IBM System Storage N series

SnapManager 6.1 for Microsoft SharePoint Server Installation and Administration Guide

GC27-2097-04
NA 210-05267_A0

Copyright and trademark information

Copyright information

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S.A. patents, foreign patents, or pending applications.

Trademark information

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe on any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, N.Y. 10504-1785
U.S.A.

For additional information, visit the web at:
http://www.ibm.com/ibm/licensing/contact/

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM web sites are provided for convenience only and do not in any manner serve as an endorsement of those web sites. The materials at those web sites are not part of the materials for this IBM product and use of those web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

Contents

Preface

Supported Features

IBM System Storage N series storage systems are driven by NetApp Data ONTAP software. Some features described in the product software documentation are neither offered nor supported by IBM. Please contact your local IBM representative or reseller for further details.

Information about supported features can also be found on the N series support website (accessed and navigated as described in "Websites" on page xi).

Websites

IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. The following web pages provide N series information:

- A listing of currently available N series products and features can be found at the following web page:

  www.ibm.com/storage/nas/

- The IBM System Storage N series support website requires users to register in order to obtain access to N series support content on the web. To understand how the N series support web content is organized and navigated, and to access the N series support website, refer to the following publicly accessible web page:

  www.ibm.com/storage/support/nseries/

  This web page also provides links to AutoSupport information as well as other important N series product resources.

- IBM System Storage N series products attach to a variety of servers and operating systems. To determine the latest supported attachments, go to the IBM N series interoperability matrix at the following web page:

  www.ibm.com/systems/storage/network/interophome.html

- For the latest N series hardware product documentation, including planning, installation and setup, and hardware monitoring, service and diagnostics, see the IBM N series Information Center at the following web page:

  publib.boulder.ibm.com/infocenter/nasinfo/nseries/index.jsp

Getting Information, Help, and Service

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you. This section contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your IBM N series product, and whom to call for service, if it is necessary.

Before You Call

Before you call, make sure you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure they are connected.
- Check the power switches to make sure the system is turned on.
- Use the troubleshooting information in your system documentation and use the diagnostic tools that come with your system.
- Refer to the N series support website (accessed and navigated as described in "Websites" on page xi) for information on known problems and limitations.

Using the Documentation

The latest versions of N series software documentation, including Data ONTAP and other software products, are available on the IBM N series support website, (accessed and navigated as described in "Websites" on page xi).

Current N series hardware product documentation is shipped with your hardware product in printed documents or as PDF files on a documentation CD. For the latest N series hardware product documentation PDFs, go to the IBM N series support website.

Hardware documentation, including planning, installation and setup, and hardware monitoring, service, and diagnostics, is also provided in an IBM N series Information Center at the following web page:

publib.boulder.ibm.com/infocenter/nasinfo/nseries/index.jsp

Hardware Service and Support

You can receive hardware service through IBM Integrated Technology Services. Visit the following web page for support telephone numbers:

www.ibm.com/planetwide/

Firmware Updates

IBM N series product firmware is embedded in Data ONTAP. As with all devices, it is recommended that you run the latest level of firmware. Any firmware updates are posted to the IBM N series support website (accessed and navigated as described in "Websites" on page xi).

Note

If you do not see new firmware updates on the IBM N series support website, you are running the latest level of firmware.

Verify that the latest level of firmware is installed on your machine before contacting IBM for technical support.

How to Send Your Comments

Your feedback helps us to provide the most accurate and high-quality information. If you have comments or suggestions for improving this document, please send them by e-mail to starpubs@us.ibm.com.

Be sure to include the following:

- Exact publication title
- Publication form number (for example, GC26-1234-02)
- Page, table, or illustration numbers
- A detailed description of any information that should be changed

Overview 1

About SnapManager for SharePoint

SnapManager for SharePoint is an enterprise strength backup, recovery, and data management solution for Microsoft SharePoint versions including Windows SharePoint Services 3.0, Microsoft Office SharePoint Server 2007, SharePoint Foundation 2010 (including SharePoint Foundation 2010 Service Pack 1), and SharePoint Server 2010 (including SharePoint Server 2010 Service Pack 1).

Operating on the latest distributed software platform from IBM, SnapManager for SharePoint is accessible from anywhere in the network through Internet Explorer®, and can monitor multiple SharePoint environments across a network. SnapManager for SharePoint Manager's main features include the following:

- The ability to centrally manage SharePoint backup and recovery jobs including scheduling, monitoring, reporting, user account management, and software agent management across multiple SharePoint farms from a single accessible-from-anywhere web interface.
- Fast backup speeds leveraging Snapshot backups, as well as real-time granular restore of items, item versions, lists, libraries, sites, and site collections directly onto the production server (or an alternate location).
- Backup coverage of all SharePoint 2007 and 2010 databases.
- Backup of SharePoint search index files.
- Backup of various SharePoint component settings including SharePoint solutions, IIS settings on web front-end servers, SharePoint Global Search settings, and InfoPath Forms Services.
- SnapMirror replication for backups of SharePoint databases and search indexes, and verification of SnapMirror database targets.
- SnapVault data set backup for backups of SharePoint databases and verification of SnapVault targets.
- Configure multiple schedules for different restore granularity levels in a single backup plan.
- Separately schedule verification jobs apart from backup or restore jobs.
- Separately schedule granular indexing jobs apart from backup jobs.
- Ability to browse and restore individual items from backup directly without generating an index at backup time.
- Different retention settings for the same backup components in multiple plans.
- Archive contents from the primary SQL content database storage to more affordable file system based locations (for example, CIFS devices) leveraging the EBS (SharePoint 2007/SharePoint 2010) and RBS (SharePoint 2010).

- End-user initiated archiving (SharePoint 2007).
- Integration with N series SnapLock technology.
- Integration with N series ASUP system for streamlined support.
- Integration with MOM (Microsoft Operations Manager) and SCOM (Microsoft System Center Operations Manager) event log.
- Support to backup and restore FAST Search Server Farms.

Preparing to Install SnapManager for SharePoint

2

Modules Required for Installation of SnapManager

SnapManager for SharePoint consists of two modules:

SnapManager for SharePoint Manager and SnapManager for SharePoint Agents.

Both modules must be installed in order to run SnapManager for SharePoint.

This section describes the tasks that you must complete before installing SnapManager 6.1 for SharePoint:

- Windows Host System Requirements
- Determining Storage Space Needs

Windows Host System Requirements

SnapManager for SharePoint Manager Requirements

The following table lists the hardware and software minimum requirements for SnapManager for SharePoint Manager:

Component	Requirement
Computer and Processor	PC with an Intel® Pentium® III-compatible 700 MHz processor (dual Intel Xeon® 3.0 GHz or faster recommended)
Memory	2 GB of RAM minimum, 3 GB recommended
Hard Disk	2 GB minimum, 5 GB or more recommended

Component	Requirement
Operating System	One of the following: • Windows Server 2003 Standard Edition with SP1 or SP2 (x86, x64) • Windows Server 2003 Enterprise Edition with SP1 or SP2 (x86, x64) • Windows Server 2003 R2 Standard Edition (x86, x64) • Windows Server 2003 R2 Enterprise Edition (x86, x64) • Windows Server 2003 R2 Standard Edition with SP2 (x86, x64) • Windows Server 2003 R2 Enterprise Edition with SP2 (x86, x64) • Windows Server 2008 Standard Edition (x86, x64) • Windows Server 2008 Standard Edition with SP1 or SP2 (x86, x64) • Windows Server 2008 Enterprise Edition (x86, x64) • Windows Server 2008 Enterprise Edition with SP1 or SP2 (x86, x64) • Windows Server 2008 R2 Standard Edition (x64) • Windows Server 2008 R2 Enterprise Edition (x64) **Note** SnapDrive for Windows 6.1 or later 6.1 or later must be installed in order to set up a LUN as a media service. **Note** From SnapManager 6.1 for SharePoint, Windows Clustering environment is supported. See "Windows Cluster Support" on page 19 for the details.
Framework	.NET Framework v3.5 required

SnapManager for SharePoint Agent Requirements

The following table lists the hardware and software requirements for the SnapManager for SharePoint Agent.

Component	Requirement
Computer and Processor	PC with an Intel Pentium III-compatible 700 MHz processor (dual Intel Xeon 3.0 GHz or faster recommended)
Memory	1 GB of RAM minimum, 2 GB recommended
Hard Disk	1 GB minimum, 3 GB recommended

Component	Requirement
Operating System	One of the following: • Windows Server 2003 Standard Edition with or SP2 (x86, x64, IA64) • Windows Server 2003 Enterprise Edition with or SP2 (x86, x64, IA64) • Windows Server 2003 R2 Standard Edition (x86, x64, IA64) • Windows Server 2003 R2 Enterprise Edition (x86, x64, IA64) • Windows Server 2003 R2 Standard Edition with SP2 (x86, x64, IA64) • Windows Server 2003 R2 Enterprise Edition with SP2 (x86, x64, IA64) • Windows Server 2008 Standard Edition (x64, x86, IA64) • Windows Server 2008 Enterprise Edition (x64, x86, IA64) • Windows Server 2008 R2 Standard Edition (x64, IA64) • Windows Server 2008 R2 Enterprise Edition (x64, IA64) **Note** IA64 only supported on SQL member agent. **Note** SharePoint Server 2010 and SharePoint Foundation 2010 both require 64-bit Operating Systems.
Framework	.NET Framework v3.5 required.

Component	Requirement
Microsoft SQL Server	The following list shows the requirements for Microsoft SQL Server. • SQL Server 2008 Standard Edition (x86, x64, IA64) • SQL Server 2008 R2 Standard Edition (x86, x64, IA64) • SQL Server 2008 R2 Enterprise Edition (x86, x64, IA64) • SQL Server 2008 Enterprise Edition (x86, x64, IA64) • SQL Server 2005 Standard Edition (x86, x64, IA64) • SQL Server 2005 Standard Edition with SP1, SP2 or SP3 (x86, x64, IA64) • SQL Server 2005 Enterprise Edition (x86, x64, IA64) • SQL Server 2005 Enterprise Edition with SP1, SP2 or SP3 (x86, x64, IA64) • SQL Server 2000 Standard Edition SP4 (x86) • SQL Server 2000 Enterprise Edition SP4 (x86)
SnapManager for Microsoft SQL Server Version	SnapManager for Microsoft SQL Server 5.0R1P2 or later must be installed and configured on the SQL Server containing your SharePoint databases. For the detailed information about SnapManager for Microsoft SQL Server, refer to the relevant *SnapManager® for Microsoft® SQL Server® Installation and Administration Guide.* You can find the guide on the N series support website (accessed and navigated as described in "Websites" on page xi). **Note** This requirement only pertains to the SnapManager for SharePoint Member Agent.

Component	Requirement
Microsoft SharePoint	SnapManager 6.1 for SharePoint requires one of the following Microsoft SharePoint environments to be installed: SharePoint Server 2010, SharePoint Foundation 2010, Microsoft Office SharePoint Server (MOSS) 2007 with SP1 or later or Windows SharePoint Services (WSS) 3.0 with SP1 or later. SnapManager 6.1 for SharePoint Storage Optimization requires one of the following Microsoft SharePoint environments to be installed: SharePoint Server 2010, Microsoft Office SharePoint Server (MOSS) 2007 with SP1 or later, or Windows SharePoint Services (WSS) 3.0 with SP1 or later. **Note** SharePoint Server 2010 and SharePoint Foundation 2010 require a 64-bit operating system.
SnapDrive and Data ONTAP	SnapManager 6.1 for SharePoint requires the installation of SnapDrive 6.1 for Windows or later on the SharePoint Index Server and the SharePoint SQL Servers and Data ONTAP 7.2.1 or later on your IBM N series storage system. For more detailed information about SnapDrive for Windows and Data ONTAP, refer to the relevant *Installation and Administration Guide*. You can find the guide on the N series support website (accessed and navigated as described in “Websites” on page xi).

Component	Requirement
VMDK	SnapManager 6.1 for SharePoint supports VMDK (VMware Virtual Machine Disk Format) disks. The following dependencies are required to support VMDK: • VMware ESX Server 4.0 or later • vCenter/vSphere 4.0 or later • SMVI 3.0 • SnapDrive 6.3 • SnapManager for SQL Server 5.1 For more detailed information about VMDK, refer to the *SnapDrive Installation and Administration Guide.* You can find the guide on the N series support website (accessed and navigated as described in "Websites" on page xi).

Determining Storage Space Needs

Storage Space Recommendations

The required storage space for content databases, indexes, and other storage requirements are unique to each SharePoint environment and must be estimated for each individual environment.

You can assess the general volume size requirements for SnapManager for SharePoint in the same way as SnapManager for Microsoft SQL Server. For more information, see the section assessing volume size in the *SnapManager for Microsoft SQL Server Installation and Administration Guide*. You can find the guide on the N series support website (accessed and navigated as described in "Websites" on page xi).

The general guidelines for sizing IBM N series volumes, storage devices, content databases, and indexes are described in the following table:

Component	**Size**	**Description**
Recommended Maximum Content Database Size	100GB (SharePoint2007) 200GB (SharePoint2010)	This is not an absolute maximum size but a general recommendation for performance and scalability. Refer to the links below for the detailed information from Microsoft: Microsoft TechNet Library - Storage and SQL Server capacity planning and configuration (SharePoint Server 2010) Microsoft TechNet Library - SharePoint Server 2010 capacity management: Software boundaries and limits
Recommended Maximum Number of Content Databases per Storage Device	10	This is a recommendation and not a limitation.

Component	Size	Description
Maximum Number of Content Databases per IBM N series Volume	100	Every database located on an IBM N series volume could potentially be backed up in a single backup operation. In this case, the SQL Server must still be able to manage all the databases while they are being backed up. Each database that is being backed up requires SQL Server resources. A typical SQL Server might not be able to manage any more than 100 databases. See the *SnapManager for Microsoft SQL Server Installation and Administration Guide* for more information. You can find the guide on the N series support website (accessed and navigated as described in “Websites” on page xi).
The recommendations in the following rows are based on the information found in the following Microsoft articles: For SharePoint 2007: Performance and Capacity Planning Resource Center for Microsoft Office SharePoint Server 2007 For SharePoint 2010: Performance and capacity technical case studies		
Database Log Files		Disk space needs for log files vary based on log settings and the number of databases. For more information, see the following article: Physical Database Storage Design This article also applies to SQL Server 2008.
Recommended Maximum Configuration Database Size	1.5 GB	Most configuration databases do not grow larger than this size. This is an estimated maximum size, not a boundary.

Component	Size	Description
Recommended Formula for Estimating Content Database Size Requirements		Estimate the initial volume of content that will be stored in content databases. ● In SharePoint 2007 environment Multiply the value of the size of the initial content by 1.2 to get the value of the size of stored content in an SQL Server database. For example, 30 GB of actual content x1.2 = a recommended 36 GB minimum database size. If versions are used for documents, a copy of each version is stored in the database. This means that when estimating, the final value of the size of documents stored must then be multiplied by the estimated number of versions for the documents. ● In SharePoint 2010 environment The formula to use is Database size = ((D x V) x S) + (10 KB × (L + (V x D))) D stands for number of documents. V stands for number of non-current versions. S stands for average size of documents. L stands for list items. The value of 10 KB in the formula is a constant that roughly estimates the amount of metadata required by SharePoint Server 2010. If your system requires significant use of metadata, you may want to increase this constant.

Component	Size	Description
Calculating Future Growth Data Storage Needs		● For SharePoint 2007 environment, plan for twice the amount of data that you initially plan to store. For more information, refer to Estimate performance and capacity requirements for Windows SharePoint Services ● For SharePoint 2010 environment, refer to Performance and capacity technical case studies
Content Index Server Recommended LUN Size		● In SharePoint 2007 environment, typically, content indexes require thirty percent of the space required by the amount of content in the content databases (see Content Database Estimated Size Requirements above) that will be indexed by the index server. The formula to use is: Size of data crawled = Y Size of index on index server = a range of 5% through 12% × Y = X Initial disk space = 2.5 x X. This is just an estimate to begin with, it may need to be larger. ● In SharePoint 2010 environment, refer to Storage and SQL Server capacity planning and configuration

Component	Size	Description
Archive Index Server Recommended LUN Size		Typically, archive indexes require 256 bytes per archived item. If full text index is enabled, add in the estimation of the content server index from above.

Installing SnapManager for SharePoint

3

This section describes how to install the SnapManager for SharePoint Manager and Agents.

The following topics are covered:

- Where to Install SnapManager for SharePoint Components
- Installing SnapManager for SharePoint Manager
- Installing SnapManager for SharePoint Agent

Where to Install SnapManager for SharePoint Components

Where to Install SnapManager for SharePoint Manager

SnapManager for SharePoint Manager can be installed on any machine on the network meeting the requirements described in “Windows Host System Requirements” on page 4. The machine it is installed on serves as the interface to access the SnapManager for SharePoint application from other machines. Therefore, you should install SnapManager for SharePoint Manager on a machine with high availability. This can be on the same machine where SnapManager for SharePoint Agent is installed.

Where to Install SnapManager for SharePoint Agent

There are four types of agents in SnapManager for SharePoint Agent, which can be deployed separately or on the same server depending on the needs of the environment:

Control Agent: Used to coordinate the backup process. It should only be installed on the SharePoint server that hosts the Central Administration role.

Member Agent: Does the actual backup of related SharePoint data. It should be installed on all the servers in the SharePoint farm that contain data to be backed up. For example: the Microsoft SQL Server (for database backups), the SharePoint index server (for search index backups), and the SharePoint web front-end server (for web front-end resource backups such as IIS backups).

Archiver Agent: This should be installed on all web front-end servers and the Central Administration server in this farm.

Extender Agent: This should be installed on all web front-end servers and the Central Administration server in this farm.

Required Permissions for SMSP Agent Account

The agent account performs the corresponding Agent activities. The detailed permissions of the agent account are as follows:

- On the Control Agent, an account with Farm Administrator and Local Administrator permissions and ViewServerState permission on SQL server is required.
- On the SQL Member Agent, an account with SQL *sysadmin* permission to SharePoint databases and Local Administrator permission is required.
- On the Archiver Agent and Extender Agent, an account with Farm Administrator, Local Administrator, owner of the corresponding content

database and full control for the corresponding web application permissions is required.

SQL Cluster Support

SnapManager for SharePoint supports SQL clustering. If cluster failover support is required, a member agent must be installed on each SQL cluster node.

Windows Cluster Support

SnapManager for SharePoint supports Windows clustering. Refer to the following table for the detailed installation steps:

Step	Action
1	On the active node, install SnapManager for SharePoint Manager on the shared disk. When installing, select only the *SMSP Manager* check box.
2	On the active node, navigate to **Start** > **Administrative Tools** > **Failover Cluster Manager**.
3	Right click on one cluster group under **Services and applications** node on the left, and click **Add a resource**. Select **4 - Generic Service**.
4	Add the SMSP Control Service and SMSP Web Service to the cluster group.
5	Double click the SMSP Control Service in the middle area, a window will pop up. Switch to the **Dependencies** tab. Add a dependency on the shared disk by selecting the shared disk in the **Resource** drop-down list.
6	Double click the SMSP Web Service in the middle area, a window will pop up. Switch to the **Dependencies** tab. Add a dependency on the SMSP Control Service by selecting the SMSP Control Service in the **Resource** drop-down list.
7	On the active node, navigate to **Start** > **Run**, and enter **regedit** in the pop-up window. Click **OK** to open the Registry Editor.

Step	Action
8	Export the following registry files: <\HKEY_LOCAL_MACHINE\Software\IBM\SnapManager for SharePoint> <\HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\SMSPControlServer> <\HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\SMSPWebServer> <\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\SMSPManager>
9	Import the registry files on each passive node and then restart the server. **Note** It is recommended to back up the corresponding registry files on the passive node before importing.

Installing SnapManager for SharePoint Manager

Installation Prerequisites

Before installing SnapManager for SharePoint Manager, complete the following steps:

Step	Action
1	If necessary, install the Microsoft .NET Framework v3.5+ on the machine which will host the Manager.
2	Verify that the installation account has local administrator rights on the Windows system.
3	Install SnapManager for Microsoft SQL Server on all machines containing Microsoft SQL Server SharePoint Databases. **Note** If you wish to use LUNs as media devices, you must install SnapDrive on the machine where you have installed SnapManager for SharePoint Media Service as well as on your SQL server. For more detailed information about SnapDrive, refer to *SnapDrive® for Windows® Installation and Administration Guide*

Installation Steps

You can install the product software either from the physical media kit or from software updates available for download. Downloads are available only to entitled N series customers who have completed the registration process on the N series support website (accessed and navigated as described in “Websites” on page xi).

Step	Action
1	Check the publication matrix page at www.ibm.com/systems/storage/network/interophome.html for important alerts, news, interoperability details, and other information about the product before beginning the installation.
2	Insert the CD-ROM into your host machine.

Step	Action
3	Browse to the SnapManager for SharePoint Manager installation package and double-click setup.exe.
4	Launch the software installation program from the CD-ROM or from where you downloaded the software, and then follow the prompts.
5	Review the license agreement for SnapManager for SharePoint. Read the terms of the agreement and select **I accept the terms in the license agreement**. Click **Next**.
6	Enter the desired installation or operating username and an organization name in the Customer Information window. Click **Next**.
7	Select **Change** to install the package to a drive or path other than the default path. By default, the installation creates a path <C:\Program Files\IBM> under your system disk. Click **Next**.
8	Click **Install** to proceed, click **Back** to return to the previous step, and click **Cancel** to exit the installation. The installation is therefore aborted and all the configurations, including the physical folders, are deleted.
9	You can choose to install only the SMSP Manager, only the Media Service, or both by checking the corresponding check boxes. Click **Install**. **Note** If you want to change which features are installed after finishing the installation, double-click the setup file to run it. Then select the **Modify** radio button in the installation wizard, and check or uncheck the corresponding check boxes for modifying.

Step	Action
10	After the installation is complete, review the SnapManager for SharePoint Manager configuration details and click **Test** to ensure your configuration is correct and functional. **SMSP Control Service Address:** Specify the current machine's hostname or IP address. If the Manager is installed in Windows Cluster environment, input the cluster name here. The Control Service manages internal configuration data, user access control, scheduling, and job monitoring. **SMSP Control Service Port:** The default port number is 12000. **Manager Web Service Port:** This port is used to access the CLI from other servers. The default port is 12011. **SMSP Media Service Address:** Specify the current machine's hostname or IP address. The Media Service manages backup job data (for example, job metadata and backup index, and archived content from Archiver and Extender). **SMSP Media Service Control Port:** The default port number is 12001. **SMSP Web Server Address:** Specify the current machine's hostname or IP address. The Web Service is the display engine for the browser console. **SMSP Web Server Port:** The default port number is 8080 for HTTP, and 8443 for HTTPS. **Enable HTTPS:** Selecting this checkbox enables users to access the SnapManager for SharePoint interface over HTTPS. By default, this checkbox is not selected. **Enable IPv6:** The IP address of the machines with the manager services installed must be IPv6 to utilize this protocol. By default, this checkbox is not selected.

Step	Action
11	**Enable Active Directory (AD):** Select this checkbox to integrate with AD and add existing AD users to the SnapManager for SharePoint platform. Enter the username and password of an AD account; the user is not required to be an AD administrator. **Note** The user entered here should have the Read and Write permissions of the following folder: <...\IBM\SnapManager for SharePoint\VaultServer\Control\bin\login\bin>. **Note** It is recommended that you use the default settings unless a known conflict with an existing port exists.
12	If SnapManager for SharePoint Manager is installed without enabling Active Directory, only local SnapManager for SharePoint accounts can be created and added to SnapManager for SharePoint. Change the settings according to your requirements and click **Next**.
13	The installer configures SnapManager for SharePoint Manager with the chosen name and port designations.
14	Click **Finish** to exit SnapManager for SharePoint Manager Install wizard.

There are some other ports that would be used by SnapManager, the ports are listed in the following:

- For Unattended Installation, it relies on Windows WMI on the Agent machine:

  Remote Procedure Call (RPC): 135

  Windows Management Instrumentation (WMI): 445

- The Connection to Filer requires the following ports on Filer:

  HTTP:80

  HTTPS:443

  Remote Procedure Call (RPC): 135

Installing SnapManager for SharePoint Agent

Installation Prerequisites

Before installing SnapManager for SharePoint Agent, complete the following steps:

Step	Action
1	If necessary, install the Microsoft .NET Framework v3.5 on all machines which you will be installing agents upon.
2	Install SharePoint Server 2010, SharePoint Foundation 2010, Microsoft Office SharePoint Server 2007, or Windows SharePoint Services 3.0 on related servers. **Note** If Storage Optimization functions are to be used on a SharePoint 2007 environment, Microsoft Office SharePoint Server 2007 with SP1 or Windows SharePoint Services 3.0 with SP1 is required.
3	Verify that the installation account has local administrator rights on the Windows system.
4	Install SnapManager for Microsoft SQL Server on all machines containing Microsoft SQL Servers (SnapManager for SharePoint Member Agent will be installed on this server) for the Data Protection agent type.

Installing the software

You can install the product software either from the physical media kit or from software updates available for download. Downloads are available only to entitled N series customers who have completed the registration process on the N series support website (accessed and navigated as described in “Websites” on page xi).

Step	Action
1	Check the publication matrix page at www.ibm.com/systems/storage/network/interophome.html for important alerts, news, interoperability details, and other information about the product before beginning the installation.
2	Agent Insert the CD-ROM into your host machine.
3	Browse to the SnapManager for SharePoint Agent installation package and double-click setup.exe.
4	Enter the Customer Information including the installation or operating username and organization in the field provided.
5	After the installation is complete, review the SnapManager for SharePoint Agent configuration details and then click **Test** to ensure your configuration is correct and functional. **SMSP Control Service Address:** Specify the hostname or the IP address of the server where the SnapManager for SharePoint Control Service is installed. If the Manager is installed in Windows Cluster environment, input the cluster name here. **SMSP Control Service Port:** This is the port used for communication with the Control Service and should match the information provided during the Manager configuration. The default port number is 12000. **SMSP Agent Address:** Specify the current server's host name, IP address or fully qualified domain name (FQDN). **SMSP Agent Port:** The port specified here is used by the Manager or other Agents for communication. The default port number is 10103. **SMSP Archiver Port:** This port is used for Archiver/Extender communication with SMSP BLOB Provider. The default port number is 10107. **Note** It is recommended that you use the default settings above, unless a known conflict with an existing port exists.

Step	Action
6	**User Account:** Specify the agent account under which the Agent activities are performed. See “Required Permissions for SMSP Agent Account” on page 18 for the detailed permissions. **Password:** This option requires the user to input the password of the user entered above. Click **Test** button to ensure whether the user account is existed and the password is valid.
7	**Enable IPv6:** This option should be configured to match the Manager. The IP address of the machines installed the agent service must be IPv6.
8	For all Agent types, local administrator rights are required. **Agent Type:** Check the box in front of the agent function. See “Where to Install SnapManager for SharePoint Agent” on page 18 for more information. **Note** This will also install the SMSP BLOB Provider during the Storage Optimization agent type installation, for which you must enable EBS/RBS in Storage Optimization > Enable EBS/RBS Settings after the installation is completed on all web front-end servers and the central administration server on the farm. See “Enabling EBS”/“Enabling RBS” on page 189 of this guide for more information about how to enable EBS/RBS settings. **Note** Agent types are logical types for different modules, they can reside on the same physical server.
9	Change the settings according to your needs and click **Next**.
10	Click **Finish** to exit SnapManager for SharePoint Agent Install wizard.

Upgrading SnapManager for SharePoint 4

This section describes how to upgrade the SnapManager for SharePoint Manager and Agents.

The following topics are covered:

- Upgrading SnapManager for SharePoint Manager
- Upgrading SnapManager for SharePoint Agent

Note

Contact Technical Support before upgrading if you have custom patches applied to your current version.

Upgrading SnapManager for SharePoint Manager

Preparing to Upgrade

Before upgrading your SnapManager for SharePoint Manager, we recommend performing a System Recovery backup for rollback purposes. See your relevant *SnapManager for SharePoint Installation and Administration Guide* for further instructions.

Note

This option is only available in SnapManager for Microsoft Office SharePoint Server 2.0 and later.

Note

It is recommended to upgrade Manager before upgrading Agent.

Installing the software

You can install the product software either from the physical media kit or from software updates available for download. Downloads are available only to entitled N series customers who have completed the registration process on the N series support website (accessed and navigated as described in "Websites" on page xi).

Step	Action
1	Check the publication matrix page at www.ibm.com/systems/storage/network/interophome.html for important alerts, news, interoperability details, and other information about the product before beginning the installation.
2	Download the SnapManager for SharePoint Manager package from the network and Browse to the SnapManager for SharePoint and double-click **SMSP_Manager**.
3	Launch the software installation program from where you downloaded the software, and then follow the prompts.
4	Review the license agreement for SnapManager for SharePoint. Read the terms of the agreement and click the radio button to select **I accept the terms in the license agreement**. Click **Next**.

Step	Action
5	After the installation is complete, review the SnapManager for SharePoint Manager configuration details. By default, the configuration information is the same as the configuration before the upgrade, and only requires customizing if any ports in your environment need to be changed. For further details on these fields, see the Manager installation instructions in "Installing SnapManager for SharePoint Manager" on page 21. After you are satisfied with the configuration settings, click **Next**.
6	The installer configures the SnapManager for SharePoint Manager with the chosen name and port designations.
7	Click **Finish** to exit SnapManager for SharePoint Manager Install wizard. **Note** If you are using Archiver in a SharePoint 2007 environment, after upgrading to SnapManager 6.1, select the checkbox that reads **To ensure that the Archiver externalized content can be accessed through stubs, please configure a default device for Archiver first.** Configure the default logical device in **Advanced Settings** of **Storage Optimization** before using Archiver. The default logical device must be configured before using Archiver.

Upgrading SnapManager for SharePoint Agent

Upgrade Steps

You can install the product software either from the physical media kit or from software updates available for download. Downloads are available only to entitled IBM N series customers who have completed the registration process on the IBM N series support website (accessed and navigated as described in "Websites" on page xi).

Step	Action
1	Check the publication matrix page at www.ibm.com/systems/storage/network/interophome.html for important alerts, news, interoperability details, and other information about the product before beginning the installation.
2	Download the SnapManager for SharePoint Agent package from the network and Browse to the SnapManager for SharePoint and double-click **SMSP_Agent**.
3	Launch the software installation program from where you downloaded the software, and then follow the prompts.
4	Review the license agreement for SnapManager for SharePoint. Read the terms of the agreement and click the radio button to select **I accept the terms in the license agreement**. Click **Next**.
5	After the installation is complete, review the SnapManager for SharePoint Agent configuration details. By default, the configuration information is the same as the configuration before the upgrade, and only requires customization if any ports in your environment need to be changed. For further details on these fields, see the Manager installation instructions in "Installing SnapManager for SharePoint Agent" on page 25.
6	After you are satisfied with the configuration settings, click **Next**.
7	Click **Finish** to exit SnapManager for SharePoint Agent Install wizard.

If storage optimization function was used prior to upgrade. It is recommended to perform the following steps to minimize the impact of upgrade on SharePoint end users:

Step	Action
1	Upgrade the SnapManager for SharePoint Media Service one by one.
2	Remove the current agent which will be upgraded from the Network Load Balancing environment.
3	Run the upgrade procedure as above for the Agent.
4	Add this agent back to the NLB environment after the upgrade has completed successfully.
5	Repeat steps 2-4 until all the agents in the NLB environment have been upgraded.

In the environment which enables EBS, if some DLL files of Storage Optimization module are still occupied by the process during the upgrade, you need to restart the IIS and SharePoint Timer Service to complete the upgrade. Click **Yes** in the corresponding pop-ups.

In the environment which enables RBS, if some DLL files of Extender module are still occupied by the process during the upgrade, you need to restart the IIS to make sure the Extender stubs can be accessed and downloaded normally after the upgrade. Click **Yes** in the corresponding pop-up.

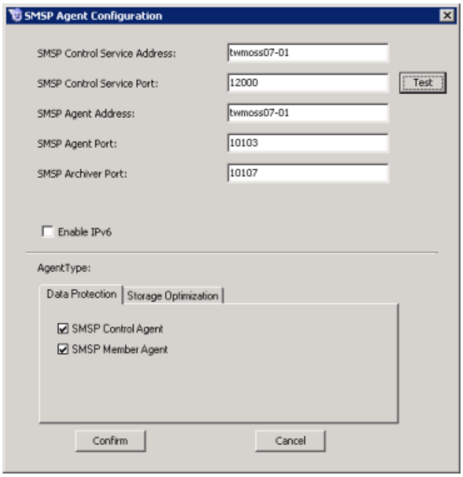
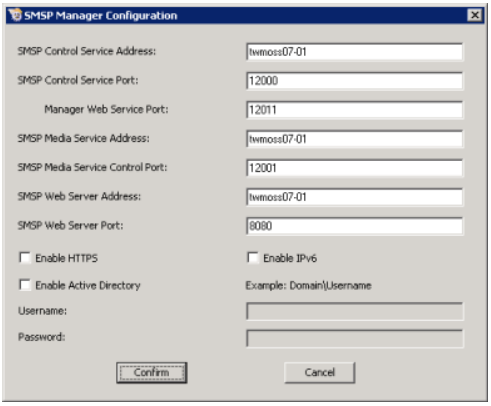
Verifying the SnapManager for SharePoint Installation

5

Verifying the Installation

To verify a proper installation, complete the following steps:

Step	Action
1	Open the **Services** tool on the machine where SnapManager for SharePoint is installed. This is located under **Administrative Tools** of the Windows **Control Panel**.
2	Verify that the following services are listed and started: ● SnapManager for SharePoint Communication Service (Agent) ● SnapManager for SharePoint Control Service (Manager) ● SnapManager for SharePoint Media Service (Manager) ● SnapManager for SharePoint Web Service (Manager)

Step	Action
3	To change any configuration settings (for example: an address or a port number) use the **Configuration** tool. This tool is available for both the Manager and the Agent, and is located in the SnapManager for SharePoint group in the Start menu of the respective machine.  SMSP Agent Configuration Test Data Protection Storage Optimization Confirm Cancel SMSP Control Service Address: twmoss07-01 SMSP Control Service Port: 12000 SMSP Agent Address: twmoss07-01 SMSP Agent Port: 10103 SMSP Archiver Port: 10107 ☐ Enable IPv6 AgentType: ☑ SMSP Control Agent ☑ SMSP Member Agent  SMSP Control Service Address: twmoss07-01 SMSP Control Service Port: 12000 Manager Web Service Port: 12011 SMSP Media Service Address: twmoss07-01 SMSP Media Service Control Port: 12001 SMSP Web Server Address: twmoss07-01 SMSP Web Server Port: 8080 ☐ Enable HTTPS ☐ Enable IPv6 ☐ Enable Active Directory Example: Domain\Username Username: Password:

Step	Action
4	**Note** If the *Archiver* module under *Storage Optimization* tab is unchecked in the Agent Configuration Tool, the corresponding solution will be retracted from the local machine. But the solution is not deleted from the SharePoint farm. **Note** If you un-check all the modules enabled in the Storage Optimization tab in the Agent Configuration Tool, after you click **Confirm**, a prompt message will pop up indicating that the externalized content may not be accessed through stubs on this machine. It is recommended you taking this SharePoint Front-end Web Server out of the environment if it is a Network Load Balanced one.
5	To restart any of the services that are down, use the **Restart Services** tool, which is available for both the Manager and the Agent. This tool is located in the Programs folder for SnapManager for SharePoint.
6	To ensure proper communication between SnapManager for SharePoint Manager and Agent, the ports listed in the table below must be open and available if a firewall is in place.

Ports Used by SnapManager for SharePoint Manager and Agent

The following ports should be open and available to ensure proper communication:

Component	Service Name	Default Port	Description	Public
Manager	Web Service	8080	Web server for the interface when HTTP is used	Y
		8443	Web server for the interface when HTTPS is selected	Y
	Control Service	12000	Control Service communication port	Y
	Media Service	12001	Media service control messages and data transfer port	Y
Agent	Communication Service	10103	Agent communication port	Y
		10107	Archiver port	Y
CLI		12011	CLI port	Y

Refer to the information below to enable the corresponding ports used by the Manager and the Agent:

SMSP Control Service Port: The port for Control Service; it will be used to connect with the agent. The default port number is 12000.

Manager Web Service Port: This port is used to access the CLI from other servers. The default port is 12011.

SMSP Media Service Control Port: The port is used by the Control Service to connect with the Media Service and used by the Agent to send the corresponding data to Media Server. The default port number is 12001.

SMSP Web Service Port: The port is used for accessing the Web Service using the browser. The default port number is 8080 for HTTP, and 8443 for HTTPS.

SMSP Agent Port: The port is used by the Manager or other Agents for communication. The default port number is 10103.

SMSP Archiver Port: This port is used for Archiver/Extender communication with SMSP BLOB Provider. The default port number is 10107.

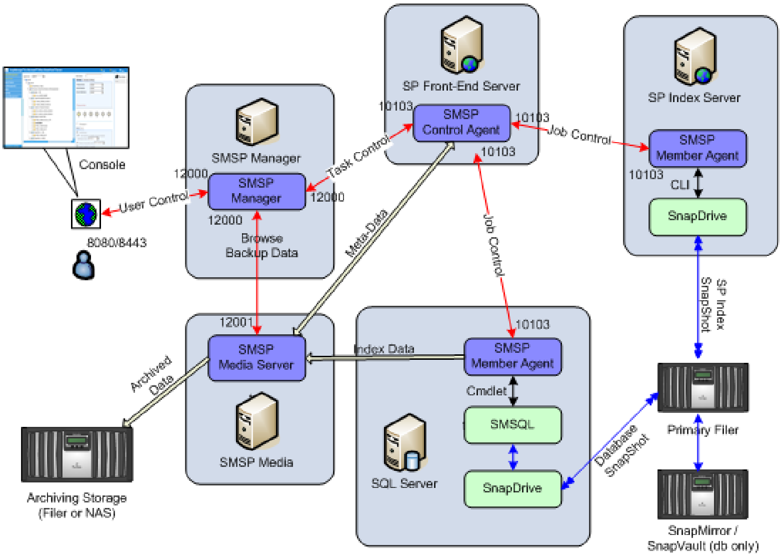
Note

The ports above are all default ports used for the Manager and the Agent. If you have changed the ports, you can find the corresponding ports in the **Manager Configuration Tool** or **Agent Configuration Tool**.

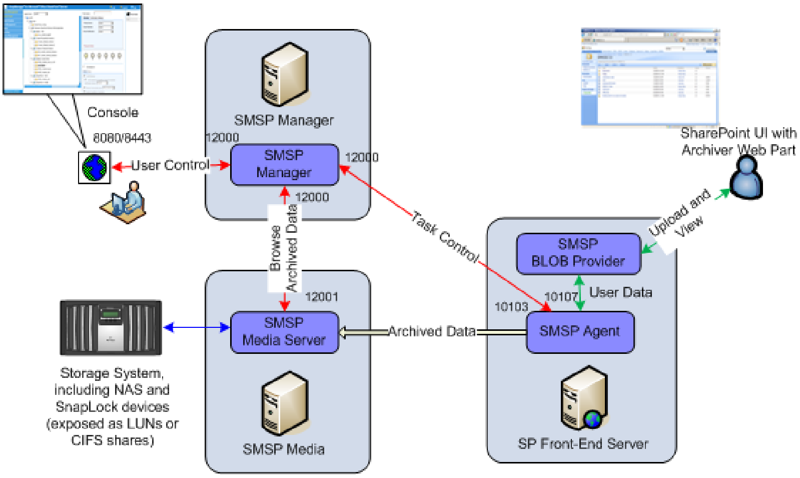
Topology Diagram for Ports

The following diagrams illustrate all of the internal and external connections that are used:

Data Protection Diagram



Storage Optimization Diagram



Accessing SnapManager for SharePoint 6

Accessing the Server

To access SnapManager for SharePoint, complete the following steps:

Step	Action
1	In the Internet Explorer address bar, enter the following: http://machine:8080/smsp or https://machine:8443/smsp Where *machine* is the host name or IP address of the machine running SnapManager for SharePoint Manager, and *8080* or *8443* represents the Web Service port defined during the configuration of the Manager (which depends on whether HTTP (*8080*) or HTTPS (*8443*) is configured). **Note** Another method to access SnapManager for SharePoint is through the link titled Start SMSP for Manager Application. By default, this link is located in the Start menu on the machine containing SnapManager for SharePoint Manager.
2	At the Login screen, select **Local System**, enter the initial login information and click **Login**. The default login information is as follows: Login ID: **admin** Password: **admin**

Note

The ability to access the SnapManager for SharePoint control panel should be limited to users with the highest level of administrative privileges.

Types of Login Modes

There are two kinds of login modes that you can specify:

Local User Login: A local user is also called a SnapManager for SharePoint user. Local users must be created and added to a group in the SMSP Account Manager first. The default admin account is prestored on the local database due to the installation of the system being owned by the SnapManager for SharePoint Administrators group, and cannot be deleted. When you log in as a local user, choose the Local System mode in the login page.

Active Directory (AD) User Login: This will create a separate domain available in the list where Local System is selected when you first log in to the platform. If you want the system to support the AD user login mode, you must enter a domain user account during the SnapManager for SharePoint Manager installation, or after installation from the Manager Configuration Tool. After logging in to the Local System for the first time, you can add AD users to the platform to log in later.

See the Control Panel - Account Manager section of this guide for details on setting up new local users or adding AD users.

Uninstalling SnapManager for SharePoint 7

Uninstallation Steps

Both SnapManager for SharePoint Manager and Agent can be removed using the Microsoft Windows **Add or Remove Programs** tool. To uninstall SnapManager for SharePoint Manager and Agent, complete the following steps:

Step	Action
1	Open the **Add or Remove Programs** tool from the Windows Control Panel.
2	To uninstall SnapManager for SharePoint Agent, locate the SnapManager for SharePoint Agent entry, and click **Remove**.

Step	Action
3	To remove SharePoint solutions or features, select the **Remove SharePoint solutions/features installed by SMSP** checkbox on the first screen of the uninstall interface. This option should only be selected when permanently uninstalling all Agents. The option will be shown when uninstalling an agent from a machine that has SharePoint installed. **Note** An account with Farm Administrator permission and Local Administrator permission is required for this task. To disable EBS/RBS settings in the SharePoint farm, select the **Disable EBS/RBS settings in SharePoint farm** option. The option will be shown when there is SharePoint installed on the Agent server. **Note** Only check this option when permanently uninstalling all Agents. If the SMSP Agents on all SharePoint servers are uninstalled, the stubs created by Archiver or Extender will no longer be accessible. The Convert Stubs to Content operation is recommended before uninstallation is performed. If the SharePoint solutions or features are not removed, it will be possible to reinstall the same version of the SnapManager for SharePoint Agent software while still using the existing configurations. An IIS reset is required to complete the uninstallation and user would be unable to access to your SharePoint environment during this time. Click **Yes** to proceed and **No** to exit the process.
4	Click **Finish** to end the uninstallation process.
5	To uninstall SnapManager for SharePoint Manager, locate SnapManager for SharePoint Manager, and click **Remove**.
6	To continue uninstalling SnapManager for SharePoint Manager, click **Yes** to verify removal.

Step	Action
7	Select to remove SMSP Manager, SMSP Media Service, or both of them. By removing SMSP Manager, the overall SMSP activities such as schedules, job controlling, and access controlling are disabled or terminated; meanwhile, the SMSP console interface cannot be accessed. By removing SMSP Media Service, the data created by SMSP is therefore no longer managed.
8	To remove the configuration data, select the **Remove the Configuration Data** checkbox on the last screen of the uninstall interface (before clicking **Finish**). If the configuration data is not removed, it will be possible to reinstall the same version of the SnapManager for SharePoint Manager software and use the existing configurations. **Note** The backup data from jobs managed by the Media Service are not deleted when you uninstall, even if the configurations are removed. If needed, you can manually delete these files from the system.

Preparing and Managing SharePoint Data 8

Planning for Volumes and LUNs in IBM N series storage

It is important to fully understand the implications of N series storage volumes and their LUNs during the backup and restore process. During the backup process, a Snapshot backup is created for SharePoint databases and SharePoint search index files located in an N series storage volume. The backup set can contain one or multiple Data ONTAP® LUNs with multiple databases.

If a LUN in a backup set contains multiple databases, but only a subset of databases needs to be restored, a stream-based database restore is performed.

