

Features - SharePoint Server *i*DataAgent

TABLE OF CONTENTS

OVERVIEW

SYSTEM REQUIREMENTS - SHAREPOINT SERVER /DATAAGENT

INSTALLATION

- Install the SharePoint Server *i*DataAgent

BACKUP DATA - SHAREPOINT SERVER /DATAAGENT

RESTORE DATA - SHAREPOINT SERVER /DATAAGENT

CONFIGURATION

- Backup Sets - SharePoint Server *i*DataAgent
- Subclients - SharePoint Server *i*DataAgent

MANAGEMENT

- Backup Job History
 - Restore Job History
-

Overview - SharePoint Server iDataAgent

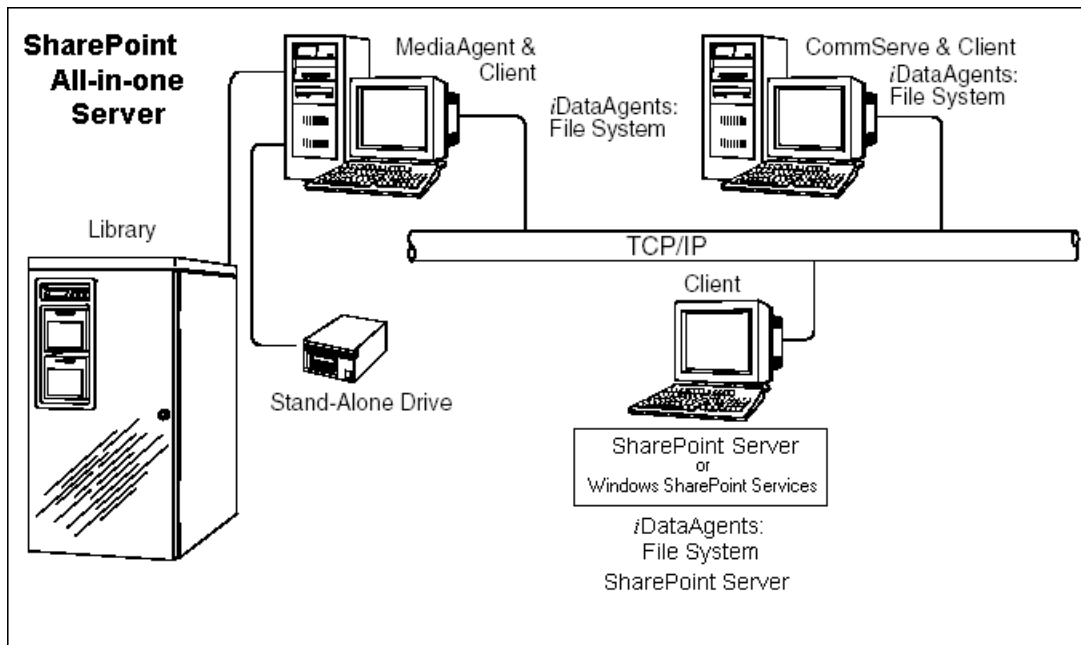
Choose from the following topics:

- Introduction
 - SharePoint Servers, SharePoint Clients, and Clients
- Supported Data Types
- Tree Levels in the SharePoint Server iDataAgent
- License Requirement
- Disaster Recovery Considerations

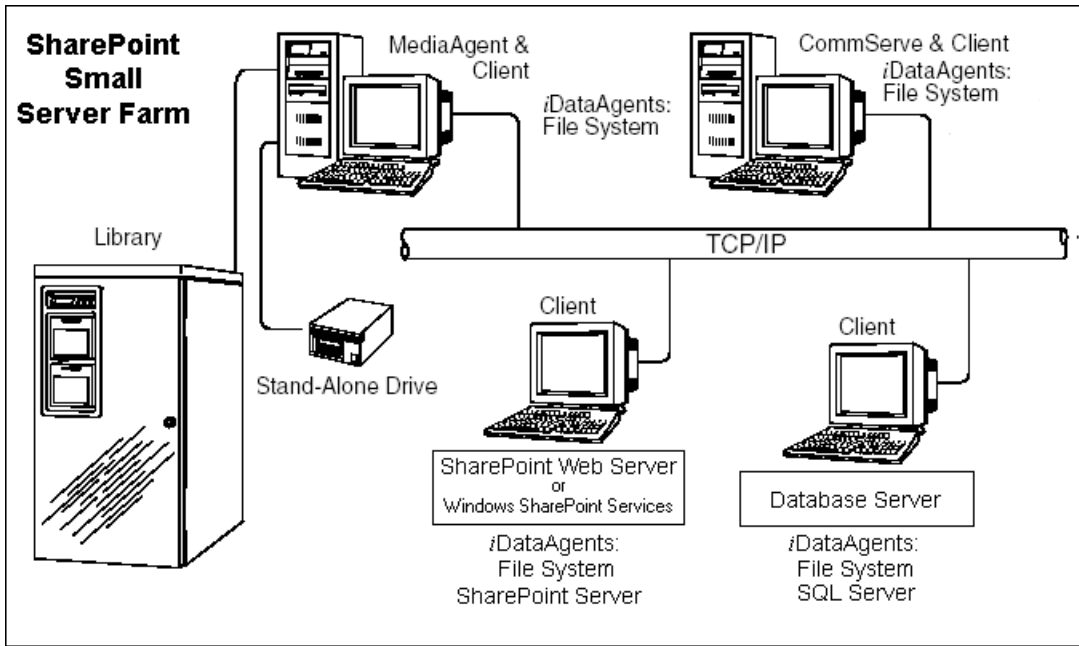
INTRODUCTION

Microsoft SharePoint Server and Windows SharePoint Services include components that are backed up by the SharePoint Server iDataAgent, as well as data which must be backed up using the File System iDataAgent. SharePoint database files can also reside on separate SQL servers; to secure this data, you must back up these files using the appropriate SQL Server iDataAgent. The SharePoint entities that can be backed up by the system are described in detail in the following sections.

The following figure shows the iDataAgents needed to fully secure a SharePoint all-in-one Server or Windows SharePoint Services single-box installation:



The following figure shows the iDataAgents needed to fully secure SharePoint Server components in a small server farm, or with the database for Windows SharePoint Services on a separate SQL Server:



SHAREPOINT SERVERS, SHAREPOINT CLIENTS, AND CLIENTS

The following definitions are offered to prevent any confusion that may arise from the use of the term *client*:

- A SharePoint Server is a computer on which the appropriate Windows Server software and Microsoft SharePoint Server, or Windows SharePoint Services software have been installed. You can secure file system data on a SharePoint Server using the Windows File System iDataAgent for the server's file system.
- SharePoint Clients are computers that access SharePoint data through the SharePoint Server or Windows SharePoint Services.
- A client is a computer whose data is backed up via an iDataAgent.

[Back to Top](#)

SUPPORTED DATA TYPES

A SharePoint Server consists of many components, listed in more detail below, and supports indexing of network file shares, Web shares, Lotus Notes databases, and other SharePoint Servers. This information is stored in a logical view of information as needed for various user types, as opposed to a folder view. This information is presented to the user via the digital dashboard web page serviced by the IIS web server. Users will have specific permissions to access the content of workspace folders.

In addition to the database on the SharePoint Server, there may be SharePoint Server entities or application data that is not backed up by the SharePoint iDataAgent. To secure this data you must back it up using the File System iDataAgent, and in the case of a server farm, the SQL Server iDataAgent.

Data Secured by the Database Backup Sets

The Database Backup Sets are used to back up and restore the database components of the system. Click on a checkmark ✓ below to view the How To procedure:

	WSS (V2)	SHAREPOINT PORTAL SERVER 2003	WSS (V3)	SHAREPOINT 2010 FOUNDATION	MOSS 2007	SHAREPOINT SERVER 2010/FAST 2010	FORMS SERVER 2007	PROJECT SERVER 2007/2010	SEARCH SERVER 2008/2010 (EXPRESS)
Site Collections (up to 15 GB for SharePoint 2003 and 2007, and up to 100 GB for any 2010 version)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Web Application Content Databases	✓	✓	✓	✓	✓	✓	✓	✓	✓
Configuration Database	Only for restore as offline Databases								
Shared Service Provider:									
SSP WebApp Content DB					✓		✓	✓*	
Shared Services Content DB					✓		✓	✓*	✓
Search Database					✓				✓

Search Index Files					✓				✓
WSS Search (Search Database and Index Files)			✓	✓	✓	✓	✓	✓	✓
Single Sign-on (Database and Encryption Key)		✓			✓	✓			
Portal Sites, including Service, Profile, and Site Databases		✓							
Portal Site Indexes (Content Sources)		✓							
Site Content Databases		✓							
Team Site Databases		✓							
Service Applications and Service Application Proxies				✓		✓		✓	

- You can use SharePoint Server 2003, WSS v2 and v3, MOSS 2007, Project Server 2007, Forms Server 2007, and Search Server 2007 site collection backup for site collections up to 15 GB.
- You can use SharePoint Server 2010, SharePoint 2010 Foundation, Project Server 2010 and Search Server 2010 site collection backup for site collections up to 85 GB.
- * Applicable for Project Server 2007 only

Data Secured by the Document Backup Sets

The Document Backup Sets are used to back up and restore sub-sites, Areas (content on SharePoint 2003 Areas and the Area itself), Libraries, and Lists.

Data	SharePoint Server 2003	SharePoint Server 2007	SharePoint Server 2010
Columns	<ul style="list-style-type: none"> • User-defined Columns: <ul style="list-style-type: none"> ○ Number ○ Single line of text ○ Multiple lines of text ○ Yes/No ○ Calculated ○ Date and Time 	<ul style="list-style-type: none"> • User-defined Columns: <ul style="list-style-type: none"> ○ Number ○ Single line of text ○ Multiple lines of text ○ Yes/No ○ Calculated ○ Date and Time 	<ul style="list-style-type: none"> • User-defined Columns: <ul style="list-style-type: none"> ○ Number ○ Single line of text ○ Multiple lines of text ○ Yes/No ○ Calculated ○ Date and Time
Alerts	Alerts associated with Documents and List Items (requires creating registry key dwBackupAlerts, which will back up the Alerts associated with Documents and List Items. For more information, see SharePoint registry keys).	Alerts associated with Documents and List Items (requires creating registry key dwBackupAlerts, which will back up the Alerts associated with Documents and List Items. For more information, see SharePoint registry keys).	Alerts associated with Documents and List Items (requires creating registry key dwBackupAlerts, which will back up the Alerts associated with Documents and List Items. For more information, see SharePoint registry keys).
Libraries	<ul style="list-style-type: none"> • Document Libraries • Form Libraries • Picture Libraries 	<ul style="list-style-type: none"> • Document Libraries • Form Libraries • Picture Libraries • Page Libraries • Report Libraries • Slide Libraries • Translation Management Libraries • Wiki Page Libraries 	<ul style="list-style-type: none"> • Document Libraries • Form Libraries • Picture Libraries • Page Libraries • Report Libraries • Slide Libraries • Translation Management Libraries • Wiki Page Libraries • Asset Libraries
Lists	<ul style="list-style-type: none"> • Announcements • Calendars • Contacts • Custom Lists (and in Datasheet Views) • Discussions • Issues • Links • Surveys • Tasks 	<ul style="list-style-type: none"> • Announcements • Calendars • Contacts • Custom Lists (and in Datasheet Views) • Discussions • Issues • Links • Surveys • Tasks • Converted Forms • Custom Workflow Process • Data Connection History • Datasources • Languages and Translators • No Code Workflows 	<ul style="list-style-type: none"> • Announcements • Calendars • Contacts • Custom Lists (and in Datasheet Views) • Discussions • Issues • Links • Surveys • Tasks • Converted Forms • Custom Workflow Process • Data Connection History • Datasources • Languages and Translators • No Code Workflows • Status Lists

Views	Library and List Views	Library and List Views	Library and List Views.
--------------	------------------------	------------------------	-------------------------

SharePoint Data Secured by the File System iDataAgent

In addition to the data stored on the SharePoint Server, there may be data stored on Web Server. Such data is not backed up by the SharePoint Server iDataAgent. To secure this data you must back it up using the File System iDataAgent on the Web Server computer.

- Alternate Access Mapping
- Root Directories of SharePoint Services - Extended Virtual Servers
- Custom Solutions Deployed
- Custom Web Part Assemblies
- Custom Templates
- IIS metabase
- IIS Root Directories (including web.config files)
- Add-in software:
 - Language Template Packs
 - Web Part page solutions (3rd-party developed aspx pages that include Web Parts)
 - Templates that work with Microsoft Office
 - Microsoft Office Web Parts and Components, which is a collection of Web Parts

SharePoint Data Secured by the SQL iDataAgent in a Server Farm

- SQL Database on a remote server
- If the Content Database is configured to support SQL Server 2008 R2 Remote Blob Storage (RBS), the table below explains which method supports backing up and restoring unstructured data in the RBS. Currently, we recommend to use Filestream Provider that comes with MS SQL 2008R2 feature pack. For details, see Microsoft SQL Server 2008 R2 Feature Pack:

Agent/Configuration	Filestream Provider/Third Party RBS Supported
SQL Server iDataAgent	Yes
SQL Server iDataAgent (Snap Backup or VSS)	Yes
SharePoint Server iDataAgent (Database Backup Sets)	Yes
SharePoint Server iDataAgent (Document Backup Sets)	Yes*
SharePoint Server iDataAgent (with Snap Mining)	No**

* Direct Database Access option is not supported.

** Please contact Support for this option.

DATA THAT IS NOT SECURED BY THE SHAREPOINT SERVER iDATAAGENT

Record this information and store it in a safe place, as part of your disaster recovery planning. For more information about Full System Restore, refer to Restore Data - SharePoint Server iDataAgent - Full System Restore.

Data that is not Secured by the Database Backup Set

The following information is not backed up by the system and the farm must be rebuilt in the event a Full System Restore is required:

SharePoint Server 2003/2007/2010 (common)	SharePoint Server 2007/2010 (common)
<ul style="list-style-type: none"> • Configuration Database 	<ul style="list-style-type: none"> • Global Search Settings • Central Administration Web Application • Central Administration Content Database • Project Web Access (PWA) Sites
<p>The following information must be recorded for use in the event a Full System Restore is required:</p> <ul style="list-style-type: none"> • E-Mail Server Settings • Anti-virus Settings • Blocked File Types • Logging Settings • HTML Viewer • Usage Analysis Processing • Shared Services 	

Data that is not Secured by the Document Backup Set

The following information is not backed up by the system, and must be recorded for use in the event a Full System Restore is required:

- For Sites, Alerts, Registry Keys
- For Meeting Workspaces, Pages list – multiple-page Meeting Workspaces, Meeting Series list, Recurring Meeting workspaces -- not restored as recurring and only List items for current meeting are backed up.
- Library items that have a size of 0Kb will not be backed up. Exceptions may be thrown with these empty library items.
- For Lists, Issues List (Issue Items are restored but the Issue History is not)
- Information Management Policy Settings for libraries and lists.
- Library document templates.
- If a backslash ('\') character is present in a List item name, it cannot be backed up. To successfully back up the List item, it is recommended to rename the item without the backslash.
- Picture Library Photos associated with a Blog site
- Portal and Area listings (**SharePoint 2003 only**)
- Recycle Bins
- Views for Galleries (List Template, Site Template, Web Part Template)¹
- Web Discussions

¹Views can be backed up with a Database Backup Set via a Site Collection.

Data that cannot be retrieved with SharePoint Offline Mining

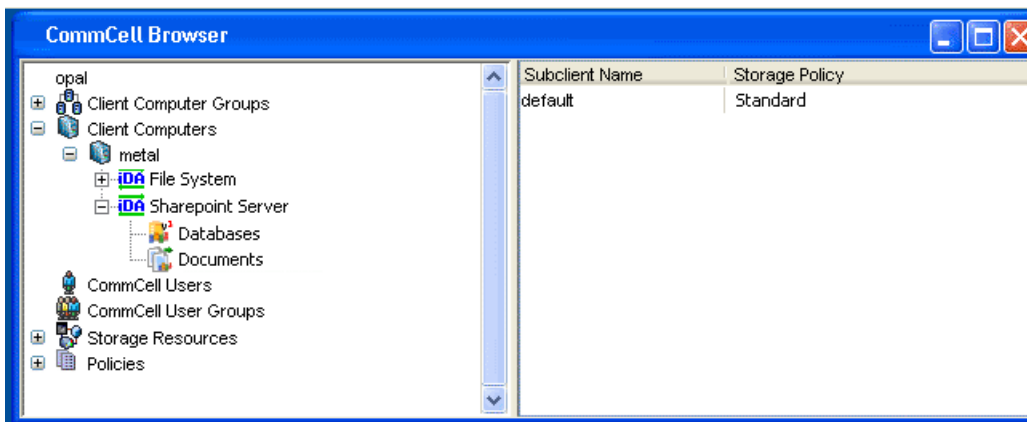
The following types of data cannot be retrieved when mining SharePoint data from an offline mining database:

- Documents from Portal Area Libraries for SharePoint 2003 databases.

[Back to Top](#)

TREE LEVELS IN THE SHAREPOINT SERVER iDATAAGENT

When the SharePoint Server iDataAgent is installed, the following levels are automatically created in the CommCell Browser:



metal: Client

default: Subclients

SharePoint Server

MS SharePoint Server iDataAgent: Agent

Databases: Backup Sets

Documents: Backup Sets

[Back to Top](#)

LICENSE REQUIREMENT

To perform a data protection operation using this Agent a specific Product License must be available in the CommServe® Server.

Review general license requirements included in License Administration. Also, View All Licenses provides step-by-step instructions on how to view the license information.

The SharePoint Server iDataAgent requires the following two licenses:

- **iDataAgent for MS SharePoint Database** is consumed during the installation of the software and each installed instance uses a license.

- **iDataAgent for MS SharePoint Document** is consumed during the installation of the software and each installed instance uses a license.

[Back to Top](#)

DISASTER RECOVERY CONSIDERATIONS

- Before you use your agent, be sure to review and understand the associated full system restore (or disaster recovery) procedure. The procedure for some agents may require that you plan specific actions or consider certain items before an emergency occurs. See Disaster Recovery for more information regarding your agent.

[Back to Top](#)

System Requirements - Microsoft SharePoint Server iDataAgent

System Requirements | **Supported Features**

The following requirements are for the SharePoint Server iDataAgent:

APPLICATION

Microsoft Windows SharePoint Services version 2.0 up to the latest Service Pack
Microsoft SharePoint Portal 2003 Server up to the latest Service Pack
Microsoft Windows SharePoint Services version 3.0 up to the latest Service Pack
Microsoft Office SharePoint Server 2007 up to the latest Service Pack
Microsoft Office Forms Server 2007 up to the latest Service Pack
Microsoft Office Project Server 2007 up to the latest Service Pack
Microsoft Search Server 2008 up to the latest Service Pack
Microsoft Search Server 2008 Express up to the latest Service Pack
Microsoft SharePoint Server 2010
Microsoft FAST Search Server 2010
Microsoft Search Server 2010
Microsoft Office Project Server 2010
Microsoft SharePoint 2010 Standard and Enterprise
Microsoft SharePoint Foundation 2010
Microsoft Search Server 2010 Express

OPERATING SYSTEM

WINDOWS SERVER 2008

Microsoft Windows Server 2008 32-bit and x64 Editions*

*Core Editions not supported

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.

HARD DRIVE

708 MB minimum of hard disk space for installing the software.

500 MB of free disk space is required for log directory.

An appropriate amount of temporary space must be allotted in the Job Results folder to accommodate staging of the SharePoint Service Application Databases, Site Collections and subsites. Calculated based on the size of the largest Service Application Database, 5 largest site collections and 5 largest subsites in the Farm.

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.

The File System iDataAgent will be automatically installed during installation of this software, if it is not already installed. For System Requirements specific to the File System iDataAgent, refer to System Requirements - Microsoft Windows File System iDataAgent.

.NET FRAMEWORK

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

SQL 2005 SDK

SQL 2005 SDK is required to be installed where SharePoint agent is installed.

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

Install the SharePoint Server iDataAgent

TABLE OF CONTENTS

Install Requirements

Before You Begin

Install Procedure

- Getting Started
- Select Components for Installation
- Configuration of Other Installation Options
- Download and Install Latest Packs
- Client Group Selection
- Global Filters Selection
- Schedule Automatic Update
- Storage Policy Selection
- SharePoint Server Information
- SharePoint Administration Account
- Verify Summary of Install Options
- Setup Complete

Post-Install Considerations

INSTALL REQUIREMENTS

The following procedure describes the steps involved in installing the Windows File System and SharePoint Server iDataAgent. The MS SharePoint Server iDataAgent can be installed on a Front-End Web Server only on Microsoft Office SharePoint Server or Windows SharePoint Services computer, or on a computer with SQL Server iDataAgent for offline mining and browsing of data from SQL, or on any Windows Server 2003/2008 without any SharePoint Server software for snap mining data protection jobs. The machine on which the MS SharePoint Server iDataAgent is installed is referred to as the *Client* computer in this install procedure.

Verify that the computer in which you wish to install the software satisfies the minimum system requirements; refer to System Requirements - Microsoft SharePoint iDataAgent and System Requirements - Microsoft Windows File System iDataAgent.

Review the following Install Requirements before installing the software:

GENERAL

- Review Install Considerations before installing the software.
- Agents should be installed only after the CommServe and at least one MediaAgent have been installed in the CommCell. Also, keep in mind that the CommServe® software and MediaAgent must be installed and running (but not necessarily on the same computer), before you can install the Agent.
- Close all applications and disable any programs that run automatically, including anti-virus, screen savers and operating system utilities. Some of the programs, including many anti-virus programs, may be running as a service. Stop and disable such services before you begin. You can re-enable them after the installation.
- Ensure there is an available license on the CommServe software for the Agent.
- Verify that you have the Software Installation Disc that is appropriate to the destination computer's operating system.
- If the SharePoint Server iDataAgent is installed on the same machine as the CommServe, Media Agent, or File Archiver for Windows, ensure that all services are running under the same SharePoint Administration Account that is specified below.

BEFORE YOU BEGIN

- Log on to the client as local Administrator or as a member of the Administrators group on that computer.

INSTALL PROCEDURE

GETTING STARTED

1. Place the Software Installation Disc for the Windows platform into the disc drive.

After a few seconds, the installation program is launched.

If the installation program does not launch automatically:

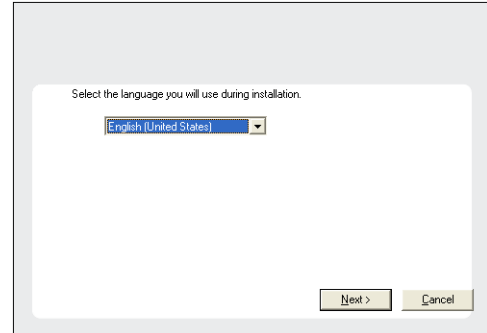
- Click the **Start** button on the Windows task bar, and then click **Run**.
- Browse to the installation disc drive, select **Setup.exe**, click **Open**, then click **OK**.

NOTES

- If you are installing on Windows Server Core editions, mount to Software Installation Disc through command line, go to the **AMD64** folder and run

Setup.exe.

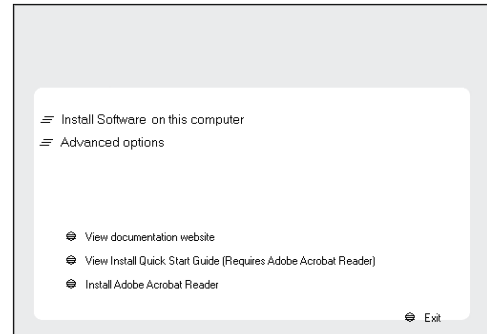
- Choose the language you want to use during installation. Click the down arrow and select the desired language from the drop-down list, and click **Next** to continue.



