

HP Data Protector A.06.11

Integration guide for HP Service Information Portal

Part number: B6960-90167
First edition: September 2009



Legal and notice information

© Copyright 2009 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Intel, Itanium, Pentium, Intel Inside, and the Intel Inside logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Microsoft®, Windows®, Windows XP®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java™ is a US trademark of Sun Microsystems, Inc.

Oracle is a registered US trademark of Oracle Corporation, Redwood City, California.

UNIX is a registered trademark of The Open Group.

Printed in the US

Contents

About this guide	9
Intended audience	9
Documentation set	9
Guides	9
Online help	12
Documentation map	13
Abbreviations	13
Map	14
Integrations	15
Document conventions and symbols	16
General Information	17
HP technical support	17
Subscription service	17
HP websites	17
Documentation feedback	18
1 Introduction	19
Component list	20
Product capabilities and integration benefits	20
How Data Protector integrates with SIP	21
Related Data Protector integrations	22
2 Installing the integration	23
Planning the integration	23
Installing the integration	24
Prerequisites	24
Dependencies	26
Installing on the Data Protector Cell Server	26
Establishing Data Protector/SIP Communication	26
Installing on a Windows SIP Server	26
Installing on an HP-UX SIP server	27
Installing on a Solaris SIP server	28

Installing on a web server	28
Installing on a Windows web server	29
Installing on an HP-UX web server	29
Installing on a Solaris web server	30
3 Customizing the integration	33
Setting up backup groups on Data Protector	33
Editing ConfigSpec.xml	33
Log Location, Log Level	34
Filter Level	34
Refresh Rate	34
Gauge Settings	35
Cell Manager Setting	36
4 Creating customer models and portal views	37
Customer models	37
Importing the customer model	38
Management data filter	38
Adding and removing services in a portal view	39
5 Modules	41
Data Protector protection status module	41
Data Protector protection status gauge	41
All Hosts Backup Statistics report	41
Client Host Backup report	42
Host Statistics report	43
Detail view	44
Editing the Data Protector protection status module	44
Using the Protection Status—Edit page	44
Protection status criteria	45
Editing PortalView.xml directly	45
Data Protector reports module	45
Data list trees	46
Object last backup	46
Editing the Data Protector reports module	46
Editing PortalView.xml directly	47
Establishing global settings for reports	47
Data Protector backup session list report module	47
Editing the Data Protector backup session list report module	48
Editing PortalView.xml directly	48
Establishing global settings for reports	48

Data Protector error messages module	49
Adding a Data Protector error message module to your portal view—GUI	49
Editing the Data Protector message module	50
Editing PortalView.xml directly	51
Establishing Global Settings for Reports	51
6 Uninstalling the integration	53
7 Troubleshooting	55
Error messages	55
Index	57

Figures

1 Backup group mappings	33
2 Customer model	38
3 Management data filter overview	39

Tables

1 Document conventions	16
2 Software requirements—Data Protector	25
3 Software requirements—SIP	25

About this guide

This guide describes how to install, configure, and use the integration of Data Protector with HP Service Information Portal. It discusses how to use the portal for Data Protector service management.

Intended audience

This guide is intended for backup administrators, with knowledge of:

- HP Service Information Portal (SIP)
- HP Data Protector concepts

Documentation set

Other documents and online Help provide related information.

Guides

Data Protector guides are available in printed format and in PDF format. Install the PDF files during the Data Protector setup procedure by selecting the `English documentation & Help` component on Windows or the `OB2-DOCS` component on UNIX. Once installed, the guides reside in the `Data_Protector_home\docs` directory on Windows and in the `/opt/omni/doc/C/` directory on UNIX.

You can find these documents from the `Manuals` page of the HP Business Support Center website:

<http://www.hp.com/support/manuals>

In the `Storage` section, click **Storage Software** and then select your product.

- *HP Data Protector concepts guide*

This guide describes Data Protector concepts and provides background information on how Data Protector works. It is intended to be used with the task-oriented online Help.

- *HP Data Protector installation and licensing guide*
This guide describes how to install the Data Protector software, taking into account the operating system and architecture of your environment. This guide also gives details on how to upgrade Data Protector, as well as how to obtain the proper licenses for your environment.
- *HP Data Protector troubleshooting guide*
This guide describes how to troubleshoot problems you may encounter when using Data Protector.
- *HP Data Protector disaster recovery guide*
This guide describes how to plan, prepare for, test and perform a disaster recovery.
- *HP Data Protector integration guides*
These guides describe how to configure and use Data Protector to back up and restore various databases and applications. It is intended for backup administrators or operators. There are four guides:
 - *HP Data Protector integration guide for Microsoft applications: SQL Server, SharePoint Portal Server, Exchange Server, and Volume Shadow Copy Service*
This guide describes the integrations of Data Protector with the following Microsoft applications: Microsoft Exchange Server, Microsoft SQL Server, and Volume Shadow Copy Service.
 - *HP Data Protector integration guide for Oracle and SAP*
This guide describes the integrations of Data Protector with Oracle, SAP R3, and SAP DB/MaxDB.
 - *HP Data Protector integration guide for IBM applications: Informix, DB2, and Lotus Notes/Domino*
This guide describes the integrations of Data Protector with the following IBM applications: Informix Server, IBM DB2, and Lotus Notes/Domino Server.
 - *HP Data Protector integration guide for VMWare, Sybase, Network Node Manager, and Network Data Management Protocol Server*
This guide describes the integrations of Data Protector with VMware Virtual Infrastructure, Sybase, Network Node Manager, and Network Data Management Protocol Server.
- *HP Data Protector integration guide for HP Service Information Portal*
This guide describes how to install, configure, and use the integration of Data Protector with HP Service Information Portal. It is intended for backup administrators. It discusses how to use the applications for Data Protector service management.

- *HP Data Protector integration guide for HP Reporter*
This guide describes how to install, configure, and use the integration of Data Protector with HP Reporter. It is intended for backup administrators. It discusses how to use the applications for Data Protector service management.
- *HP Data Protector integration guide for HP Operations Manager for UNIX*
This guide describes how to monitor and manage the health and performance of the Data Protector environment with HP Operations Manager and HP Service Navigator on UNIX.
- *HP Data Protector integration guide for HP Operations Manager for Windows*
This guide describes how to monitor and manage the health and performance of the Data Protector environment with HP Operations Manager and HP Service Navigator on Windows.
- *HP Data Protector integration guide for HP Performance Manager and HP Performance Agent*
This guide provides information about how to monitor and manage the health and performance of the Data Protector environment with HP Performance Manager (PM) and HP Performance Agent (PA) on Windows, HP-UX, Solaris and Linux
- *HP Data Protector zero downtime backup concepts guide*
This guide describes Data Protector zero downtime backup and instant recovery concepts and provides background information on how Data Protector works in a zero downtime backup environment. It is intended to be used with the task-oriented *HP Data Protector zero downtime backup administrator's guide* and the *HP Data Protector zero downtime backup integration guide*.
- *HP Data Protector zero downtime backup administrator's guide*
This guide describes how to configure and use the integration of Data Protector with HP StorageWorks Virtual Array, HP StorageWorks Enterprise Virtual Array, EMC Symmetrix Remote Data Facility and TimeFinder, and HP StorageWorks Disk Array XP. It is intended for backup administrators or operators. It covers the zero downtime backup, instant recovery, and the restore of filesystems and disk images.
- *HP Data Protector zero downtime backup integration guide*
This guide describes how to configure and use Data Protector to perform zero downtime backup, instant recovery, and standard restore of Oracle, SAP R/3, Microsoft Exchange Server, and Microsoft SQL Server databases. The guide also describes how to configure and use Data Protector to perform backup and restore using the Microsoft Volume Shadow Copy Service.
- *HP Data Protector MPE/iX System user guide*

This guide describes how to configure MPE/iX clients and how to back up and restore MPE/iX data.