If all databases contained in the LUN need to be restored, a LUN restore is performed, which is more efficient than the stream-based method. As such, for optimal restore speed, each database should ideally be on its own LUN. However, depending on the number of databases, this is not always possible because of the maximum number of LUNs that the system can have. In that case, putting the largest database on its own LUN, and keeping other related databases on another LUN (that is, the content databases pertaining to one SharePoint Web application) is the preferred method.

For the SharePoint search index, a similar recommendation applies. It is recommended that the SharePoint index for each SharePoint Shared Services Provider (SSP) reside on its own dedicated LUN. If the SharePoint search index is not the only folder on the LUN, the stream-based restore is used.

During backup, SharePoint databases use SnapManager for Microsoft SQL Server to generate a Snapshot backup, and the SharePoint search index LUNs use SnapDrive to generate their Snapshot backup. To minimize the number of Snapshots created during backup, it is recommended to use different volumes for database LUNs and search index LUNs.

Note

If SharePoint databases share a LUN with SQL Server system databases, only stream-based backup and restore can be utilized. This means SMSQL creates the full database backup by streaming out the contents of the databases individually, and no snapshot is created. As such, SnapManager for SharePoint does not support this configuration. Always put SharePoint databases on different LUNs from the SQL server system database LUN. For more information, see the *SnapManager for Microsoft SQL Server Installation and Administration Guide*. You can find the guide on the N series support website (accessed and navigated as described in “Websites” on page xi).

Planning for Storage Used by Archiver and Extender

With Archiver and Extender, SharePoint BLOB content can be stored outside of the primary SQL storage, on either SMSP managed storage, SAN, or NAS storage. The archived data can be protected periodically by using volume level snapshot backups. To reduce data management complexity, it is recommended to use separate volumes to host data from different farms. It is also recommended not to mix LUN and CIFS shares as storage devices.

Archiver/Extender storage devices have two main categories: index devices and data devices. Index devices are used to store the BLOB index and full-text index for Archiver data; data devices are used to store BLOB data and meta-data. Both devices can overflow to the next device if the current device is full. However, index devices have a higher performance impact when overflow happens. It is recommended to allocate index devices large enough to accommodate data growth. The average index device size is about 15% to 20% of the BLOB data size, depending on the nature of the content.

Database and Index Migration

Database Migration

SharePoint databases must be located on storage systems (LUNs) running data ONTAP to be backed up by SnapManager for SharePoint. If SharePoint databases are not located on storage systems, they need to be migrated to storage systems.

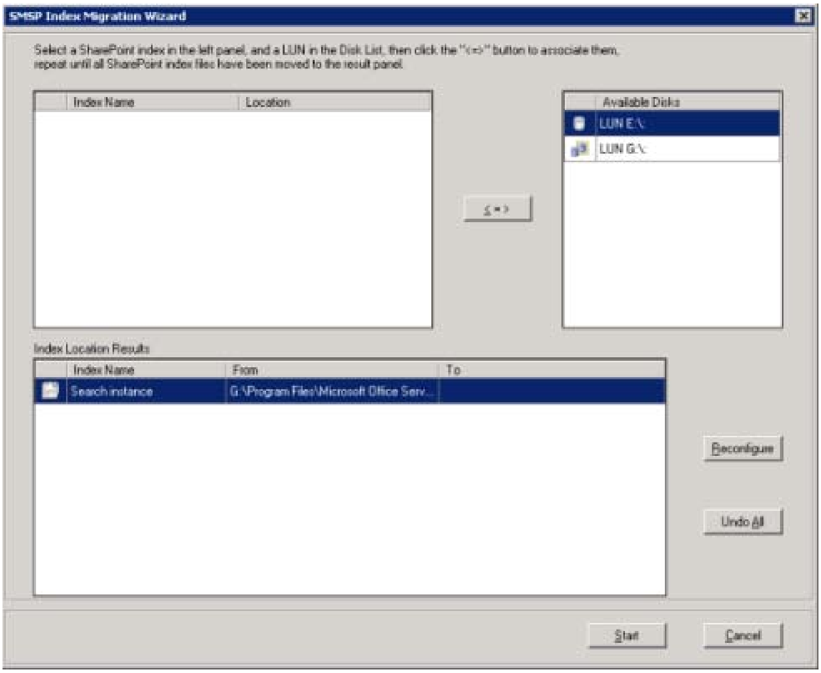
SnapManager for Microsoft SQL Server can be used to perform these operations. SharePoint Database and Index Migration Tool for SharePoint 2007/SharePoint Database and Index Migration Tool for SharePoint 2010 can also be used to facilitate this process. The tools are included in the SnapManager for SharePoint Agent installation, and can be used to attach and detach SharePoint-related databases for migration onto storage systems.

You can find the tools in the following paths:

<...\IBM\SnapManager for SharePoint\VaultClient\bin\SMSP2007PlatformMigrationTool.exe>

<...\IBM\SnapManager for SharePoint\VaultClient\bin\SMSP2010PlatformMigrationTool.exe>

The tools are also listed in SMSP Agent Tools (**Start > All Programs >** IBM **> SMSP Agent Tools**).



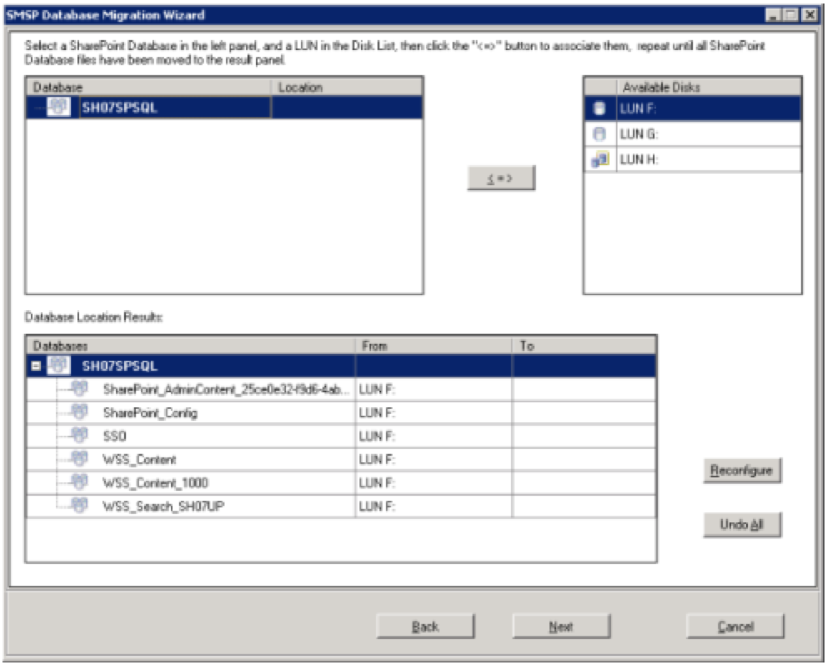
Select a SharePoint index in the left panel, and a LUN in the Disk List, then click the "<=>" button to associate them, repeat until all SharePoint index files have been moved to the result panel.

	Index Name	Location

	Available Disks
	LUN E:\
	LUN G:\

Index Location Results

	Index Name	From	To
	Search instance	G:\Program Files\Microsoft Office Serv...	



Select a SharePoint Database in the left panel, and a LUN in the Disk List, then click the "<=>" button to associate them, repeat until all SharePoint Database files have been moved to the result panel

Database	Location
SH07SPSQL	

	Available Disks
	LUN F:
	LUN G:
	LUN H:

Database Location Results:

Databases	From	To
SH07SPSQL		
SharePoint_AdminContent_25ce0e32-f9d6-4ab...	LUN F:	
SharePoint_Config	LUN F:	
SSO	LUN F:	
WSS_Content	LUN F:	
WSS_Content_1000	LUN F:	
WSS_Search_SH07UP	LUN F:	

The SMSP SharePoint Database\Index Migration Tool provides a way to move SharePoint databases or indexes to LUNs. If both SQL Server and SharePoint have been installed in your environment, you need to select the migration type to proceed. If only SQL Server or SharePoint has been installed in your environment, running this tool will directly lead you to the Database Migration Tool or Index Migration Tool Wizard accordingly.

Migrating a Content Database

The database migration tool is used for the migration of a SharePoint database in SMSQL, such as the Config DB or SSP DB. Go to SMSP Agent and find SharePoint Database and Index Tool for SharePoint 2007\2010 to open the tool wizard, then select **SharePoint Database** radio button to run the database migration tool. After starting to run this tool, complete the following steps:

Step	Action
1	Enter the Control Agent Information in the field provided, including the Address and Port number. For the Address, you may enter either an IP address or the Computer Name. Click **Next**.

Step	Action
2	Select the SharePoint database on the left panel and a LUN in the Available Disc list on the right, and click the <=> button; the database location result will be shown below.
3	You can click **Reconfigure** if you want to change the database location, or click **Next** to continue.
4	Configure the SnapInfo directory, either the **Single** or **Advanced** type.
5	After the SnapInfo is configured, click **Start**. A dialog box displays to remind you that the necessary SharePoint services will be stopped. If the server does not have SMSP installed, you must manually stop the services. If you click the **Show Detail** button, you can view the detailed information about which services will be restarted and which servers have the SMSP agent installed.
6	Click **OK** to continue, and the migration will start.
7	The Migration Information window will appear during the migration, and you can also download a detailed report by clicking the Download Report button after the job is completed. If there are still SQL connections open with the database, the tool will warn you with the detailed information.

Migrating the SharePoint Search index Files to a LUN

Use the Index Migration Tool to migrate the index files of Office SharePoint Server Search (OSearch) and Windows SharePoint Services Search (SPSearch) of SharePoint 2007 or Server Search and Foundation Search of SharePoint 2010 to a LUN. Go to SMSP Agent and find SharePoint Database and Index Tool for SharePoint 2007\2010 to open the tool wizard, then select **SharePoint Index** option to run the Index Migration Tool. To migrate the index files using Index Migration Tool, process the following steps:

Step	Action
1	Select the SharePoint index on the left panel and a LUN in the available disc list on the right, and then click the <=> button. The database location result will be shown below.

Step	Action
2	You can click **Reconfigure** if you want to change the index location, or click **Next** to continue. Click **Undo All** to clear the configuration.
3	Click **Start** to start the migration. The Migration Information window will appear, and you can download a detailed report by clicking the **Download Report** button after the job has completed.

Note

Do not select the same LUN for the location of both the SharePoint database and its index.

Creating a New Content Database

To create a new content database, create a new empty SQL database using the 'LATIN1_General_CI_AS_KS_WS' collation and move it onto the storage system running Data ONTAP. Next, in Microsoft SharePoint choose to create a new content database and point it to the precreated databases. For more information regarding this option, consult Microsoft SharePoint documentation. This is the recommended approach to create new content databases.

Deploying SharePoint with DBA-created Databases

If the storage system has already been allocated, but the SharePoint environment has not been created, the SharePoint databases can be set up first and then SharePoint can be deployed using DBA-created databases later. For instructions, go to the following Microsoft Website:

Microsoft TechNet Library - Deploy by using DBA-created databases (SharePoint Server 2010)

General Administrative Services 9

This chapter describes the following general administrative services accessible through the SnapManager for SharePoint Control Panel:

The following topics are covered:

- **SMSP Services**
  - Control Service
  - Agent Group
  - Account Manager
  - System Recovery
  - Remote Installation
  - Command With Operation
  - Server Email Notification
  - LUN and Physical Device Monitor
- **Data Management**
  - Device Manager
  - Data Retention
  - Verification and Index
  - Storage System
- **Reporting**
  - Log Manager
  - E-mail Notification
  - AutoSupport Settings
  - System Center Operations Manager Settings
  - Microsoft Operations Manager Settings
- **License Manager**

Control Service

About Server Monitor

Server Monitor provides a central interface to monitor SnapManager for SharePoint Media Service, Web Service, and Control Service. You can also view the port information, the hostname for the machine, product version, and the status for these services in the appropriate columns. The services are as follows:

- SnapManager for SharePoint Media Service is the component responsible for storing backup jobs and archive data.
- SnapManager for SharePoint Web Service provides an interface for sessions opened through browser consoles.
- SnapManager for SharePoint Control Service maintains internal SnapManager for SharePoint data such as backup plans and configurations, coordinates with the Agent during operations of this platform, maintains backup schedules, and performs other tasks related to the management of this platform.

About Agent Monitor

Agent Monitor provides a central interface to monitor and restart multiple SnapManager for SharePoint Agent hosts and enables you to adjust other settings.

You can use the **Restart**, **Disable**, and **Remove** buttons under the Control column to perform the following functions:

Restart: This restarts SnapManager for SharePoint Agent Service on the Agent machine (Communication Service). This does not reset all services, only those pertaining to this platform.

Disable: This suspends all backup or restore jobs corresponding to this Agent. All plans that were scheduled are skipped if an agent is disabled, but they will still be visible from all the modules.

Remove: This removes the specific Agent from SnapManager for SharePoint Manager. The plans for this Agent no longer run and this Agent is not available from either the Backup or Restore modules. This also means that the Agent Monitor no longer shows this agent in the interface. This option should be used only in instances when uninstalling an Agent does not remove it from the Agent Monitor.

To configure the Agent information, complete the following steps:

Note

In order to use agents from a remote install, you must configure them first.

Step	Action
1	Click **Configure**.
2	On the top-left of the dialog box, select the log level from the list. There are four options: **Error**, **Warn**, **Info**, and **Debug**. The default option is **Info**. **Note** When troubleshooting issues, the recommended setting for the log level is **Debug**.
3	On the bottom-left of the interface, select the **Account Configuration** you want to use to connect to the SharePoint environment. This account is the default option, and uses the domain name, username, and password specified when installing the Agent. The Control Agent account should be a farm administrator and should have the ViewServerState permission in SQL. The SQL Member Agent should have database operator (DBO) permissions to the SharePoint database. For other agent types, farm administrator permission is needed.

Step	Action
4	Within Agent Type, you can modify the agent types enabled for the specified Agent. **Note** If the Archiver module under **Storage Optimization** tab is unchecked in the Agent Configuration Tool, the corresponding solution will be retracted from the local machine. The solution will not be deleted from the SharePoint farm. **Note** If you uncheck all the modules enabled in the **Storage Optimization** tab, a prompt message will pop up indicating that the externalized content may not be accessed through stubs on this machine. We recommend you taking this SharePoint Front-end Web Server out of the environment if it is a Network Load Balanced one.
5	Within **Farm Information**, you can view the **Farm Name** and F**arm Version**. If it is a non-SharePoint agent, you can select to allow all SharePoint farm to use this agent or select the one(s) you want to allow to use it by clicking the edit icon.
6	After modifying any of the fields described in the previous steps, click **Save**. Click **Cancel** if you do not want to keep your changes.

Agent Group

About Agent Group

Agent Groups provide a central interface to monitor farm and agent configurations. You can select several agents and save them as one group. Using an agent group configuration will allow for high availability and load balanced access to the data. This feature is only supported by the Storage Optimization module.

Adding Agents to a Group

To add agents to a group, complete the following steps:

Step	Action
1	Select a farm from the **Farm** list. This will allow you to see all agent groups under this farm.
2	You can add the agent to a new group or to an existing group. If you want to add an agent to a new group, input the group name into the **Group Name** field. If you want to add an agent to an existing group, click the group name in the **Agent Group** area.
3	Drag the agent icon from the **Available Agents** field to the **Agents In Group** field.
4	Click **Save**. The agent group will be displayed under the **Agent Group** column on the right.

Modifying a Group

You can modify a group by clicking the corresponding **Group Name** in the **Agent Group** list. You can also modify the Group's name by using the **Group Name** field. Once all modifications are complete, click **Save** to save changes.

Note

The default group cannot be modified.

Deleting a Group

You can delete a group by clicking the corresponding **Delete** icon in the **Agent Group** list.

Note

The default group cannot be deleted.

Account Manager

Overview

In SnapManager for SharePoint, you can create users and assign them specific rights. Account Manager enables you to easily control and maintain the access rights to SnapManager for SharePoint from a central location, which ensures the integrity of the accounts. Additionally, you can add users to certain groups that are categorized by specific permissions. The following section describes the use of SnapManager for SharePoint's Account Manager.

About Users

To log in and use SnapManager for SharePoint, a username and corresponding password is needed. By default, the system has only one username: **admin** and password: **admin**. The **admin** user has full rights and this account cannot be deleted, though the password and other properties can be edited. Logging in as **admin** enables you to create other users and assign specific rights to those new users. New users can also be given the same rights as an administrator or restricted from certain actions by limiting their rights.

Note

You cannot directly assign rights to an individual user. You must first create a group and assign rights to that group. After adding a user to that group, you have then assigned the corresponding rights to the user.

About Groups

You can create groups in SnapManager for SharePoint and assign a series of rights to that group. You can then add specific users to a certain group. This is the only way to assign rights to users.

There are several built-in groups, including **Administrators**, **Managers**, and **Operators**. These have predefined permission levels and cannot be deleted. SnapManager for SharePoint **Administrators** have full access rights to the Account Manager (view and update) and can view all the items in the Control Panel.

Two types of groups can be created: local groups and Active Directory (AD) groups. A local group is managed within SnapManager for SharePoint only. An AD group is defined and maintained in the AD. To use an AD group, a domain user account must be specified during the installation of SnapManager for SharePoint Manager, or specified through the Manager Configuration Tool.

You can view all members in a local group by clicking the **Members** tab when the group is selected from the list. This is not available for AD groups, except through the AD itself.

In SnapManager 6.1, as with previous versions, groups are utilized to assign permissions regarding SMSP functions. Once a user has been added to a group, that user will be granted the permissions associated with that group.

Multi-Tenancy Control

SnapManager now allows multi-tenant security control, where SnapManager administrators can create agent groups and assign the permission scope for tenant administrators. Tenant administrator permission is controlled at SharePoint farm level.

For a typical multi-tenant scenario, SnapManager administrators will configure the followings:

- Create agent groups for tenant administrators, specify their permission scope.
- Common SnapManager settings, mainly Control Panel functions like devices, storage system and etc, as well as association with SharePoint farms if necessary.

Tenant administrators do not have access to the common settings but they will be able to access the SnapManager main functions (Data Protection, Storage Optimization). In each function, they can only operate on the SharePoint farms where they have access.

Creating a New Group

To create a new group or add an AD group, complete the following steps:

Step	Action
1	Click the **Account Manager** tab on the left of the window.
2	Click the Add Group icon (👤+). The add new group window displays. By default, a **local group** is created. An AD group can also be added by using the AD radio button. When an AD group is defined, all AD users in that group can log in to the SnapManager for SharePoint platform and perform actions as allowed by that AD group’s permissions.

Step	Action
3	Input the group name and a brief description of this group. If you are adding a pre-existing AD group, you can use the **Find** button to locate the name specified.
4	Click **Save** to save the group.

All the groups created or added in the Account Manager are added to the **User Defined** tab on the left, represented by a group icon in the **Account Type** column. For a list of groups predefined by SnapManager for SharePoint (including the Administrators group), click the **System Defined** tab.

Assigning Permissions to a Group

After a group is created, you must define its permissions. Permissions are separated into four groups: the permission to access the **Data Protection**, the permission to access or view the **Control Panel**, the permission to access the **Storage optimization**, and the permission to access the **Job Monitor**.

To change the access rights of a group, complete the following steps:

Step	Action
1	Click the **Group name** on the list on the left to load the group's information.
2	Click the **Permission** tab under the group name on the right. There are five options in the **Module** drop-down box under the **Permissions** tab.
3	Select the **Group with tenant administration permission** checkbox. A dialog box will open and allow you to select the farms you wish to allow this group to manage. By default, all farms are selected. This option is not selected by default; once it is checked, the group members will be treated as tenant administrators.
4	Select a **Module** from the drop-down box. This shows the permissions for the module you selected. Check if the group should have permission to either of these, or use the **Select All** and **Clear** buttons on the bottom of the interface.

Step	Action
5	For Control Panel and Job Monitor Module, with each permission item, you will always have at least two options: **View** and **Update**. Certain items will have a third option: **Control**. Control enables the user to take action from these modules (for example: restart services on an Agent). Choose which permissions to apply, or use the **Select All** and **Clear** buttons on the bottom.
6	Click **Apply** to assign the selected permissions to this group.

Note

Only the user in a group which has the right to update Account Manager can edit the profiles of other users and groups. By default, all users in the SnapManager Administrators group have the right to update the Account Manager. Therefore, the members of the SnapManager Administrators group can edit the profiles and permissions of other users and groups.

Creating a New Local User

To add a new user to a previously created, complete the following steps.

Step	Action
1	Click the **Add Users** icon (👤+). The add new user window displays. By default, the **Local user** radio button is selected.
2	Input a username, password, confirm the password and e-mail in the text boxes provided. Click **Save** to save the user, or click **Cancel** to cancel the configuration. If you save the user, the user appears under the **User Defined** tab on the left.

All users created in the Account Manager are added to the **User Defined** tab on the left, represented by a single-user icon in the **Account Type** column.

Note

The Admin user is the only predefined SnapManager for SharePoint Local user and cannot be removed. To edit the password for this account, click the **System Defined** tab, and click the **Admin** entry.

Adding a New AD User

To add an AD user, complete the following steps:

Step	Action
1	Click the **Add Users** icon (👤+). The add new user window displays.
2	Click the **AD** radio button.
3	Enter the username and click **Find** to find the user.
4	Make the user a member of a pre-existing group using the drop-down list.
5	Click **Save** to save the user, or click **Cancel** to cancel the configuration.

Editing a User or a Group

To edit a user or group’s attributes, click the corresponding name on the left, and the detailed information appears on the right of the screen. Modify the information, and click **Save** to save the modification.

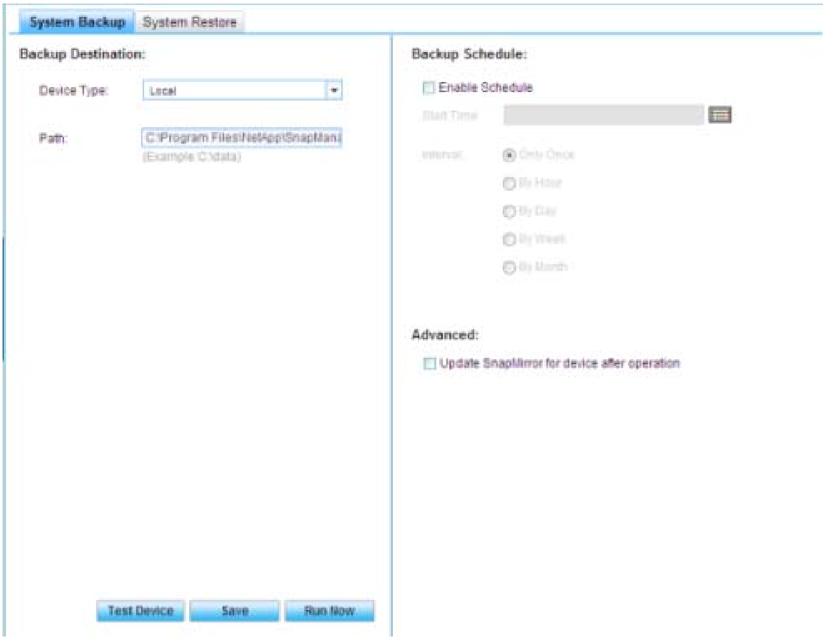
Deleting a User or a Group

To delete a user or group, click the ✕ sign or **Delete** icon next to the name on the right. Note that the system-defined accounts and users cannot be removed.

System Recovery

Overview

SnapManager for SharePoint System Recovery enables you to set up a manual or automatic backup job for the SnapManager for SharePoint system and then restore the system when needed. SnapManager system data consist of all the settings, including plans, policies, device configurations, users, and etc. SnapManager for SharePoint System Recovery can also be used to configure a new SnapManager for SharePoint deployment, provided the agent names remain the same.



Backup Destination:

Device Type: Local

Path: C:\Program Files\NetApp\SnapMan
(Example C:\data)

Backup Schedule:

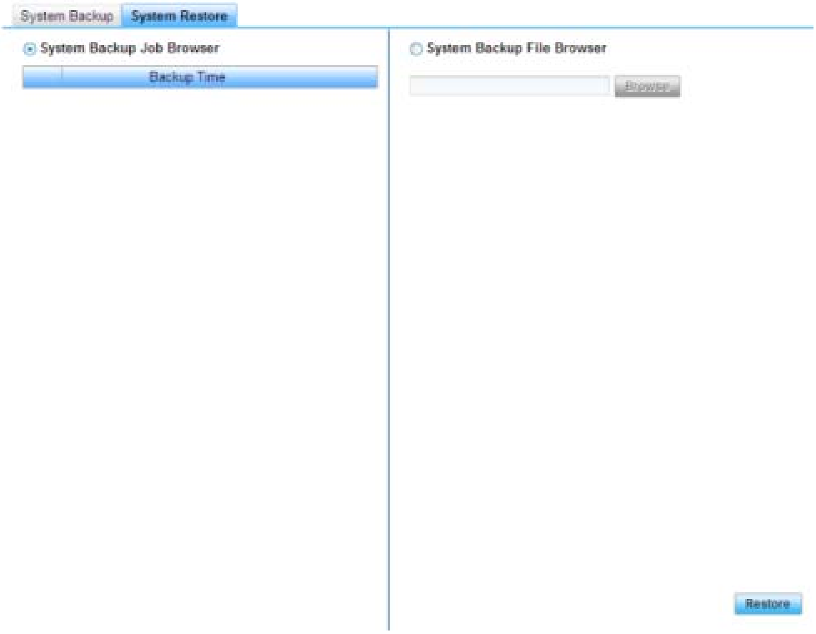
□ Enable Schedule

Start Time

Interval: ● Only Once
○ By Hour
○ By Day
○ By Week
○ By Month

Advanced:

□ Update SnapMirror for device after operation



Note

SnapManager for SharePoint System Recovery does not support System Recovery between different SMSP versions.

There are two parts in the SnapManager for SharePoint System Recovery: **System Backup** and **System Restore**.

System Backup

The **System Backup** tab enables you to execute a backup job of the system settings in this SnapManager for SharePoint deployment. System Backup saves the system settings into a flat file to the location defined under backup destination. Before a backup job can be executed, the backup schedule and backup destination settings must be configured.

To perform a backup, complete the following steps:

Step	Action
1	Specify the location where the System Recovery backup job file should be stored by selecting either Local, Network or CIFS Share in the **Device Type** drop-down box. The **Local** option stores data locally in the SnapManager for SharePoint Control Service machine.
2	If you select **Local**, you need to input a path such as “C:\data”. The default path is <C:\Program Files\IBM\SnapManager for SharePoint Server\SMSPData It's recommended to use a non-default location. LUN can also be used as the location to store system backup data. If the LUN is SnapMirror enabled and **Update SnapMirror for device after operation** option is checked, system backup data will be automatically replicated to the SnapMirror destination after a system backup job is completed. For disaster recovery purposes, it is recommended to use a LUN with SnapMirror enabled. Otherwise, the backup data need to be manually copied over to the DR site. You can choose not to update the SnapMirror for the device by not selecting the **Update SnapMirror for device after operation** option.
3	If you select **Network**, you need to input a path in standard UNC or “\\server\data” format. In the network device field, input the domain name, username and password with write permission.
4	If you select **CIFS Share**, you need to select the **Filer** and **Share Name** from the corresponding drop-down box and input the username and password. You can choose to update the SnapMirror for the device by selecting the **Update SnapMirror for device after operation** option. If the configuration is valid, when you enter the page again, the **Total Size** and **Free Space** will be shown in the corresponding fields.

To set up the backup schedule, complete the following steps:

Step	Action
1	Select the **Enable Schedule** check box to activate the backup schedule. This is not required if you only intend to create a one-time manual backup. Note that you can only specify one schedule.
2	Click the calendar icon next to the **Start Time** field and a calendar opens. Use the calendar to specify when the backup should begin.
3	Specify the interval at which an automatic or recurring backup should occur: **Only Once**, **By Hour**, **By Day**, **By Week**, or **By Month**.

To test the settings, complete the following steps:

Step	Action
1	After specifying the backup destination, click the **Test Device** button. If there is no problem accessing the backup location, you receive a **Test successful** message. Otherwise, an alert prompts you to check the backup device and try again.
2	Click **Save** and click **Run Now** to execute the backup job, or click **Save** to save the backup plan and run it at a later scheduled time and date. If the backup job is saved, it will be reloaded the next time this interface is opened.

Monitoring a Backup Job: After configuring the backup job, you can monitor it through the Backup Job Report at the bottom of the GUI. Click the white arrow on the right of the tool bar to expand and collapse it. The report includes the Start Time, the backup Path, the User who initiated the job, the Status, the backup Data Size, and the Progress. You can delete the job report by clicking the **Delete** button.

System Restore

After the backup is completed, it is listed with the **Backup Time** in the **System Restore Job** browser. You can restore to any point in time by choosing the radio button next to the appropriate job and clicking the **Restore** button.

Because the system settings are backed up to a file, the backup file can be physically transported and restored to a new SnapManager Server in a disaster recovery scenario. To restore the backup plans and SnapManager Control Panel profiles to a new SnapManager Server, use the System Backup File browser on the new machine to load the backup file. Click **Restore** to begin the restore process after selecting a file.

Note

Because the system settings are highly coupled with the topology of the environment, the new environment should have the same topology for the restored system settings to work as before.

Monitoring a Restore Job: You can monitor the restore job in the Restore Job Report. The report includes the Start Time, the Path the data is loaded from, the User who initiated it, the Status, the Data Size restored, and the Progress. You can delete the job report by clicking the **Delete** button.

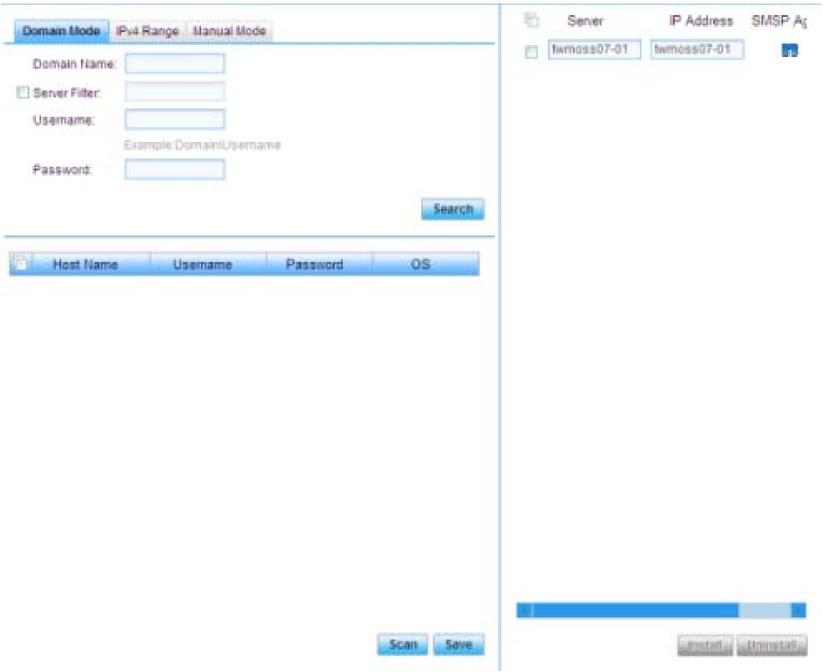
Note

In case multiple users are logged on to SnapManager for SharePoint System during a System Restore, when other users attempt any type of operation during the system restore, SnapManager for SharePoint displays a message stating that a system restore is executing and the action cannot be performed.

Remote Installation

About Remote Installation

The Remote Installation component of SnapManager for SharePoint enables you to install SnapManager for SharePoint Agents remotely.



□	Server	IP Address	SMSP Ag
□	fwmoss07-01	fwmoss07-01	

There are three methods in the SnapManager for SharePoint Remote Installation: Domain Mode, IPv4 Range Mode, and Manual Mode.

Searching for the Target Machine by Domain Mode

To search for the target machine by domain mode, complete the following steps:

Step	Action
1	Within the **Domain Mode** tab, enter the domain name, username, and password in the provided field. You can also enable a server filter by checking the corresponding checkbox, this will search the domain by the specific server. **Note** The **Server Filter** field supports wildcards (*****).
2	Click the **Search** button to find the target machine, and the following information will be displayed in the table underneath the search field. **Host Name:** The name of the agent. **Username and Password:** Here you may enter more specific username and password information if you have not been granted enough permission to view the agent information in the search results based on the previous entry. **OS:** This field will display the detailed information of the Operating System running on the agent.
3	Select the check box in front of the machine you wish to choose. Click the **Scan** button to find whether the selected machine installed the agent or not. You can click the **Save** button to save the information.

Note

You can search the machine only when the SMSP Manager can access the specified domain.

Searching the Target Machine by IPv4 Range Mode

To search the target machine by IPv4 Range mode, complete the following steps:

Step	Action
1	Within the **IPv4 Range** tab, input a valid IP range, username, and password in the fields provided. The table below will be populated with the information you have filled in. **Note** The valid IP range should be from smallest to largest, for example, 192.168.1.1-192.168.1.255.
2	Click the **Add** button, you will see the search criteria displayed underneath the search field.
3	Select the corresponding checkbox(es) for the IP Range you wish to search for, and then click the **Scan** button to find whether the selected machine installed the agent or not. Where the SMSP server and agent are not in the same domain, the searching result could be an IP address; in this situation, it is recommended to change the IP address into computer name in order to ensure the agent can be loaded normally in Data Protection module.

Adding the Server Manually

To add the server manually, complete the following steps:

Step	Action
1	Within the **Manual Mode** tab, input a valid hostname, username, and the corresponding password where you want to install/uninstall the agent in the fields provided. You can click the **Add** or **Remove** icon to add or remove a server. **Note** You can search the machine only when the SMSP Manager can connect with the machine by hostname. The hostname can be an IP address.

Step	Action
2	Click the **Scan** button to find whether the selected machine installed the agent or not.

Installing Agent on the Target Machine

To install the agent on the target machine, complete the following steps:

Step	Action
1	On the right-hand side of the screen, you can view the search results. The SMSP icon indicates that the agent has been installed for the particular instance. Select the checkbox next to the server on which you wish to do the remote installation.
2	Click the **Install** button. The configuration window will appear.
3	All the information about the agent and manager, such as agent port, archiver port, destination folder, user name, and password, will be acquired automatically.
4	Click the **Confirm** button to start installation process. You can view the installation progress and the results in Job Monitor.

Note

The agent installed through Remote Install must be configured before it can be used.

Uninstalling Agent on the Target Machine

To uninstall the agent on the target machine, complete the following steps:

Step	Action
1	Select the checkbox next to the server on which you wish to perform the remote uninstallation.

Step	Action
2	Click **Uninstall**; a dialog box will appear. See “Uninstalling SnapManager for SharePoint” on page 43 for the detailed information of the **Remove SharePoint solution/features installed by SMSP** option and **Disable EBS/RBS settings in SharePoint farm** option.
3	Click the **OK** button to start the uninstallation process. You can go to the Job Monitor to view the uninstallation status and results.

Command With Operation

How to Launch the Program or Script

For a SMSP database backup, database restore or database verification operation, you have the option to automatically run a command before the command starts or after the operation completes. If you choose this option, you will be prompted to specify the following information which will be stored as a command profile before the database backup or database restore or database verification operation can begin:

- The type of the command, which is either Pre-Operation command or Post-Operation command
- The host system from which the command is to be run
- The full path of the command that you want SMSQL to run before the database backup or database restore or database verification starts or after the database backup or database restore or database verification is complete
- Any parameters that are to be passed to the command

  Because the command (your own program or script) is invoked from within the context of a specific backup or database verification, you can pass the command information about the components of that operation. In your script, any occurrence of the text string **%1** corresponds to the first parameter passed; the text string **%2** corresponds to the second parameter, and so on.

After you have completed specifying the command and parameters, you can start the backup or restore or database verification operation.

Both SharePoint 2007 and SharePoint 2010 support *Command With Operation* function.

Note

The Post-Operation command or script will only be run only after a successful backup or restore or verification. If the backup or restore is not completed successfully, or if the verification fails, the Post-Operation command or script is not run.

Command Arguments passing Information to the Program or Script

The Run Command With Operation feature supports the following variables, which can pass operation-specific information to your program or script:

Variable	Description

$SqlSnapshot	Expands to the name of a SQL Server database Snapshot copy. This argument is used for backup and verification operations.
	Examples:
	`sqlsnap__winsrvr2__01-31-2005_15.03.09`
	`sqlsnap_winserver_recent`
	Note
	The number of database Snapshot copies in a SnapManager backup set depends on the number of volumes used to store the databases included in the backup.
	For restore operation, this argument specifies the name of the Snapshot copy to be restored.
	Example:
	`sqlsnap__winsrvr2__01-31-2005_15.03.09`
	`sqlsnap__winsrvr2__recent`

$InfoSnapshot	Expands to the name of a SnapInfo directory Snapshot copy.
	Examples:
	`sqlinfo__winsrvr2__01-31-2005_15.03.09`
	`sqlinfo__winsrvr2__recent`

Variable	Description

$SnapInfoName	Expands to the name of the SnapInfo directory.
	Examples:
	`WINSRVR2__recent`
	`WINSRVR2_11-23-2004_16.21.07__Daily`
	Note
	If you use this variable, you must also provide the correct path to the directory.

$SnapInfoPath	Expands to the name of the SnapInfo subdirectory. This argument is used in backup and verification operations.
	Example:
	`I:\SMSQL_SnapInfo\SQL__WINSRVR2\DB__Northwind`
	For restore operation, this argument specifies the path to the Snapshot copy information metadata that is being used for the database restore.
	Example:
	`U:\SMSQL_SnapInfo\VDISK__E\FG__\05-14-2010_15.33.41\SnapInfo__05-14-2010_15.33.41.sml`

$LogBackupFile	Expands to the full path name of the transaction log backup file. Example: `I:\SMSQL_SnapInfo\SQL__WINSRVR2\DB__Northwind\LogBackup\ 11-01-2004_13.34.59__Northwind.TRB`

Variable	Description

$Database	Specifies the logical name of the database processes.
	Note
	To prevent PowerShell from interpreting the value of this parameter, be sure to enclose the entire parameter value with single quotes. For example: `-PreCmdArg ‘$Database $ServerInstance’`
	Example:
	`DatabaseAccounting`
	If you want to have more than one database expanded, repeat the parameter as many times as you want.
	Example:
	`AccountingDB1 AcmeServer1/SqlInst1 FinanceDB2`
	`AcmeServer1/SqlInst2`

$ServerInstance	Specifies the name of the SQL server instance that is actually processed. Example: `ACMESERVER1\SQLINSTANCE1`
$OperationStatus	Provides the status of the SMSQL operation. Example: 5234
$PreCommandStatus	Provides the pre-command status to the post-command if the post-command is executed based on the status of the earlier pre-command. Example: 5234

Note

Several parameters like the `$SnapInfoPath` and `$LogBackupFile` variables are automatically enclosed within double quotes so that the actual path name can contain spaces without affecting the script invocation on the Windows command-line. If you do not want the double quotes to appear in your command-line, remove them from the Command Arguments field.

How to Specify a Run Command With Operation

To store a command profile, complete the following steps:

Step	Action
1	Select **Control Panel > SMSP Services > Command With Operation.**
2	Select one or more agents on which you want to Run Command With Operation.
3	Click **Configure**.

Step	Action
4	Choose the **Pre-Operation Command** tab and specify the details of the command: ● Check the Run pre-command or script before the SnapManager Operation starts checkbox to enable this function. ● If the Treat pre-command errors as fatal by stopping the remaining SnapManager operation option is selected and the pre-command does not complete successfully, the following backup or restore or the verification operation will not be run. ● Specify the hostname or IP address of one computer where you want to run the command (your own program or script) in the Specify a computer where you want to run the command: text box. ● Specify the full path to the command in the program or script you want to run: text box. ● Select the sequence of SnapManager variables that you want to pass to the command in the SnapManager Variables: field, all the variables that you have selected will be shown in Command Arguments: field. Choose the **Post-Operation Command** tab and specify the details of the command: ● Check the Run post-command or script after the SnapManager Operation completes checkbox to enable this function. ● If the Treat post-command errors as fatal by stopping the remaining SnapManager operation option is selected and the post-command does not complete successfully, the result of running the post-command will be considered as failed. ● Specify the hostname or IP address of one computer where you want to run the command (your own program or script) in the Specify a computer where you want to run the command: textbox. ● Specify the full path to the command in the program or script you want to run: textbox. ● Select the sequence of SnapManager variables that you want to pass to the command in the SnapManager Variables: field; all of the variables that you have selected will be shown in Command Arguments: field.

Step	Action
5	Click **OK** to save the configuration.
6	Specify a **Profile** name, and then click **Save** to save it.

Step	Action
1	Select **Data Protection > Backup Builder** and select an agent.
2	Specify a database, a logical device, and plan name. Click **Save**.
3	Click **Backup Now**. In the dialog box, go to the **Advanced** tab, select a preconfigured command profile to run with the operation. Click **Run**.

To specify a command profile while starting a restore operation, complete the following steps:

Step	Action
1	Select **Data Protection > Restore Controller** and select an agent.
2	Specify a time range in the **Time Window** field and click **Load Timeline** to load the plan. Click a plan's point-in-time icon to load the data for this plan. Select the data you want to restore.
3	In **Restore Options**, select a preconfigured command profile to run with the operation. Click **Go**.

To specify a command profile while starting a database verification operation, complete the following steps:

Step	Action
1	Select **Data Protection > Backup Builder**. In Plan Viewer, load a plan.

Step	Action
2	Go to the **Backup Maintenance** tab, check the checkbox before **Verify last**, and select a preconfigured command profile to run with the operation. Click **Save**.
3	Click **Run Now**.

To specify a command profile while scheduling a backup operation, complete the following steps:

Step	Action
1	Select **Data Protection > Backup Builder** and select an agent.
2	Specify a database, a media server, and plan name, click **Save**.
3	Check the checkbox before **Schedule A**. Go to the **Advanced** tab and select a preconfigured command profile to run with the operation. Specify a schedule time, Click **Save**.

To specify a command profile while scheduling a restore operation, complete the following steps:

Step	Action
1	Select **Data Protection > Restore Controller** and select an agent.
2	Specify a time range in the **Time Window** field and click **Load Timeline** to load the plan. Click a plan's point-in-time icon to load the data for this plan. Select the data you want to restore.
3	In **Restore Options**, select a preconfigured command profile to run with the operation. Specify a start time and click **Go**.

To specify a command profile while scheduling a database verification operation, complete the following steps:

Step	Action
1	Select **Data Protection > Backup Builder**. In Plan Viewer, load a plan.
2	Go to the **Backup Maintenance** tab, check the checkbox before **Verify last**, and select a preconfigured command profile to run with the operation. Uncheck **No Schedule**, and then specify a schedule time. Click **Save**.

The following are some helpful notes on the **Command With Operation** function:

- The machine specified in the Specify a computer where you want to run the command: textbox should have SMSQL installed to run the command.
- If the version of SMSQL is 5.0 on the machine which runs the database backup or database restore or database verification job, only the post-command will be executed.
- If the version of SMSQL is 5.1 on the machine which runs the database backup or database restore or database verification job, both the pre-command and the post-command will be executed.

Server Email Notification

Overview

Server Email Notification enables you to get a notification Email when one or several of the following items exceed the specified threshold: CPU Usage, Threads, Memory Usage, and Network Utilization.

Media Server

This area shows all the Media Servers connected to the SnapManager. Click on the name of one Media Server and you can configure an Email Notification for it.

Email Notification

Check the **Email Notification** check box to enable the corresponding settings. You can select one Email Notification Profile in the drop-down box. Click the **Email Notification** link to navigate to the corresponding setting page. However, all the unsaved changes will be lost.

Threshold

The user can monitor and configure the corresponding threshold for the following four options:

- **CPU Usage**

  Enter the percentage to specify the CPU occupied by the Media Service. The time period can be measured by Minutes or Seconds.

  If the CPU Usage for the Media Service is higher than the specified percentage for more than the corresponding time period, it will trigger an Email Notification when SnapManager performs the check.

- **Threads**

  Enter the number to specify the threads used by the Media Service. The time period can be measured by Minutes or Seconds. If the Media Service uses more than the specified number of threads for more than the corresponding time period, it will trigger an Email Notification when SnapManager performs the check.

- **Memory Usage**

  Enter the number to specify the Memory used by the Media Service. The time period can be measured by Minutes or Seconds. If the Media Service uses more than the specified number of Memory for more than the corresponding time period, it will trigger an Email Notification when SnapManager performs the check.