- 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.



- Read the license agreement, then select **I accept the terms in the license agreement**.

Click **Next** to continue.



SELECT COMPONENTS FOR INSTALLATION

- Select the component(s) to install.

NOTES

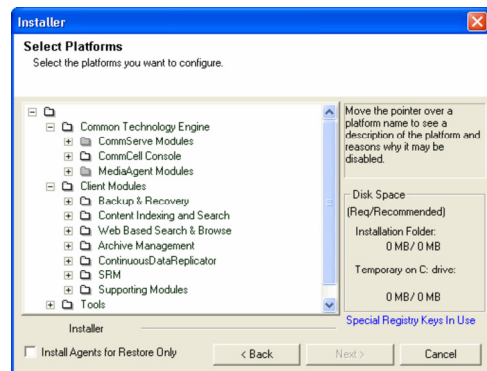
- Your screen may look different from the example shown.
- Components that either have already been installed, or which cannot be installed, will be dimmed. Hover over the component for additional details.
- If you wish to install the agent software for restore only, select **Install Agents for Restore Only** checkbox. See Installing Restore Only Agents for more information.
- The **Special Registry Keys In Use** field will be highlighted when `GalaxyInstallerFlags` registry key is enabled. Move the mouse pointer over this field to see a list of registry keys that have been created in this computer.

Click **Next** to continue.

To install the Microsoft SharePoint Server iDataAgent, expand the following `Client Modules` folder, `Backup & Recovery` folder and `SharePoint` folder. Then select the following:

- SharePoint iDataAgent

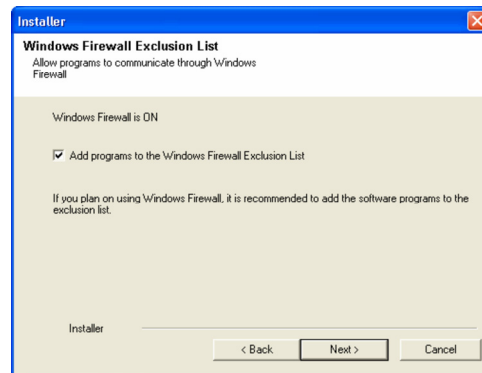
When you select the SharePoint iDataAgent for install, the appropriate Windows File System iDataAgent is automatically selected for install.



CONFIGURATION OF OTHER INSTALLATION OPTIONS

You can either select this option during install or add the programs and services after installation. For adding the programs and services after installation, see Configure Windows Firewall to Allow CommCell Communication.

Click **Next** to continue.



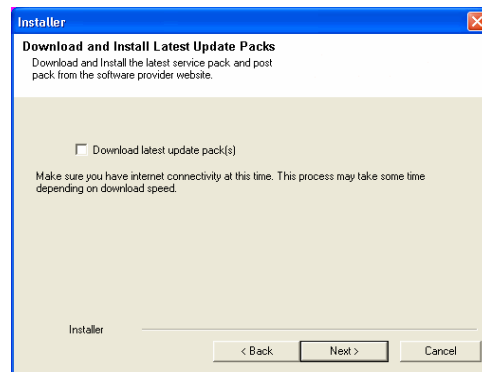
DOWNLOAD AND INSTALL LATEST PACKS

11. Select **Download latest update pack(s)** to automatically download and install the latest service packs and/or post packs if applicable at the end of this agent install.

NOTES

- Internet connectivity is required to download updates.
- Updates are downloaded to the following directory:
<software installation>/Base/Temp/DownloadedPacks.
They are launched silently and installed automatically for the first instance.

Click **Next** to continue.



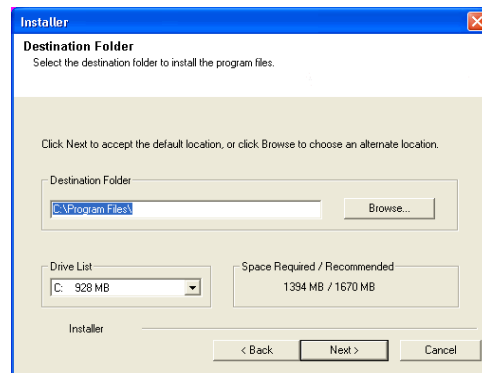
12. Specify the location where you want to install the software.

NOTES

- 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.
- If you intend to install other components on this computer, the selected installation directory will be automatically used for that software as well.
- If a component is already installed in this computer, this screen may not be displayed. The software will be automatically installed in the same location that was previously specified.

Click **Browse** to change directories.

Click **Next** to continue.



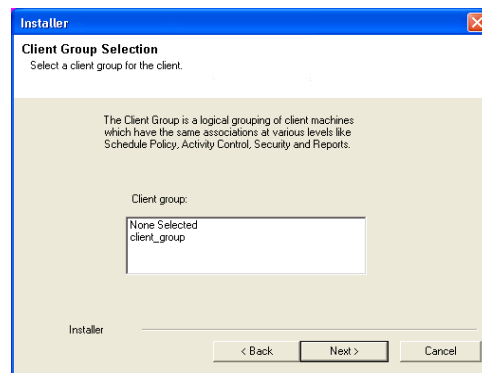
CLIENT GROUP SELECTION

13. Select a Client Group from the list.

Click **Next** to continue.

NOTES

- This screen will be displayed if Client Groups are configured in the CommCell Console. For more information, see Client Computer Groups.



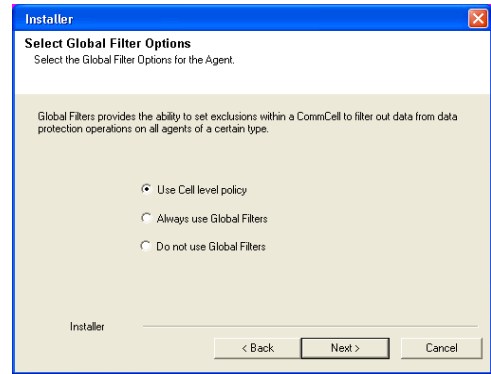
GLOBAL FILTERS SELECTION

- Select the necessary Global Filter option for the default subclient and Click **Next** to continue.

NOTES

- Select **Use Cell level Policy** to inherit the global filter policy configuration set for the CommCell, i.e., if the **Use Global Filters on All Subclients** option is selected in the **Global Filters** dialog box (from the CommCell Console's Control Panel), then this policy will be applied to the default subclient as well. If is not selected, then the global filters will not be applied to the default subclient.
- Select **Always use Global filters** to apply the global filters policy to the default subclient regardless of the policy set for the CommCell.
- Select **Do not use Global filters** to disregard applying the global filters to the default subclient regardless of the policy set for the CommCell.

Click **Next** to continue.



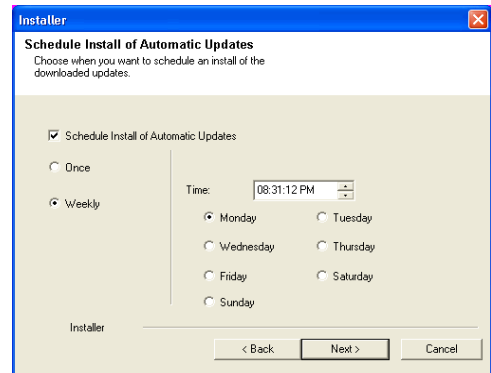
SCHEDULE AUTOMATIC UPDATE

- If necessary, select this option to schedule an automatic installation of software updates.

NOTES

- Schedule Install of Automatic Updates allows automatic installation of the necessary software updates on the computer on a single or weekly basis. If you do not select this option, you can schedule these updates later from the CommCell Console.
- To avoid conflict, do not schedule the automatic installation of software updates to occur at the same time as the automatic FTP downloading of software updates.
- If a component has already been installed, this screen will not be displayed; instead, the installer will use the same option as previously specified.

Click **Next** to continue.



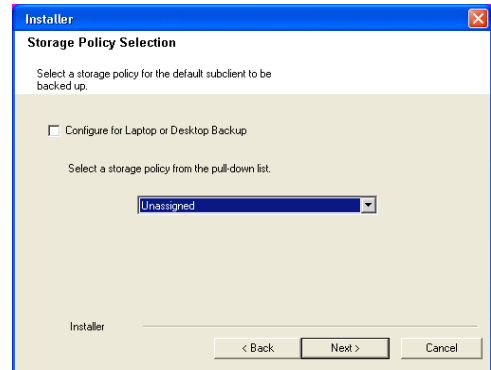
STORAGE POLICY SELECTION

- Select the storage policy through which you want to back up/archive the agent.

NOTES

- A storage policy directs backup data to a media library.
- If desired, you can change your storage policy selection at any time after you have installed the client software.
- This screen may appear more than once, if you have selected multiple agents for installation. You will be prompted to configure the storage policy association for each of the selected agents.

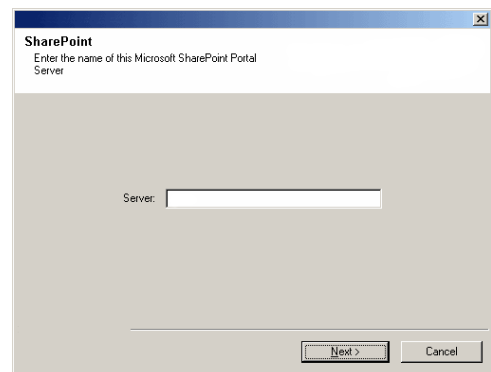
Click **Next** to continue.



SHAREPOINT SERVER INFORMATION

- You are prompted for the Microsoft SharePoint Server name. The computer name is displayed by default; if this is not correct, enter the correct name.

Click **Next** to continue.



SHAREPOINT ADMINISTRATION ACCOUNT

18. Enter the User Name and Password for the SharePoint Administration Account.

Click **Next** to continue.

NOTES

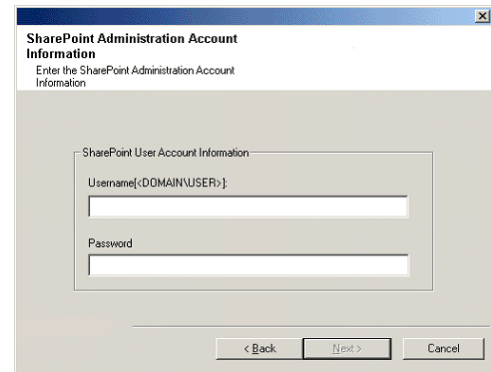
- The Base Services of the client will run under the user account that is specified. Use an account that meets this criteria:
 - member of the local Administrator Group
 - member of the SharePoint Administrator Group
 - System Administrator role on the SQL Server Instance

In addition, this account must have "**Log on as Service**" permissions to ensure the Communication (CVD) Services will start. For more information on Base and Communication (CVD) Services, see Services.

Refer to the Knowledge Base article *Galaxy Service Account User Information for Windows 2003 and Window Server 2003 clients* available from the Maintenance Advantage web site.

- When installing the SharePoint Server iDataAgent on a job server, the user account entered through this screen must have administrative privileges to the Single Sign-On Service.

See the SharePoint Agents section in **User Accounts and Passwords** for more information.



VERIFY SUMMARY OF INSTALL OPTIONS

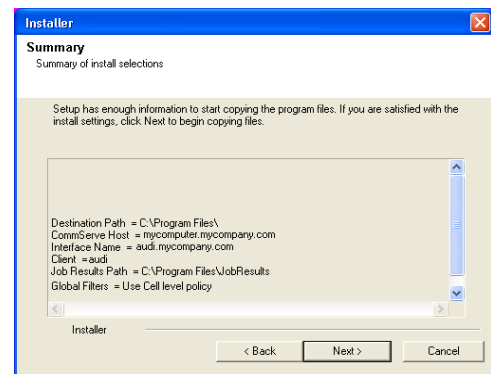
19. Verify the summary of selected options.

NOTES

- The **Summary** on your screen should reflect the components you selected for install, and may look different from the example shown.

Click **Next** to continue or **Back** to change any of the options.

The install program now starts copying the software to the computer. This step may take several minutes to complete.



SETUP COMPLETE

20. Click **Next** to continue.

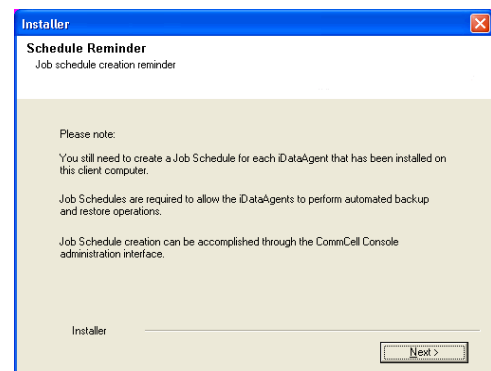
NOTES

- Schedules help ensure that the data protection operations for the Agent are automatically performed on a regular basis without user intervention. For more information, see Scheduling.

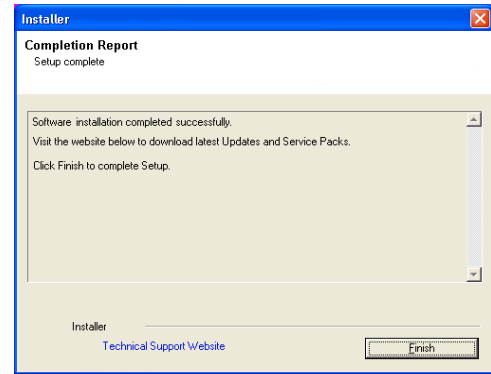
21. Setup displays the successfully installed components.

NOTES

- The **Setup Complete** message displayed on your screen will reflect the components you installed, and may look different from the example shown.
- If you install an Agent with the CommCell Console open, you need to refresh the CommCell Console (F5) to see the new Agents.
- If **Reboot Now** button is displayed make sure to reboot the computer before performing any other operations from the computer.



Click **Finish** to close the install program.
The installation is now complete.



POST-INSTALL CONSIDERATIONS

GENERAL

- Review Install Considerations after installing the software.
- Install post-release updates or Service Packs that may have been released after the release of the software. When you are installing a Service Pack, ensure that it is the same version as the one installed in the CommServe Server. Alternatively, you can enable Automatic Updates for quick and easy installation of updates in the CommCell component.

Backup - Microsoft SharePoint Server

Topics | How To | Related Topics

Overview

Supported Backup Types

Backup Considerations for This Agent

Advanced Backup Options

OVERVIEW

Plan your backup jobs for this agent by reviewing the following information:

- For an overview of backup jobs, see Backup Data.
 - For a list of supported data types for this agent, see Supported Data Types.
 - For information on subclients, see Subclients.
 - For information on configuring subclients for this agent, see Subclients - SharePoint Server.
 - For information on excluding data via subclients, see Excluding Data from Data Protection Operations.
-

SUPPORTED BACKUP TYPES

The SharePoint Database backup sets support the following backup types:

- Full Backups

The SharePoint Document backup sets support the following backup types:

- Full Backups
 - Incremental Backups
 - Differential Backups
 - Synthetic Full Backups
-

BACKUP CONSIDERATIONS FOR THIS AGENT

Before performing any backup procedures for this agent, review the following information:

PERMISSIONS

- The Base Services of the client will run under the user account that is specified. Use an account that meets this criteria:
 - member of the local Administrator Group
 - member of the SharePoint Administrator Group
 - System Administrator role on the SQL Server Instance

In addition, this account must have "**Log on as Service**" permissions to ensure the Communication (CVD) Services will start. For more information on Base and Communication (CVD) Services, see Services.

Refer to the Knowledge Base article *Galaxy Service Account User Information for Windows 2003 and Window Server 2003 clients* available from the Maintenance Advantage web site.

- For successful backup and restore of site collections or personal sites, the SharePoint Administrator Account should also be added as user with Full control for all sites. It can be done using Policy for Web Application (**Application Management - Application Security - Policy for Web Application**).
 - For backups with the Direct Database Access option, in addition to having Policy for Web Application permissions, the SharePoint administrator account must be the site collection administrator in order to back up SharePoint list and library views.
-

MS SHAREPOINT SERVER DATABASE

- For Microsoft Sharepoint Foundation 2010 and SharePoint Server 2010 stand-alone environments, the SQL Server service credentials for SharePoint instance should be changed to Local System Account from Network Service for the Database backupset to properly backup site collections as well as database files.
- When SharePoint is configured in a Server Farm configuration, SQL databases must be backed up using the SQL iDataAgent. See Microsoft SQL Server Run

backups using the SharePoint Database backup set at approximately the same time as the SQL iDataAgent backups of the respective databases.

- Farm configuration SQL Databases with Unicode names should be backed up using other SQL backup tools since only standard alphanumeric characters are supported for the Microsoft SQL Server iDataAgent. The SQL Server iDataAgent does not support databases with Extended ASCII or UNICODE characters in their names.
- To prevent SharePoint Database backup sets backup errors (e.g., ".The log file for database 'DB_NAME' is full. Back up the transaction log for the database to free up some log space...") caused by full SQL Database Transaction Logs, it is recommended to back up SQL Database and Transaction logs using the Microsoft SQL Server iDataAgent or other SQL backup tools.
- When backing up a Site Collection, the data is moved from the server to a local file under the Job Results directory. SharePoint Database operations stage data to the Job Results directory that can be set from the CommCell Console. See Change the Job Results Path of a Client for step-by-step instructions.
- When the bUseSPAPI registry key is created, SharePoint API's are used to back up and restore site collections.
- When the dwUseSqlSnapshot registry key is created, SharePoint 2010 site collections can be backed up using SQL database snapshots if the database server is running an Enterprise Edition of Microsoft SQL Server.
- To backup SharePoint Database data, the nMixedModeOverrideVersion registry key value can be set to 2003 or 2007 respectively. By default, if the key does not exist, SharePoint 2007 data will be backed up. When the key is set to 2003, SharePoint 2003 data will be backed up. If set to 2007, SharePoint 2007 data will be backed up.
- For SharePoint 2003 and 2007 Site Collection that is 15 gigabytes (GB) or smaller can successfully be backed up and restored using a DataBase Backup Set Site Collection level backup and restore. For a SharePoint 2003 and 2007 Site Collection that is larger than 15 gigabytes (GB), you need to backup and restore using a Content Database level backup and restore. For more information, see Restore Data - SharePoint Server - How To.
- In an environment where two different versions of SharePoint Server (e.g., 2003 and 2007) co-exist on the same client with the SharePoint Server iDataAgent, an additional Database type backup set should be created to backup SharePoint Database components for other version.
- To successfully backup a SharePoint Database in a Windows SharePoint Services (WSS) environment, where the instance name of the Windows Internal Database resembles something like `MachineName\Microsoft##SSEE`, you need to:
 1. Change the flag **Hide Instance** to **No** in **SQL Server Configuration Manager→Protocols for MachineName\Microsoft##SSEE**.
 2. Ensure that the **SQL Server Browser** service is running in **SQL Server Configuration Manager→SQLServer 2005 Services**.
 3. Ensure that **Named Pipes** is enabled in **SQL Server Configuration Manager→Protocols for MachineName\Microsoft##SSEE**.
- The four databases namely Archive, Draft, Published and Reporting cannot be distributed over multiple subclient. They need to be backed up and restored together as they belong to the same PWA (Project Web Access) Site.
- For SharePoint database backups in an all-in-one configuration, install the Calypso software with either 32 or 64-bit Microsoft SQL Server 2005 Management Objects Collection or SQL Server 2008 Shared Management Objects.
If you have installed the 32-bit SQL Server 2008 Shared Management Objects on a 64-bit client, then you may see this error: `Could not load file or assembly "Microsoft.SqlServer.BatchParser, Version=10.0.0.0"`.
- For SharePoint Server 2010, the lock state parameter initially has the settings of `none` or `no additions`. During backup, the site collection lock state is temporarily set to `read-only` mode during the backup. By specifying the `dwNoSiteLock` registry key, the lock settings can be set to `Read` and `Write` mode. The backup would record the original site collection lock state so that it can be restored to its original state.

MS SHAREPOINT SERVER DOCUMENT

- For SharePoint Server iDataAgent installed on a SharePoint Server 2003 client, incremental and differential backups of version-enabled libraries will back up the previous version and any new versions since the last backup.
- A full backup is recommended if upgrading SharePoint 2003 to 2007 on a SharePoint Server iDataAgent client. This ensures that new metadata will be included in the backup.
- In a SharePoint Farm environment, to ensure a successful backup when the **Use direct database access** option is selected, a SQL Server Native client should be installed. For more information, see Direct Database Access. This feature is not supported for host-named site collections, for site collections which Content database is configured with RBS, site collections on WSS version 2.0 or SharePoint Server 2003.
 - For direct database backups of Document backup sets, you can use the **nItemDataChunkSizeInMBForBackup** registry key to specify the amount of data in each chunk of backup content. The more data that is allowed in a single chunk, the fewer number of queries that are executed on the backup contents. If the amount of data exceeds the total amount specified in the registry key, more chunks will be created, up to the specified number of chunks. For details, see the entry in Registry Keys.
 - For direct database backups of the Document backup sets, you can use the **nItemBatchSize** registry key to specify the number of items that are included in a batch. The greater number of items in a batch, the fewer number of queries executed for the remaining items. The minimum and maximum item thresholds are determined by the available resources on the machine. For details, see the entry in Registry Keys.
- Due to Loopback check functionality in Microsoft Windows, backups of Major/Minor versioned documents may be unsuccessful. This can be corrected by setting the **DisableLoopbackCheck** registry key to 1 under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\DisableLoopbackCheck` and reboot the SharePoint Web Server. Refer to Microsoft Article ID: 887993 at <http://support.microsoft.com/kb/887993> for details.

- Filters can be used in conjunction with the "Items That Failed" list on the data protection Job History Report to eliminate backup or archive failures by excluding items which consistently fail 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.

- For Document backup sets, the `nLargeFileSizeThresholdValInMBForBackup` registry key can be used to specify backing up files over a certain size. For example, if 40 is specified, all files larger than 40MB it will be backed up. This is logged in `SPDocBackup.log`, which will state the file size threshold value. Default is 50 Mb.
- Set the `dwDisableAutoDiscovery` registry key to **1** if you want to disable auto-discovery of sites for user-created subclients.
- While `.aspx` files for basic Web Part and Dashboard Pages from a Library can be backed up and restored, restoring the file will not restore the Web Part to the page. Modifications made to the page using the Content Editor Web Part will not be restored and cannot be made to the file after it has been restored.
- Library items that have a size of 0Kb will not be backed up. Exceptions may be thrown with these empty library items.
- If a backslash ('\') character is present in a List item name, it cannot be backed up. To successfully back up the List item, it is recommended to rename the item without the backslash.

[Back to Top](#)

Backup - Microsoft SharePoint Server - How To

[Topics](#) | [How To](#) | [Related Topics](#)

[Start a Backup](#)

[Start a Synthetic Full Backup](#)

[Schedule Backups](#)

[Start a Backup in the Suspended State](#)

[Start a Backup on New Media](#)

[Start a Backup that Marks Media Full on Completion](#)

[Start a Backup with a Set Job Priority](#)

[Start a Backup with Vault Tracking enabled](#)

[Backup SharePoint Farm with SQL Server RBS Enabled](#)

START A BACKUP

Before You Begin

- Depending on your agent, you can perform the following types of backup operations: **Full**, **Incremental**, **Differential** or **Synthetic Full**.
 - Read Full Backups before performing a Full Backup.
 - Read Incremental Backups before performing an Incremental Backup.
 - Read Differential Backups before performing a Differential Backup.
 - Read Synthetic Full Backups before performing a Synthetic Full Backup.