- *HP Data Protector Media Operations user guide*
This guide provides information for network administrators responsible for maintaining and backing up systems on the tracking and management of offline storage media. It describes the tasks of installing and configuring the application, performing daily media operations and producing reports.
- *HP Data Protector product announcements, software notes, and references*
This guide gives a description of new features of HP Data Protector A.06.11. It also provides information on supported configurations (devices, platforms and online database integrations, SAN, and ZDB), required patches, and limitations, as well as known problems and workarounds. An updated version of the supported configurations is available at <http://www.hp.com/support/manuals>
- *HP Data Protector product announcements, software notes, and references for integrations to HP Operations Manager, HP Reporter, HP Performance Manager, HP Performance Agent, and HP Service Information Portal*
This guide fulfills a similar function for the listed integrations.
- *HP Data Protector Media Operations product announcements, software notes, and references*
This guide fulfills a similar function for Media Operations.
- *HP Data Protector Command Line Interface Reference*
This guide describes the Data Protector Command Line Interface commands, their options and usage as well as providing some basic command line examples.

Online help

Data Protector provides context-sensitive (F1) Help and Help Topics for Windows and UNIX platforms.

You can access the online help from the top-level directory on the installation DVD-ROM without installing Data Protector:

- **Windows:** Unzip `DP_help.zip` and open `DP_help.chm`.
- **UNIX:** Unpack the zipped tar file `DP_help.tar.gz`, and access the online help system through `DP_help.htm`.

Documentation map

Abbreviations

Abbreviations in the documentation map that follows are explained below. The guide titles are all preceded by the words “HP Data Protector.”

Abbreviation	guide
CLI	Command line interface reference guide
Concepts	Concepts guide
DR	Disaster recovery guide
GS	Getting started guide
Help	Online Help
IG-IBM	Integration guide for IBM applications: Informix, DB2, and Lotus Notes/Domino
IG-MS	Integration guide for Microsoft applications: SQL Server, SharePoint Portal Server, Exchange Server, and Volume Shadow Copy Service
IG-O/S	Integration guide for Oracle and SAP
IG-OMU	Integration guide for HP Operations Manager for UNIX
IG-OMW	Integration guide for HP Operations Manager for Windows
IG-PM/PA	Integration guide for HP Performance Manager and HP Performance Agent
IG-Report	Integration guide for HP Reporter
IG-SIP	Integration guide for HP Service Information Portal
IG-Var	Integration guide for VMware Virtual Infrastructure, Sybase, Network Node Manager, and Network Data Management Protocol Server
Install	Installation and licensing guide
MO GS	Media Operations getting started guide

Abbreviation	guide
MO RN	Media Operations product announcements, software notes, and references
MO UG	Media Operations user guide
MPE/iX	MPE/iX system user guide
PA	Product announcements, software notes, and references
Trouble	Troubleshooting guide
ZDB Admin	ZDB administrator's guide
ZDB Concpt	ZDB concepts guide
ZDB IG	ZDB integration guide

Map

The following table shows where to find information of different kinds. Shaded squares are a good place to look first.

	Help	GS	Concepts	Install	Trouble	DR	PA	Integration guides						ZDB			MO		MPE/iX	CLI		
								MS	O/S	IBM	Var	OV	OV/OU	OV/OW	Concept	Admin	IG	GS			User	PA
Backup	X	X	X					X	X	X	X			X	X	X					X	
CLI																						X
Concepts/ Techniques	X		X					X	X	X	X	X	X	X	X	X						X
Disaster Recovery	X		X			X																
Installation/ Upgrade	X	X		X			X					X	X	X			X	X				X
Instant Recovery	X		X										X	X	X							
Licensing	X		X				X											X				
Limitations	X				X		X	X	X	X	X		X		X						X	
New features	X						X															
Planning strategy	X		X								X		X									
Procedures/ Tasks	X			X	X	X		X	X	X	X	X	X	X	X		X	X				
Recommendations			X				X						X								X	
Requirements			X				X	X	X	X	X		X				X	X	X			
Restore	X	X	X					X	X	X	X			X	X							X
Supported configurations													X									
Troubleshooting	X			X	X			X	X	X	X	X			X	X						

Integrations

Look in these guides for details of the following integrations:

Integration	Guide
HP Operations Manager for UNIX/for Windows	IG-OMU, IG-OMW
HP Performance Manager	IG-PM/PA
HP Performance Agent	IG-PM/PA
HP Reporter	IG-R
HP Service Information Portal	IG-SIP
HP StorageWorks Disk Array XP	all ZDB
HP StorageWorks Enterprise Virtual Array (EVA)	all ZDB
HP StorageWorks Virtual Array (VA)	all ZDB
IBM DB2 UDB	IG-IBM
Informix	IG-IBM
Lotus Notes/Domino	IG-IBM
MaxDB	IG-O/S
Media Operations	MO User
MPE/iX System	MPE/iX
Microsoft Exchange Servers	IG-MS, ZDB IG
Microsoft Exchange Single Mailbox	IG-MS
Microsoft SQL Servers	IG-MS, ZDB IG
Microsoft Volume Shadow Copy Service (VSS)	IG-MS, ZDB IG
NDMP Server	IG-Var
Network Node Manager (NNM)	IG-Var

Integration	Guide
Oracle	IG-O/S
Oracle ZDB	ZDB IG
SAP DB	IG-O/S
SAP R/3	IG-O/S, ZDB IG
Sybase	IG-Var
Symmetrix (EMC)	all ZDB
VMware	IG-Var

Document conventions and symbols

Table 1 Document conventions

Convention	Element
Blue text: Table 1 on page 16	Cross-reference links and e-mail addresses
Blue, underlined text: http://www.hp.com	website addresses
Bold text	<ul style="list-style-type: none"> • Keys that are pressed • Text typed into a GUI element, such as a box • GUI elements that are clicked or selected, such as menu and list items, buttons, tabs, and check boxes
<i>Italic text</i>	Text emphasis
Monospace text	<ul style="list-style-type: none"> • File and directory names • System output • Code • Commands, their arguments, and argument values
<i>Monospace, italic text</i>	<ul style="list-style-type: none"> • Code variables • Command variables
Monospace, bold text	Emphasized monospace text



NOTE:

Provides additional information.

General Information

General information about Operations Manager can be found at <http://www.hp.com/go/dataprotector>

HP technical support

For worldwide technical support information, see the HP support website:

<http://www.hp.com/support>

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

<http://www.hp.com/go/e-updates>

After registering, you will receive e-mail notification of product enhancements, new driver versions, firmware updates, and other product resources.

HP websites

For additional information, see the following HP websites:

- <http://www.hp.com>

- <http://www.hp.com/go/storage>
- <http://www.hp.com/support/manuals>
- <http://www.hp.com/support/downloads>

Documentation feedback

HP welcomes your feedback.

To make comments and suggestions about product documentation, please send a message to DP.DocFeedback@hp.com. All submissions become the property of HP.

1 Introduction

This guide describes the integration of Data Protector with HP Service Information Portal.

- **HP Data Protector** is a backup and recovery solution designed specifically for enterprise-wide and distributed environments.
Data Protector provides information that can be used, through reports and messaging tools, to help you monitor the status of processes, in addition to providing backup and recovery functionality.
- **HP Service Information Portal (SIP)** creates a “portal” view into a customer’s services for a service provider. It allows you present data from your internal applications such as Data Protector, HP Internet Services, HP Reporter, and HP Operations Manager as reports on custom web pages for each of your clients.

This chapter describes how to install, configure, and use Data Protector with Service Information Portal (SIP) to serve customer-defined reports in the portal.

The integration allows information from Data Protector to be used by SIP its portal capabilities. With SIP, you can monitor and control Data Protector backup and recovery processes. More details are given in the following sections.

The integration of Data Protector and Service Information Portal (SIP) assists Service Level Management (SLM) to help you achieve a specific, consistent and measurable level of service. It provides a simple, effective way for the following:

- Convenient data protection service monitoring through web access from any machine.
- Specification of resource in terms of machine and group names.
- Segmentation of accessible data by different backup administrators.
- Information aggregation from other services (not related to Data Protector) to the portal, using SIP’s configuration mechanisms. Single presentation format for all modules.
- Easy configuration: GUI configuration editor and XML document editing only.
- Stability and reliability. The integration modifies very little code and relies upon SIP customization features and components.

OV SIP portal components and modules include Service Browser, Service Graph, and Service Cards.

Component list

- Data Protector—a backup solution that provides reliable data protection and maximum accessibility for your business data. Data Protector offers comprehensive backup and restore functionality specifically tailored for enterprise-wide and distributed environments.
- SIP (Service Information Portal)—a tool that aggregates information collected from various services. The information is presented and formatted through various portal components and is made available through a web page. Portal components and modules include Service Browser, Service Graph, and Service Cards.