- **Network Utilization**

  Enter the percentage to specify the Network used by the machine which has installed the Media Service. The time period can be measured by Minutes or Seconds.

  If the Network Utilization for the Media Server is higher than the specified percentage for more than the corresponding time period, it will trigger an Email Notification when SnapManager performs the check.

Note

If more than one option above has been selected, SnapManager will send out one Notification Email when any of the thresholds is met.

Interval

This option is used to set the corresponding interval for the check operation of SnapManager.

Select one time unit for the check from Minute, Hour, Day, Week and Month and enter a number in the corresponding textbox.

Click **Apply** to save the corresponding Configuration.

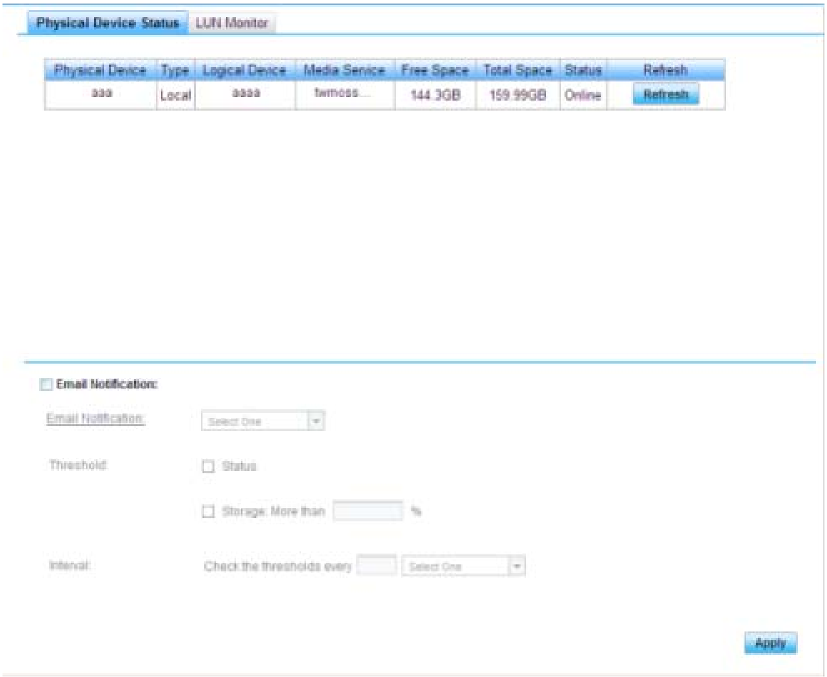
Note

The interval of the check operation can be configured here. However, SnapManager will collect the information every second.

LUN and Physical Device Monitor

Physical Device Status

Physical Device Status provides a central interface to monitor the status of all the Physical Devices of the Logical Devices. The following information can be viewed in the **Physical Device Status** tab.



Physical Device	Type	Logical Device	Media Service	Free Space	Total Space	Status	Refresh
aaa	Local	aaaa	twmoss...	144.3GB	159.99GB	Online	Refresh

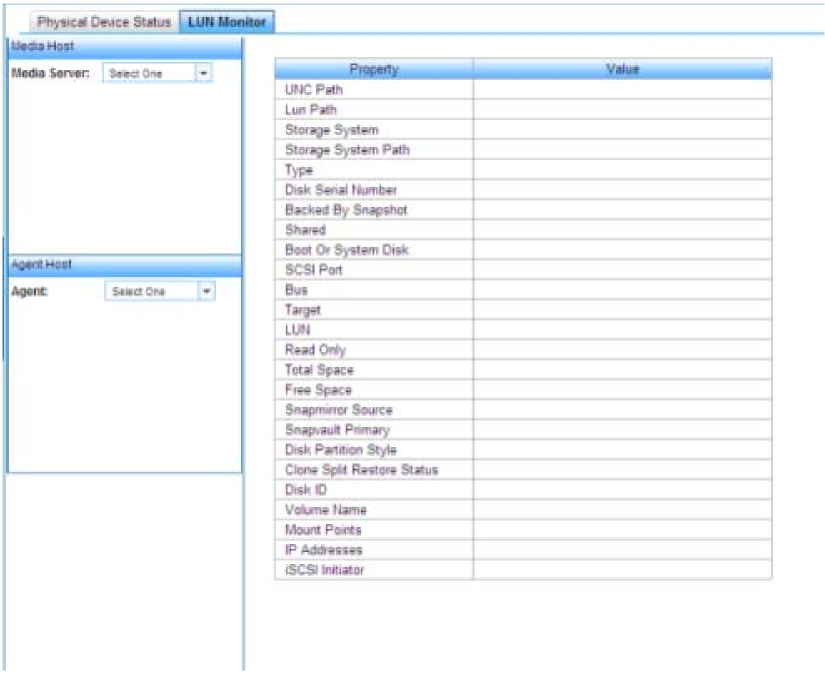
□ Email Notification:

Email Notification: Select One

Threshold: □ Status

□ Storage: More than %

Interval: Check the thresholds every Select One



Media Server: Select One

Agent: Select One

Property	Value
UNC Path	
Lun Path	
Storage System	
Storage System Path	
Type	
Disk Serial Number	
Backed By Snapshot	
Shared	
Boot Or System Disk	
SCSI Port	
Bus	
Target	
LUN	
Read Only	
Total Space	
Free Space	
Snapmirror Source	
Snapvault Primary	
Disk Partition Style	
Clone Split Restore Status	
Disk ID	
Volume Name	
Mount Points	
IP Addresses	
iSCSI Initiator	

- Physical Device

  The name of the Physical Device.
- Type

  The type of the Physical Device. It can be one of the following types: Local, Network, LUN, CIFS Share and SnapLock.
- Logical Device

  The name of the Logical Device that contains this Physical Device.
- Media Service

  The Media Service used by the corresponding Logical Device.
- Free Space

  The free space of the storage location.
- Total Space

  The total size of the storage location.
- Status

  The status of the Physical Device. It can be Online or Offline. Offline means the Physical Device is not available.

Click **Refresh** in the **Refresh** column of the table; the information in the table will be refreshed.

Email Notification

Check the **Email Notification** check box to enable the settings in the field below. You can select one Email Notification Profile in the drop-down box, Click the **Email Notification** link to navigate to the corresponding setting page. However, all the unsaved changes will be lost.

Threshold

The user can configure the following thresholds for the Email Notification:

- Status

  This option is selected by default. If the status of some Physical Device is Offline, it will trigger an Email Notification when SnapManager performs the check.

- Storage: More than__%

  This option is selected by default. If the percentage of the space occupied by some Physical Device is higher than the specified percentage, it will trigger an Email Notification when SnapManager performs the check.

Interval

This option is used to set the corresponding interval for the check operation of SnapManager.

Select one time unit for the check from Minute, Hour, Day, Week and Month and enter a number in the corresponding textbox.

Click **Apply** to save the corresponding Configuration.

LUN Monitor

LUN Monitor provides a central interface to view the detailed information of the LUN on the Media Server and Agent Host.

If you want to view the information of the LUN on the Media Server, complete the steps below.

Step	Action
1	Select one Media Service from the **Media Server** drop-down box.

Step	Action
2	After the loading process finishes, all the LUN on the Media Server will be shown in the area below. You can click the **Refresh** button next to the **Media Server** drop-down box to refresh the LUN information on the Media Server.
3	Click on the name of one LUN; all the detailed information will be shown in the table on the right. **Note** If the LUN has not been saved as a Physical Device, a ⊘ icon will be shown next to the LUN's name.

If you want to view the information of the LUN on the Agent Host, complete the steps below.

Step	Action
1	Select one Agent Host from the **Agent** drop-down box.
2	After the loading process finishes, all the LUN on the Agent Host will be shown in the area below. You can click the **Refresh** button next to the **Agent** drop-down box to refresh the LUN information on the Agent Host.
3	Click on the name of one LUN; all of the detailed information will be shown in the table on the right. **Note** If the LUN has not been saved as a Physical Device, a special icon will be shown next to the LUN's name.

Device Manager

Overview

Device Manager allows administrators to configure logical devices for backup jobs and archive jobs. There are five kinds of logical devices (Local, Network, LUN, CIFS, Share/SnapLock).

Note

For each logical device type, multiple physical devices can be defined. Once a physical device from the top of the physical devices list is full, data will automatically be written to the next physical device with enough free space.

The SharePoint databases and SharePoint index are stored in the storage system as Snapshot copies, but the following data is stored on the physical device:

- Job metadata
- Backup index
- SharePoint component properties
- SharePoint solutions
- SharePoint front-end resources

As the index is frequently accessed, it is recommended to store the index data on a separate drive, typically a LUN to increase the access speed.

Data from Archiver and Extender are stored in Archive type devices. The index and data are stored separately in Archived Index and Archived Data devices respectively. No default devices are created for Archiver and Extender data. They must be configured in Device Manager first before using Archiver or Extender.

Multiple CIFS share devices may be required when the data volume hosting the archived data is not large enough or cannot be easily expanded. Likewise, you may configure multiple media servers if some web applications have large user loads. After configuring multiple media servers, SMSP will perform better than when a dedicated media server is used.

When planning Archive storage, it is recommended to use separate volumes for easier disaster recovery. In addition, the following needs to be taken into consideration:

For the Archiver module, including end-user archiver, after you specify a logical device for a web application in an archiver plan, the data from the web application is stored in the same logical device only. This cannot be changed further. Several web applications can be specified to use the same logical device. For Extender module, data from one site collection (or one content database in RBS) is stored on the same logical device. Like with Archiver, once the relationship between archived content and its Logical Device is established, it cannot be changed.

Note

The space minimum for the physical device is 1G, and the SMSP Manager checks the space of the physical device every 30 minutes. When there is no free space in the device, you can enlarge the device space. If you enlarged the device space and want to reuse the device immediately, select the device in **Device Manager** and save it again; otherwise, the device will be reused after the checking.

VMDK Disk

SnapManager now also supports VMDK disks. Its behavior will be the same as is LUNs to SnapManager, except that SnapVault integration is not supported on VMDK disks.

In the following sections, all the areas that mention LUN will also apply to VMDK disks. For more information about VMDK disk, refer to *SnapDrive Installation and Administration Guide.*

Multi-Tenant vs. Devices

For all device types, the association between physical devices and SharePoint farms can be specified to allow flexible control over where each tenant's data is stored. In this case, **Allow all farms use this device** checkbox can be unchecked, and then define the association.

Creating a Local Physical Device

To create a local physical device, complete the following steps:

Step	Action
1	Select **Local** in **Data Type** drop-down box and click **Add** in the **Physical Device** column.
2	Input a name for the new physical device in the **Physical Device** text box on the right.

Step	Action
3	Input a valid path in the **Path** text box. **Note** If the path does not exist in the system, Device Manager will create the path automatically. For example, if the backup path is set to **d:\backupdata** and there is no **backupdata** folder on the **d:** drive, the folder will be created automatically after the physical device is added to a logical device, and the configuration is saved.
4	Click **Save** in the pop up to save the configuration and click **Cancel** to cancel it.

Creating a Logical Device

To create a logical device, complete the following steps:

Step	Action
1	Click **New** and select **Local in Data Type** drop-down box.
2	Input a name for the new logical device in the **Logical Device Name** text box in the middle.
3	In the **Physical Device** tab, drag at least one physical device in the **Physical Device** column to the blank area below. Multiple types of physical devices can be added here. If you want to add another type of physical device, select the corresponding type in the **Data Type** drop-down box and drag the specified physical device(s) to the blank area below. **Note** The Index storing type physical device and the Data storing type physical device both need to be specified for the logical device.

Step	Action
4	In the **Media Service** tab, drag one media service in the **Media Service** column to the blank area below. In the **Media Service** column, you can perform the operations below: ● Click the ⓘ icon next to the media service and the detailed information of the media service will be shown in a pop up window. ● Click the **Download** button next to Export Media Service configuration to download the detailed information of Media Service configuration for viewing. Click **OK** to close the pop up.
5	Click **Test** on the bottom of the screen to test the new logical device. If the information set is valid, a dialog box will display to confirm that the test was successful.
6	Click **Save** to save the profile for the new logical device. It will now be listed under the **Logical Device** column.

Creating a Network Physical Device

The Device Manager can also use a network path to build a network drive to any UNC path accessible from SnapManager for SharePoint Manager.

To create a network physical device, complete the following steps.

Step	Action
1	Select **Network** in **Data Type** drop-down box and click **Add** in **Physical Device** column.
2	Input a name for the new physical device in the **Physical Device** text box on the right.
3	Enter a UNC path in the following format: **\\<server>\<share>\<path>** in **UNC Path** text box. **Note** The specified path needs to exist already; a new path cannot be created automatically.

Step	Action
4	Input the domain, username, and password to set up access to the network path.
5	Click **Save** in the pop up to save the configuration and click **Cancel** to cancel it.

Creating a Logical Device

To create a logical device, complete the following steps:

Step	Action
1	Click **New** and select **Network** in **Data Type** drop-down box.
2	Input a name for the new logical device in the **Logical Device Name** text box in the middle.
3	In the **Physical Device** tab, drag at least one physical device in the **Physical Device** column to the blank area below. Multiple types of physical devices can be added here. If you want to add another type of physical device, select the corresponding type in the **Data Type** drop-down box and drag the specified physical device(s) to the blank area below. **Note** The Index storing type physical device and the Data storing type physical device both need to be specified for the logical device.
4	In the **Media Service** tab, drag at least one media service in the **Media Service** column to the blank area below. In the **Media Service** column, you can perform the operations below: ● Click the ⓘ icon next to the media service and the detailed information of the media service will be shown in a pop up window. ● Click the **Download** button next to Export Media Service configuration to download the detailed information of Media Service configuration for viewing. Click **OK** to close the pop up.

Step	Action
5	Click **Test** on the bottom of the screen to test the new logical device. If the information set is valid, a dialog box will display to confirm that the test was successful.
6	Click **Save** to save the profile for the new logical device. It will now be listed under the **Logical Device** column.

Creating a LUN Physical Device

To create a LUN physical device, complete the following steps:

Step	Action
1	Select **LUN** in **Data Type** drop-down box.
2	Switch to the **Media Service** tab and drag one media service in the **Media Service** column to the blank area below.
3	Click **Add** in **Physical Device** column.
4	Input a name for the new physical device in the **Physical Device** text box on the right.
5	In **For Storing** field, check the corresponding **Data/Index** checkbox to specify whether the physical device will save the Archived Data/Archived Index. **Note** The Data Physical Device is for storing Archived data and the Index Physical Device is for storing the Archiver index, the Archiver full text index and the Extender index. They are not available for Data Protection.
6	Select a LUN from the **LUN** drop-down list. The **Total Size** and **Free Space** will be shown in the corresponding fields below. **Note** If the LUN of the path you entered has SnapMirror enabled, SnapManager for SharePoint will automatically update the SnapMirror according to the corresponding settings of each module after finishing the job.

Step	Action
7	Click **Save** in the pop up to save the configuration and click **Cancel** to cancel it.

Note

In order to list LUNs in the Device Manager configuration, SnapDrive needs to be installed on the server where SMSP Media Service is installed. Preferably you should use a LUN with SnapMirror enabled. This automatically replicates all related data to the SnapMirror target site for disaster recovery (DR) situations. If you use a regular storage location or UNC path without SnapMirror enabled, you will have to move the backup data to a remote site manually for DR protection. For more information about SnapDrive and SnapMirror, refer to *SnapDrive® for Windows® Installation and Administration Guide* and *Data ONTAP® Documentation Operations Manager Help* or *N Series Management Console online Help.*

Creating a Logical Device

To create a logical device, complete the following steps:

Step	Action
1	Click **New** and select *LUN* in *Data Type* drop-down box.
2	Input a name for the new logical device in the **Logical Device Name** text box in the middle.
3	In the **Physical Device** tab, drag at least one physical device in the **Physical Device** column to the blank area below. Multiple types of physical devices can be added here. If you want to add another type of physical device, select the corresponding type in the **Data Type** drop-down box and drag the specified physical device(s) to the blank area below. **Note** The Index storing type physical device and the Data storing type physical device both need to be specified for the logical device.

Step	Action
4	In the **Media Service** tab, the specified media service will be automatically added to the blank area below. In the **Media Service** column, you can perform the operations below: ● Click the ℹ icon next to the media service and the detailed information of the media service will be shown in a pop up window. ● Click the **Download** button next to Export Media Service configuration to download the detailed information of Media Service configuration for viewing. Click **OK** to close the pop up.
5	Click **Test** on the bottom of the screen to test the new logical device. If the information set is valid, a dialog box will display to confirm that the test was successful.
6	Click **Save** to save the profile for the new logical device. It will now be listed under the **Logical Device** column.

Creating a CIFS Share Physical Device

To create a CIFS Share physical device, complete the following steps:

Note

In order to use CIFS Shares, they must be configured on the storage system first. Refer to the Data ONTAP user guide for details.

Step	Action
1	Select **CIFS Share** in **Data Type** drop-down box and click **Add** in **Physical Device** column.
2	Input a name for the new physical device in the **Physical Device** text box on the right.

Step	Action
3	In **For Storing** field, check the corresponding **Data/Index** checkbox to specify whether the physical device will save the Archived Data/Archived Index. **Note** The Data Physical Device is for storing Archived data and the Index Physical Device is for storing the Archiver index, the Archiver full text index and the Extender index. They are not available for Data Protection.
4	Select the **Filer** profile from the **Filer** drop-down list. **Note** You need to set up the Storage System in the Data Management module first.
5	Select a **Share** from the **Share Name** drop-down list. After a Share is selected, the **UNC Path** field will display the Share's UNC path. **Note** For **Total Size** and **Free Space** fields, they will display the corresponding detailed information after the configuration of the physical device is saved and reloaded by clicking the **Edit** icon in **Physical Device** column.
6	Enter the **Username** and **Password** into the provided fields.
7	Click **Save** in the pop up to save the configuration and click **Cancel** to cancel it.

Creating a Logical Device

To create a logical device, complete the following steps:

Step	Action
1	Click **New** and select **CIFS Share in Data Type** drop-down box.

Step	Action
2	Input a name for the new logical device in the **Logical Device Name** text box in the middle.
3	In the **Physical Device** tab, drag at least one physical device in the **Physical Device** column to the blank area below. Multiple types of physical devices can be added here. If you want to add another type of physical device, select the corresponding type in the **Data Type** drop-down box and drag the specified physical device(s) to the blank area below. **Note** The Index storing type physical device and the Data storing type physical device both need to be specified for the logical device.
4	In the **Media Service** tab, drag at least one media service in the **Media Service** column to the blank area below. In the **Media Service** column, you can perform the operations below: ● Click the ℹ icon next to the media service and the detailed information of the media service will be shown in a pop up window. ● Click the **Download** button next to Export Media Service configuration to download the detailed information of Media Service configuration for viewing. Click **OK** to close the pop up.
5	Click **Test** on the bottom of the screen to test the new logical device. If the information set is valid, a dialog box will display to confirm that the test was successful.
6	Click **Save** to save the profile for the new logical device. It will now be listed under the **Logical Device** column.

Creating a SnapLock Physical Device

To create a SnapLock physical device, complete the following steps:

Step	Action
1	Select **SnapLock** in **Data Type** drop-down box and click **Add** in **Physical Device** column.
2	Input a name for the new physical device in the **Physical Device** text box on the right.
3	In **For Storing** field, the **Data** checkbox is checked by default and the configuration cannot be changed. **Note** The Data Physical Device is for storing Archived Data.
4	Select the Filer profile from the **Filer** drop-down list. **Note** You need to set up the Storage System in the Data Management module first.
5	Select a **Share** from the **Share Name** drop-down list. After a Share is selected, the **UNC Path** field will display the Share's UNC path. **Note** The **Type** field will display the type of the SnapLock Volume. For **Total Size** and **Free Space** fields, they will display the corresponding detailed information after the configuration of the physical device is saved and reloaded by click **Edit** icon in **Physical Device** column.
6	Enter the **Username** and **Password** into the provided fields.
7	Click **Save** in the pop up to save the configuration and click **Cancel** to cancel it.

Note

In order to use SnapLock devices, they must be configured on your storage system first. Refer to the *Data ONTAP User Guide* for details.

Note
The source of the SnapLock devices on your storage system is SnapLock enabled.

Creating a Logical Device

To create a logical device, complete the following steps:

Step	Action
1	Click **New** and select **SnapLock** in **Data Type** drop-down box.
2	Input a name for the new logical device in the **Logical Device Name** text box in the middle.
3	In the **Physical Device** tab, drag at least one physical device in the **Physical Device** column to the blank area below. Multiple types of physical devices can be added here. If you want to add another type of physical device, select the corresponding type in the **Data Type** drop-down box and drag the specified physical device(s) to the blank area below. **Note** The Index storing type physical device and the Data storing type physical device both need to be specified for the logical device.
4	In the **Media Service** tab, drag at least one media service in the **Media Service** column to the blank area below. In the **Media Service** column, you can perform the operations below: ● Click the ℹ icon next to the media service and the detailed information of the media service will be shown in a pop up window. ● Click the **Download** button next to Export Media Service configuration to download the detailed information of Media Service configuration for viewing. Click **OK** to close the pop up.
5	Click **Test** on the bottom of the screen to test the new logical device. If the information set is valid, a dialog box will display to confirm that the test was successful.

Step	Action
6	Click **Save** to save the profile for the new logical device. It will now be listed under the **Logical Device** column.

Deleting a Device

- **Delete a Physical Device**

  To delete a physical device from a logical device, click the **Edit** icon of the corresponding logical device in the **Logical Device** list, and click the red ✕ in the **Physical Device** tab to remove it.

  A prompt message will pop up indicating that the physical device to be deleted is currently being used by the corresponding logical device. Make sure the data in the physical device is not being used currently before deleting it.

  There must always be at least one physical device in the **Physical Device** tab of a logical device.

Note

When deleting a physical device, only the link between the physical device and the logical device is removed; the **actual data is not deleted** and can be restored at a later time by recreating the physical device and add it to the original logical device.

- **Delete a Logical Device**

  To delete a logical device, click the red ✕ following the corresponding logical device in the logical device column.

Note

If the corresponding logical device you are deleting is used by the Data Protection or Storage Optimization module, a warning message is displayed.

Data Retention

About Data Retention

The Data Retention component of SnapManager for SharePoint enables you to define data retention and expiration policies.

There are two kinds of data retention policies: **backup data** retention, and **archived data** retention. The backup data retention policies are a method of pruning old backup data to make room for new backups, and a Backup Data Retention Rule specifies the number of backup process cycles that trigger data pruning as well as the number of backup sets to keep of a given backup management group.

The archived data retention policies are a method of pruning the old archived data to make room for new archived data, and an Archived Data Retention Rule specifies the retention time to keep of the archived data in the given interval for one archiver plan.

The retention policy works together with the retention setting in the SnapLock device. When the archived data is stored in the SnapLock device, they work together using the following rules:

- If the SMSP retention time is shorter than the shortest default retention time of SnapLock device, the retention time of the archived data will be the smallest default retention time of SnapLock device.
- If the SMSP retention time is longer than the longest default retention time of SnapLock device, the retention time of the archived data will be the longest default retention time of SnapLock device.
- If the SMSP retention time is in the range of the shortest default retention time of SnapLock device and longest time of default retention time of SnapLock device, the retention time of the archived data will be the SMSP retention time configured.

Specifying a Backup Data Retention Rule

To specify a **Backup** data retention rule, complete the following steps:

Step	Action
1	In the **Data Retention** tab, enter a data retention **Profile Name** in the field provided.

Step	Action
2	Select the type of backup management group to prune from the drop-down box.
3	Select the number of backups to trigger the data pruning: **In excess of ___ backups, and/or older than ___ days**. For example, if you set the backup management group as `Weekly` and data retention rule to `In excess of 2 backups`, only the two newest backup sets of type `Weekly` will be kept. If you set the data retention rule to `older than 2 days`, only the `weekly` type data backed up in the latest two days will be kept.
4	Click **Save**, located on the bottom of the screen. The profile now appears on the right-side of the screen. You can click the title of this profile later to modify it, or use the red ✖ button to delete it.
5	After saving your data retention rule, you can select it from the **Data Protection Plan Builder**.

Specifying an Archived Data Retention Rule

To specify an **Archived** data retention rule, complete the following steps:

Step	Action
1	Within the **Archived Data Retention** tab, enter an **Archived retention Profile Name** in the field provided.
2	Enter the time to run before data retention begins to prune data. To delete the stubs when pruning data, select the **Delete stub when retention is reached** option.
3	Click **Save**. The profile appears on the right side of the screen. You can click the title of this profile later to modify it, or use the red ✖ button to delete it.
4	After saving your data retention rule, you can select it from the Archiver Plan Builder module.

Archived Data Retention vs. Orphan Retention

The data retention policy is a method of pruning old data to make room for new data, and by default is not applied for any Archiver or Extender plan.

The orphan retention policies, or stub restore policies, are a method of pruning data whose stub does not exist anymore after a specified time. For example, if the delay time is set to 6 months, after the first time a stub is found to be deleted in SharePoint, the stub is marked and archived from SharePoint. If the file is not accessed or the stub is not restored in 6 months, the data will be deleted.

For Extender, deleting extended data from SharePoint actually deletes the stub (once the SharePoint Recycle Bin is emptied). The BLOB remains in storage for a duration that is dependent upon Extender’s Delete Stub Policy. If the Delete Stub Policy is configured to run on a schedule and is enabled for the corresponding web application, then the orphan BLOB is deleted from storage once the specified retention duration expires.

Note

It is recommended to set the Backup retention shorter than the Archiver orphan retention length, and to set the Archiver orphan retention shorter than the Archiver retention.

Verification and Index

Defining a Verification Server

A verification server is a SQL server which is used to run database verification or run backup indexing.

You can define a Verification Server to be used in Backup Builder Module or Restore Controller Module for verifying SQL databases using SnapManager for SQL Server.

To create a Verification and Index profile, complete the following steps:

Step	Action
1	Enter a **Profile Name** in the space provided at the top of the **Verification and Index** interface.
2	Input a SQL Server to be used as a Verification Server in the **Server Name** field. **Note** SnapManager for SQL Server must be installed on this SQL Server and the SQL virtual server should not be used in a Microsoft Cluster Service (MSCS) environment.
3	Select an authentication mode from the corresponding drop-down list. You can select either Windows Authentication or SQL Server Authentication. If you select the SQL Server Authentication option, enter the username and the password of the SQL Server in the corresponding fields.
4	You can deselect the **Allow all farms to use this verification server** checkbox to choose the farms you want to use this verification server.
5	Click **Save** to save the profile.

After saving your verification and index rule, you can select it from the verification server section of the Backup Builder and Restore Controller modules.

You can edit pre-existing profiles by clicking the name on the right-side of the screen. After editing any information, click **Save** to save the changes. You can also delete a pre-existing profile by using the red ❌ button next to the name in the profile list.

Storage System

About Storage System

The Storage System component of SnapManager for SharePoint enables you to configure the information for connection to an N series storage system. It is used when configuring a device of CIFS share. If SnapMirror is configured for the volumes hosting archive data, profiles for the SnapMirror destination storage systems must be created. Otherwise SnapMirror update will fail.

Configuring a Storage System

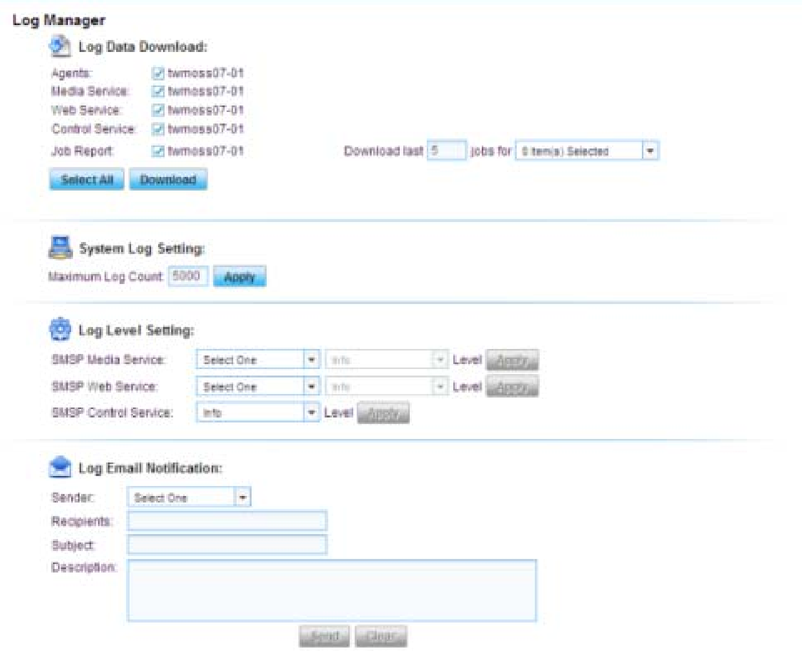
To configure a storage system, complete the following steps:

Step	Action
1	Enter a profile name into the provided field.
2	Specify the storage system name or IP address you want to connect to. **Note** If you specify a Storage System name, make sure the SMSP Manager can connect the machine by the specified name. **Note** If you are using ONTAP 8.1 c mode, enter the cluster management IP in the **Storage System** text box.
3	Select the connection type for the Storage System in the **Connection Type** drop-down list. By default, the connection type is **HTTP**.
4	Enter the username, password, and the port number to set up access to the storage system, this account must have access to the storage system console. If you want to use the RPC, the username and password should be the username and the password of the storage system administrator.
5	Click the **Save** button to keep the configuration. The configuration will now be displayed in the **Profile** panel.

Log Manager

About Log Manager

SnapManager for SharePoint Log Manager provides several options for managing the logs associated with SnapManager for SharePoint components. Logs are stored as:



Log Manager

Log Data Download:

Agents: ☑ twmoss07-01
Media Service: ☑ twmoss07-01
Web Service: ☑ twmoss07-01
Control Service: ☑ twmoss07-01
Job Report: ☑ twmoss07-01

Download last 5 jobs for 0 item(s) Selected

System Log Setting:

Maximum Log Count: 5000

Log Level Setting:

SMSP Media Service: Select One Info Level
SMSP Web Service: Select One Info Level
SMSP Control Service: Info Level

Log Email Notification:

Sender: Select One
Recipients:
Subject:
Description:

System logs: These include all actions performed under SnapManager for SharePoint Manager services. These are stored in the internal Manager databases and can be viewed from **Job Monitor** > **Log Viewer**.

Manager logs: Detailed log files of each Manager service are stored on the Manager machine.

Agent logs: Detailed logs of each Agent are stored on the Agent machine’s event viewer called SMSP.

You can set the amount of logs to record from the **Log Level Setting** dialog box and the number of system log entries to retain from the **System Log Setting** panel. Additionally, you can send these logs from the **E-mail Notification Settings** panel.

Downloading Logs

Log Data Download is used to centrally download logs from multiple SnapManager for SharePoint components, including the Control, Media, and Web services, as well as any Agents. Select all agents or services that you require logs from and click **Download**. You can save the consolidated zip file to any destination you choose. To limit the job numbers and job type you want to download in the report by setting up the corresponding value. By default, all the items are selected.

Note

The logs related to the SQL exceptions are stored in the installation path of the Agent, which is <...\IBM\SnapManager for SharePoint\VaultClient\data\logs> by default. The log files will also be downloaded when clicking the **Download** button.

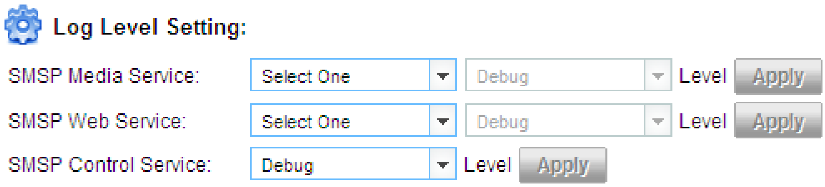
Pruning Logs with System Log Settings

System Log Setting is used to specify the maximum Log count for the SnapManager for SharePoint system log to keep on the system. By default, 5000 log entries are kept, but you can change this number and click **Apply** to create alternate settings. If the specified value is smaller than the current log size, all older log messages are pruned.

Setting Log Levels

Log Level Settings are used to set log levels for log recording for the following services:

- SnapManager for SharePoint Web Service
- SnapManager for SharePoint Media Service
- SnapManager for SharePoint Control Service



Log Level Setting:

SMSP Media Service: Select One | Debug Level Apply

SMSP Web Service: Select One | Debug Level Apply

SMSP Control Service: Debug Level Apply

To make these changes, choose one of the services from the drop-down list and the appropriate log level setting (either **Debug**, **Info**, **Warning**, **Error**, or **Fatal**). Click **Apply** to save your changes. Because there is only one Control Service, you do not need to select a service to apply the new settings.

Note

To change the log level of an Agent, use the **Agent** configuration page in the Agent Monitor.

Setting up E-mail Notifications

You can use **E-mail Notification Settings** to send the logs to a specified recipient directly from the GUI. You can also add a subject or write a description for the log.

E-mail Notification

Overview

The E-mail Notification manager enables you to create various e-mail profiles containing different mailing lists. Backup plans can then be configured to e-mail different profiles for errors, success, or warning conditions. This enables you to effectively control which personnel gets notified under which conditions.

E-mail Notification also enables you to specify what is reported, from simple summary reports to detailed URL-specific reports. The e-mail report sent out from SnapManager for SharePoint displays the backup status and the reason for failure if the backup job fails.

Configuring a General Mailing List Profile

To configure a general mailing list profile, complete the following steps:

Step	Action
1	Input the e-mail notification name.
2	Select the **General** option for the **Notification Type**.
3	Enter your SMTP server addresses.
4	Select the **Secure Password Authentication** option if you require this for your e-mail account configuration.
5	Specify a port. The default port is 25.
6	Enter the e-mail address you want to use as the source of the e-mail notifications in the **Sender** field, as well as the login credentials for this address (username, password, confirm password.) Select the SSL **Authentication** option according to your e-mail settings.

Step	Action
7	Enter the e-mail recipients under the **Summary Report Recipients** and **Detailed Report Recipients.** **Note** Multiple recipients can be added to the recipient text box, separated by a semicolon.
8	Select a notification level for both **Summary Report Notification Level** and **Detailed Report Notification Level**: either **All Levels**, **Success**, **Failure**, **Warning** or **Skipped**. Depending on the results of each job, these reports are sent out according to the levels set here. **Note** Notification levels can be customized by profile. For instance, you might want a specific person or group of people to only receive reports for backups that have failed. You can manage this by adding a new e-mail notification for each person or group based on your needs.
9	Select the format in which the message will be delivered: **HTML** or **Plain Text**.
10	Select the **Send All Logs to Recipient** checkbox if you want to see all error logs when a job has failed. These are not included for successful jobs.
11	Select the **Allow all farms use this e-mail notification** checkbox if you want to apply it for all farms. Or else, a window will pop up, and then you can select the farms you wish to use this e-mail notification.
12	Select the **Customize E-mail Template** checkbox if you wish to create/edit the e-mail you received from SnapManager with the current status of Backup/Restore and others.

Step	Action
13	Click the **Test** button to ensure that your notification profile is configured properly. All e-mail recipients entered in the **Summary** and **Detailed Report** fields will receive a test message from the e-mail address specified in the **Sender** field.
14	Click **Save As**, create a notification name for this profile, and click **OK**. The new profile is added to the list on the right of the screen. All e-mail notification profiles are selectable from the Backup Builder module.
15	To modify a profile, click the name of the profile in the list on the left and modify the fields on the right. After you finish your modifications, click **Save**. If you want to clear the configuration, click **Clear**.

Configuring a Service Status E-mail Notification

Service Status E-mail Notification is used to send an e-mail automatically when any services (except Control Service) are down.

To configure a Service Status E-mail Notification, complete the following steps:

Step	Action
1	Input the **Service Status E-mail Notification** name.
2	Select **Service Status** option from the **Notification Type**.
3	Enter your SMTP Server address.
4	Select the **Secure Password Authentication** option if you set up this option in your E-mail Account Configuration.
5	Specify a port. The default port is 25.

Step	Action
6	Enter the e-mail address you want to use as the source of the e-mail notifications in the **Sender** field, as well as the login credentials for this address (username, password, confirm password) in the applicable fields. Select the **SSL Authentication** option according to your e-mail setting.
7	Enter the e-mail recipients under the **Summary Report Recipients** and **Detailed Report Recipients**. **Note** Multiple recipients can be added to the recipient text box, separated by a semicolon.
8	Select the format in which the message will be delivered: **HTML** or **Plain Text**.
9	Select the **Send All Logs to Recipient** checkbox if you want to see all error logs when a job has failed. These are not included for successful jobs.
10	Click the **Test** button to ensure that your notification profile is configured properly. All e-mail recipients entered in the **Summary** and **Detailed Report** fields receive a test message from the e-mail address you specified in the **Sender** field.
11	Click **Save As**, create a notification name for this profile, and click **OK**. The new profile is added to the list on the right side of the screen. All e-mail notification profiles are selectable from the Backup Builder module.
12	To modify a profile, click the name of the profile in the list on the left and modify the fields on the right. After you finish your modifications, click **Save**. If you want to clear the configuration, click **Clear**.

AutoSupport Settings

About AutoSupport Settings

The AutoSupport feature of SnapManager for SharePoint allows SnapManager operational details to be logged in specified storage systems, as well as optionally sending AutoSupport messages.

Enabling AutoSupport

To enable AutoSupport, complete the following steps:

Step	Action
1	Check the **Log SnapManager events to storage system syslog** option.
2	Select the **Filer** profile from the drop-down list. **Note** To enable the AutoSupport on storage system, you need to set up the Storage System in the Data Management module first.
3	If you want to send AutoSupport alerts, select the **Send AutoSupport Notification** option. Select the **On failure only** option to only send the alert when SnapManager operations fail.
4	Click the **Apply** button to save the settings.

System Center Operations Manager Settings

About SCOM Settings

SCOM Settings can be configured to send SnapManager operational details to the System Center Operations Manager (SCOM) as event logs.

Required Permissions for SCOM integration

- The AD account specified in Manager configuration tool will be used for SCOM integration. This account must be the DB Owner for SCOM DB.
- The status of OpsMgr SDK Service on SCOM Server(2007 SP1) must be Started.

Enabling SCOM Settings

To enable the SCOM integration, complete the following steps:

Step	Action
1	Select the **Enable System Center Operations Manager (SCOM) Integration** checkbox. Enter in the SCOM Servername, Localhost Full Name, Event Source Name, Records Per Sync, and the Log Level as described below. **SCOM Server Name:** The full computer name of your SCOM Server. **Localhost Full Name:** This is the full computer name of the machine that has the SMSP Web Server and must have the SCOM client installed (which will communicate with the SCOM server.) **Event Source Name:** Identifier for the SCOM event source; this field can be filled in with any name. **Records per Sync:** The number of records that the SCOM client will wait to collect before sending to the server. This number can range from 10 records to 100 records. The lower the number, the slower the performance as the client will use resources sending more lines of log individually to the SCOM server. **Log Level:** Set to **warning**, **error** or **info** according to your preference.

Step	Action
2	After entering the configuration information, click **Test.** You will receive a **Complete** message if SMSP can connect to the SCOM server successfully.
3	Click the **Apply** button to save the settings.

Microsoft Operations Manager Settings

About MOM Settings

MOM Settings can be integrated for users who make use of the Microsoft Operations Manager (MOM).

Required Permissions for MOM integration

The user account entered in the manager configuration tool must be the IIS (MOM Site) pool user or Local admin.

Enabling MOM Settings

You can enable the MOM integration from **Reporting**, on the **MOM Logging Settings** tab in the **Control Panel**.

Step	Action
1	Select the **Enable Microsoft Operations Manager (MOM) Integration** checkbox. Enter in the MOM Server name, MOM Port Number, MOM Connection Name, Resolution State ID, Alert Name, Records Per Sync, and Log level as described below. **MOM Server:** The full computer name of your MOM Server or IP address. **MOM Port Number:** The TCP port number of MOM connection in IIS services manager. **MOM Connection Name:** A connection with MOM server with the specified name will be created. This name must be unique. **Resolution State ID:** A resolution state ID which had not been occupied. **Alert Name:** The log with the specified name will be sent to MOM server. **Records Per Sync:** The number of records that the MOM server will wait to collect before sending to the server. This number can range from 10 records to 100 records. The lower the number, the slower the performance as the client will use resources sending more lines of log individually to the MOM server. **Log Level:** Set to **Debug**, **Error**, **Fatal**, **warning**, **error** or **info** according to your preference.
2	After entering the configuration information, click **Test.** You will receive a **Complete** message if SMSP can connect to the MOM server successfully.
3	Click the **Apply** button to save the settings.

After entering the configuration information, click the **Test Now** button. You will receive a **Complete** message if SMSP connects to the MOM server successfully.

License Manager

Overview

SnapManager for SharePoint License Manager controls the license that is in use by SnapManager for SharePoint. The license controls the available length of usage time for different SnapManager features. Demo licenses expire in 60 days. Applying a full enterprise edition license to a SnapManager for SharePoint Demo Package installation converts it into the full enterprise edition without any time limit.

Viewing Current License Information

To view the permissions granted in the current license, open the **License Manager** under **Control Panel**. View the licensing information by selecting the various features and solutions which SnapManager for SharePoint provides from the list on the left of the interface.

Creation Date: The date when the license was created.

Applied Date: The date when the license was applied. This is either the first day you installed SnapManager for SharePoint, or the first day you applied the license in License Manager.

Expiration Date: The date when the license will expire. If the license you have applied is an enterprise license, it will display as **Unlimited**.

Note

SnapManager will prompt you with a pop-up window if the license is about to expire or when the license has expired. If you do not want to see the window again, check the **Do not remind me again** check box in the pop-up and click **OK**.

Quantity (Agents): The number of the agents whose status is not **Disabled** or **Uninstalled** for the corresponding module. For the Backup module, it is the number of member agents.

Applying a License File

To apply a license file, complete the following steps:

Step	Action
1	Click **Browse** and locate the license file you want to import.

Step	Action
2	Click **Apply** to load the selected license file.
3	For the license update to take effect, you must relogin to the SnapManager for SharePoint interface.

Data Protection - Backup Builder 10

Overview of Backup

SnapManager for SharePoint can perform full SharePoint farm-level backups and restore different levels of SharePoint components from a single document version up to the contents of entire farm.

The SharePoint components covered are (including both SharePoint 2007 and SharePoint 2010):

- All SharePoint databases
- Project Server databases (for SharePoint 2007 only)
- SharePoint search index
- SharePoint components and settings (see "SharePoint Components" on page 138)
- SharePoint solutions
- SharePoint front-end resources (including IIS settings, SharePoint hive and Global Assembly Cache)

SnapManager for Microsoft SQL Server is used to perform database Snapshot backups; SnapDrive is used to perform Snapshot backups of the search index. Backup data of other SharePoint components is sent to the SnapManager for SharePoint Media Service, and is stored together with backup job metadata and index. For more information about SnapManager for Microsoft SQL Server, refer to *SnapManager for Microsoft SQL Server Installation and Administration Guide.*

For disaster recovery purposes, this backup data can be replicated to a SnapMirror destination volume automatically. See "Disaster Recovery" on page 165 for more information. For longer retention of the backup data, database backups can be archived to a SnapVault destination when Protection Manager is configured for SnapManager for Microsoft SQL Server.

Required Permissions for backup job

To run a backup job, the following permissions are required:

- Administrator for operating system
- Query permission for registration table (HKEY_LOCAL_MACHINE)
- Sysadmin and DB Owner for SQL Server and Farm Administrator for SharePoint Farm
- Local administrator for the server with SQL Server installed

You can click the **Test Run** button to check the permissions after saving the backup plan. You can view the detailed information in Job Monitor.

General Actions

In SnapManager for SharePoint **Backup Builder**, you can perform the following actions:

- Set up scheduled or immediate backups for any SharePoint environment (as long as SnapManager for SharePoint Agents are installed)
- Select data retention profiles created in the **Control Panel's Backup Data Retention** tab.
- Select e-mail notifications created in the **Control Panel's E-mail Notification** manager
- Choose a designated SnapManager logical device to manage backup work
- Monitor real-time progress of any backup or restore jobs (through the Job Monitor)

Plan Options

SnapManager performs the backup using backup plans, where each backup plan allows you to specify the following:

- What SharePoint components to back up through a tree view of the farm
- When to perform backups (up to six schedules can be customized per plan)
- Where to store backup data (through Media Services, which then writes data to the designated network: NAS, SAN, local disk drives, or CIFS)
- How to handle backing up data in terms of data retention or restore granularity level

Note

By using the Snapshot technology, SnapManager backup plans do not lock up the SharePoint SQL database and index files, and therefore can be scheduled to run during normal production hours.

