

# **HP OpenView Storage Data Protector**

## **Integration Guide**

### **for**

# **HP OpenView Service Information Portal**

**Version: A.02.01**

**HP-UX, Solaris and Windows**



**Manufacturing Part Number: None (PDF-only)**

**July 2003**

© Copyright 2002-2003 Hewlett-Packard Development Company, L.P.

---

## Legal Notices

### **Warranty.**

*Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.*

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

### **Restricted Rights Legend.**

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company  
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

### **Copyright Notices.**

©Copyright 2002-2003 Hewlett-Packard Development Company, L.P.

No part of this document may be copied, reproduced, or translated to another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

©Copyright 1979, 1980, 1983, 1985-93 Regents of the University of California

This software is based in part on the Fourth Berkeley Software Distribution under license from the Regents of the University of California.

©Copyright 1986-1992 Sun Microsystems, Inc.

©Copyright 1985-86, 1988 Massachusetts Institute of Technology

©Copyright 1989-93 The Open Software Foundation, Inc.

©Copyright 1986-1997 FTP Software, Inc. All rights reserved

©Copyright 1986 Digital Equipment Corporation

©Copyright 1990 Motorola, Inc.

©Copyright 1990, 1991, 1992 Cornell University

©Copyright 1989-1991 The University of Maryland

©Copyright 1988 Carnegie Mellon University

©Copyright 1991-1995 by Stichting Mathematisch Centrum,  
Amsterdam, The Netherlands

©Copyright 1999, 2000 Bo Branten

**Trademark Notices.**

Reproduction, adaptation, or translation of this document without prior written permission is prohibited, except as allowed under the copyright laws.

Adobe® is a trademark of Adobe Systems Incorporated.

HP-UX Release 10.20, HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Oracle® is a registered U.S. trademarks of Oracle Corporation, Redwood City, California.

UNIX® is a registered trademark of The Open Group. .

Windows NT™ is a U.S. trademark of Microsoft Corporation. Microsoft®, MS-DOS®, Windows® and MS Windows® are U.S. registered trademarks of Microsoft Corporation.



**1. Introduction**

Overview .....	22
Data Protector .....	22
OpenView Products Integrated with Data Protector .....	22
OpenView Service Information Portal .....	22
OpenView Operations .....	22
Service Level Management Integrations .....	23
Data Protector-SIP .....	23
Data Protector-OVO-SIP .....	23

**2. Data Protector-SIP Integration**

Introduction .....	26
Prerequisites .....	26
Product Capabilities and Integration Benefits .....	26
Component List .....	27
Dependencies .....	27
Data Protector/SIP Integration .....	28
Data Protector Integration Module .....	29
Cell Request Server (CRS) .....	29
How Data Protector Integrates with SIP .....	29
Deployments .....	31
Deployment A .....	31
Deployment B .....	32
Deployment C .....	33
Setup Process .....	34
Installation Procedures .....	34
Prerequisite Information .....	34
On the Data Protector Server .....	35
Establishing Data Protector/SIP Communication .....	35
Installing on a SIP Server .....	35
Installing on a Windows NT SIP Server .....	35
Installing on a UNIX SIP Server .....	36
Installing on a Web Server .....	37
Installing on a Windows Web Server .....	37
Installing on an UNIX Web Server .....	38
Customization .....	40
Setting Up Backup Groups on Data Protector .....	40
Editing ConfigSpec.xml .....	41

---

# Contents

Creating Customer Models and Portal Views .....	45
Customer Models .....	45
Importing the Customer Model .....	46
Management Data Filter .....	47
Adding and Removing Services in a Portal View .....	48
Error Messages Module .....	49
Understanding Data Protector Error Messages .....	49
Data Protector Error Messages .....	49
Editing Data Protector Message Modules .....	51
Editing the PortalView.XML File Directly .....	51
Protection Status Module .....	52
Understanding the Protection Status Module .....	52
Protection Status Gauge .....	52
All Hosts Backup Statistics Report .....	53
Client Host Backup Report .....	54
Host Statistics Report .....	55
Detail View .....	56
Editing the Backup Health Module .....	57
Using the Backup Health - Edit page .....	57
Backup Health Criteria .....	58
Directly Editing the PortalView.xml File .....	58
Data Protector Reports Module .....	59
Understanding Data Protector Reports .....	59
Data Protector Reports .....	59
Editing the Data Protector Reports Module .....	61
Using the Reports - Edit page .....	61
Directly Editing the PortalView.xml File .....	62
Establishing Global Settings for Reports .....	62
Backup Sessions Module .....	63
Understanding Data Protector Backup Sessions Module .....	63
Setting Up New Data Protector Backup Sessions Modules .....	64
Editing Data Protector Backup Sessions Module .....	65
Internationalization Issues .....	66
Language Support .....	66
Internationalization Issues .....	66
Troubleshooting .....	68
Error Messages .....	68
Data Unavailable .....	68