Product capabilities and integration benefits

The integration of Data Protector and Service Information Portal (SIP) assists Service Level Management (SLM) to help you achieve a specific, consistent and measurable level of service. It provides a simple, effective way for the following:

- Convenient data protection service monitoring through web access from any machine.
- Specification of resource in terms of machine and group names.
- Segmentation of accessible data by different backup administrators.
- Information aggregation from other services (not related to Data Protector) to the portal, using SIP's configuration mechanisms. Single presentation format for all modules.
- Easy configuration: GUI configuration editor and XML document editing only.
- Stability and reliability. The integration modifies very little code and relies upon SIP customization features and components.

The integration consists of two main elements:

- The *Data Protector Integration module*, installed on the SIP server or a separate web server.

The module's components are automatically installed with SIP, and are on your SIP web server or on a separate web server, depending on your deployment.

The module consists of two primary elements:

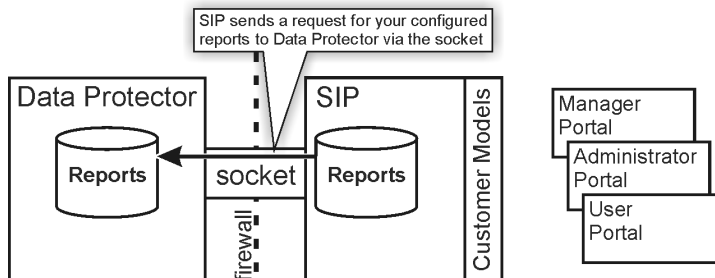
- SIP components, including SIP XML, XSL, and module definitions.

- SIP-Data Protector servlets, including the following Java servlets, as well as the Configuration Specifications, `ConfigSpec.xml`:
 - `CustomerGroup` servlet: provides the customer model to the SIP Management Data Filter.
 - `Reporter` servlet: generates and creates XML reports, and includes a configurable threading option.
 - `StatusGauge` servlet: generates status gauges.
- The *Cell Request Server (CRS) process*, installed on the Data Protector cell manager, which sends reports to SIP via the socket. For information on configuring this module, see “[Installing the integration](#)” on page 24.

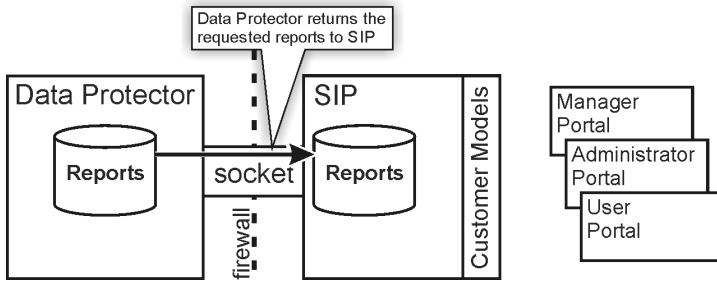
How Data Protector integrates with SIP

To integrate with SIP, Data Protector’s CRS daemon sends reports to the Java servlets on the SIP or web server, as shown in the following illustrations.

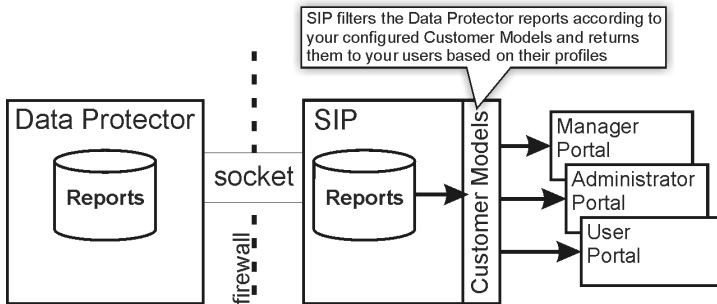
1. You, a user, request a report.
2. The request goes to the Customer Group servlet, which:
 - a. maps you to the groups in your customer profile,
 - b. sends the request to Data Protector’s report database via the socket connection between the SIP portal and Data Protector.



3. Data Protector sends report data via the socket connection to the Docs servlet and/or the Gauges servlet to be formatted.



4. The information is formatted. The final reports and gauges pass through the security filter, and are returned to you.



See the next section for detailed information about how SIP and Data Protector work together.

Related Data Protector integrations

Data Protector also integrates with:

- **HP Operations Manager**, an operations management solution that gives you control over the IT infrastructure. It monitors, controls and reports on network, systems, storage, databases and applications. The integration is covered in two guides:
 - *HP Data Protector integration guide for HP Operations Manager for UNIX*
 - *HP Data Protector integration guide for HP Operations Manager for Windows*
- **HP Reporter**, a management reporting tool that transforms data captured by Operations Manager agents into management information, including real-time and historical availability and performance reports. Reporter can also generate reports on systems managed by HP Operations Manager. After collecting information based on pre-defined and user-specified lists of metrics, Reporter formats the collected data into Web page reports.

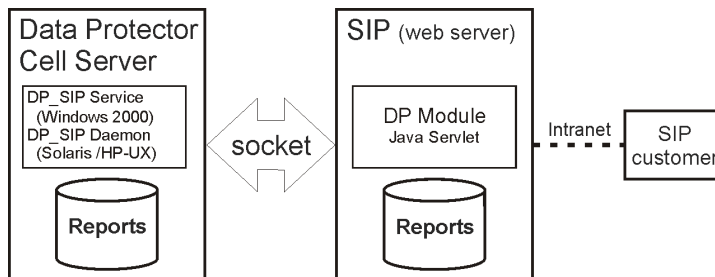
2 Installing the integration

Planning the integration

Before setting up your Data Protector cell manager with SIP, you need to determine which deployment model to use. There are three basic models:

- **Deployment A:** Data Protector and SIP communicate through a socket that runs through a firewall. The SIP portal host may also be exposed through the firewall and accessed by an external customer.

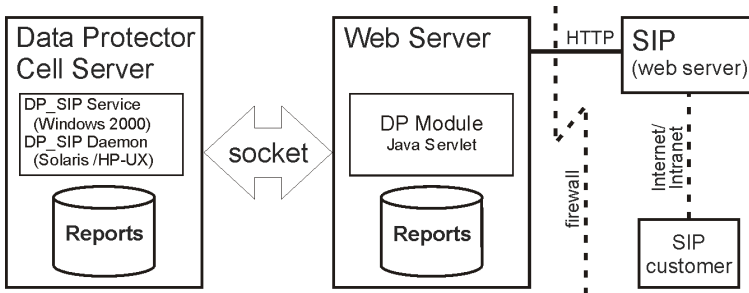
This option is for cases in which all customers are internal. It can be implemented either completely behind a firewall or with access to SIP via port 8080 to a user portal outside the firewall.



In this model, the Data Protector module runs on the SIP server and communicates with the cell manager and intranet users via socket. The SIP portal host may also be exposed through the firewall via the web server's port (8080) and accessed by an external customer.

- **Deployment B:** The Data Protector integration module resides on a web server that communicates with SIP via HTTP through the firewall.

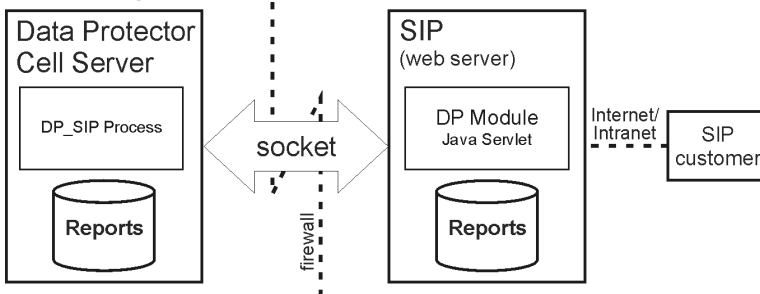
The Data Protector module for SIP is run on a web server within the firewall. This module communicates with SIP remotely through the firewall via HTTP, and communicates with the Data Protector cell manager through sockets completely contained within the firewall.



The benefits of this model are that socket connections are secured and deployment functions are compartmentalized. It does, however, require that you run a separate web server for the Data Protector module.

- **Deployment C:** Data Protector and SIP communicate through a socket completely contained within the firewall.