Note

When browsing the Farm tree, the product will check the Agent version. If the Agent version is lower than the Manager version, the Agent will be treated as an unavailable Agent and the corresponding data cannot be loaded. To check the version of Agent or Manager, navigate to **Control Panel** > **SMSP Services** > **Control Service**. Check the **Manager** version on the **Server Monitor** tab and **Agent** version on the **Agent Monitor** tab.

Selecting Data to Back Up

To select the SharePoint data you wish to back up, open the Backup Builder and complete the following steps:

Step	Action
1	Select a farm in the **Farm** drop-down list and select an agent from the **Agent** drop-down list. Then expand the SharePoint farm tree.
2	Click the SnapManager for SharePoint **Agent name**. By default, the **Verify Storage Layout** option is selected, which means that the SnapManager for SharePoint tries to obtain information for all the database and search index components regarding storage from SnapManager for Microsoft SQL Server and SnapDrive, respectively. This process may take some time to complete depending on the number of databases on the SQL servers. When the **Verify Storage Layout** option is selected, the process will check the databases and index file; if they are not transferred to the LUN, a red cross appears in front of the database or index file. If this option is not selected, SnapManager will retrieve only the farm tree structure from SharePoint, which means that the farm tree loads faster. However, because the storage layout is unknown in this case, you must ensure that all the components are correctly configured on their respective LUN. A warning appears if a component with unknown storage layout is included in backup plan.

Step	Action
3	Click the **name** of the selected agent host. This expands the host to display the SharePoint farm structure, including the various SharePoint components such as Shared Services Provider (SSP), Web applications, content databases, Nintex Databases, FAST Search server (for SharePoint 2010 only) and front-end server resources. When loading the tree, SnapManager for SharePoint will check whether there is a default logical device. If there is no default logical device, the pop-up window will prompt **There is not an available logical device for this farm, you cannot save a profile for the backup plan, are you sure you want to continue?** Click **OK** to continue loading the tree or click **Cancel** to stop it. There is a checkbox corresponding to each SharePoint component on the Backup Builder tree. Selecting this box indicates that the component is to be included in the backup plan. Select the check boxes for the components to be included in this plan. **Note** For SharePoint 2007, it is supported to back up and restore Form-Based-Authentication (FBA) site. For SharePoint 2010, it is supported to back up and restore Claims-Based-Authentication (CBA) site.

Note

The selected databases and search index must be on an N series storage. If the storage layout for a selected component is unknown, the Verify Storage Layout option has not been selected, or the Manager failed to obtain its status, a dialog box displays reminding you that the selected component should be in a storage system.

Note

The Nintex database does not support the Restore Granularity Level setting. If you only select the Nintex database to back up, the Restore Granularity Level option will be grayed out and cannot be selected.

The Nintex Content database will be selected automatically if you select the Nintex Config database. You can uncheck it manually.

Note

If you want to back up a FAST Search server, you must install Member Agents on all of them.

If the Verify Storage Layout option is selected, certain icons are displayed to indicate the storage status, as shown in the following table.

Type	Database	Index
In LUN with SnapMirror and SnapVault enabled	🛢🛢	N/A
In LUN with SnapMirror enabled	🛢🛢	🔍
In LUN with SnapVault enabled	🛢	N/A
In LUN	🛢	🔍
Invalid, no database or index in LUN	🛢✗	🔍✗
Browse the tree without selecting the **Verify storage layout** option, or unknown error occurs while browsing	🛢?	🔍?
No Agent is installed, the database cannot be backed up	❗🛢	N/A

Configuring Additional Backup Options

When you are constructing a new backup plan, there are many options that can be configured. Some of the options available here should be configured ahead of time in the **Control Panel**.

To configure a backup plan, complete the following steps:

Step	Action
1	After you have selected the data to be backed up as described above, begin to configure the options in the next column to the right.
2	Specify a **Logical Device** from the drop-down box under the **Backup** tab. This contains a list of all Media Services that designate where the backup data is stored. For more information about configuring the location for backup data, see the Device Manager section within the **Control Panel**.
3	Select a **Data Retention rule** from the corresponding drop-down box. The Data Retention policies enable you to specify the pruning policy for the data generated by this backup plan. By picking a Data Retention profile, you can specify how long the data generated by this plan is kept on the disk. Specifying a Data Retention profile is optional but highly recommended. **Note** A SharePoint component can be saved in multiple backup plans, but the backup management group (Standard, Daily, and Weekly) must be different.
4	Select an **E-mail Notification profile** from the drop-down box. The **E-mail Notification** drop-down box contains a list of profiles that have been associated with both a sender and a list of recipients. These profiles are set in the **E-mail Notification** section within the **Control Panel**. Specifying an **E-mail Notification profile** is optional.

About Data Retention

Retention of backup data is configured based on the number of backups or the amount of time to keep backup data, and is automatically triggered when a backup job that triggers the preset criteria is completed.

When a retention policy is configured, SnapManager for SharePoint checks with SnapManager for Microsoft SQL Server to see if a local or remote copy of that Snapshot backup set still exists (the remote instance is only when SnapVault is used). If a copy of the backup data still exists, the metadata and index for this plan will not be deleted. In this way, you can always browse backup data and restore, even if local backups are deleted due to retention. After both the local and remote backups are deleted, the corresponding backup data information in SnapManager for SharePoint is deleted as well.

Retention of backup sets is dependent on a combination of databases. This can create problems when a backup set contains multiple databases. For example, suppose a backup set contains three databases db1, db2, and db3. The retention policy is configured to keep the three most recent backup sets (DbSet1, DbSet2, and DbSet3). Each time the three databases are backed up as a set, a new backup set (DbSet4) is created and the oldest backup set (DbSet1) is deleted.

However, if db2 is deleted, the next backup set contains only two databases (db1 and db3). As a result of this inconsistency, the retention policy, which automatically keeps only the three most recent backups and deletes the older ones, does not work. Therefore, to delete the older backups, you need to explicitly delete the backup data. This can be done by deleting the related backup jobs from Job Monitor, which deletes the backup job information as well as the Snapshot backup of the database and index.

For more information about the retention details when multiple databases are involved, see the *SnapManager for Microsoft SQL Server Installation and Administration Guide*.

Note

If you saved one database in two plans, you must specify two different retention rules for this database in these two plans.

Setting Up Backup Options

After selecting the components to be backed up and selecting any maintenance options you may need, you can determine when and at what frequency the backup job plan should run. You can select multiple schedules, accessed by cycling through the schedule clocks. Select the **Schedule** checkbox to activate a new schedule. An active schedule is highlighted in blue, and inactive schedules are highlighted in yellow.

There are several options available under the **Options** and **Advanced** tabs of the schedule:

Restore Granularity Level: Enables you to set the level of granularity you can restore. Choosing the **Item** or **Item Version** level enables you to restore individual files and file versions. Different restore granularity levels can be used in different schedules. Choosing the level of indexing is a trade-off between backup performances and restore granularity.

Note

Simultaneous backup jobs of different granularities of a single plan are not supported.

Defer indexing to maintenance jobs: If selected, the backup jobs will only backup the databases without generating a granular restore index. The granular restore index will be generated in backup maintenance jobs which can be scheduled at a later time.

Granularity Index Server: If you select **Site**, **Folder**, **Item**, or **Item Version** in **Restore Granularity Level**, this function will be available. The index will be created in the specified index server. Click the drop-down list and select the profile created in **Control Panel > Data Management > Verification and Index**. You can select **Assign Mount Point** to specify a Mount Point path. If you do not select this option, it will use the default Mount Point of SQL Server.

Verify Backup: If selected, the **Verify On Available SnapMirror Destination Volumes** and the **Verify Archive Backup On Secondary Storage** check boxes are activated. If your environment has SnapMirror enabled, you can select this option to verify both the data in the source and the data that is mirrored to the destination. Select a verification server from the drop-down list defined in the **Control Panel**. You can select **Assign Mount Point** to specify a Mount Point path of MS SQL to store the temporary LUN. If you do not select this option, it will use the default Mount Point Directory.

Update SnapMirror After Operation: If your environment has SnapMirror enabled for databases and the search index, you can select this option to automatically update the SnapMirror destination after backup. Only the default SnapMirror target is updated.

Archive Backup to Secondary Storage: If your environment has SnapVault enabled for databases, you can select this option to archive the backup data to the SnapVault storage system.

In SMSP version 6.1, only the Data Protection section is integrated with SnapVault and only the database nodes can support the SnapVault functions. Before you trigger the archive operations of SnapVault, the end user needs to verify that the SharePoint databases have been migrated to the LUNs configured for SnapVault. You can view the detailed information referring to *SnapDrive for*

Windows Installation and Administration Guide or *Data ONTAP Documentation Operations Manager Help*. You can find the guide on the N series support website (accessed and navigated as described in "Websites" on page xi). When backup completed, you can check it by SMSQL. The snapshot saved in SnapVault primary storage is called Local Backups and the one saved in SnapVault secondary storage is called Remote Backups.

When restoring SharePoint data, SnapManager will automatically check where the backup copy is located. If a local backup copy still exists, it will be used for restore. If only remote backup copy exists, restore will be performed from the remote backup (SnapVault). The restore from remote backup will be stream based. VMDK does not support SnapVault integration.

Run command with operation: If you select this option, the command profile that selected **Backup operation** in Control Panel will be listed in the drop-down list. The command will be run according to the command profile you selected.

Check old backups to be deleted: When this option is selected, the data retention process is triggered after the backup. By default, this option is selected. If SnapVault is used, it is possible that some backups cannot be deleted until their remote backups are deleted. In this case, the data retention process takes longer to complete and you can select this option only in certain backup schedules.

Run transaction log backup after full database backup: When this option is selected, the transaction log will be backed up after full database backup. By default, this option is selected.

Backup BLOB data for this farm: When this option is selected, the archived data in the entire farm will be backed up. This function is the same as the Archived Data Backup in the Archiver module. By default, it is not selected.

To set up a start time for you backups, complete the following steps:

Step	Action
1	Click the calendar icon next to the **Start Time** field. Use the calendar to specify when the backup should begin.
2	Specify the interval at which the backup occurs: **Only Once**, **By Hour**, **By Day, By Week**, **By Month**, or an **Advanced** schedule.
3	After successfully scheduling the time and frequency at which the backup plan should run, save the plan by clicking **Save**.

After the plan has been saved successfully, it is displayed in the column on the right. The plan will be executed according to the set schedule. You can edit these options later by clicking the plan name. You can also delete a plan by using the red ❌ sign next to the name.

To manually execute a scheduled plan at any time, click the **Backup Now** button. After you click the **Backup Now** button, a dialog box will appear, enabling you to configure further options.

Backup Maintenance

For large SharePoint environments, database verification and granular restore index generation during the backup job may create considerable overhead on the production environment and slow down the completion time for the backup job. You can select to perform data verification and index generation at a different time from the backup schedule.

To schedule backup maintenance jobs, complete the following steps:

Step	Action
1	Go to the **Backup Maintenance** tab to select the options to verify the backup data.
2	Select the **Index last ___ deferred indexing** option, and enter the number of the jobs you want to generate indexes for. This will generate indexes for the backup jobs with the **Defer Indexing to maintenance jobs** option. For example, setting this option to **Index last 3 deferred indexing** will generate the indexes for the latest three backup jobs whose status is deferred/failed/partly.
3	Select the **Verify Last...** option and enter a positive integer in the provided field to specify how many unverified backup jobs to verify. If SnapMirror or SnapVault is enabled, you can also select the V**erify On Available SnapMirror Destination Volumes** or the **Verify Archive Backup On Secondary Storage** check boxes.
4	Choose a **Verification Server** from the drop-down list. See the **Control Panel** section of this guide for instructions on defining a Verification Server.

Step	Action
5	If SnapMirror is enabled in your environment and you did not enable the SnapMirror update at backup time, you can use the **Update SnapMirror After Operation** option to trigger SnapMirror replication for the Snapshot backups of SharePoint databases and search index.
6	If SnapVault is enabled through Protection Manager in your environment and you did not select the archive backup option at backup time, you can use the **Archive Backup To Secondary Storage** option to archive the Snapshot backups of SharePoint databases to the SnapVault storage.
7	If you select **Run command with verification**, the command profile which selected **Verify operation** in Control Panel will be listed in the drop-down list. The command will be run according to the command profile you selected.
8	You can also set up a schedule for the verification by clearing the **No Schedule** checkbox. Using the calendar icon next to the **Start Time** field, select a date and time for the backup maintenance job to run. You can also set an interval for recurring rules based on **Only Once**, **Hourly**, **Daily**, **Weekly**, or **Monthly** schedules. If you want to run this job immediately, click the **Run Now** button.

Synchronizing the Farm Data

After the SharePoint farm structure is changed (that is new content databases are created), you can load the saved backup plan and click the **Sync Farm Data** button to show the latest SharePoint structure. You can then add these new components to the backup plan.

Note

Synchronizing the content of Front-End Web node is not supported, which means all the data in Front-End Web node cannot be synchronized.

Running a backup plan

After configuring the backup settings, click **Save** to save the settings. To run the plan immediately, click **Run now**. This will display a window; select a backup type, and then click **Run** to run this plan.

You can click **Go to The Job Report** to Job Monitor to view the job's process, or click **Close** to return in the pop-up window.

Note

The database errors reported from SMSQL while running backup plans are recorded in Job report and Agent logs.

Custom Backup CLI

SMSP Custom Backup supports the administrator to run the backup plan by using CLI (Command line Interface). Also refer to introduction of New-SMSPBackupJob command in "Run the Data Protection Backup Job Using CLI" on page 357.

You need to configure **SMSPCLI.bat** under the directory *IBM<\SnapManager for SharePoint \VaultServer\CLI\bin\>*.

To run a backup job, execute the following command:

backup -f agentHost -n planName -r restoreLevel

There are several settings you need to configure.

agentHost: The control agent host. At least one plan of this agent host was saved in the GUI.

planName: The plan name which you want to run, ensure the plan already is created in **Plan Builder**. If the plan name contains the space, quote the plan name by " ", or ' '.

restoreLevel: The restore Granularity level of the job.

restoreLevel = "1002" represents Site Collection

restoreLevel = "1003" represents Site

restoreLevel = "1004" represents Folder

restoreLevel = "1005" represents Item

restoreLevel = "1006" represents Item Version

After executing the command line, you can use the **SMSPDownloadLog.bat** under *IBM<\SnapManager for SharePoint \VaultServer\CLI\bin\>* to download the log.

To download the log, execute the following command:

SMSPDownloadLog [-f download path]

download path: The location you want to save the logs. If you leave it blank or the path is invalid, the file will be downloaded to *IBM*<*SnapManager for SharePoint* *VaultServer**CLI**bin*\>.

Backup of SharePoint Components

SharePoint Components

SnapManager for SharePoint can back up the following SharePoint 2007 components:

All SharePoint databases: The configuration database, central administrator content database, content databases, SSO database, SSP database, and search database are included. These databases are backed up by the SQL Member Agent using SnapManager for Microsoft SQL Server Snapshot backup.

Project Server database: This includes the Draft database, Published database, Archive database, and Reporting database.

SharePoint search index: This includes the OSearch index and SPSearch index. The search index files are backed up on Index Member Agent using SnapDrive Snapshot copies.

SharePoint components and settings: This includes Web applications, SSO, SSP, InfoPath Forms, and Global Search Settings. This data is backed up to the Logical Device specified in the backup plan, along with backup job data.

SharePoint solutions: This includes any SharePoint customizations deployed to SharePoint in the form of solutions. These solutions and their deployment statuses are backed up to the Logical Device specified in the backup plan.

Nintex databases: This includes Nintex workflow, config database, and content database.

SharePoint front-end resources: The front-end Member Agent backs up the IIS settings (both meta-data and files) and SharePoint hive files to the Logical Device specified in the backup plan.

Note

If SharePoint 2007 SSP and SPSearch are selected in Backup Builder and it is crawling, SnapManager for SharePoint will try to pause the crawler service. SnapManager for SharePoint includes a timeout period. If the crawler service is unavailable and cannot connect with SnapManager for SharePoint, the backup job will fail instead of hanging for an endless period of time. You can check the detailed job information in Job Monitor.

SnapManager for SharePoint can back up the following SharePoint2010 components:

All SharePoint databases: The configuration database, central administrator content database, content databases, State service database, Application Registry Service Database, Shared Service Application Database (from SnapManager 6.1 for SharePoint, PerformancePoint Service Application database is supported) and search database are included. These databases are backed up by the SQL Member Agent using SnapManager for Microsoft SQL Server Snapshot backup.

SharePoint search index: This includes the Server Search index and Foundation Search index. The search index files are backed up on Index Member Agent using SnapDrive Snapshot copies.

SharePoint components and settings: This includes Web applications, InfoPath Forms, State Service, Microsoft SharePoint Foundation Sandboxed Code Service, Microsoft SharePoint Server Diagnostics Service, Microsoft SharePoint Foundation Diagnostics Service, Application Registry Service, Shared Service Applications, Shared Service Proxies, Global Search Settings and Managed Metadata Web Service. This data is backed up to the Logical Device specified in the backup plan, along with backup job data.

SharePoint solutions: This includes any SharePoint customizations deployed to SharePoint in the form of solutions. These solutions and their deployment statuses are backed up to the Logical Device specified in the backup plan.

Nintex databases: This includes Nintex workflow, config database, and content database.

FAST Search Server Farms: From SnapManager 6.1 for SharePoint, FAST Search Server Farms backup and restore are supported. It can be backed up as long as the DB is in LUN, even if the FAST Search Server farm is not in LUN.

SharePoint front-end resources: The front-end Member Agent backs up the IIS settings (both meta-data and files), SharePoint hive files, and GAC files to the Logical Device specified in the backup plan.

Some components have multiple related sub-components that need to be backed up together and when you select a component, its sub-components will be auto-selected. For example, OSearch and SPSearch index files need to be backed up with their corresponding search database.

The SSP database, the Web application hosting the SSP admin site, and OSearch can be backed up together. If OSearch is not selected for backup, the search setting needs to be reconfigured and the index needs to be recrawled after an SSP restore.

Note

To back up the SSO database, the account specified in the Agent needs to be able to back up and restore the master key.

Note

To back up the Project Server database Backup, the related web application will be selected together. You cannot only back up the Project Server database.

Note

FAST search integrated with Search Service Application backup is supported now. You can also back up it manually. Refer to Full backup and restore (FAST Search Server 2010 for SharePoint) for more information.

Supported for backing up FAST Search Server for SharePoint 2010:

- For SharePoint SSA (FAST Content SSA and FAST Query SSA), there is a tool named *SharePoint Database and Index Migration for SharePoint 2010* to migrate the database and index to an N series LUN.
- SMSP uses SharePoint Content SSA to load the FAST farm topology and perform the full farm backup.
- If FAST Search Server is installed on an N series LUN, SMSP will perform snapshot backup. If FAST Search Server is installed on the local disk, SMSP will send the backup data to Media.
- SMSP allows you to perform the full farm backup of FAST Search Server for SharePoint 2010. The backup content includes all components, index files, configuration files and any other physical files of the FAST Search Server.

Unsupported for backing up FAST Search Server for SharePoint 2010:

- It is not supported to move FAST files on Admin and Index Servers to an N series LUN. Install FAST Search Server on an N series LUN or local disk originally.
- SMSP only allows you to perform the full FAST farm backup. It is not supported to back up a specific component or an Index partition.

- In SMSP, it is not supported to provide an estimate time to back up FAST Search Server by sending test packets or measuring throughput of customer’s CIFS configuration.
- In SMSP, it is not supported to provide the disk space consumed by FAST backups without Dedupe and it is not supported to indicate that Dedupe is turned off for N series storage systems.
- It is not supported to create FAST devices in SMSP.

Limitations of Backup Builder

SnapMirror and SnapVault Limitations

For integration with SnapMirror and SnapVault, you must use other methods to check the status of the following options, as the actual operations are performed outside of SnapManager and the status information is not available:

- **SnapMirror Update and Verification Results**: Use OnCommand System Manager or OnCommand Host to check the SnapMirror status and replicated Snapshot copies.
- **SnapVault Archiving and Retention**: Use Protection Manager to check SnapVault backup and retention status. The Protection Manager can also be used to delete SnapVault backups. Since SnapVault is not supported by VMDK, the VMDK archiving is not supported either.
- **Archive Backup to Secondary Storage**: This feature does not support archiving of any SharePoint data that is not managed by the SMSQL.

About SharePoint Customizations

SnapManager for SharePoint does not include system backups like AD, File System, and System State backups. Therefore, customizations with external dependencies are not backed up. Typically, such customizations are deployed through an installer or configured manually and require the use of some binaries, registry entries, or other databases.

SharePoint customizations deployed using the SharePoint solution framework can be backed up and restored to the state in backup. For example, if you deployed a solution after backing up it, after the restoration, the status of the solution is still Not Deployed and you need to deploy it again.

Simple customizations that involve only some self-contained files in the SharePoint hive folder can be covered by the Front-End Member Agent backup of the SharePoint hive. You can then select the related files for restore.

Data Protection - Restore Controller 11

Overview of Restore

From the SnapManager for SharePoint Restore Controller screen, you can perform the following actions:

- Browse and search the backup data contents displayed on a timeline, representing all available restore points.
- Set up scheduled or immediate restores for any SharePoint environment (as long as a SnapManager for SharePoint Agent is installed).
- Selectively restore SharePoint components, from the whole farm down to specific document versions, with all security, metadata, and original properties preserved
- Monitor real-time progress of any restore jobs (through the Job Monitor)

After a backup job has completed successfully, the backup data is ready for browsing. To perform a restore, click the **Restore Controller** to begin browsing the backup data.

Restore Level

There are two restore levels available:

Farm Component Level: Under the **Farm Browser** tab, the SharePoint backup farm structure is displayed. Multiple farm components, such as content databases, Web applications, SSP, or even the entire farm and its settings can be selected for restoration.

Granular Level: If granular indexing options were selected during backup, individual site collections, sites, lists, folders, items, or item versions can be restored from the content databases.

The restore options available for each restore level are different and are described in the following sections.

Job Based View vs. Historic Content View

Job Based View

Job Based View is the default view for the Restore module. This allows you to view your backup data on a job-by-job basis by using a timeline view to display all available backup points for a single farm. If you want to restore or find several web applications or other components for one job, it is recommended to use this view. Job Based View supports both the Database level and Item level restore.

Step	Action
1	Select a farm or an agent from the drop-down box. When a farm is selected, all the jobs for that farm will be displayed; when an agent is selected, only jobs from this control agent will be displayed.
2	You can hide the jobs that have not been indexed by checking the corresponding check boxes.
3	You can select a time range in the **Time Window** fields for **From** and **To**. By default, this is set to one week from the current time. You can click on the calendar icon to the right of the **From** and **To** fields to change the time range. Select a date and time in the calendar dialog box and click **OK**.
4	Click **Load Timeline**. This will display the time points at which you ran backup jobs on the time line.
5	Moving the mouse on the timeline will list detailed information of each job in a pop-up bubble.
6	You can review the content of the job in the **Farm Browser** area by clicking on the point in the **Timeline**

Historic Content View

Historic Content View is convenient when user already knows where the data desired to restore is located. After the site collection is identified, the backup history for that site collection will be displayed, and the user can explore further to see granular content.

Step	Action
1	Click **Historic Content View** on the top-right of the screen.
2	Select the farm and agent from the drop-down box, and the farm will be listed underneath the **Farm Browser**.
3	Click the farm name to expand the data tree. All the backed up web applications under the farm will be listed.
4	Select the site collection you want to view by clicking the corresponding radio box.
5	Click **Show Backups**. The **Backup Finder** page will appear.
6	You can choose a time range in the **Time Window** fields for **From** and **To**. By default, this is set to one week from the current time.
7	Click **Load Timeline**. This will display the time points which you ran backup jobs on the time line.
8	You can review the content of the job in the **Detail** area by clicking on a time point.

Loading the Timeline

To select content to populate the Timeline Browser, complete the following steps:

Step	Action
1	Open the **Restore Controller** interface and locate the options section on the top of the screen.
2	Select a **SnapManager for SharePoint Agent** from the drop-down list. This contains all Agents that have a successful backups stored in the Media Service.
3	Select a specific plan from the drop-down list, or select **All Plans** to load data for this Agent that has been backed up in multiple plans.

Step	Action
4	Specify a time range in the **Time Window** field by clicking the calendar icon to the right of **From**. This enables you to specify a start time for the search. In the window that pops up, select a date and time and click **OK**. By default, SnapManager displays the last 7 days.
5	Click the calendar icon to the right of the **To** field to choose an end time, and use the calendar dialog box to specify a date and time. Click **OK** to set this time. By default, the **To** field is populated with the current time when the interface is loaded.
6	If you want to hide incomplete jobs from the Timeline, including any that are still being indexed, select the **Hide Incomplete Jobs** checkbox.
7	Click the **Load Timeline** button. The time points at which the backup jobs were run are displayed on the timeline. When you hover your mouse over each available point, details about the backup time and plan name, restore granularity level, plan status, and verification status are shown in the pop-up bubble. Additionally, verified jobs are shown with a check mark over the point-in-time icon.
8	Click a plan's point-in-time icon to load the data for this plan. You can review the contents of the job in the tree mode on the bottom-left of the screen.
9	Browse through the backup data in the tree by clicking the name of the Agent host or the SharePoint instance to expand the backup content.

Common Restore Options

Scheduling the Restore Job

By default, all restore jobs are set to **run now**. If you want to run a restore job later, you can fill out the **Start Time** schedule in the **Restore Option** section of the interface. Click the calendar icon to set the time to run the job.

Restore Option Types

Another common setting for Restore is the type of Restore Option to use: **Not Overwrite, Overwrite, and Append.**

Not Overwrite: SnapManager for SharePoint will not restore the content if it already exists at the destination. For example, if an entire folder's contents are selected for restore but only one document was removed from the destination folder, only the one document is restored.

Overwrite: This option restores the content over whatever exists on the destination. This deletes the content on the target destination and replaces it with the content selected to be restored.

Append: The **Append** option updates the destination with the selected data to be restored. Data that already exists is not deleted, but an additional copy is added along with any data that is not already present.

Note

The **Append** option is unavailable at the Farm Component level because SharePoint does not allow two identical farm components to coexist in the same farm. This is because their internal IDs would conflict with each other.

Restore from SnapVault

By integrating with SnapVault, it is possible to have longer retention for backup data. The restore process from SnapVault backup data is the same as the features listed in the previous section.

In the background of a restore from SnapVault, SnapManager for SharePoint checks if a local backup for the selected object exists. The SnapVault backup data (or the remote backup data) is used only when local backup is already deleted. The restore from remote backup (SnapVault) will be stream based.

Note

Only database backup to SnapVault is supported. Restoring the SharePoint search index from SnapVault is not supported.

Running a Restore Job

After configuring the settings, click the **Go** button. SnapManager will initiate the restore process immediately or you can assign a schedule for the restore job to be run later.

Note

The database errors reported from SMSQL while running restore jobs will be recorded in Job report and Agent logs.

Granular Level Restore

Selecting Content for Restore

To choose site collections, sites, or any other SharePoint content to restore from a content database, you must first load the contents using the tree in the lower left of the interface by following the steps below:

Step	Action
1	Begin by either searching for the site collection directly, or loading the tree from the main SharePoint farm tree. To perform a site collection search, click the **Find Site Collection** button at the top of the SharePoint tree and enter the search criteria for the site collection in the dialog box provided (including wildcard *). Click **Search** to open an additional tab called **DB Browser** to list the databases that site collections are contained in. For case-sensitive searches, select the **Case Sensitive** check box.
2	Click the **Detail** button next to the selected content database either in the site collection search results or in the main SharePoint tree. This opens a new **Detail** tab, which displays the contents of this database.
3	To view or restore the granular content, the following two options are available: **Browse/restore granular content using index:** The granular restore index generated during backup jobs or backup maintenance jobs will be used to view the granular content within the site collection. **Browse/restore granular content from backup data:** When this option is used, the SharePoint content database backup snapshot will be mounted as a temp database first, then users can browse and restore the granular content. This option will appear slower when the first browse request is processed.

Step	Action
4	Click the site collection name to expand the tree. You can continue to expand the tree further to show all sub sites, lists, libraries, and folders located beneath that specific site collection. **Note** The tree can only expand to the level set by the Restore Granularity level during backup when granular restore index is used.
5	Select the content to restore by selecting the checkbox next to each node. By default, after you select a container, all items in it are also selected. If some items are not selected, the checkbox for this node becomes a dash symbol. To view items or item versions available for restore, click the Content Browser icon ⓘ to view the content of a list, library, or folder, and select the corresponding check box to select the content to restore.

If the whole site collection needs to be restored, it is recommended to perform the restore at site collection level (Uncheck the **Browse/Restore Granular Content** checkbox). In this case, the restore is similar to STSADM site collection level restore which using SQL statement instead of SharePoint API. It is faster and will keep internal document IDs.

Searching for Backup Data to Restore

For large backups that contain a significant amount of content, browsing through a large content database for the data needed for the restore can be time consuming and inefficient. In such situations, using the Search function 🔍 is recommended.

To search for the data to restore, complete the following steps:

Step	Action
1	Expand the **Backup Data Browser** tree and locate the node you want to search under.
2	As you hovering your mouse over the node, the Search icon appears to the right of the node. Click this icon to open the search dialog box.

Step	Action
3	Enter the search criteria. You can search on any level beneath the current node. For instance, searching from a site collection node enables you to search on the site, list or library, folder, or item level. Searching on a list or library level enables you only to define criteria for a folder or an item.
4	Enter a search term in the **Criteria** field. Wildcards (*****) are accepted. You can select the **Case Sensitive** checkbox at the bottom of the window if you want to limit the search further.
5	Click the **Add** button. You can apply multiple search terms. The search is performed based on AND logic (each item found must meet every search term specified.) You can also delete terms using the **Delete** button.
6	Click **OK** to load a list of search results. These open in a new tab called **Search Results**. You can select contents from this search result using the check boxes available.

Performing a Granular Level Restore

There are two types of Granular Level Restore: **In Place** or **Out of Place**.

In Place Restore: Restores backup data to the original location.

Out of Place Restore: Restores backup data to any alternate SharePoint location either in the same farm or across different farms.

After you select one of the restore types (in the steps below an **Out of Place Restore**), complete the following steps:

Step	Action
1	After selecting the **Out of Place Restore** option, click the **Set Destination** button.
2	Choose a destination in the new window that appears. Select the **Agent Name** for the destination location from the drop-down list at the top of the window. The destination must already have a SnapManager for SharePoint Agent installed to be selectable from this list.

Step	Action
3	Click the farm name to expand the tree. You can continue to click each node to expand the tree to the destination you want to restore to.
4	Use the radio button next to the destination node to select a location to restore to. If you want to restore to a location that does not exist in SharePoint, you can use the blank box at the bottom of each level in the SharePoint tree. To create a new site collection, the full URL is needed, but for other levels (from site down to folder), only the name needs to be specified. If the site collection to be created is a FBA site collection, click the **Configure** button next to the URL to configure it in the pop-up window. Select a **Content Database** in the drop-down list and input the name of the FBA user who creates the destination site collection in **Site Collection Administrator** field. You can click the **Check Names** icon to check the user you input, or click the **Browse** icon to search the user. If you click the **Browse** icon, there will be a pop-up window. Enter the key word in the **Find** field and click the **Search** icon. All the users contain the key word will be listed in the table. Select the user you want to add to the **Site Collection Administrator** field and click **Add** button. Only one user can be added. Click **OK**. **Note** You should always select a container for the content either on the same level or one level higher than what is being restored. For example, a site should always be restored either to a site or a site collection, and a list or library should always be restored either to a site or another list or library.
5	Click **OK**. The **Farm Name** and **Destination** information is populated below the **Out of Place** restore option.

Restore Options for Items

For both **In Place** and **Out of Place** restores, the detailed contents of each container object can be displayed in a new window by clicking the **Details** icon as described previously. In the item details window, you can select individual items in the resulting table listing all restorable items. You can use the following options for the selected items and container:

- **Container Security:** Select this option to restore the security settings of the container object, if unique permissions are used.
- **Container Property:** Select this option to restore the container properties. For example, if the container is a list, this includes all the columns, settings, and other options.
- **Item Security:** Use the check boxes in the last column of the item dialog box to restore the security settings of the items. This is useful if unique permissions are used.

If **Item Version restore granularity** was used during backup, item versions are listed in the item details window. History versions are displayed as **Item Name Version Number**. The most current version is displayed as the item name without any version information. You can either choose to restore a single version or only the most current version.

Note

To restore a site with the **Lookup** field and its value is looked up to another site, the **Lookup** field cannot be restored properly if you only restore the site with the **Lookup** field.

Farm Component Level Restore Options

Restoring a Database to its Most Recent State

This option enables you to use SnapManager for SharePoint to restore a SharePoint database to its most recent state.

Note

To use this option, you must select the latest backup data.

If this option is not used, a point-in-time restore is performed, which creates multiple recovery paths for the database. A later up-to-the-minute restore using the same backup data will fail. In that case, the SnapManager for Microsoft SQL Server interface can be used for up-to-the-minute restores. A detailed explanation of this limitation is documented in the following section.

After the database is restored, it must be reattached to the SharePoint environment before SharePoint Services can access it. You can use either the Mount-SPContentDatabase cmdlet in Windows PowerShell, or the addcontentdb STSADM command to reattach a content database to a Web application. Refer to the commands below:

```
Mount-SPContentDatabase -Name <DatabaseName> -DatabaseServer <ServerName> -
WebApplication <URL>
```

```
%COMMONPROGRAMFILES%\Microsoft Shared\web server extensions\12\bin\stsadm.exe -o
addcontentdb -url URL name - databasename database name
```

Where the *URL name* entry is a valid URL (such as http://server_name) and *database name* is a valid content database name. For more details about the **S**harePoint **T**eam **S**ervices **ADM**inistration (STSADM) command, visit the Microsoft TechNet Library

Microsoft TechNet Library-Addcontentdb: Stsadm operation (Office SharePoint Server)

Note

The preceding STSADM command can be used only on a content database. For other SharePoint databases, the **Restore From Alternate Storage Location** option can be used for the manual restore process.

Restoring a Database to a Point in Time

In a point-in-time restore, databases are restored to a point in time selected from the timeline browser.

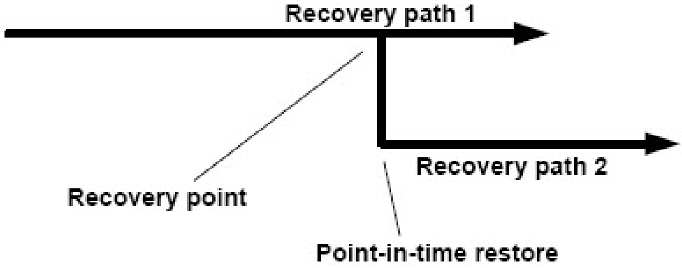
A point-in-time restore occurs in two restore scenarios:

- The database is restored to a given time from a backed up transaction log.
- The database is restored but only a subset of backed up transaction logs are applied to it.

Note

Performing a point-in-time database recovery results in a new recovery path.

The following image illustrates the potential problems when a point-in-time restore is performed.



In this image, Recovery path 1 consists of a full backup followed by a number of transaction log backups (a point-in-time backup). New transaction log backups are created after the point-in-time restore takes place, which results in Recovery path 2. It is not possible to tie the transaction logs created in Recovery path 2 to the full backup belonging to Recovery path 1.

Therefore, to preserve database integrity, the only way to restore the database to its most current state after a point-in-time restore is to complete a new full backup that has only one recovery path.

Note

To avoid the problems listed previously, ensure that you always create a full backup after restoring a database to a point-in-time.

Verifying Backup Data before Restoring

This option enables you to verify backup data before restoring it to ensure that the restore is successful. Select a **Verification Server** from the drop-down list, defined previously in the Control Panel. The Default option uses the Verification Server configured in the SnapManager for Microsoft SQL Server interface.

Restore Databases Only

When this option is used, only the selected databases are restored with no attempt to connect them to the SharePoint environment. This is useful in the instance when a SharePoint environment has not yet been set up (i.e. during a whole farm restore). This can also be used in cases where you want to perform manual steps to bring up or down a specific environment after the database has been restored.

Note

Configuration databases and Central Administration databases can only be restored by selecting this option.

Restore Front-end File Security

This option only applies to the front-end files backed up, including IIS site files and SharePoint hive files. When the option is used, both file contents and security permissions are restored. Otherwise, only the file content is restored.

Restore Front-end Files to Alternate Location

This option enables you to select a location to restore the front-end files and templates files.

Step	Action
1	Click the **Browser** button, and a dialog box will appear.
2	Select an **Agent** from the drop-down box.
3	Expand the destination tree by clicking the **Agent** name. Click each node to expand the tree further.
4	Select the location for the files you want to restore by clicking the corresponding radio button.
5	Click **OK** to save this destination, or use **Cancel** to clear the settings.

Run command with operation

When this option is selected, the command profiles which selected Restore operation in Control Panel will be listed in the drop-down list. The command will be run according to the profile you select.

Farm Component Level Restore Considerations

Supported SharePoint 2007 Farm Level Components for Restore

For a list of all the farm components available of SharePoint 2007 for restore, see the following list:

Farm component	Notes
Configuration Database	Can only be restored during a whole farm restore
Central Administrator Web Application	Can only be restored during a whole farm restore
Admin Content Database	Not Applicable
Web Application	Not Applicable
Content Databases	Allows granular restore of individual items
Shared Services Provider (SSP)	SSP properties, SSP database, and search index
SSP Search Index	Must be backed-up and restored together with SSP
Global Search Settings	Farm-level search settings and crawler impact rules
SharePoint Help Search	Not Applicable
InfoPath Form Services	InfoPath Forms Services Settings and InfoPath Forms Services form templates
Single Sign On (SSO)	SSO database and configurations
Windows SharePoint Solutions	SharePoint solutions and their deployment status
Nintex Databases	Nintex workflow config database and content database
Front-End Resources	IIS settings and files, SharePoint 12 Hive folder

Farm component	Notes
Project Server database	Must be backed-up and restored together with the related web application

Supported SharePoint 2010 Farm Level Components for Restore

For a list of all the farm components available of SharePoint 2010 for restore, see the following list:

Farm component	Notes
Configuration Database	Can only be restored during a whole farm restore
Central Administrator Web Application	Can only be restored during a whole farm restore
Admin Content Database	Not Applicable
Web Application	Not Applicable
Content Databases	Allows granular restore of individual items
State Service	Not Applicable
User Code Service	Settings for the Sandboxed Code Service
Diagnostics Service	Settings for the diagnostics service
Application Registry Service	Backwards compatible Business Data Connectivity API
Shared Services Applications	From SnapManager 6.1 for SharePoint, PerformancePoint Service Application database is supported
Shared Services Proxies	Not Applicable
Managed Metadata Web Service	It is supported from SnapManager 6.1 for SharePoint
SharePoint Foundation Search	Not Applicable

Farm component	Notes
InfoPath Form Services	InfoPath Forms Services Settings and InfoPath Forms Services form templates
Global Search Settings	Farm-level search settings and crawler impact rules
Windows SharePoint Solutions	SharePoint solutions and their deployment status
Nintex Databases	Nintex workflow config database and content database
FAST Search Server Farms	All the FAST Search Server Farms associated with SharePoint
Front-End Resources	IIS settings and files, SharePoint 14 Hive folder

Note

SharePoint components that are not listed in the preceding table are not supported. For example, custom Web parts not deployed through a SharePoint solution.

Restore Details about Specific Farm Components

Some of the details and conditions pertaining to restoring each farm component type:

Configuration database: This is the core component of the SharePoint farm. It can only be restored during a whole farm restore. See the full farm restore section of this guide for details regarding this process.

Web applications: Web applications can be selected from the farm tree and restored, including the settings and associated IIS sites. Content databases under the Web applications are also restored if selected. However, if there are any changes on the IIS sites (resulting from manual changes or third party software) the IIS site backup on the front-end Member Agent will also need to be restored.

Shared Services Applications: Fast search integrated with Search Service Application restore is supported now. You can also restore it manually. Refer to Manually Restore Fast Search Server for SharePoint 2010.

Content databases: Content databases include SharePoint data such as site collections, sites, lists, libraries, and all items. When a content database is restored, SnapManager for SharePoint automatically reattaches them to the original Web application.

SSO: To back up and restore the Single Sign-On encryption key, the control agent must be on the encryption key server. The encryption key, SSO database, and SSO settings are restored.

Project Server database (SharePoint 2007 only): Project Server database includes four databases: Draft database, Published database, Archive database, and Reporting database. It can be selected from the farm tree and restored, and the Project Server database must be backed-up and restored together with the related web application, you cannot only restore the Project Server node.

SSP and search index (SharePoint 2007 only): Shared Services Provider has multiple sub-components including the SSP database, search index files, search database, and SSP admin site collection hosting Web application. In addition, other Web applications might be related to SSP, such as the web application hosting the My Sites site collections. Before the SSP is restored, the following must be restored:

- Any related Web applications must be restored before the SSP can be restored.
- The OSearch service must be started in the SharePoint Central Administrator interface.
- In addition, the search index must be restored together with SSP.

SharePoint solutions: When a SharePoint solution is restored, it is deployed to the related Web applications as during the state of the backup. Depending on the customizations contained in the SharePoint solution, it may need to be re-configured after the deployment.

Nintex databases: This includes Nintex workflow config database and content database.

Front-end resources: If only out-of-the-box SharePoint features are used, there is no need to restore the front-end resources, as everything is covered by the other farm components. If there are manual customizations applied to the IIS site (including web.config), the IIS site should be restored.

If customizations are self-contained within the SharePoint hive folder, they can be restored as well by restoring those files. Both IIS site files and hive files can be restored out-of-place to another location for further examination.

Note

Front-end resources cannot be restored together with other farm components. They need to be restored separately after any other farm components are restored.

Deleting SnapManager for Microsoft SQL Server Restore Copies

SnapManager for Microsoft SQL Server creates a snapshot copy of LUNs as part of restoring SQL server databases to their original locations. These snapshot copies of LUNs cannot be deleted by SnapManager for SharePoint. You must use SnapManager for Microsoft SQL Server to delete these copies.

To delete these copies, complete the following steps:

Step	Action
1	Launch the SnapManager for Microsoft SQL Server interface.
2	Select the **Action** menu, and choose the **Delete Backup** option.
3	Select the option to **Delete Snapshot Copy of LUN Created During Restore** to delete these copies. You can also select any additional options at this point.

Note

This situation only applies to the restore of farm components, because granular level restore only clones the original snapshot backup and does not restore the database.

Automatically Restore FAST Search Server for SharePoint 2010

Restore FAST Search Server

After you automatically backed up FAST Search Server, you can also restore it automatically by following the steps below:

Step	Action
1	Open the **Restore Controller** interface and locate the options section on the top of the screen.
2	Select a **SnapManager for SharePoint Agent** from the drop-down list. This contains all Agents that have a successful backups stored in the Media Service.
3	Select a specific plan from the drop-down list, or select **All Plans** to load data for this Agent that has been backed up in multiple plans.
4	Specify a time range in the **Time Window** field by clicking the calendar icon to the right of **From**. This enables you to specify a start time for the search. In the window that pops up, select a date and time and click **OK**. By default, SnapManager displays the last 7 days.
5	Click the calendar icon to the right of the **To** field to choose an end time and use the calendar dialog box to specify a date and time. Click **OK** to set this time. By default, the **To** field is populated with the current time when the interface is loaded.
6	If you want to hide incomplete jobs from the Timeline, including any that are still being indexed, select the **Hide Incomplete Jobs** checkbox.

Step	Action
7	Click the **Load Timeline** button. The time points at which the backup jobs were run are displayed on the timeline. When you hover your mouse over each available point, details about the backup time and plan name, restore granularity level, plan status, and verification status are shown in the pop-up bubble. Additionally, verified jobs are shown with a check mark over the point-in-time icon.
8	Click a plan's point-in-time icon to load the data for this plan. You can review the contents of the job in the tree mode on the bottom-left of the screen.
9	Browse through the backup data in the tree by clicking the name of the Agent host or the SharePoint instance to expand the backup content.
10	Select the FAST Search Server Farm by checking the corresponding checkbox of Admin server. It will prompt **Configuration and content on all FAST search servers will be overwritten, are you sure to continue?** in the pop-up window. Click **OK** to select the farm and click **Cancel** to unselect it.
11	Click the **Restore Settings** button beside the Admin server name to configure the settings in the pop-up window.
12	If you want to restore associated SharePoint Content SSAs, check the corresponding checkbox.
13	If you want to restore FAST certificate, check the corresponding checkbox. Select **Generate new FAST certificate or Use the certificate from backup** and enter the password.
14	Click **OK** to save the configuration.
15	Select the **In Place Restore** option.
16	Select a **Restore Option** from the drop-down list. For more information, see "Farm Component Level Restore Options" on page 154 of this manual.