Required Capability: See Capabilities and Permitted Actions

▶ To start an immediate backup job:

1. From the CommCell Browser, expand **Client Computers** by double-clicking **Client Computers** | **iDA File System** | **defaultBackupSet**. The default and other subclients (if available) are displayed on the right-hand windowpane.
2. To back up the default subclient, right-click the subclient, and click **Backup**.
3. From the Backup Options dialog box, select **Run Immediately**.
4. Select **Full**, **Incremental**, **Differential** or **Synthetic Full** backup.

In certain circumstances a non-full backup may automatically be converted to a full backup. For a listing of these circumstances, see [When a Non-Full Backup is Automatically Converted to a Full Backup](#).

5. Click **OK**. You can track the progress of the backup job from the **Job Controller** window. If you are using a stand-alone drive, you are prompted to load a

specific cartridge into the drive. If you are using a library, you will not receive this prompt. The system loads the tapes automatically. Your cartridges should be appropriately labeled. This will enable you to locate the correct cartridge for a restore job, if necessary.

- When the backup has completed, the Job Controller displays `Completed`.

After running a backup, you may want to verify the backup data. You can do this by viewing the Backup History. For more information, see Backup Job History.

- You can also run backups of the following:
 - For a user-defined backup set or instance, right-click the backup set you want to back up, click **All Tasks**, and click **Backup All Subclients**.
 - For the Lotus Notes Document `iDataAgent`, to back up a partition, right-click the partition you want to back up, click **All Tasks**, and click **Backup Default Backup Set**.
For the Lotus Notes Database `iDataAgent`, to back up a partition, right-click the partition you want to back up, click **All Tasks**, and click **Backup All Subclients**.
 - For Agents that do not have backup set or instance levels, to back up all subclients, right-click the agent icon, click **All Tasks**, and click **Backup All Subclients**.
 - If you chose a level higher than subclient (i.e., backup set, etc.), you are prompted to confirm that you want to back up all the subclients below that level/node. Click **Yes**.
 - Starting a data protection operation on a backup set, instance or agent level causes the system to start individual data protection operations for each subclient contained therein. If the subclients are associated with the same storage policy, then their operations will run sequentially unless that storage policy is configured to accommodate multiple data streams.

START A SYNTHETIC FULL BACKUP

Before You Begin

- Read Synthetic Full Backups before performing a Synthetic Full Backup.
- For SharePoint Document, for a versioned document that has multiple versions, all of the backed up versions can be viewed in the **View All Versions** window and restored, until a Synthetic Full backup is run. After running the Synthetic Full backup you can only view and restore the latest backed up version for the document.

Required Capability: See Capabilities and Permitted Actions

▶ To start an immediate backup job:

- From the CommCell Browser, expand **Client Computers** by double-clicking **Client Computers | iDA File System | defaultBackupSet**. The default and other subclients (if available) are displayed on the right-hand windowpane.
- To back up the default subclient, right-click the subclient, and click **Backup**.
- From the Backup Options dialog box, select **Run Immediately**.
- Select **Synthetic Full** backup.

Running an incremental backup immediately before the synthetic full ensures that any new or recently changed data is included in the synthetic full. Running an incremental backup immediately 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. Remember, a synthetic full consolidates data; it does not actually back up data from the client computer.

- Click **OK**. You can track the progress of the backup job from the **Job Controller** window. If you are using a stand-alone drive, you are prompted to load a specific cartridge into the drive. If you are using a library, you will not receive this prompt. The system loads the tapes automatically. Your cartridges should be appropriately labeled. This will enable you to locate the correct cartridge for a restore job, if necessary.
- When the backup has completed, the **Job Controller** displays `Completed`.

After running a backup, you may want to verify the backup data. You can do this by viewing the Backup History. For more information, see Backup Job History.

You can also run synthetic full backups of the following:

- For a user-defined backup set or instance, right-click the backup set you want to back up, click **All Tasks**, and click **Backup All Subclients**.
- For the Lotus Notes Document `iDataAgent`, to back up a partition, right-click the partition you want to back up, click **All Tasks**, and click **Backup Default Backup Set**.
For the Lotus Notes Database `iDataAgent`, to back up a partition, right-click the partition you want to back up, click **All Tasks**, and click **Backup All Subclients**.
- For Agents that do not have backup set or instance levels, to back up all subclients, right-click the agent icon, click **All Tasks**, and click **Backup All Subclients**.
 - If you chose a level higher than subclient (i.e., backup set, etc.), you are prompted to confirm that you want to back up all the subclients below that level/node. Click **Yes**.
 - Starting a data protection operation on a backup set, instance or agent level causes the system to start individual data protection operations for each subclient contained therein. If the subclients are associated with the same storage policy, then their operations will run sequentially unless that storage policy is configured to

accommodate multiple data streams.

SCHEDULE BACKUPS

You can schedule backups to occur with the following procedure. You will be prompted to create a schedule for the data protection operation after selecting your data protection options.

Before You Begin

- **All Agents**

- Be sure all of the subclients are backed up, or scheduled to be backed up as needed, in order to secure all of the data for the agent. Note this does not apply to archive operations.

Required Capability: See Capabilities and Permitted Actions

▶ To schedule a backup operation:

1. From the CommCell Browser, select one of the following:
 - To back up a subclient, right-click the subclient and click **Backup**.
 - To back up a backup set or instance, right-click the backup set or instance, click **All Tasks**, and click **Backup All Subclients**.
 - To back up the default backup set, right-click the agent or instance node, click **All Tasks**, and click **Backup Default Backup Set**.
 - For the Lotus Notes Document iDataAgent, to back up a partition, right-click the partition you want to back up, click **All Tasks**, and click **Backup Default Backup Set**.
For the Lotus Notes Database iDataAgent, to back up a partition, right-click the partition you want to back up, click **All Tasks**, and click **Backup All Subclients**.
 - For Agents that do not have backup set or instance levels, to back up all subclients, right-click the agent icon, click **All Tasks**, and click **Backup All Subclients**.
2. If you chose a level higher than subclient (i.e., backup set, etc.), you are prompted to confirm that you want to back up all the subclients below that level/node. Click **Yes**.
3. From the Backup Options dialog box, select the type of backup that you want to initiate. In certain circumstances a non-full backup may automatically be converted to a full backup. For a listing of these circumstances, see *When a Non-Full Backup is Automatically Converted to a Full Backup*.
4. Click **Schedule**. Click **OK** to continue.
5. From the Schedule Details (Schedule Details) dialog box, create a schedule for this operation. For step-by-step instructions, see *Create a Job Schedule*. Click **OK** to continue.
6. Your backup operation will execute according to the specified schedule.

Starting a data protection operation on a backup set, instance or agent level causes the system to start individual data protection operations for each subclient contained therein. If the subclients are associated with the same storage policy, then their operations will run sequentially unless that storage policy is configured to accommodate multiple data streams.

START A BACKUP IN THE SUSPENDED STATE

Use the following procedure to start a backup in the suspended state.

Before You Begin

- Be sure all of the subclients are backed up, or scheduled to be backed up as needed, in order to secure all of the data for the agent. Note this does not apply to archive operations.

Required Capability: See Capabilities and Permitted Actions

▶ To start an immediate backup job with advanced backup options:

1. From the CommCell Browser, select one of the following:
 - To backup a subclient, right-click the subclient to want to backup and click **Backup**.
 - To backup a user-defined backup set or instance, right-click the backup set you want to backup, click **All Tasks**, and click **Backup All Subclients**.
 - To backup the default backup set, right-click the agent or instance node, click **All Tasks**, and click **Backup Default Backup Set**.
 - For Lotus Notes iDataAgent, to backup a partition, right-click the partition you want to backup, click **All Tasks**, and click **Backup Default Backup Set**.
 - For Agents that do not have backup set or instance levels, to backup all subclients, right-click the agent icon, click **All Tasks**, and click **Backup All Subclients**.
2. If you chose a level higher than subclient (i.e., backup set, etc.), you are prompted to confirm that you want to back up all the subclients below that

level/node. Click **Yes**.

3. From the Backup Options dialog box, select **Run Immediately**.
4. Select the type of backup that you want to initiate.
In certain circumstances a non-full backup may automatically be converted to a full backup. For a listing of these circumstances, see *When a Non-Full Backup is Automatically Converted to a Full Backup*.
5. Click the **Advanced** button to open the **Advanced Backup Options** dialog box.
6. Click on the Advanced Backup Options (Startup) tab, and select **Startup in suspended state** and click **OK**.
7. From the **Backup Options** dialog box, click **OK**. You can track the progress of the backup job from the Job Controller window.
8. If you are using a stand-alone drive, you are prompted to load a specific cartridge into the drive. If you are using a library, you will not receive this prompt. The system loads the tapes automatically.

Your cartridges should be appropriately labeled. This will enable you to locate the correct cartridge for a restore job, if necessary.

9. When the backup has completed, Job Controller displays *Completed*.

Starting a data protection operation on a backup set, instance or agent level causes the system to start individual data protection operations for each subclient contained therein. If the subclients are associated with the same storage policy, then their operations will run sequentially unless that storage policy is configured to accommodate multiple data streams.

START A BACKUP ON NEW MEDIA

Use the following procedure to start a backup on new media.

Before You Begin

- Be sure all of the subclients are backed up, or scheduled to be backed up as needed, in order to secure all of the data for the agent. Note this does not apply to archive operations.

Required Capability: See Capabilities and Permitted Actions

▶ To start an immediate backup job with advanced backup options:

1. From the CommCell Browser, select one of the following:
 - To backup a subclient, right-click the subclient to want to backup and click **Backup**.
 - To backup a user-defined backup set or instance, right-click the backup set you want to backup, click **All Tasks**, and click **Backup All Subclients**.
 - To backup the default backup set, right-click the agent or instance node, click **All Tasks**, and click **Backup Default Backup Set**.
 - For Lotus Notes iDataAgent, to backup a partition, right-click the partition you want to backup, click **All Tasks**, and click **Backup Default Backup Set**.
 - For Agents that do not have backup set or instance levels, to backup all subclients, right-click the agent icon, click **All Tasks**, and click **Backup All Subclients**.
2. If you chose a level higher than subclient (i.e., backup set, etc.), you are prompted to confirm that you want to back up all the subclients below that level/node. Click **Yes**.
3. From the Backup Options dialog box, select **Run Immediately**.
4. Select the type of backup that you want to initiate.
In certain circumstances a non-full backup may automatically be converted to a full backup. For a listing of these circumstances, see *When a Non-Full Backup is Automatically Converted to a Full Backup*.
5. Click the **Advanced** button to open the **Advanced Backup Options** dialog box.
6. Click on the Advanced Backup Options (Media) tab, and select **Start new media** and click **OK**.
If you would like jobs with other Job IDs to use this new media, also select the **Allow other schedule to use media set** option.
7. From the **Backup Options** dialog box, click **OK**. You can track the progress of the backup job from the Job Controller window.
8. If you are using a stand-alone drive, you are prompted to load a specific cartridge into the drive. If you are using a library, you will not receive this prompt. The system loads the tapes automatically.

Your cartridges should be appropriately labeled. This will enable you to locate the correct cartridge for a restore job, if necessary.

9. When the backup has completed, Job Controller displays *Completed*.

Starting a data protection operation on a backup set, instance or agent level causes the system to start individual

data protection operations for each subclient contained therein. If the subclients are associated with the same storage policy, then their operations will run sequentially unless that storage policy is configured to accommodate multiple data streams.

START A BACKUP THAT MARKS MEDIA FULL ON COMPLETION

Use the following procedure to start a backup that marks media full on completion.

Before You Begin

- Be sure all of the subclients are backed up, or scheduled to be backed up as needed, in order to secure all of the data for the agent. Note this does not apply to archive operations.

Required Capability: See Capabilities and Permitted Actions

▶ To start an immediate backup job with advanced backup options:

1. From the CommCell Browser, select one of the following:
 - To backup a subclient, right-click the subclient to want to backup and click **Backup**.
 - To backup a user-defined backup set or instance, right-click the backup set you want to backup, click **All Tasks**, and click **Backup All Subclients**.
 - To backup the default backup set, right-click the agent or instance node, click **All Tasks**, and click **Backup Default Backup Set**.
 - For Lotus Notes iDataAgent, to backup a partition, right-click the partition you want to backup, click **All Tasks**, and click **Backup Default Backup Set**.
 - For Agents that do not have backup set or instance levels, to backup all subclients, right-click the agent icon, click **All Tasks**, and click **Backup All Subclients**.
2. If you chose a level higher than subclient (i.e., backup set, etc.), you are prompted to confirm that you want to back up all the subclients below that level/node. Click **Yes**.
3. From the Backup Options dialog box, select **Run Immediately**.
4. Select the type of backup that you want to initiate.
In certain circumstances a non-full backup may automatically be converted to a full backup. For a listing of these circumstances, see When a Non-Full Backup is Automatically Converted to a Full Backup.
5. Click the **Advanced** button to open the **Advanced Backup Options** dialog box.
6. Click on the Advanced Backup Options (Media) tab, and select **Mark media full after successful operation** and click **OK**.
7. From the **Backup Options** dialog box, click **OK**. You can track the progress of the backup job from the Job Controller window.
8. If you are using a stand-alone drive, you are prompted to load a specific cartridge into the drive. If you are using a library, you will not receive this prompt. The system loads the tapes automatically.

Your cartridges should be appropriately labeled. This will enable you to locate the correct cartridge for a restore job, if necessary.

9. When the backup has completed, Job Controller displays *Completed*.

Starting a data protection operation on a backup set, instance or agent level causes the system to start individual data protection operations for each subclient contained therein. If the subclients are associated with the same storage policy, then their operations will run sequentially unless that storage policy is configured to accommodate multiple data streams.

START A BACKUP WITH A SET JOB PRIORITY

This option allows you to manually set a job priority. This is useful if you have jobs that are very important and must complete, and/or jobs that can be moved to a lower priority. For more information, see Job Priorities and Priority Precedence.

Before You Begin

- Be sure all of the subclients are backed up, or scheduled to be backed up as needed, in order to secure all of the data for the agent. Note this does not apply to archive operations.

Required Capability: See Capabilities and Permitted Actions

▶ To start an immediate backup job with advanced backup options:

1. From the CommCell Browser, select one of the following:
 - To backup a subclient, right-click the subclient to want to backup and click **Backup**.
 - To backup a user-defined backup set or instance, right-click the backup set you want to backup, click **All Tasks**, and click **Backup All Subclients**.

- To backup the default backup set, right-click the agent or instance node, click **All Tasks**, and click **Backup Default Backup Set**.
 - For Lotus Notes iDataAgent, to backup a partition, right-click the partition you want to backup, click **All Tasks**, and click **Backup Default Backup Set**.
 - For Agents that do not have backup set or instance levels, to backup all subclients, right-click the agent icon, click **All Tasks**, and click **Backup All Subclients**.
2. If you chose a level higher than subclient (i.e., backup set, etc.), you are prompted to confirm that you want to back up all the subclients below that level/node. Click **Yes**.
 3. From the Backup Options dialog box, select **Run Immediately**.
 4. Select the type of backup that you want to initiate.
In certain circumstances a non-full backup may automatically be converted to a full backup. For a listing of these circumstances, see *When a Non-Full Backup is Automatically Converted to a Full Backup*.
 5. Click the **Advanced** button to open the **Advanced Backup Options** dialog box.
 6. Click on the Advanced Backup Options (Startup) tab, and select **Change Priority** and then enter a value. Click **OK** to continue.
 7. From the **Backup Options** dialog box, click **OK**. You can track the progress of the backup job from the Job Controller window.
 8. If you are using a stand-alone drive, you are prompted to load a specific cartridge into the drive. If you are using a library, you will not receive this prompt. The system loads the tapes automatically.

Your cartridges should be appropriately labeled. This will enable you to locate the correct cartridge for a restore job, if necessary.

9. When the backup has completed, Job Controller displays *Completed*.

Starting a data protection operation on a backup set, instance or agent level causes the system to start individual data protection operations for each subclient contained therein. If the subclients are associated with the same storage policy, then their operations will run sequentially unless that storage policy is configured to accommodate multiple data streams.

START A BACKUP WITH VAULT TRACKING ENABLED

Use the following procedure to start a backup with Vault Tracking enabled.

For additional information, see the following:

- VaultTracker
- VaultTracker Enterprise

Before You Begin

- Be sure all of the subclients are backed up, or scheduled to be backed up as needed, in order to secure all of the data for the agent.

Required Capability: See *Capabilities and Permitted Actions*

▶ To start an immediate backup job with advanced backup options:

1. select one of the following:
 - To backup a subclient, right-click the subclient to want to backup and click **Backup**.
 - To backup a user-defined backup set or instance, right-click the backup set you want to backup, click **All Tasks**, and click **Backup All Subclients**.
 - To backup the default backup set, right-click the agent or instance node, click **All Tasks**, and click **Backup Default Backup Set**.
 - For Lotus Notes iDataAgent, to backup a partition, right-click the partition you want to backup, click **All Tasks**, and click **Backup Default Backup Set**.
 - For Agents that do not have backup set or instance levels, to backup all subclients, right-click the agent icon, click **All Tasks**, and click **Backup All Subclients**.
2. If you chose a level higher than subclient (i.e., backup set, etc.), you are prompted to confirm that you want to back up all the subclients below that level/node. Click **Yes**.
3. From the Backup Options dialog box, select **Run Immediately**.
4. Select the type of backup that you want to initiate.
In certain circumstances a non-full backup may automatically be converted to a full backup. For a listing of these circumstances, see *When a Non-Full Backup is Automatically Converted to a Full Backup*.
5. Click the **Advanced** button to open the **Advanced Backup Options** dialog box.
6. Click on the **Vault Tracking** tab, and select the vault tracking options you want to use and click **OK**.
7. From the **Backup Options** dialog box, click **OK**. You can track the progress of the backup job from the Job Controller window.

8. If you are using a stand-alone drive, you are prompted to load a specific cartridge into the drive. If you are using a library, you will not receive this prompt. The system loads the tapes automatically.

Your cartridges should be appropriately labeled. This will enable you to locate the correct cartridge for a restore job, if necessary.

9. When the backup has completed, Job Controller displays *Completed*.
-

BACKUP SHAREPOINT FARM WITH SQL SERVER RBS ENABLED

If the Content Database is configured to support SQL Server 2008 R2 Remote Blob Storage (RBS), follow the steps given below to back up the unstructured data in the RBS. This is applicable when using RBS with Filestream Provider. For details, see FILESTREAM (SQL Server).

1. Configure the SQL subclient to backup the Content database that has the RBS data enabled.
2. From the CommCell Browser, expand **Client Computers** by double-clicking **Client Computers | Sharepoint Server | Database**. The default and other subclients (if available) are displayed on the right-hand windowpane.
3. Right-click the **<subclient>**, and click **Properties**.
4. Configure the SharePoint subclient to backup the farm and to automatically backup the SQL subclient as follows:
 - o Click the **Pre/Post Process** tab and in the **PreBackup process** field mention the following command:
`F:\<Software_Name>\Base\operation backup -cs <CS Name> -c <Client Name> -a Q_MSSQL -i <Instance name> -s <SQL Subclient Name> -t Q_FULL`
 - o Click **Ok**.
5. To back up a **<subclient>**, right-click the subclient, and click **Backup**.
6. From the Backup Options dialog box, select **Run Immediately**.
7. When the backup has completed, the Job Controller displays *Completed*.

After running a backup, you may want to verify the backup data. You can do this by viewing the Backup History. For more information, see Backup Job History.

To restore this data, please refer to Restore SharePoint Data Secured by the SQL iDataAgent in a Server Farm.

[Back To Top](#)

[Back To Top](#)

Restore Data - SharePoint Server

Topics | How To | Full System Restore | Troubleshoot | Related Topics

Overview

Restore Considerations for This Agent

Restore Destinations

- In-Place Restore
- Out-of-place Restore
- Cross-Application Restores

OVERVIEW

The following page describes the agent-specific restore options. Additional restore options are accessible from the Related Topics menu.

SHAREPOINT DATABASE

The SharePoint Database backup sets allow you to restore SharePoint Database Components and Site Collections.

You can perform the following types of restores:

Application	Specific Restore Procedures	Common Restore Procedures
Microsoft SharePoint Foundation 2010 SharePoint Server 2010 (Standard and Enterprise) Microsoft Office Project Server 2010 Fast Search Server 2010 for SharePoint Microsoft Search Server 2010 Microsoft Search Server 2010 Express	Restore a Service Application Restore a Service Application Proxy	Restore a Site Collection Restore an Individual Site Restore a WSS Web Application Content Database Restore a WSS Search
Microsoft Search Server 2008 Microsoft Search Server 2008 Express	Restore a Search Server Shared Service Provider Restore a Shared Service Provider	Restore a Site Collection Restore an Individual Site Restore a WSS Web Application Content Database Restore a WSS Search
Windows SharePoint Services (WSS) version 3		Restore a Site Collection Restore an Individual Site Restore a WSS Web Application Content Database Restore a WSS Search
Microsoft Office SharePoint Server (MOSS) 2007	Restore a Search Server Shared Service Provider Restore a Shared Service Provider Restore a Single Sign-on Database	Restore a Site Collection Restore an Individual Site Restore a WSS Web Application Content Database Restore a WSS Search
Microsoft Office Project Server 2007	Restore Project Server Shared Service Provider	Restore a Site Collection Restore an Individual Site Restore a WSS Web Application Content Database Restore a WSS Search
Microsoft Office Forms Server 2007	Restore a Shared Service Provider	Restore a Site Collection Restore a Teamsite Database
Windows SharePoint Services (WSS) version 2		Restore a Site Collection Restore a Teamsite Database
Microsoft SharePoint Portal Server 2003	Restore a Portal Site Restore a Site Content Database Restore a Site Index Restore a Single Sign-on Database Restore a Webstorage System Database	

When you restore the SharePoint data, you are over-writing your existing data. Data from after the date of that backup will be lost. The restore operation only provides data from the point in time when it was backed up.

If the SQL databases for the SharePoint Server were not backed up by the SharePoint Server iDataAgent, then they must first be restored on the SQL Server

using the Microsoft SQL iDataAgent before performing the SharePoint Server Database Restore Procedure.

For SharePoint Portal Server 2003, if you configure Shared Services, the Portal Site that provides the Shared Services must be restored/exist before restoring any other Portal Sites.

SHAREPOINT DOCUMENT

The SharePoint Document backup sets restore the Top Level sites, sub-sites, Areas, Libraries, and Lists.

RESTORING A SHAREPOINT SERVER DOCUMENT

The system offers the following options for restoring selected Library items when the object already exists in Non-Versioned Libraries, which are available in the **Restore Options** dialog box.

- **Unconditional Overwrite** - If an item that is selected for restore already exists, then that item will be overwritten by the restored item.
- **Skip** - If an item is selected for restore and that item already exists, it will not be restored.
- **Restore All Versions** - Specifies that all versions of a multi-versioned document will be restored to a Version Enabled Library.

NOTES

- Documents restored to Version Enabled libraries will be restored with **Unconditional Overwrite** regardless of the option selected.
- Documents restored to Version Disabled libraries will be restored with **Skip** regardless of the option selected.

RESTORE CONSIDERATIONS FOR THIS AGENT

Before performing any restore procedures for this agent, review the following information:

SHAREPOINT SERVER - GENERAL

If you have not already done so for the Client to which you are restoring data, ensure the Client is configured as follows:

The Base Services of the client will run under the user account that is specified. Use an account that meets this criteria:

- member of the local Administrator Group
- member of the SharePoint Administrator Group
- System Administrator role on the SQL Server Instance

In addition, this account must have "**Log on as Service**" permissions to ensure the Communication (CVD) Services will start. For more information on Base and Communication (CVD) Services, see [Services](#).

Refer to the Knowledge Base article *Galaxy Service Account User Information for Windows 2003 and Window Server 2003 clients* available from the Maintenance Advantage web site.