The Data Protector module for SIP runs on the SIP server outside the corporate firewall. It communicates with the Data Protector cell manager via socket on port 5555 through the firewall.



This model is simple, effective, and accessible to users, but it can be difficult to secure due to the socket connection running through the firewall.

Installing the integration

This section describes how to install the integration modules that let Data Protector and Service Information Portal communicate and work together.

Prerequisites

SIP and Data Protector must already be installed:

- To install SIP, see the *Service Information Portal installation guide*.

- To install Data Protector, see the *HP Data Protector installation and licensing guide*.

Table 2 Software requirements—Data Protector

Operating System	Data Protector Version			
	5.5	6.0	6.1	6.11
HP-UX 11.11	Yes	Yes	Yes	Yes
HP-UX 11.23 IA	Yes	Yes	Yes	Yes
HP-UX 11.23 PA		Yes	Yes	Yes
HP-UX 11.31 IA & PA			Yes	Yes
Solaris 7	Yes	Yes		
Solaris 8	Yes	Yes	Yes	Yes
Solaris 9	Yes	Yes	Yes	Yes
Solaris 10		Yes	Yes	Yes
Microsoft Windows XP Professional (32-bit)	Yes	Yes	Yes	Yes
Microsoft Windows 2000	Yes	Yes	Yes	Yes
Microsoft Windows Server 2003	Yes	Yes	Yes	Yes
SUSE Linux Enterprise Server 9 (32-bit)		Yes		
SUSE Linux Enterprise Server 10 (32-bit)			Yes	Yes
RedHat Enterprise Linux 4.0 (32-bit))			Yes	Yes
RedHat Enterprise Linux 5.0 (32-bit)			Yes	Yes

Table 3 Software requirements—SIP

Operating System	Version
HP-UX 11.11 Windows 2003 (32-bit) Solaris 8 and 9	3.2

Before installing the integration (on any platform or server), ensure you know the following:

- Base language of the SIP server
- Fully qualified path name of each cell manager you want to track
- Fully qualified path name of the SIP server

Dependencies

- Java Developer's Kit 1.4.2 is required for SIP 3.2.
- Some Operations Manager components require Netscape Navigator 4.7 to be installed. This is unnecessary as long as alternative means of browsing HTML pages is available (such as a web browser on a separate machine, or an alternative compatible web browser).
- The environment must be properly set and configured before installing the integration components. This may include patches, environment variables, kernel parameters, and other software components as required. For detailed information about specific requirements, see the installation guides for those components.
- This integration uses Data Protector backup specification groups. See the Data Protector online Help index: "backup specification groups" for more information and how to configure them.

Installing on the Data Protector Cell Server

Data Protector can communicate with SIP without any additional modules. There are no integration-specific installation procedures. However, the Data Protector Administrator must configure backup groups which must then be associated with a SIP role and user.

Establishing Data Protector/SIP Communication

After the installation you must establish communication with the Data Protector server from the SIP side. To do this, associate the Data Protector organizations (imported via the customer model) with Roles. See the *SIP deployment and integration guide* for more information.

Installing on a Windows SIP Server

1. Insert the Data Protector Windows installation DVD.
2. Change directory to `HP_BTO_software_Integrations`.

3. Run `DP-SIP-WIN_A.06.11.exe`.
4. Follow the steps in the Setup Wizard.
5. Import the Customer Model, as described in [“Creating customer models and portal views”](#) on page 37.
6. Create users and user roles, as described in the *SIP deployment and integration guide*.
7. Customize `ConfigSpec.xml` (see [“Editing ConfigSpec.xml”](#) on page 33).

Installing on an HP-UX SIP server

1. Insert the Data Protector HP-UX installation DVD.
2. As root, use `swinstall` to install the following depot:
`DP-SIP-HPUX_A.06.11.depot`
3. Select and install all the components.
4. When the installation is complete, run the following setup script:
`/opt/OV/SIP/dp_setup.sh`
Follow the on-screen instructions. At the end of Data Protector Management Server list, enter `q` or `Q` to quit.
5. Import the Customer Model, as described in [“Creating customer models and portal views”](#) on page 37.
6. Create users and user roles, as described in the *SIP deployment and integration guide*.
7. Customize `ConfigSpec.xml` (see [“Editing ConfigSpec.xml”](#) on page 33).
8. Customize the communication between the web server (Apache) and the servlet container (TOMCAT) as follows:
 1. Edit the file `APACHE_HOME/apache/conf/jk.conf`
 2. For SIP 3.1: Find the line:
`JkMount /ovportal/* ajp12`
 3. For SIP 3.1: Add the following lines:
`JkMount /dpreporter/* ajp12 JkMount /dpreporter ajp12`
 4. Stop and restart Apache and TOMCAT.

Installing on a Solaris SIP server

1. Insert the Data Protector Solaris installation DVD.
2. As root, use `pkgadd` to install the following depot:
`DP-SIP-SUN_A.06.11.pkg`
3. Select and install all the components.
4. When the installation is complete, run the following setup script:
`/opt/OV/SIP/dp_setup.sh`
Follow the on-screen instructions. At the end of Data Protector Management Server list, enter `q` or `Q` to quit.
5. Import the Customer Model, as described in [“Creating customer models and portal views”](#) on page 37.
6. Create users and user roles, as described in the *SIP deployment and integration guide*.
7. Customize `ConfigSpec.xml` (see [“Editing ConfigSpec.xml”](#) on page 33).
8. Customize the communication between the web server (Apache) and the servlet container (TOMCAT) as follows:
 1. Edit the file `/opt/OV/SIP/apache/conf/jk.conf`
 2. For SIP 3.1: Find the line:
`JkMount /ovportal/* ajp12`
 3. For SIP 3.1: Add the following lines:
`JkMount /dpreporter/* ajp12 JkMount /dpreporter ajp12`
 4. Stop and restart Apache and TOMCAT.

Installing on a web server

To install the Data Protector integration servlets on a web server, follow the steps in this section appropriate for the operating system of the server.

If you install this integration on a web server, only the Java servlets are installed on that server. The other components must be installed subsequently on the SIP server.

 **NOTE:**

If you have chosen this installation option, it is assumed that you have IIS with TOMCAT running on Windows and Apache with TOMCAT running on HP-UX. You are responsible for configuring the application server that hosts these servlets. The servlets must be directly accessible via <http://hostname/servlet> and *not* via a specified port (<http://hostname:8080/servlet>).

This may mean that you must perform special configuration steps for your application server and may need to restart both web server and application server. This is not covered in the steps below. Refer to your application server and web server documentation.

Installing on a Windows web server

1. Insert the Data Protector Windows installation DVD.
2. Change directory to `HP_BTO_software_Integrations`.
3. Run `DP-SIP-WIN_A.06.11.exe`.
4. Follow the steps in the Setup Wizard, selecting `SIP Servlet Only`.

On the SIP portal machine, insert the Data Protector Windows installation DVD:

1. Change directory to `HP_BTO_software_Integrations`.
2. Run `DP-SIP-WIN_A.06.11.exe`.
3. Follow the steps in the Setup Wizard, selecting the `SIP Module Component` option.
4. Import the Customer Model, as described in “[Creating customer models and portal views](#)” on page 37.
5. Create users and user roles, as described in the *SIP deployment and integration guide*.
6. Customize `ConfigSpec.xml` (see “[Editing ConfigSpec.xml](#)” on page 33).

Installing on an HP-UX web server

To install the integration on an HP-UX web server:

1. Insert the Data Protector HP-UX installation DVD.

2. As root, use `swinstall` to install the following depot:
`DP-SIP-HPUX_A.06.11.depot`
3. Select and install the `Java Servlets and Setup Scripts` components.
4. When the installation is complete, run the following setup script:
`/opt/OV/SIP/dp_setup.sh`
 Follow the on-screen instructions. At the end of Data Protector Management Server list, enter `q` or `Q` to quit.
5. Customize `ConfigSpec.xml` (see [“Editing ConfigSpec.xml”](#) on page 33).
6. Customize the communication between the web server (Apache) and the servlet container (TOMCAT) by doing the following:
 - a. Edit the file `APACHE_HOME/apache/conf/jk.conf`
 - b. For *SIP 3.1*: Find the line:
`JkMount /ovportal/* ajp12`
 - c. For *SIP 3.1*: Add the following lines:
`JkMount /dpreporter/* ajp12`
`JkMount /dpreporter ajp12`
 - d. Stop and restart Apache and TOMCAT.

