. Each user must be listed in a separate line.

Activity Control

Use this dialog box to enable or disable data management and data recovery on a selected client computer group, client computer, agent, or subclient. Note that not all agents support subclients. For the File Archiver for Windows Agent, use this dialog box to enable or disable Data Classification. Also note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent for which the information is being displayed.

If data management and data recovery operations are disabled at the client computer group or client level, then these operations below these levels will be disabled. If data management / data recovery operations are enabled at the client computer group or client level, then these operations below these levels will be enabled.

Enable Data Management / Backups / Archive / QR Volume Creation

Specifies whether data management operations (Backups / Archive / QR Volume Creation) will occur from this client computer group, client computer, agent or subclient.

If cleared:

● The button **Enable after a Delay** appears to the right side of this operation activity. It allows to pre-determine the date and time at which data management operations will begin on the selected client computer group, client computer, agent, or subclient.
● Data management operations from this client computer group, client computer, agent, or subclient cannot be started and are skipped.
● Running and waiting data management operations for this client computer group, client computer, agent, or subclient run to completion.
● Stopped data management operations for this client computer group, client computer, agent, or subclient cannot be resumed until this option is enabled.
● Pending data management operations for this client computer group, client computer, agent, or subclient do not run until this option is enabled.

(Job states are indicated in the Job Controller.)

Enable Data Recovery / Restores / Retrieve / QR Volume Recovery (Not applicable for the subclient level)

Specifies whether data recovery operations (Restores / Retrieve / QR Volume Recovery) will occur from this client computer group, client computer or agent.

If cleared:

● The button **Enable after a Delay** appears to the right side of this operation activity. It allows to pre-determine the date and time at which data recovery operations will begin on the selected client computer group, client computer, or agent.
● Data recovery operations for this client computer group, client computer or agent cannot be started and are skipped.
● Running data recovery operations for this client computer group, client computer or agent run to completion.
● Pending data recovery operations for this client computer group, client computer or agent do not run until data recovery operations are enabled.

(Job states are indicated in the Job Controller.)

Enable Content Indexing

Specifies whether Content Indexing operations will occur from this client computer group, client computer or agent.

If cleared:

● The button **Enable after a Delay** appears to the right side of this operation activity. It allows to pre-determine the date and time at which Content Indexing operations will begin on the selected client computer group, client computer, or agent.
● Content Indexing operations are not started and are skipped.
● Running and waiting Content Indexing operations run to completion.
● Content Indexing operations in a pending, queued, or suspended state cannot be resumed until this option is enabled.
● Pending Content Indexing operations cannot run until this option is enabled.

(Job states are indicated by the Job Controller.)

Enable SRM Data Collection

Specifies whether data collection operations will occur from this agent.

If cleared:

● The button **Enable after a Delay** appears to the right side of this operation activity. It allows to pre-determine the date and time at which data collection operations will begin on the selected agent.
● Data Collection operations are not started and are skipped.
● Running and waiting Data Collection operations run to completion.
● Data Collection operations in a pending, queued, or suspended state cannot be resumed until this option is enabled.
● Pending Data Collection operations cannot run until this option is enabled.

(Job states are indicated in the Job Controller.)

Enable Discovery

Specifies whether discovery operations will occur.

Script Preview

Click to display the backup script, based on the current subclient configuration, that will be submitted to RMAN when backups are performed for the selected Oracle subclient.

Back to Top

Subclient Properties (General)

Use Subclient Properties (General) tab to add, modify or view general information on the selected subclient. Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent or enabler for which the information is being displayed.

Client Computer / Client Name

Displays the name of the Client computer to which this subclient belongs.

Billable Entity

The name of the Billable Entity assigned to this subclient.

Billing Department

Displays the name of the billing department, when the subclient is associated with a billing department. For more information on Billing and Costing See the *CommNet Books Online*.

iDataAgent/Agent Type

Displays the name of the Agent to which this subclient belongs.

Backup Set

Displays the name of the Backup Set to which this subclient belongs.

Instance

Displays the name of the Instance to which this subclient belongs.

Policy (External Data Connector Only)

Displays the name of this policy. You can use this space to enter or modify the name of the policy.

Database Name

Displays the name of the Database to which this subclient belongs.

Partition

Displays the Lotus Domino Server data path under which data is found for this subclient.

Subclient Name

Displays the name of this Subclient. You can use this space to enter or modify the name of the subclient.

Policy Name

Displays the name of this policy. You can use this space to enter or modify the name of the policy.

Subclient Type

Displays whether this subclient is a database or file/file group type.

Incremental Support Using

- **CXBF**

  Select this option to perform a CXBF backup for the selected subclient.

- **Checksum**

  Select this option to perform a non-CXBF (Checksum) backup for the selected subclient.

Discover Criteria (External Data Connector Only)

- **All**

  This option discovers all clients associated with the master server.

- **By Agent Type**

  This option discovers clients containing the Agent selected in the drop-down menu.

- **By Client Names**

  This option discovers clients by their names.

- **Select Client Group for Discovered Clients**

  Select a Client group to associate discovered clients to. If desired, you can also **Create a New Group**.

Disable Auto-Discovery

Specified to disable the auto-discovery and pre-assignment of SQL databases to the default subclient. By default, SQL databases are automatically discovered and assigned to the default subclient.

Create New Index Every *nn* Archive Operations

Displays the interval for index creation by number of archive operations on this subclient. You can use this space to modify the interval setting. This setting can be overridden by selecting the Create New Index option on the Advanced Backup/Archive Options (Data) tab. If overridden, the new index interval counter will start again at zero.

Set index cycle to every *nn* backup jobs

For the default subclient of an On Demand Backup Set, displays the interval for index creation by number of backup or migration operations on this subclient. You can use this space to modify the interval setting. This setting can be overridden by selecting the Create New Index option on the Advanced Backup/Migration Options (Data) tab.

Use Direct Database Access

Specifies to use the alternate read-only direct access to the SharePoint database to backup objects (e.g., documents, list items) and their metadata. This method can increase the backup speed and is applicable for Document backup sets, WSS v3.0, and MOSS 2007 environments. Requires installing specifically Microsoft SQL Server Native Client 2005 on Front-End Web Server. When selected or deselected, the next backup that is run will be a Full backup.

Use Direct Access to Restore Selected Entities

Specifies to restore individual files into the database directly. This is applicable for files in Document backup sets. When restoring the files directly into the database, the IDs of the files will remain the same and will not change.

Use content file provided by SRM

Uses content file consisting of files and directories provided by SRM report with on demand action.

Use VSS

Specifies whether VSS will be used to back up data for this subclient.

Use VSS for System State

Specifies whether VSS will be used to back up the system state for this subclient.

Use QSnap to handle backup of locked files

Specifies whether QSnap will be used to back up data (locked files) for this subclient.

Number of Data Readers

Use this space to specify the number of simultaneous backup data streams allowed for this subclient. For best performance, this should be set no higher than the number of physical drives that hold this subclient's data, except for specialized hardware such as RAID. For more information, see *Automatic File System Multi-Streaming* or *Backup - NAS NDMP* in Books Online.

Allow multiple data readers within a drive or mount point

Specifies whether multiple data reads are allowed for a single Windows physical drive or Unix mount point during backups on this subclient. This should be selected only for specialized hardware such as RAID, or possibly in the case of spanned volumes. For more information, see *Automatic File System Multi-Streaming* in Books Online.

Incremental backup should use

- **UNIX mtime**

  Select this option to determine which files are selected for incremental backup by changes in the mtime timestamp.

- **UNIX ctime**

  Select this option to determine which files are selected for incremental backup by changes in the ctime timestamp.

  When you select **Use Data Classification** in Backup Set Properties, it is recommended not to select "UNIX mtime" and "UNIX ctime" options in this properties box as Incremental Backups for Data Classification scan does not support these options.

Informix Server

Displays the name of the Informix instance to which this subclient belongs.

Default Subclient

Displays whether this is the default subclient. When a subclient is designated as the default subclient, it will back up/archive all the data for the subclient that is not assigned to any other subclients within the backup set/archive, and it cannot be deleted.

Offline Archive

Specifies whether to enable Offline Archive operations on this subclient to allow Outlook Add-In users the capability of retaining a full copy of archived items in local cache on the Outlook client.

Celerra Proxy Stub Subclient

Use the following group of options to enter or change the configuration information for the Proxy Stub Subclient feature.

- **Proxy Stub Path**

  Use this space to enter, or **Browse** to, the location of the directory on the server where the stubs will reside.

- **HTTP/CIFS Address**

  Use this space to enter the HTTP/CIFS address of the proxy stub path specified in the connection configured between the filer and the server.

- **NAS HTTP Port No.**

  Displays the port number used for communication with the proxy computer.

Collect User Identity

Specifies that during an archive operation, additional ownership/user information is collected and archived . This information is later used to perform owner based searches.

Operate in Archive Mode (Domino Mailbox Archiver Agent)

When selected, the Domino Mailbox Archiver Agent will perform archive operations based on the rules established in the **Archive Rules** tab of the **Subclient Properties** dialog box.

- **Operate in Backfill Mode** (Domino Mailbox Archiver Agent)

  When selected, this mode allows you to backup and populate the content index with messages that were sent and/or delivered before the point-in-time at which archives of the journaling mailbox begin.

Operate in Backup Mode Domino Mailbox Archiver Agent)

When selected, this mode allows you to perform full, incremental, differential, or synthetic full backups of mailbox databases using the Domino Mailbox Archiver Agent. The **Archive Rules** tab of the **Subclient Properties** dialog box is disabled, backup operations run with no stubbing phase, and all mailbox data (with the exception of design documents) is backed in a similar fashion to the Lotus Notes Document *i*DataAgent.

Description

Use this field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.

Back to Top

Subclient Properties (Content)

Use this tab to define the contents of a new subclient or to change the content of an existing subclient. Items included in subclient content are backed up/migrated/content indexed by the subclient. Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent for which the information is being displayed.

Contents of subclient

Displays a list of paths of data/workspaces/categories/documents/folders included as content for this subclient. Special characters (such as "\" "/" "." ",") represent content of the default subclient, that is not assigned to other subclients within the backup set. For Unix, when a symbolic link is included in the subclient content, the target of the symbolic link along with the link itself can be displayed.