SHAREPOINT SERVER DATABASE

- When restoring a Site Collection, temp space is required under the Job Results folder for staging Site Collections, Portal Indexes, and SharePoint metadata.
- After restore, a Site Collection will have a new SiteID and will show up as new content during a discover/backup operation. You should manually find the restored site collection and reassign it to the previously assigned subclient.

Otherwise, the backup of an empty subclient may fail, which displays an "ArchiveIndexfailed on MediaAgent - index files are missing, possibly due to a failover" error message and generates an "Failed to record actual create time in index files" event.

- The four databases namely Archive, Draft, Published and Reporting cannot be distributed over multiple subclient. They need to be backed up and restored together as they belong to the same PWA (Project Web Access) Site.
- For WSS Web Application Content Database restores with **Extend URL** option selected, these registry keys are applicable:
 - The sOwnerLogin registry key is used during an in-place restore of a web application with the original name using the specified owner login.
 - The sOwnerEmail registry key is used during an in-place restore of a web application with the original name using the specified owner email address.
 - The bDoNotUseNTLM registry key is used to change the default authentication type of a restored Web application from NTLM to Negotiate (Kerberos).
- For SharePoint 2010 stand-alone deployments, ensure that the SQL Server instance service account and SharePoint 2010 Timer service account are switched to `Local System`. Once the restore is finished, you can switch back to using the previous accounts (e.g., `Network Service`).
- For SharePoint Server 2010, these registry keys are applicable for site collection restore operations:
 - Site collections that are overwritten can be gradually deleted over time by a timer job instead of all at once by enabling the `dwGradualDelete` registry key. This key can reduce impact on SharePoint and SQL Server performance and is recommended for large site collections.
 - The `sDatabaseName` registry key can be used to specify the SQL Server content database as to where the site collection data should be restored. If the

content database is not specified, the site collection data will be restored to the location where there is a high unused capacity of the site location and also its database status is ready.

- The sDatabaseServer registry key can be used to specify the SQL Server containing the content database specified by the sDatabaseName registry key. Both registry keys need to be configured.
- The sHostHeaderWebApplication registry key can be used to restore a site collection with the host name.

SHAREPOINT SERVER DOCUMENT

- When both SharePoint 2003 and SharePoint 2007 servers co-exist on the same client with the SharePoint Agent, the subclient content needs to be properly configured.

See Subclient Content when SharePoint 2003 and 2007 Servers Co-exist for more information.

- The dSharePointDocLocalRestoreDir key is used to restore SharePoint documents to anywhere on the file system. Docs will be restored to location specified by dSharePointDocLocalRestoreDir key only if nLargeFileSizeThresholdValInMBForRestore key is set to 0.
- Option "Unconditional Overwrite" is not applicable for Site Pages. Web Parts on such pages are not overwritten and the user will see duplicate Web Parts. Therefore it is recommended to delete Site Page prior to running recovery operations.

SITE COLLECTIONS, TOP LEVEL SITES, SUBSITES, WEB APPLICATIONS

- For full-fidelity restores, Site Collections should be restored using SharePoint Database backup sets.
- A Portal Site (SharePoint 2003) must be restored using the SharePoint Database backup sets.
- After restoring a Top Level Site, re-configure the connection to the Portal in the Site Settings.
- For successful backup and restore of site collections or personal sites, the SharePoint Administrator Account should also be added as user with Full control for all sites. It can be done using Policy for Web Application (**Application Management - Application Security - Policy for Web Application**).
- To restore a site when standard Libraries and Lists were renamed (e.g., Shared Documents renamed to Instructions), create an empty site using a site template and then restore the content.
- To restore a Top Level Site that was created using a custom template from the central template gallery, it is recommended to create an empty site using the same template type prior to restoring.
- For SharePoint 2003, you should upgrade the virtual servers if they are in the "Upgrade" state prior to restoring entire sites to the virtual servers.
- To restore sites created using a Room Equipment Reservations template, it is recommended to Restore a SharePoint Server Site Collection from the database backup set level. Restoring individual lists, such as Resources, Reservations, and Resource Type is not supported unless the site and lists exist and they are restored in the following order:
 - Items from List Resource Type
 - Items from List Resources
 - Items from List Reservations

AREAS

- Portal Site bucket Areas will be restored into the first available bucket.

DISCUSSION BOARDS

- Some columns may be duplicated when restoring a Discussion Board from SharePoint Portal Server 2003 to SharePoint Server 2007. If so, delete any duplicate columns that are not needed.
- During entire Discussion Board restore:
 - On SharePoint 2003, restored Threaded Views are restored as Flat Views.
 - On SharePoint 2007, it is recommended to delete restored Flat and Threaded Views and use those that are automatically created (Flat.aspx and Threaded.aspx).

LIBRARY AND LIBRARY ITEMS

- While .aspx files for basic Web Part and Dashboard Pages from a Library can be backed up and restored, restoring the file will not restore the Web Part to the page. Modifications made to the page using the Content Editor Web Part will not be restored and cannot be made to the file after it has been restored.
- SharePoint Server 2010 Asset and Dashboard Libraries can be backed up and restored.
- Document versions are always restored as new versions for Version Enabled Libraries. A restored document will not be available with the same version number it had when it was backed up.
- If a document from a Version Enabled Library is restored to a Version Disabled library, only the latest document version will be restored.
- If all document versions from a Library that tracks Major and Minor versions are restored to the same Library or a different Library with the same settings, then all versions will be restored as Minor versions.
- If all document versions from a Library that tracks Major and Minor versions are restored to a Library that tracks only Major versions, then all versions will be restored as Major versions.
- During a library restore, the library's document template is set to default value. If the library used a different template file, or none at all, you must change

the document template properties to the desired value using the "Specify a Custom Template" procedure under "Set up a template for a library" in <http://office.microsoft.com> to work around this issue.

- If the dAddDocWithFPRPC registry key is set to 1, some metadata for SharePoint items (e.g., comments, "Modified By") are restored using FrontPage RPC (FPRPC) as opposed to the standard object model API.
- Restoring Explorer Views may overwrite or corrupt existing Explorer Views and may not work properly. If an Explorer View is overwritten or corrupted, to recreate a Explorer View for SharePoint 2007 libraries:
 - Go to "Create View" menu.
 - Click on "Explorer View" under the "Start from a view template".
 - Type in "Explorer View" as the View Name.

To recreate Explorer Views for SharePoint 2003, the entire Library must be restored and the Explorer View that is created will automatically work.

- While browsing documents in CommCell Console, the size of documents may not match the size that appears in the SharePoint Server User Interface. This is due to metadata being backed up with the document, which artificially could increase its size.
- After restoring an XML form to a Forms Library, do the following to relink it to the Forms Library:
 1. Open the Forms Library in Internet Explorer.
 2. Go to Form Library settings.
 3. Click **Relink forms to this form library**.
 4. Select the restored form.
 5. Click **Relink Forms**.

LIST AND LIST ITEMS

- List items can only be restored to Lists of the same type.
- For versioned list items, since list items are always restored as new items without the same list ID, multiple lists and multiple list items with the same name are allowed. Therefore, you may see duplicates of lists and their items.
- Threaded discussion boards are restored and displayed as Flat views. After restoring, a Threaded view can be simulated if you select the Group By "Subject" View setting.
- Any deleted Lists linked to by Outlook, Excel, Access, etc. must be relinked after the restore.
- Delete any unwanted List Views after the restore (they will appear numerous times).
- Restore of a List may fail if restored to a site that does not have that list template type. For example, some Meeting Workspaces have lists that are specific to the Meeting Workspace, so these cannot be restored to a Document Workspace or a Team Site. List template keywords from Knowledge Base site might not exist on Non-English setup.
- For Survey Lists, the "Allow Multiple Responses" option must be selected in SharePoint List Settings, or the restore will complete with errors.
- For a restored list, list item, versioned document, workflow, or view, the value of the "Modified By" column will be the name of the user account that backed up the item and the "Modified Time" column will be the date and time when the item was backed up as long as the **Use direct database access to restore selected entities** option is selected in Subclient Properties. The versioned documents and items were created in a Document Library, Form Library, Wiki Library, Picture Library, Custom Lists and Tasks, etc.
- Restoring multi-versioned list items (individual items or the entire list) with a renamed "Title" column causes each version of the item to be restored as a separate item.

SHAREPOINT OFFLINE MINING

- When the **Browse data from SQL** browse option is selected in the Browse Options dialog box, virtual server names are displayed instead of virtual server URLs while browsing content of an offline SharePoint 2003 database.
- When the **Browse data from SQL** browse option is selected in the Browse Options dialog box, items from Libraries located in Portal Areas are not available for restore while browsing content of an offline SharePoint 2003 database.

RESTORE DESTINATIONS

SHAREPOINT SERVER DOCUMENT

IN-PLACE RESTORE

- Same path/destination

By default, the SharePoint Server iDataAgent restores data to the client computer and path from which it originated; this is referred to as an in-place restore.

- To restore a Site Collection, you should restore a Top-Level Site first and then the subsites.

- To restore a deleted Sub-site, browse and select the site and leave all restore options by default.

The following section enumerates the types of restore destinations that are supported by the SharePoint Server iDataAgent. See Restore/Recover/Retrieve Destinations - Support for a list of Agents supporting each restore destination type.

OUT-OF-PLACE RESTORE

- Same path/destination
- Different path/destination

You can also restore the data to another Client computer in the CommCell. Keep in mind the following considerations when performing such restores:

- The destination client must reside in the same CommCell as the client whose data was backed up.
- The restore destination must be on another SharePoint Server with the SharePoint Server iDataAgent installed and operational.
- The destination server must either be in the same domain as the original server, or be in a domain having the proper trust relationship established both with the original domain, as well as all of the domains with which the original server's domain had trust relationships.
- The restore data will assume the rights (i.e., permissions) of the parent directory.
- To restore a site created by a user-defined Site Template to a server in a different farm, the Site Template must exist with the same ID in the destination computer. To change the configuration ID for user defined templates, open the `CustomTemplates` table in the Configuration database and modify the ID column for the row for the custom template used.
- To restore a Top Level Site to a different path, browse and select the Site Collection level for the restore destination path.
 - For SharePoint Server Document backup sets, select only one **site** at a time for an out-of-place restore of an entire site.
 - For SharePoint Server Database backup sets, restore operations across clients with different Windows SharePoint Services (WSS) Service Pack levels are not supported.
 - For SharePoint Portal Server 2003 and SharePoint Server 2007, an out-of-place restore of Lookup column types for lists and libraries is not supported because the dependent list or library (which the Lookup column refers to) will not be present on the target machine.

CROSS-APPLICATION RESTORES

SHAREPOINT SERVER DATABASE

- Cross-application restores of databases between different versions of SharePoint Servers are not supported.

SHAREPOINT SERVER DOCUMENT

- Cross-application restores for library and list items to the same or higher SharePoint Server version are supported.

Restore Data - SharePoint Server - How To

[Topics](#) | [How To](#) | [Full System Restore](#) | [Troubleshoot](#) | [Related Topics](#)

[Restore a Site Collection](#)

[Restore an Individual Site](#)

[Restore a WSS Web Application Content Database](#)

[Restore a WSS Search](#)

[Restore a Service Application](#)

[Restore a Service Application Proxy](#)

[Restore a Shared Service Provider](#)

[Restore a Single Sign-on Database](#)

[Restore a Project Server Shared Service Provider](#)

[Restore a Search Server Shared Service Provider](#)

[Restore SharePoint Data Secured by the SQL iDataAgent in a Server Farm](#)

Microsoft Office SharePoint Portal Server 2003

[Restore a Site Collection](#)

[Restore a Teamsite Database](#)

[Restore a Portal Site](#)

Restore a Site Content Database

Restore a Site Index

Restore a Single Sign-on Database

Restore a Webstorage System Database

RESTORE A SITE COLLECTION

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.

Required Capability: See Capabilities and Permitted Actions

▶ To restore the Site Collection database:

1. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
 2. From the **Browse Data** window, select **Site Collection**.
 3. From the **Restore Options** dialog box, enter the required information in the Site Collection tab.
 4. Continue with the restore procedure.
-

RESTORE AN INDIVIDUAL SITE

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.
- Using this procedure will restore all site permissions and all versions of the site.
- Before backing up the site, the bSiteExportEnabled registry key must have been set to 1.

Required Capability: See Capabilities and Permitted Actions

▶ To restore an individual Site from a Database backup set:

1. Right-click a SharePoint database backup set and select **Browse Backup Data**. See Browse and Restore for step-by-step instructions.
 2. Click **OK**.
 3. From the **Browse Data** window, select **Site** or select **Site** under **Site Collections** if the Site Collection was backed up.
 4. Click **Recover All Selected...**
 5. In Report Options dialog box, click the **Site** tab.
 6. Select the site to restore from the list and click **Overwrite URL**. The existing site will be deleted and restored only when **Overwrite URL** is selected. If the site cannot be deleted, the content will be merged into an existing site.
 - For out-of-place restores, the top-level sites will be restored as top-level sites and subsites will be restored as subsites.
 - Set the bSiteImportRetainObjectIdentity to 1 to override the object identity if the Site URL path is similar to the original one for out-of-place restore operations.
 7. Click **OK**.
-

RESTORE A WSS WEB APPLICATION CONTENT DATABASE

STAND-ALONE DEPLOYMENT

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.
- If the Web Application Content Database was removed from the Virtual Server but the database was not deleted from the SQL Instance, delete it before beginning the restore (for Stand-alone or Single server with SQL Server Deployments).
- If the Web Application was deleted, or if SharePoint was removed from the IIS web site with the option "Delete IIS Web sites", or if an IIS web site does not exist, then the IIS web site should be manually created in IIS.
- If SharePoint was removed from an IIS web site, delete the WSS Web Application prior to restoring the WSS Web Application Content Database.

Required Capability: See Capabilities and Permitted Actions

▶ To restore the Windows SharePoint Services (WSS) Web Application:

1. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
2. From the **Browse Data** window, expand the WSS Web Application node and select **Web Application Database**. Click **Recover all Selected**.
3. From the **Restore Options** dialog box, enter the required information in the Restore Options Windows SharePoint Services Web App Tab.
4. Continue with the restore procedure.

SERVER FARM (SMALL, MEDIUM, LARGE)

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.
- If SharePoint was removed from an IIS web site, delete the WSS Web Application prior to restoring the WSS Web Application Content Database.
- If the Web Application was deleted or SharePoint was removed from the IIS web site with the option "Delete IIS Web sites", then the IIS web site should be manually created in IIS.
- To preserve the original Web Application name, set the sOwnerLogin and sOwnerEmail registry keys, and then restore the WSS Web Application Content Database with the **Extend URL** option selected.

Required Capability:: See Capabilities and Permitted Actions

▶ To restore the WSS Web Application:

1. Restore the WSS Web Application Database using the SQL iDataAgent. Refer to Recovering Database for step-by-step instructions. [Do not restore the SharePoint Configuration Database].
2. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
3. From the **Browse Data** window, expand the WSS Web Application node and select **Web Application Database**.
4. From the **Restore Options** dialog box, enter the required information in the Restore Options Windows SharePoint Services Web App Tab.
5. Continue with the restore procedure.
6. For SharePoint 2010: After you restore a Web Application with the **Extend URL** option, you must do the following:
 - a. Open **IIS Manager**.
 - b. Under **Web Site**, select the restored Web Application, and then check the Application Pool name assigned to it.
 - c. If the Application Pool credentials are set to **NetworkService**, then stop the Web Site.
 - d. Select a different Application Pool with Managed Account credentials.
 - e. Start the Web Site.

RESTORE A WSS SEARCH

STAND-ALONE DEPLOYMENT

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.
- If the WSS Search database was not deleted from the SQL Instance, delete it before beginning the restore (for Stand-alone or Single server with SQL Server Deployments).
- In Windows Services, stop the Windows SharePoint Services Search service and delete WSS Search Index that is typically located under `.. \Microsoft Office Servers\12.0\Data Application`.

Required Capability: See Capabilities and Permitted Actions

▶ To restore a WSS Search:

1. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
2. From the **Browse Data** window, select the **SP Search** node. Click **Recover all Selected**.
3. From the **Restore Options** dialog box, enter the required information in the Restore Options WSS Search DB tab.
4. Continue with the restore procedure.

SERVER FARM (SMALL, MEDIUM, LARGE)

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.
- In Windows Services, stop the Windows SharePoint Services Search service and delete WSS Search Index that is typically located under `.. \Microsoft Office Servers\12.0\Data Application`.

Required Capability: See Capabilities and Permitted Actions

▶ To restore a WSS Search:

1. Restore the WSS Search Database using the SQL iDataAgent. Refer to Recovering a Database for step-by-step instructions. Do not restore the SharePoint Configuration Database.
2. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
3. From the **Browse Data** window, select **SP Search**. Click **Recover all Selected**.
4. From the **Restore Options** dialog box, enter the required information in the Restore Options WSS Search DB tab.
5. Continue with the restore procedure.

RESTORE A SERVICE APPLICATION**STAND-ALONE DEPLOYMENT****Before You Begin:**

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.
- This procedure applies only to database backup sets.
- For a successful restore, ensure that the SQL Server instance service account and SharePoint 2010 Timer service account are switched to `Local System`. Once the restore is finished, you can switch back to using the previous accounts (e.g., `Network Service`).
- To restore Microsoft Office Project Server 2010 Project Web Access (PWA) Sites, follow the procedure below. These sites cannot be restored using the Restore a SharePoint Server Site Collection procedure or the Restore a 2007 Project Web Access (PWA) Site procedure.

Required Capability: See Capabilities and Permitted Actions

▶ To restore a Service Application:

1. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
2. From the **Browse Data** window, select **Service Application**.
3. From the **Restore Options** dialog box, enter the required information in the Service Application tab.
4. Continue with the restore procedure.

SERVER FARM (SMALL, MEDIUM, LARGE)**Before You Begin:**

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.
- This procedure applies only to database backup sets.

Required Capability: See Capabilities and Permitted Actions

▶ To restore a Service Application:

1. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
2. From the **Browse Data** window, select **Service Application**.
3. From the **Restore Options** dialog box, enter the required information in the Service Application tab.
4. Continue with the restore procedure.

RESTORE A SERVICE APPLICATION PROXY**STAND-ALONE DEPLOYMENT****Before You Begin:**

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.

- This procedure applies only to database backup sets.
- For a successful restore, ensure that the SQL Server instance service account and SharePoint 2010 Timer service account are switched to `Local System`. Once the restore is finished, you can switch back to using the previous accounts (e.g., `Network Service`).
- To restore Microsoft Office Project Server 2010 Project Web Access (PWA) Sites, follow the procedure below. These sites cannot be restored using the Restore a SharePoint Server Site Collection procedure or the Restore a 2007 Project Web Access (PWA) Site procedure.

Required Capability: See Capabilities and Permitted Actions

▶ To restore a Service Application Proxy:

1. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
2. From the **Browse Data** window, select **Service Application Proxy**.
3. From the **Restore Options** dialog box, enter the required information in the Service Application Proxy tab.
4. Continue with the restore procedure.

SERVER FARM (SMALL, MEDIUM, LARGE)

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.
- This procedure applies only to database backup sets.

Required Capability: See Capabilities and Permitted Actions

▶ To restore a Service Application Proxy:

1. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
2. From the **Browse Data** window, select **Service Application Proxy**.
3. From the **Restore Options** dialog box, enter the required information in the Service Application Proxy tab.
4. Continue with the restore procedure.

RESTORE A SITE COLLECTION

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.

Required Capability: See Capabilities and Permitted Actions

▶ To restore the Site Collection database:

1. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
2. From the **Browse Data** window, select **Site Collection**.
3. From the **Restore Options** dialog box, enter the required information in the Site Collection tab.
4. Continue with the restore procedure.

RESTORE A WSS WEB APPLICATION CONTENT DATABASE

STAND-ALONE DEPLOYMENT

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.
- If the Web Application Content Database was removed from the Virtual Server but the database was not deleted from the SQL Instance, delete it before beginning the restore (for Stand-alone or Single server with SQL Server Deployments).
- If the Web Application was deleted, or if SharePoint was removed from the IIS web site with the option "Delete IIS Web sites", or if an IIS web site does not exist, then the IIS web site should be manually created in IIS.
- If SharePoint was removed from an IIS web site, delete the WSS Web Application prior to restoring the WSS Web Application Content Database.

Required Capability: See Capabilities and Permitted Actions

▶ To restore the Windows SharePoint Services (WSS) Web Application:

1. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.

2. From the **Browse Data** window, expand the WSS Web Application node and select **Web Application Database**. Click **Recover all Selected**.
3. From the **Restore Options** dialog box, enter the required information in the Restore Options Windows SharePoint Services Web App Tab.
4. Continue with the restore procedure.

SERVER FARM (SMALL, MEDIUM, LARGE)

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.
- If SharePoint was removed from an IIS web site, delete the WSS Web Application prior to restoring the WSS Web Application Content Database.
- If the Web Application was deleted or SharePoint was removed from the IIS web site with the option "Delete IIS Web sites", then the IIS web site should be manually created in IIS.
- To preserve the original Web Application name, set the sOwnerLogin and sOwnerEmail registry keys, and then restore the WSS Web Application Content Database with the **Extend URL** option selected.

Required Capability: See Capabilities and Permitted Actions

▶ To restore the WSS Web Application:

1. Restore the WSS Web Application Database using the SQL iDataAgent. Refer to Recovering Database for step-by-step instructions. [Do not restore the SharePoint Configuration Database].
2. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
3. From the **Browse Data** window, expand the WSS Web Application node and select **Web Application Database**.
4. From the **Restore Options** dialog box, enter the required information in the Restore Options Windows SharePoint Services Web App Tab.
5. Continue with the restore procedure.
6. For SharePoint 2010: After you restore a Web Application with the **Extend URL** option, you must do the following:
 - a. Open **IIS Manager**.
 - b. Under **Web Site**, select the restored Web Application, and then check the Application Pool name assigned to it.
 - c. If the Application Pool credentials are set to **NetworkService**, then stop the Web Site.
 - d. Select a different Application Pool with Managed Account credentials.
 - e. Start the Web Site.

RESTORE A WSS SEARCH

STAND-ALONE DEPLOYMENT

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.
- If the WSS Search database was not deleted from the SQL Instance, delete it before beginning the restore (for Stand-alone or Single server with SQL Server Deployments).
- In Windows Services, stop the `Windows SharePoint Services Search` service and delete `WSS Search Index` that is typically located under `..\Microsoft Office Servers\12.0\Data Application`.

Required Capability: See Capabilities and Permitted Actions

▶ To restore a WSS Search:

1. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
2. From the **Browse Data** window, select the **SP Search** node. Click **Recover all Selected**.
3. From the **Restore Options** dialog box, enter the required information in the Restore Options WSS Search DB tab.
4. Continue with the restore procedure.

SERVER FARM (SMALL, MEDIUM, LARGE)

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.
- In Windows Services, stop the `Windows SharePoint Services Search` service and delete `WSS Search Index` that is typically located under `..\Microsoft`

Office Servers\12.0\Data Application.

Required Capability: See Capabilities and Permitted Actions

▶ To restore a WSS Search:

1. Restore the WSS Search Database using the SQL iDataAgent. Refer to Recovering a Database for step-by-step instructions. Do not restore the SharePoint Configuration Database.
2. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
3. From the **Browse Data** window, select **SP Search**. Click **Recover all Selected**.
4. From the **Restore Options** dialog box, enter the required information in the Restore Options WSS Search DB tab.
5. Continue with the restore procedure.

RESTORE A SHARED SERVICE PROVIDER

STAND-ALONE DEPLOYMENT

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.
- Delete the Shared Services Provider if it is not default. If it is the default and others do not exist, create new Shared Services Provider for temporal usage and set it as default.
- Delete old Shared Services Provider.
- Delete the WSS Web Application that hosted the Shared Services Provider.