On the SIP portal machine, insert the Data Protector HP-UX DVD:

1. As root, use `swinstall` to install the following depot:
`DP-SIP-HPUX.depot`
2. Select and install the `HP-UX SIP` component.
3. Import the Customer Model, as described in [“Creating customer models and portal views”](#) on page 37.
4. Create users and user roles, as described in the *SIP deployment and integration guide*.

Installing on a Solaris web server

To install the integration on a Solaris web server:

1. Insert the Data Protector Solaris installation DVD.

2. As root, use `pkgadd` to install the following depot:
`DP-SIP-SUN_A.06.11.pkg`
3. Select and install the `Java Servlets and Setup Scripts` components.
4. When the installation is complete, run the following setup script:
`/opt/OV/SIP/dp_setup.sh`
 Follow the on-screen instructions. At the end of Data Protector Management Server list, enter `q` or `Q` to quit.
5. Customize `ConfigSpec.xml` (see “[Editing ConfigSpec.xml](#)” on page 33).
6. Customize the communication between the web server (Apache) and the servlet container (TOMCAT) by doing the following:
 - a. Edit the file `APACHE_HOME/apache/conf/jk.conf`
 - b. For *SIP 3.1*: Find the line:
`JkMount /ovportal/* ajp12`
 - c. For *SIP 3.1*: Add the following lines:
`JkMount /dpreporter/* ajp12`
`JkMount /dpreporter ajp12`
 - d. Stop and restart Apache and TOMCAT.

On the SIP portal machine, insert the Data Protector Solaris DVD:

1. As root, use `pkgadd` to install the following depot:
`DP-SIP-SUN_A.06.11.pkg`
2. Select and install the `Solaris SIP` component.
3. Import the Customer Model, as described in “[Creating customer models and portal views](#)” on page 37.
4. Create users and user roles, as described in the *SIP deployment and integration guide*.

3 Customizing the integration

Setting up backup groups on Data Protector

To receive reports via SIP, set up appropriate backup groups on Data Protector. These groups are mapped to Organizations within SIP, which then maps those Organizations to Roles, and Roles to users, as shown in [Figure 1](#). For more information about configuring groups, see the Data Protector online Help index: “backup specification groups”.

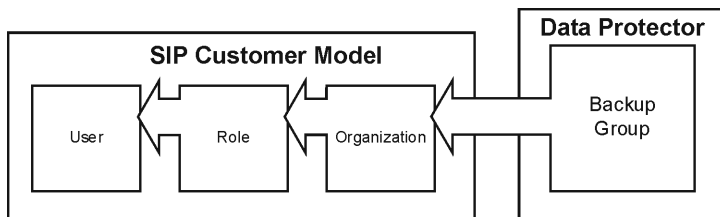


Figure 1 Backup group mappings

ⓘ **IMPORTANT:**

Backup specification group names must *not* include periods (.) or question marks (?).

If you define a role containing overlapping backup groups, users with that role will see redundant data in their reports.

Editing ConfigSpec.xml

There are several options for customizing your integration in the file `ConfigSpec.xml`, located in `$SIP_HOME/webapps/dpsip` (for servlets installed on the SIP server) or `$TOMCAT_Home/webapps/dpsip` directory (for servlets installed on a web server). The following sections describe these options.

Log Location, Log Level

Log Level determines the level at which events will be logged (1–5).

Log Location specifies the name and location of your log file. You must specify an existing directory.

Syntax:

```
<LogLoc logLevel = "x">qualified_path/log_file_name</LogLoc>
```

Example: The log level is 3, so events with a severity of 3, 2, or 1 will be logged. The log file msgtxt is located in the directory d:/tmp/logging/:

```
<LogLoc logLevel = "3">d:/tmp/logging/msgtxt</LogLoc>
```

Filter Level

Determines which types of messages are delivered. Set each message type as true (delivered) or false (not delivered).

Example: Messages tagged Major and Critical are delivered; those tagged Minor and Warning are not:

```
<FilterLevel Warning = "false" Minor = "false" Major = "true"
Critical = "true"/>
```



NOTE:

Message filters in `ConfigSpec.xml` apply at system level. Any message levels filtered out here will not be logged to your SIP or web server.

Refresh Rate

By default, Data Protector refreshes reports when SIP requests a report from the servlet (which happens every time a user logs on). You can set the refresh rate so that reports refresh automatically at specified intervals. In this case, reports are gathered at each refresh interval and are archived on the system. This is a universal parameter, so setting a value will cause all reports to refresh and expire at the specified rate.

To set the refresh rate, edit the line:

```
<RefreshRate update_rate = "time" archive_rate = "time"
file_loc = "path"/>
```

- `update_rate` is the refresh rate in minutes. Avoid values <10.
- `archive_rate` is the rate at which archived reports expire from the system, that is, the time in minutes that a recently accessed report will be maintained on the system. The recommended minimum is five minutes. `Archive_rate` should be greater than `update_rate`.
- `file_loc` is the location of the files gathered and archived to support `RefreshRate`. Enter a valid, existing directory. This repository may need to be very large if you expect many users to log on at the same time.

Example: The refresh rate for updates is set to ten minutes and the archive rate for archived reports is set to thirty minutes.

```
<RefreshRate update_rate = "10" archive_rate = "30" file_loc
= "d:/tmp/" />
```

Gauge Settings

System gauges display Data Protector system health graphically using a gauge with three ranges: green, yellow, and red, indicating the protection status.

You can change the default settings to reflect the sensitivity of your data or the critical nature of systems you are backing up.

To set the gauges, edit the line:

```
<BackupGauge green_band = "range" yellow_band = "range"
red_band = "range" />
```

Example:

```
<BackupGauge green_band = "0-60" yellow_band = "60-80"
red_band = "80-100" />
```

Do not allow color bands to overlap. If you change green to 0-70, you must also change the lower value of yellow to 70.

NOTE:

Gauge settings in `ConfigSpec.xml` are applied to your entire system. If you want some settings to be specific to a given module view, see [“Editing the Data Protector protection status module”](#) on page 44. You can still change the bands for each gauge that you create.

Cell Manager Setting

The `CellServer` variable provides the integration with information about your Cell Managers, including language, port number, and Java user password. If the Data Protector Administrator has changed either the Data Protector port or added a password for a Java user, edit this variable so that the integration servlets can communicate with Data Protector.

To identify a cell manager, edit the line:

```
<CellServer locale = "language" port = "xxxx" password =  
"pwd">host_name</CellServer>
```

where:

- *locale*: the language of the cell manager. Required.
- *port*: the port the integration uses to communicate with the cell manager. *Default*: 5555
- *password*: optional. Only needed if the Data Protector Administrator wants to create a Java user account. *Default*: none
- *host_name*: identifies the cell manager using a fully qualified host name or IP address. Required.

NOTE:

If you edit the cell manager setting directly, you must verify the cell manager is visible to the Data Protector/SIP integration. Ping the fully qualified host name or IP address to make sure the integration can resolve the host name and find the cell manager.

Example: `cellserver_1.example.com` has English as its language, uses port 5555, and has a password of `pwd`:

```
<CellServer locale = "english" port = "5555" password =  
"pwd">cellserver_1.example.com</CellServer>
```

4 Creating customer models and portal views

When you have set up a communications socket between SIP and Data Protector, you can set up your customer models and configure SIP to display custom portal views for each customer group.

This chapter discusses:

- [Customer models](#), page 37: the concept and how they are used within Data Protector and SIP.
- [Management data filter](#), page 38: how it is used to serve appropriate information to users.
- [Adding and removing services in a portal view](#), page 39: how to configure Data Protector services for display within a SIP portal view.

For more information, see the *SIP deployment and integration guide*.

Customer models

To help you present the correct information to your users, SIP employs an expandable concept of customer models. With these, you can create and fine-tune different portals for users according to the department they work in, their job functions, security considerations, and so on.

To generate reports properly, each cell manager is used to create a basic organization named `group@cellserver` where the host is specified. Detailed instructions for segmenting data and creating customer models are in the *SIP deployment and integration guide*.

A customer model maps users to different hosts, interfaces, and services.