Step	Action
17	Select a time for the restore job. By default, **Now** is selected and the job will be run as soon as **Go** is clicked. You can set a scheduled date and time for this restore by clicking the calendar icon and select a date and time in the calendar pop-up window and click **OK**.
18	You may enter a **Description** in the field provided to help distinguish this job in the Job Monitor.
19	Click **Go**. If you set the start time as **Now**, it will run the restore job immediately; otherwise, it will run the job at the specified time.

Supported for restoring FAST Search Server for SharePoint 2010:

- For SharePoint SSA (FAST Content SSA and FAST Query SSA), there is a tool named *SharePoint Database and Index Migration for SharePoint 2010* to migrate the database and index to an N series LUN.
- SMSP allows you to perform the full farm restore of FAST Search Server for SharePoint 2010.

Unsupported for restoring FAST Search Server for SharePoint 2010:

- It is not supported to move FAST files on Admin and Index Servers to an N series LUN. Install FAST Search on an N series LUN or local disk originally.
- SMSP only allows you to perform the full FAST farm restore. It is not supported to restore a specific component or an Index partition.

Note

You can also restore FAST Search Server manually. For more information, refer to Full backup and restore (FAST Search Server 2010 for SharePoint)

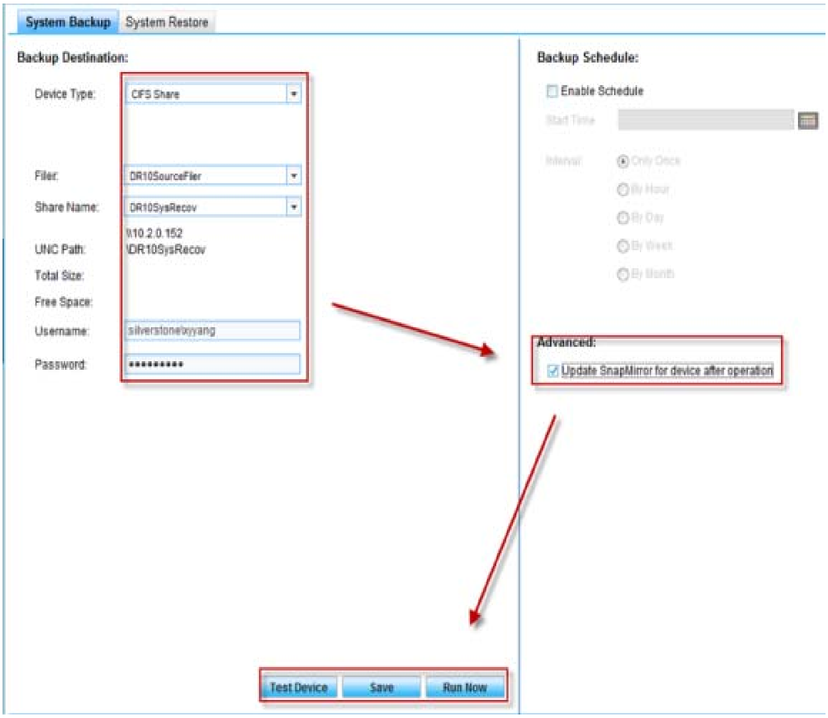
Disaster Recovery

Prerequisites for Performing a Disaster Recovery

This section describes how to perform a disaster recovery (DR) using backup data from SnapMirror from the perspective of SharePoint and SnapManager for SharePoint. It does not cover how to recover Active Directory (AD) or any other components not covered by SnapManager for SharePoint.

Prior to performing this restore:

- The SharePoint database and search index backups must be available. Typically these are automatically replicated through SnapMirror.
- SnapManager for SharePoint backup jobs data and system backup data must be available. If Logical Device and System Backup locations are using SnapMirror enabled LUNs, it should be automatically synchronously replicated.



Backup Destination:

Device Type: CIFS Share

Filer: DR10SourceFiler

Share Name: DR10SysRecov

UNC Path: \\10.2.0.152\DR10SysRecov

Total Size:

Free Space:

Username: silverstone\xyyang

Password: **********

Backup Schedule:

□ Enable Schedule

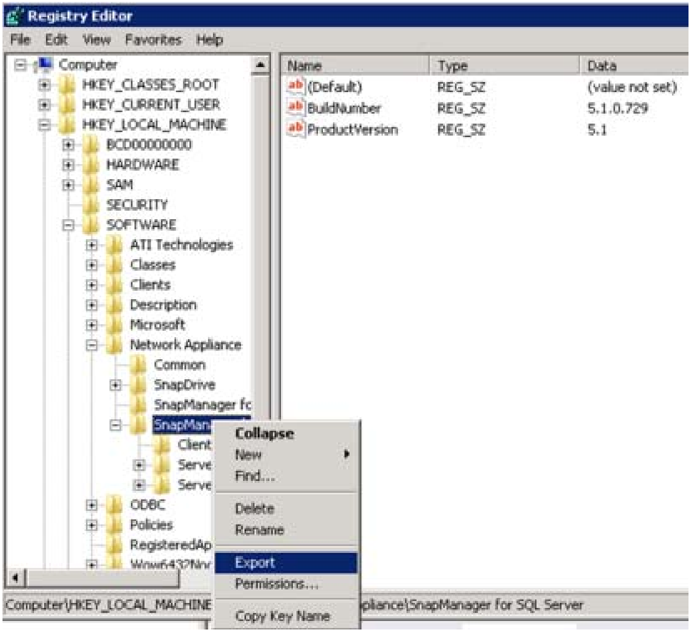
Start Time

Interval ● Only Once ○ By Hour ○ By Day ○ By Week ○ By Month

Advanced:

☑ Update SnapMirror for device after operation

- The registry backup of SnapManager for SQL Server must be available (**HKEY_LOCAL_MACHINE > SOFTWARE > IBM > SnapManager for SQL Server**).



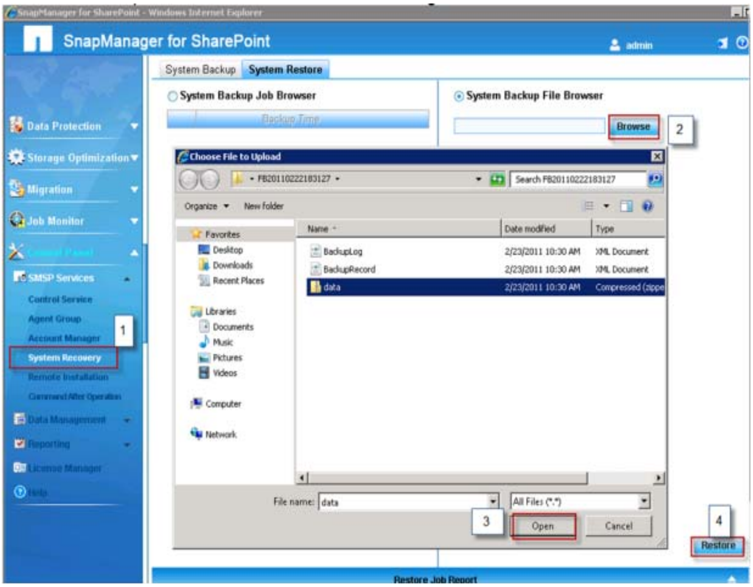
Name	Type	Data
(Default)	REG_SZ	(value not set)
BuildNumber	REG_SZ	5.1.0.729
ProductVersion	REG_SZ	5.1

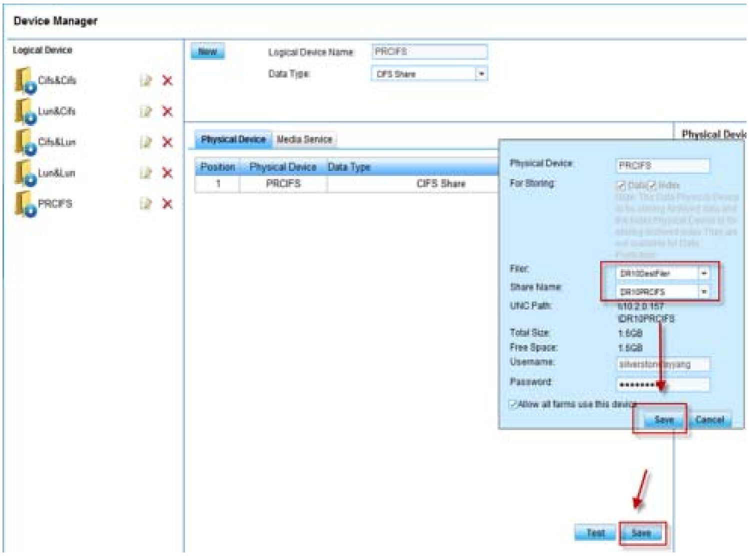
- At the DR site, all server topology should be identical to the production site, which includes both the SharePoint farm topology and SnapManager for SharePoint topology. The hostname of the source and the destination should be the same. If you use IP in the configuration, for example, using IP to configure SharePoint or media, the IP should be the same. For SQL, except port, the instance name and alias of the source and the destination should be the same. If you install SnapManager for SharePoint in other places, you should use identical hostname or IP for SnapManager for SharePoint Manager. The port can be different.
  There are several ways to achieve this. For example, a separate AD domain for the DR site can be used to keep the same server topology, or if the DR site does not need to coexist with the production site, disk imaging or virtualization technology can be used to ensure the same topology is used.
- If a separate AD domain is used at DR site, that domain should have a trusted relationship with the primary site's AD so that users can still access SharePoint content. This can also be run if the DR site is in the same AD domain as the original location.

Preparing the DR Site for Recovery

After the servers are rebuilt and the preceding prerequisites are met, complete the following steps for disaster recovery:

Step	Action
1	Configure iSCSI Initiator settings for the server which needs to use SnapDrive LUN.
2	Install all required software components, including SnapDrive, SQL server, and SnapManager for Microsoft SQL Server. For more information of the installation, you can refer to *SnapDrive for Windows Installation and Administration Guide* and *SnapManager for Microsoft SQL Server Installation and Administration Guide*. **Note** Do not connect SQL Server using SnapManager for Microsoft SQL Server right now to make sure the source data and the destination data are the same.
3	Connect the following LUNs in destination volumes with SnapDrive (Keep the drive letters the same as LUNs in source). ● Destination SharePoint LUN ● Destination SQL LUN ● Destination SMSP LUN
4	Import SMSQL registry key from the file that saves the exported SMSQL registry key. Add SQL Server to SMSQL management list. Run SMSQL configuration wizard.
5	Install SharePoint. If only farm components like Web applications or SSP need to be restored, in the destination you can create a new farm which has the same name and farm topology as the source farm. Otherwise, SharePoint can be left unconfigured when performing an entire farm restore.

Step	Action
6	Install SnapManager for SharePoint Manager according to the steps listed in this guide. **Note** Make sure all software versions and patch levels are the same as the original production site. Also ensure that all the users and permissions are created and set to the same production site.
7	Perform a SnapManager for SharePoint system restore using the System Recovery backup data.  SnapManager for SharePoint - Windows Internet Explorer SnapManager for SharePoint admin Data Protection Storage Optimization Migration Job Monitor Control Panel SMSP Services Control Service Agent Group Account Manager System Recovery Remote Installation Command After Operation Data Management Reporting License Manager Help 1 System Backup System Restore System Backup Job Browser Backup Time System Backup File Browser Browse 2 Choose File to Upload FB20110222183127 Search FB20110222183127 Organize New folder Favorites Desktop Downloads Recent Places Libraries Documents Music Pictures Videos Computer Network Name Date modified Type BackupLog 2/23/2011 10:30 AM XML Document BackupRecord 2/23/2011 10:30 AM XML Document data 2/23/2011 10:30 AM Compressed (zippe File name: data All Files (*.*) 3 Open Cancel 4 Restore Restore Job Report

Step	Action
8	Connect the SnapMirror LUN containing the Media Service backup job data, or manually copy this data to a location that the DR site Logical Device can access.  Device Manager Logical Device: Cifs&Cifs, Lun&Cifs, Cifs&Lun, Lun&Lun, PRCIFS Logical Device Name: PRCIFS Data Type: CIFS Share Physical Device | Media Service Position: 1 — Physical Device: PRCIFS — Data Type: CIFS Share Physical Device: PRCIFS For Storing: ☑ Data ☑ Index Filer: DR10DestFiler Share Name: DR10PRCIFS UNC Path: \\10.2.0.157\DR10PRCIFS Total Size: 1.5GB Free Space: 1.5GB Username: silverstone\yyang Password: •••••••• ☑ Allow all farms use this device **Note** The DR site's Media Service location can be changed to point to the new location. This is recommended to maintain the Media Service to make sure the source data and the destination data are the same. For Archiver or Extender DR, you need to run a System Restore to restore all of the physical devices. If the filer used to configure the mirror is damaged and you must access the data in the mirror, you must first configure the destination volume location as a physical device by CIFS Share, and then add the physical device to the original logical device. Note that you must specify the volume-share of the mirror to the original media to make sure the Logical Device can access the data properly. If mirrored CIFS Share is on a different filer, reconfigure CIFS Share on the destination filer and update the physical device.
9	Install SnapManager for SharePoint Agents according to the steps listed in this guide.

Performing the DR Restore

After installing SnapManager for SharePoint in the DR site and completing the preceding steps, you can continue with the full farm restore.

SharePoint 2007 DR Restore

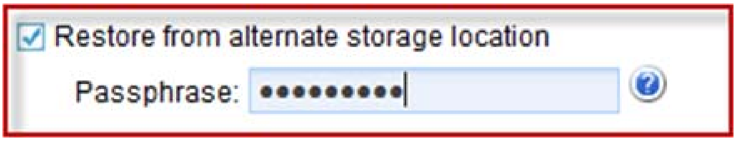
Refer to the steps below for the detailed steps of SharePoint 2007 DR Restore.

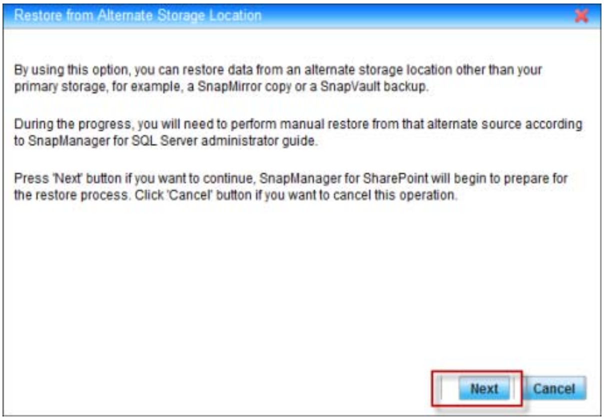
Step	Action
1	Navigate to **Restore Controller** in SnapManager for SharePoint.
2	Reconfigure CIFS Share in the destination filer and update the physical device. You will see the backup data. Browse for the backup data and choose the **Restore From Alternate Storage Location** option. How to use this option is described in "Restore from Alternate Storage Location" on page 182.
3	Use SnapManager for Microsoft SQL Server to restore any related databases. Refer to the *SnapManager® for Microsoft® SQL Server® Installation and Administration Guide* for the detailed steps. You can find the guide on the N series support website (accessed and navigated as described in "Websites" on page xi). The databases are contained in the selected farm node. For example, if you select a Web application, the content database should be restored.
4	Reconnect the SharePoint search index LUN using SnapDrive. Refer to the *SnapDrive Installation and Administration Guide* for the detailed steps. You can find the guide on the N series support website (accessed and navigated as described in "Websites" on page xi).
5	Complete the manual restore wizard.
6	If the whole farm restore was performed, follow the procedure described in the full farm restore section to reconnect SharePoint servers and complete other post-restore steps.
7	After the restore is complete, you can make a DNS switch to redirect users to the DR site. If the configuration process does not involve IP, it only needs to make sure the hostname of the source and the destination is the same and the corresponding record of each hostname in DNS points to the destination.

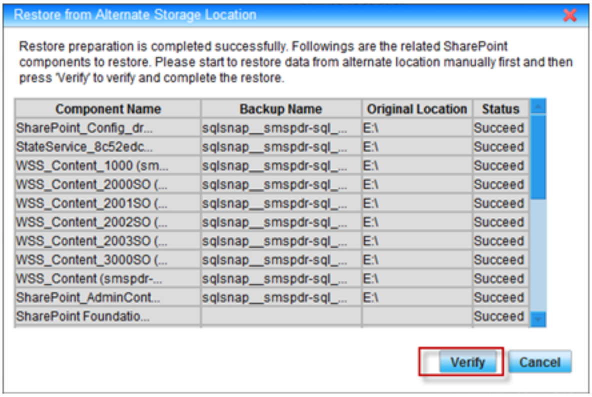
SharePoint 2010 DR Restore

For SharePoint 2010, the logic of DR restore is changed in SMSP 6.1. In SMSP 6.1, the Logical Devices and Physical Devices are used to store the backup data. Back up data using the logical device of the CIFS Share type before performing the full farm restore. In earlier SMSP versions, it is necessary to manually reconnect the farm after DR restore.

Back up data using the logical device of CIFS Share type before performing the full farm restore. And in earlier SMSP versions, you need to reconnect the farm after DR restore manually. Now, the farm after DR restore can be connected automatically through the new option **Restore from alternate storage location > Passphrase.** The restore operation steps are simpler than before.

Step	Action
1	Change the path of the physical device which binds with the logical device to the destination CIFS Share path.
2	Navigate to **Data Protection** > **Restore Controller** and load the backup job you want to restore. Select the Farm node to make the whole farm selected.
3	Select **Restore from alternate storage location** in the right pane and enter the passphrase in the provided textbox. Click **GO**.  ☑ Restore from alternate storage location Passphrase: ●●●●●●●●●

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>4</td><td>A message indicator pops up. Click <b>Next.</b>


By using this option, you can restore data from an alternate storage location other than your primary storage, for example, a SnapMirror copy or a SnapVault backup.
During the progress, you will need to perform manual restore from that alternate source according to SnapManager for SQL Server administrator guide.
Press 'Next' button if you want to continue, SnapManager for SharePoint will begin to prepare for the restore process. Click 'Cancel' button if you want to cancel this operation.
</td></tr>
<tr><td>5</td><td>Another dialog as seen below will pop up.


Restore preparation is completed successfully. Followings are the related SharePoint components to restore. Please start to restore data from alternate location manually first and then press 'Verify' to verify and complete the restore.
<table>
<tr><th>Component Name</th><th>Backup Name</th><th>Original Location</th><th>Status</th></tr>
<tr><td>SharePoint_Config_dr...</td><td>sqlsnap__smspdr-sql_...</td><td>E:\</td><td>Succeed</td></tr>
<tr><td>StateService_8c52edc...</td><td>sqlsnap__smspdr-sql_...</td><td>E:\</td><td>Succeed</td></tr>
<tr><td>WSS_Content_1000 (sm...</td><td>sqlsnap__smspdr-sql_...</td><td>E:\</td><td>Succeed</td></tr>
<tr><td>WSS_Content_2000SO (...</td><td>sqlsnap__smspdr-sql_...</td><td>E:\</td><td>Succeed</td></tr>
<tr><td>WSS_Content_2001SO (...</td><td>sqlsnap__smspdr-sql_...</td><td>E:\</td><td>Succeed</td></tr>
<tr><td>WSS_Content_2002SO (...</td><td>sqlsnap__smspdr-sql_...</td><td>E:\</td><td>Succeed</td></tr>
<tr><td>WSS_Content_2003SO (...</td><td>sqlsnap__smspdr-sql_...</td><td>E:\</td><td>Succeed</td></tr>
<tr><td>WSS_Content_3000SO (...</td><td>sqlsnap__smspdr-sql_...</td><td>E:\</td><td>Succeed</td></tr>
<tr><td>WSS_Content (smspdr-...</td><td>sqlsnap__smspdr-sql_...</td><td>E:\</td><td>Succeed</td></tr>
<tr><td>SharePoint_AdminCont...</td><td>sqlsnap__smspdr-sql_...</td><td>E:\</td><td>Succeed</td></tr>
<tr><td>SharePoint Foundatio...</td><td></td><td></td><td>Succeed</td></tr>
</table>
</td></tr>
<tr><td>6</td><td>Restore all the databases from SnapManager for Microsoft SQL Server.</td></tr>
<tr><td>7</td><td>Restore the snapshot of Index LUN manually.</td></tr>
<tr><td>8</td><td>Go back to SMSP Manager and click <b>Verify</b>.</td></tr>
<tr><td>9</td><td>After the full farm restore process completed, click <b>OK</b>.</td></tr>
</table>

Workaround for Search Service Application (for SharePoint 2010)

If the Query Component status of Search Service Application is disabled after the full farm restore, delete Search Service Application manually from Central Administration and restore Search Service Application separately.

Manually Create WSS_Logging Database

If you have configured the settings in SharePoint 2010 **Central Administration** > **Monitoring** > **Configure usage and health data collection**, a database named WSS_Logging will be generated. This database cannot be backed up by either using SharePoint platform backup, or SMSP Data Protection Backup. Therefore, while doing DR restore, this database will be missing. To avoid this error and manually repair it, complete the following steps:

Step	Action
1	Go to SharePoint 2010 **Central Administration** > **Application Management** > **Manage Service Application**.
2	Select **Delete data associated with the Service Applications** option and delete the service application **Usage and Heath data collection**.
3	Go to SharePoint 2010 **Central Administration** > **Monitoring** > **Configure usage and health data collection**.
4	Reconfigure the settings in **Configure web analytics and health data collection.**
5	The WSS_Logging will be created. **Note** The previous data in database WSS_Logging will not exist in this new one.

Helpful Notes on Archiver Restore

Refer to the detailed information below.

- Modify the CIFS Share physical device, and change the filer to the one in SnapMirror destination and revise the corresponding Share Name.
- To change the filer to the destination one, the SnapMirror relation has to be broken. Otherwise SMSP will filter out the CIFS share volume in Mirror status when loading.
- Due to the Filer which the LUN uses has been changed, the LUN Device also needs to be reset. Navigate to **Control Panel** > **Data Management** >

Device Manager and click the **Edit** icon next to the LUN Device which needs to be reset. Select the LUN which is before the System Recovery backup.

- Check the RBS status. The selection condition of Content DB is the same as the condition before System Recovery backup. But the RBS status is Not Installed; click **Run Now** to reinstall RBS.

Helpful Notes on Extender Restore

Refer to the detailed information below.

- Due to the content databases reinstalled RBS, though the Extender settings which were set in the source still can be shown on GUI, they will never take effect. Reset Extender settings.
- Retract the content database in which the stub is located before restore.

Helpful Notes on Archived Data Recovery

Refer to the detailed information below.

- When only one farm’s archived data exists in the CIFS Share and **Use Volume Level Snap Restore For Volumes With Single CIFS Share** option is selected, the entire Snapshot will be restored. Any data added to the volume after the Archived data backup will be lost. The data which is not in the farm will also be lost.
- Here is a special case for Archived Data Recovery: Some other data exists in the CIFS Share together with the farm’s archived data. In this case, no matter the **Use Volume Level Snap Restore for Volumes With Single CIFS Share** option is selected or not, only the Archive Data Backup of this farm will be restored and other data will not be affected in the CIFS Share.

Full Farm Restore

Overview

SnapManager for SharePoint Backup and Restore solution enables you to back up your entire SharePoint farm, including all of the SharePoint farm components listed previously and then restore it to another (or the same) location.

Prerequisites for a Full Farm Restore

To do a full farm level restore, the following requirements need to be met:

- A backup copy of the data for the entire farm (including the SharePoint configuration database and the central administration database) must be available.
- The SharePoint server topology should be identical to the topology at the time of backup. The system platform should also match the platform at the time of backup. For example, a x64 system should be used if an x64 system was used at the time of backup.
- All related software installed on the destination should be the identical version and the patch level as before. Examples of related software are: SharePoint, SQL Server, SnapManager for Microsoft SQL Server, SnapManager for SharePoint, as well as the .NET Framework.
- User permissions on both the local server and SQL Server should be set to the same as before.
- The hostname of SharePoint server and the instance name of SQL should be the same as the source.
- The hostname of the new SMSP Manager should have the same name as the source.
- The SharePoint host, SQL server and SMSP Manager host should be in the same domain as the source.
- Configure the same LUN storage layout as before.
- SnapManager for SharePoint Control Agent should be installed on the SharePoint Central Administration server.
- Also, to restore Single Sign-On, SnapManager for SharePoint Control Agent must be on the SSO master key managing server.
- SMSP Member Agent should be installed on the SQL server.

Performing a Full Farm Restore

To perform a full farm restore, complete the following steps:

Step	Action
1	Before performing the **in place** restore (same farm) in the Restore Controller, evaluate the status of the farm: ● If the farm you are restoring to is a newly deployed or re-installed one, disconnect all front-end web servers using the SharePoint Products and Technologies Configuration Wizard. See your SharePoint user guide for more details. ● If the farm you are restoring to is a new installation, proceed to the next step.
2	Using Restore Controller (described in the previous sections), load the backup plan and data for this farm. Using the tree, choose the Configuration DB and Admin Content DB. **Note** If the Configuration DB and Admin Content DB were not backed up, any missing configurations need to be put back manually. If so, you can create a new farm and continue from Step 7.
3	Choose the **Restore Databases Only** option next to the restore options. This option is used because the SharePoint environment is not available at this time, and therefore is not required to connect to the databases yet.
4	Click **Go** to start the restore process.
5	Connect all of the SharePoint web front-end servers to the Config DB restored in the previous step. You can use the SharePoint Products and Technologies Configuration Wizard to perform this action. **Note** At least one web front-end server should be used to host the Central Administration Web Application. When using the SharePoint Products and Technologies Configuration Wizard, select the **Use This Machine To Host The Web Site** option under **Advanced Settings** > **Host Central Administration Web Application**.

Step	Action
6	Under certain circumstances, front-end resources backed up by a SnapManager for SharePoint Front-End Member Agent need to be restored. For example, IIS site settings or files (that is, web.config) might have been changed after the Web application was created, either manually or through third-party software. **Note** Front-end resources should be restored separately from the farm component restore. They cannot be selected at the same time with farm components in Restore Controller.
7	To ensure that all solutions have been properly deployed, select the **Windows SharePoint Solutions** node in the restore tree and run a restore. **Note** The **Database Only** option should **not** be used in this case.
8	If the following features need to be restored, restart the related Windows services and make sure they are running before restore: **Single Sign-On (SSO) (SharePoint 2007 only):** Restart the Microsoft Single Sign-On Service Windows service. **SPHelpSearch (SharePoint 2007 only):** Restart the Windows SharePoint Services Search Windows service **Shared Services Provider (SSP) (SharePoint 2007 only):** Restart the Office SharePoint Server Search (OSearch) Windows service. In SharePoint 2007, you also need to restart the SSP service in the SharePoint Central **Administration** > **Operations** > **Services** setting on the Server list.

Step	Action
9	To complete the restore of the index data for the SSP (SharePoint 2007 only), select the corresponding nodes and children in the tree of the Restore Controller tree and perform an in-place restore. Make sure you are not using the **Database Only** restore option. If this SSP is the parent of an inter-farm deployment, all children will take 5-10 minutes to establish a connection after the restore is complete. This happens automatically. **Note** You can also manually crawl the SharePoint index again. From Central Administration, choose to edit the properties and specify an index server for the SSP. Navigate to the SSP admin site and choose **Search Setting** > **Restart Crawl Index Files.**
10	If any customizations have been installed using a third-party install wizard, rerun those installations to complete the restore.
11	Using the instructions provided in the Granular and Farm Component Restore sections above, restore the SharePoint content databases back to the environment.

Restoring Web Front-end Settings

You can restore customizations to your web front-end server for your farm by using Restore Controller. You can also use this to restore the IIS settings, GAC files, and the SharePoint hive.

Using Restore Controller, perform an in-place restore of any of the nodes listed under the web front-end server level. For instance, if you only want to restore the IIS settings for a single Web application (that is, the only one with customizations), you can restore a single front-end resource node from this tree. You can also remove all the customizations and return these to the original settings.

General Troubleshooting Tips for Full Farm Restore

Some of the most common problems when performing a full farm backup and restore are detailed in the following sections.

SharePoint central administration cannot be accessed after restore:

You can recover Central Administration by using one of the following methods:

- Make sure that the web front-end servers were used to host the Admin Web (described previously). If not, disconnect a front-end server and reconnect it using the SharePoint Products and Technologies Configuration Wizard, select the **Use This Machine To Host The Web Site** option under **Advanced Settings** > **Host Central Administration Web Application**. Consult your SharePoint guide for more information about this process.
- Recycle the application pool for Central Administration.

If index data is not accurate or corrupted: You can use one of the following methods to restore the index data.

- Use Restore Controller (without the **Database Only** option) to restore the index records from the last available backup.
- Restart the Office SharePoint Server Search Services and set the index server for the SSP and recrawl the environment.

A Web application cannot be accessed after restore: If you want to fix this issue, make sure you perform the following first.

- If customized features or site-definitions were used, verify that all prerequisite steps for the web front-end server were performed before performing the restore.
- Make sure that Web Site Status is started in IIS Manager with the proper settings.
- Reset the password for the application pool and perform an IIS reset.

If there are problems with user profiles and properties or search settings in SSP: Perform the following steps if you are having trouble with the SSP.

- Restart the Office SharePoint Server Search Services in SharePoint.
- Restore the SSP using Restore Controller.

Restore Hive and IIS Files

Overview

After Backing up selected Hive and IIS nodes, you can go to the Restore Controller to restore these files. If you are going to restore IIS files, you can go to the Restore Controller and select the node you want to restore. If you are going to restore Hive files, complete the following steps:

Step	Action
1	Go to SMSP Restore Controller, and select the SharePoint Hive files you want to restore. **Note** It is recommended to select the files you need to restore instead of selecting all SharePoint Hive folders, since some of the files (such as dbghelp.dll, onetnative.dll, onetutil.dll, stswel.dll, owssvr.dll and some files in the bin folder) are being used and restoring them will cause an error.
2	Two important Options for restoring IIS and SharePoint Hive files: **Restore front-end file security:** This option will allow you to restore the content with securities. If you specify a path in the option. **Restore front-end files to alternate location**, but the path and the location of the backup files are in different machines, there will be some invalid permission settings caused by the different users and groups in these two machines. **Restore front-end files to alternate location:** This option will allow you to restore front-end files to an alternate location. You can either select a location on the agent tree or manually input a folder name as the location to restore the content. **Note** If the folder you selected as a destination is a new folder or an existing folder without any files which is in use and with the same name as the backup data, you can restore the data directly without stopping the services and the progress mentioned in step 1 and 2, otherwise, you need to stop the mentioned services and progress. This will keep the level structure of the folders.

Note

Before the restore, make sure the following Windows services are running: **Windows SharePoint Services Timer** and **Windows SharePoint Services Administration** (in SharePoint 2007) or **SharePoint 2010 Timer** and **SharePoint 2010 Administration** (in SharePoint 2010)

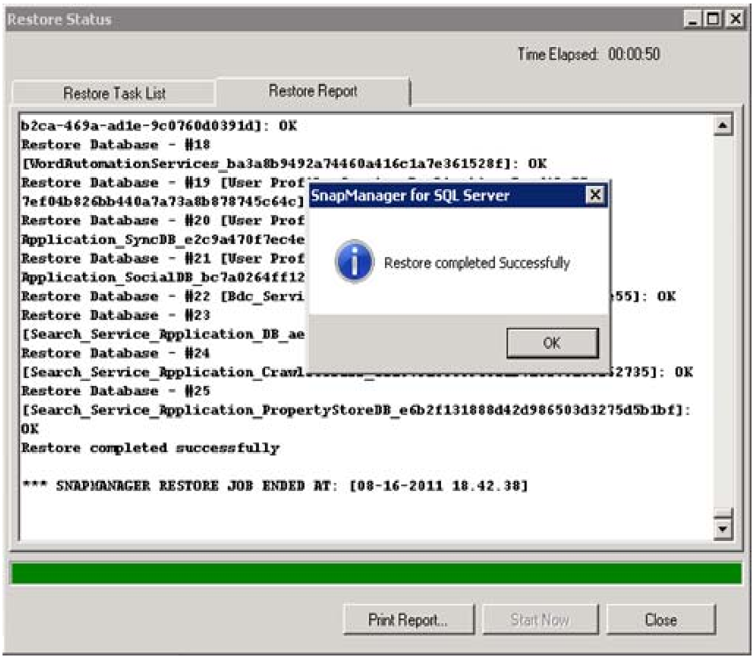
Restore from Alternate Storage Location

About Restoring from an Alternate Storage Location

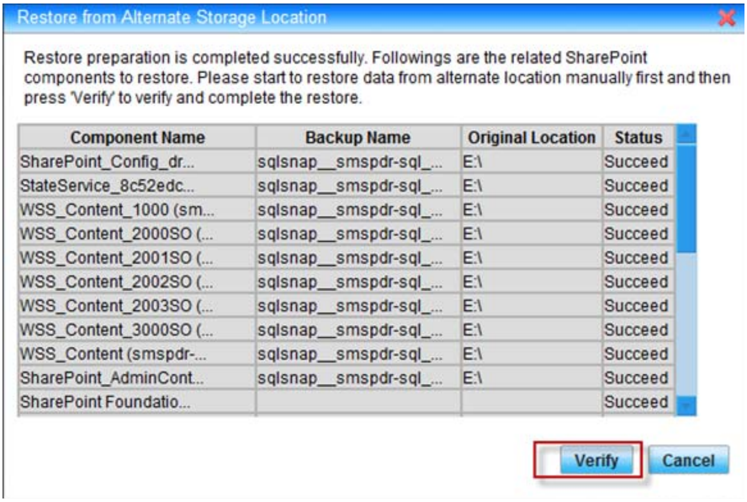
By using this option, you can restore data from an alternate storage location other than your primary storage (for example, if your data is stored on a SnapMirror copy or as a SnapVault backup). A wizard within the SnapManager for SharePoint interface will guide you through the restore process and the data will be restored manually using other tools (like SnapManager for Microsoft SQL Server). You need to find the snapshot of the DB backup according to the prompt and restore the data in SnapManager for Microsoft SQL Server.

To restore from an alternate storage location, complete the following steps:

Step	Action
1	From Restore Controller, select the content you need to restore.
2	Select the **Restore From Alternate Storage Location** option under **Restore Options**.
3	Click the **Go** button to launch the wizard.
4	Click **Next** to continue. SnapManager for SharePoint begins the process to prepare for the restore. During this process, the following processes occur: ● If the SSP was selected for restore, the SSP is deleted and all the related databases are detached from SharePoint. The search index is also deleted as part of the SSP deletion process. ● For any other SharePoint components, the related databases are detached from SharePoint.
5	After the restore preparation has completed successfully, the detailed information regarding all related components for manual restore is listed, including the detached databases and the location of the search index.

Step	Action
6	Perform a manual restore of the necessary components. The different databases are restored and different restore methods are used according to the different contents to be restored. For example, if restoring SSP, you should perform a DB restore to all the related databases. If restoring item, you should perform a clone restore to the content database that the item located.  Restore Status Time Elapsed: 00:00:50 Restore Task List Restore Report Print Report... Start Now Close SnapManager for SQL Server OK b2ca-469a-ad1e-9c0760d0391d]: OK Restore Database - #18 [WordAutomationServices_ba3a8b9492a74460a416c1a7e361528f]: OK Restore Database - #19 [User Prof 7ef04b826bb440a7a73a8b878745c64c] Restore Database - #20 [User Prof Application_SyncDB_e2c9a470f7ec4e Restore Database - #21 [User Prof Application_SocialDB_bc7a0264ff12 Restore Database - #22 [Bdc_Servi 55]: OK Restore Database - #23 [Search_Service_Application_DB_ae Restore Database - #24 [Search_Service_Application_Crawl 2735]: OK Restore Database - #25 [Search_Service_Application_PropertyStoreDB_e6b2f131888d42d986503d3275d5b1bf]: OK Restore completed successfully *** SNAPMANAGER RESTORE JOB ENDED AT: [08-16-2011 18.42.38] Restore completed Successfully For instructions regarding a restore from an alternate source, see the *SnapManager for SQL Server Administrator's Guide*.

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>7</td><td>
<p>After the manual restore is completed, click the <b>Verify</b> button to continue the restore process.</p>



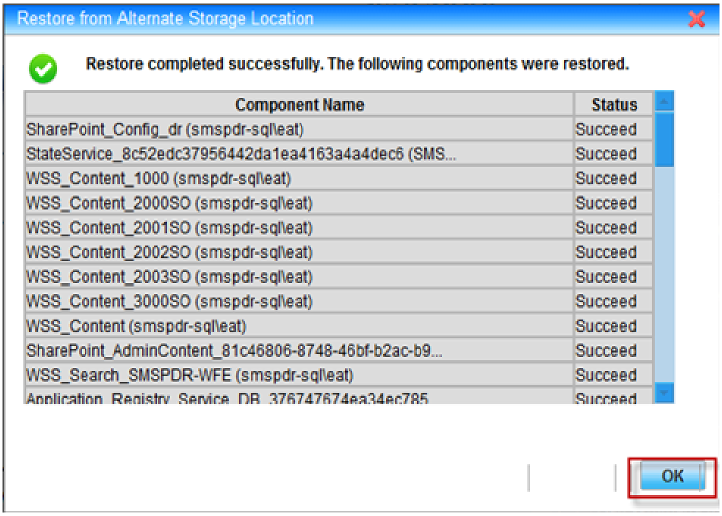
<p>Restore from Alternate Storage Location</p>

<p>Restore preparation is completed successfully. Followings are the related SharePoint components to restore. Please start to restore data from alternate location manually first and then press 'Verify' to verify and complete the restore.</p>

<table>
<tr><th>Component Name</th><th>Backup Name</th><th>Original Location</th><th>Status</th></tr>
<tr><td>SharePoint_Config_dr...</td><td>sqlsnap__smspdr-sql_...</td><td>E:\</td><td>Succeed</td></tr>
<tr><td>StateService_8c52edc...</td><td>sqlsnap__smspdr-sql_...</td><td>E:\</td><td>Succeed</td></tr>
<tr><td>WSS_Content_1000 (sm...</td><td>sqlsnap__smspdr-sql_...</td><td>E:\</td><td>Succeed</td></tr>
<tr><td>WSS_Content_2000SO (...</td><td>sqlsnap__smspdr-sql_...</td><td>E:\</td><td>Succeed</td></tr>
<tr><td>WSS_Content_2001SO (...</td><td>sqlsnap__smspdr-sql_...</td><td>E:\</td><td>Succeed</td></tr>
<tr><td>WSS_Content_2002SO (...</td><td>sqlsnap__smspdr-sql_...</td><td>E:\</td><td>Succeed</td></tr>
<tr><td>WSS_Content_2003SO (...</td><td>sqlsnap__smspdr-sql_...</td><td>E:\</td><td>Succeed</td></tr>
<tr><td>WSS_Content_3000SO (...</td><td>sqlsnap__smspdr-sql_...</td><td>E:\</td><td>Succeed</td></tr>
<tr><td>WSS_Content (smspdr-...</td><td>sqlsnap__smspdr-sql_...</td><td>E:\</td><td>Succeed</td></tr>
<tr><td>SharePoint_AdminCont...</td><td>sqlsnap__smspdr-sql_...</td><td>E:\</td><td>Succeed</td></tr>
<tr><td>SharePoint Foundatio...</td><td></td><td></td><td>Succeed</td></tr>
</table>

<p>SnapManager attempts to verify the manually restored components and completes the restore.</p>

<p>If the verification or the restore fails, a list of errors detected is displayed.</p>



<p>Restore from Alternate Storage Location</p>

<p>Restore completed successfully. The following components were restored.</p>

<table>
<tr><th>Component Name</th><th>Status</th></tr>
<tr><td>SharePoint_Config_dr (smspdr-sql\eat)</td><td>Succeed</td></tr>
<tr><td>StateService_8c52edc37956442da1ea4163a4a4dec6 (SMS...</td><td>Succeed</td></tr>
<tr><td>WSS_Content_1000 (smspdr-sql\eat)</td><td>Succeed</td></tr>
<tr><td>WSS_Content_2000SO (smspdr-sql\eat)</td><td>Succeed</td></tr>
<tr><td>WSS_Content_2001SO (smspdr-sql\eat)</td><td>Succeed</td></tr>
<tr><td>WSS_Content_2002SO (smspdr-sql\eat)</td><td>Succeed</td></tr>
<tr><td>WSS_Content_2003SO (smspdr-sql\eat)</td><td>Succeed</td></tr>
<tr><td>WSS_Content_3000SO (smspdr-sql\eat)</td><td>Succeed</td></tr>
<tr><td>WSS_Content (smspdr-sql\eat)</td><td>Succeed</td></tr>
<tr><td>SharePoint_AdminContent_81c46806-8748-46bf-b2ac-b9...</td><td>Succeed</td></tr>
<tr><td>WSS_Search_SMSPDR-WFE (smspdr-sql\eat)</td><td>Succeed</td></tr>
<tr><td>Application_Registry_Service_DB_376747674ea34ec785</td><td>Succeed</td></tr>
</table>

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

Note

For SharePoint 2010, when you select **SharePoint_Config** from the farm tree in the left pane, the option **Restore from alternate storage location** is checked by default. And a new field named **Passphrase** is added under this option. You can get the usage information of this field from the tooltip by putting the mouse on the icon next to the **Passphrase** textbox.

Granular Level Restore

You can also perform a granular level restore using the backup data in the alternate storage location:

Step	Action
1	In the granular restore interface, select the objects you want to restore.
2	Select the **Restore From Alternate Storage Location** checkbox.
3	Click **Go**. A GUI wizard opens to guide you through the manual restore process.
4	Follow the prompts to manually restore the content database backup to the temporary database, and then click **Verify**.
5	SnapManager for SharePoint uses the manually restored temporary database to complete the restore process. After the restore is completed, the detailed information about the restore is displayed.

Note

After the granular restore, you must delete the temporary database and disconnect the LUN.

Restore Limitations

SharePoint Component Restore Limitations

SnapManager for SharePoint has some limitations when performing a restore of SharePoint components:

- Only SharePoint components explicitly available for backup are covered; all other components that store information externally are not covered. For example, the Form-Based-Authentication (FBA) user database cannot be backed up or restored (FBA site collection is supported). Customizations deployed by SharePoint solutions can be restored to their deployed state. Similar to the previous limitation, if the specific customization stores information externally, these cannot be backed up or restored. If the original state was not restored for this reason, additional configurations of these features and solutions might need to be done after the restore.
- Customizations not deployed as SharePoint solutions (either deployed manually or through a separate installer) are not supported. If the customization is self-contained within the SharePoint hive scope, you may be able to restore it from the hive backup, but this is not supported.

Granular Restore Limitations

For the granular restore option, SnapManager for SharePoint does not support the following.

- Workflows are not supported at the site collection level granular restore and below. Only SharePoint built-in workflows can be restored from the content database level and the site collection level granular restore.

If there is other third party SharePoint related software running at the time of restore, conflicts may happen as they might be changing the same content as the restore process does. It is recommended to temporarily disable these applications during restore.

Storage Optimization 12

This section describes how to optimize your storage solutions using the SnapManager for SharePoint Storage Optimization Module.

The following topics are covered:

- **BLOB Provider Settings**
- **Advanced Settings**
- **Archiver**
- **Extender**
- **Archived Data Recover Overview**
- **Deleted Stub Policy**

Overview of Storage Optimization

The key to optimal SharePoint performance and productivity is efficient SQL storage management. SnapManager for SharePoint's Storage Optimization solutions provide the tools you need to keep your SQL resources optimized with intelligent archiving and real-time BLOB offloading.

With SnapManager for SharePoint Archiver, you can offload content to more cost-effective storage based on fully-customizable business rules or perform on-demand archiving, all without effecting end-user accessibility in SharePoint.

With SnapManager for SharePoint Extender, you can directly offload BLOB content to file-based storage, relieving SQL of such content while providing end-user access via SharePoint. Combined, these tools deliver the industry's most comprehensive and robust SharePoint storage optimization and performance solution.