- **Delete**

  Click to delete the selected path/data/folder from the Contents list for this subclient.

- **Browse**

  Click to browse for new content that you want to add to this subclient.

	When browsing content while configuring SharePoint subclients, you can add content via multiple selections with the CTRL or SHIFT keys.

- **Add Paths**

  Click to enter a new content path.

  Enter the UNC path of the share to configure a subclient to backup and restore.

	Type in the UNC path of the share that has to be added in the **Enter New Content** field and click **Add**. Repeat this step to add more files and/or folders to the content.
	
	 1. If this is the first UNC path being entered as subclient content the **Impersonate NT User** dialog box will appear. Enter the user account information for the Domain User with permissions for that path. Note the following:
	
	  ○ Login name must be provided in the following format: \<domain>\UserName
	     For example, to log on as `usr1` in a domain called `MyDomain`, enter **MyDomain\usr1** as the user name
	
	  ○ The domain user that you specify should have access to all the UNC paths entered as contents of the subclient.
	
	  ○ Adding a UNC shared path as subclient content of a member server that points to a server in a workgroup requires the local user name and password is identical to a domain user's name and password. (This is a scenario where \<UserName> and password is accepted.)
	
	  ○ Adding a UNC shared path as subclient content of a non-member (workgroup) server that points to a member server requires the local user name and password is identical to a domain user's name and password. (This is a scenario where \<UserName> and password is accepted.)
	
	  ○ The domain user can be changed at a later time with the **As User** button.
	
	 2. To save your content changes, click **OK**.

	For File Archiver for Windows, UNC paths are not supported with subclients associated with Local File System.

- **As User**

  Click to enter/modify the User Name and Password required to access the UNC path when a UNC path is entered as content.

Discover

Click to display the data paths to which the symbolic links in the data contents are pointing. The paths will be displayed in **Contents of subclient**. This button is enabled only when **Expand symbolic links of subclient content** below is enabled.

	Instead of clicking **Discover**, wait until the backup completes and then refresh the subclient. Then go to **Contents of subclient**. The data contents for the symbolic links should be displayed.

Perform backup using mining off snapshot

Click to run a data protection job from an offline copy of a SharePoint database. The offline copy is created by using the SQL Server iDataAgent to create a SnapProtect backup. Snap mining can improve performance in that it offloads processing on the production application server since processing calls are not required from the SharePoint Server during backup.

SQL DB client

Specifies the client computer where the SharePoint Database and SQL Server iDataAgent is installed.

Agents

Specifies the SQL Server iDataAgent that was used to create the SnapProtect backup of the SharePoint Database.

Instance

Specifies the instance of the SQL Server *i*DataAgent that was used to create the SnapProtect backup

SQL DB subclient to use

Specifies the subclient to use for mining the SnapProtect backup.

Proxy Client

Click if you want the data protection job of the SnapProtect backup to run on the Proxy Client. Then specify the computer for the Proxy Client.

Configure

Click to discover and change the associations of the mailboxes to the subclients. Any mailboxes included as content for a user-defined backup set/subclient will be automatically excluded from the default backup set/subclient.

Backup Content Path

Click the drop-down list arrow to display the root volumes on the file server. To change the root volume, click one in the list. If you want to refine the content path further, use the space to the right of (or below) the root volume list to enter additional path information. Note the following:

- For NetApp, the root volume is the mount path of each volume.
  Example: for volume `FS1` the root volume will be `/vol/FS1`.

- For EMC Celerra, the root volume is the mount point created for a volume.
  Example: for volume `FS1` with mount point `/FS1` the root volume will be `/FS1`.

- For Hitachi, no root volumes are shown in the drop down list. Type the full path of the root volume.
  Example: for volume `FS1` with mount point `/mnt/FS1` the root volume will be `/mnt/FS1`.

- For BlueArc, the root volume is a combination of a descriptor of the path and the volume name.
  Example: for volume `FS1` with a mount point of `/` the root volume will be `/__VOLUME__/FS1`.

For Celerra tape silvering, specify the source path of the replication that was created from the Celerra Management Console or command line. Append `.ts` to the path name. For example, `/sourcefs/.ts`.

Enter new content

Use this space to specify the paths of other data that you want the subclient to contain.

Add

Click to add the data that you specified in **Enter new content** or **Backup Content Path** to the Contents list.

Treat characters as regular expressions

Specifies whether regular expressions (i.e., strings that use wildcard characters) will be interpreted as wildcards or as literal strings. Select this option to recognize wildcard characters in the content path. See Wildcards for a list of supported wildcards.

Case Sensitive

Specifies whether content paths will be case sensitive. Selecting this option will cause the system to recognize the difference between upper case and lower case characters in the content path.

Backup System State

Specifies whether the system state will be backed up with this subclient. Selecting this option causes the system state to be backed up with the file system for this subclient.

Backup Office Communication Server

Specifies whether the Office Communications Server will be backed up with this subclient. Selecting this option causes the OCS data & settings to be backed up with the file system for this subclient.

- **Edit**

  Click to enter/modify the User Name and Password required to access the Office Communications Server.

Only backup files that qualify for archiving

Click to backup only those files within the specified content, which meets the archiving rules.

Enable Apple Double Support

Specifies whether to facilitate the management of resource fork data in Apple Double-encoded Macintosh files.

	This option may not work on Solaris subclients.

Expand symbolic links of subclient content

Specifies whether to display the data paths to which the symbolic links (if any) in the subclient content are pointing. Whenever this option is enabled, the **Discover** button discussed above is enabled and used to this purpose.

Back to Top

Filters

Use this tab to add, modify or view the data protection or discovery filter on the selected subclient or Replication Set. Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent for which the information is being displayed.

Include Policy Filters

Specifies whether Subclient Policy filters will be used for this subclient, and is applicable only for subclients associated to a Subclient Policy. Selecting this option will cause this subclient to inherit the filter specified in the associated Subclient Policy. Clearing this option overrides the use of Subclient Policy filters on this subclient. See Subclient Policy - Filtering Rules for more information.

Include CommCell Level Global Filters / Global Filter

Specifies whether filters set under Control Panel (Global Filters) will be used in addition to the filters set at the subclient level to exclude data from data protection operations for this subclient.

Include Global Filters

Displays a list of options for enabling or disabling Global Filters which can be used in addition to the filters set at the subclient level to exclude data from data protection operations for this subclient. To change the setting, select one of the following values from the list:

- **OFF** - Disables Global Filters for this subclient.
- **ON** - Enables Global Filters for this subclient.
- **Use Cell Level Policy** - Enables or disables Global Filters for this subclient depending on whether the **Use Global Filters on All Subclients** option is enabled or disabled on the Control Panel (Global Filters) dialog. If the **Use Global Filters on All Subclients** option is enabled, then the **Use Cell Level Policy** option will enable Global Filters on this subclient. If the **Use Global Filters on All Subclients** option is disabled, then the **Use Cell Level Policy** option will disable Global Filters on this subclient.

Exclude these files/folders/directories/patterns/containers/objects

Displays entries that will be excluded from data protection operations for this subclient or Replication Set.

Regular Expressions

Provided below are details regarding support for the use of regular expressions (or wildcard characters) when adding entries to this exclusion list:

- Exchange Public Folder, Exchange Public Folder Archiver, Novell Directory Services (NDS), and SharePoint Document do not support the use of wildcards when adding entries to this set of exclusions.
- File Share Archiver - If a disk mount path is pointing to a filer share that will be archived, do not include UNC paths in the subclient content. UNC paths cannot be manually filtered out.
- For NAS NDMP *i*DataAgents:
  - BlueArc NAS NDMP - has no limitations. The `*` wild card is supported at the end of a directory filter (filters starting with `/`) or at the beginning or end of a file filter (not starting with `/`).
  - EMC Celerra NAS NDMP:
    - For older versions of DART OS (prior to 5.5), backup filters are not supported. Overlapping content cannot be configured. You cannot have one subclient with `/myfs` and another with `/myfs/dir3`. For example, if the default subclient specifies `/` as the content, and another subclient has `/myfs/dir3` defined in the content, then backing up the default subclient will skip all of `/myfs`.
    - For DART OS 5.5 and above, filters are supported but do not work with volume-based backups. They are not blocked from being specified as an Advanced Backup/Archive Option , but a warning is displayed that the filters are ignored.
    - For DART OS 5.5 and above, a maximum of six directory filters (filters starting with `/`) and six file filters can be specified in either the default or user-defined subclients. If more filters are specified, a warning is displayed in the Event Viewer. For example, if a subclient specifies `/myfs` as the content, and another subclient specifies a total of 12 paths (`/myfs/dir1` through `/myfs/dir12`), then when backing up the first subclient, you will receive six warnings indicating `/myfs/dir7` through `/myfs/dir12`) were not filtered.
      - For directory filters, the `*` wild card is supported only at the end of the filter.
      - For file filters (not starting with /) the `?` wild card matches a single character and the `*` wild card matches a string of characters. One of these wild cards can be used at the beginning or at the end of the filter.
  - Hitachi NAS NDMP - backup filters are not supported.
  - NetApp NAS NDMP:
    - Backup filters can be used for file or folder names, but not paths. Thus, if the same filtered file name exists in multiple folders, all occurrences will be filtered. See *Subclients - NAS NDMP* in *Books Online* for details.
    - A maximum of 32 filters can be specified. The `*` wild card is supported, but only as the first or last character in the filter.
    - Filters are not supported for the GX model.
- For the Windows, NetWare, Unix, File Archiver Agents, and ContinuousDataReplicator Agents, see Wildcards for more information.

System State Filters

Following is a list of acceptable exclusion filters for Windows File System System State:

- ○ {System Protected Files}
- ○ {IIS}
- ○ {COM+ Database}
- ○ {Event Logs}
- ○ {One Touch Files}
- ○ {RSM}
- ○ {Terminal Services Licensing}
- ○ {Disk Quotas}
- ○ {Content Indexing Catalogs}
- ○ {WMI Database}
- ○ {DHCP}
- ○ {WINS}
- ○ {UDDI Database}
- ○ {Remote Storage Database}
- ○ {Certificate Services }
- ○ {Offline Files}
- ○ {Active Directory Application Mode}
- ○ {File Server Resource Manager}
- ○ {NPS Database}

Exclude the following mailboxes/folders

Displays mailboxes or folders that will be excluded from data protection operations for this subclient. Wildcards are not supported when adding entries to this exclusion list.