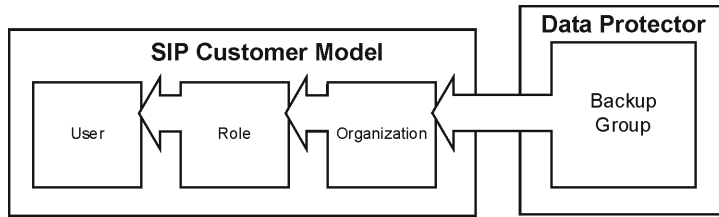


Figure 2 Customer model

Importing the customer model

Import the customer model from the SIP servlet as follows:

1. Log in to SIP as `admin`.
2. Navigate to the **Customer Model** tab.
3. Scroll to the **Customer Model Sources** section.
4. In the **New Customer Model Source URL** field enter:

```
http://servlet_host.com/dpreporter/customer
```

where `servlet_host.com` is the fully qualified host name of the web server on which the servlets are installed.

5. Click **Add**.
6. Click **Apply** at the bottom of the page.

Management data filter

After SIP receives reports from Data Protector, it passes them through management data filtering.

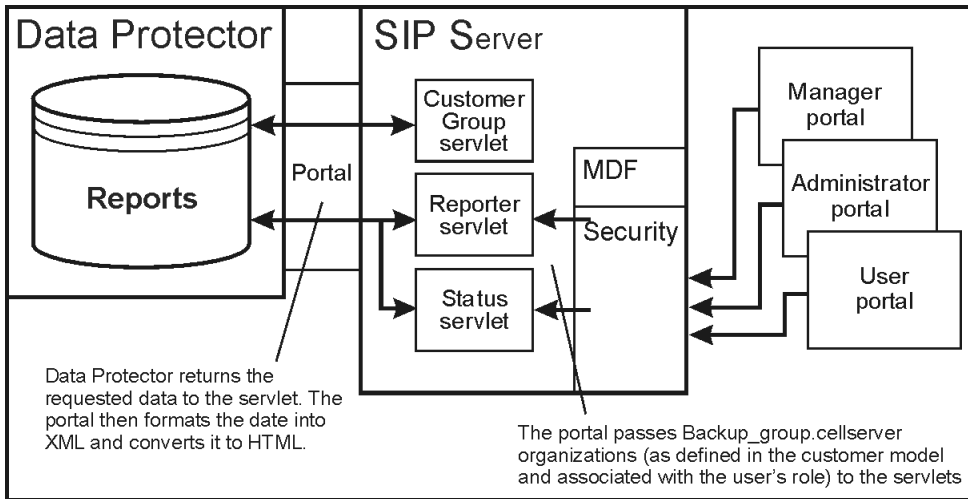


Figure 3 Management data filter overview

Customers are mapped to a user and the user is mapped to a role. The role has organization information that maps a backup group to a cell manager, and can include multiple organizations.

Filtering uses organizations to return only report data applicable to the customer.

For more details of SIP's filtering process, see the *SIP deployment and integration guide*.

Adding and removing services in a portal view

To add a Data Protector module to a portal view:

1. Access the portal view by logging on to SIP as a user with access to the appropriate role. If this user has access to multiple roles, switch to a role with ViewAdmin editing permissions.
2. Navigate to the **Storage** tab.
3. At the bottom of either wide column, either:
 - Select a Data Protector module from the **Select Module to Add** list box, and click **Add**, or
 - Click **Edit** to access the **Modify Column** page. Insert the Data Protector module and place it in the desired location among other modules in the column. Click **OK** to save the changes and return to the main portal page.

A copy of the default version of the Data Protector module is inserted into your `PortalView.xml` file and displayed in the portal view. To edit the modules, see [“Data Protector error messages module”](#) on page 49, [“Data Protector protection status module”](#) on page 41, or [“Data Protector reports module”](#) on page 45.

5 Modules

Data Protector protection status module

This section provides an overview of what Protection Status gauges are and how to configure and use them.

The Data Protector Protection Status module displays a visual representation of the success rates of your backups.

The module has two components: Protection Status gauge and Host Statistics report.

Gauges appear when the tab first displays in your portal. They indicate the overall health rating for services monitored by each gauge. View details by clicking on a gauge or a health title link.



Data Protector protection status gauge

The Data Protector Protection Status gauge shows the status of the backup statistics for all organizations associated with the current role. This is calculated by averaging information from all the organizations.



All Hosts Backup Statistics report


Click a Protection Status Gauge on the main portal window to see the All Hosts Backup Statistics report, a detailed listing of information about your system's protection status.

All Hosts Backup Statistics over the last 30 days							
Client Host	User Group	% Success	Data Written	# Completed Objects	# Failed Objects	# Running DA	# Pending Objects
da-an.cnd.hp.com	one	 100.00%	0.381627	16	0	0	0
da-an.cnd.hp.com	two	 100.00%	3.220528	4	0	0	0

Client Host	Name of the cell manager
User Group	Name of the customer group
% Success	Percentage of successful backup requests. The number in this field is expandable. See “Detail view” on page 44 for details.
Data Written	Amount of backup data written (gigabytes)
# Completed Objects	Number of completed backup jobs
# Failed Objects	Number of failed backup jobs
# Running DA	Number of disk agents currently running
# Pending Objects	Number of pending backup jobs

Client Host Backup report

Click on the % **Success** field in the **All Hosts Backup Statistics** page to see the Client Host Backup Report, an expanded detail view of the protection status for the selected customer group on the cell manager.




Client Host Backup over the last 30 days	
Details : da-an.cnd.hp.com	
Group	one
% Success	100.00% 
Data Written	38 GB
# Files	22042
# Backup Objects	16
# Completed Objects	16
# Failed Objects	0
# Running DA	0
# Pending Objects	0

Details:	Name of the cell manager to which the report applies
Group	Name of the customer group

% Success	Percentage of successful backup requests. The number in this field is expandable. See “ Detail view ” on page 44 for details.
Data Written	Amount of backup data written
# Files	Number of files backed up
# Backup Objects	Number of objects backed up. A backup object is any data selected for a backup, such as a disk, a file, a directory, a database, or a part of the database.
# Completed Jobs	Number of completed backup jobs
# Failed Objects	Number of failed backup jobs
# Running DA	Number of disk agents currently running
# Pending Objects	Number of pending backup jobs

Host Statistics report

The Host Statistics report provides backup statistics for all hosts associated with the current role.

Data Protector Protection Status	
evaluation copy expires: Mar 1, 2006	
Host Statistics Report	over the last 180.0 days
Client Host	% Success
alder.india.hp.com	100.00% 
fagus.india.hp.com	100.00% 
fagus.india.hp.com	100.00% 

Time Frame	Time frame for which data is collected/displayed (“over the last 30 days” in the example above)
Client Host	Qualified host name of the cell manager
% Success	Percentage of successful backup requests. The number in this field is expandable. See the following section for details.

Detail view


Click on a percentage in the main portal window to see the All Hosts Backup Statistics report, a detailed listing of information about your system's protection status. See "[All Hosts Backup Statistics report](#)" on page 41 for more information.

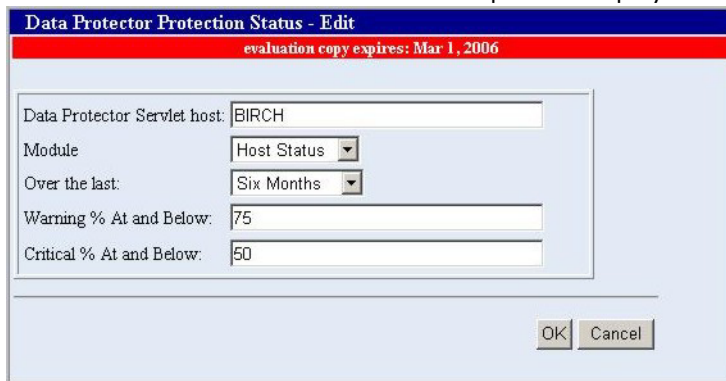
Click on a percentage in the All Hosts Backup Statistics report to display the Client Host Backup Report and a further level of detail. See "[Client Host Backup report](#)" on page 42 for more information.

Editing the Data Protector protection status module

The Protection Status Module provides a gauge or a report that displays information about the overall health of the backup process for all of a customer's groups. Use the **Edit** page to customize the module.