Note

Both FBA and CBA are supported when archiving using the User rules, such as archiving at the list level using the *Owner* rule and archiving at the document level using the built-in metadata *Author*.

Note

For the Archiver module, including End-user archiving, the data for one web application can be stored in only one logical device, once you specify one logical device for a web application in one archiver plan, this relationship cannot be changed. Several web applications can be specified to use one logical device.

BLOB Provider Settings

About the EBS/RBS Provider Settings

The External BLOB Storage (EBS)/Remote BLOB Storage (RBS) interface was added to offload SharePoint content from SQL server storage. SnapManager for SharePoint Storage Optimization utilizes this interface to achieve this function. SnapManager for SharePoint BLOB Provider interacts with SharePoint for stub related operations:

- When a user accesses an Archiver stub, SharePoint will ask the BLOB Provider for the data stream. BLOB Provider will load data from the Media Service by the SnapManager for SharePoint Archiver Agent.
- When a user accesses an Extender stub, SharePoint will ask the BLOB Provider for the data stream. BLOB Provider will load data from the SnapManager for SharePoint Extender Agent directly.
- In Extender, if a user uploads a file, SharePoint will transfer the data stream to the BLOB Provider and the Extender Agent will then send the data to the corresponding logical device.

Installing BLOB Provider

You must install the BLOB Provider on all web front-end servers and the central administration server in the SharePoint farm before enabling the EBS/RBS option. The BLOB Provider can be installed when you enable the Storage Optimization agent.

Note

BLOB Provider must be installed during agent installation.

EBS vs. RBS

The following are the difference between EBS and RBS, and a brief explanation of where to use EBS or RBS.

- RBS can only be used in SharePoint 2010; EBS can be used in both SharePoint 2007 SP1+ and 2010, but it is on the deprecation list, which means its support will end in a future release of SharePoint.
- EBS must be enabled at SharePoint farm level; RBS can be enabled at content database level
- EBS can allow Extender settings at granularity of site collection; RBS is at content database level

- To perform migration from SharePoint 2007 EBS stubs to SharePoint 2010 RBS stubs, you must upgrade the SharePoint 2007 EBS stubs to SharePoint 2010 EBS stubs first and then upgrade the SharePoint 2010 EBS stubs to SharePoint 2010 RBS stubs.

Enabling EBS

To enable EBS, complete the following steps:

Step	Action
1	Select the farm you want to enable this feature on in the **Farm** field. Once selected, you can see the current EBS status and the appropriate information of the servers on the right hand of the screen.
2	You can click the **Refresh** button to update the farm's information. If the status in the **BLOB Provider** column is **Installed**, the BLOB Provider is already installed. If the status in the **BLOB Provider** column is **Uninstalled**, the BLOB Provider is not enabled. Check whether you have installed the SMSP agent with the Storage Optimization agent type properly, or confirm the information in Agent configuration tool again.
3	Click the **Enable** button to enable EBS, or the **Disable** button to disable it. When EBS is enabled, the **Enable** button will be grayed.

Enabling RBS

For SharePoint 2010 farm, you can select to enable Remote Blob Storage (RBS) and set it to use SnapManager for SharePoint external storage before utilizing any of SMSP's Storage Optimization capabilities.

RBS is a library API set that is incorporated as an add-on feature pack for Microsoft SQL Server. It can be run on the local server running Microsoft SQL Server 2008 R2, SQL Server 2008 or SQL Server 2008 R2 Express. To run RBS on a remote server, you must be running SQL Server 2008 R2 Enterprise edition. RBS is not supported for Microsoft SQL Server 2005.

To enable RBS, complete the following steps:

Step	Action
1	Select the desired farm from the left panel. If the selected farm is a SharePoint 2010 farm, you will see the EBS and RBS radio buttons on the right panel.
2	Select the RBS. Within the **General** tab, you can view the **RBS Provider** status of the selected farm.
3	Within **Settings** tab, select the Web application and the appropriate database in which you want to install the RBS provider by checking the corresponding checkbox. Clicking the corresponding content database, you can view the site collection in it.
4	If you want to install the RBS Provider for the new database of specific Web application, you can select the Web application and set a schedule for it. **Note** If RBS is installed for a content database and the RBS is not uninstalled later, before using the content database in Storage Optimization module, you must disable its RBS settings first and enable it again. Use the calendar icon next to the **Start Time** field to select a date and time for the archive job to run. You may also optionally set an interval for the Archiving job to run on an only once, hourly, daily, weekly, or monthly basis.
5	Click **Apply** to apply the settings. If you want to run the installation immediately, click **Run Now**.

Check the RBS Status Using the Tool

In the SharePoint 2010 RBS environment, you can check the RBS status of the content databases, which have installed RBS using the *SMSPTool2010StorageCheckRBSStatus.exe* tool in the installation path of the Agent which is <*C:\Program Files\IBM\SnapManager for SharePoint\VaultClient\bin*> by default.

Note

You should use the Agent Account to run the tool.

Double-click the tool to run it and the following information will be shown in the command line interface:

- **Content Database Name**

  The name of the content database.

- **Active Provider Name**

  The RBS Provider being used.

- **Minimum Blob Storage Size**

  It is the *Document Size* configured in *Extender* module. If the *Document Size* is not configured, the value will be *9223372036854775807*. The unit of this value is **Byte**.

Press **Enter** to exit the tool after it completes.

Note

If no content database enabled RBS or the RBS client library was not installed on the server (where you run the tool), no information will be shown in the tool interface after the execution. Click ☒ to close the tool.

Advanced Settings

About the Advanced Settings

In SharePoint 2007 environment, in order to make sure the archived/extended Microsoft Office files can be accessed and modified correctly, a default device must be configured for the corresponding SharePoint 2007 farm in **Advanced Settings**.

Note

For SharePoint 2010 environment, there is no need to configure the default device due to enhancement on accessing the archived/extended Microsoft Office files.

How to Configure the Default Device

To configure the default device for the SharePoint 2007 farm, complete the steps below.

Step	Action
1	Click on the corresponding SharePoint 2007 farm in the left panel.
2	Select a default device from all the available logical devices in the **Default Device** drop-down box. **Note** You can click the **Default Logical Device** link in the **Device Settings** field to navigate to the **Device Manager**; however, all the unsaved changes will be lost.
3	Click **Apply** to save the setting.

Archiver

Overview of the Archiver

The Archiver is an item level archiving engine that seamlessly moves business-rule selected content off of the production SQL servers while still allowing that content to be indexed, searched, viewed, and accessed from within the SharePoint environment. Archiver will move the specified content off of the SQL database where SharePoint normally writes data, and into a data file that can be stored on a LUN, or CIFS from SAN or NAS.

In order to use the Archiver module, we recommend using an account with full administrative access to SharePoint and the SQL servers. However, backup and restore can still be performed using an account with the following access right:

- Member of the local admin group (enough to access the files on the local SharePoint server).
- Member of the SharePoint farm admin group.
- Member of the database owner group of the SharePoint content DB.
- Full control for the corresponding web application.

Note

To run Archiver, make sure all front-end servers and the central admin server in this farm have the Archiver Agent installed.

Note

Managed Metadata Web Service is supported in Archiver module. You can perform the Archiver job based on the specified Managed Metadata column or Content Type.

Plan Builder - Setting the Scope

The scope of an Archiver plan defines the areas of SharePoint that will be searched each time the plan runs. New content under these selected areas will automatically be scanned as well.

To set the scope of an Archiver plan, complete the following steps:

Step	Action
1	Select a farm from the **Farm name** drop-down box. Make sure that the selected agent has content enabled for archiving as described in the section above.
2	Select an **Agent Group** from the available list. See "Agent Group" on page 59 of this manual for more information on Agent Groups. The selected **Farm name** is now displayed.
3	Click on the **Farm name** to expand the tree, and then select the desired content using the check boxes next to each corresponding level.

Include/Exclude New Content in SharePoint When Archiving

In order to include/exclude the new SharePoint content, see the detailed information below:

- **To Include New SharePoint Content**

  Select the corresponding node on the tree in the Plan Builder of Archiver.

- **To Exclude New SharePoint Content**

  Expand the data tree under the specific node. Click the triangle symbol at the bottom-right corner of the node's icon once; all of the expanded nodes except the top node will exclude the new SharePoint content. Click the triangle symbol at the bottom-right corner of the node's icon twice; all the nodes besides the top node will exclude the new SharePoint content.

Configuring Basic Plan Settings

Under the **Settings** tab, you will see four options: **Storage Manager**, **Configuration**, **Reporting**, **and Advanced**.

Storage Manager:

- **Logical Device**

  Select a logical device from the drop-down list. This will list all the available logical devices.

- **Data Retention**

Select the data retention policy from the drop-down list. This lists all of the retention policies which have been previously configured in Control Panel.

- **Integrate with SnapLock**

  If you select this option, Archiver will save the archived data to available SnapLock devices. Make sure you have set up a SnapLock Archiver Data device before using this option.

Configuration:

- **Compression**

  Allows you to specify whether to compress data once it has been archived and whether the Media Service or the SharePoint Agent should perform the compression. Note that by default, **Compression** is not enabled.

Reporting:

- **E-mail Notification**

  Select an **E-mail Notification Profile**. See "E-mail Notification" on page 113 of this User Guide for instructions on creating e-mail notification profiles.

Advanced:

- **Create Stub**

  Selecting this option will create a stub placeholder for the archived content in SharePoint. You can select to change the file's icon as shown in SharePoint, add a metadata column, or make the stub read-only by checking the corresponding check boxes. By default, the file icon in SharePoint is set to change to the **archived** icon.

Note

SharePoint performance may be affected if there are many objects with unique permissions. Take this into consideration when use the **Read-only Stub** option.

- **Generate Full Text Index**

  Ensures that the archived content can be fully indexed and searched. To enable indexing check the **Generate Full Text Index** checkbox.

- **Include data from Extender**

  Archives the data in SharePoint which has been already be moved by Extender.

About Data Retention

Retention of archived data is configured based on the amount of time to keep archived data, and is automatically triggered when an archived job is completed that fits the preset criteria. You can view "Data Retention" on page 104 of this manual for more information.

If SnapLock devices are used, SnapManager Media Service will set the expiration date for the archived data according to retention settings. If this length is shorter than the SnapLock device minimum retention, and the data already expired according to SnapManager retention setting, the deletion will fail and be retried in future retention maintenance operations. Set the length no shorter than the SnapLock device minimum retention.

Note

It is recommended to set the archiver retention time longer than orphan retention time as orphan data will be deleted when running the archiver retention rule.

Setting Plan Rules

Under the **Rules** tab, you can select various levels to assign archiving rules. Wildcards (***.***) are supported when configuring rules for Documents, Document version, Attachments, and other rules.

Stubs will be created in your SharePoint Document Libraries, allowing you to view the archived contents directly from SharePoint.

For SharePoint 2010, the archiving rules at site collection, site and list level are supported from SnapManager 6.1 version.

Archiving at the Site Collection level:

Archiving at the Site Collection-level allows users to archive entire sites (with their child nodes) according to established archiving rules.

- **Name**

  Enter the name of a specific site or enter any wildcard (*).

- **Created Time or Modified Time**

  Fill in the optional time fields by selecting the **...** button.

  If you select **Before**, any sites created or modified before this time will be archived.

  If you select **Older Than**, you must enter a positive integer for the number of days, weeks, months, or years. Only the content which is older than the specified time period will be archived.

- **Owner**

  Enter the specified owner set in SharePoint.

- **Template**

  Enter a name in the **Template** field to select sites that all follow a certain template.

- **Site Size Trigger**

  Enter a positive integer set to KB, MB, or GB. Any site larger than the specified number will be archived.

- **How Long to Keep Stub**

  This option will limit the amount of time a stub is kept in the SharePoint environment, and check whether the stub exceeded the specified time in the next archiver job. Once this stub is marked and removed, the content can no longer be accessed through SharePoint, and must be restored from SnapManager for SharePoint. This value can be specified in Days, Weeks, Months, or Years.

Archiving at the Site-level:

Archiving at the Site-level allows for the archiving of sites with their child nodes according to established archiving rules.

- **Name**

  Enter the name of a specific site or enter any wildcard (*).

- **Created Time or Modified Time**

  Fill in the optional time fields by selecting the **...** button.

  If you select the **Before**, any sites created or modified before this time will be archived.

  If you select the **Older Than**, you must enter a positive integer for the number of days, weeks, months, or years. Only the content which is older than the specified time period will be archived.

- **Owner**

  Enter the specified owner set in SharePoint.

- **Template**

  Enter a name in the **Template** field to select sites that all follow a certain template.

- **How Long to Keep Stub**

  This option will limit the amount of time a stub is kept in the SharePoint environment, and check whether the stub exceeded the specified time in the next archiver job. Once this stub is marked and removed, the content can no longer be accessed through SharePoint, and must be restored from SnapManager for SharePoint. This value can be specified in Days, Weeks, Months, or Years.

Archiving at the List-level:

- **Name**

  Enter the name of a specific site or enter any wildcard (*).

- **Created Time or Modified Time**

  Fill in the optional time fields by selecting the ... button.

  If you select the **Before**, any sites created / modified before this time will be archived.

  If you select the **Older Than**, you must enter a positive integer for the number of days, weeks, months, or years. Only the content which is older than the specified time period will be archived.

- **Owner**

  Enter the specified owner set in SharePoint.

- **How Long to Keep Stub**

  This option will limit the amount of time a stub is kept in the SharePoint environment, and check whether the stub has exceeded the specified time in the next archiver job. Once this stub is marked and removed, the content can no longer be accessed through SharePoint, and must be restored from SnapManager for SharePoint. This value can be specified in Days, Weeks, Months, or Years.

Archiving at the Item-level:

- **Name**

  Enter the name of a specific item or enter any wildcard (*). For example, to archive all items enter * in this field.

- **Created Time or Modified Time**

  Fill in the optional time fields by selecting the **...** button.

  If you select the **Before**, any item created / modified before this time will be archived.

  If you select the **Older Than**, you must enter a positive integer for the number of days, weeks, months, or years. Only the content which is older than the specified time period will be archived.

- **Owner**

  Enter the specified owner set in SharePoint.

- **Last Modifier**

  Enter the specified last modifier set in SharePoint.

- **Content Type**

  Enter the **Content Type** to be archived in the field provided. This can either be a standard SharePoint content type (Announcement, Contact, etc.) or a custom type.

Managed Metadata Web Service is supported here. You can perform the Archiver job based on the specified Content Type.

- **Column**

  You can also archive based on the Column rule by clicking the **Column Settings** button. This refers to any column related to an item in the SharePoint environment.

  Within the **Built in Metadata** tab, you can select the condition from the drop-down box and enter the values for the given fields. Click the **Apply** button to save your settings.

  Within the **Customized Metadata** tab, click the **Add** button to add a search line. Enter the field information; select the **Type** and **Condition** from the drop-down list, and enter the corresponding value. Click the **Apply** button to save your settings.

  Managed Metadata Web Service is supported here. You can perform the Archiver job based on the specified **Managed Metadata** column.

Archiving Based on the Item Version:

- **Name**

  Enter the name of a specific item or enter any wildcard (*). For example, to archive all the versions of item **test**, enter **test** in this field.

- **Modified Time**

  Fill in the optional time fields by selecting the **...** button.

  If you select **Before**, any content on this level modified before this time will be archived.

  If you select **Older Than**, you must enter a positive integer for the number of days, weeks, months, or years. Only the content which is older than the specified time period will be archived.

- **Last Modifier**

  Enter the specified last modifier set in SharePoint.

- **Keep History Version**

  Enter the number of past versions to keep on the SharePoint production server.

Note

The current version does not count. If **1** is entered, the current version is kept along with one additional version history.

Archiving at the Document-level:

Archiving at the Document-level allows users to archive documents and all of their corresponding versions according to established archiving rules.

- **Document Name**

  Enter the name of a specific document or enter any wildcard (*). For example, to archive all Microsoft Word documents, enter ***.doc** in this field.

- **Created Time or Modified Time**

  Fill in the optional time fields by selecting the **...** button.

  If you select the **Before**, any content on this level created / modified before this time will be archived.

  If you select the **Older Than**, you must enter a positive integer for the number of days, weeks, months, or years. Only the content which is older than the specified time period will be archived.

- **Owner**

  Enter the specified author set in SharePoint.

- **Last Modifier**

  Enter the specified last modifier set in SharePoint.

- **Document Size**

  A positive integer can be entered (and set to KB, MB, or GB). Any file larger than the specified number will be archived.

- **How Long to Keep Stub**

  This option will limit the amount of time a stub is kept in the SharePoint environment, and check whether the stub exceeded the specified time in the next archiver job. Once this stub is marked and removed, the content can no longer be accessed through SharePoint, and must be restored from SnapManager for SharePoint. This value can be specified in Days, Weeks, Months, or Years.

- **Column**

  You can also archive based on the **Column** rule by clicking the **Column Settings** button. This refers to any column related to an item in the SharePoint environment.

  Within **Built in Metadata** tab, you can select the condition from the drop-down box and enter the values for the given fields. Click the **Apply** button to save your settings.

  Within **Customized Metadata** tab, click the **Add** button to add a search line. Enter the field information; select the **Type** and **Condition** from the drop-down list, and enter the corresponding value. Click the **Apply** button to save your settings.

Managed Metadata Web Service is supported here. You can perform the Archiver job based on the specified Managed Metadata column.

Archiving Based on Document Version:

Archiving based on the Document Version will archive based on the versions on a particular document or document type.

- **Document Name**

  Enter the name of a specific document or enter any wildcard (*). For example, to archive all Microsoft Word documents, enter ***.doc** in this field.

- **Modified Time**

  Fill in the optional time fields by selecting the **...** button.

  If you select the **Before**, any content on this level modified before this time will be archived.

  If you select the **Older Than**, you must enter a positive integer for the number of days, weeks, months, or years. Only the content which is older than the specified time period will be archived.

- **Modifier**

  Enter the name of the last person to modify this document.

- **Document Size**

  A positive integer can be entered (and set to KB, MB, or GB). Any file larger than the specified number will be archived.

- **How Long to Keep Stub**

  This option will limit the amount of time a stub is kept in the SharePoint environment, and check whether the stub exceeded the specified time in the next archiver job. Once this stub is marked and removed, the content can no longer be accessed through SharePoint, and must be restored from SnapManager for SharePoint. This value can be specified in Days, Weeks, Months, or Years.

- **Keep History Version**

  Enter the number of past versions to keep on the SharePoint production server.

Note

The current version does not count. If **1** is entered, the current version is kept along with one additional version history.

Archiving Based on Attachment:

The Attachment rule will archive attachments to list items within SharePoint.

- **Attachment Name**

  Enter the name of a specific attachment or enter any wildcard (*). For example, to archive all Microsoft Word documents, enter ***.doc** in this field.

- **Created Time**

  Fill in the optional time fields by selecting the **...** button.

  If you select the **Before**, any content on this level created before this time will be archived.

  If you select the **Older Than**, you must enter a positive integer for the number of days, weeks, months, or years. Only the content which is older than the specified time period will be archived.

- **Owner**

  Enter the specified owner set in SharePoint.

- **Attachment Size**

  A positive integer can be entered (and set to KB, MB, or GB). Any file larger than the specified number will be archived.

- **How Long to Keep Stub**

  This option will limit the amount of time a stub is kept in the SharePoint environment, and check whether the stub exceeded the specified time in the next archiver job. Once this stub is marked and removed, the content can no longer be accessed through SharePoint, and must be restored from SnapManager for SharePoint. This value can be specified in Days, Weeks, Months, or Years.

Results of Archive Rules

Site Collection Rule: After a site collection is archived, only a shell site collection will be left. All of the lists, sub sites, and web parts have been deleted, and the default page is blank. The site collection description will indicate that it was archived.

Site Rule: The content of the specified site will be archived. If all the sites of the site collection are archived using this rule and you do not select to create stubs, only the shell of the top level site will be kept. All of the lists, sub sites, and web parts have been deleted, and the default page is blank.

List Rule: Items in the list will be archived and deleted. The list will still exist without any content. The list description will indicate that it was archived.

Item Rule: The item will be deleted after it is archived.

Item Version Rule: After the version is archived by the rule, the history version will be deleted.

Document Rule: If you select to create a Stub, the document will be saved as a stub, and its content will be backed up into the corresponding logical device. If you do not select this option, after the content is backed up into media, the document will be deleted.

Document Version Rule: After the eligible version is archived, it will not be deleted in the history version.

Attachment Rule: After the attachment is archived, it does not change in item view, but you must enable the EBS to open it.

Setting Plan Filters

Under the **Scope Filter** tab, you can set the filters on Site Collection, Site, and List level in order to set the scope for archiving. This can be done by typing either the exact URL or using wildcards (*****) in the appropriate fields.

To setup these filters, complete the following steps:

Step	Action
1	Under the **Scope** tab, uncheck the **No filtering** option to enable the Scope Filter.
2	You can select **Site Collection**, **Site**, and **List** level to enter the corresponding information. The level you select in the **Scope Filter** will limit the scope of all levels below it in the Rules. **Example**: If you select the site collection in the **Scope Filter**, then all levels below the Site Collection such as Site, List, Item you set in the Rules will be limited for this scope filter. Only the content which matches the setting's rules and is under the search scope will be archived.

Rules vs. Filters

In order to run an archiving plan, you must set up the archiving rules (mandatory), and set up the filter rules (optional). Archiver will find the content which matches the rule conditions specified and archive the content. Archiver rules check content from the top down, from site collection rules down to attachment rules. Once one level's content matches the applied rules, it does not check the lower level rules. For example, once there is a site matching a rule on the site level, it does not check whether the lists under the site matched the rule on the list level, and the matched site will be archived.

With regards to filters, Archiver finds the filtered content, and then applies the archiving rule on the filtered content, archiving any content fitting the specified rules.

Scheduling

Select a time zone from the time zone drop-down box, and then using the calendar icon next to the Start Time field, select a date and time for the Archiver job to run. You may also set the job to run on an hourly, daily, weekly, or a monthly schedule. The advanced intervals are as follows:

- **Hourly:**

  You can set the plan to run during production hours only, specified in the time window provided, or at specific hours set in the **Select Time Below** fields.
- **Daily:**

  Runs the plan once a day on weekends only or weekdays only.
- **Weekly:**

  Specify which days of the week to run the plan on, and after how many weeks to recur.
- **Monthly:**

  Sets up a custom monthly plan.

You can also specify a **Time Window** for this job under the **Advanced options**. This will allow you to terminate the plan after a number of occurrences, or by an appointed date and time.

Running an Archiving Plan

After setting the scope, the basic settings, the rules, and an optional scope filter, you can now run an Archiver plan.

To run an archiving plan, complete the following steps:

Step	Action
1	Enter the plan name into the provided field.

Step	Action
2	Click the **Save** button. If you desire to begin the archiving process immediately, click the **Run Now** button; otherwise, wait for the schedule. The corresponding SnapMirror will be updated automatically after the Archiver job.

Archiver Restore

Although you can choose to allow individual users to restore archived content to production direct from the SharePoint Site, the Archiver Restore is a quick way to restore archived documents from the SnapManager for SharePoint GUI back on to the SharePoint environment directly. To execute an archive restore through the Archiver Restore, complete the following steps:

Step	Action
1	Select a farm from the drop-down list. The selected farm name will appear underneath.
2	You can select the **Site Cascade** option. If checked, the site and all the sub sites in this structure will be included in the restore. If left unchecked, selecting a site will only include the contents of this site. This should be used in the instance when sub sites appear on the same level as their parent node in the SharePoint tree (due to display restrictions).
3	Click the farm name to expand the tree.
4	You can also find the content you want to restore by clicking the **Advanced Search** or **Search** button after the URL.
5	Browse the tree structure for the content you want to restore. In order to see the content inside a folder or list, you can click the **Browse Content** icon after the URL. The content will be listed in the pop-up window. Select the documents to restore. Check the corresponding box if you want to restore it. To view the item's detailed information, click the **Details** button.
6	If you want to restore the data to SharePoint, you can select the **Show the items in SnapLock** option to load the content in SnapLock.

Step	Action
7	Select the content you want to restore by checking corresponding box.
8	Select an **Agent Group** to restore to on the bottom of the screen.
9	Select a start time for the restore to run. By default, **Now** is selected and will run the process as soon as the **Go** button is clicked. You can set a scheduled date and time for this restore by pressing the calendar icon and selecting a date and time in the calendar dialog box. Click the **OK** button.
10	Select a restore option from the drop-down list: **Not Overwrite** or **Overwrite**. **Not Overwrite:** SnapManager for SharePoint does not restore the content if it already exists on the destination. For example, if an entire folder's content is selected for restore but only one document was removed from the destination folder, only that one document is restored. **Overwrite:** This option restores the content over whatever exists on the destination. This deletes the content on the destination and replaces it with the content selected to be restored.
11	You may enter a description in the field provided to help distinguish this job in the Job Monitor.
12	Click the **Go** button. If you set the start time as now, the restore job will run immediately, otherwise, it will run the job at the scheduled time. You can view the job report by clicking the **Go to Job Report** button in the dialog box, or click the **Close** button to close the dialog box.

Converting Stubs to Content

You can convert archived content back to the original SharePoint location according to the stub. To convert a stub back to content, complete the following steps:

Step	Action
1	Select a farm and an agent group from the list. The selected farm name will appear underneath.
2	You can select the **Site Cascade** option. If this is checked, the site and all the sub sites in this structure will be included. If left unchecked, selecting a site will only include the contents of this site. This should be used in the instance when sub sites appear on the same level as their parent node in the SharePoint tree (due to display restrictions). You can also select to restore the data from Extender by checking the corresponding checkbox.
3	Click the farm name to expand the data tree. Select the content you want to restore by checking the corresponding box.
4	Click the **Go** button to run the job, all of the stubs will be converted to content.

Searching the Content

Archiver Restore allows you to search through all archived data using specified search scopes and settings. In order to use the Archiver Restore to browse the data you must first set the **Search Scope** described below. **Offline Download Location** setup can also be implemented to allow you to view the data while offline.

To search the specified content, complete the following steps:

Step	Action
1	Click the advanced search magnifying glass icon after the URL. A search setting dialog box will appear.

Step	Action
2	There are several options for the user to set up the search scope conditions: **Keyword:** This field allows you to search for keywords in the content selected. It will return all results for this keyword in either content or names. Multiple entries can be separated by entering a semicolon, **OR**, or **-** . For more information about keywords, see "Keyword Usage Options" on page 209. **Matching results:** Selecting either **content** or **metadata** will limit the keyword results returned to either content or metadata. **Type:** Selecting either **document** or **item** will limit the keyword results returned to SharePoint type. **Archive date range:** This allows the user to specify the date range that the content was archived. **File format:** Using this field, you can specify multiple file types to either be included for the search. Use **Ctrl+click** to select multiple options. You can also specify a custom extension in the **Other...** field provided. **Content Type:** Using this field, you can specify multiple content types to either return for the search. Use **Ctrl+click** to select multiple types. You can also specify custom content in the **Other...** field provided.
3	Click the **More Metadata** button for additional search options. Under the **Built-in Metadata** tab, select the **Condition** from the drop-down boxes in the middle column. Enter the corresponding **Value** in fields provided. You can also go to the **Customized Metadata** tab to add search conditions for customized SharePoint metadata. Click the **Add** button and fill out the new field provided. You can add and delete from this list as much as necessary.
4	Click the **Search** button, the search result will be displayed under the **Search Mode** tab.

Step	Action
5	Select the item or items you want to download by checking the corresponding checkbox. Click the **Export** button to export the item or items immediately. If you want to download the items offline, click the **Offline Download** button, and enter the job name and select a download location for the items in the dialog box. Click **OK** to run the download job.

Keyword Usage Options

The following table is a keyword logic list:

	Keyword	Description
Logic relation	b AND c / +b+c	This serves as **AND** logic, all search results listed will include **b** and **c.**
	b OR c / b c	This serves as **OR** logic, all search results listed will include **b** or **c**.
	b AND NOT c / +b-c	This serves as **AND NOT** logic, all search results listed will include **b** but exclude **c**.
Wildcards	*	This wildcards represents random characters.
	?	This wildcards represents one character.
Field	title: **“The Right Way”**	This field represents to search the content whose title is **“The Right Way”**.

About End User Archiving

End User Archiving allows you to install the Archiver feature on SharePoint for users who do not have permissions for the SnapManager for SharePoint to archive selected SharePoint content. You can also view the job process and detailed information via the Job Monitor.

Note

End-User Archiving function is not available for SharePoint 2010 in this SnapManager version.

If you enabled End-User Archiving in SharePoint 2007 environment and upgrade to SharePoint 2010, you can perform **one** of the following operations to disable End-User Archiving:

- Retract Solution Manually

  Navigate to SharePoint 2010 Central Administration. Click **System Settings** and find **Manage farm solutions** under **Farm Management.** Retract the *smsp2007archiveenduserarchiving.wsp* solution.

- Configure the SMSP Agent

  Find the *A*gent Configuration Tool and uncheck the **Archiver** module under **Storage Optimization** tab; click **Confirm** to confirm the configuration. After the Agent service is restarted, run the Agent Configuration Tool and check the **Archiver** module under **Storage Optimization** tab. Click **Confirm** to confirm the configuration and click **Yes** to restart the Agent service.

Installing the End-User Archiver Feature

After setting up the End User Archiving settings, you can install the Archiver feature.

To install the End User Archiver Feature, complete the following steps:

Step	Action
1	Select the farm where you want to install the Archiver Feature in the left column, the available Web Applications will be listed on the right-hand side of the screen.
2	Click **Install Feature** to install the solution.
3	Select the **End User Archiving Setting** from the drop-down list.

Step	Action
4	Click **Apply** to apply the corresponding setting to the Web Application, and then the **Enable** button in the **Enable End User Archiving** column will be enabled.
5	Click the **Enable** button. The feature for the corresponding Web Application will be enabled. **Note** If your SMSP is upgraded from a previous version, you must enable the Web Application you want to enable again.

Configuring the End User Archiving Setting

You must configure the basic settings under **End User Archiving Settings** before installing this feature.

To Configuring the End User Archiving settings, complete the following steps:

Step	Action
1	Enter the profile name into the provided field.
2	Within the **Storage Manager** tab, you can set up the storage for the archived data. **Logical Device:** Select the logical device from the drop-down list. This lists all the available logical devices. This item is mandatory. **Data Retention:** Select the retention policy from the drop-down list. This lists all of the retention policies configured in the Control Panel. **Integrate with SnapLock:** If you select this option, The archived data will be saved to the SnapLock devices. Make sure you have set up a SnapLock Archiver Data device. **Note** For one web application, the end user archiving data needs to use the same logical device as the one used by the corresponding Archiver plan.

Step	Action
3	Within the **Configuration** tab, you can specify whether to compress the archived data, and if so, whether such activities will be carried out on the Media Agent or the SharePoint Agent. Note that by default, compression is not enabled.
4	Within the **Advanced** tab, there are two options you can select: **Make Stub Read-Only:** Makes the stub read-only. **Automatically Generate Full Text Index:** This option will generate a full text index for the content you select in the archiver plan. You can then use **Full Text** type to search the content when you do the restore.
5	Click the **Save** button. The profile will be listed on the right panel.

End-User Archiving Data in SharePoint

Data can be archived in five levels: Site Collection, Site, List, folder, Document, and item by using the End-user Archiver feature in SharePoint.

For Site Collection, Site, or List level, go to the corresponding **Settings** page to archive. For Document or Item level, you should select the appropriate object to archive it. If you archive a folder, it will archive all of the content in this folder and its subfolder.

End-User Archiver User Permissions

In order to run an archiver job, you must have permissions for different levels.

Site Collection: You can use the **Archive this Site Collection** feature, if you have the **Site Collection Administrators** permissions.

Site: If you want to archive the Site by using the End-user Archiver feature, make sure that you have the **Full Control** permissions or above.

List: You need have **Full Control** Permission of the list to run a List level End User archiver job.

Item: You must have **Contribute** permissions of the Item level, you can archive the item, document, and folder by using End-user Archiver feature.

Offline Download Location

To set up a download location for the Archiver content, complete the following steps:

Step	Action
1	Enter the profile name into the provided field.
2	Input the username in **domain\username** format and the password to set up access to the path where the data will be written to and stored.
3	Click the **Test** button to test the path. After testing successfully, click the **Save** button to save the configuration.

Upgrade SharePoint 2007 EBS Stubs to SharePoint 2010 EBS Stubs

After attaching one content database containing stubs of SharePoint 2007 EBS environment to a SharePoint 2010 EBS environment, complete the following steps to ensure these stubs can be used.

Note

Make sure the SharePoint Agents on both SharePoint 2007 environment and SharePoint 2010 environment are pointing to the same SnapManager and the appropriate Logical Device which stores the real data of the stubs can be connected.

Step	Action
1	Find BLOB Provider Settings and enable the EBS setting on the specified SharePoint 2010 farm.
2	Go to the Plan Builder of Archiver, select all the nodes which contain the SharePoint 2007 EBS stubs, and set the corresponding plan settings. All the site collections and the content whose levels are below Site Collection must be selected. **Note** Make sure no SharePoint data will be archived by the Archive Rules configured above.

Step	Action
3	Click **Save** to save the plan, and click **Run Now** to run the plan. After the job completes successfully, the upgrade is completed. **Note** If you want to store different site collections into different Logical Devices, create several separate plans.

Upgrade SharePoint 2007 EBS Stubs to SharePoint 2010 RBS Stubs

For the SharePoint 2010 environment which upgrades from the SharePoint 2007 environment, complete the following steps to upgrade the EBS Stubs in SharePoint 2007 to SharePoint 2010 RBS Stubs.

Note

Make sure the SharePoint Agents on both SharePoint 2007 environment and SharePoint 2010 environment are pointing to the same SnapManager and the appropriate Logical Device which stores the real data of the stubs can be connected.

Step	Action
1	Find BLOB Provider Settings and enable the EBS setting on the specified SharePoint 2010 farm.
2	Go to the Plan Builder of Archiver, select all the nodes which contain the SharePoint 2007 EBS stubs, and set the corresponding plan settings. All the site collections and the content whose levels are below Site Collection must be selected. **Note** Make sure no SharePoint data will be archived by the Archive Rules configured above.
3	Click **Save** to save the plan, and click **Run Now** to run the plan. **Note** If you want to store different site collections into different Logical Devices, create several separate plans.

Step	Action
4	Find BLOB Provider Settings, select the **RBS** option, and select all the Content Databases which contain the EBS Stubs in the **Settings** tab. Click **Apply**, then click **Run Now** to install RBS for the SharePoint 2010 environment.
5	Run **Command Prompt** using the Agent Account.
6	Find the convert tool in the following path on SMSP Agent server: *<…\ SnapManager for SharePoint\VaultClient\bin\SMSP2010EBSToRBSStubConvertTool.exe>*

Step	Action
7	Drag the tool into the command line interface and execute it to convert the EBS stubs to RBS stubs. You can also switch to the path first and then run the tool by entering its name and the corresponding parameters. There are several parameters you can select: **-help:** The user can use this parameter to get more information. The format of the command is: SMSP2010EBSToRBSStubConvertTool.exe -help **-preview:** The user can use this parameter to get the hierarchy of the site collections where the EBS stubs exist. Multiple URLs of the web applications can be entered when separated by semicolons. The format of the command is: SMSP2010EBSToRBSStubConvertTool.exe [-farm|-webapplication|-sitecollection] –url <urls> -preview For example: SMSP2010EBSToRBSStubConvertTool.exe -webapplication –url http://test1:4000; http://test2:5000 -preview Enter Y to proceed with the convert process on the specified SharePoint content. Enter any other key to exit the convert process without running. **Note** If the scope is -farm, no URL needs to be entered.
8	After the tool finishes running, find BLOB Provider Settings and disable the EBS setting on the specified SharePoint 2010 farm. The upgrade is completed.

Upgrade SharePoint 2010 EBS Stubs to SharePoint 2010 RBS Stubs

Complete the steps below to upgrade the SharePoint 2010 EBS Stubs to SharePoint 2010 RBS Stubs.

Step	Action
1	Find BLOB Provider Settings, select the **RBS** option, and select all the Content Databases which contain the EBS Stubs in the **Settings** tab. Click **Apply**, then click **Run Now** to install RBS for the SharePoint 2010 environment.
2	If the URL of the archived content changes, go to the Plan Builder of Archiver, select all the nodes which contain the site collections whose URLs are changed, and set the corresponding plan settings. After the plan is saved, go to Step 3. If the URL of the archived content does not change, go directly to Step 3. **Note** If you want to store different site collections into different Logical Devices, create several separate plans.
3	Run **Command Prompt** using the Agent Account.
4	Find the convert tool in the following path on SMSP Agent server: *<…\ SnapManager for SharePoint\VaultClient\bin\SMSP2010EBSToRBSStubConvertTool.exe>*

Step	Action
5	Drag the tool into the command line interface and execute it to convert the EBS stubs to RBS stubs. You can also switch to the path first and then run the tool by entering its name and the corresponding parameters. There are several parameters you can select: **-help:** The user can use this parameter to get more information. The format of the command is: SMSP2010EBSToRBSStubConvertTool.exe -help **-preview:** The user can use this parameter to get the hierarchy of the site collections where the EBS stubs exist. Multiple URLs of the web applications can be entered when separated by semicolons. The format of the command is: SMSP2010EBSToRBSStubConvertTool.exe [-farm|-webapplication|-sitecollection] –url <urls> -preview For example: SMSP2010EBSToRBSStubConvertTool.exe -webapplication –url http://test1:4000; http://test2:5000 -preview **Note** If the scope is -farm, no URL needs to be entered.
6	Enter **Y** to proceed with the convert process on the specified SharePoint content. Enter any other key to exit the convert process without running.
7	After the tool finishes running, find BLOB Provider Settings and disable the EBS setting on the specified SharePoint 2010 farm. The upgrade is completed.

Extender

About the Extender

SnapManager for SharePoint Extender module invokes Microsoft's BLOB storage APIs to route content being uploaded to SharePoint to either the SQL content database or to file-based storage based on a customizable file-size trigger.

For any site collections for EBS or content database for RBS which have the Extender rule applied, if the file matches the extender rule, it will be archived when uploading to this site collection, and the original file will be saved in the specified physical device. EBS\RBS settings must be enabled before Extender can be used.

Extender Settings

To configure a real time archiving, complete the following steps:

Step	Action
1	Select a **Farm** from the drop-down list, and expand the data tree by clicking the farm name.
2	Select the site you want to enable the Extender feature by checking the corresponding checkbox. If you used RBS provider, you can select the content database you want to enable Extender feature. The site collections in the content database can be viewed. **Note** If the database icon is gray, it means that this database has not enabled RBS and the Extender rule cannot apply to this database. You must navigate to BLOB Provider Settings page to enable RBS for the application of Extender rule. If the database icon is yellow, it means that this database has already enabled RBS and the Extender rule can apply to this database.

Step	Action
3	Within the **Site Property**, you must set up the extended criteria for the target content. **Document Size:** Specify the size for the document. If the size for the uploading document is larger than specified here, the document will be extended while uploading. It is recommended to set up this option with a file size larger than 200 KB, as this will filter out some system files. **All Documents:** Extends all documents uploaded to the location specified in SharePoint regardless of size (except for SharePoint quota limits). Depending on the size and number of documents in the external location, this may take several minutes to complete.
4	Select a logical device from the drop-down list. This lists all the available logical devices. **Note** If you specified a logical device for one site collection (or a content database in RBS), you cannot change the logical device any more. **Note** The index device stores the information that will be used when performing the Delete Stub Policy of Extender. The information of each stub is about 250 bytes in size. See "Device Manager" on page 91 for the detailed information of setting up the Index Device for Extender.
5	You can specify to compress the content, and if so whether the compression will be carried out on the Media Agent or the SharePoint Agent. Note that by default, compression is not enabled.
6	If you want to extend all of the existing content that complies with the new Extender rule at this time, you can select the **Extend existing content** option, and click the calendar icon to specify the time.
7	Click the **Apply** button to save the settings. You can click the **Retract** button to cancel the current setting for the specific site.

Note

Once a database has RBS enabled and the Extender settings are configured, if RBS is turned off and then on again, the Extender settings must be set up again in order to take effect.

Converting Stubs to Content

To convert the stubs to content, complete the following steps:

Step	Action
1	Select a **Farm** from the drop-down box.
2	Select an agent group from the drop-down box; the farm name will be displayed.
3	You can choose to select the **Site Cascade** option. If checked, all of the sub sites in this structure will be included when running this job. If left unchecked, selecting a site will only include the contents of that site. This should be used when sub sites appear on the same level as their parent node in the SharePoint tree (due to display restrictions). You can also select to restore the data from Archiver by checking the corresponding checkbox.
4	Click the farm name to expand the data tree. Select the content you want to restore by checking the corresponding box. **Note** When running the Extender restore job of the content of one site collection which has enabled Extender before, you must retract the Extender policies first and then perform the restore.
5	Click the **Go** button to run the job; all of the extender data which had been converted to stubs will be restored.

Upgrade Extender Stubs

Complete the steps in the corresponding section to upgrade the Extender stubs.

Upgrade SharePoint 2007 EBS Stubs to SharePoint 2010 EBS Stubs

After attaching one content database containing stubs of SharePoint 2007 EBS environment to a SharePoint 2010 EBS environment, complete the following steps to ensure these stubs can be used.

Note

Make sure the SharePoint Agents on both SharePoint 2007 environment and SharePoint 2010 environment are pointing to the same SnapManager and the appropriate Logical Device which stores the real data of the stubs can be connected.

Step	Action
1	Find BLOB Provider Settings and enable the EBS setting on the specified SharePoint 2010 farm.
2	Find the job.properties file in the SnapManager Installation Path, which is <…\IBM*SnapManager for SharePoint\VaultServer\Control\etc\job.properties*> by default, and open it with the Notepad.
3	Find the **Smmoss.Extender.EBSUpgrade** attribute, and then change its value to **1**. If there is no such attribute in the file, add it manually in the following format: Smmoss.Extender.EBSUpgrade=1.
4	Go to **Extender Settings** page, select all the nodes which contain the SharePoint 2007 EBS stubs, and then select the **Extend Existing Content** option.
5	Configure the settings (Document Size, Logical Device and Data Configuration) according to your requirements.
6	Click **Apply** to apply the settings.
7	After the job completes successfully, change the value of the **Smmoss.Extender.EBSUpgrade** attribute back to **0**. The upgrade process is completed.

Upgrade SharePoint 2007 EBS Stubs to SharePoint 2010 RBS Stubs

For the SharePoint 2010 environment which upgrades from the SharePoint 2007 environment, complete the following steps to upgrade the EBS Stubs in SharePoint 2007 to SharePoint 2010 RBS Stubs.

Note

Make sure the SharePoint Agents on both SharePoint 2007 environment and SharePoint 2010 environment are pointing to the same SnapManager, and the appropriate Logical Device which stores the real data of the stubs can be connected.

Step	Action
1	Find BLOB Provider Settings and enable the EBS setting on the specified SharePoint 2010 farm.
2	Find the job.properties file in the SnapManager Installation Path, which is <…\IBM*SnapManager for SharePoint\VaultServer\Control\etc\job.properties*> by default, and open it with the Notepad.
3	Find the **Smmoss.Extender.EBSUpgrade** attribute, and then change its value to **1**. If there is no such attribute in the file, add it manually in the following format: Smmoss.Extender.EBSUpgrade=1.
4	Go to **Extender Settings** page, select all the nodes which contain the SharePoint 2007 EBS stubs, and then select the **Extend Existing Content** option.
5	Configure the settings (Document Size, Logical Device and Data Configuration) according to your requirements.
6	Click **Apply** to apply the settings.
7	After the job completes successfully, change the value of the **Smmoss.Extender.EBSUpgrade** attribute back to 0.
8	Find BLOB Provider Settings, select the **RBS** option, and select all the Content Databases which contain the EBS Stubs in the **Settings** tab. Click **Apply**, then click **Run Now** to install RBS for the SharePoint 2010 environment.
9	Go to **Extender Settings** page and select all of the nodes which contain the SharePoint 2010 EBS stubs.
10	Configure the settings (Document Size, Logical Device and Data Configuration) according to your requirements.
11	Click **Apply** to apply the settings.