Exclude the folders that contain the following patterns

Displays mailbox folder name wildcard patterns that will be excluded from data protection operations for this subclient. The Exchange Mailbox Archiver Agent, and the Exchange Compliance Archiver Agent support the use of wildcard expressions when adding entries to this exclusion list. See Wildcards for more information.

The following paths and files are excluded

Displays entries that will be excluded from discovery operations for this subclient. The Lotus Notes Database, Domino Mailbox Archiver, and Lotus Notes Document *i*DataAgents support the use of wildcard expressions when adding entries to this exclusion list. See Wildcards for more information.

Pattern/path to be excluded

Use this space to enter the path of a folder or file that you want to exclude from discovery operations for this subclient. The path must start with a (\), and it must be relative to the data path of the partition. The Lotus Notes Database, Domino Mailbox Archiver, and Lotus Notes Document *i*DataAgents support the use of wildcard expressions when adding entries to this exclusion list. See Wildcards for more information.

Except for these files/folders/directories/containers/objects

Displays entries that will be included in data protection operations for this subclient or Replication Set in cases where a parent object is listed in the Exclude filter.

Provided below are details regarding adding entries to this exceptions list:

- Wildcards are not supported in Exception filters.
- For NAS NDMP *i*DataAgents, only file names or folder names are valid entries when adding entries to this set of exceptions; paths are not supported.

Include these files/folders/patterns with every archive

Displays entries that will be included in archive operations for this subclient in cases where a parent object is listed in the Exclude filter. Note that File Archiver Agents do not support the use of regular expressions (or wildcard characters) when adding entries to this inclusions list.

- File Share Archiver - If a disk mount path is pointing to a filer share that will be archived, do not include UNC paths in the subclient content. UNC paths cannot be manually filtered out.

Add

Click to manually add an entry to be included in, or excluded from, data protection operations for this subclient or Replication Set.

Browse

Click to browse for an entry to be included in, or excluded from, data protection operations for this subclient or Replication Set.

Edit

Click to manually edit an entry to be included in, or excluded from, data protection operations for this subclient.

Delete

Click to delete a selected filter entry.

Back to Top

Pre/Post Process

Use the Pre/Post Process tab to add, modify or view Pre/Post processes for the selected subclient or Replication Set. Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent or enabler for which the information is being displayed.

Pre Backup/Scan/Migrate/Archive/Copy/Snap/Recovery Point process

Displays the name/path of the process that you want to run before the respective phase. You can use this space to enter a process that will execute before this phase on the subclient or Replication Set, or you can use the **Browse** button to search for and select the name/path of the process. The system allows the use of spaces in the name/path, provided they begin with an opening quotation mark and end with a closing quotation mark.

	If you are using the Linux File System iDataAgent to back up VMware virtual machines, you must create a PreBackup process script that will allow the system to create the required REDO files. See "Create Pre/Post Backup Process Scripts to Back up VMware Virtual Machines Using the Linux File System iDataAgent" in Books Online for step-by-step instructions.

Post Backup/Scan/Migrate/Archive/Copy/Snap/Recovery Point process

Displays the name/path of the process that you want to run after the respective phase. You can use this space to enter a process that will execute after this phase on the subclient or Replication Set, or you can use the **Browse** button to search for and select the name/path of the process. The system allows the use of spaces in the name/path, provided they begin with an opening quotation mark and end with a closing quotation mark.

	If you are using the Linux File System iDataAgent to back up VMware virtual machines, you must create a PostBackup process script that will allow the system to post data back to the virtual machines. See "Create Pre/Post Backup Process Scripts to Back up VMware Virtual Machines Using the Linux File System iDataAgent" in Books Online for step-by-step instructions.

On Source

Specifies whether the PreSnap/PostSnap process will execute on the source computer.

On Proxy

Specifies whether the PreSnap/PostSnap process will execute on the proxy computer.

Run Post Backup/Scan/Migrate/Archive/Copy/Snap Process for all attempts

Specifies whether this process will execute for all attempts to run the phase. Selecting this option will execute the specified process for all attempts to run the phase, including situations where the job phase is interrupted, suspended, or fails. Otherwise, when the checkbox is cleared the specified process will only execute for successful, killed, or failed jobs.

On Primary Host/Backup Host/MediaAgent

Specifies the location of the batch file or shell script that you want to execute after a phase, either on the Primary Host (production server), Backup Host or MediaAgent.

Run As / User Account

Displays either the Local System Account, or for added security, another account as having permission to run these commands.

	SharePoint Server iDataAgent:
	Even if the Local System Account is selected as the account to run the Pre/Post processes, the account that actually will be used is the SharePoint Administrator Account for the site in which the SharePoint Server resides. This account was configured during installation and can be changed in Agent Properties.

Change

Click to add or modify the account that has permission to run these commands.

Browse

Click to search for and select the Pre/Post Process.

Encryption

Use this dialog box to select the data encryption options for the selected content. When accessing this dialog box from the Subclient Properties Encryption tab, this setting applies only to the selected subclient content for operations run from the CommCell Console. When accessing this dialog box from the Instance Properties Encryption tab, this setting applies only to third-party Command Line operations. The functionality is not propagated to the Subclient Properties Encryption tabs.

None

When selected, no encryption will take place during a data protection operations.

Media Only (MediaAgent Side)

When selected, for data protection operations, data is transmitted without encryption and then encrypted prior to storage. During data recovery operations, data is decrypted by the client.

When using this setting in conjunction with the client property **With a Pass-Phrase**, you will be required to provide a pass-phrase for data recovery operations unless you export the client pass-phrase to the destination client(s). When using pass-phrase security for third-party Command Line operations or DataArchiver Agents stub recovery operations, you must export the pass- phrase to the destination client.

Network and Media (Agent Side)

When selected, for data protection operations, data is encrypted before transmission and is stored encrypted on the media. During data recovery operations, data is decrypted by the client.

When using this setting in conjunction with the client property **With a Pass-Phrase**, you will be required to provide a pass-phrase for data recovery operations unless you export the client pass-phrase to the destination clients.

Network Only (Agent Encrypts, MediaAgent Decrypts)

When selected, for data protection operations, data is encrypted for transmission and then decrypted prior to storage on the media. During data recovery operations, data is encrypted by the MediaAgent and then decrypted in the client.

When using this setting in conjunction with the client property **With a Pass-Phrase**, you will not be required to provide a pass-phrase for data recovery operations.

Script Preview

Click to display the backup script, based on the current subclient configuration, that will be submitted to RMAN when backups are performed for the selected Oracle subclient.

Storage Device

Use this dialog box to establish the storage device related settings on the selected subclient. Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent or enabler for which the information is being displayed.

The following tabs are displayed:

- (Data) Storage Policy
- Data Transfer Option
- Deduplication

STORAGE POLICY

Use this tab to select or view storage policy settings on the selected subclient.

Data/Database/Transaction Log Storage Policy

Displays the storage policy to which this subclient is currently associated. To associate a storage policy to a new subclient or to change the storage policy associated with an existing subclient, click one in the list.

Incremental Storage Policy

Displays the name of the Incremental Storage Policy associated with this subclient, if the storage policy has the Incremental Storage Policy option enabled.

Data Paths

Click to view or modify the data paths associated with the primary storage policy copy of the selected storage policy.

Number of Data/Database/Transaction Log Backup Streams

Displays the number of streams used for backup operations. To change the number of streams, click one in the list. For DB2 DPF, be sure to set the appropriate number of streams for each database partition by double-clicking the appropriate **Stream** space and typing the desired number.

Client/Instance/Status/Stream

Displays the names of the instances according to current backup priority along with other associated information that are included in the Oracle RAC node. To change the backup priority of the instances, click the instance name as appropriate and use the directional arrows provided.

Maximum Backup Streams

For Informix, displays the maximum number of streams used for database backup operations, which is determined from the ONCONFIG file. The number of streams for backups cannot be set currently from the CommCell Console. Instead, you must set the BAR_MAX_BACKUP parameter in the $ONCONFIG file on the Informix client. Also, the number of streams specified by the storage policy must be greater than or equal to the number specified by the BAR_MAX_BACKUP parameter.

Data Threshold Streams

For Oracle RAC, specifies whether to run the backup job immediately when the total number of reserved streams is greater than or equal to the value in this field. If you click this option, use the space provided to change this value if desired.

Create Storage Policy

Click to launch the Create a Storage Policy wizard. Once the storage policy has been created, it will be displayed in the list of storage policies to which the selected subclient can be associated.

Buffer Size

Use this space to specify the size (in 4 KB pages) of each buffer to be used for building the backup image. The minimum value is 8, and the default value is 1024. If you select value 0, the value of the `backbufz` database manager configuration parameter will be used as the buffer allocation size.

DATA TRANSFER OPTION

Use this tab to establish the options for data transfer. Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent for which the information is being displayed.

Software Compression

Indicates whether software compression for the subclient or instance is enabled or disabled, and if enabled whether it is performed on the client or MediaAgent computer.

- **On Client**

  Click to enable software compression on the client computer.

- **On MediaAgent**

  Click to enable software compression on the MediaAgent computer.

- **Use Storage Policy Settings**

  Click to use the settings enabled on deduplicated storage policy copy.

  This option applies when subclient is associated with a storage policy copy that is deduplicated. See Copy Properties (Deduplication) - Advanced tab for compression settings on deduplicated storage policy copy.

- **Off**

  Click to disable software compression.

Note that hardware compression has priority over the software compression. Hardware compression is established in the Data Path Properties dialog box. The above software compression option will take effect when the data path is associated with a disk library, or when hardware compression is disabled in the data path associated with tape libraries.

> For non-deduplicated storage policy copy, select **On Client** or **On MediaAgent** options to turn on compression, depending upon your environment.

Resource Tuning

Indicates the processes used by the client to transfer data based and whether bandwidth throttling is enabled or not.

- **Network Agents**

  Specifies the number of data pipes/processes that the client uses to transfer data over a network. Increasing this value may provide better throughput if the network and the network configuration in your environment can support it. On non-UNIX computers, the default value is 2 and a maximum of 4 can be established if necessary. On UNIX computers the default value is 1 and a maximum of 2 can be established if necessary.