Using the Protection Status—Edit page

To customize the Protection Status module, click on the **Edit** button  in the title bar. The **Data Protector Protection Status - Edit** pane is displayed.



Data Protector Servlet host:	Fully qualified name of the host on which the servlets are running and the port on which the servlets are communicating.
Module	Select the version of the module to display: Status Gauge or Host Status .
Over the last:	Time frame from which to display results.

Warning % At and Below:	Success percentage above which the protection status is considered normal/successful. Status at or below are considered warning.
Critical % At and Below:	Success percentage at or below which the protection status is considered to be critical.

Protection status criteria

Criteria for gauging protection status are pre-configured in this system, so you do not need to configure these gauges. You can, however, configure thresholds for the general protection status, or severity.

Protection status are generally defined as follows:

Normal	Safe health range; severity and incidence of errors is acceptable.
Minor	Although there is probably no imminent danger of data loss from system errors, the administrator should look into the situation.
Critical	Loss of data is probably imminent; the situation should be resolved immediately.

You can change thresholds for these statuses globally based on factors within your unique environment. See “[Editing ConfigSpec.xml](#)” on page 33 for details.

Editing PortalView.xml directly

You can edit `PortalView.xml` file directly. Take care; incorrect editing may cause anomalous results in the integration. See the *SIP deployment and integration guide* for details.

Data Protector reports module

The Reports module provides a variety of information from Data Protector on one or more cell managers in your management domain.

The following reports are pre-configured for SIP:

Data list trees

This basic report has information on all directory trees backed up by the cell manager, but is limited to the directories of the groups associated with the SIP customer. One report is generated per group; customers with multiple groups get multiple reports.

Data Protector Reports				
evaluation copy expires: Mar 1, 2006				
Data List Tree Report				
Backup Specification	Object Type	Client Host	Mountpoint	Tree
New1	Windows FS	fagus.india.hp.com	/C	C:/backup/Backup.4BP
New1	Windows FS	fagus.india.hp.com	/C	C:/backup/MediaDB005.4BK
New1	Windows FS	fagus.india.hp.com	/C	C:/backup/MediaDB005.4BR
New1	Windows FS	fagus.india.hp.com	/C	C:/backup/MediaDB006.4BK
New2	Windows FS	alder.india.hp.com	/C	C:/BuildsNPatches
Test3	Windows FS	fagus.india.hp.com	/C	C:/j2sdk1.4.1_03


Object last backup

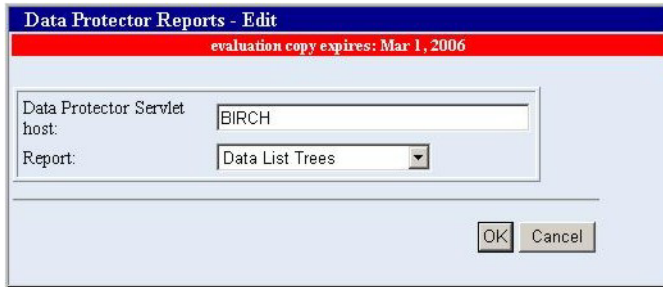
This basic report shows all objects owned by a group and the data of the last full and partial backup for that group. One report is generated per group; customers with multiple groups get multiple reports.

Data Protector Reports						
evaluation copy expires: Mar 1, 2006						
Object Last Backup Report						
Backup Specification	Object Type	Client Host	Mountpoint	Description	Last Full Backup	Last Incremental Backup
New1	Windows FS	fagus.india.hp.com	/C	C:	10/20/05 5:47 PM	-
New2	Windows FS	alder.india.hp.com	/C	C:	8/17/05 9:02 PM	-
Test3	Windows FS	fagus.india.hp.com	/C	C:	10/20/05 5:47 PM	-
filelib	Windows FS	fagus.india.hp.com	/C	C:	10/20/05 5:47 PM	-

Editing the Data Protector reports module

Use the **Edit** page to customize the Reports module:

Click on the **Edit** button  in the title bar. The **Data Protector Reports - Edit** pane is displayed.



Data Protector Servlet host:	Fully qualified name of the host on which the servlets are running and the port on which the servlets are communicating.
Report	Select which report to display, Data List Trees or Object Last Backup.

Editing PortalView.xml directly

You can edit `PortalView.xml` directly. Take care; incorrect editing may cause anomalous results in the integration. See the *SIP deployment and integration guide* for details.

Establishing global settings for reports

For more information about establishing global settings for reports, see “[Editing ConfigSpec.xml](#)” on page 33.


Data Protector backup session list report module


The Backup Session List Report module provides backup session information over a period from Data Protector on one or more cell managers in your management domain. This basic report details all backup sessions associated with backup specifications of groups associated with the SIP customer.

Data Protector Backup Sessions														
evaluation copy expires: Mar 1, 2006														
Session List Report														
Client Host	Backup Specification	Status	Schedule Type	Start Time	End Time	Duration (hours:mins)	Queuing (hours:mins)	GB Written	# Media	# Errors	# Warnings	# Files	% Success	Session ID
fagus.india.hp.com	New1	Completed	Full	8/8/05 11:11 AM	8/8/05 11:18 AM	0:6	0:0	0.854710	1	0	0	57	100.0	2005/08/08-6
fagus.india.hp.com	New1	Completed	Full	8/8/05 11:28 AM	8/8/05 11:33 AM	0:5	0:0	0.216846	1	0	1	273	100.0	2005/08/08-8
fagus.india.hp.com	New1	Completed	Full	8/17/05 7:36 PM	8/17/05 7:41 PM	0:5	0:0	0.216846	1	0	0	273	100.0	2005/08/17-2
fagus.india.hp.com	New1	Completed	Full	8/17/05 9:02 PM	8/17/05 9:02 PM	0:0	0:0	0.021723	1	0	0	2	100.0	2005/08/17-3
fagus.india.hp.com	New1	Completed	Full	8/17/05 9:04 PM	8/17/05 9:04 PM	0:0	0:0	0.032687	1	0	0	4	100.0	2005/08/17-4
fagus.india.hp.com	New1	Completed	Full	8/17/05	8/17/05	0:0	0:0	0.032687	1	0	0	4	100.0	2005/08/17-

Editing the Data Protector backup session list report module

Use the **Edit** page to customize the Backup Session List Report module:

Click on the **Edit** button  in the title bar. The **Data Protector Backup Sessions - Edit** pane is displayed.

Data Protector Backup Sessions - Edit	
evaluation copy expires: Mar 1, 2006	
Data Protector Servlet host:	<input type="text" value="BIRCH"/>
Over the last:	<input type="text" value="Six Months"/> 
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Editing PortalView.xml directly


You can edit `PortalView.xml` directly. Take care; incorrect editing may cause anomalous results in the integration. See the *SIP deployment and integration guide* for details.

Establishing global settings for reports

For more information about establishing global settings for reports, see ["Editing ConfigSpec.xml"](#) on page 33.

Data Protector error messages module

The Messages module presents backup and recovery process messages from Data Protector running on one or more Data Protector stations within your management domain. The module displays changes each time the portal view is displayed or refreshed. The message lists are continually updated in SIP memory.

Data Protector Error Messages				
evaluation copy expires: Mar 1, 2006				
Report Messages other than Normal [Common]			Number of Messages: 1	
	BMA@alder.india.hp.com	8/8/05 11:15 AM	HP:Ultrium 1-SCSI_1_alder	Physical position of the last segment is not consistent with the position information from the database. Instead of expected last segment number 4, last segment on the tape is 6.
12/15/05 12:40 PM				
No backup messages were found matching either your group or the timeframe.				

The module provides access to the following messages from your SIP portal:

- Alarm
- Backup error
- Database corrupted
- Database purge needed
- Database space low
- Device error
- End of session
- Health check failed
- License will expire
- Mail slots full
- Mount request
- Not enough free media
- Unexpected events

For more information on these messages and how to configure them, see Data Protector online Help index: "notifications/types".