Required Capability: See Capabilities and Permitted Actions

▶ To restore a Shared Service Provider:

1. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
2. Follow the procedure Restore a SharePoint Server WSS Web Application Content Database to restore the WSS Web Application that hosted the Shared Services Provider.
3. Using `stsadm.exe` command, delete site `../ssp/admin` from restored Web Application. For example, `stsadm -o deletesite -url http://<URL of WebApp Hosting SSP>/ssp/admin`.
4. From the **Browse Data** window, expand the Shared Services Provider, select **Shared Services**. Click **Recover all Selected**.
5. From the **Restore Options** dialog box, enter the required information in the Restore Options Shared Service Provider DB, Search Shared DB, and Search Index Server tabs.
6. Continue with the restore procedure.
7. Set restored Shared Services Provider as default if necessary and re-associate regional Web Application back to it. Delete Shared Services Provider for temporal usage if it was created.

SERVER FARM (SMALL, MEDIUM, LARGE)

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.

Required Capability: See Capabilities and Permitted Actions

▶ To restore a Shared Service Provider:

1. Follow the procedure Restore a SharePoint Server WSS Web Application Content Database to restore the WSS Web Application that hosted the Shared Services Provider.
2. Using `stsadm.exe` command, delete site `../ssp/admin` from restored Web Application. For example, `stsadm -o deletesite -url http://<URL of WebApp Hosting SSP>/ssp/admin`.
3. Restore the Shared Services Provider Databases using the SQL iDataAgent. Refer to Recovering Database for step-by-step instructions. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
4. From the **Browse Data** window, expand the Shared Services Provider, select **Shared Services**. Click **Recover all Selected**.
5. From the **Restore Options** dialog box, enter the required information in the Restore Options Shared Service Provider DB, Search Shared DB, and Search Index Server tabs.
6. Continue with the restore procedure.

7. Set restored Shared Services Provider as default if necessary and re-associate regional Web Application back to it. Delete Shared Services Provider for temporal usage if it was created.

RESTORE A SINGLE SIGN-ON DATABASE

STAND-ALONE OR SINGLE SERVER WITH SQL SERVER DEPLOYMENTS

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.

Required Capability: See Capabilities and Permitted Actions

▶ To restore the Single Sign-on database / Stand-alone or Single server with SQL Server Deployments:

1. Stop the Microsoft Single Sign-on Service.
2. If the SSO SQL database still exists, delete it.
3. Start the Microsoft Single Sign-on Service.
4. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
5. From the **Browse Data** window, select **Single Sign-on Database**.
6. From the **Restore Options** dialog box, enter the required information in the Single Sign-on Database tab.
7. Continue with the restore procedure.

SERVER FARM (SMALL, MEDIUM, LARGE)

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.

Required Capability: See Capabilities and Permitted Actions

▶ To restore the Single Sign-on database / Server Farm (Small, Medium, Large):

1. Stop the Microsoft Single Sign-on Service on All Servers in the farm.
2. Restore the Single Sign-On Database on the SQL Server using the SQL iDataAgent. Refer to Recovering Database for step-by-step instructions.
3. Start the Microsoft Single Sign-on Service on the Job Server.
4. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
5. From the **Browse Data** window, select **Single Sign-on Database**.
6. From the **Restore Options** dialog box, enter the required information in the Single Sign-on Database tab.
7. Continue with the restore procedure.
8. Restart the Microsoft Single Sign-on Service on the Job Server.
9. Start the Microsoft Single Sign-on Service on all other Servers in the Farm.

RESTORE A PROJECT SERVER SHARED SERVICE PROVIDER

STAND-ALONE DEPLOYMENT

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.
- Project Web Access (PWA) sites cannot be restored using the Restore a SharePoint Server Site Collection procedure. Instead, follow the procedure outlined below.
- These Project Server databases can typically be restored: `Project server_Archive`, `Project server_Draft`, `Project server_Published`, and `Project server_Reporting`. These cannot be distributed over multiple subclient. They need to be backed up and restored together as they belong to the same PWA (Project Web Access) Site.

Required Capability: See Capabilities and Permitted Actions

▶ To restore a Project Web Access (PWA) Site:

1. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
2. From the **Browse Data** window, select the **Project Server Application** node. Click **Recover all Selected**.
3. From the **Restore Options** dialog box, enter the required information in the Restore Options Project Server Application tab.
4. Continue with the restore procedure.

SERVER FARM (SMALL, MEDIUM, LARGE)

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.

Required Capability: See Capabilities and Permitted Actions

▶ To restore a Project Web Access (PWA) Site:

1. Restore the Project Server Database using the SQL iDataAgent. Refer to Recovering Database for step-by-step instructions. Do not restore the SharePoint Configuration Database.
2. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
3. From the **Browse Data** window, select **Project Server Application**. Click **Recover all Selected**.
4. From the **Restore Options** dialog box, enter the required information in the Restore Options Project Server Application tab.
5. Continue with the restore procedure.

RESTORE A SEARCH SERVER SHARED SERVICE PROVIDER

STAND-ALONE DEPLOYMENT

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.

Required Capability: See Capabilities and Permitted Actions

▶ To restore a Shared Service Provider:

1. At the **Databases** backup set level, begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
2. From the **Browse Data** window, expand the Shared Services Provider, select **SharedServices**. Click **Recover all Selected**.
3. From the **Restore Options** dialog box, enter the required information in the Restore Options Shared Service Provider DB, Search Shared DB, and Search Index Server tabs.
4. Continue with the restore procedure.

SERVER FARM (SMALL, MEDIUM, LARGE)

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.

Required Capability: See Capabilities and Permitted Actions

▶ To restore a Shared Service Provider:

1. Restore the Shared Services Provider Databases using the SQL iDataAgent. Refer to Recovering a Database for step-by-step instructions
2. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
3. From the **Browse Data** window, expand the Shared Services Provider, select **SharedServices**. Click **Recover all Selected**.
4. From the **Restore Options** dialog box, enter the required information in the Restore Options Shared Service Provider DB, Search Shared DB, and Search Index Server tabs.
5. Continue with the restore procedure.

RESTORE A SITE COLLECTION

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.

Required Capability: See Capabilities and Permitted Actions

▶ To restore the Site Collection database:

1. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
2. From the **Browse Data** window, select **Site Collection**.
3. From the **Restore Options** dialog box, enter the required information in the Site Collection tab.
4. Continue with the restore procedure.

RESTORE A TEAMSITE DATABASE

STAND-ALONE OR SINGLE SERVER WITH SQL SERVER DEPLOYMENTS

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.
- If the Teamsite database was not deleted from the SQL Instance, delete it before beginning the restore (for Stand-alone or Single server with SQL Server Deployments).

Required Capability: See Capabilities and Permitted Actions

▶ To restore a Teamsite database:

1. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
2. From the **Browse Data** window, select the **Teamsite Database**.
3. From the **Restore Options** dialog box, enter the required information in the Restore Options Teamsite Databases tab.
4. Continue with the restore procedure.
5. Restore the directory for the IIS Virtual Server using the File System iDataAgent.
6. Restart IIS.

SERVER FARM (SMALL, MEDIUM, LARGE)

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.

Required Capability: See Capabilities and Permitted Actions

▶ To restore a Teamsite database:

1. Restore the Teamsite Databases using the SQL iDataAgent. Refer to Recovering Database for step-by-step instructions. Do not restore the SharePoint Configuration Database.
2. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
3. From the **Browse Data** window, select the **Teamsite Database**.
4. From the **Restore Options** dialog box, enter the required information in the Restore Options Teamsite Databases tab.
5. Continue with the restore procedure.
6. Restore the directory for the IIS Virtual Server using the File System iDataAgent.
7. Restart IIS.

Microsoft Office SharePoint Portal Server 2003 Procedures

RESTORE A SITE COLLECTION

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.

Required Capability: See Capabilities and Permitted Actions

▶ To restore the Site Collection database:

1. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
 2. From the **Browse Data** window, select **Site Collection**.
 3. From the **Restore Options** dialog box, enter the required information in the Site Collection tab.
 4. Continue with the restore procedure.
-

RESTORE A TEAMSITE DATABASE

STAND-ALONE OR SINGLE SERVER WITH SQL SERVER DEPLOYMENTS

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.
- If the Teamsite database was not deleted from the SQL Instance, delete it before beginning the restore (for Stand-alone or Single server with SQL Server Deployments).

Required Capability: See Capabilities and Permitted Actions

▶ To restore a Teamsite database:

1. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
2. From the **Browse Data** window, select the **Teamsite Database**.
3. From the **Restore Options** dialog box, enter the required information in the Restore Options Teamsite Databases tab.
4. Continue with the restore procedure.
5. Restore the directory for the IIS Virtual Server using the File System iDataAgent.
6. Restart IIS.

SERVER FARM (SMALL, MEDIUM, LARGE)

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.

Required Capability: See Capabilities and Permitted Actions

▶ To restore a Teamsite database:

1. Restore the Teamsite Databases using the SQL iDataAgent. Refer to Recovering Database for step-by-step instructions. Do not restore the SharePoint Configuration Database.
 2. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
 3. From the **Browse Data** window, select the **Teamsite Database**.
 4. From the **Restore Options** dialog box, enter the required information in the Restore Options Teamsite Databases tab.
 5. Continue with the restore procedure.
 6. Restore the directory for the IIS Virtual Server using the File System iDataAgent.
 7. Restart IIS.
-

RESTORE A PORTAL SITE

STAND-ALONE OR SINGLE SERVER WITH SQL SERVER DEPLOYMENTS

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.
- If the portal site databases were not deleted from the SQL Instance, delete them before beginning the restore (for Stand-alone or Single server with SQL Server Deployments).
- Disconnect any Virtual Servers that are mapped to the portal site.

Required Capability: See Capabilities and Permitted Actions

▶ To restore a Portal Site:

1. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
2. From the **Browse Data** window, expand the Portal Site node, select Portal Site, and deselect the **Index** and any **Site Content Databases**; these should be restored after the Portal Site restore is complete. Click **Recover all Selected**.
3. From the **Restore Options** dialog box, enter the required information in the Restore Options Site Databases tab.
4. Continue with the restore procedure.
5. When the restore completes, perform the Site Content Database restore.
6. When the Site Content database restore completes, perform the Site Index restore.
7. Restore the directory for the IIS Virtual Server using the File System iDataAgent.
8. Restart IIS.

SERVER FARM (SMALL, MEDIUM, LARGE)

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.
- Disconnect any Virtual Servers that are mapped to the portal site.

Required Capability: See Capabilities and Permitted Actions

▶ To restore a Portal Site:

1. Restore the Portal Site Databases using the SQL iDataAgent to Recovering a Database. Do not restore the SharePoint Configuration Database.
2. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
3. From the **Browse Data** window, expand the Portal Site node, select Portal Site, and deselect the **Index** and any **Site Content Databases**; these should be restored after the Portal Site restore is complete. Click **Recover all Selected**.
4. From the **Restore Options** dialog box, enter the required information in the Restore Options Site Databases tab.
5. Continue with the restore procedure.
6. When the restore completes, perform the Site Content Database restore.
7. When the Site Content database restore completes, perform the Site Index restore.
8. Restore the directory for the IIS Virtual Server using the File System iDataAgent.
9. Restart IIS.

RESTORE A SITE CONTENT DATABASE

STAND-ALONE OR SINGLE SERVER WITH SQL SERVER DEPLOYMENTS

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.
- If the Site Content Database restore is part of Portal Site Restore do not restore the Site Content database before the Portal Site Restore.
- If the Site Content Database was removed from the Virtual Server but the database was not deleted from the SQL Instance, delete it before beginning the restore (for Stand-alone or Single server with SQL Server Deployments).

Required Capability: See Capabilities and Permitted Actions

▶ To restore the Site Content database:

1. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
2. From the **Browse Data** window, expand the Portal Site node and select **Site Content Database**.
3. From the **Restore Options** dialog box, enter the required information in the Restore Options Site Content Databases tab.
4. Continue with the restore procedure.

SERVER FARM (SMALL, MEDIUM, LARGE)

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.
- If the Site Content Database restore is part of Portal Site Restore do not restore the Site Content database before the Portal Site Restore.

Required Capability: See Capabilities and Permitted Actions

▶ To restore the Site Content database:

1. Restore the Site Content Databases using the SQL iDataAgent. Refer to Recovering a Database for step-by-step instructions. Do not restore the SharePoint Configuration Database.
 2. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
 3. From the **Browse Data** window, expand the Portal Site node and select **Site Content Database**.
 4. From the **Restore Options** dialog box, enter the required information in the Restore Options Site Content Databases tab.
 5. Continue with the restore procedure.
-

RESTORE A SITE INDEX

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.
- Restore the Portal Site before restoring the Index.

Required Capability: See Capabilities and Permitted Actions

▶ To restore the Site Index:

1. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
 2. From the **Browse Data** window, expand the Portal Site node and select the **Index**.
 3. From the **Restore Options** dialog box, enter the required information in the Restore Options Site Index tab.
 4. Continue with the restore procedure.
-

RESTORE A SINGLE SIGN-ON DATABASE

STAND-ALONE OR SINGLE SERVER WITH SQL SERVER DEPLOYMENTS

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.

Required Capability: See Capabilities and Permitted Actions

▶ To restore the Single Sign-on database / Stand-alone or Single server with SQL Server Deployments:

1. Stop the Microsoft Single Sign-on Service.
 2. If the SSO SQL database still exists, delete it.
 3. Start the Microsoft Single Sign-on Service.
 4. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
 5. From the **Browse Data** window, select **Single Sign-on Database**.
 6. From the **Restore Options** dialog box, enter the required information in the Single Sign-on Database tab.
 7. Continue with the restore procedure.
-

SERVER FARM (SMALL, MEDIUM, LARGE)

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.

Required Capability: See Capabilities and Permitted Actions

▶ To restore the Single Sign-on database / Server Farm (Small, Medium, Large):

1. Stop the Microsoft Single Sign-on Service on All Servers in the farm.
2. Restore the Single Sign-On Database on the SQL Server using the SQL iDataAgent. Refer to Recovering Database for step-by-step instructions.
3. Start the Microsoft Single Sign-on Service on the Job Server.
4. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.

5. From the **Browse Data** window, select **Single Sign-on Database**.
 6. From the **Restore Options** dialog box, enter the required information in the Single Sign-on Database tab.
 7. Continue with the restore procedure.
 8. Restart the Microsoft Single Sign-on Service on the Job Server.
 9. Start the Microsoft Single Sign-on Service on all other Servers in the Farm.
-

RESTORE A WEBSTORAGE SYSTEM DATABASE

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.
- The Document Management component for Microsoft Office SharePoint Portal Server 2003 must be installed on the server.
- On the "List and Manage Document Libraries" page of the SharePoint Portal Server Central Administration, disconnect any existing document libraries.

Required Capability: See Capabilities and Permitted Actions

▶ To restore the Webstorage System database:

1. Begin a restore procedure using the SharePoint Server iDataAgent. See Browse and Restore for step-by-step instructions.
 2. From the **Browse Data** window, select **Webstorage System Database**.
 3. Continue with the restore procedure.
 4. After successfully completing a restore, any restored document libraries that were disconnected or deleted will come back with a Portal Association value of "None". To associate the library with a Portal Site, disconnect and then reconnect the library manually.
-

RESTORE SHAREPOINT DATA WITH SQL SERVER RBS ENABLED IN A SERVER FARM

To restore unstructured data in RBS, which was either backed up by SnapProtect or the SQL Server iDataAgent, in a server farm configuration follow the steps given below:

1. Ensure that the RBS is enabled on the destination instance.
 2. From the CommCell Browser, navigate to the **SQL agent | Backup set** and click **All Tasks** and then click **Browse**.
 3. Run a browse operation.
 4. From the Browse window, Select Objects From the Browse Window for Restore.
 5. After completing your selections, you can either start an immediate restore or schedule the restore.
 - If you want to schedule the job, click the Job Initiation tab from the Restore Options dialog box, click **Schedule**, schedule the job, and then click **OK**.
 - If you want to run the job now, accept or click **Run Immediately** in the same tab and then click **OK**.
 6. From the CommCell Browser, navigate to the **SharePoint agent | Database** and click **All Tasks** and then click **Browse**.
 7. Run a browse operation.
 8. From the Browse window, Select Objects From the Browse Window for Restore.
 9. After completing your selections, you can either start an immediate restore or schedule the restore.
 - If you want to schedule the job, click the Job Initiation tab from the Restore Options dialog box, click **Schedule**, schedule the job, and then click **OK**.
 - If you want to run the job now, accept or click **Run Immediately** in the same tab and then click **OK**.
 10. For Out-of-Place, ensure that the RBS is installed on the destination client.
 11. From SharePoint Management Shell type the following commands to re-attach the restored content database with web application:


```
$cdb = Get-SPContentDatabase <Content database Name>
$rbss = $cdb.RemoteBlobStorageSettings
$rbss.Installed()
$rbss.Enable()
$rbss.SetActiveProviderName($rbss.GetProviderNames()[0])
```
-

Basic Restore

Topics | How To | Related Topics

Overview

Time Range Options

OVERVIEW

There are two functions that help you retrieve backed up data from the backup media: Browse and Restore. Browse operations allow you to view the data that has been backed up for a client computer without actually restoring the data. Restore operations retrieve the data from the backup media and restore it to the desired location.

In the CommCell Browser, the Browse and various Restore commands appear in the right-click menus at the agent, instance and/or backup set levels, depending on agent.

Using the Restore commands, i.e., restoring without browsing, is most appropriate when you want to restore the latest backup job for an agent, instance or backup set and want to retain the current file structure.

In certain situations and for supported agents, Restore operations can run without utilizing the Browse feature. For example, if you know the path/name of the volume of the data that you want to restore, you can restore it without browsing. In these agents, this procedure is most appropriate when the number of paths for the data that you want to restore is small or when the data that you want to restore is at a single volume. If you want to restore data from many different paths or volumes, you should probably select the data from the Browse window.

TIME RANGE OPTIONS

In a Basic Restore, point-in-time data can be restored by specifying time range options in the Advanced Restore Options (Time Range) dialog box. See Time Range Options for Basic Restore for step-by-step instructions. When a time range is specified for a Basic Restore, the latest version of the backup job within the given time range will be restored.

Basic Restore - How To

Topics | How To | Related Topics

Basic Restore

Time Range Options for Basic Restore

BASIC RESTORE

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.

Required Capability: See Capabilities and Permitted Actions

▶ To restore data without using browse:

1. From the CommCell Browser, right-click the agent, instance or backup set that contains the data you want to restore, click **All Tasks** and then click the available **Restore** command (command names vary by agent).
2. In the **Restore** dialog box, type the starting path of the data you want to restore.
3. From the **Restore Options** and **Advanced Restore Options** dialog boxes, select the restore options that you want to use. When you accept all the default settings, you will be restoring the selected data to its original location. See Restore Backup Data for complete information on the agent-specific restore options.
4. After completing your selections, you can either start an immediate restore or schedule the restore.
 - If you want to schedule the job, click the Job Initiation tab from the Restore Options dialog box, click **Schedule**, and enter your selections in the Schedule Details (Schedule Details) dialog box. Clicking **OK** from this dialog box saves your schedule. See Scheduled Data Recovery Operations for an overview of this feature.
 - If you want to run the job now, accept or click **Run Immediately** in the same tab and then click **OK**.

You can monitor the progress of the restore job in the Job Controller. While the job is running, you can right-click the job in the Job Controller and select **Detail**

to view information on the job.

After the data has been restored, you will see a job completion message in the Job Controller and Event Viewer.

TIME RANGE OPTIONS FOR BASIC RESTORE

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.

Required Capability: See Capabilities and Permitted Actions

▶ To provide time range options for basic restore:

1. From the CommCell Browser, right-click the agent, instance or backup set that contains the data you want to restore, click **All Tasks** and then click the available **Restore** command (command names vary by agent).
 2. In the **Restore** dialog box, type the starting path of the data you want to restore.
 3. From the **Restore Options** and **Advanced Restore Options** dialog boxes, select the Time Range tab.
 4. In the Advanced Restore Options (Time Range) dialog box, clear the **Show Deleted Items** option, if required.
 In the Specify Restore Time area select the **Time Zone** for the time range options. Select the **Exclude Data Before** option and select the start date and time from which you wish to restore data, and select the **Browse Data Before** option and select the end date and time until which you wish to restore data.
 5. Click **OK** in the Advanced Restore Options dialog box.
 6. Click **OK** in the Restore Options dialog box to execute the restore.
-

[Back To Top](#)

Browse and Restore

[Topics](#) | [How To](#) | [Related Topics](#)

OVERVIEW

There are two functions that help you retrieve backed up data from the backup media: browse and restore. In the CommCell Browser, the browse and variously-named restore commands appear, depending on agent, in the right-click menus at the agent, instance and/or backup set levels.

Browse operations allow you to view data that has been backed up by the agent on the client computer and select all or some of that data. Depending on the agent, there are several options available to customize your browse. See [Browse Data](#) for comprehensive information on Browse operations.

Restore operations allow you to retrieve data from backup media and restore it to the desired location. Restoring without browsing is most appropriate when you want to restore the latest backup job for an agent, instance or backup set and want to retain the current file structure. See [Basic Restore](#) for more information on restoring without using browse.

Browse and Restore

The Browse and Restore procedure is a sequential procedure that combines the two procedures. When you select a **Browse** command from the CommCell Browser, you can define and run one of many potential browse sequences. At the end of the browse, when you are looking at the resulting information presented in the Browse window, you can continue with a restore procedure simply by selecting data and clicking the **Recover All Data** button. As with the browse, depending on the agent, there are several options available to customize your restore.

Perform a **browse and restore** operation when you want to:

- restore from an earlier backup
 - restore only select files/objects
 - restore deleted files/objects
 - when you don't want or don't need to retain the current file structure
 - utilize browse options
-

Browse and Restore - How To

[Topics](#) | [How To](#) | [Related Topics](#)

BROWSE AND RESTORE

Before You Begin:

- Review the general and agent-specific restore requirements accessed from Restore Backup Data prior to performing any restore operation.

Required Capability: See Capabilities and Permitted Actions

▶ To browse and restore data:

1. From the CommCell Browser, right-click the agent, instance, backup set, or Legal hold set (for Legal Hold data) that contains the data you want to restore, click **All Tasks** and then click the available **Browse** command (command names vary by agent).
2. Run a browse operation. See Browse Data for a list of customized browse operations and their step-by-step instructions. If you accept all defaults, you will be browsing the latest backups for the selected data.
3. From the Browse window, Select Objects From the Browse Window for Restore.
4. From the agent's **Restore Options** and **Advanced Restore Options** dialog boxes, select the restore options that you want to use. For agents with multiple tabs, do not click **OK** until you have used all of the desired tabs. When you accept all the default settings, you will be restoring the selected data to its original location. See Restore Backup Data for access to complete information on the agent-specific Restore Destination options and procedures available.
5. When restoring encrypted data, refer to Data Encryption for comprehensive feature information and procedures for using the Encryption tab of the Advanced Restore Options dialog box.
6. After completing your selections, you can either start an immediate restore or schedule the restore.
 - If you want to schedule the job, click the Job Initiation tab from the Restore Options dialog box, click **Schedule**, schedule the job, and then click **OK**.
 - If you want to run the job now, accept or click **Run Immediately** in the same tab and then click **OK**.

While the job is running, you can right-click the job in the Job Controller and select **Detail** to view information on the job. After the data has been restored, you will see a job completion message in the Job Controller and Event Viewer.