- **Throttle Network Bandwidth (MB/HR)**

  Specifies whether the backup throughput is controlled or not. (By default this option is not selected and therefore the throughput is not controlled). When selected, use the space to specify a value for the throughput. By default, this is set to 500. The minimum value is 1 and there is no limit to the maximum value. (In this case the backup throughput will be restricted to the maximum bandwidth on the network.)

Use this option to set the backup throughput, based on the network bandwidth in your environment. Use this option to reduce the backup throughput, so that the entire network bandwidth is not consumed, especially in slow links. Increasing this value will end up consuming the bandwidth with the maximum throughput limited to the network bandwidth capability.

Note that throttling is done on a per Network Agent basis.

Application Read Size

This option specifies the amount of application data (such as SQL data, Windows File System data, and virtual machine data) backup jobs will read for each unit transferred to the MediaAgent.

The default value for this options is 64KB; however, this value may be increased to reduce the amount of data read from the given application, which in turn reduces the amount of I/O operations performed against it. As a result, overall backup performance may increase. However, backup memory usage may also increase, which may inadvertently consume additional resources from the application. Thus, it is recommended that this value be set at either the default value or match the block size directed by the application.

DEDUPLICATION

Use this tab to establish the options for deduplication on the subclient. It indicates whether deduplication for the subclient is enabled or disabled, and if enabled whether the signature generation (a component of deduplication) is performed on the client or MediaAgent computer.

Note that deduplication is supported on disk storage devices. So the deduplication options are applicable only if the subclient is associated with a Storage Policy containing disk storage.

On Client

Click to enable signature generation on the client computer.

On MediaAgent

Click to enable signature generation on the MediaAgent computer.

Subclient Properties (SnapProtect Operations)

SnapProtect Backup with hardware Snap Engines | SnapProtect Backup with Data Replicator

Use this tab to enable SnapProtect backup and to establish the options for SnapProtect backup operation, for the selected subclient.

These options are available if you select a hardware Snap Engine. Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent for which the information is being displayed.

SnapProtect

Specifies whether SnapProtect backup for the selected subclient is enabled or disabled.

Available Snap Engines

Lists the available snapshot engine vendors. To select a snapshot engine vendor, click the pull-down arrow and click the one that you want to use.

● **Enter Array Credentials**

Click to access the Array Management dialog box, which enables you to add or modify access information for a array.

Use Proxy

Use this list to specify the name of the proxy server that will be used for performing the SnapProtect backup operations.

Use source if proxy is unreachable

Select to use the source machine for SnapProtect backup if the proxy client is not available.

Use RMAN for Tape Movement

Select to use RMAN for movement to media operations.

Allow multiple data readers within a drive or mount point

Specifies whether multiple data reads are allowed for a single physical drive or mount point during backups on this subclient. It is recommended that this option is selected for specialized hardware such as RAID, or possibly in the case of spanned volumes. For more information, see Automatic File System Multi-Streaming in Books Online.

Number of Data Readers for Backup Copy

Use this space to specify the number of simultaneous backup data streams allowed for this subclient, during the movement to media operation. For best performance, this should be set no higher than the number of physical drives that hold this subclient's data, except for specialized hardware such as RAID.

Back to Top

Open Files Failure Actions

Use this dialog box to select the action to be taken in case the snapshot fails to be created during the backup job.

Archiving files or running applications that utilizes file access time have special considerations. Ordinarily the action of backing up a file using the backup agent will cause the file access time to change to the time of the backup. This action of the backup agent may have an undesired effect on the application or archiver agent if you want to archive files based on access times. To workaround this situation, you should use a software snapshot (VSS or Qsnap) to accomplish the backup. If the software snapshot were to fail (i.e. VSS service unavailable or unable to quiesce the volume) you can choose the following subclient options to control what happens.

Open files failure actions

Select the action to be taken in case the software snapshot creation fails during a backup job.

● **Fail the job**

If selected, the backup job will fail and not continue in the case where the software is unable to create the snapshot. Use this option, if you want to perform the backup using only the software snapshot.

● **Continue and reset access time**

If selected, the backup job will fall back to legacy (non snapshot) methods. After backing up the file, the access time will be reset back to its original time before the backup occurred. Use this option, if you are archiving files based on access time. Note that resetting the access time introduces a small amount of additional overhead in the backup (may be slightly slower).

● **Continue and do not reset access time**

If selected, the backup job will fall back to legacy (non snapshot) methods. After backing up the file, the access time will NOT be reset back to its original time. Use this option, if you are NOT archiving files based on access time.

Subclient Properties (1-Touch Recovery)

Use this tab to establish 1-Touch Recovery items. Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent for which the information is being displayed.

1-Touch Recovery

Click to configure this subclient with 1-Touch Recovery options.

- **1-Touch server**

  Displays the name of the server that will be used as the 1-Touch (boot) server for this client. You can use this space to add or modify the name of the 1-Touch server. The server must reside within the same subnet as the client. If the server name is changed, the client's name must be manually removed from the previous 1-Touch server's database.

- **1-Touch server directory**

  Displays the name of the directory on the 1-Touch server where the files required to boot the client in case of a crash are stored. You can use this space to add or modify the 1-Touch server directory.

  ○ For 1-Touch for AIX, this is the directory where the NIM Master environment is set up and installed.
  ○ For 1-Touch for HP-UX, this is the directory where the HP-UX Ignite Server files are installed.
  ○ For 1-Touch for Solaris, this is the directory where the Solaris JumpStart files are installed.

Subclient Properties (SRM Options)

Use this dialog box to specify the Data Collection requirements.

SRM Data Collection

This option will be enabled if **Enable SRM feature** option is selected in the agent's Properties tab.

- **Discovery**

  Select this option for the collection of less detailed information for the client.

Subclient Properties (Rules)

Use Subclient Properties (Rules) tab to view or change archiving rules for this subclient.

- File Rules
- Stub Rule

FILE RULES

Use this tab to create rules that enable or disable the Archiving Rules. These rules specify the free space on volumes, age and/or size of the files, for determining whether to scan a volume for archiving.

Enable all rules

When selected, all archiving rules, except for Stub Management rules, will be enabled for this subclient.

Begin scan for file selection when free volume is less than _n_ %

- Enter the low watermark value for the volume.
- The free space of the volume is checked where the subclient content resides.
- If the free space on the volume is greater than the specified value, then the volume will not be scanned for archiving.

For example:

If you entered a value of 60% for this field, and the free space currently on the volume is 50%, then the volume will be scanned for files that meet the archiving criteria.

End scan if volume is freed to _n_ %

- Enter the high watermark value for the volume.
- It determines the point at which the migration archiving operation will stop archiving files.
- The archiving will continue until the free space on the volume is equal to the value specified here.

  Note that in the case of a very large file, archiving will continue even beyond the specified high watermark value until the entire file has been archived.

For example:

If you entered a value of 70% for this field, and archiving has freed up 70% of the space on the volume, then archiving of files within that volume will cease.

Archive file access time older than _n_ Days

- Enter the number of days elapsed (i.e., the age of the file) since the last accessed time of each file.
- For archiving, the last accessed date of each file within that volume or folder/directory is checked to see if it is older than the number of days specified.
- If the last accessed date of files is older than the number of days entered, the files will be archived.

For example:

If you entered a value of 30 days, then all files older than 30 days in the scanned volume or folder/directory will be archived.

Archive file modified time older than _n_ Days

- Enter the number of days elapsed (i.e., the age of the file) since the modified time of each file.
- For archiving, the modified date of each file within that volume or folder/directory is checked to see if it is older than the number of days specified here.
- If the modified date of files is older than the number of days entered in this field, then those files will be archived.

For example:

If you entered a value of 30 days, then all files older than 30 days in the scanned volume or folder/directory will be archived.

Archive file created time older than _n_ Days

- Enter the number of days elapsed (i.e., the age of the file) since the file was created.
- For archiving, the creation date of each file within that volume or folder/directory is checked to see if it is older than the number of days specified here.
- If the creation date of files is older than the number of days entered in this field, then those files will be archived.

For example:

If you entered a value of 30 days, then all files older than 30 days in the scanned volume or folder/directory will be archived.

Archive file if size is greater than _n_ KB

- Enter the size a file must be in order for the file to be archived.
- If a file size within a scanned volume or folder/directory is greater than this value, then it will be archived.

For example:

If you entered a value of 50 KB, then all files greater than 50 KB in the scanned volume or folder/directory will be archived.

Maximum File Size *n* KB

- Enter the size a file must be in order for the file to be archived.
- If a file size within a scanned volume or folder/directory is less than this value, then it will be archived.

For example:

- If you entered a value of 50 KB, then all files less than 50 KB in the scanned volume or folder/directory will be archived.

Archive if: Any of the file selection rules are satisfied

This rule determines that a file has to satisfy a minimum of one of the rules (i.e., Age or Size) in order to be archived.

Archive if: All of the file selection rules are satisfied

This rule determines that a file has to satisfy both rules (i.e., Age and Size) in order to be archived.

STUB RULE

Replace the File with a Stub

Select this option to replace the files with stubs after running an archive job.

Never

Select this option to retain the stubbed items forever.

Prune stubs only after *n* Days

Select this option and specify the number of days, the stubs will be retained before they are pruned.

For example:

If you enter 120 days then stubs of the archived files will be pruned after 120 days.

Delete the file

Select this option to delete the file from the primary storage after it has been archived.

Prune Archived Items

Select this option to specify the number of days after which the deleted archived items will be pruned. The default value is 730 days.

Compress the File

Select this option to compress files that meet the archiving rules.

Back to Top

Backup Set / Archive Set Properties (General)

- Use the **Backup Set / Archive Set (General)** tab to change the configuration of the selected backup set / archive set.
- Use the **New Backup Set / New Archive Set** dialog box to define a new backup set.
- Use the **On Demand Backup Set / Archive Set (General)** tab to change the configuration of the selected backup set / archive set.
- Use the **Create New On Demand Backup Set / Archive Set** dialog box to define a new on demand backup set / archive set.

Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent for which the information is being displayed.

Client Name / Client Computer

Displays the name of the Client computer on which this backup set / archive set is found.

Billing Department

Displays the name of the billing department, when the backup set is associated with a billing department. For more information on Billing and Costing See the *CommNet Books Online*.