Adding a Data Protector error message module to your portal view—GUI

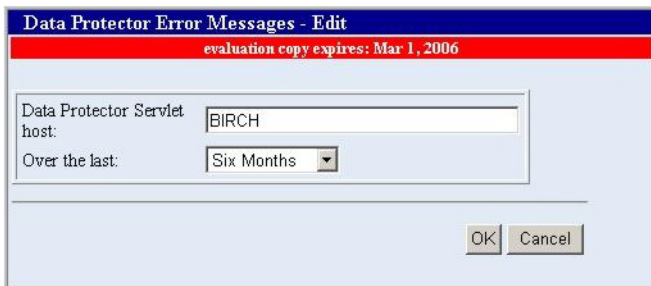
To add a Data Protector message module to a SIP portal:

1. Access the portal view by logging on to SIP as a user with access to the appropriate role. If this user has access to multiple roles, switch to one with ViewAdmin editing permissions.
2. Navigate to the **Storage** tab.
3. At the bottom of the right column, either:
 - Select **Data Protector Error Messages** from the **Select Module to Add** list box, and click **Add**, or
 - Click **Edit** to access the **Modify Column** page. Choose `Data Protector Error Messages` from the list of **Available Modules** and place it in the desired location among other modules in the column. Click **OK** to save the changes and return to the main portal page.
4. If the module displays no messages, click on the **Edit** button on the upper right corner of the module and configure the module to point to the correct servlet for a suitable timeframe.

Editing the Data Protector message module

To modify the Message module in your SIP portal:

1. Access the portal view by logging on to SIP as a user with access to the appropriate role. If this user has access to multiple roles, switch to one with ViewAdmin editing permissions.
2. Navigate to the **Storage** tab.
3. Scroll to the Error Message module you want to edit.
4. Click on the **Edit** button  in the title bar. The **Data Protector Error Messages - Edit** pane is displayed.



- From the `Over the last:` menu, choose a timeframe.
- In the **Data Protector Servlet host:** field, enter the qualified host name and port of the appropriate servlet.

5. Click **OK** to apply the changes and return to the main portal view.

Editing PortalView.xml directly

You can edit `PortalView.xml` directly. Take care; incorrect editing may cause anomalous results in the integration. See the *SIP deployment and integration guide* for details.

Establishing Global Settings for Reports

For more information about establishing global settings for reports, see “[Editing ConfigSpec.xml](#)” on page 33.

6 Uninstalling the integration

Uninstall the SIP integration as follows:

1. Remove the Data Protector Organization.
 - a. Start the SIP Configuration Editor:
 - *On Windows:* **Start: Programs -> HP OpenView -> Service Information Portal -> Configuration Editor** (or from a command prompt, type: `SIP-Config`).
 - *On UNIX:* `/opt/OV/SIP/bin/SIPConfig`
 - b. Under **UserRole Packages**, remove the DP organization from the management data, roles and users.
2. Delete the imported customer model.
 - a. Log in to SIP as `admin`.
 - b. Navigate to the **Customer Model** tab.
 - c. Scroll to the **Customer Model Sources** section.
 - d. Select the url:
`http://servlet_host.com/dpreporter/customer`
where `servlet_host.com` is the fully qualified host name of the web server on which the servlets are installed.
 - e. From the customer model sources textbox, click **Delete**.
 - f. Click **Apply** at the bottom of the page.
3. Uninstall the Data Protector integration.
 - On Windows:
Go to **Control panel -> Add and Remove Programs -> Data Protector-SIPIntegration -> Remove**
 - On HPUX:
Use `swremove` to uninstall the integration:
 - If the Web server and SIP server are on the same machine:
`swremove DP-SIP DP-SIP-Servlets DP-SIP-Setup`

- If the Web server and SIP server are on different machines:
on the Web server: `swremove DP-SIP-Servlets DP-SIP-Setup`
on the SIP server: `swremove DP-SIP`
- On Solaris:
Use `pkgrm` to uninstall the integration:
 - If the Web server and SIP server are on the same machine:
`pkgrm HPDPsip DPSIPServ HPDPsetup`
 - If the Web server and SIP server are on different machines:
on the Web server: `pkgrm DPSIPServ HPDPsetup`
on the SIP server: `pkgrm HPDPsip`

7 Troubleshooting

Error messages

Data unavailable

If this message appears after adding a module while viewing reports, you are missing either a valid servlet host or data within the specified timeframe.

Check the following in the `ConfigSpec.xml` file, located in `$SIP_HOME/webapps/dpsip` (for servlets installed on the SIP server) or `$TOMCAT_Home/webapps/dpsip` directory (for servlets installed on a web server):

- The hostname (including port number) is valid.
- The set timeframe is large enough to be likely to contain data.

Parse rest of config

If you receive the Java exception message *Exception: parse Rest of Config*, the log directory may not have been installed correctly. Verify that the log directory is present at the location specified in the `ConfigSpec.xml` file, and that read/write access for the directory is set to `all`.

Index

A

All Hosts Backup Statistics report, [41](#)
Apache, [29](#)
audience, [9](#)

B

backup groups, setting up on Data Protector, [33](#)

C

cell manager settings, [36](#)
Cell Request Server, [21](#)
Client Host Backup report, [42](#)
ConfigSpec.xml, editing, [33](#)
conventions
 document, [16](#)
CRS, [21](#)
customer models, [37](#)
 importing, [38](#)
customizing
 Data Protector-SIP integration, [33](#)
 reports module, [46](#)

D

Data List Trees report, [46](#)

Data Protector, [19](#), [20](#)

 error messages, [49](#)
 integration with SIP, [21](#)
 OM integration, [22](#)
 reports, [45](#)
 SIP integration, [19](#)
 versions, [25](#)

Data Protector Integration module, [20](#)

Data Protector-SIP

 backup groups, [33](#)
 cell manager settings, [36](#)
 ConfigSpec.xml, editing, [33](#)
 customizing, [33](#)
 filter level, [34](#)
 gauge settings, [35](#)
 logging, [34](#)
 refresh rate, [34](#)

Data Protector-SIP integration
installing,
customer models, 37
deployments, 23
installing on a Solaris SIP server, 28
installing on a Solaris web server,
30
installing on a web server, 28
installing on a Windows SIP server,
26
installing on a Windows web server,
29
installing on an HP-UX SIP server, 27
installing on an HP-UX web server,
29
installing on the Data Protector
server, 26
management data filter, 38
portal view services, 39
portal views, 37
protection status gauges, 41
protection status module, 41
uninstalling, 53

document
conventions, 16
related documentation, 9
documentation
HP website, 9
providing feedback, 18

E

editing reports module, 46
error messages, 55
module, 49

F

filter level, 34

G

gauge settings, 35

gauges, protection status, 41

H

help
obtaining, 17
Hosts Statistics report, 43
HP
technical support, 17

I

IIS, 29
installing Data Protector-SIP integration,
24
on a Solaris SIP server, 28
on a Solaris web server, 30
on a web server, 28
on a Windows SIP server, 26
on a Windows web server, 29
on an HP-UX SIP server, 27
on an HP-UX web server, 29
on the Data Protector server, 26

J

Java Developer's Kit, 26

L

logging, 34

M

management data filter, 38

N

Netscape Navigator, 26

O

Object Last Backup report, 46

P

- planning Data Protector-SIP integration, [23](#)
- portal view services, [39](#)
- portal views, [37](#)
- PortalView.xml, editing, [47](#)
- protection status
 - gauges, [41](#)
 - module, [41](#), [44](#)
- protection status criteria, [45](#)

R

- refresh rate, [34](#)
- related documentation, [9](#)
- reports, [45](#)
 - All Hosts Backup Statistics, [41](#)
 - Client Host Backup, [42](#)
 - customizing reports module, [46](#)
 - Data List Trees, [46](#)
 - global settings, [47](#)
 - Host Statistics, [43](#)
 - module, [45](#)
 - Object Last Backup Up, [46](#)
- requirements, [25](#)

S

- Service Level Management, [20](#)
- SIP, [19](#), [20](#)
 - versions, [25](#)
- SLM, [19](#), [20](#)
- software requirements, [25](#)
- status gauges, [21](#)
- Subscriber's Choice, HP, [17](#)

T

- technical support
 - HP, [17](#)
 - service locator website, [17](#)
- TOMCAT, [29](#)
- troubleshooting, [55](#)

U

- uninstalling
 - Data Protector-SIP integration, [53](#)

W

- websites
 - HP, [17](#)
 - HP Subscriber's Choice for Business, [17](#)
 - product manuals, [9](#)