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>12</td><td>Run <b>Command Prompt</b> using the Agent Account.</td></tr>
<tr><td>13</td><td>Find the convert tool in the following path on SMSP Agent server:
<i><…\ SnapManager for SharePoint\VaultClient\bin\SMSP2010EBSToRBSStubConvertTool.exe></i></td></tr>
<tr><td>14</td><td>Drag the tool into the command line interface and execute it to convert the EBS stubs to RBS stubs. You can also switch to the path first and then run the tool by entering its name and the corresponding parameters.
There are several parameters you can select:
<b>-help:</b> The user can use this parameter to get more information. The format of the command is:
SMSP2010EBSToRBSStubConvertTool.exe -help
<b>-preview:</b> The user can use this parameter to get the hierarchy of the site collections where the EBS stubs exist. Multiple URLs of the web applications can be entered when separated by semicolons. The format of the command is:
SMSP2010EBSToRBSStubConvertTool.exe [-farm|-webapplication|-sitecollection] –url <urls> -preview
For example:
SMSP2010EBSToRBSStubConvertTool.exe -webapplication –url http://test1:4000;http://test2:5000 -preview
<b>Note</b>
If the scope is -farm, no URL needs to be entered.</td></tr>
<tr><td>15</td><td>Enter <b>Y</b> to proceed with the convert process on the specified SharePoint content. Enter any other key to exit the convert process without running.</td></tr>
<tr><td>16</td><td>After the tool finishes running, find BLOB Provider Settings and disable the EBS setting on the specified SharePoint 2010 farm. The upgrade is completed.</td></tr>
</table>

Upgrade SharePoint 2010 EBS Stubs to SharePoint 2010 RBS Stubs

Complete the steps below to upgrade the SharePoint 2010 EBS Stubs to SharePoint 2010 RBS Stubs.

Step	Action
1	Find BLOB Provider Settings, select the **RBS** option, and select all the Content Databases which contain the EBS Stubs in the **Settings** tab. Click **Apply**, then click **Run Now** to install RBS for the SharePoint 2010 environment.
2	Go to **Extender Settings** page, select all the nodes which contain the SharePoint 2010 EBS stubs.
3	Configure the settings (Document Size, Logical Device and Data Configuration) according to your requirements.
4	Click **Apply** to apply the settings.
5	Run **Command Prompt** using the Agent Account.
6	Find the convert tool in the following path on SMSP Agent server: *<…\ SnapManager for SharePoint\VaultClient\bin\SMSP2010EBSToRBSStubConvertTool.exe>*

Step	Action
7	Drag the tool into the command line interface and execute it to convert the EBS stubs to RBS stubs. You can also switch to the path first and then run the tool by entering its name and the corresponding parameters. There are several parameters you can select: **-help:** The user can use this parameter to get more information. The format of the command is: SMSP2010EBSToRBSStubConvertTool.exe -help **-preview:** The user can use this parameter to get the hierarchy of the site collections where the EBS stubs exist. Multiple URLs of the web applications can be entered when separated by semicolons. The format of the command is: SMSP2010EBSToRBSStubConvertTool.exe [-farm|-webapplication|-sitecollection] –url <urls> -preview For example: SMSP2010EBSToRBSStubConvertTool.exe -webapplication –url http://test1:4000;http://test2:5000 -preview **Note** If the scope is -farm, no URL needs to be entered.
8	Enter **Y** to proceed with the convert process on the specified SharePoint content. Enter any other key to exit the convert process without running.
9	After the tool finishes running, find BLOB Provider Settings and disable the EBS setting on the specified SharePoint 2010 farm. The upgrade is completed.

Upgrade SharePoint 2010 Filestream Stubs to SharePoint 2010 RBS Stubs

Complete the steps below to upgrade the SharePoint 2010 Filestream Stubs to SharePoint 2010 RBS Stubs.

Step	Action
1	Find the SMSP2010StorageRBSTool.exe tool in the following path on SMSP Agent server : ...\IBM\SnapManager for SharePoint\VaultClient\bin
2	Double-click the tool to run it.
3	Load the tree in the lower-left corner of the pop-up window and select all the content databases which contain the Filestream Stubs.
4	Click **Enable** to enable RBS for the content databases.
5	Go to **Extender Settings** page and select all the nodes which contain the SharePoint 2010 Filestream stubs.
6	Configure the settings (Document Size, Logical Device and Data Configuration) according to your requirements. If the new Document Size is not the same as the old one, there will be different results: • If the new Document Size is bigger than the old one, all of the stubs of the documents whose sizes are between the two sizes will be converted to real data. • If the new Document Size is smaller than the old one, all of the documents whose sizes are between the two sizes will be extended to the external storage device.
7	Click **Apply** to apply the settings.
8	After the job completes successfully, find the SMSP2010StorageRBSTool.exe tool in the following path on SMSP Agent server : <...\IBM\SnapManager for SharePoint\VaultClient\bin>
9	Double-click the tool to run it.
10	Load the tree in the lower-left corner of the pop-up window and select all the content databases which contain the Filestream Stubs and have configured the new Extender settings.

Step	Action
11	Click **Migrate** to start the upgrade.

Upgrade Extender Data Stored on LUN

After upgrading to SnapManager 6.1, perform the following steps to upgrade the Extender data generated by the previous version from LUN to CIFS devices.

Note
The tool must be run on the server which has installed the SMSP Control Service.

Step	Action
1	Navigate to **Device Manager** under **Data Management** in **Control Panel**. Find the upgrade logical device for storage optimization module. For example, **Upgrade Logical Device WIN-AvePoint for storage optimization**. Add the CIFS physical devices which are used to save the Archived index and Archived data to the upgrade logical device.
2	Navigate to the installation path of SnapManager, which is <*C:\Program Files\IBM\SnapManager for SharePoint\VaultServer\Control\bin*> by default.
3	Double click **SMSPToolExtenderUpgrade.exe** to run it.
4	Select one media service in the **Media Service** drop-down box. The corresponding upgrade logical device will be displayed in the **Logical Device** area.
5	The LUN devices which store the Extender data to be upgraded will be displayed under the specific farm in the **Farms** field.
6	Select a CIFS physical device for storing Archived index in the **Index Device** drop-down box.
7	Select a CIFS physical device for storing Archived data in the **Data Device** drop-down box.

Step	Action
8	Select an upgrade method in **Options** in the **Settings** field. **Copy:** The Extender data will be upgraded and copied to the CIFS devices. **Move:** The Extender data will be upgraded and moved to the CIFS devices. The original Extender data stored in the LUN devices will be deleted.
9	Click **OK** to start the upgrade. Click **Cancel** to cancel the upgrade and exit the tool.

Archived Data Recover Overview

Since SharePoint content will be stored outside of SQL server when Archiver or Extender is used, it is important to regularly backup archive storage to safeguard disaster situations. SnapManager for SharePoint Archived Data Recovery enables you to set up a manual or automatic backup job for the SnapManager for SharePoint archived data.

Backup jobs are performed at the farm level. SnapManager Media Service will find out all the related storage devices (both Archive Index and Data type devices) used by Archiver and Extender for the specified farm and create snapshot backups for them.

Note

If the total number of the Snapshots exceeds the maximum number of Snapshots or the size of the physical drive, the backup job will not run properly. Therefore, retention policy needs to be set properly.

There are two parts in the SnapManager for SharePoint Archived Data Recovery: Archived Data Backup and Archived Data Restore.

Archived Data Backup

The **Archived Data Backup** tab enables you to execute a backup of the Archived Data in a SnapManager for SharePoint deployment. To set up a backup schedule, complete the following steps:

Step	Action
1	Select the **Enable Schedule** checkbox to activate a backup schedule. This is not required if you only intend to create a one-time manual backup **Note** You can only specify one schedule for backing up Archived Data.
2	Click the calendar icon next to the **Start Time** field. Use the calendar to specify when the backup should begin.
3	Specify the interval at which the recurring backup should occur: once, hourly, daily, weekly, or monthly.

The archived data retention rule is a method of pruning the old backed up archive data to make room for new backups of archive data. Note that you can only prune old data by running a retention rule, deleting the job report will not do anything to the backed up archive data.

To set up a retention rule, complete the following steps:

Step	Action
1	Select the **Enable Retention** checkbox to activate the backup retention rule.
2	There are two retention rules you can select. **Keep last... backups:** Specify the total number of previous backups you want to keep. This will prune backups older than the specified number before running a new backup. **Keep backups from last:** Specify the time of the backups you want to keep. This will prune any backups made before the specified retention time.
3	Click the **Save** button to save the settings. This will prune the old archived data at the specified time.

Check the **Update SnapMirror for device after Operation** option in the **Advanced** field to update the SnapMirror for the corresponding device after the backup operation. The option is not selected by default.

Monitoring a Backup Job: After starting a backup job, you can monitor it through the Archived Data Backup Job Report in the Job Monitor. The report includes the start time, backup path, the user who initiated the job, the job's current status, the backup data size, and the progress. You can delete the job report by clicking the **Delete** button.

Archived Data Restore

Archived Data Restore is very different from granular restore performed in Data Protection Restore Controller or in Archiver Restore Controller. The latter is considered a normal operation that can be performed regularly according to business needs. Granular restores reads data from storage managed by SnapManager.

On the other hand, Archived Data Restore is meant for disaster situation only, where the storage managed by SnapManager got corrupted or lost. Also, after restore, the storage will be in a status as of the backup time; any new content saved in the storage after backup will no longer be available.

Archived Data Restore is also performed at farm level. If disaster recovery is needed at a lower granular level, it is possible to copy back the archived content from snapshot backup manually, at site collection level.

After the Archived Data Backup job is completed, it is listed by its backup time in the Archived Data Restore Job browser. You can restore to any point-in-time by choosing the radio button next to the appropriate job and clicking the **Restore** button if the physical archived data becomes corrupt or lost.

SMSP Media Service will then find the storage devices (LUNs or CIFS shares) holding the archived data for restore. Snapshot based restore will be performed for the SMSP archived data from the selected farm on LUN devices. For CIFS shares, SnapRestore will be used when ALL the following conditions are true. Otherwise, copy -based restore will be used, which may take more time for the restore process.

- The **Use Volume Level Snap Restore For Volumes With Single CIFS Share** option is checked in the Archived Data Restore.
- The CIFS share is defined at volume root level (i.e. the CIFS path on local system storage is the same as volume path).
- Only SMSP archived data from the selected farm is on the CIFS share.

Monitoring a Restore Job: You can monitor a restore job through the Archived Data Restore Job Report in the Job Monitor. The report includes the start time, the path the data is loaded from, the user who initiated the restore, the status, the data size of the restore, and the progress. You can delete the job report by clicking the **Delete** button.

Note

Data in a SnapLock device cannot be restored due to the protective nature of the SnapLock device.

Note

If you select the **Use Volume Level Snap Restore For Volumes With Single CIFS Share** option for the restore job, all snapshot backups after a restore job is run will be gone. It is recommended you not use this restore method unless absolutely necessary.

Recovering the Archived Data for a Site Collection Manually

To recover the archived data for a site collection manually, see the following steps.

If the restore is not for farm level, you must do the recovery manually, such as only one site needs to be recovered. And if there are snapshots for the volume performed outside of SMSP, the end user needs to do the recovery manually.

Step	Action
1	View the archived data backup job for the specific site collection in the **Archived Data Restore**.
2	Go to Job Monitor, and find the backup job.
3	Click the **Detail** button, and download the report.
4	Open the report, and find the information of the specific site collection in the report. Its format is *<SiteCollectionInfo path="site collection path">*. You can find the *<DataInfo>* for the archived data (both Archiver data and Extender data) information including which physical device data is backed up, and the location of the backup data in the physical device in the *<ArchiverData>* or *<ExtenderData>* under the *<SiteCollectionInfo>*. The format of the path information is *[share path]\SMMOSS\.snapshot\[snapshot name]\[data path]* , and location for the restore data is *[share path]\SMMOSS\[data path].*
5	Copy the path into the **Address** box to find the backup data, and then copy the data to the destination. After copying all data under the *<DataInfo>*, the site collection is recovered successfully.

Deleted Stub Policy

Deleted Stub Policy Overview

SnapManager for SharePoint **Deleted Stub Policy**, also called **Orphan Retention Policy**, enables you to set up a rule to remove the archived data after deleting its stub in SharePoint. This feature is only enabled when applying the deleted content retention settings.

To configure the deleted stub settings for a specific web application, complete the following steps:

Step	Action
1	Select a farm from the column on the left-hand side. The applicable web applications will be listed under the **Delete Settings** section.
2	Select the data, from Extender or Archiver, you want to remove by checking the corresponding checkbox. When this option is checked, the SharePoint environment will be periodically scanned to find deleted content. This process is called **Sync Deletion**. The identified deleted content is called **Orphan data**.
3	Specify the delete time for the Archiver or Extender data. Select a time zone from the drop-down list, set up the interval and the time when the deletion job should run.
4	You can set up the interval for checking the archived data whose stub has already been deleted by using the **Delay deletion by** option.

Note

This setting will cause SnapManager for SharePoint to delete archived data after the specified number of days after the stub is marked and deleted from SharePoint. We recommend enforcing a minimum delay time to ensure contents are not inadvertently deleted by SharePoint users.

Note

From SnapManager 6.1 version, if the data is considered to be orphan data, it still can be accessed, searched, or restored. The delete flag will be reset if the file is accessed or the stub of the file is restored back. It is recommended to set the Backup retention shorter than the Archiver orphan retention length, and the Archiver orphan retention to be shorter than the Archiver retention length.

Note

If you set a retention policy for a web application and delete one site collection from the web application, the archived data of the Archiver\Extender stubs in the site collection cannot be deleted by the corresponding **Deleted Stub Policy**.

Storage Orphan Stub Tool

The **SMSPTool2010StorageOrphanStubClean.exe** tool locates in the installation path of the Agent, which is *<C:\Program Files\IBM\SnapManager for SharePoint\VaultClient\bin>* by default.

In the SharePoint 2010 environment, you can use the tool to perform the following actions:

- Search for the orphan stubs and record the result in the specified .csv file.
- View the orphan stubs' information from the specified .csv file and delete the corresponding files from SharePoint.

To run the tool by running the **SMSPTool2010StorageOrphanStubClean.exe** file, complete the following steps:

Step	Action
1	Navigate to the installation path of the Agent which is *<C:\Program Files\IBM\SnapManager for SharePoint\VaultClient\bin>* by default.
2	Find **SMSPTool2010StorageOrphanStubClean.exe** and double-click the tool to run it.
3	Enter the command `RBSOrphanCleanUp -Help` to view the detailed information of all parameters.

Step	Action
4	Below is the detailed information of all the parameters: - **RBSOrphanCleanUp** It is mandatory, and must be input before entering the other parameters. - **-Action** It is mandatory and is the operation to be executed. If `-Action` *`Report`* is used, the orphan stubs' information will be written to a CSV file. The path of the file should be specified in the mandatory `File` parameter which follows `-Action` *`Report`*. The format of the path is *C:\test\result.csv*. If `-Action` *`Clean`* is used, the corresponding files in SharePoint will be deleted according to the orphan stubs' information in the CSV file. The path of the file should be specified in the mandatory `File` parameter which follows `-Action` *`Clean`*. The format of the path is *C:\test\result.csv*. - **-WebApp(it is used for -Action Report)** It is mandatory and is the URL of the web application where you want to search for the orphan stubs. The format is: *`http://test:4000.`* - **-ContentDB(Optional, it is used for -Action Report)** It is the content database where you want to search for the orphan stubs. If you skip it, the tool will search in all the content databases of the specified web application. The content database specified here must belong to the web application specified in `WebApp` parameter. - **-SiteCollection(Optional, it is used for -Action Report)** It is the site collection where you want to search for the orphan stubs. If you skip it, the tool will search in all the site collections. The site collection specified here must belong to the web application specified in `WebApp` parameter. If the `ContentDB` parameter is used, the site collection should also belong to the specified content database. - **-AfterTime** It is mandatory if you have specified the parameter `-Action` *`Report`*. All the stubs created on the specified date and after it will be searched out. The format is: *year-month-day*.

Step	Action
5	The interface will prompt you to enter the parameter's value again if it is invalid. See Step 4 and Step 6 if the value of `-Action` is *Report*. See Step 4 and Step 7 if the value of `-Action` is *Clean*.
6	If the value of `-Action` is *Report*, the tool will search for the RBS orphan stubs and write the result to the CSV file specified in the `File` parameter. After verifying the parameter, the interface will display *Starting to run* and show the job's progress. If the job completes successfully, **Job completed** will be prompted and the CSV file will be created in the specified path. Otherwise, it will prompt **Job Failed**.
7	If the value of `-Action` is **Clean**, the tool will read the orphan stubs' information from the CSV file and delete the corresponding files from SharePoint. After verifying the parameter, the interface will display **Starting to run** and show the job's progress. If the job completes successfully, **Job completed** will be prompted and the files' amount and the deletion amount will be displayed. Otherwise, it will prompt **Job Failed**.
8	Press any key to exit when the job is finished.

To run the tool in the command line interface, complete the following steps:

Step	Action
1	Click **Start** and click **Run...**, enter **cmd** in the **Open:** text box.
2	Click **OK** to open the command line interface.
3	Use the **cd** command to navigate to the installation path of the Agent, which is <*C:\Program Files\IBM\SnapManager for SharePoint\VaultClient\bin*> by default.

Step	Action

4	Enter the corresponding command to run the tool. See the first table in “Storage Orphan Stub Tool” on page 235 for the detailed information of the parameters to be entered here. Such as:
	`SMSPTool2010StorageOrphanStubClean.exe RBSOrphanCleanUp -webapp http://test:4000 -action report -file c:\test.csv -aftertime 2011-05-18`
	`SMSPTool2010StorageOrphanStubClean.exe RBSOrphanCleanUp -action clean -file c:\test.csv`

5	You can view the progress in the tool interface and press any key to exit when the job is finished.

Job Monitor 13

Overview of the Job Monitor

From the SnapManager for SharePoint Job Monitor module, you can monitor the progress of any backup, backup maintenance, or restore job and view the detailed information upon completion of any successful or failed job.

The SnapManager for SharePoint Job Monitor module has three sections: **Log Viewer**, **Job Monitor** and **Schedule Job Monitor**.

Log Viewer

About the Log Viewer

To monitor the detailed processes involved in the SnapManager for SharePoint platform, use the Log Viewer to view the logs generated during any job process. You can customize the Log Viewer to show different services and log levels to narrow your search scope.

Using the Log Viewer

When troubleshooting errors in SnapManager for SharePoint, you can use the Log Viewer to track down each step that led to a failure. You can configure the view in the Log Viewer by setting up the following four options:

Level: In this drop-down box, you can select to view all the levels or the Fatal, Error, Warning, Info, or Debug levels.

Service: You can view logs for the Control Service.

Refresh: You can use this button to update the Log Viewer with the latest logs. You can also refresh the view immediately by clicking the **Refresh** button.

Per Page: You can customize the number of logs that appear per page by selecting 5, 10, or 20 items to list from the drop-down menu.

If you click the Log ID number located in the first column for any log, you can see the detailed information for each log, including the log level, the ID number, the Date and time generated, the Service that generated the log, and the Host that the service was located on. To be specific, the ID number, when being clicked, allows the user to view the detailed log information in the window emerges afterwards.

To view all logs, you can either page through the main list of logs or you can click the ID of a log and use the **Previous** and **Next** buttons to navigate through the logs one at a time.

Job Monitor

About the Job Monitor

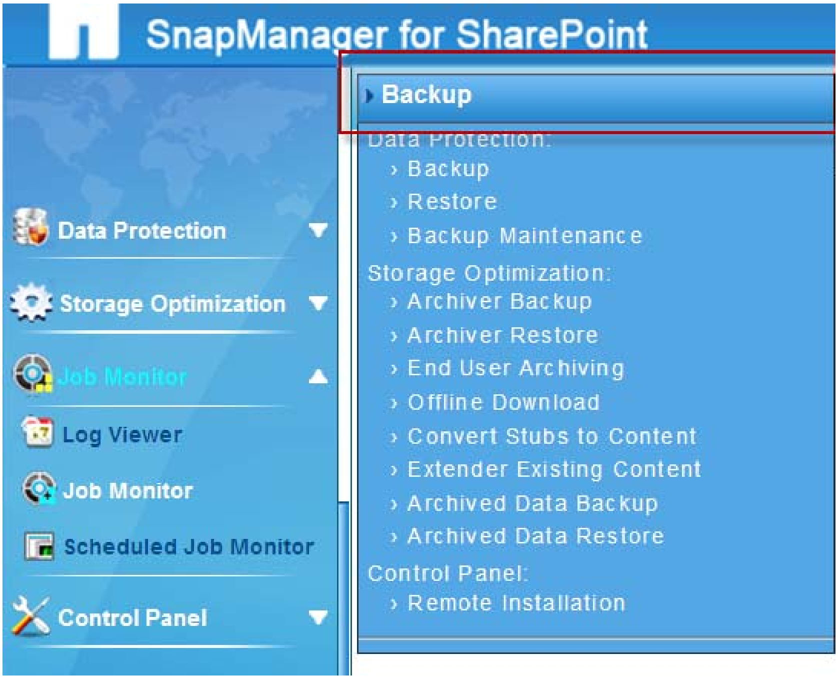
Through the SnapManager for SharePoint Job Monitor screen, you can monitor the progress of any backup, backup maintenance, restore job, storage optimization job, Control Panel- related job. Additionally, detailed information about the job is listed upon completion.

You can view the following information for each job from the default view: the Status, the Plan Name, the Progress, the Start Time, the Finish Time, the User who initiated the job, and a Detail field to download a detailed job report. Additional columns may be available depending on the customized views as well as the type of job.

Loading the Job Monitor

To launch the Job Monitor, you can either navigate to the menu on the side of SnapManager for SharePoint, or click the **Go To Job Report** button that appears when a job is running. It automatically loads the screen showing the job information when you run a job.

If you want to change the view to show either a Restore, a Backup, or a Backup Maintenance job, select the corresponding options in the drop-down list on the upper-left of the interface.



To sort the Job Monitor table, click any of the column titles. If there are many jobs, you can also use the page navigation controls.

Downloading Detailed Job Reports

To download a detailed job report, scroll to the Detail column and click the **View Detail Report** button. A window appears showing a brief summary of the details regarding this job. You can save the detailed job report by clicking the **Download** button and selecting a location to save the .zip file. This is useful for cases where advanced troubleshooting is required.

For backup and backup maintenance jobs, the related SnapDrive and SnapManager for Microsoft SQL Server API outputs and the Index Report will be recorded for the download as well. This option will appear as a second Download option in the dialog box.

Note

When a backup job is deleted, its associated backup job data and snapshot backups in storage system will also be deleted. Therefore, restore from that backup job is no longer possible after the deletion.

Customizing Job Monitor View

You can view all items by selecting **All Items** from the **View** list. You can also customize the job monitor view to list the items you want to view, and select the **Default View** to make it as the default view.

Note
The customized view can be only used for the current module.

To create a new view, complete the following steps:

Step	Action
1	Click **Create View** from the **View** list. A dialog box appears.
2	Input a **View Name** into the **View Name** text box.
3	You can check **Make this the default view** checkbox to make it the default view.
4	Check the radio button to specify the audience (**Public View\Personal View**) for a specified module. In contrast to Public View, you can create a Personal View for the specified user. This setting is specially designed for privacy, even an SMSP Administrator has no access to your Personal View.
5	Check the corresponding checkbox to select the items and their positions to be displayed in the current page.
6	Specify the number of jobs to display per page into the provided text box.
7	Click **Apply** to save the configuration, or click **Cancel** to exit the window.

You can also modify the current view by clicking **Modify This View**, and updating the view as you like.

Deleting Jobs in Job Monitor

You can select the job you want to delete by checking the corresponding checkbox, and then clicking on the trash bin icon to delete it.

Deleting the jobs from job monitor only deletes the job record, it does not delete the real data, and does not disturb the retention jobs. But for backup jobs, the backup data, including Snapshot backups, will be deleted together. If you want to only delete the backup job record, you can select the **Only delete job data in** SMSP option.

Scheduled Job Monitor

About Scheduled Job Monitor

Through the SnapManager for SharePoint Schedule Monitor screen, you can view information on the scheduled jobs.

Viewing the Detailed Information

To view detailed information on the scheduled plan, complete the steps below:

Step	Action
1	Select the module you want to view from the drop-down list.
2	Select the interval for the job you want to view in the **Time Window** area.
3	Select the number from the **Page** drop-down list to specify the job number displayed in each page.
4	Click the **Show Results** button to load the corresponding jobs. You can view the Job Order, Plan Name, Start Time, and Backup Type.
5	You can click the **Disable** button to cancel a job and the job will not run on the specified time, or the **Enable** button to enable it to run.

SnapManager CLI 14

About SnapManager CLI

In SnapManager 6.1.0.0, it supports deployment of SnapManager by using CLI (Command line Interface). The CLI is used when deploying SnapManager to a large SharePoint environment.

Note

Windows PowerShell V2 must be installed on the machine which runs the script.

Before Running SnapManager CLI in an Environment with firewall

In order to run the CLI in an environment with firewall, complete the following steps:

Step	Action
1	On the remote server, navigate to **Start > Control Panel** > **Windows Firewall** > **Advanced settings** > **Windows Firewall with Advanced Security on Local Computer** > **Inbound Rules,** find *File and Printer Sharing (Echo Request - ICMPv4-In)*, right click on the rule and click **Enable Rule** to enable it.
2	On the server where you run the command, navigate to **Start** > **Control Panel** > **Windows Firewall** > **Allow a program or feature through Windows Firewall**, click **Allow another program...** and click **Browse...** in the pop-up window. Find <powershell.exe> in <C:\Windows\System32\WindowsPowerShell\v1.0> and click **Open**. Click **Add** to add it to *Allowed programs and features* list and check the Domain, Home/Work (Private) or Public check boxes according to your requirements.
3	On the remote server, open the corresponding ports used by the Manager and the Agent. See "Ports Used by SnapManager for SharePoint Manager and Agent" on page 38 for more information.

Before Running the SnapManager CLI in PowerShell

Before running the SnapManager CLI, you must ensure all the required DLL files are imported. To import the DLL files, complete the following steps:

Step	Action
1	Extract the <SMSP61_ExtendedPack_The serial number.zip> file to the installation path of SMSP, which is <...\IBM\SnapManager for SharePoint\>.
2	Double-click on <SMSPCmdletLauncher.bat> in the PowerShellSnapIn folder inside the extracted folder. Then all the required DLL files will be imported automatically in the pop-up PowerShell window. You can run the commands. **Note** If the DLL files could not be imported automatically due to the local Security Policies of PowerShell, open a PowerShell window and use the following command: **`Import-Module "The path of the .dll file"`** to import all the DLL files in the PowerShellSnapIn folder manually.

Note

If the command fails with the following error:
Invalid timestamp The security semantics of the message have expired
The issue may be caused by the following reasons:
The System Time of the machine where the SnapManager for SharePoint Control Service installed is different from the System Time of the machine where running the command line by using PowerShell based on the same time zone. The margin of error is 5 minutes.
For example, if the System Time of the machine where the SnapManager for SharePoint Control Service is installed is 14:00 (GMT +8). The System Time of the machine which uses PowerShell in GMT+6 must be in the following time range: 11:55 (GMT+6)~12:05 (GMT+6) to ensure the command line run properly.
If you modify the System Time on these two machines, the command line must be run again.

Generate/edit the Answer File using the SMSP Setup Manager Tool

The Answer File is used for maintaining installation configuration data for Remote Installation. Since the Answer File's structure is complex and hard to edit manually, this tool is used to help you to generate/edit the Answer File.

Note

The Answer File must be generated before running the following command: Install-SMSPManager and Install-SMSPAgent.

To set up the Answer File, complete the steps below:

Step	Action
1	The <SMSPSetupManager.exe> file is packaged in the Tool folder inside <SMSP61_ExtendedPack_The serial number.zip>. If you want to execute the program, extract <SMSP61_ExtendedPack_The serial number.zip> file to the installation path of SMSP, which is <...\IBM\SnapManager for SharePoint\>, find <SMSPSetupManager.exe> and double click it.
2	Click **Next** in the pop-up.
3	You can choose to create a new Agent Answer File or a new Manager Answer File or modify an existing Answer File by selecting the corresponding option.
4	If you choose to create a new Agent Answer File or a new Manager Answer File, enter the corresponding information in the text-boxes provided, you can view "Installing SnapManager for SharePoint" on page 17 for more information about how to set up the Agent/Manager Configurations. Then you can save the Answer File to the specified path.
5	If you choose to modify an existing Answer File, click **Browse** to browse for the corresponding Answer File, then click **Next** to modify the selected Answer File. After modifying the Answer File, save the Answer File to the specified path.

Install Manager/Agent Remotely

In order to install Control Service and Media Service, or Media Service only, or Agent remotely, run the:

```
Install-SMSPManager
```

```
Install-SMSPAgent
```

The examples of the commands are:

```
Install-SMSPAgent -Host 10.0.0.1 -User test\admin -Password admin -
RemoteTempPath "C:\Temp\SMSP" -PackagePath "C:\Documents and
Settings\Administrator\Desktop\IBM\Agent.exe" -AnswerFilePath
"C:\AgentAnswerFile1.xml"
```

```
Install-SMSPManager -Host 10.0.0.1 -User test\admin -Password admin
-RemoteTempPath "C:\Temp\SMSP" -PackagePath "C:\Documents and
Settings\Administrator\Desktop\IBM\Manager.exe" -AnswerFilePath
"C:\ManagerAnswerFile.xml"
```

Note

You can use the command **Install-SMSPManager** to install SMSP Manager on the Windows cluster node with SMSP Control service and Media service configured to be cluster service.

To configure the command arguments, see the table below.

Argument	Type	Comment
-Host	Required	The hostname or the IP address of the remote host to install the Manager/Agent on.
-User	Required	The user used for performing the installation in the remote host. The user must be a domain user and in the Administrator group of the remote server. The format of the user is domain\user.

Argument	Type	Comment
-Password	Required	The user's password for logging on the remote server. **Note** If you do not want to show the password on the interface, you can skip this argument, and after you enter this command line and press the **Enter** key to run this command, the interface will prompt you to enter the password, this password is encrypted.
-RemoteTempPath	Required	The path in the remote host where the installation files will be copied to. For example, <d:\temp\install>. You can enter the local path for this argument, if the specific path does not exist in the remote machine, this path will be created automatically. **Note** The installation files will be deleted automatically after the installation completes.

Argument	Type	Comment
-PackagePath	Required	The path where the installation package is. The path should be detailed to the name of the installation package. Both local path on the server where you configure the script and network path can be used. The path must be an existing one.
-AnswerFilePath	Required	The path where the answer file is. The path must be an existing one. The path must be detailed to the name of the answer file. Both local path on the server where you configure the script and network path can be used. See "Generate/edit the Answer File using the SMSP Setup Manager Tool" on page 249 for the detailed steps to configure an Answer File.
-UseIPv6ForCommunication	Optional	This argument is used to make sure the availability of IPv6 communication in IPv6 environment. If this argument is not used, IPv4 communication will be used by default.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, *<Install-SMSPManager_201105161530.log>*. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, *<C:\test.log>*. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Check Whether the Manager/Agent Can be Installed Remotely

The two commands are newly added in SMSP 6.1.

To check whether the Manager/Agent can be installed remotely, run the command below:

```
Verify-SMSPManagerInstall
```

```
Verify-SMSPAgentInstall
```

The example of the command is:

```
Verify-SMSPAgentInstall –Host 10.0.0.1 –User test\admin -Password
admin –RemoteTempPath "C:\Temp\SMSP" –Verifier
"D:\SMSPInstallAndConfigVerifier.exe" –AnswerFilePath
"C:\AgentAnswerFile.xml"
```

```
Verify-SMSPManagerInstall –Host 10.0.0.1 –User test\admin -Password
admin –RemoteTempPath "C:\Temp\SMSP" –Verifier
"D:\SMSPInstallAndConfigVerifier.exe" –AnswerFilePath
"C:\ManagerAnswerFile.xml"
```

To configure the command arguments, see the table below:

Argument	Type	Comment
-Host	Required	The hostname or the IP address of the remote host to check whether the Manager/Agent can be installed on.
-User	Required	The user used for performing the verification in the remote host. The user must be a domain user and in the Administrator group of the remote server. The format of the user is domain\user.

Argument	Type	Comment
-Password	Required	The user's password for logging on the remote server. **Note** If you do not want to show the password on the interface, you can skip this argument, and after you enter this command line and press the Enter key to run this command, the interface will prompt you to enter the password, this password is encrypted.
-RemoteTempPath	Required	The path in the remote host where the <*SMSPInstallAndConfigVerifier.exe*> file and the Answer file will be copied to. For example, d:\temp\install. You can enter the local path for this argument, if the specific path does not exist in the remote machine, this path will be created automatically. **Note** The <*SMSPInstallAndConfigVerifier.exe*> file and the Answer file will be deleted automatically after the verification completes.

Argument	Type	Comment
-Verifier	Required	The path where the <*SMSPInstallAndConfigVerifier.exe*>file lies. The path must be an existing one. The path must be detailed to the name of the <*SMSPInstallAndConfigVerifier.exe*> file. Both local path on the server where you configure the script and network path can be used. **Note** The <*SMSPInstallAndConfigVerifier.exe*> file can be found in the *PowerShell-SnapIn* folder of the extracted <*SMSP61_ExtendedPack_The serial number.zip*> file.
-AnswerFilePath	Required	The path where the answer file lies. The path must be an existing one. The path must be detailed to the name of the answer file. Both local path on the server where you configure the script and network path can be used. See "Generate/edit the Answer File using the SMSP Setup Manager Tool" on page 249 for the detailed steps to configure an Answer File.

Argument	Type	Comment
-UseIPv6ForCommunication	Optional	This argument is used to make sure the availability of IPv6 communication in IPv6 environment. If this argument is not used, IPv4 communication will be used by default.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, *<C:\test>* (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, *<Install-SMSPManager_201105161530.log>*. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, *<C:\test.log>*. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Modify Manager’s Configuration

To modify the Manager’s configuration remotely, run the command below:

```
Config-SMSPManager
```

The example of the command is:

```
Config-SMSPManager -Host 10.0.0.1 -User test\admin1 -Password
admin1 -IgnoreRunningJob true -ControlServiceAddress 10.0.0.1 -
ControlServicePort 12000 -ManagerWebServicePort 12011 -
MediaServiceAddress 10.0.0.1 -MediaServiceControlPort 12001 -
WebServiceAddress 10.0.0.1 -WebServicePort 8080 -EnableHTTPS false
-EnableIPv6 false -EnableActiveDirectory true -ADUserName
test\admin2 -ADPassword admin2
```

To configure the command arguments, see the table below:

Argument	Type	Comment
-Host	Required	The hostname or the IP address of the remote host to configure Manager on.
-User	Required	The user used for performing the configuration in the remote host. The user must be a domain user and in the Administrator group of the remote server. The format of the user is domain\user.

Argument	Type	Comment
-Password	Required	The user’s password for logging on the remote server. **Note** If you do not want to show the password on the interface, you can skip this argument, and after you enter this command line and press the **Enter** key to run this command, the interface will prompt you to enter the password, this password is encrypted.
-IgnoreRunningJob	Required	Specify whether to skip the running job(s). The value of the argument is **false** or **true**. ● If the value is **true**, the configuration will continue even if there are jobs running. ● If the value is **false**, the configuration will not be performed if there is a job running.
-ControlServiceAddress	Optional	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service is installed.
-ControlServicePort	Optional	The port for Control Service, it will be used to connect with the agent.

Argument	Type	Comment
-ManagerWebServicePort	Optional	The port for the web service, it will be used to access the CLI from other servers. **Note** The argument should not be entered if there is no Control Service installed on the remote server.
-MediaServiceAddress	Optional	Specify the hostname or IP address of the machine where the Media Service installed. **Note** The argument should not be entered if there is no Media Service installed on the remote server.
-MediaServiceControlPort	Optional	The port is used by the Control Service to connect with the Media Service and used by the Agent to send the corresponding data to the Media Server. **Note** The argument should not be entered if there is no Media Service installed on the remote server.

Argument	Type	Comment
-WebServiceAddress	Optional	Specify the hostname or IP address of the machine where the Web Service is installed. **Note** The argument should not be entered if there is no Web Service installed on the remote server.
-WebServicePort	Optional	The port is used for accessing the Web Service using the browser. **Note** The argument should not be entered if there is no Web Service installed on the remote server.
-EnableHTTPS	Optional	Specify whether to enable users to access the SnapManager for SharePoint interface over HTTPS. The value of the argument could be **false** or **true**. **Note** The argument should not be entered if there is no Control Service or Web Service installed on the remote server.

Argument	Type	Comment
-EnableIPv6	Optional	Specify whether IPv6 will be used. The IP address of the machine with the Manager Service installed must be IPv6 to utilize this protocol. The value of the argument is **false** or **true**.
-EnableActiveDirectory	Optional	Specify whether to integrate with AD and add existing AD users to the SnapManager for SharePoint platform. The value of the argument is **false** or **true**. **Note** The argument should not be entered if there is no Control Service or Web Service installed on the remote server.
-ADUserName	Optional	The name of the AD user. The user is not required to be an AD administrator. The username must be in the following format: domain\username. **Note** This argument must be entered once the value of EnableActiveDirectory argument is **true**.

Argument	Type	Comment
-ADPassword	Optional	The password for the specified AD user. **Note** This argument must be entered once the value of EnableActiveDirectory argument is **true**.
-UseIPv6ForCommunication	Optional	This argument is used to make sure the availability of IPv6 communication in IPv6 environment. If this argument is not used, IPv4 communication will be used by default.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, <*Install-SMSPManager_201105161530.log*>. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, <*C:\test.log*>. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Check Whether the Manager Can be Configured Remotely

This is a newly added command in SMSP 6.1.

To check whether the Manager can be configured remotely, run the command below:

```
Verify-SMSPManagerConfig
```

The example of the command is:

```
Verify-SMSPManagerConfig -Host 10.0.0.1 -User test\admin1 -Password
admin1 -RemoteTempPath "C:\Temp\SMSP" -Verifier
"D:\SMSPInstallAndConfigVerifier.exe" -ControlServiceAddress
10.0.0.1 -ControlServicePort 12000 -ManagerWebServicePort 12011 -
MediaServiceAddress 10.0.0.1 -MediaServiceControlPort 12001 -
WebServiceAddress 10.0.0.1 -WebServicePort 8080 -EnableHTTPS true -
EnableIPv6 false -EnableActiveDirectory true -ADUserName
test\admin2 -ADPassword admin2
```

To configure the command arguments, see the table below:

Argument	Type	Comment
-Host	Required	The hostname or the IP address of the remote host to verify the configuration of the Manager on.
-User	Required	The user used for performing the verification in the remote host. The user must be a domain user and in the Administrator group of the remote server. The format of the user is domain\user.

Argument	Type	Comment
-Password	Required	The user’s password for logging on the remote server. **Note** If you do not want to show the password on the interface, you can skip this argument, and after you enter this command line and press the Enter key to run this command, the interface will prompt you to enter the password, this password is encrypted.
-RemoteTempPath	Required	The path in the remote host where the <*SMSPInstallAndConfigVerifier.exe*> file will be copied to. For example, <d:\temp\install>. You can enter the local path for this argument, if the specific path does not exist in the remote machine, this path will be created automatically. **Note** The <*SMSPInstallAndConfigVerifier.exe*> file will be deleted automatically after the verification completes.

Argument	Type	Comment
-Verifier	Required	The path where the <*SMSPInstallAndConfigVerifier.exe*> file lies. The path must be an existing one. The path must be detailed to the name of the <*SMSPInstallAndConfigVerifier.exe*> file. Both local path on the server where you configure the script and network path can be used. **Note** The <*SMSPInstallAndConfigVerifier.exe*> file can be found in the *PowerShell-SnapIn* folder of the extracted <*SMSP61_ExtendedPack_The serial number.zip*> file.
-ControlServiceAddress	Optional	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service installed.
-ControlServicePort	Optional	The port for Control Service, it will be used to connect with the agent.
-ManagerWebServicePort	Optional	The port for the web service, it will be used to access the CLI from other servers. **Note** The argument should not be entered if there is no Control Service installed on the remote server.

Argument	Type	Comment
-MediaServiceAddress	Optional	Specify the hostname or IP address of the machine where the Media Service installed. **Note** The argument should not be entered if there is no Media Service installed on the remote server.
-MediaServiceControlPort	Optional	The port is used by the Control Service to connect with the Media Service, and by the Agent to send the corresponding data to Media Server. **Note** The argument should not be entered if there is no Media Service installed on the remote server.
-WebServiceAddress	Optional	Specify the hostname or IP address of the machine where the Web Service installed. **Note** The argument should not be entered if there is no Web Service installed on the remote server.

Argument	Type	Comment
-WebServicePort	Optional	The port is used for accessing the Web Service using the browser. **Note** The argument should not be entered if there is no Web Service installed on the remote server.
-EnableHTTPS	Optional	Specify whether to enable users to access the SnapManager for SharePoint interface over HTTPS. The value of the argument could be **false** or **true**. **Note** The argument should not be entered if there is no Control Service or Web Service installed on the remote server.
-EnableIPv6	Optional	Specify whether IPv6 will be used. The IP address of the machine with the Manager Service installed must be IPv6 to utilize this protocol. The value of the argument is **false** or **true**.

Argument	Type	Comment
-EnableActiveDirectory	Optional	Specify whether to integrate with AD and add existing AD users to the SnapManager for SharePoint platform. The value of the argument is **false** or **true**. **Note** The argument should not be entered if there is no Control Service or Web Service installed on the remote server.
-ADUserName	Optional	The name of the AD user. The user is not required to be an AD administrator. The username must be in the following format: domain\username. **Note** This argument must be entered once the value of EnableActiveDirectory argument is **true**.
-ADPassword	Optional	The password for the specified AD user. **Note** This argument must be entered once the value of EnableActiveDirectory argument is **true**.

Argument	Type	Comment
-UseIPv6ForCommunication	Optional	This argument is used to make sure the availability of IPv6 communication in IPv6 environment. If this argument is not used, IPv4 communication will be used by default.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, <*Install-SMSPManager_201105161530.log*>. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, <*C:\test.log*>. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Modify Agent’s Configuration

To modify the Agent’s configuration remotely, run the command below:

```
Config-SMSPAgent
```

The example of the command is:

```
Config-SMSPAgent -Host 10.0.0.2 -User test\user -Password user -
AgentUser test\admin -AgentPassword admin -ControlServiceAddress
10.0.0.1 -ControlServicePort 12000 -AgentAddress 10.0.0.2 -
AgentPort 20103 -ArchiverPort 20207 -EnableIPv6 true -ControlAgent
true -MemberAgent true -Archiver true -IISResetNow -Extender true
```

To configure the command arguments, see the table below:

Argument	Type	Comment
-Host	Required	The hostname or the IP address of the remote host to configure Agent on.
-User	Required	The user used for performing the configuration in the remote host. The user must be a domain user and in the Administrator group of the remote server. The format of the user is domain\user.

Argument	Type	Comment
-Password	Required	The user’s password for logging on the remote server. **Note** If you do not want to show the password on the interface, you can skip this argument, and after you enter this command line and press the **Enter** key to run this command, the interface will prompt you to enter the password, this password is encrypted.
-AgentUser	Required	The user used for the remote server to connect to the Manager and SharePoint content database. The format of the user is domain\username. You can view “Installing SnapManager for SharePoint” on page 17 for more information about the permissions required for the Agent user. **Note** You can use the Agent Account as the Agent user since the Agent user has the same permissions as the Agent Account.

Argument	Type	Comment
-AgentPassword	Required	The password of the user entered in AgentUser argument. **Note** If you do not want to show the password on the interface, you can skip this argument, and after you enter this command line and press the **Enter** key to run this command, the interface will prompt you to enter the password, this password is encrypted.
-ControlServiceAddress	Optional	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service installed.
-ControlServicePort	Optional	The port used for communication with the Control Service and it should match the information provided during the Manager configuration.
-AgentAddress	Optional	The host name or IP address of the remote server where the Agent installed.
-AgentPort	Optional	The port used by the Manager or other Agents for communication.
-ArchiverPort	Optional	The port is used to allow Archiver/Extender to communication with SMSP BLOB Provider.

Argument	Type	Comment
-EnableIPv6	Optional	The argument must be the same as the configuration in the Manager. If its value is *true*, the IP address of the machine installed the Agent Service must be IPv6. The value of the argument is **false** or **true**.
-ControlAgent	Optional	It is the SMSP Control Agent used by the Data Protection module. The value of the argument is **false** or **true**. **Note** The argument should not be entered if there is no SharePoint 2007 or SharePoint 2010 installed on the remote server.
-MemberAgent	Optional	It is the SMSP Member Agent used by the Data Protection module. The value of the argument is **false** or **true**. **Note** The argument should not be entered if there is no SharePoint 2007 or SharePoint 2010 or SQL Server installed on the remote server.