[Back To Top](#)

Backup Sets - SharePoint Server iDataAgent

Topics | How To | Related Topics

Overview

Microsoft SharePoint Server iDataAgent Configurable Properties

- User Security

Using Backup Sets

OVERVIEW

During installation of the SharePoint Server iDataAgent, the system automatically creates two default backup sets (`Documents` and `Databases`) and each contains a default subclient. Types are assigned to a backup set. When creating a new backup set, the types that can be selected are either:

- **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 can specify backing up SharePoint 2007 site collections, WSS web application content databases, shared service providers, WSS searches, global search settings. If **Force use of V2 APIs** is selected, then the content of the backup set will backup SharePoint 2003 site collections, portal sites, site content databases, site indexes, teamsite databases, and webstorage system databases.

After installation, you have the option of creating a User-defined Backup Set, which also will contain a default subclient.

See Backup Sets for information on the different types of backup sets.

MICROSOFT SHAREPOINT SERVER iDATAAGENT CONFIGURABLE PROPERTIES

Once installed, the agent is configured and is therefore able to manage the data on the client computer. However, you can change certain aspects of the backup set configuration to manage the data in the manner that best suits your needs.

You can view or change the backup set configuration from the Backup Set Properties dialog box. The following information can be configured for all File Systems:

BACKUP SET/ARCHIVE SET NAME

You can rename a backup set or archive set. For step-by-step instructions, see [Rename a Backup Set/Archive Set](#).

USER SECURITY

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.

For more information, see [User Administration and Security](#).

Subclients - SharePoint Server

Topics | How To | Related Topics

Overview

Configurable Properties

Things to Consider when Creating and Configuring SharePoint Subclients

OVERVIEW

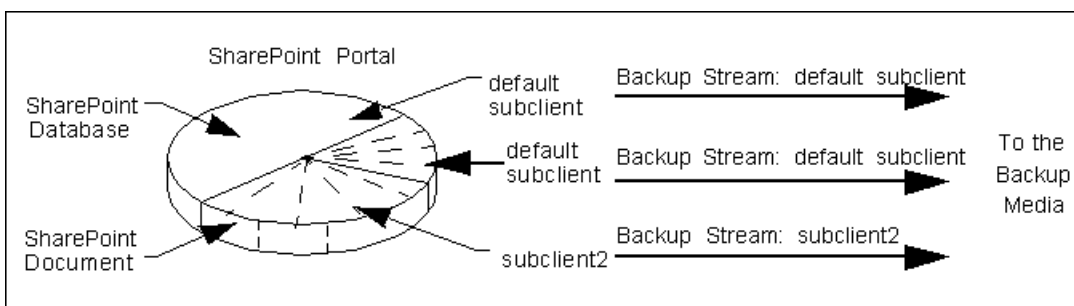
The following table shows subclient creation and configuration details specific to SharePoint Server iDataAgent.

	Type of Data	Default Subclient created during install of the Agent	Supports Default Subclient	Supports User Defined Subclient	Contents of the default subclient when user-defined subclient is present	Other Types of subclients supported by the Agent	Notes
SharePoint Database Backup Set	SharePoint databases	Yes	Yes	Yes	portion of database(s) not assigned to other subclients, unless otherwise configured*	Do Not Backup	None
SharePoint Document Backup Set	SharePoint documents	Yes	Yes	Yes	portion of documents not assigned to other subclients, unless otherwise configured*	None	*See Caution Against Re-configuring Default Subclient Content.

The following figure shows a simple subclient configuration for a SharePoint Server iDataAgent.

For the SharePoint Database backup sets, the default subclient, when backed up or restored, establishes a logical data channel through which data can travel to or from the backup media.

For the SharePoint Database backup sets, Subclient2 comprises of a user-defined set of data. The default subclient consists of all other data. Each subclient, when it is backed up or restored, establishes a logical data channel through which data can travel to or from the backup media.



For SharePoint Database backup sets, you can schedule the backups of the default subclient and subclient2 either at different times or simultaneously. Splitting the backups into two time periods can be useful if you need to perform backups on a large amount of data around a particularly busy time of network or client utilization.

CONFIGURABLE PROPERTIES

Once installed, the agent is configured and is therefore able to manage the data or volumes on the client computer. However, you can change certain aspects of the subclient configuration to manage the data in the manner that best suits your needs.

You can view or change the subclient configuration from the Subclient Properties dialog box. The following information can be configured.

ACTIVITY CONTROL

You can enable or disable all operations for this CommCell object and all objects below it. For more information, see Activity Control.

CONTENT/DATABASES

You can define the content of the subclient. Most agents include a configure button that displays a dialog where you can add or modify the data included as subclient content. For step-by-step instructions, see Configure Subclient Content.

DATA TRANSFER OPTIONS

Several configurable options to efficiently use available resources for transferring data secured by data protection operations are provided in the subclient. 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.

DATA ENCRYPTION

You can enable or disable the encryption of data for transmission over unsecure networks and for storage on media. For more information, see Data Encryption.

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 for the subclient including their priority. For additional information, see Configuring Alternate Data Paths for Subclients.

DATA PROTECTION FILTERS

You can perform the following functions:

- Define data protection filters to exclude specified subclient data from being backed up or archived. For more information, see Filters.
- Perform in-place editing of subclient data protection filter exclusions and exceptions. See Editing Filters for more information.

DIRECT DATABASE ACCESS

If selected, the backup operation will use an alternate read-only direct access to the SharePoint database to backup objects (e.g., documents, list items) and their metadata. This is applicable for Document backup sets. This feature is not supported for host-named site collections, WSS version 2.0, and SharePoint Server 2003.

When selected or deselected, the next backup that is run will be a Full backup. Requires installing specifically Microsoft SQL Server Native Client 2005/2008/2008 R2 Native Client (depending on SQL Server version) on Front-End Web Server - see <http://technet.microsoft.com/en-us/library/ms131321.aspx> for more information. For step-by-step instructions, see Use Direct Database Access.

PRE/POST PROCESSES

You can add, modify or view Pre/Post processes for the subclient. These are batch files or shell scripts that you can run before or after certain job phases. For more information, see Pre/Post Processes.

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.

See SharePoint Agents in **User Accounts and Passwords** for more information on this account.

STORAGE POLICIES

You can associate the subclient to a storage policy. For more information, see Storage Policies.

SUBCLIENT NAME

You can rename a subclient. For step-by-step instructions, see Rename a Subclient.

USER ACCOUNTS

You can define an account with permissions to execute Pre/Post commands for the agent's archive, backup, or volume creation jobs.

See SharePoint Agents: Other User Accounts in **User Accounts and Passwords** for more information.

USE DIRECT ACCESS TO RESTORE SELECTED ENTITIES

If selected for a backup, the restore operation will be able to restore individual documents into the database directly. This is applicable for documents of a Document backup set. For version-enabled libraries, the document will be restored as the same version when restored at an item level. When restoring the files directly into the database, the IDs of the files will remain the same and will not change. This is supported for traditional backups and for backups with **Use Direct Database Access** option enabled. For step-by-step instructions, see Use Direct Access to Restore Selected Entities.

USER SECURITY

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.

For more information, see User Administration and Security.

The Security tab is not available for the SharePoint Server iDataAgent.

THINGS TO CONSIDER WHEN CREATING AND CONFIGURING SHAREPOINT SUBCLIENTS

When creating and configuring subclients for SharePoint Server iDataAgents, keep in mind the following considerations:

- For SharePoint Database backup sets after the Application Upgrade of SharePoint Server, all content will be auto-discovered into the default subclient. Backup for other subclients may fail because they have no content. It is recommended to perform a manual discovery and assign content to proper subclients after the Application Upgrade of SharePoint Server.

- **Caution Against 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 "catch-all" entity for client data. As a result, the likelihood that some data will not get backed up or scanned for archiving would increase.

- **Subclient Content when Different Versions of SharePoint Servers Co-exist**

For SharePoint Database backup sets:

Create an additional Database type backup set to backup SharePoint Database components for other version.

For SharePoint Document backup sets:

- The subclient content should pertain to only one version. For example, the content of a subclient cannot specify both 2003 virtual servers and 2007 virtual servers.
 - If the default subclient has "ALL Folders" as content, it will only backup/archive the virtual server that appears first in the list.
- For SharePoint Server 2010, ensure that all service applications and the corresponding proxy applications are included in the same subclient.

[Back to Top](#)

Subclients - SharePoint Server - How To

[Topics](#) | [How To](#) | [Related Topics](#)

[Add/Edit a Data Protection Filter for a Subclient \(SharePoint Document\)](#)

[Assign Data Types to Another Subclient \(SharePoint Database\)](#)

[Associate a Subclient to a Storage Policy](#)

[Associate or Disassociate a User Group to a CommCell Object \(SharePoint Document\)](#)

[Change Account for Executing Pre/Post Commands \(Data Protection\)](#)

[Configure a Subclient for Pre/Post Processing of Data Protection Operations](#)

[Configure Subclient Content](#)

[Configure the Subclient for Data Encryption](#)

[Create a New Subclient](#)

[Delete a Data Protection Filter from a Subclient \(SharePoint Document\)](#)

[Delete a User-Defined Subclient](#)

[Discover and Assign New Data Types \(SharePoint Database\)](#)

Enable or Disable Operations

Enable Software Compression for a Subclient

Remove a Process from Pre/Post Processing of Data Protection Operations

Rename a Subclient

Use Direct Database Access

Set the Network Bandwidth and Network Agents for a Data Protection Operation

Use Direct Access to Restore Selected Entities

View Data Paths Associated with a Subclient

View Subclient Content

ADD/EDIT A DATA PROTECTION FILTER FOR A SUBCLIENT

Before You Begin

- Review Filters.
- Do not change the data protection or discovery filter of a subclient that has a data protection operation in progress.
- The system does not allow you to add entries that are not content of a particular subclient to that subclient's filter.
- For BlueArc and EMC Celerra (running at least DART OS 5.6.x) subclients, the filter string with or without wildcards must match the name or path of the file or directory being filtered.
- For NetApp subclients only name type filters (with wildcards) are supported:
 - You cannot enter paths as a filter (e.g. /vol/vol0/data1). Since NetApp does not support the use of paths in filters, if there are multiple files with the same name, even though they may be in different directories, all of them will be excluded from backups.
 - Name of the file or directory must exactly match the filter string.
 - You can specify a maximum of 32 strings in the exclude list.

Select the desired procedure:

- To add a data protection or discovery filter for a subclient
- To edit a data protection filter for a subclient

Required Capability: Capabilities and Permitted Actions

 To add a data protection or discovery filter entry for a subclient:

1. From the CommCell Browser, right-click the subclient whose data protection or discovery filter you want to add, and then click **Properties** from the shortcut menu.
2. Click the Filters tab of the Subclient Properties dialog box.
3. For Exchange Mailbox, Exchange Mailbox/Public Folder Archiver Agents and Exchange Compliance Archiver, to specify a mailbox or folder that you want to exclude from data protection operations:
 - Click the upper **Add** button.
 - From the Browse window, expand the mailbox tree of the client computer.
 - Click the mailbox or folder that you want to exclude from the backup/archive operations on the selected subclient, and then click **Add**. (Repeat this step for each additional entry.)
 - From the Browse window, click **OK**.

The mailboxes or folders that you selected appear as entries in the upper pane. Repeat this step if you want to add more mailboxes and/or folders to the filter.
4. For NAS NDMP iDataAgents, click the **Add** button and, in the input window, type the name of the file, directory, (or path for BlueArc) that you want to exclude from the backups and click **OK**. The name displays as an entry in the **Exclude these files/folders/patterns** pane. Repeat this step if you want to add more files, directories, or paths to the filter.
5. For SharePoint Server iDataAgents, to specify a URL/file/folder/pattern that you want to exclude from data protection operations or to specify an exception filter for database backup sets, do one of the following:
 - Click the **Add** button next to **Exclude these files/folder/patterns**: input window and type the URLs of site collections that you want to exclude from the backups and click **OK**. The site collection displays as an entry in the **Exclude these files/folders/patterns** pane. Wildcards are supported. See [Wildcards](#) for more information. Repeat this step if you want to add more URLs, files, directories, or paths to the filter.
 - Click the **Add** button next to **Except for these files/folders**: input window and type the URLs/folders of site collections that you want to be exceptions for the exclusion filter and click **OK**. These exceptions will be included in the data protection operations. Wildcards are not supported for

exception filters.

6. For Exchange Public Folder iDataAgents and SharePoint Server iDataAgent, to specify a workspace/folder that you want to exclude from the backups, click the upper **Browse** button and expand the iDataAgent of the client computer. Click the workspace/folder that you want to exclude from the backups and then click **Add**. Repeat this step for each additional entry.
7. For Windows/Unix/Macintosh File System iDataAgents, File Archiver for Windows/Unix Agents, and ProxyHost iDataAgent, to specify a file/folder/directory that you want to exclude from data protection operations, do one of the following:
 - Click the upper **Add** button and, in the **Enter Path** window, type the complete path (including drive letter) of the file/folder/directory that you want to exclude from the backups/archive operations. Repeat this step if you want to add more files/folders/directories to the filter.
 - Click the upper **Browse** button and expand the file system of the client computer. Click the file/folder/directory that you want to exclude from backups/archive operations and then click **Add**. Repeat this step for each additional entry.
8. For NetWare File System/NDS iDataAgents, to specify data that you want excluded from the backups, do one of the following:
 - To manually enter the path:
 - Click the **Add** button.
 - In the Input window, type the complete path (e.g., VOL1:\demo\disk2) of the data that you want to exclude.
 - Click **OK**. (The path that you typed displays as an entry in the upper pane.) Repeat this step if you want to exclude more data.
 - To browse and select a path:
 - Click the **Browse** button.
 - From the Backup Data window, expand the file system or NDS tree of the NetWare server.
 - Select the data that you want to exclude, and then click **Add**. Repeat this step for each additional entry.
 - From the Backup Data window, click **OK**. The data that you selected displays as entries in the upper pane.
9. For Lotus Notes Database and Lotus Notes Document iDataAgents, to specify a file or folder that you want to exclude from discovery, do one of the following:
 - Select the **Pattern/path to be excluded** field. Then type in a file or folder that you want to exclude. The format of the entry should start with a slash (\). The path entered is always relative to the data path of the partition. Then click **Add**. Repeat this step for each additional entry.
 - Click the upper **Browse** button and expand the file system of the client computer. Click the file or folder that you want to exclude from the backups and then click **Add**. Repeat this step for each additional entry.
10. For Exchange Mailbox, Exchange Mailbox/Public Folder Archiver Agents and Exchange Compliance Archiver, to specify a wildcard pattern of the folders that you want to exclude across all mailboxes within the subclient:
 - Click the lower **Add** button.
 - In the Input window, type the wildcard pattern of the folders that you want to exclude from backup/archive operations on the selected subclient.
 - Click **OK**. The path that you typed appears as an entry in the lower pane. Repeat this step if you want to add more entries to the filter.
11. For Exchange Public Folder iDataAgents and SharePoint Server iDataAgent, to specify an exception to an excluded workspace/folder (i.e., a folder/document that you want included in the backups, but whose parent directory has been excluded), click the lower **Browse** button and expand the iDataAgent of the client computer. Click the workspace/folder that you want to include in the backups and then click **Add**. Repeat this step for each additional entry.
12. For Windows/Unix/Macintosh File System iDataAgents, File Archiver for Windows/Unix Agents, and ProxyHost iDataAgent, to specify an exception to an excluded folder/directory (i.e., a file or folder/directory that you want included in the data protection operations, but whose parent folder/directory has been excluded), do one of the following:
 - Click the lower **Add** button and, in the **Enter Path** window, type the complete path (including drive letter) of the file/folder/directory that you want to include in the backups/archive operations. Repeat this step if you want to add more exceptions to the filter.
 - Click the lower **Browse** button and expand the file system of the client computer. Click the file/folder/directory that you want to include in the backups/archive operations and then click **Add**. Repeat this step for each additional entry.
13. For NetWare File System/NDS iDataAgents, to specify an exception to an excluded directory or NDS container (i.e., data that you want included in the backups, but whose parent directory or NDS container has been excluded), do one of the following:
 - To manually enter the path:
 - Click the **Add** button.
 - In the Input window, type the complete path (e.g., VOL1:\demo\disk2\readme) of the data that you want to include.
 - Click **OK**.
 - To browse and select a path:
 - Click the **Browse** button.
 - From the Backup Data window, expand the file system or NDS tree of the NetWare server.
 - Click the file or folder that you want to include in the backups and then click **Add**. Repeat this step for each additional entry.
 - Click **OK**. The selected data displays as entries in the lower pane.

- Click **OK** to save your changes.

Required Capability: Capabilities and Permitted Actions

▶ To edit a data protection filter entry for a subclient:

- From the CommCell Browser, right-click the subclient whose data protection filter you want to edit, and then click **Properties** from the shortcut menu.
- Click the Filters tab of the Subclient Properties dialog box.
- Click the filter entry that you want to edit, and then click the **Edit** button associated with that pane.
- Type the changes into the **Enter Path** dialog box, then click **OK**.
- Click **OK** to save your changes.

NOTES

- When you change a data protection or discovery filter, the change is effective the next time a data protection operation is run on the applicable subclient.
- Performing a full backup after changing filters or exceptions is recommended.

ASSIGN DATA TYPES TO ANOTHER SUBCLIENT

All unconfigured data types are assigned to the default subclient at backup time (if no other subclients are present or new items are present). However, you can reassign any item to any other subclient. Once assigned, the item becomes part of the content of that subclient.

Before You Begin

- Do not reassign content to another subclient while either subclient is being backed up.

Required Capability: See Capabilities and Permitted Actions

▶ To assign items to another subclient:

- From the CommCell Browser, right-click the iDataAgent to which you want to assign data types, click **All Tasks** and then click **Configure**. Alternatively, you can perform this using the **Configure** button on the Subclient Properties (Content) tab.
- From the Add/Modify Subclients dialog box, click the **Subclient** field of each item that you want to assign and select the desired subclient from the list. Alternatively, you can select and assign a range of items using the **Change all selected data types to list**.

Regardless of the assignment method, your choices always include:

- The default subclient
 - Any user-defined subclients
- To save the configuration, click **OK**.

ASSOCIATE A SUBCLIENT TO A STORAGE POLICY

Required Capability: See Capabilities and Permitted Actions

▶ To associate a subclient to a storage policy:

- From the CommCell Browser, right-click the subclient whose associated storage policy you want to change, then click **Properties** from the shortcut menu.
- Click the Storage Device tab of the Subclient Properties dialog box.
- From the **Storage Policy** list of the **Data Storage Policy** tab, select a data storage policy to associate with this subclient. If necessary, click the **Create Storage Policy** button to create a new storage policy to which the subclient can then be associated.
- From the Changing a Storage Policy window select the next type of backup operation. Click **OK**.
- If applicable for your agent, you can change the number of data streams from the **Number of Data/Database Backup Streams** field.
- If applicable for your agent, click the **Log Storage Policy** tab and select a storage policy to associate with this transaction log subclient from the **Transaction Log Storage Policy** list. Also, you can set the **Number of Transaction Log Backup Streams** from this tab.
- Click **OK** to save your changes and close the Subclient Properties Storage Device tab.

ASSOCIATE OR DISASSOCIATE A USER GROUP TO A COMMCELL OBJECT

Required Capability: See Capabilities and Permitted Actions

► To associate or disassociate a user group to a CommCell entity:

1. From the CommCell Browser, click the CommServe, client computer group, client computer, agent, MediaAgent, Library, Storage Policy, backup set, subclient, or Shelf media, and then select **Properties**.
2. From the **Security** tab, 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.
3. Click **OK**.

CHANGE ACCOUNT FOR EXECUTING PRE/POST COMMANDS (DATA PROTECTION)

Required Capability: See Capabilities and Permitted Actions

► To change a user account for executing pre/post commands for Data Protection jobs:

1. From the CommCell Browser, expand the tree to view the appropriate level icon for the affected agent.
 - From the agent, instance/partition, or backup set/archive set level, right-click the appropriate icon, click **All Tasks**, and click **New Subclient** from the short-cut menu.
 - From the subclient level, right-click the subclient icon and click **Properties** from the short-cut menu.
2. From the Subclient Properties dialog box, create and/or configure the subclient as appropriate. Then click the **Pre/Post Process** tab.
3. From the **Pre/Post Process** tab, click **Change**.
4. From the User Account dialog box, select one of the account options. If you select **Impersonate User**, type the appropriate user name and password.
5. Click **OK** to save the settings.

CONFIGURE A SUBCLIENT FOR PRE/POST PROCESSING OF DATA PROTECTION/ARCHIVE OPERATIONS

Before You Begin

- We recommend not configuring a pre/post process for a subclient that is currently running a data protection or archive operation.
- Verify that there are no pre/post processes already assigned for the subclient.
- Review the Overview and Agent-Specific Guidelines for your agent before configuring pre/post processes for data protection/archive operations.
- Pre-process commands for the iDataAgents will be executed only when the necessary resources (e.g., media, library, drive, etc.) are available.

Required Capability: Capabilities and Permitted Actions

► To configure a subclient for Pre/Post processing of data protection/archive operations:

1. From the CommCell Browser, right-click the subclient for which you want to configure a pre/post process, and then click **Properties** from the shortcut menu.
2. Click the Pre/Post Process tab of the Properties dialog box.
3. For an agent other than the Oracle RAC iDataAgent, click inside the space that corresponds to one of the following phases and type the full path of the process that you want executed during that phase. Alternatively, click **Browse** to locate the process (applicable only for paths that do not contain any spaces). For the Oracle RAC iDataAgent, click **Browse** for the corresponding process, click the name of the control node client in the Select Client for Browse dialog box, and click **OK**. Then browse for and click the process.
 - PreBackup
 - PreScan
 - PreArchive
 - PreCopy
 - PreSnap
 - PostBackup
 - PostScan
 - PostArchive
 - PostCopy
 - PostSnap

Click **OK**.
4. If you want to run a Post Process for all attempts to run that job phase, then select the corresponding checkbox.
5. For subclients on Windows platforms, if **Run As** displays **Not Selected**, or if you want to change the account that has permission to run these commands,

click **Change**.

- a. In the User Account dialog box, select **Use Local System Account**, or select **Impersonate User** and enter a user name and password. Click **OK**.
 - b. If you selected Local System Account, click **OK** to the message advising you that commands using this account have rights to access all data on the client computer.
6. Click **OK** to save your changes and close the Pre/Post Process tab of the Properties dialog box.


CONFIGURE SUBCLIENT CONTENT

Before You Begin

- Review Subclients.
- Do not configure the content of a subclient while the parent node or any sibling subclient has a data protection or archive operation currently running on it.
- Exchange Mailbox iDataAgents and Exchange Mailbox/Public Folder Archiver Agents: If you change the contents of the default backup set or archive set then the auto-discover feature will be disabled. If you disable the auto-discovery feature, newly created mailboxes will not be backed up/archived unless they are manually discovered and assigned to a subclient.
- NAS NDMP iDataAgents: You must ensure there is no overlap in content between all subclients. Overlap in subclient content will result in loss of data. An existing subclient's contents are not automatically changed when another subclient is added with overlapping contents.
- SharePoint Server iDataAgent: The Site Content Database, the Site Collection Database, the Site Database, and the Site Index for the virtual server must all be assigned to the same subclient.
- Lotus Notes Document iDataAgent: Review Assigning Restore View Names to Newly-discovered Databases
- QR Agent: Follow these guidelines when adding a volume to a QR Agent subclient:
 - The volume must correspond to a physical disk or RAID array.
 - A volume created by volume management software other than VxVM is not valid subclient content.
 - Subclients may have overlapping content; however, if two or more subclients overlap, they all must use the same snapshot engine. If the QR policies associated with the subclients are configured to use different snap engines, they must be reconfigured to use the same snap engine in this scenario.
- **Caution Against 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 "catch-all" entity for client data. As a result, the likelihood that some data will not get backed up or scanned for archiving would increase.