Agent Type / *i*DataAgent

Displays the name of the *i*DataAgent to which this backup set / archive set belongs.

Instance

Displays the name of the instance to which this backup set belongs.

Partition

Displays the Lotus Domino Server data path under which this data is found.

Database Name

Displays the name of the database.

Replication Set

The name of the Replication Set for which the system automatically created this backup set and its default subclient.

Backup Set / New Backup Set Name

Specifies the name of the Backup Set. You can use this space to create or modify a name. (Backup Sets for certain *i*DataAgents cannot be modified.)

Choose Backupset Type

- **SharePoint Server Document**

  The content of this backup set can specify backing up site collections, sub-sites, areas, libraries, and lists.

- **SharePoint Server Database**

  The content of this backup set specifies backing up SharePoint 2007 site collections, WSS web application content databases, shared service providers, WSS searches, global search settings.

- **Force use of V2 APIs**

  Specifies to backup SharePoint 2003 site collections, portal sites, site content databases, site indexes, teamsite databases, and webstorage system databases.

Image Backup Set

Specifies whether the selected backup set will perform a SnapMirror to Tape (aka smtape) block backup. These backup types are supported for NetApp file servers running ONTAP 8.0 or higher. These types of backups are useful if the volumes on the filers contain mirrored snapshots. Moving mirrored snapshots to tape saves filer disk space and provides fast point-in-time volume recovery of mirrored data.

Type

Displays the SharePoint Server version. Applicable only on machines where both SharePoint Server 2003 and 2007 versions exist.

Archive Set / New Archive Set Name

Displays the name of the archive set. If applicable, use this space to enter or change the name of the archive set.

On Demand

Displays whether the selected backup set / archive set is an On Demand Backup Set / Archive Set.

Make this the Default backup set

Specifies whether the selected backup set is the default or a user-defined backup. Selecting this option asserts this backup set as the default. The previously

designated default backup set is automatically reallocated as a user-defined backup set. Clearing this option, is accomplished by opening the Backup Set Properties dialog box of some other backup set and clicking this option there, thereby designating that backup set as the default.

Subclient Content may contain Wildcard Entries

Allows for the selection of files with specified extensions that can be backed up during the backup operation.

Make this the Default archive set

Displays whether the selected archive set is the default, in cases where other types of archive sets are also supported on the same agent (for example: User-Defined Archive Set, DataClassSet, On Demand Archive Set).

Subclient Policy

Displays the name of the Subclient Policy associated with this backup set. If no Subclient Policy is associated with this backup set, it will display "<None>".

Job Options

● **Use Change Journal**

Specifies that NTFS change journal is used to determine whether files have been modified for all subclients within the backup set.

● **Use Classic File Scan**

Specifies that the classic file scan is used to determine whether files have been modified for all subclients within the backup set.

Preserve File Access Time

Specifies whether the file access time is preserved and therefore not modified at the time of backup. Selecting this option may increase the time required to complete a backup.

Check Archive Bit During Backups

Specifies whether files are considered modified and therefore backed up based on either the state of the archive bit or the file modification time. In addition, the system resets the Archive bit of every file that it backs up. This option influences the way incremental and differential backups are conducted for all subclients within the backup set. It does not affect the behavior of full backups.

● **Use Data Classification**

Specifies that the Data Classification Enabler is used to determine whether files have been modified for all subclients within the backup set.

	This field is disabled for Online Content Indexing for NAS File Servers.

● **Decompress Data before Backup**

Specifies that data on a compressed drive is decompressed before being sent to the backup media, thereby preventing data recovery failures when restoring data to a volume that does not support compression. By default, data is backed up in compressed format if the data is on a volume that supports compression. When this option is initially selected, the next backup for each subclient within the backup set is converted to a full. This ensures that all of the client's compressed data is decompressed, including all data backed up prior to this selection.

Next Backup

Displays whether the next backup job may be full or non-full. When Next Backup displays Full the next backup job will be changed to a full.

Available DB Names

Select the database name(s) to be used as backup set name(s) by clicking the database name(s) and then clicking > to move the name(s) into `Selection`.

Selection

Specify the appropriate backup set (database) name(s) from the Available `DB Names`.

Storage Policy for All Log Files

Specifies the storage policy for all the log files in this backup set. You can use the list to change the storage policy.

Catalog Partition No.

Specifies the number of the catalog partition database for the DB2 DPF instance. This is the partition through which access to all system tables must go.

Connect as a Different User

Specifies to connect to the DB2 application using a different DB2 user account.

User Account

Displays the application User account used by the system to perform all Data Protection and Recovery operations for this backup set.

Change

Click to change the application user account.

Status of <database>

Displays the status of the database (backup set) as either CONNECTED or DISCONNECTED.

Refresh

Displays the most current status of the database.

Subclient

Displays those subclients that belong to the backup set / archive set.

Storage Policies

Select a storage policy from the list.

Enable Auto-Discover

Specifies whether to enable auto-discovery of new databases for all subclients of this backup set. Selecting this option will cause the system to discover and assign any new databases at the beginning of each backup operation. This option is available only for default dump backup set of postgresql *i*DataAgents.

Description

Use this field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.

Add

Click to create a subclient for the backup set / archive set.

Edit

Click to change the properties of a subclient that you select from the list.

Delete

Removes a subclient that you select from the list.

Back to Top

Security

Use this dialog box to:

- Associate this object with a user group.
- Disassociate this object from a user group.

Available Groups

Displays the names of the user groups that are not associated with this CommCell object.

Associated Groups

Displays the names of user groups that are associated with this CommCell object.

Backup/Archive Options

Use this dialog box to schedule or immediately run a backup/archive job. Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent for which the information is being displayed.

Select Backup Type

- **Full**

  Specifies the job as a Full backup, which backs up all data for the selected subclient(s).

- **Incremental**

  Specifies the job as an Incremental backup, which backs up only that portion of the data that is new or has changed since the last backup.

  ○ **Transaction Log**

  Specifies the job as a transaction log backup. This will back up the transaction log, providing point-in-time restore functionality.

  Do not truncate log

  Specifies the operation will back up the transaction log in situations where the database is damaged or has not been recovered.

  Skip full after log backup

  Specifies that a full backup will be skipped after a transaction log backup has taken place.

  > For the Oracle, DB2, Informix, and SAP for Oracle *i*DataAgents, **Incremental** backup works like **Differential** backups described in the online documentation.

  ○ **Level**

  Specifies the level of incremental backup for Oracle backups. Valid values are from 1 to 4.

  ○ **Cumulative**

  Specifies a Cumulative Incremental backup at level 1 to 4 for Oracle backups. When cleared, the system performs a non-cumulative backup.

- **Differential**

  Specifies the job as a Differential backup, which backs up only that portion of the data that is new or has changed since the last full backup.

  Delta

  Specifies the job as a delta backup, which backs up all data that is new or has changed since the last backup for the selected subclient.

- **Pre-Selected Backup Type**

  Specifies the job as either an Incremental or Differential backup, as determined during installation or later through client configuration. An Incremental backup backs up all data that is new or has changed since the last backup for the selected subclient. A Differential backup backs up all data that is new or has changed since the last Full backup for the selected subclient.

- **Synthetic Full**

  Specifies the job as a Synthetic Full backup, which creates a Full backup from existing backup data for the selected subclient or backup set (if applicable). The Synthetic Full backup consolidates the backup data; it does not actually back up data from the client computer.

  > If applicable for your agent, the **Verify Synthetic Full** option in the Advanced Backup Options dialog box will include never-changing files in the next backup. This option is enabled by default.

  Run Incremental Backup

  Specifies the options for running an Incremental backup either immediately before a Synthetic Full backup or immediately after a successfully completed Synthetic Full backup when selected. When cleared, an Incremental backup is not automatically run either immediately before or after the Synthetic Full backup.

  ○ **Before Synthetic Full**: Specifies the operation will back up any data that is new or changed since the previous backup in order to have it included as part of the Synthetic Full backup.

  ○ **After Synthetic Full**: Specifies the operation will back up any data that is new or changed since the backup that occurred prior to the Synthetic Full backup.

Job Initiation

- **Run Immediately**

  Specifies this job will run immediately.

- **Schedule**

Specifies this job will be scheduled. Click **Configure** to specify the schedule details.

Configure Alert

- **Alert**

  The currently configured Alert.

- **Add/Modify Alert**

  When clicked, opens the Alert Wizard to configure alerts for this operation.

- **Delete Alert**

  When clicked, deletes any existing alerts that are already configured.

Directive File

Use this space to specify the Directive File to be used when running On Demand Data Protection operations. For NAS NDMP *i*DataAgents and the File Archiver for Windows Agents, you will specify a Content file instead of a Directive File.

- **Browse**

  When clicked, opens a window in which you can browse to and select the Directive File (or Content File for NAS NDMP *i*DataAgents and the File Archiver for Windows Agents).

Description

Use this field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.

Advanced

Click to select advanced backup/archive options, such as create a new index, start new media, and mark media as full.

Save As Script

Click to open the Save As Script dialog, which allows you to save this operation and the selected options as a script file (in XML format). The script can later be executed from the Command Line Interface using `qoperation execute` command.

When you save an operation as a script, each option in the dialog will have a corresponding xml parameter in the script file. When executing the script, you can modify the value for any of these XML parameters as per need.

To view the XML values for each of the options in the dialog, see the following:

- Command Line XML Options for Active Directory *i*DataAgent
- Command Line XML Options for Lotus Notes Database *i*DataAgent
- Command Line XML Options for Lotus Notes Document *i*DataAgent
- Command Line XML Options for Image Level *i*DataAgent
- Command Line XML Options for Image Level ProxyHost *i*DataAgent
- Command Line XML Options for Netware File System *i*DataAgent
- Command Line XML Options for NAS NDMP *i*DataAgent
- Command Line XML Options for PostGreSQL *i*DataAgent
- Command Line XML Options for ProxyHost *i*DataAgent
- Command Line XML Options for Microsoft Windows File System *i*DataAgent
- Command Line XML Options for Macintosh File System *i*DataAgent
- Command Line XML Options for Microsoft Data Protection Manager
- Command Line XML Options for Novell GroupWise *i*DataAgent

Back to Top

Advanced Backup/Archive Options (Data)

You can select advanced backup/archive data options for the operation. Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent or enabler for which the information is being displayed.