Argument	Type	Comment
-Archiver	Optional	It is the Archiver agent type used by the Storage Optimization module. The value of the argument is **false** or **true**. **Note** The argument should not be entered if there is no SharePoint 2007 or SharePoint 2010 installed on the remote server. **Note** If you run the command to disable all the modules enabled in the Storage Optimization tab, a warning message will show up indicating that the externalized content may not be accessed through stubs on this machine. We recommend you taking the SharePoint Front-end Web Server out of the environment if it is a Network Load Balanced one.

Argument	Type	Comment
-IISResetNow	Optional	This argument specifies whether to restart the IIS. If Archiver argument is configured as **true**, the IISResetNow argument must be entered. The value of the argument is **true** or **false**. If it is configured as **true**, the IIS will be restarted at the end of the configuration. If it is configured as **false**, the IIS will not be restarted during the configuration process and it must be restarted manually after the configuration completes. **Note** If the IISResetNow argument is not entered when the Archiver argument is configured as **true**, there will be a warning message which let you choose whether to restart the IIS now or later. **Note** The IISResetNow argument will not be effective in the following conditions: the Archiver argument is not configured, the Archiver argument is configured as **false**, or the Archiver module has already been enabled.

Argument	Type	Comment
-Extender	Optional	It is the Extender agent type used by the Storage Optimization module. The value of the argument is **false** or **true**. **Note** The argument should not be entered if there is no SharePoint 2007 or SharePoint 2010 installed on the remote server. **Note** If you run the command to disable all the modules enabled in the Storage Optimization tab, a warning message will show up indicating that the externalized content may not be accessed through stubs on this machine. We recommend you taking the SharePoint Front-end Web Server out of the environment if it is a Network Load Balanced one.
-UseIPv6ForCommunication	Optional	This argument is used to make sure the availability of IPv6 communication in IPv6 environment. If this argument is not used, IPv4 communication will be used by default.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, *<Install-SMSPManager_201105161530.log>*. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, *<C:\test.log>*. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument can is to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Check Whether the Agent Can be Configured Remotely

This is a newly added command in SMSP 6.1.

To check whether the Agent can be configured remotely, run the command below:

```
Verify-SMSPAgentConfig
```

The example of the command is:

```
Verify-SMSPAgentConfig -Host 10.0.0.2 -User test\user -Password
user -RemoteTempPath "C:\Temp\SMSP" -Verifier
"D:\SMSPInstallAndConfigVerifier.exe" -AgentUser test\admin -
AgentPassword admin -ControlServiceAddress 10.0.0.1 -
ControlServicePort 12000 -AgentAddress 10.0.0.2 -AgentPort 20103 -
ArchiverPort 20207 -EnableIPv6 true -ControlAgent true -MemberAgent
true -Archiver true -Extender true
```

To configure the command arguments, see the table below:

Argument	Type	Comment
-Host	Required	The hostname or the IP address of the remote host to verify the configuration of the Agent on.
-User	Required	The user used for performing the verification in the remote host. The user must be a domain user and in the Administrator group of the remote server. The format of the user is domain\user.

Argument	Type	Comment
-Password	Required	The user's password for logging on the remote server. **Note** If you do not want to show the password on the interface, you can skip this argument, and after you enter this command line and press the **Enter** key to run this command, the interface will prompt you to enter the password, this password is encrypted.
-RemoteTempPath	Required	The path in the remote host where the <*SMSPInstallAndConfigVerifier.exe*> file will be copied to. For example, <d:\temp\install>. You can enter the local path for this argument, if the specific path does not exist in the remote machine, this path will be created automatically. **Note** The <*SMSPInstallAndConfigVerifier.exe*> file will be deleted automatically after the verification completes.

Argument	Type	Comment
-Verifier	Required	The path where the <*SMSPInstallAndConfigVerifier.exe*> file lies. The path must be an existing one. The path must be detailed to the name of the <*SMSPInstallAndConfigVerifier.exe*> file. Both local path on the server where you configure the script and network path can be used. **Note** The <*SMSPInstallAndConfigVerifier.exe*> file can be found in the *PowerShell-SnapIn* folder of the extracted <*SMSP61_ExtendedPack_The serial number.zip*> file.
-AgentUser	Required	The user used for the remote server to connect to the Manager and SharePoint content database. The format of the user is domain\username. You can view "Installing SnapManager for SharePoint" on page 17 for more information about the permissions required for the Agent user. **Note** You can use the Agent Account as the Agent user since the Agent user has the same permissions as the Agent Account.

Argument	Type	Comment
-AgentPassword	Required	The password of the user entered in AgentUser argument. **Note** If you do not want to show the password on the interface, you can skip this argument, and after you enter this command line and press the **Enter** key to run this command, the interface will prompt you to enter the password, this password is encrypted.
-ControlServiceAddress	Optional	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service installed.
-ControlServicePort	Optional	The port used for communication with the Control Service and it should match the information provided during the Manager configuration.
-AgentAddress	Optional	The host name or IP address of the remote server where the Agent installed.
-AgentPort	Optional	The port used by the Manager or other Agents for communication.
-ArchiverPort	Optional	The port is used for Archiver/Extender communication with SMSP BLOB Provider.

Argument	Type	Comment
-EnableIPv6	Optional	The argument must be the same as the configuration in the Manager. If its value is **true**, the IP address of the machine installed the Agent Service must be IPv6. The value of the argument is **false** or **true**.
-ControlAgent	Optional	It is the SMSP Control Agent used by the Data Protection module. The value of the argument is **false** or **true**. **Note** The argument should not be entered if there is no SharePoint 2007 or SharePoint 2010 installed on the remote server.
-MemberAgent	Optional	It is the SMSP Member Agent used by the Data Protection module. The value of the argument is **false** or **true**. **Note** The argument should not be entered if there is no SharePoint 2007, SharePoint 2010 or SQL Server installed on the remote server.

Argument	Type	Comment
-Archiver	Optional	It is the Archiver agent type used by the Storage Optimization module. The value of the argument is **false** or **true**. **Note** The argument should not be entered if there is no SharePoint 2007 or SharePoint 2010 installed on the remote server. **Note** If you run the command to disable all the modules enabled in the Storage Optimization tab, a warning message will show up indicating that the externalized content may not be accessed through stubs on this machine. We recommend you take the SharePoint Front-end Web Server out of the environment if it is a Network Load Balanced one.

Argument	Type	Comment
-Extender	Optional	It is the Extender agent type used by the Storage Optimization module. The value of the argument is **false** or **true**. **Note** The argument should not be entered if there is no SharePoint 2007 or SharePoint 2010 installed on the remote server. **Note** If you run the command to disable all the modules enabled in the Storage Optimization tab, a warning message will show up indicating that the externalized content may not be accessed through stubs on this machine. We recommend you take the SharePoint Front-end Web Server out of the environment if it is a Network Load Balanced one.
-UseIPv6ForCommunication	Optional	This argument is used to make sure the availability of IPv6 communication in IPv6 environment. If this argument is not used, IPv4 communication will be used by default.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, <*Install-SMSPManager_201105161530.log*>. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, <*C:\test.log*>. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Get Manager's/Agent's Configuration

In order to get the Manager's/Agent's configuration remotely, run the command below:

```
Get-SMSPManagerConfig
```

```
Get-SMSPAgentConfig
```

The examples of the commands are:

```
Get-SMSPManagerConfig -Host 10.0.0.1 -User test\admin -Password
admin
```

```
Get-SMSPAgentConfig -Host 10.0.0.1 -User test\admin -Password admin
```

To configure the command arguments, see the table below:

Argument	Type	Comment
-Host	Required	The hostname or the IP address of the remote host where to find the Manager's/Agent's configuration.
-User	Required	The user used for performing the configuration in the remote host. The user must be a domain user and in the Administrator group of the remote server. The format of the user is domain\user.

Argument	Type	Comment
-Password	Required	The user's password for logging on the remote server. **Note** If you do not want to show the password on the interface, you can skip this argument, and after you enter this command line and press the **Enter** key to run this command, the interface will prompt you to enter the password. This password is encrypted.
-UseIPv6ForCommunication	Optional	This argument is used to make sure the availability of IPv6 communication in IPv6 environment. If this argument is not used, IPv4 communication will be used by default.
-AnswerFilePath	Optional	The Manager's/Agent's configuration will be exported to an xml file in the local path specified here. The format of the path is: <C:\test\answerfile.xml>. **Note** If this argument is used, the configuration will not be displayed on the interface but be exported to the specified xml file.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, <*Install-SMSPManager_201105161530.log*>. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, <*C:\test.log*>. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument can is to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Install the RBS Provider

To install the RBS Provider on the specified content database (as the function in Blob Provider Settings page), run the command below:

```
Install-SMSPRBSProvider
```

The examples of the command are:

```
Install-SMSPRBSProvider -ControlServiceAddress 10.0.0.1 -Port 12011
-SMSPLoginName admin -SMSPLoginPassword admin -FarmName "FARM(CLI-
SP10:SHAREPOINT_CONFIG)" -ContentDatabaseNames
"contentDB1","contentDB2" -OperationMode Apply
```

```
Install-SMSPRBSProvider -ControlServiceAddress 10.0.0.1 -Port 12011
-SMSPLoginName admin -SMSPLoginPassword admin -FarmName "FARM(CLI-
SP10:SHAREPOINT_CONFIG)" -ContentDatabaseIDs "48d7e039-6837-46ef-
8722-6042ace546ae" -OperationMode Apply
```

To configure the command arguments, see the table below:

Argument	Type	Comment
-ControlServiceAddress	Required	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service is installed.
-Port	Required	The port used to access the CLI from other servers. It is the same as the Manager Web Service Port.
-SMSPLoginName	Required	The username for logging on SMSP Manager.
-SMSPLoginPassword	Required	The password for logging on SMSP Manager.

Argument	Type	Comment
-FarmName	Required	The farm that will install the RBS Provider. The format of farm name is: FARM (*the SQL instance's name where the SharePoint configuration database lies*: *the name of the configuration database*)
-ContentDatabaseNames (or -ContentDatabaseIDs)	Required	The content database(s) that will install the RBS Provider. Multiple content databases can be specified when separated by comma. For example, content-db-1, content-db-2, content-db-3 **Note** If the content databases have the same name in the environment, the ContentDatabaseIDs option must be used.

Argument	Type	Comment
-OperationMode	Required	The argument has two values. ● RunNow: The operation will be run immediately. ● Apply: The settings will be saved but the operation will not run until the schedule is triggered. **Note** For more information of enabling/disabling a schedule, refer to the introduction of the command Enable-<SMSPRBSProviderSchedule/ Disable-SMSPRBSProviderSchedule>.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, *<Install-SMSPManager_201105161530.log>*. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, *<C:\test.log>*. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Switch the EBS BLOB Provider of One Farm to the RBS Provider

This is a newly added command in SMSP 6.1.

To switch the EBS BLOB provider of a farm to the RBS provider, run the command below:

```
ConvertTo-SMSPRBS
```

The example of the command is:

```
ConvertTo-SMSPRBS -ControlServiceAddress 10.0.0.1 -Port 12011 -
SMSPLoginName admin -SMSPLoginPassword admin -FarmName "FARM(CLI-
SP10:SHAREPOINT_CONFIG)"
```

To configure the command arguments, see the table below:

Argument	Type	Comment
-ControlServiceAddress	Required	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service installed.
-Port	Required	The port used to access the CLI from other servers. It is the same as the Manager Web Service Port.
-SMSPLoginName	Required	The username for logging on SMSP Manager.
-SMSPLoginPassword	Required	The password for logging on SMSP Manager.

Argument	Type	Comment
-FarmName	Required	The command will switch the EBS provider of the farm specified here to the RBS provider of SMSP. The format of farm name is: FARM (*the SQL instance's name where the SharePoint configuration database lies*: *the name of the configuration database*) **Note** If the farm specified here does not use the EBS BLOB provider or the RBS provider, after running the command, the RBS provider will be used.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, <*Install-SMSPManager_201105161530.log*>. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, <*C:\test.log*>. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Uninstall the RBS Provider

To uninstall the RBS Provider on the specified content database (as the function in Blob Provider Settings page), run the command below:

```
Uninstall-SMSPRBSProvider
```

The examples of the command are:

```
Uninstall-SMSPRBSProvider -ControlServiceAddress 10.0.0.1 -Port
12011 -SMSPLoginName admin -SMSPLoginPassword admin -FarmName
"FARM(CLI-SP10:SHAREPOINT_CONFIG)" -ContentDatabaseNames
"contentDB1","contentDB2" -OperationMode RunNow
```

```
Uninstall-SMSPRBSProvider -ControlServiceAddress 10.0.0.1 -Port
12011 -SMSPLoginName admin -SMSPLoginPassword admin -FarmName
"FARM(CLI-SP10:SHAREPOINT_CONFIG)" -ContentDatabaseIDs "48d7e039-
6837-46ef-8722-6042ace546ae" -OperationMode RunNow
```

To configure the command arguments, see the table below:

Argument	Type	Comment
-ControlServiceAddress	Required	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service is installed.
-Port	Required	The port used to access the CLI from other servers. It is the same as the Manager Web Service Port.
-SMSPLoginName	Required	The username for logging on SMSP Manager.
-SMSPLoginPassword	Required	The password for logging on SMSP Manager.

Argument	Type	Comment
-FarmName	Required	The farm that will uninstall the RBS Provider. The format of farm name is: FARM (*the SQL instance's name where the SharePoint configuration database lies*: *the name of the configuration database*)
-ContentDatabaseNames (or -ContentDatabaseIDs)	Required	The content database(s) that will uninstall the RBS Provider. Multiple content databases can be specified when separated by comma. For example, content-db-1, content-db-2, content-db-3 **Note** If the content databases have the same name in the environment, the ContentDatabaseIDs option must be configured in the comment line.

Argument	Type	Comment
-OperationMode	Required	The argument has two values. ● **RunNow**: The operation will be run immediately. ● **Apply**: The settings will be saved but the operation will not run until the schedule is triggered. **Note** For more information of enabling/disabling a schedule, refer to the introduction of the command Enable-SMSPRBSProviderSchedule/Disable-SMSPRBSProviderSchedule.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, <*Install-SMSPManager_201105161530.log*>. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, <*C:\test.log*>. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Enable the Schedule for Applying the RBS Provider Settings

To enable the schedule for applying the RBS Provider settings, run the command below:

```
Enable-SMSPRBSProviderSchedule
```

Note

Only one schedule can be set for applying the RBS Provider settings.

The example of the command is:

```
Enable-SMSPRBSProviderSchedule -ControlServiceAddress 10.0.0.1 -
Port 12011 -SMSPLoginName admin -SMSPLoginPassword admin -FarmName
"FARM(CLI-SP10:SHAREPOINT_CONFIG)" -StartTime "2012-01-01 00:00:00"
-Interval onlyonce
```

To configure the command arguments, see the table below:

Argument	Type	Comment
-ControlServiceAddress	Required	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service installed.
-Port	Required	The port used to access the CLI from other servers. It is the same as the Manager Web Service Port.
-SMSPLoginName	Required	The username for logging on SMSP Manager.
-SMSPLoginPassword	Required	The password for logging on SMSP Manager.

Argument	Type	Comment
-FarmName	Required	The farm that will enable the schedule for applying the RBS Provider settings. The format of farm name is: FARM (*the SQL instance's name where the SharePoint configuration database lies*: *the name of the configuration database*)
-StartTime	Required	The start time of the schedule, it is the same as that in the GUI. The time string should be in the following format: yyyy-mm-dd hh:mm:ss. For example, 2011-03-20 22:30:00.

Argument	Type	Comment
-Interval	Required	The interval for the schedule. The following values are some examples for the argument: ● Onlyonce The schedule will run for only one time. ● 2h The schedule will run every 2 hours. You can change 2 to any positive integer. ● 3d The schedule will run every 3 days. You can change 3 to any positive integer. ● 4w The schedule will run every 4 weeks. You can change 4 to any positive integer. ● 5m The schedule will run every 5 months. You can change 5 to any positive integer.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, <*Install-SMSPManager_201105161530.log*>. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, <*C:\test.log*>. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Disable the Schedule for Applying the RBS Provider Settings

To disable the schedule for applying the RBS Provider settings, run the command below:

```
Disable-SMSPRBSProviderSchedule
```

The example of the command is:

```
Disable-SMSPRBSProviderSchedule -ControlServiceAddress 10.0.0.1 -
Port 12011 -SMSPLoginName admin -SMSPLoginPassword admin -FarmName
"FARM(CLI-SP10:SHAREPOINT_CONFIG)"
```

To configure the command arguments, see the table below:

Argument	Type	Comment
-ControlServiceAddress	Required	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service is installed.
-Port	Required	The port used to access the CLI from other servers. It is the same as the Manager Web Service Port.
-SMSPLoginName	Required	The username for logging on SMSP Manager.
-SMSPLoginPassword	Required	The password for logging on SMSP Manager.
-FarmName	Required	The farm that will disable the schedule for applying the RBS Provider settings. The format of farm name is: FARM (*the SQL instance's name where the SharePoint configuration database lies*: *the name of the configuration database*)

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, <*Install-SMSPManager_201105161530.log*>. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, <*C:\test.log*>. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Get RBS Provider Installation Status

In order to get a list that shows which content database has installed the RBS Provider, and which has not (as the function in Blob Provider Settings page), run the command below:

```
Get-SMSPRBSProviderSetting
```

The examples of the command are:

```
Get-SMSPRBSProviderSetting -ControlServiceAddress 10.0.0.1 -Port
12011 -SMSPLoginName admin -SMSPLoginPassword admin -FarmName
"FARM(CLI-SP10:SHAREPOINT_CONFIG)" -ContentDatabaseName
"contentDB1"
```

```
Get-SMSPRBSProviderSetting -ControlServiceAddress 10.0.0.1 -Port
12011 -SMSPLoginName admin -SMSPLoginPassword admin -FarmName
"FARM(CLI-SP10:SHAREPOINT_CONFIG)" -ContentDatabaseID "48d7e039-
6837-46ef-8722-6042ace546ae"
```

To configure the command arguments, see the table below.

Argument	Type	Comment
-ControlServiceAddress	Required	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service is installed.
-Port	Required	The port used to access the CLI from other servers. It is the same as the Manager Web Service Port.
-SMSPLoginName	Required	The username for logging on SMSP Manager.
-SMSPLoginPassword	Required	The password for logging on SMSP Manager.

Argument	Type	Comment
-FarmName	Required	The command will get a list of the status of RBS Provider Settings of the farm specified here. The format of farm name is: FARM (*the SQL instance's name where the SharePoint configuration database lies*: *the name of the configuration database*)
-ContentDatabaseName (-ContentDatabaseID)	Optional	The command will get the status of RBS Provider Settings of the content database specified here. **Note** Only one content database could be entered here.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, <*Install-SMSPManager_201105161530.log*>. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, <*C:\test.log*>. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Get the General Information of RBS Provider

In order to get the list that shows the general information of the RBS Provider in the specified farm (as the information shown in the *General* tab of BLOB Provider Settings page), run the command below:

```
Get-SMSPRBSProviderGeneralInfo
```

The example of the command is:

```
Get-SMSPRBSProviderGeneralInfo -ControlServiceAddress 10.0.0.1 -
Port 12011 -SMSPLoginName admin -SMSPLoginPassword admin –FarmName
"FARM(CLI-SP10:SHAREPOINT_CONFIG)"
```

To configure the command arguments, see the table below:

Argument	Type	Comment
-ControlServiceAddress	Required	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service installed.
-Port	Required	The port used to access the CLI from other servers. It is the same as the Manager Web Service Port.
-SMSPLoginName	Required	The username for logging on SMSP Manager.
-SMSPLoginPassword	Required	The password for logging on SMSP Manager.

Argument	Type	Comment
-FarmName	Required	The command will show the general information of the RBS Provider settings of the farm specified here. The format of farm name is: FARM (*the SQL instance's name where the SharePoint configuration database lies*: *the name of the configuration database*)

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, <*Install-SMSPManager_201105161530.log*>. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, <*C:\test.log*>. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Get the Status of the Schedule of Installing the RBS Provider

To get the status of the schedule of installing the RBS Provider, run the command below:

```
Get-SMSPRBSProviderSchedule
```

The example of the command is:

```
Get-SMSPRBSProviderSchedule -ControlServiceAddress 10.0.0.1 -Port
12011 -SMSPLoginName admin -SMSPLoginPassword admin -FarmName
"FARM(CLI-SP10:SHAREPOINT_CONFIG)"
```

To configure the command arguments, see the table below:

Argument	Type	Comment
-ControlServiceAddress	Required	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service installed.
-Port	Required	The port used to access the CLI from other servers. It is the same as the Manager Web Service Port.
-SMSPLoginName	Required	The username for logging on SMSP Manager.
-SMSPLoginPassword	Required	The password for logging on SMSP Manager.
-FarmName	Required	The command will get a list of the status of the schedule of installing the RBS Provider of the farm specified here. The format of farm name is: FARM (*the SQL instance's name where the SharePoint configuration database lies*: *the name of the configuration database*)

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, <*Install-SMSPManager_201105161530.log*>. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, <*C:\test.log*>. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Set Extender Settings

To set the Extender policy by specifying a content database and the corresponding policy (including Document Size, Logical Device and so on, which is just as the configuration in Extender Setting GUI), run the command below:

```
Set-SMSPExtenderSetting
```

The examples of the command are:

```
Set-SMSPExtenderSetting -ControlServiceAddress 10.0.0.1 -Port 12011
-SMSPLoginName admin -SMSPLoginPassword admin -FarmName "FARM(CLI-
SP10:SHAREPOINT_CONFIG)" -ContentDatabaseNames "contentDB1" -
DocumentSize 12MB -LogicalDevice "LogicalDeviceName" -Compression
"Agent" -ExtendExistingContent "Now"
```

```
Set-SMSPExtenderSetting -ControlServiceAddress 10.0.0.1 -Port 12011
-SMSPLoginName admin -SMSPLoginPassword admin -FarmName "FARM(CLI-
SP10:SHAREPOINT_CONFIG)" -ContentDatabaseIDs "48d7e039-6837-46ef-
8722-6042ace546ae" -DocumentSize 12MB -LogicalDevice
"LogicalDeviceName" -Compression "Agent" -ExtendExistingContent
"Now"
```

To configure the command arguments, see the table below:

Argument	Type	Comment
-ControlServiceAddress	Required	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service installed.
-Port	Required	The port used to access the CLI from other servers. It is the same as the Manager Web Service Port.
-SMSPLoginName	Required	The username for logging on SMSP Manager.
-SMSPLoginPassword	Required	The password for logging on SMSP Manager.

Argument	Type	Comment
-FarmName	Required	The farm that will configure the Extender Settings. The format of farm name is: FARM (*the SQL instance's name where the SharePoint configuration database lies*: *the name of the configuration database*)
-ContentDatabaseNames (or -ContentDatabaseIDs)	Required	The content database(s) that will configure the Extender Settings. Multiple content databases can be specified when separated by comma. For example, content-db-1, content-db-2, content-db-3 **Note** If the content databases have the same name in the environment, the ContentDatabaseIDs option must be configured in the command line.

Argument	Type	Comment
-DocumentSize	Optional	A positive integer can be entered (the unit could be KB or MB). Any file larger than the specified number will be extended, such as *500 KB*, *2 MB* and so on. *0 KB* (or *0 MB*) means all the documents will be extended. The size should be in the following ranges: *0 KB~2097151 KB* or *0 MB~2047 MB.*
-LogicalDevice	Optional	Specify the name of the Logical Device which is used to store the extended data. **Note** The argument is required when the Extender Settings are configured for the first time. It is optional when modifying the Extender Settings. **Note** The index device stores the information that will be used when performing the Delete Stub Policy of Extender, and the information of each stub is about 250 bytes in size. See "Device Manager" on page 91 for the detailed information of setting up the Index Device for Extender.

Argument	Type	Comment
-Compression	Optional	Allows you to specify whether to compress data once it has been extended, and whether the Media Service or the SharePoint Agent should perform the compression. The value of the argument is **No**, **Media** or **Agent**.
-ExtendExistingContent	Optional	Allows you to extend all of the existing content that complies with the new extender rule at the specified time. The values of the argument could be one of the following: ● No The existing content will not be extended. ● Now The existing content will be extended immediately. ● A specified time. The format of the time should be yyyy-mm-dd hh:mm:ss. For example, 2011-03-20 22:30:00.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, *<Install-SMSPManager_201105161530.log>*. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, *<C:\test.log>*. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Retract Extender Settings

To retract the Extender policy (Just as the configuration in Extender Setting GUI), run the command below:

```
Retract-SMSPExtenderSetting
```

The examples of the command are:

```
Retract-SMSPExtenderSetting -ControlServiceAddress 10.0.0.1 -Port
12011 -SMSPLoginName admin -SMSPLoginPassword admin -FarmName
"FARM(CLI-SP10:SHAREPOINT_CONFIG)" -ContentDatabaseNames
"contentDB1"
```

```
Retract-SMSPExtenderSetting -ControlServiceAddress 10.0.0.1 -Port
12011 -SMSPLoginName admin -SMSPLoginPassword admin -FarmName
"FARM(CLI-SP10:SHAREPOINT_CONFIG)" -ContentDatabaseIDs "48d7e039-
6837-46ef-8722-6042ace546ae"
```

To configure the command arguments, see the table below.

Argument	Type	Comment
-ControlServiceAddress	Required	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service installed.
-Port	Required	The port used to access the CLI from other servers. It is the same as the Manager Web Service Port.
-SMSPLoginName	Required	The username for logging on SMSP Manager.
-SMSPLoginPassword	Required	The password for logging on SMSP Manager.

Argument	Type	Comment
-FarmName	Required	The command will retract the Extender Settings of the content databases under the farm specified here. The format of farm name is: FARM (*the SQL instance's name where the SharePoint configuration database lies*: *the name of the configuration database*)
-ContentDatabaseNames (or -ContentDatabaseIDs)	Required	The content database(s) that will retract the Extender Settings. Multiple content databases can be specified when separated by comma. For example, content-db-1, content-db-2, content-db-3 **Note** If the content databases have the same name in the environment, the ContentDatabaseIDs must be configured in the command.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, <*Install-SMSPManager_201105161530.log*>. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, <*C:\test.log*>. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Get Extender Settings

To get the Extender policy of a specified content database (all the settings displayed in the Extender Setting GUI), run the command below:

```
Get-SMSPExtenderSetting
```

The examples of the command are:

```
Get-SMSPExtenderSetting -ControlServiceAddress 10.0.0.1 -Port 12011
-SMSPLoginName admin -SMSPLoginPassword admin -FarmName "FARM(CLI-
SP10:SHAREPOINT_CONFIG)" -ContentDatabaseName "contentDB1"
```

```
Get-SMSPExtenderSetting -ControlServiceAddress 10.0.0.1 -Port 12011
-SMSPLoginName admin -SMSPLoginPassword admin -FarmName "FARM(CLI-
SP10:SHAREPOINT_CONFIG)" -ContentDatabaseID "48d7e039-6837-46ef-
8722-6042ace546ae"
```

To configure the command arguments, see the table below:

Argument	Type	Comment
-ControlServiceAddress	Required	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service installed.
-Port	Required	The port used to access the CLI from other servers. It is the same as the Manager Web Service Port.
-SMSPLoginName	Required	The username for logging on SMSP Manager.
-SMSPLoginPassword	Required	The password for logging on SMSP Manager.

Argument	Type	Comment
-FarmName	Required	The command will get the Extender policy of some content database under the farm specified here. The format of farm name is: FARM (*the SQL instance's name where the SharePoint configuration database lies*: *the name of the configuration database*)
-ContentDatabaseName (or -ContentDatabaseID)	Optional	The command will get the Extender policy of the content database specified here. **Note** Only one content database can be specified here.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, <*Install-SMSPManager_201105161530.log*>. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, <*C:\test.log*>. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Create a New CIFS Physical Device

This is a newly added command in SMSP 6.1.

To create a new CIFS physical device, run the command below:

```
New-SMSPCIFSPhysicalDevice
```

The example of the command is:

```
New-SMSPCIFSPhysicalDevice -ControlServiceAddress 10.0.0.1 -Port
12011 -SMSPLoginName admin -SMSPLoginPassword admin -
PhysicalDeviceName physical -ForStoring Index -FilerProfile filer -
ShareName share -UserName test\admin -Password admin -ForFarms All
```

To configure the command arguments, see the table below:

Argument	Type	Comment
-ControlServiceAddress	Required	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service installed.
-Port	Required	The port used to access the CLI from other servers. It is the same as the Manager Web Service Port.
-SMSPLoginName	Required	The username for logging on SMSP Manager.
-SMSPLoginPassword	Required	The password for logging on SMSP Manager.
-PhysicalDeviceName	Required	The name of the physical device.
-ForStoring	Required	The type of the data to be stored in the CIFS physical device. The values of this argument can be *Index* or *Data* or *Both*.

Argument	Type	Comment
-FilerProfile	Required	The Filer used for the CIFS physical device. **Note** The corresponding Filer profile should be configured in Storage System page before running the command. See "Storage System" on page 109 for more information about how to set up the Filer profile.
-ShareName	Required	The Share Name of the corresponding volume.
-UserName	Required	The name of the user used to read data from the volume and write data to the volume. **Note** The user should have permissions to read data from the volume and write data to the volume.
-Password	Required	The password of the user specified in the argument UserName.
-ForFarms	Required	Specify the farm(s) that can use this device. Multiple farms can be specified when separated by comma. For example, Farm (SP01:SP_CFG), Farm (SP02:SP_CFG). You can use *All* to include all the farms that have connected to the SMSP Manager.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, *<Install-SMSPManager_201105161530.log>*. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, *<C:\test.log>*. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Add a CIFS Physical Device into an Existing CIFS Logical Device

This is a newly added command in SMSP 6.1.

To add a CIFS physical device into an existing CIFS logical device, run the command below:

```
Add-SMSPCIFSPhysicalDevice
```

The example of the command is:

```
Add-SMSPCIFSPhysicalDevice -ControlServiceAddress 10.0.0.1 -Port
12011 -SMSPLoginName admin -SMSPLoginPassword admin -
LogicalDeviceName logical -PhysicalDeviceNames physical1, physical2
```

To configure the command arguments, see the table below:

Argument	Type	Comment
-ControlServiceAddress	Required	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service installed.
-Port	Required	The port used to access the CLI from other servers. It is the same as the Manager Web Service Port.
-SMSPLoginName	Required	The username for logging on SMSP Manager.
-SMSPLoginPassword	Required	The password for logging on SMSP Manager.
-LogicalDeviceName	Required	The physical device(s) will be added to the logical device specified here. Only one logical device can be entered.
-PhysicalDeviceNames	Required	Specify the physical device(s) to be added to the logical device. Multiple physical devices can be entered when separated by the comma.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, *<Install-SMSPManager_201105161530.log>*. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, *<C:\test.log>*. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Get Information on CIFS Physical Devices of CIFS Logical Device

This is a newly added command in SMSP 6.1.

To get the information of the CIFS physical devices of a specified CIFS logical device, run the command below:

```
Get-SMSPCIFSPhysicalDevice
```

The example of the command is:

```
Get-SMSPCIFSPhysicalDevice -ControlServiceAddress 10.0.0.1 -Port
12011 -SMSPLoginName admin -SMSPLoginPassword admin –
LogicalDeviceName logical
```

To configure the command arguments, see the table below:

Argument	Type	Comment
-ControlServiceAddress	Required	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service installed.
-Port	Required	The port used to access the CLI from other servers. It is the same as the Manager Web Service Port.
-SMSPLoginName	Required	The username for logging on SMSP Manager.
-SMSPLoginPassword	Required	The password for logging on SMSP Manager.
-LogicalDeviceName	Required	The command will get the information of the CIFS physical devices of the logical device entered here. Only one logical device can be entered.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, <*Install-SMSPManager_201105161530.log*>. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, <*C:\test.log*>. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Run the Data Protection Backup Job Using CLI

This is a newly added command in SMSP 6.1.

To run the Data Protection Backup job, run the command below:

```
New-SMSPBackupJob
```

The example of the command is:

```
New-SMSPBackupJob -ControlServiceAddress 10.0.0.1 -Port 12011 -
SMSPLoginName admin -SMSPLoginPassword admin -FarmName "FARM(CLI-
SP10:SHAREPOINT_CONFIG)" -PlanName plan -ScheduleName A -
WaitForJobComplete
```

To configure the command arguments, see the table below:

Argument	Type	Comment
-ControlServiceAddress	Required	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service installed.
-Port	Required	The port used to access the CLI from other servers. It is the same as the Manager Web Service Port.
-SMSPLoginName	Required	The username for logging on SMSP Manager.
-SMSPLoginPassword	Required	The password for logging on SMSP Manager.
-FarmName	Required	The name of the farm to run the backup job. Only one farm could be entered here.
-PlanName	Required	The name of the plan.

Argument	Type	Comment
-ScheduleName	Required	Specify one enabled schedule in the interface, and the command will run the plan immediately according to the settings in the schedule. The value of the argument could be *A*, *B*, *C*, *D*, *E*, or *F*. Only one schedule can be entered here. **Note** There should be at least one schedule enabled for the corresponding plan.
-WaitForJobComplete	Optional	If this argument is used, the CLI will wait for the command to complete and there will be a progress bar shown for the corresponding job. You can continue to enter another command if this argument is not used.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, *<Install-SMSPManager_201105161530.log>*. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, *<C:\test.log>*. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Get the Job Status

This is a newly added command in SMSP 6.1.

To get the status of the specified job, run the command below:

```
Get-SMSPJobStatus
```

The example of the command is:

```
Get-SMSPJobStatus -ControlServiceAddress 10.0.0.1 -Port 12011 -
SMSPLoginName admin -SMSPLoginPassword admin -JobType Backup -JobID
FB20110505120012
```

To configure the command arguments, see the table below:

Argument	Type	Comment
-ControlServiceAddress	Required	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service installed.
-Port	Required	The port used to access the CLI from other servers. It is the same as the Manager Web Service Port.
-SMSPLoginName	Required	The username for logging on SMSP Manager.
-SMSPLoginPassword	Required	The password for logging on SMSP Manager.
-JobType	Required	The type of the job. The value of this argument is *Backup*.

Argument	Type	Comment
-JobID	Required	The job ID of the corresponding job. It will be returned after the `New` command of the corresponding plan is finished. Only one job ID can be specified here.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, <*Install-SMSPManager_201105161530.log*>. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, <*C:\test.log*>. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Get the Job Report

This is a newly added command in SMSP 6.1.

To get the job report of the specified job, run the command below:

```
Download-SMSPJobReport
```

The example of the command is:

```
Download-SMSPJobReport -ControlServiceAddress 10.0.0.1 -Port 12011
-SMSPLoginName admin -SMSPLoginPassword admin -JobType Backup -
JobID FB20110505120012 -Path c:\report -Name report.zip -Force
```

To configure the command arguments, see the table below:

Argument	Type	Comment
-ControlServiceAddress	Required	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service installed.
-Port	Required	The port used to access the CLI from other servers. It is the same as the Manager Web Service Port.
-SMSPLoginName	Required	The username for logging on SMSP Manager.
-SMSPLoginPassword	Required	The password for logging on SMSP Manager.
-JobType	Required	The type of the job. The value of this argument is *Backup*.

Argument	Type	Comment
-JobID	Required	The job ID of the corresponding job. It will be returned after the `New` command of the corresponding plan is finished. Only one job ID could be specified here.
-Path	Required	The existing UNC path to save the report file to. The user who runs the command should have the **Write** permission of the corresponding path. You can specify the name of the report file in the *Name* argument, or include it in the *Path* argument. Multiple paths can be entered here when separated by the comma.

Argument	Type	Comment
-Name	Required	The name of the report file. You can specify the name of the report file in the *Name* argument. You can also specify the path to save the report file to in the *Name* argument or *Path* argument. The extension of the report file must be **.zip**. **Note** Only one name or one path could be specified in this argument.
-Force	Optional	If you use this argument, the former report file with the same name as the current one will be overwritten without a prompt. If you do not use this argument, the command will exit with an error when the former report file has the same name as the current one.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, <*Install-SMSPManager_201105161530.log*>. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, <*C:\test.log*>. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Create a Local User in Account Manager Using CLI

This is a newly added command in SMSP 6.1.

To create a local user in Account Manager, run the command below:

```
New-SMSPLocalUser
```

The example of the command is:

```
New-SMSPLocalUser -ControlServiceAddress 10.0.0.1 -Port 12011 -
SMSPLoginName admin -SMSPLoginPassword admin –LocalUserName
localuser -Password local -Email localuser@avepoint.com -GroupName
Administrators
```

To configure the command arguments, see the table below:

Argument	Type	Comment
-ControlServiceAddress	Required	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service installed.
-Port	Required	The port used to access the CLI from other servers. It is the same as the Manager Web Service Port.
-SMSPLoginName	Required	The username for logging on SMSP Manager.
-SMSPLoginPassword	Required	The password for logging on SMSP Manager.
-LocalUserName	Required	The name of the local user you want to create.
-Password	Required	Specify the password for the local user. It is used when logging on SMSP Manager.
-Email	Required	The email address of the new local user.

Argument	Type	Comment
-GroupName	Optional	If a group's name is entered here, the new local user will be added to the group.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, *<Install-SMSPManager_201105161530.log>*. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, <*C:\test.log*>. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Add an AD User in Account Manager Using CLI

This is a newly added command in SMSP 6.1.

To add an existing AD user in Account Manager, run the command below:

```
New-SMSPADUser
```

The example of the command is:

```
New-SMSPADUser -ControlServiceAddress 10.0.0.1 -Port 12011 -
SMSPLoginName admin -SMSPLoginPassword admin -ADUserName
test\aduser -GroupName Administrators -Email aduser@avepoint.com
```

Note

Before running this command, make sure the Enable Active Directory checkbox is selected and the corresponding information is entered in SMSP Manager Configuration Tool.

To configure the command arguments, see the table below:

Argument	Type	Comment
-ControlServiceAddress	Required	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service installed.
-Port	Required	The port used to access the CLI from other servers. It is the same as the Manager Web Service Port.
-SMSPLoginName	Required	The username for logging on SMSP Manager.
-SMSPLoginPassword	Required	The password for logging on SMSP Manager.
-ADUserName	Required	The name of the AD user which you want to add. The format of the name is domain\username.

Argument	Type	Comment
-GroupName	Required	The specified AD user will be added to the group entered here.
-Email	Optional	The email address of the newly added AD user.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, *<Install-SMSPManager_201105161530.log>*. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, *<C:\test.log>*. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Get the Information of the Users from Account Manager

This is a newly added command in SMSP 6.1.

To get the users' information (including the user's name, the group that the user is added to and the email address of the user) from the Account Manager, run the command below:

```
Get-SMSPUser
```

The examples of the command are:

```
Get-SMSPUser -ControlServiceAddress 10.0.0.1 -Port 12011 -
SMSPLoginName admin -SMSPLoginPassword admin -Type Both
```

```
Get-SMSPUser -ControlServiceAddress 10.0.0.1 -Port 12011 -
SMSPLoginName admin -SMSPLoginPassword admin -UserName admin
```

To configure the command arguments, see the table below:

Argument	Type	Comment
-ControlServiceAddress	Required	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service installed.
-Port	Required	The port used to access the CLI from other servers. It is the same as the Manager Web Service Port.
-SMSPLoginName	Required	The username for logging on SMSP Manager.
-SMSPLoginPassword	Required	The password for logging on SMSP Manager.

Argument	Type	Comment
-Type	Optional	The value of this argument can be **Both**, or **LocalUser**, or **ADUser**. ● If **Both** is used, all users' information will be displayed. ● If **LocalUser** is used, only the local users' information will be displayed. ● If **ADUser** is used, only the AD users' information will be displayed. **Note** Only one of the Type and UserName arguments can be used.
-UserName	Optional	It is the user's name in the Account Manager. For AD user, the name's format is domain\username. **Note** Only one of the Type and UserName arguments can be used.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, <*Install-SMSPManager_201105161530.log*>. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, <*C:\test.log*>. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Delete One User from Account Manager

This is a newly added command in SMSP 6.1.

To delete a user from the Account Manager, run the command below:

```
Remove-SMSPUser
```

The example of the command is:

```
Remove-SMSPUser -ControlServiceAddress 10.0.0.1 -Port 12011 -
SMSPLoginName admin -SMSPLoginPassword admin -UserName user
```

To configure the command arguments, see the table below:

Argument	Type	Comment
-ControlServiceAddress	Required	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service installed.
-Port	Required	The port used to access the CLI from other servers. It is the same as the Manager Web Service Port.
-SMSPLoginName	Required	The username for logging on SMSP Manager.
-SMSPLoginPassword	Required	The password for logging on SMSP Manager.

Argument	Type	Comment
-UserName	Required	The name of the user you want to delete from the Account Manager. Only one user can be entered. For AD user, the name's format is domain\username. The user cannot be deleted in the following conditions: ● If you are logging in SMSP Manager using a user, it cannot be deleted using this command. ● The default user *admin* cannot be deleted using this command.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, *<Install-SMSPManager_201105161530.log>*. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, *<C:\test.log>*. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Update the Information of a Local User in Account Manager

This is a newly added command in SMSP 6.1.

To update the information of a local user in the Account Manager, run the command below:

```
Update-SMSPLocalUser
```

The example of the command is:

```
Update-SMSPLocalUser -ControlServiceAddress 10.0.0.1 -Port 12011 -
SMSPLoginName admin -SMSPLoginPassword admin -LocalUserName
localuser -Email localusernew@avepoint.com -OldPassword local -
NewPassword localnew -GroupName Administrators
```

To configure the command arguments, see the table below.

Argument	Type	Comment
-ControlServiceAddress	Required	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service installed.
-Port	Required	The port used to access the CLI from other servers. It is the same as the Manager Web Service Port.
-SMSPLoginName	Required	The username for logging on SMSP Manager.
-SMSPLoginPassword	Required	The password for logging on SMSP Manager.
-LocalUserName	Required	The information of the local user specified here will be updated. **Note** Only one user can be entered here.

Argument	Type	Comment
-Email	Optional	The new email address of the local user.
-OldPassword	Optional	The old password of the local user.
-NewPassword	Optional	The new password of the local user.
-GroupName	Optional	The new group that you want to add the local user to.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, <*Install-SMSPManager_201105161530.log*>. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, <*C:\test.log*>. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

Update the Information of an AD User in Account Manager

This is a newly added command in SMSP 6.1.

To update the information of an AD user in the Account Manager, run the command below:

```
Update-SMSPADUser
```

The example of the command is:

```
Update-SMSPADUser -ControlServiceAddress 10.0.0.1 -Port 12011 -
SMSPLoginName admin -SMSPLoginPassword admin -ADUserName
test\aduser -Email adusernew@avepoint.com –GroupName Operators
```

To configure the command arguments, see the table below:

Argument	Type	Comment
-ControlServiceAddress	Required	The hostname or the IP address of the server where the SnapManager for SharePoint Control Service installed.
-Port	Required	The port used to access the CLI from other servers. It is the same as the Manager Web Service Port.
-SMSPLoginName	Required	The username for logging on SMSP Manager.
-SMSPLoginPassword	Required	The password for logging on SMSP Manager.
-ADUserName	Required	The information of the AD user specified here will be updated. The format of the name is domain\username. **Note** Only one user can be entered here.

Argument	Type	Comment
-Email	Optional	The new email address of the AD user.
-GroupName	Optional	The new group that you want to add the AD user to.

Argument	Type	Comment
-Log	Optional	You can specify a path here to save the logs of the command. The value of this argument can be a path of an existing folder or specified file. ● If the path is a folder. For example, <*C:\test*> (test is an existing folder under disk C). The corresponding log file will be created in the folder using the following format: *CommandName_DateAndTime*. For example, *<Install-SMSPManager_201105161530.log>*. **Note** If the folder does not exist, there will be an error in the interface and the command will exit. ● If the path is a specified file. For example, <*C:\test.log*>. **Note** If the file specified in the path does not exist, the corresponding file will be created. If the file is an existing one, the logs will be appended to the existing content of the existing file.

Argument	Type	Comment
-Verbose	Optional	This argument is used to display more detailed logs on the interface. If the Log argument is used, using this argument can also write more detailed logs to the specified log file.

NA 210-05267_A0, Printed in USA

GC27-2097-04