Required Capability: See Capabilities and Permitted Actions

 To configure subclient content:

1. From the CommCell Browser, right-click the subclient for which you want to configure content, click **All Tasks** (if applicable) and then click **Properties**.
2. Follow the procedure below that is applicable for your agent:
 - For File System, Active Directory, File Archiver, Exchange Public Folder iDataAgents, NDS, and SharePoint Server iDataAgents click the Subclient Properties (Content) tab and configure content for the subclient as described below for your agent:
 - For File System, Active Directory, File Archiver, NDS, and SharePoint Server iDataAgents: Type the full path of the data that you want to include as subclient content in the **Enter New Content** field, then click **Add**. Optionally, click **Browse** to enter the content. When browsing content while configuring SharePoint subclients, you can add content via multiple selections with the CTRL or SHIFT keys. For Windows, when specifying a UNC Path, click **As User**, and enter the user account information for the domain user with permissions for that path. For NetWare/DNS, see the Notes section below for content path examples. For Unix File Systems, you can enter the mount point of an NFS-mounted file system, see the Notes section below for examples.
 - For Exchange Public Folder iDataAgents: Click **Browse**, select folders to include as content, then click **Add**.
 - For the Unix File System iDataAgents, to facilitate the management of resource fork data in Apple double-encoded Macintosh files, click **Enable Apple Double Support**.
 - For the Unix File System iDataAgents, to view the actual data path for any symbolic link in the subclient content, click **Expand symbolic links of subclient content** and then click **Discover**.
 - For NAS NDMP iDataAgents, configure the **Backup Content Path** field(s) as described below, then click **Add**:
 - 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.
 - Optionally, for NetApp NAS NDMP, click **Browse** to enter the content.
 - For Exchange Mailbox and Exchange Mailbox/Public Folder Archiver Agents follow the procedure to Discover and Assign New Mailboxes or Assign Mailboxes to Another Subclient.
 - For Lotus Notes Database and Document iDataAgents follow the procedure to Discover and Assign New Databases or Assign Databases to a Subclient.
 - For DB2, DB2 DPF, Exchange Database, Novell GroupWise, SharePoint Server, SQL Server Database, Sybase, and MySQL iDataAgents, click the Subclient Properties (Content) tab and configure content for the subclient as described below for your agent:
 - For the DB2 iDataAgent, specify whether you want to include the entire database or a subset of this data as content for the subclient. For the DB2 DPF iDataAgent, specify whether you want to include all the affected database partitions or a subset of this data as content for the subclient.
 - For Exchange and GroupWise iDataAgents: Click **Configure**. From the Add/Modify Subclients dialog box click the subclient entry for the database element/Storage Group that you want to add to the new subclient and select the name of the destination subclient from the list that appears. Alternatively, you can select and assign a range of databases/storage groups using the **Change all selected databases/storage groups to list**. Note that you must have at least one database element/Storage Group assigned to this subclient in order to save the configuration.

A database/Storage Group that is not configured for a subclient does not appear in the list. This can be the case if the subclient containing the database/Storage Group was deleted. If this happens, click **Discover** to display all databases/Storage Groups.
 - For the SharePoint Server iDataAgent, follow the procedure to Discover and Assign New Data Types.
 - For the Sybase iDataAgent, follow the procedure to Manually Discover Databases.
 - For the MySQL iDataAgent, follow the procedure to Configure MySQL Databases.
 - For the Informix iDataAgent, click the Subclient Properties (Content) tab and define the contents of the subclient. Specifically, establish the backup mode for the data to be backed up, set the backup level, and decide whether to back up the emergency boot file and/or the ONCONFIG file.
 - For the Oracle, SAP for Oracle, or Oracle RAC iDataAgent, click the Subclient Properties (Content) tab and define the contents of the subclient. To configure this subclient for specialized types of backups, follow the appropriate procedure below:
 - Create Subclient for Backing Up Archived Redo Log Files
 - Create Subclient for Backing Up Offline Databases
 - Create Subclient for Backing Up Online Databases
 - Create Subclient for Performing Selective Online Full Backups
 - For SAN iDataAgents, click the Subclient Properties (Content) tab and configure content for the subclient as described below for your agent:
 - Image Level on Unix iDataAgent: Click **Add**. From the Add Content Path dialog box, select the volume(s) that you want to back up (use CTRL + click to select multiple volumes). Click **OK**. The selected volumes are added to the **Contents of subclient** list. These volumes are automatically configured to be CXBF devices. Alternatively, use Volume Explorer per specific scenarios to configure CXBF devices.

To configure an unmounted block device or raw device as content, first use Volume Explorer to configure the device as a CXBF device. Then select the configured CXBF device as subclient content. You can ignore the warning that is displayed.

For more information, see When to Use Volume Explorer. For a step-by-step procedure, see Configure a CXBF Device in Volume Explorer.
 - Image Level and Image Level ProxyHost on Windows iDataAgents: Click **Add**. Then in the **Add Content** dialog box, type the full path of the volume or mount point that you want to include as subclient content, then click **Add**. Optionally, click **Browse** to select the content. Click **OK**. The volume or mount point is added to the **Contents of subclient** list. Add additional content by repeating this step.
 - ProxyHost iDataAgent: Select a backup host from the **Backup Host** list. This is the computer to which the BCV is connected. Click **Add**. In the **Content** field of the Add/Edit Content for Subclient dialog box, type the primary host path of the content that you want to back up, or click **Browse** to find and select this data. In the **Backup Host BCV Path** field of the Add/Edit Content for Subclient dialog box, type the path through which the backup host accesses this data on the BCV, or click **Browse** to find and select this path. Click **OK**. The primary host data path and corresponding backup host BCV path are added as a single entry in the **Contents of subclient** list. To add additional entries, repeat these steps. Refer to Notes below for more information.
 - For Quick Recovery Agents, click the Subclient Properties (Content) tab and configure the following options:
 - Click **Add Volume**. From the Adding Volume dialog box, select volume(s) that you want to add to the subclient content (use CTRL + click to select multiple volumes). You can add/edit additional advanced options for the selected volume by select **Advanced** on the Adding Volume dialog box. Click **OK**.
 - Click Add App to select an application and associated volumes. Click **OK**.

Any instances you intend to protect and recover with the QR Agent must be configured in the QR Agent properties Authentication tab. They will not appear in the Add App dialog box if they are not configured. Only volumes containing datafiles and archive log files will be detected by Add App. Volumes containing control files and redo log files will not be detected.

For a clustered Exchange Server, if you are *not* using VSS to perform an online quiesce, sufficient permissions are required in order to be able to perform an offline quiesce; in such cases, ensure that the **User Name** specified has Exchange Administrator rights.

See also Configure Subclients for Overlapping Content.

3. Click **OK** to save your content configuration.

NOTES

- Content examples for NetWare are **OU=prospects.O=engineering.[Root]**, (for NDS content), and **SYS:\public** (for File System content).
- Content examples for adding an NFS-mounted file system to subclient content of a Unix File System iDataAgent:
 - `/mountpointA` to include the entire file system at mountpointA
 - `/mountpointA/projects` for only the `projects` directory within the file system at mountpointA.
- Informix subclients include one or more dbspaces. As databases are added to the dbspaces, the subclients are updated automatically.
- Exchange Mailbox iDataAgents and Exchange Mailbox/Public Folder Archiver Agents: Initially, all unconfigured mailboxes are assigned to the default subclient. You can create a new subclient and reassign mailboxes to this new subclient (within the same backup set/archive set). Once assigned, the mailboxes become part of the content of the new subclient.
- SharePoint Server iDataAgent: Initially, all unconfigured data types are assigned to the default subclient. You can create a new subclient and reassign data types to this new subclient. Once assigned, they become part of the content of the new subclient.
- ProxyHost iDataAgent: The primary host data path is backed up by the subclient and is the path through which the backup host accesses this data on the BCV. A primary host path and its corresponding backup host path are listed in the following format:

<primary_host_path> --> <backup_host_path>

For example, assume that you want to back up the **D:\data** directory from your primary host and **D:** is mirrored by a BCV, which is mapped to the backup host as **F:**. Consequently, the path to this data on the backup host is **F:\data**. When you add this directory to a subclient, it is listed in the **Contents of subclient** pane as **D:\data --> F:\data**.

The primary host path in the **Content** field is used for browse and restore purposes. However, it is the data in the **Backup Host BCV Path** which is actually backed up. If these two paths do not accurately correspond, the path that appears when data is browsed for restore does not accurately reflect the data that will be restored. In the example given above, assume that **D:\data** is entered in the **Content** field, while **F:\data1** is accidentally entered in the **Backup Host BCV Path**. If you browse and select **D:\data** to be restored, it is actually **D:\data1** that is restored. (Remember, **F:\Data1** is the path on the backup host that corresponds to **D:\data1** on the primary host.)

CONFIGURE THE SUBCLIENT FOR DATA ENCRYPTION

Encryption settings made at the subclient level are for data protection and recovery operations run from the CommCell Console and are not related in any way to settings made at the instance level which is for third-party Command Line operations only.

See Data Encryption - Support for a list of supported products.

Before You Begin

- Encryption must be enabled at the client level prior to configuring any subclients residing on that client. See Configure the Client for Data Encryption.
- If you are attempting to configure for third-party Command Line operations, do not use this procedure. See Configure Third-party Command Line Operations for Encryption.

Required Capability: Capabilities and Permitted Actions

▶ To configure the subclient for data encryption:

1. From the CommCell Console, right-click the subclient and click **Properties**.
2. From the Subclient Properties (Encryption) tab, select an option based on the criteria described in the Encryption tab help.
3. Click **OK** to save your settings and close subclient properties.

CREATE A NEW SUBCLIENT**Before You Begin**

- Review Subclients.
- Do not create a subclient while the parent node or any sibling subclient has a data protection or archive operation currently running on it.
- In cases where a new subclient is created with the same name as a deleted subclient, the system will append a Unix time stamp to the deleted subclient's name in data protection job history reports and views to distinguish the two subclients. For example, `subclientname_1104257351`.
- Informix iDataAgents: If you will be using the Informix ONBAR utility to create backup and restore scripts, you need not create subclients. Otherwise, if you will be using the CommCell Console to back up and restore Informix database objects (subsets/dbspaces), then you will need to create a subclient.
- ProxyHost iDataAgents: If you are using a BCV, you must prepare a batch file or a shell script file on the backup host containing commands to synchronize and split the BCV. The Resource Pack includes information on configurations for these batch files or shell scripts, as well as examples that apply to specific applications and hardware (e.g., Exchange databases in an EMC Symmetrix environment). See Resource Pack for more information on the Resource Pack.

The ProxyHost iDataAgent also requires that you set permissions for the batch/shell script file on the backup host.

- SQL Server Database iDataAgents: When running on Windows Server 2003 and VSS is enabled, the **New Subclient** command is not available.
- PostgreSQL iDataAgents: Once you configure the PostgreSQL instance, the system automatically generates the default backup sets and default subclients. However, you can use the CommCell Console to create user-defined subclients for dump backup sets to distribute some of the database content. You cannot create user-defined subclients for FS backup sets.

Required Capability: See Capabilities and Permitted Actions

▶ To create a new subclient:

1. From the CommCell Browser, right-click the node (agent/backup set/archive set/instance) for which you want to create a new subclient, click **All Tasks** (if applicable), and then simply click **New Subclient** for most agents.
 - For the SQL Server iDataAgent, expand **New Subclient** and click either **Database** to include individual databases or **File/File Group** to include database elements.
2. Click the General tab or General (Quick Recovery Agent) tab of the Subclient Properties dialog box and type the name (up to 32 characters) of the subclient that you want to create.
 - For supported agents identified in Support Information - Snapshot Engines, you can select a QSnap option to snap data and then perform a data protection operation on the data.
 - For Image Level on Unix and Image Level ProxyHost on Unix, use the **Incremental Support Using** field to configure either a CXBF subclient or a checksum subclient and to enable incremental support for either subclient type.
 - For QR Agents, you must also select a QR Policy from the **QR Policy** list.
 - For the Windows iDataAgents that support VSS, you can optionally Enable VSS on a Subclient.
3. Select other options from the General tab as appropriate for the agent.
4. Click the **Content** or **Databases** tab of the Subclient Properties dialog box and Configure Subclient Content as appropriate for your agent.
5. For all agents (except QR), click the Storage Device (Data Storage Policy) tab of the Subclient Properties dialog box, then select a data storage policy to associate with this subclient from the storage policy list.
 - For the DB2 and DB2 DPF iDataAgents, you can also change the number of data backup streams. For the DB2 DPF iDataAgent, the default stream threshold should be equal to the total number of database partitions for the subclient.
 - For SQL Server iDataAgents, you can also click the Storage Device (Log Storage Policy) tab of the Subclient Properties dialog box, then select a log storage policy to associate with this subclient from the storage policy list and select the number of backup streams for transaction log backup jobs.
 - For 1-Touch for Unix, it is strongly recommended that the storage policy that you select for the subclient configured for 1-Touch use a MediaAgent on a different computer. If you do this, and if the system crashes, the media will not have to be exported to another MediaAgent in order to recover the system.
6. For Oracle and DB2 iDataAgents, click the Backup Arguments (Oracle) or Backup Arguments (DB2, DB2 DPF) tab of the Subclient Properties dialog box and Configure Backup Arguments as appropriate for your agent. Note that the backup arguments for Informix are located on the Content tab.
7. For Migration Archiver Agents, click the **Archiving Rules** or **Rules** tab of the Subclient Properties dialog box and configure archiving rules as appropriate for your agent. In order to perform rules-based migration archiving operations, the **Disable All Rules** checkbox must be cleared.

If the File Archiver for Windows supports Data Classification, several filter-like configuration fields are defined as archiving rules and are available from the Subclient Properties (Rules) tab. If you want to define content and archiving rules based on file attributes other than volumes, size, and modified time (i.e., if you want to customize your rules), click the Advanced tab and configure as appropriate. Also, stub management options can be configured from the Stub Rule tab. See Configure Archiving Rules - File Archiver Agents for step-by-step instructions.
8. For ProxyHost and Image Level ProxyHost iDataAgents, click the Pre/Post Process tab of the Subclient Properties dialog box. In the **PreScan** field, type the path to the batch file/shell script file that contains those commands that are to run before each backup of the subclient, or click **Browse** to locate and select this file. For ProxyHost and Image Level ProxyHost, the file must reside on the backup host or primary host.
9. Optionally (if supported for your agent) you can:
 - Add a Data Protection or Discovery Filter for a Subclient on the Filters tab.
 - Configure a Subclient for Pre/Post Processing of Data Protection/Archive Operations on the Pre/Post Process tab.
 - Enable Software Compression for a Subclient on the Software Compression tab of the **Storage Device** tab.
 - Configure the Subclient for Data Encryption on the Encryption tab.
 - Enable or Disable Operations for this subclient on the Activity Control tab.
 - Configure Mailbox Stores for Auto-Discovery on the Auto-discovery tab.
 - Configure the Subclient for 1-Touch on the 1-Touch Recovery tab.
 - View or change the user group security associations for this subclient from the Security tab.
 - Determine location from where archive logs will be backed up or deleted from the Log Destinations tab.
10. Click **OK** to save the subclient configuration. For QR Agents, this procedure is now complete. For all other agents, continue on to the next step.
11. The Backup Schedule dialog box advises you to schedule data protection operations for your new subclient. It is recommended you elect to set a schedule now. You can also associate this subclient with an All Agent Types schedule policy (which is automatically created by the system, or can be a user defined

Data Protection schedule policy). If you have already associated a schedule policy at a previous level (Backup Set/Instance, Agent, Client, or Client Computer Group) the schedules defined in the Schedule Policy will be automatically applied to the new subclient. See Schedule Policy for more information.

- If you want to associate this subclient with an All Agent Types schedule policy, click **Associate with Generic Schedule Policy**, and then select that schedule policy from the drop-down list box. Click **OK**.
- If you want to associate this subclient with a specific schedule policy, click **Associate to schedule policy**, and then select the schedule policy from the drop-down list box. Click **OK**.
- If you have selected to define a schedule for this subclient:
 - Click **Schedule**.
 - From the Backup/Archive Options dialog box, select the type of data protection operation that you want to schedule.
 - If you want to set Advanced Backup/Archive Options, click **Advanced**.
 - After selecting the data protection type and any advanced options, click **OK**. The **Schedule Details** dialog box appears.
 - From the Schedule Details tab, select the scheduling options that you want to apply, then click **OK**.
- If you don't want to create a data protection schedule at this time, click **Do Not Schedule**, and then click **OK**.

This task is now complete.

DELETE A DATA PROTECTION FILTER FROM A SUBCLIENT

Before You Begin

- Review Filters.
- Do not change the data protection or discovery filter of a subclient that has a data protection operation in progress.
- File Archiver for Windows/Unix Agents: We recommend that you don't delete the following entries from the exclusion filter, as it could cause your file system to be inoperable. For Windows, these include: *.dll, *.bat, *.exe, *.cur, *.ico, *.lnk. For Unix, these include *.a, *.ksh, *.csh, *.sh, *.lib, *.so.

Required Capability: Capabilities and Permitted Actions

▶ To delete a data protection or discovery filter entry from a subclient:

1. From the CommCell Browser, right-click the subclient whose data protection or discovery filter you want to delete, and then click **Properties** from the shortcut menu.
2. Click the Filters tab of the Subclient Properties dialog box.
3. To delete an entry from the Exclusions list, click the entry in the upper pane then click the upper **Delete** button. (Repeat this step for each entry that you want to delete.)
4. To delete an entry from the Exceptions list (if applicable for your agent), click the entry in the lower pane then click the lower **Delete** button. (Repeat this step for each entry that you want to delete.)
5. Click **OK** to save your changes.

NOTES

- Whenever you delete an entry from the exclusion filter, check if the exceptions list (i.e., lower pane) contains any entries that are children of the deleted data (if applicable for your agent). If so, you should delete them as described in Step 4 since they no longer need to be listed. The system automatically deletes any exceptions that are children of a deleted exclusion unless you used wildcard expressions in the exclusion path.
- When you change a data protection or discovery filter, the change is effective the next time the subclient is backed up/archived.
- Data will not be backed up in a differential backup for a subclient after a filter was removed.
- Since Incremental backups only back up data that has been modified since the last backup, previously filtered files whose filters are now removed, will not be backed up unless they have been modified since that last backup. To back up previously filtered files that have not been modified but whose filters have been removed since the last backup, you need to run a Full backup.
- Performing a full backup after changing filters or exceptions is recommended.

DELETE A USER-DEFINED SUBCLIENT

Related Topics:

- Command Line Interface - qdelete subclient
- Subclients

Required Capability: See Capabilities and Permitted Actions

▶ To delete a user-defined subclient:

1. From the CommCell Browser, right-click the user-defined subclient that you want to delete, and then click **Delete** from the shortcut menu.
2. 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. If you click **Yes**:
 - o the subclient, and any data that may have been protected/archived by the subclient are logically deleted, and you can no longer access the corresponding data for recovery/retrieve purposes. However, the data remains valid for the length of time specified by the associated retention period. Some agents allow you to browse data from a deleted subclient provided that the Browse Data Before date and time precedes the time that the user-defined subclient was deleted.
 - o for agents that support a default subclient, once the user-defined subclient is deleted its contents are automatically reallocated to the default subclient the next time a data protection/archive/discovery operation is run on the default subclient to ensure data protection coverage.
 - o the system deletes the selected subclient node and removes it from the CommCell Browser.
 - o the system deletes any data protection/archive and recovery/retrieve job schedules that are associated with the subclient.

DISCOVER AND ASSIGN NEW DATA TYPES

Over time, new items are created to accommodate new data. By default, a subclient performs a discovery process at the beginning of each backup. The auto discovery process detects any new data types and automatically assigns them to the default subclient.

While this feature ensures that all the new data types will be automatically backed up as part of the default subclient, you may want to assign the new data types to specific subclients. To do this, you can conduct the discovery process and assign the data types yourself.

Required Capability: See Capabilities and Permitted Actions

▶ To discover and assign new data types:

1. From the CommCell Browser, right-click the iDataAgent for which you want to discover new data types, click **All Tasks** and then click **Configure**. Alternatively, you can perform this using the **Configure** button on the Subclient Properties (Content) tab.
2. From the Add/Modify Subclients dialog box, click the **Discover** button.
3. When the discovery process completes, the Add/Modify Subclients dialog box is redisplayed. The dialog box displays the data types that have already been assigned plus any newly discovered data types that have not been assigned. The unassigned data types are those that have no entry in the Subclient column.
4. To assign these data types, click the Subclient field of each data type that you want to assign and select the desired subclient from the list. Alternatively, you can select and assign a range of data types to a single subclient using the **Change all selected data types to** list.

Regardless of the assignment method, your choices always include:

- o The default subclient
 - o Any user-defined subclients
 - o The Do Not Backup subclient
5. To register your data type assignments with the system, click **Apply**.
 6. If you have no other data types to assign, click **OK**.

ENABLE OR DISABLE OPERATIONS

Required Capability: See Capabilities and Permitted Actions

Level	Capability
CommCell	Administrative Management with CommCell level association
Client Computer Group	Administrative Management with Client Computer Group level association
Client	Agent Management with Client level association
Agent	Agent Management with Agent level association
Subclient	Agent Management with Subclient level association

▶ To enable or disable activity control at the CommCell, client computer group, client, agent, or subclient levels:

1. From the CommCell Browser, right-click the CommServe, client computer group, client computer, agent, or subclient, and then click **Properties** from the short-cut menu.
2. From the Activity Control tab of the associated Properties dialog box, select or clear option(s), as desired.
3. Click **OK**.

Disabled data management and/or data recovery operations are displayed with client and/or agent icon changes in the CommCell Browser. For a comprehensive list of all icons in the CommCell Console, see CommCell Console Icons.



ENABLE OR DISABLE SOFTWARE COMPRESSION FOR A SUBCLIENT

Before you Begin

- Do not enable/disable software compression for a subclient that is being backed up/archived.

Required Capability: Capabilities and Permitted Actions

▶ To enable software compression for a subclient:

- From the CommCell Browser, right-click the subclient for which you wish to enable software compression and then click **Properties**.
- Click the **Storage Device** tab and from the Data Storage Policy tab, select the storage policy from the **Storage Policy** list.
If applicable for the selected agent, click the Log Storage Policy tab and select a storage policy from the **Transaction Log Storage Policy** list.
- Then click the Storage Device (Data Transfer Option) tab and choose the appropriate compression option for this subclient.
- Click **OK** to save your changes.

This task is now complete.

REMOVE A PROCESS FROM PRE/POST PROCESSING OF DATA PROTECTION/ARCHIVE OPERATIONS

Before You Begin

- We recommend not removing a pre/post process for a subclient that is currently running a data protection or archive operation.
- Review the Overview and Agent-Specific Guidelines for your agent before removing pre/post processes for data protection/archive operations.

Required Capability: Capabilities and Permitted Actions

▶ To remove a process from Pre/Post processing of data protection/archive operations:

- From the CommCell Browser, right-click the subclient for which you want to remove a pre/post process, and then click **Properties** from the shortcut menu.
 - Click the Pre/Post Process tab of the Subclient Properties dialog box.
 - Click the text inside the space that corresponds to one of the following phases for which you want a pre/post process removed, then press the **Delete** key:
 - PreScan
 - PreArchive
 - PreCopy
 - PreSnap
 - PostBackup
 - PostScan
 - PostArchive
 - PostCopy
 - PostSnap
 - Repeat Step 3 for any additional processes that you want to remove.
 - Click **OK**.
-

RENAME A SUBCLIENT

Before You Begin

- You can rename a subclient at any time. However, we recommend that you don't rename a subclient while a data protection or archive operation is running on that subclient.
- In cases where a subclient is renamed using the same name as a deleted subclient, the system will append a Unix time stamp to the deleted subclient's name in data protection job history reports and views to distinguish the two subclients. For example, `subclientname_1104257351`.