Create new index

Specifies the system will create a new index with a full or On Demand data protection operation, and for archive operations. Selecting this option will cause the following to occur for this job only:

● full backup transparent browse capability will be disabled, if it is supported by the agent.

● override the **Create new index on full backup** option on the **Agent Properties (Index)** tab

● for an On Demand Data Protection operation, override the **Set index cycle to every *nn* backup jobs** setting in the **Subclient Properties (General)** tab of the default subclient.

● for Archiver Agents, a new index will be automatically created during the first archiving job run after January 1st provided the associated subclient was created prior to July 1st of the preceding year. If a subclient is created between July 1st and December 31st, the new index will be automatically created during the first archiving job run after January 1st of the year after the next. For example, **Subclient A** was created on March 1st, 2009. When **Subclient A**'s first archiving job of 2010 was run on January 15th 2010, a new index was automatically created. **Subclient B**, however, was created on August 5th, 2009. Therefore, a new index for **Subclient B** will not be created until the first archiving job run in 2011.

Still, a new index can always be created on-demand for an individual job at any time. This is possible by selecting the Create New Index option in the Advanced Backup Options of a backup or schedule policy dialog box.

Follow Mount Points

When selected (default) for Macintosh File System, Unix File System, or Windows File System, specifies that the backup will include both the mount point and the data pointed to from that mount point. For Windows File System, this data is backed up even if it is included in another subclient; therefore, data for this file system can be duplicated in the backup. For all supported file systems, clearing the `Follow Mount Points` option in the Advanced Backup Options dialog box causes the configuration (i.e., the mount point) to be backed up *without backing up the data* on the mounted volume.

Back up Data in Remote Storage

For Windows file systems, specifies that the backup include the data pointed to in remote storage. By default, the system backs up only the **reparse points** — pointers to the remotely stored data — and not the data itself. You must select the `Backup data in remote storage` option in the Advanced Backup Options dialog box in order to back up the actual remote storage data.

HotFix Information

For Windows file systems, specifies that information will be collected about all hot fixes for the operating system configuration. This is useful in situations where knowledge of the operating system configuration is vital to successfully restoring a system. It is also useful in disaster recovery scenarios.

Back up Files Protected by System File Protection

Specifies the backup is to include those files that are protected by the Windows System File Protection feature. This feature protects shared files that may be overwritten by application installations, such as dynamic link libraries (DLLs). This option is available for any subclient that backs up the System State.

Stop DHCP Service when Backing up System State Data

For Windows file systems, specifies the system stop DHCP services on the client computer when System State data is backed up. This option is provided for cases where you cannot use VSS to back up the System State.

Stop WINS Service when Backing up System State Data

For Windows file systems, specifies the system stop WINS services on the client computer when System State data is backed up. This option is provided for cases where VSS cannot be used to back up the System State.

Include files that do not match with destination copy

Select this option to replicate the new, modified, or missing files to the destination computer.

Generate data verification after backup completes

Select this option to generate a data verification report after the backup job is completed, to compare files and folders between the source and the destination computers.

SQL Native Backup Compression

For SQL Server 2008 Enterprise or later, specifies that the backup will be compressed by SQL Server before being backed up. The size of the backup will be smaller than an uncompressed backup of the same data. Typically, compressing a backup will require less device I/O which should increase backup speed significantly. However, CPU usage may increase for compressed backups and you may want to evaluate performance counters. Scheduling the backup during off-peak hours or compressing only low-priority backups may be desirable. When using the SQL Native Backup Compression option, there is no need for deduplication as the data will be compressed with this option and deduplication will not consequently save any more space.

	VSS-enabled and SnapProtect backups are not supported backup types for compression.

Create Backup Copy immediately

Select to create an inline backup copy to start movement of snapshot to media, immediately after the completion of the SnapProtect backup job.

Verify Synthetic Full

Specifies to include never-changing files in the next backup when **Synthetic Full** is selected in the Backup Options dialog box. This is especially useful if you run a conventional full backup only once for a given subclient, and then run incremental (or differential) backups with periodic synthetic full backups after that for an extended period of time. This option is enabled, by default.

Ignore Error in Synthetic Full

Specifies to ignore any errors that may be encountered in synthetic full backups. This is useful when running full backups is not possible and when synthetic full backups are continuously run, even is backup media is partially corrupted. Can only be selected when **Verify Synthetic Full** is enabled.

Check for Deleted Stubs

Select this option to restore stubs that are moved anywhere within the client.

Partial (Excludes read-only Filegroups)

A partial backup resembles a full database backup, but does not contain all the filegroups. Instead, it contains all the data in the primary filegroup, every read/write filegroup, and any optionally-specified read-only files. Partial backups are useful whenever you want to exclude read-only filegroups. A partial backup of a read-only database contains only the primary filegroup.

Tail-log Backup (database is left in restoring state)

This advanced backup option is only available if the **Transaction Log** option was selected in the Backup Option dialog box. Specifies to back up the tail of the log and to leave the database in the RESTORING state.

Copy Only

A copy-only backup is an independent backup and does not affect the usual chaining involved in traditional backups. This type of backup can be performed for a special purpose and does not affect the overall backup and restore procedures. It applies to full backups, full Volume Shadow Services (VSS)-enabled backups, and full SnapProtect backups.

After taking a full copy-only backup, log backups cannot be run unless a traditional full backup is present. Differential backups can be run but they cannot be restored unless a traditional full backup exists prior to the differential.

Catalog

Use this section to select index cache sharing and granular restartability options for the job. Note that these options are not applicable for the disaster recovery data protection.

- **Use shared profile if present with transaction logging**

  Select this option if you wish to use the shared index cache profile of the MediaAgent (if configured) to save a copy of the job's index cache for index cache sharing *with* transaction logging feature for granular job restartbility.

  Shared profile with transaction logging provides job restartability in failover situations. This is a recommended configuration.

- **Use shared profile if present without transaction logging**

  Select this option if you wish to use the shared index cache profile of the MediaAgent (if configured) to save a copy of the index cache for index cache sharing *without* transaction logging feature for granular job restartbility. This is not a recommended configuration.

- **Use transaction logging**

  Select this option to use transaction logging feature to provide granular job restartbility (without using shared profile for index cache sharing).

- **None**

  Select this option to use neither shared profile nor transaction logging.

Optimize for Novell SMS-based Fast Backup

Select this option to run a full backup job, which will utilize Novell's Storage Management Services (SMS) to query the configured subclient content for the data to be backed rather than generating a collect file during the scan phase.

Perform Consistency Check

Select this option to perform a consistency check.

- **Throttle check for 1 second**

  Enter the number of I/O operations to complete before a consistency check is performed.

Enable Granular Recovery

Click to perform Granular Recovery. When clicked, allows recovery of Individual files and folders.

Advanced Backup/Archive/Content Indexing Options (Startup)

You can specify advanced backup/archive/content indexing startup options for the operation. For more information, select one of the following:

Set a Job Priority

Description

Use this field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.

Startup in Suspended State

Job Retry

Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent or operation for which the information is being displayed.

Enable Total Running Time

The maximum elapsed time, in hours and minutes, from the time that the job is created. When the specified maximum elapsed time is reached, as long as the job is in the "Running" state, it will continue; if the job is not in the "Running" state when the specified time is reached, Job Manager will kill the job.

Enable Number of Retries

The number of times that Job Manager will attempt to restart the job. Once the maximum number of retry attempts has been reached, if the job has still not restarted successfully, Job Manager will kill the job. Note that this job-based setting will not be valid if restartability has been turned off in the Job Management Control Panel.

Kill Running Jobs When Total Running Time Expires

Option to kill the job when the specified Total Running Time has elapsed, even if its state is "Running". This option is available only if you have specified a Total Running Time.

Advanced Backup/Archive Options (Media)

You can select advanced backup/archive media options for the operation. Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the agent or enabler for which the information is being displayed.

Start New Media

This option starts the backup/migration/archive operation on a new media, which causes the following to occur:

● If removable media is used, the current active media is marked as Appendable and a new media is used for the backup/migration/archive.

● If disk media is used, a new volume folder is created for the backup/migration/archive.

If cleared, the operation automatically uses the current active media or volume.

> When using the Informix *i*DataAgent, if you are using tape and do all of the following, the tape will be marked full for both the data storage policy and the logical logs storage policy, and new media will be made available for both the logs and data even though you are backing up just the logical logs:
> ● Define a subclient with different storage policies for the logical logs and the data
> ● Prepare to back up just the logical logs
> ● Select the **Start new media** option before you start the backup

Mark Media Full after Successful Operation

This option marks media full, 2 minutes after the completion of the backup/archive operation. If any jobs are initiated within the 2 minutes, they are allowed to write to the media. If the job was associated with the prior media, new media (such as a new tape) will be used for subsequent jobs. (Applies to all backup/archive types.)

Allow other Schedule to use Media Set

This option allows jobs that are part of a schedule policy or schedule and using a specific storage policy to start a new media and also prevent other jobs from writing to the set of media. It is available only when the **Start New Media** and **Mark Media Full** options are enabled, and can be used in the following situations:

● When one scheduled job initiates several jobs and you only want to start new media on the first job.

● When you want to target specific backups to a media, or a set of media if multiple streams are used.

Reserve Resources Before Scan

Normally, media is reserved for a job before the operation phase (backup or archive). When selected, this option will reserve the media before the scan phase. This reserves the media earlier because the scan phase precedes the operation phase.

Job should wait for Inline Copy Resources

If you are performing a data protection/archive operation on a subclient with a storage policy that has the Inline Copy option enabled, then this option specifies that the operation should wait until resources are available for both the data protection/archive operation and the Inline Copy. (This option is available only if an Inline Copy is created on the storage policy that is being used for this data protection operation).

If cleared, the data protection operation will create the Primary copy even if there are not enough resources to create the Inline Copy.

Override Job Retention

● **Infinite**: Select this option to retain this job indefinitely.

● **Number of Days**: Select this option to prune this job after the number of days specified.

● **Storage Policy Default**: Select this option to apply the retention rules of the associated storage policy, which is the default option.

Advanced Backup Options (Data Path)

Select the data path to be used for the backup/archive operation.

Ensure that the Library, MediaAgent, Drive Pool, and Drive selected for this operation is available online and is a part of the associated Storage Policy.

Use MediaAgent

Specifies the name of the MediaAgent that will be used to perform the backup operation. If necessary, you can change the name of the MediaAgent.

For example, if the library is shared and you wish to use a specific MediaAgent (instead of the system selected MediaAgent, or a MediaAgent which may be idle, or less critical) or if you know that the library attached to the specified MediaAgent.

Use Library

Specifies the name of the library that will be used to perform the backup operation. Use this option when you wish to backup to a specific library.

Use Drive Pool

Specifies the name of the Drive Pool that will be used to perform the backup operation. Use this option when you wish to backup using a specific Drive Pool.

Use Drive

Specifies the name of the Drive that will be used to perform the backup operation. Use this option when you wish to backup using a specific Drive from the selected Drive Pool.

Vault Tracking

Select options to export and track media, using Vault Tracker.

Vault Tracking Options will be displayed only when a Vault Tracker license is available in the CommServe.

Vault Tracking options are only applicable for data protection operations using a storage policy associated with a library containing removable media (e.g., tape, optical or stand-alone.)

Export media after the job finishes

Specifies the media used by the data protection operation and media with the specific Media Status (if specified) will be exported and tracked by Vault Tracker.

Exclude Media Not Copied

When selected, allows you to exclude media with jobs that have to be copied.

Media Status

- **All**

  Click to select all media. Clear this option to select media with a specific status.

- **Active**

  Click to select media with its status marked as active.

- **Full**

  Click to select media with its status marked as full.

- **Overwrite Protected**

  Click to select media with its status marked as read-only .

- **Bad**

  Click to select media with its status marked as bad.

Export Location

Specifies the destination location and lists the stationary locations entered using the **Export Location Details** dialog box.

Track Transit

Specifies that transit information must be tracked, and lists the transit locations entered using the **Export Location Details** dialog box.

Use Virtual Mail Slots

Specifies the exported media is stored within the library in the virtual mail slots defined in the **Library Properties (Media)** dialog box.

Filter Media By Retention

Specifies that the system must automatically filter media based on whether the media has extended retention jobs or not.

- **Media with extended retention job(s)**

  Specifies that media with at least one extended retention job will be exported.

- **Media with no extended retention job(s)**

  Specifies that media with no extended retention jobs will be exported.

Alert

Use this tab to configure an alert for a schedule policy.

Configure Alert

- **Alert**

  The currently configured Alert.

- **Add/Modify Alert**

  When clicked, opens the Alert Wizard to configure alerts for this operation.

- **Delete Alert**

  When clicked, deletes any existing alerts that are already configured.

Restore/Recover Options (General)

Use this dialog box to control how the specified data is to be restored/recovered. This dialog box is also used for selecting options related to scheduled or non-scheduled search and restore/recover operations. Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the component installed on the client.

Restore/Recover ACLs (Only) - Windows

Specifies that the backed up Access Control Lists (ACLs) will be applied to files that have been restored without their ACLs, or to the existing files at the restore destination. Clear this option to restore without ACLs and consequently the data assumes the ACLs of the parent directory.

Restore Data Only - Windows

Specifies that the files will be restored without their original ACLs. Files and folders will inherit the permissions of their parent folder or drive.

Restore Both Data and ACLs - Windows

Specifies that all data will be restored with its original access control lists (i.e., ACL) and therefore its original security attributes.

Overwrite

- **Overwrite if file on media is newer**

  If selected, this option will overwrite the existing file with the file that was backed up/archived to the media provided the backed up/archived file is newer than the existing file.

- **Unconditional Overwrite**

  Specifies whether the restored data is unconditionally written to the specified location.

  If cleared:

  ○ Files/directories whose names are the same as those in the restore path and where the backed up data is as old or older are not restored.

  ○ files/directories whose names are the same as those in the restore path and where the backed up data is newer are restored.

  ○ Files/directories whose names are different from those in the restore path are restored.

  Avoid using this option whenever you run a Restore by Jobs. Otherwise, an older version of the files might be retrieved.

- **Restore only if target exists**

  If selected, this option will only restore files that currently exist in the restore path. Files that exist on the media but not in the restore path will not be restored.

Restore Data Instead of Stub

If selected this option will restore the backed up data which may be stubbed.

Recreate Mount Points

Selection of this check box allows for the creation of Mount Points.

Restore only if Target is a DataArchive Stub

Specifies whether a DataArchiver stub will be unconditionally overwritten during recovery.

Restore/Recover Destination

- **Destination Client/Computer/Server**

  Displays the name of the client computer to which the selected data will be restored. To change the destination computer, select one from the list. The list includes clients:

  ○ Which are established as clients within the CommCell.

  ○ Clients with Operating Systems that support the cross-platform restore operation from this client. (Refer to the topic titled **Cross Platform Restore Operations** in Books Online for additional information.)

  By default, data is restored to the same computer from which it was backed up.

- **Restore/Recover to Same Paths**

  Specifies whether the restore operation will restore data to the same path from which it was backed up in the **Destination Computer**. (Clear this option to restore to a different path and activate the **Destination folder** box.)

- **Destination folder**

  Use this space to enter the path on the destination computer to which the data will be restored. If the specified path does not exist, it will be created during the restore process.

On Windows computers, UNC path of a shared drive can be specified. (e.g., `\\servername\sharename\directory`). Click the **Advanced** button, and enter the Windows logon information for this shared drive in the **Advanced Restore Options** dialog box.

- **Browse**

  Click to select a path for the **Destination folder**.

Preserve Source Paths

Specifies the action taken when the data is restored to another destination. The options are available only when the **Restore to Same Paths** option is cleared.

- **Preserve n levels from end of source path**

  Specifies whether the restore operation must keep the specified number of levels at the end of source path of the selected data. For example, if the selected data is `Documents\Memos\Sales`, this option is set to `1` and the **Destination folder** is `temp`, the data will be restored as `\temp\Sales`.

  However, if this option is used to restore a file in a path that contains any valid wildcard expression (e.g., `Documents\**\Sales`), the default value of `1` for the option cannot be changed. Therefore, only the last found occurrence of the file is restored, and the restores for all the other occurrences of the file are overwritten.

- **Remove n levels from beginning of source path**

  Specifies whether the restore operation must remove the specified number of levels from the beginning of source path of the selected data. For example, if the selected data is `Documents\Memos\Sales`, this option is set to `1` and the **Destination folder** is `\temp`, the data will be restored as `\temp\Sales`. (This option becomes available only when the **Restore to Same Paths** option is cleared.)

Advanced

Click to select additional restore options.

Virtual Server *i*DataAgent

- **Restore As (Disk-Level Restore)**

  Virtual Machines

  Select this option to restore the selected content as an entire virtual machine.

  Container Files

  Select this option to restore the selected content as a container file.

- **Restore As (Volume-Level Restore) (VMware Only)**

  Physical Volume

  Select this option to restore the selected content as a complete physical volume.

  VMD files

  Select this option to restore the selected content as an entire virtual machine disk file.

  VHDK file

  Select this option to restore the selected content as a virtual hard disk file.

- **Virtual Machine Restore Options (VMware Only)**

  VM Name

  The name of the virtual machine to be recovered.

  Server Name

  The name of the server to which the data will be recovered. The name entered in this field depends on the which of the following options are selected:

  - **Virtual Center**

    If selected, the **Server Name** field must include the name of the Virtual Center.

  - **Virtual Center ESX Server Name**

    The name of the ESX Server in the Virtual Center.

  - **ESX Server**

    If selected, the **Server Name** field must include the name of the ESX Server.

- **Authentication**

  Use this section to enter the credentials for the server selected in the **Virtual Machine Restore Options** section.

  User Name

The user account that will be used to access the operating system, application, or network path.

Password

Use the space to type the password for the **User Account.**

Confirm Password

Use the space to re-type the password for confirmation.

Save As Script

Click to open the Save As Script dialog, which allows you to save this operation and the selected options as a script file (in XML format). The script can later be executed from the Command Line Interface using `qoperation execute` command.

When you save an operation as a script, each option in the dialog will have a corresponding xml parameter in the script file. When executing the script, you can modify the value for any of these XML parameters as per need.

To view the XML values for each of the options in the dialog, see the following:

Command Line XML Options for Microsoft Windows File System *i*DataAgent

Command Line XML Options for Workstation Backup Agent

Command Line XML Options for File Archiver for Windows

Command Line XML Options for File Archiver for Unix

Advanced Restore/Recover/Retrieve Options (General)

Use this dialog box to access additional restore/recover/retrieve options. Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the component installed on the client.

Skip MountPoint Restore

Specifies whether to filter out mount points that are part of the backup data during the file system restore. When enabled, the file system restore will filter out the mount points from the backed up data. When disabled, mount points will also be restored during the file system restore.

Automatically Detect Regular Expressions

Specifies whether to use regular expressions in defining the **Source Paths**. This does not apply to **Filter Paths**. When selected, the system will recognize supported regular expressions (wildcards) in the specified **Source Path**. When cleared, the system will read the specified **Source Path** as literal.

Restore Space Restrictions

For NetWare, specifies whether to restore the user space restrictions for folders and volumes. If space restrictions were changed after backup, the backed up restrictions are restored. For example, suppose an original space restriction of 2MB is backed up, and the restriction is later changed to 4MB. If you select **Restore Space Restrictions** and restore the backed up restriction of 2MB, the restriction is reduced to 2MB and any data that exists beyond the 2MB is truncated. (Default = Enabled.)

Skip Errors and Continue

For index-based agents, this advanced restore/recover/retrieve option enables a restore/recover/retrieve job to continue despite media errors. This option also provides an output file that lists the full path names of the files that failed to restore/recover/retrieve.

Recover all protected mails

For the Exchange Mailbox Archiver Agent, specifies whether to recover all e-mail messages that were backed up or archived in the selected mailbox(es) or folder(s) from the latest data or point-in-time through the oldest available index.

Disaster recovery/Media recovery (to another machine)

For Lotus Notes Database, specifies whether to restore and replay transactions when the active extent of the transaction log is lost. This option is also used when you perform a cross-machine restore that includes transaction logs.

Do not select this option unless you are performing either disaster recovery or a cross-machine restore to a new partition.

Ignore Namespace Requirements

For NetWare, specifies whether to restore the data backed up from one namespace to another type of namespace. For example, you can restore long file names to an 8.3 namespace. However, when restoring to a namespace different than that from which the data was backed up, any filenames must be valid for at least one of the available namespaces of the destination volume.