Required Capability: See Capabilities and Permitted Actions

▶ To rename a subclient:

1. From the CommCell Browser, right-click the subclient that you want to rename, and then click **Properties** from the shortcut menu.
2. From the Subclient Properties (General) tab, or the QR Agent Subclient Properties (General) tab, type the new name in the **Subclient Name** field, and then click **OK**.

The CommCell Browser updates the subclient with its new name. The new name will also be reflected in any associated schedules and reports.

USE DIRECT DATABASE ACCESS

Before You Begin

- See Direct Database Access for the purpose of using this option.

Required Capability: See Capabilities and Permitted Actions

▶ To use an alternate method to back up data for this subclient:

1. From the CommCell Browser, right-click the subclient that you want to backup with the alternate method, and then click **Properties** from the shortcut menu.
2. From the Subclient Properties (General) tab, select **Use direct database access**, and then click **OK**.

When selected or deselected, the next backup that is run will be a Full backup.

SET THE NETWORK BANDWIDTH AND NETWORK AGENTS FOR A DATA PROTECTION OPERATION

Before you Begin

- Do not modify the network bandwidth and network agents for a subclient or instance that is being backed up.

Required Capability: Capabilities and Permitted Actions

▶ To Set the Network Bandwidth and Network Agents for a Data Protection Operation:

1. From the CommCell Browser, right-click a subclient and then click **Properties**.
For the DB2, DB2 DPF, Informix, Oracle, Oracle RAC, SAP, or Sybase iDataAgent, right-click an instance and then click **Properties**.
2. Click the **Storage Device** Data Transfer Option tab.
For the QR Agent:
 - To control network bandwidth settings, use the Throttle Network Bandwidth section in the General tab of the Subclient Properties dialog box.
 - To control the number of network agents, you must create a `nQRNetworkAgents` registry key.
3. Enter a number of **Network Agents** that must be used to perform data protection operations on the subclient/instance.
4. Click the **Throttle Network Bandwidth (MB/HR)** option and then enter the throughput as needed. Note that throttling is done on a per Network Agent basis.
5. Click **OK** to save the changes.

This task is now complete.

VIEW DATA PATHS ASSOCIATED WITH A SUBCLIENT

Required Capability: See Capabilities and Permitted Actions

▶ To view data paths:

1. From the CommCell Browser, right-click the subclient whose data paths you want to view, then click **Properties** from the shortcut menu.
 2. Click the Storage Device tab of the Subclient Properties dialog box.
 3. From the **Data [or Logs] Storage Policy** tab, click **Show Data Paths** to view the data paths used by the subclient to access the storage media for data protection operations. Click **Close** to exit the Data Paths dialog box.
 4. Click **OK** to exit the Subclient Properties Storage Device tab.
-

USE DIRECT ACCESS TO RESTORE SELECTED ENTITIES

Before You Begin

- See Use Direct Access to Restore Selected Entities for the purpose of using this option.

Required Capability: See Capabilities and Permitted Actions

▶ To restore individual files into the database directly:

1. From the CommCell Browser, right-click the subclient that you want to backup with the alternate method, and then click **Properties** from the shortcut menu.
 2. From the Subclient Properties (General) tab, select **Use direct access to restore selected entities**, and then click **OK**.
-

VIEW SUBCLIENT CONTENT

Required Capability: See Capabilities and Permitted Actions

▶ To view content of a subclient:

1. From the CommCell Browser, right-click the subclient whose content you want to view, then click **Properties**.
 2. From the Subclient Properties dialog box, click the **Content** tab (or **Databases** tab for Lotus Notes) to view the contents of the subclient.
 3. Click **OK** to close the dialog box.
-

[Back To Top](#)

Backup Job History

Topics | How To | Related Topics

Overview

Items That Were Backed Up

Items That Failed

Pruning Backup History Information

Supported Features

Content Indexing History Information

OVERVIEW

You can view the backup and restore history of *iDataAgents*, *BackupSets/Instances*, and subclients.

The **Backup Job History Filter** dialog box allows you view detailed, historical information about backup jobs. Once you have chosen your filter options, they are displayed in the **Backup Job History** window.

For information on Job Details displayed in the Job History, see [Viewing Job Information](#).

From this window, you can right-click a backup job to:

- Browse the data backed up by the backup set or instance from the **Backup Job History** window. This is provided as right-click option for each job. (This menu option, when selected, initiates the **Browse Options** dialog box preset with the values needed to browse the data.)
 - Browse the snapshots created during SnapProtect backup
 - View items that failed during the backup job
 - View details of the backup job
 - View files that were not indexed during a backup job that performed content indexing
 - View associated media
 - View events of the backup job
 - View a list of items that were backed up
 - View a list of items that were moved to media for a SnapProtect backup job
 - View the log files of the backup job.
 - View the RMAN log of an Oracle backup job.
 - View the BRTools log of a SAP for Oracle job. You can view the BRTools log for only those jobs that were initiated from the CommCell Console.
-

ITEMS THAT WERE BACKED UP

The **View backup file list** option allows you to view a list of the files that were backed up during a backup job, along with the data sizes of each backed up file. The **View backed up messages** option allows you to view a list of messages that were backed up by using, along with the alias name, display name, email address, sender name, and recipient of each message.

From these windows you can conduct searches based on a particular string, allowing to find particular files quickly and easily.



It is not recommended that this option is used to view a very large list of items that were backed up (such as lists that total over 100,000 items). It is suggested that the Browse option is used to find a list of backed up items in such cases.

See [View the Items That Were Protected During a Data Protection Operation](#) for step-by-step instructions.

ITEMS THAT FAILED

The items that failed for a data protection operation include individual files that may fail the job even though a particular job completed successfully. You can determine the degree of success for these jobs using this window.

Filters can be used in conjunction with the "Items That Failed" list on the data protection Job History Report to eliminate backup or archive failures by excluding items which consistently fail 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.



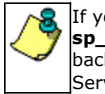
A listing of files and folders that failed is not available for the Quick Recovery Agent, or the Image Level and Image Level ProxyHost iDataAgents. These agents do not perform a file level backup/copy.

Certain application related files can never be backed up by the File System iDataAgent due to the nature of the data. For example, Microsoft SQL Server database files cannot be backed up by the File System iDataAgent. In this and other similar circumstances, consider entering files such as these as exclusions in the corresponding subclient filter.

See [View the Items That Failed For a Data Protection Operation](#) for step-by-step instructions.

PRUNING BACKUP HISTORY INFORMATION

You can prune backup history information based on the number of days established in the **Days to keep the backup job histories** option from the **Media Management Configuration (Service Configuration)** dialog box available in the **Control Panel**.



If you have installed the SQL Server iDataAgent, do not use the stored procedure **sp_delete_backuphistory**, **sp_delete_database_backuphistory** and **sp_delete_backup_and_restore_history** provided by Microsoft clean up backup history. By default backup history is automatically pruned from the CommServe database and the Microsoft SQL Server, as necessary.

SUPPORTED FEATURES

- NAS iDataAgents do not support the ability to view items that failed.
- The Image Level and Image Level ProxyHost iDataAgents do not support the ability to Browse the data of a selected backup job in Backup Job History.

CONTENT INDEXING HISTORY INFORMATION

Content Indexing history can also be viewed of iDataAgents, BackupSets/Instances, and subclients. The following information is displayed:

ITEMS THAT WERE SUCCESSFULLY CONTENT INDEXED

You can view the list of items that were successfully content indexed during a Content Indexing operation for a particular job. for step-by-step instructions, see [View the Items that Were Successfully Content Indexed](#).

CONTENT INDEXING FAILURES

Content Indexing failures allows you to look at the messages, files and documents that could not be indexed during a content indexing operation. Content Indexing looks at each file (of the supported data types) and indexes its contents allowing advanced searches of backed up/archived/migrated data.

Files that were not indexed, (perhaps because the file's content could not be read) are added to the Content Indexing Failures list, and are viewable from the [View Content Index \(Failed Items\)](#) option in the Job History window. For step-by-step instruction, see [View the Items that Failed to Content Index](#).

[Back to Top](#)

Backup Job History - How To

[Topics](#) | [How To](#) | [Related Topics](#)

[View Backup Job History](#)

[View the Items That Were Protected During a Data Protection Operation](#)

[View the Items That Failed For a Data Protection Operation](#)

[View Job History Details](#)

[View the Media or Mount Paths of a Job History](#)

[View the Events of a Job History](#)

[View the Items that were Moved to Media during SnapProtect Backup](#)

[View the Log Files of a Job History](#)

View the Items that Were Not Indexed During Content Indexing

View the Items that Were Successfully Content Indexed

Resubmit a Backup Job

VIEW BACKUP JOB HISTORY

▶ To view backup history:

1. From the CommCell Browser, right-click the entity (client computer, iDataAgent, backup set or subclient) whose backup history you want to view, click **View**, and then click **View Backup History**.
2. From the Backup History filter window select the filter options, if any, that you want to apply, and then click OK. The system displays the Backup Job History window.
3. Click **OK**.

VIEW THE ITEMS THAT WERE PROTECTED DURING A DATA PROTECTION OPERATION



This option is available for File System-like agents.

Required Capability: none required

▶ To view the list of items that were protected during a data protection operation.

1. From the CommCell Browser, right-click the entity whose history of data protection operations you want to view, click **View**, and then click the necessary options to view a job history.
2. From the Job History Filter dialog box, select the filter options, if any, that you want to apply, and then click **OK**.
3. From the Job History window, right-click the operation whose list of protected items you want to view, and then select **View backup file list/View Backed Up Messages**. The **Backup file List** window displays a list of the backed up files/messages that were included in the backup job. You can use the **Search** option to find items in the window.
4. Click **File -> Exit**.
5. Click **Close** from the **Job History** window.

VIEW THE ITEMS THAT FAILED FOR A DATA PROTECTION OPERATION



A listing of files and folders that failed is not available for the Quick Recovery Agent, nor the Image Level and Image Level ProxyHost iDataAgents. These agents do not perform a file level backup/copy.

▶ To view the list of items that failed for a data protection operation:

1. From the CommCell Browser, right-click the entity whose history of data protection operations you want to view, click **View**, and then click to view a job history.
2. From the Job History Filter dialog box, select the filter options, if any, that you want to apply, and then click **OK**.
3. From the Job History window, right-click the operation whose list of failed items you want to view, and then select **View Failed Items**. The **Unsuccessful Backup Files** window (for DataArchiver Agents, **Items On Which Archive Failed**) displays those items that failed. If no items failed, a message to that effect is displayed.
4. Click **Close**.

VIEW JOB HISTORY DETAILS

Required Capability: See Capabilities and Permitted Actions

▶ To view the details of a job history:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then click job history.
2. From the Job History Filter dialog box, select the filter options that you want to apply and click **OK**.

3. From the Data Management Job History window, right-click the job whose job details you want to view, and then click **View Job Details**.
4. The Job Details dialog box appears, displaying detailed job history in General, Details, Phase Details and Attempts tabs for the selected job.
5. Click **OK**.



If viewing the details of a job with a pending or failed status, the **Reason for Job Delay** field will contain an Error Code, which, if clicked, will launch the customer support website displaying troubleshooting article(s) related to the specific issue.

VIEW THE MEDIA OR MOUNT PATHS OF A JOB HISTORY

▶ To view media or mount paths associated with a job history:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then select the appropriate history.
2. From the Job History window select the filter options, if any, that you want to apply, and then click **OK**.
3. From the job history window, right-click the backup whose media or mount paths you want to view, and then click **View Media**.
4. The Media Used By Job ID window displays a list of media or mount paths used by the operation.
5. Click **OK**.

VIEW THE EVENTS OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

▶ To view the events associated with a job:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then click **Job History**.
2. From the Job History Filter dialog box, select the filter options that you want to apply and click **OK**.
3. From the Data Management Job History window, right-click the job whose job details you want to view, and then click **View Events**.
4. The All Found Events window gets displayed. If no events were found for the backup, a message is displayed to that effect.
5. Click **Close**.

VIEW THE ITEMS THAT WERE MOVED TO MEDIA DURING SNAPPROTECT BACKUP



This option is available for the SnapProtect Backup.

▶ To view the list of items that were moved to tape during SnapProtect Backup.

1. From the CommCell Browser, right-click the entity whose history of data protection operations you want to view, click **View**, and then click the necessary options to view a job history.
2. From the Job History Filter dialog box, select the filter options, if any, that you want to apply, and then click **OK**.
3. From the Job History window, right-click the operation whose list of items moved to media you want to view, and then select **View Backup Copy file listing**. The **Backup file List** window displays a list of the backed up files that were included in the backup copy job. You can use the **Search** option to find items in the window.



- To view the files moved to media for a backup copy job, right-click the SnapProtect backup job corresponding to the Backup Copy job and select **View Backup Copy file listing**.
- View backup items will not display anything for a Backup Copy job.

4. Click **File** -> **Exit**.
5. Click **Close** from the **Job History** window.

VIEW THE LOG FILES OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

▶ To view the log files of a Job History:

1. From the CommCell Browser, right-click the entity whose job history you want to view, and then click to view a job history.
2. From the job history filter window select the filter options, if any, that you want to apply, and then click **OK**.
3. From the job history window, right-click the job whose log files you want to view, and then click **View Logs**.
4. The contents of the log file related to the selected job history are displayed in the **Log File for Job n** window.

VIEW THE ITEMS THAT WERE SUCCESSFULLY CONTENT INDEXED



This option is available for operations that performed content indexing.

▶ To view the list items that were not indexed during content indexing:

1. From the CommCell Browser, right-click the entity whose operations you want to view, click **View**, and then click the necessary options to view a job history.
2. From the Job History Filter dialog box, select the filter options, if any, that you want to apply, and then click **OK**.
3. From the Job History window, right-click the job for which you want to view the successfully content indexed items, select **View Content Index**, and click **Successful Items**.
4. Click **Close**.
5. Click **Close** from the **Job History** window.

VIEW THE ITEMS THAT FAILED TO CONTENT INDEX



This option is available for operations that performed content indexing.

▶ To view the list of items that failed to content index:

1. From the CommCell Browser, right-click the entity whose operations you want to view, click **View**, and then click the necessary options to view a job history.
2. From the Job History Filter dialog box, select the filter options, if any, that you want to apply, and then click **OK**.
3. From the Job History window, right-click the job for which you want to view the list of items failed to content index, select **View Content Index**, and click **Failed Items**.
4. Click **Close**.
5. Click **Close** from the **Job History** window.

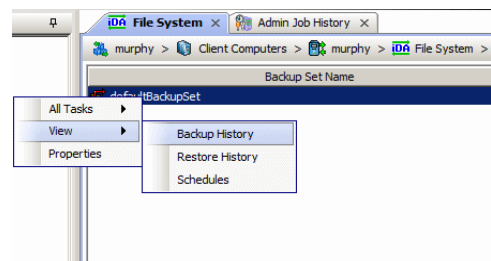
RESUBMIT A BACKUP JOB

▶ To resubmit a backup job:

1. From the CommCell Browser, right-click the subclient whose backup history you want to view, click **View**, and then click **View Backup History**.

Additionally, you can view the backup history for a client computer, iDataAgent, or backup set. However, the dialogs displayed may be different.

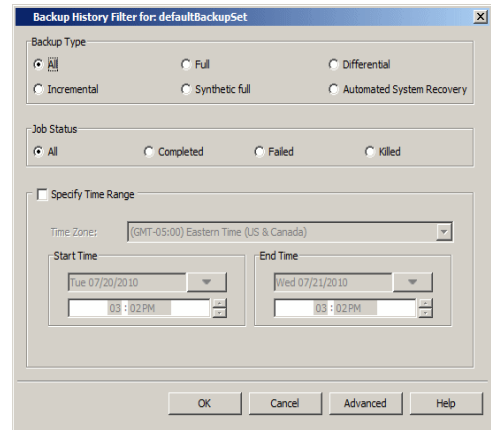
Note, if viewing the backup history for a client computer, right-click the computer name and select **Job History**.



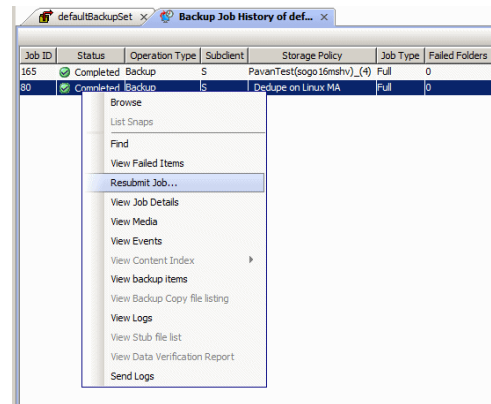
2. From the Backup History filter window select the filter options, if any, that you want to apply, and then click OK. The system displays the Backup Job History window.

Note: If viewing the job history for a client computer, ensure that the **Backup** radio button is selected.

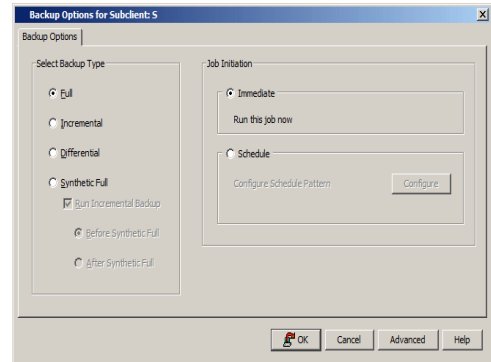
3. The Backup Job History window displays with the specified filter options.
4. Right-click on any job, and select **Resubmit Job**.



5. From the Backup Options dialog box, select the job options appropriate for the job you want to restart.

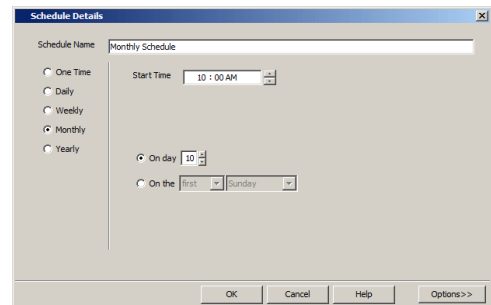


6. If you need to run the backup operation immediately, select **Immediate** from the **Job Initiation** tab. Go to step 11.
7. If you need to schedule the restore operation, select **Schedule** from the Job Initiation tab and click **Configure**.
8. From the **Schedule Details** dialog box that appears, select the appropriate scheduling options.



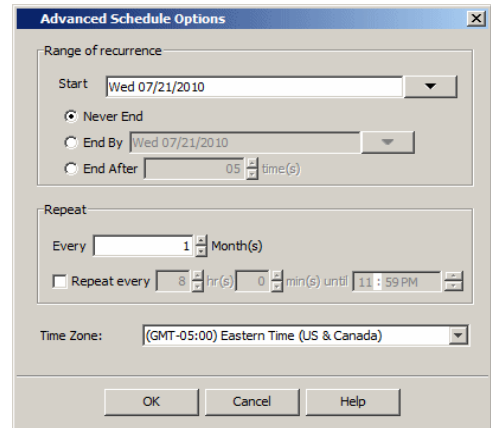
Click **Options** to view the Advanced Schedule Options dialog box.

9. From the **Advanced Schedule Options** dialog box:
 - **Range of recurrence:** Specify the date on which you want this schedule to take effect.



- **Repeat:** Select the value for which you want to run the job repeatedly on the day in which the job is scheduled to run.
- **Time Zone:** Select a specific time zone from which the job schedule time will be based.

Click **OK** to close the **Advanced Schedule Options** dialog box.



10. Click **OK** to close the **Schedule Details** window.
11. Click **OK** to close the job restart window.

[Back to Top](#)

Restore Job History

Topics | How To | Related Topics

Overview

Items That Restored

Supported Features

OVERVIEW

The **Restore History Filter** dialog box allows you to view detailed, historical information about restore jobs.

For information on Job Details displayed in the Job History, see [Viewing Job Information](#).

Once you have chosen your filter options, they are displayed in the **Restore Job History** window. From this window you can right-click a restore job to:

- View Restore Items; items in the job that were **Successful**, **Failed**, **Skipped** or **All**. These items, if any, will be listed in the **Restored Files** window.
 - View Job Details of the restore job. The job details will be listed in the **Job Details** window.
 - View Events of the restore job. The job events will be listed in the **All Found Events** window.
 - View Log files of the restore job. The job log files will be listed in the **Log File** window.
 - View the RMAN Log of an Oracle restore job. The RMAN Log will be listed in the **Oracle Restore Log** window.
 - View the BRTools log of a SAP for Oracle restore job. You can view the BRTools log for only those jobs that were initiated from the CommCell Console.
-

ITEMS THAT ARE RESTORED

When viewing files that are restored in the **Restored Files** window, each of the files is listed with the restore status level appended at the end of the file path. The possible status levels are: `RESTORED`, `FAILED` and `OLDER`.

Successfully restored files will be listed with `RESTORED` appended to the file path. If files are not restored/recovered due to errors, the file paths will be appended with `FAILED`. Under some circumstances, the system may not restore/recover certain files because they are older versions of the same files already present in the files system; these files are appended with the word `OLDER`.

SUPPORTED FEATURES

Consider the following.

- NAS iDataAgents do not support the ability to view failed/successful item lists.
 - Restore Job History will not display Oracle `rman_util` jobs at the instance level.
-

[Back to Top](#)

Restore History - How To

Topics | How To | Related Topics

[View Restore Job History](#)

[View the Events of a Job History](#)

[View the Media of a Job History](#)

[View the Log Files of a Job History](#)

VIEW RESTORE JOB HISTORY

▶ To view the restored items associated with a job:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job restore history you want to view, click **View**, and then click **Restore History**.

2. From the Job History filter window, select the filter options, if any, that you want to apply, and then click **OK**.
 3. From the Job History window, right-click the job whose restored items you want to view; click **View Restore Items**, and select from the type of items to view: **Successful**, **Failed**, **Skipped** or **All**.
 4. The **Restored Files** window will display the selected type of restored items for the job.
 5. Click **OK**.
-

VIEW THE EVENTS OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

▶ To view the events associated with a job:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then click **Job History**.
 2. From the Job History Filter dialog box, select the filter options that you want to apply and click **OK**.
 3. From the Data Management Job History window, right-click the job whose job details you want to view, and then click **View Events**.
 4. The All Found Events window gets displayed. If no events were found for the backup, a message is displayed to that effect.
 5. Click **Close**.
-

VIEW THE MEDIA OR MOUNT PATHS OF A JOB HISTORY

▶ To view media or mount paths associated with a job history:

1. From the CommCell Browser, right-click the entity (e.g., subclient, client computer, etc.) whose job history you want to view, click **View**, and then select the appropriate history.
 2. From the Job History window select the filter options, if any, that you want to apply, and then click **OK**.
 3. From the job history window, right-click the backup whose media or mount paths you want to view, and then click **View Media**.
 4. The Media Used By Job ID window displays a list of media or mount paths used by the operation.
 5. Click **OK**.
-

VIEW THE LOG FILES OF A JOB HISTORY

Required Capability: See Capabilities and Permitted Actions

▶ To view the log files of a Job History:

1. From the CommCell Browser, right-click the entity whose job history you want to view, and then click to view a job history.
 2. From the job history filter window select the filter options, if any, that you want to apply, and then click **OK**.
 3. From the job history window, right-click the job whose log files you want to view, and then click **View Logs**.
 4. The contents of the log file related to the selected job history are displayed in the **Log File for Job n** window.
-

[Back to Top](#)