This option **must** be used if you are restoring multiple objects and if some of the objects have a longer name than the available namespaces allow. This option ensures that only those files whose filename is valid for at least one of the available namespaces are restored. Those files whose filename is not supported by the available namespaces are not restored.

Impersonate (Windows, NetWare) User

Specifies whether to submit the Windows or NetWare logon information for the current restore/recover operation. This information is needed only if you intend to restore/recover data to a mapped network drive, shared network drive, or directory to which you have no write, create, or change privileges, or for restoring to applications.

Depending on the agent, there are as many as three separate User Impersonation accounts: this one for the function described, one for Pre and Post backup/migrate processes, and one for Pre and Post restore/recover processes. Each account operates independently of the other(s).

Use hardware revert capability if available

Specifies whether to revert the data to the time when the snapshot was created. Selecting this option brings back the entire LUN to the point when the snapshot was created, overwriting all the modifications to data since the snapshot creation. This option is only available if the snapshot engine used for SnapProtect backup supports the revert operation.

Startup

Select from the following options. Note that all the options described in this help may not be available and only the options displayed in the dialog box are applicable to the operation for which the information is being displayed.

Priority

- **Use Default Priority**

  If selected, the default priority for this type of job will be used in determining how the Job Manager will allocate resources for this job.

- **Change Priority**

  Use this option to manually specify the priority for the job, between 0 (highest priority) and 999 (lowest priority). The Job Manager will use the priority setting when allocating the required resources. This is useful if you have jobs that are very important and must complete, or jobs that can be moved to a lower priority.

Start up in suspended state

Specifies that this job will start in the Job Controller in a suspended state and cannot run until the job is manually resumed using the **Resume** option. This option can be used to add a level of manual control when a job is started. For example, you could schedule jobs to start in the suspended state and then choose which scheduled jobs complete by resuming the operation started in the suspended state.

Description

Use this field to enter a description about the entity. This description can include information about the entity's content, cautionary notes, etc.

Advanced Restore Options (Pre/Post)

Establish pre/post processes for restore jobs, and the account that has permissions to run these processes (for Windows-based agents).

Pre Recovery Command:

Displays the name/path of the process to run before the restore. Add or modify the name/path, or use the **Browse** button to search for and select the name/path. The system allows the use of spaces in the name/path, provided they begin with an opening quotation mark and end with a closing quotation mark.

Post Recovery Command:

Displays the name/path of the process to run after the restore. Add or modify the name/path, or use the **Browse** button to search for and select the name/path. The system allows the use of spaces in the name/path, provided they begin with an opening quotation mark and end with a closing quotation mark.

Run Post Restore Process for all attempts

Specifies whether this process will execute for all attempts to run the phase. Selecting this option will execute the specified process for all attempts to run the phase, including situations where the job phase is interrupted, suspended, or fails. Otherwise, when the checkbox is cleared the specified process will only execute for successful, killed, or failed jobs.

Pre/Post Impersonation

For Windows-based agents, you must designate either the Local System Account or, for added security, another account as having permission to run these commands for restore jobs.

- **Use Local System Account**

  Normally, the Local System Account has permissions to access all the data on the local computer.

- **Impersonate User**

  Select this check box to enable the User Name and Password boxes. If the Impersonate User account defined here is not available, restore jobs using pre/post commands will fail. This account operates independently of the Impersonate User account for backup jobs.

- **User Name**

  Enter the Window's user account name which will have permission to execute the desired commands.

- **Password**

  Enter the corresponding password for this account.

- **Confirm Password**

  Enter the password again for this account.

Advanced Restore Options (Copy Precedence)

Choose the copy from which you wish to recover or retrieve. Select from the following options:

Restore/recover from copy precedence

When selected, the system retrieves the data from the storage policy copy with the specified copy precedence number. If data does not exist in the specified copy, the operation fails even if the data exists in another copy of the same storage policy.

When cleared, (or by default) the system retrieves data from the storage policy copy with the lowest copy precedence. If the data was pruned from the primary copy, the system automatically retrieves the data from the other copies of the storage policy starting with the copy with the lowest copy precedence and proceeding through the copies with higher copy precedence. Once the data is found, it is retrieved, and no further copies are checked.

Use MediaAgent / Library / Drive Pool

See Advanced Restore Options (Data Path)

Advanced Restore Options (Data Path)

Select the data path for the restore/recovery operation. You can specify the MediaAgent, Library, Drive Pool, and Drive from which the restore operation must be performed.

Use MediaAgent

Specifies the name of the MediaAgent that will be used to perform the restore operation. If necessary, you can change the name of the MediaAgent.

For example, if the library is shared and you wish to use a specific MediaAgent (instead of the system selected MediaAgent, or a MediaAgent which may be idle, or less critical) or if you know that the media containing the data you wish to restore is available in the library attached to the specified MediaAgent.

If the media containing the data is not available in the tape/optical library attached to the MediaAgent, the system will automatically prompt you to insert the appropriate media. In the case of a disk library, the operation will fail if the requested data is not available in the disk library attached to the specified MediaAgent.

Use Library

Specifies the name of the library that will be used to perform the restore operation. Use this option when you wish to restore using a specific library.

For example, if you know that the media containing the data you wish to restore is available in a specific library.

Use Drive Pool

Specifies the name of the Drive Pool that will be used to perform the restore operation. Use this option when you wish to restore using a specific Drive Pool.

To restore NAS data, select the drive pool type that was used to perform the backup, *i.e.*, if a drive pool associated with an NDMP Remote Server was used to perform the backup, select a drive pool associated with an NDMP Remote Server. Similarly, if an NDMP drive pool was used, specify an NDMP drive pool.

Use Drive

Specifies the name of the drive in the drive pool that will be used to perform the restore operation. Use this option when you wish to restore using a specific Drive in the Drive Pool.

Use Proxy

Specifies the name of the proxy server that will be used to perform the restore operation. Use this option when you wish to restore using a proxy server.

Advanced Restore Options (Paths/Filters)

Source Paths

Displays the data that is to be restored. If you previously browsed and selected backed up data for restoration, this pane lists the paths of the selected data. Click the **Add** button to type the path of the data to be restored. Select a listed path and click the **Delete** button to remove the path of data to be restored.

Filter Paths (exclude)

Displays the data that is to be excluded from the restore/recovery. If you previously browsed the backup/migration data and deselected files/folders/directories that are children of **Source Paths** directories, then this pane lists the paths of the selected data. You can use this space along with the **Add** button to exclude manually the path of data to be restored/recovered. You can also select an entry in this space and use the **Delete** button to remove a selected entry.

You can also use wildcard characters within this pane to specify file name patterns that you want to exclude from the restore/recover operation. The supported wildcard characters are:

- * = any number or characters

- ? = any one character

- [] = any range or set of characters

When wildcard characters are utilized in the filter path, they are automatically detected by the system. In the event that the actual file, folder, or directory name in the filter path contains a character that can be used as a wildcard, you can override wildcard auto-detection by adding an exclamation mark as the first character of your path (e.g., `!/company/[test]` for Unix-based systems, `!sys:\company\[test]` for Windows-based systems). In these examples, rather than treating the square brackets as a wildcard, the system would look for (and exclude from the restore/recovery) a folder or directory named `[test]`.

Advanced Restore Options (Encryption)

Pass-Phrase

Enter the pass-phrase that is currently assigned to the client, whose data you are restoring. Note that if you have changed the pass-phrase since you secured the client data, you need to provide the new pass-phrase here, not the old one.

Re-enter Pass-Phrase

Re-enter the pass-phrase for confirmation.

If you attempt an immediate restore of encrypted data that was pass-phrase protected without entering the pass-phrase here, the restore operation will fail.

If you have an exported pass-phrase set up, and you enter the pass-phrase under **Decryption**, you over-ride (not overwrite) the client properties pass-phrase. Thus, if you enter the pass-phrase incorrectly, the restore does not complete successfully.

Advanced Restore Options (Map)

Specify the restore of individual files to a specified destination using an external map file. The map file provides the list of files to be restored and the destination to which the files are to be restored. (See **Restore Data Using a Map File** in *Books Online* for detailed information.)

Use map file

Specifies whether the restore operation must be performed using a mapping file. Enable this option to specify the map file.

Map File Path

Specifies the name of the map file. Use the space to enter the path and name of the map file. Use the browse button to browse and select the appropriate map file.

Restore unmapped files

Specifies whether the restore operation must restore the unmapped files that were selected for restore, to the specified restore destination. *i.e.*, in-place restore or out-of-place restore. Clear this option to restore only those files that are included in the specified map file.

Rename all restore files with suffix

Specify a common suffix to be added to each file as it is restored. For Windows platforms, this suffix is appended to the filename (i.e., before the extension); for Unix/Mac platforms, the suffix is appended after the extension.

Advanced Recover Options (Browse Options)

Use this dialog box to specify advanced restore options.

Restore Deleted Items

Specifies that the restore/recovery operation will include data that was secured during all backup/archive operations, including deleted items.

Specify Time Range

Specifies to restore/recover data within a specified time zone and time threshold. Select the checkbox to enable this option. Clearing the checkbox disables this option. If this option is enabled, set the following parameters:

- **Time Zone** - Restores/recovers only those jobs within a specified time zone. Click the pull-down list and click the desired time zone.
- **Start Time** - Displays the start time for the restore/recovery operation. Click the pull-down arrow and click a date; use the up and down arrows to specify a time.
- **End Time** - Displays the end time for the restore/recovery operation. Click the pull-down arrow and click a date; use the up and down arrows to specify a time.

Operation Window

Use this dialog box to add, modify, or delete operation rules for system operations.

Name

The friendly name assigned to the operation window.

Operations

The operations included in the rule.

Days

Displays the days in which the operations in this rule should not be run.

Do not run intervals

Displays the times in which the operations in this rule should not be run.

Add

Click this button to add an operation rule from the Operation Rule Details dialog box.

Modify

Click this button to modify an operation rule from the Operation Rule Details dialog box.

Delete

Click this button to delete an operation rule.

Ignore Operation Rules at Higher Levels (not applicable at the CommServe and Client group level)

Select this option to disable all operation rules set at levels above the currently selected entity.