Parse Rest of Config .....	68
<b>3. Data Protector-OVO-SIP Integration</b>	
Introduction .....	70
Prerequisites .....	70
Product Capabilities and Integration Benefits .....	70
Component List .....	72
Data Mappings .....	73
Dependencies .....	74
Setup Process .....	76
Installation .....	76
Configuration .....	77
Sample Configuration Files .....	78
Editing Configurations .....	78
Configuring the Management Stations .....	78
Updating the Customer Model .....	79
Creating a SIP User/Role Package .....	80
Add Password Authentication (optional) .....	83
Finalize the Configuration .....	85
Troubleshooting .....	88

---

# Contents



---

## Printing History

The manual printing date and part number indicate its current edition. The printing date will change when a new edition is printed. Minor changes may be made at reprint without changing the printing date. The manual part number will change when extensive changes are made.

Manual updates may be issued between editions to correct errors or document product changes. To ensure that you receive the updated or new editions, you should subscribe to the appropriate product support service. See your HP sales representative for details.

**Table 1**

### **Edition History**

<b>Part Number</b>	<b>Manual Edition</b>	<b>Product</b>
B6960-90069	August 2002	HP OpenView Storage Data Protector A.05.00
Not applicable	April 2003	HP OpenView Storage Data Protector A.05.10
	July 2003	HP OpenView Storage Data Protector A.05.10



---

## Conventions

The following typographical conventions are used in this manual.

**Table 2**

<b>Convention</b>	<b>Meaning</b>	<b>Example</b>
<i>Italic</i>	Book or manual titles, and manual page names	Refer to the <i>HP OpenView Storage Data Protector Integration Guide</i> for more information.
	Provides emphasis	You <i>must</i> follow these steps.
	Specifies a variable that you must supply when entering a command	At the prompt type: rlogin <i>your_name</i> where you supply your login name.
<b>Bold</b>	New terms	The Data Protector <b>Cell Manager</b> is the main ...
Computer	Text and items on the computer screen	The system replies: Press Enter
	Command names	Use the grep command ...
	File and directory names	/usr/bin/X11
	Process names	Check to see if Data Protector Inet is running.
	Window/dialog box names	In the Backup Options dialog box...
Computer Bold	Text that you must enter	At the prompt, type: ls -l
<b>Keycap</b>	Keyboard keys	Press <b>Return</b> .



---

## Contact Information

### General Information

General information about Data Protector can be found at

<http://www.hp.com/go/dataprotector>

### Technical Support

Technical support information can be found at the HP Electronic Support Centers at

<http://support.openview.hp.com/support.jsp>

Information about the latest Data Protector patches can be found at

[http://support.openview.hp.com/patches/patch\\_index.jsp](http://support.openview.hp.com/patches/patch_index.jsp)

For information on the Data Protector required patches, see the *HP OpenView Storage Data Protector Software Release Notes*

HP does not support third-party hardware and software. Contact the respective vendor for support.

### Documentation Feedback

Your comments on the documentation help us to understand and meet your needs. You can provide feedback at

[http://ovweb.external.hp.com/lpe/doc\\_serv/](http://ovweb.external.hp.com/lpe/doc_serv/)

### Training Information

For information on currently available HP OpenView training, see the HP OpenView World Wide Web site at

<http://www.openview.hp.com/training/>

Follow the links to obtain information about scheduled classes, training at customer sites, and class registration.



---

# Data Protector Documentation

Data Protector documentation comes in the form of manuals and online Help.

## Manuals

Data Protector manuals are available in printed format and in PDF format. Install the PDF files during the Data Protector setup procedure by selecting the `User Interface` component on Windows or the `OB2-DOCS` component on UNIX. Once installed, the manuals reside in the `\<Data_Protector_home>docs` directory on Windows and on the `/docs/C/` directory on UNIX. You can also find the manuals in PDF format at [http://ovweb.external.hp.com/lpe/doc\\_serv/](http://ovweb.external.hp.com/lpe/doc_serv/)

### ***HP OpenView Storage Data Protector Administrator's Guide***

This manual describes typical configuration and administration tasks performed by a backup administrator, such as device configuration, media management, configuring a backup, and restoring data.

### ***HP OpenView Storage Data Protector Installation and Licensing Guide***

This manual describes how to install the Data Protector software, taking into account the operating system and architecture of your environment. This manual also gives details on how to upgrade Data Protector, as well as how to obtain the proper licenses for your environment.

### ***HP OpenView Storage Data Protector Integration Guide***

This manual describes how to configure and use Data Protector to back up and restore various databases and applications.

There are two versions of this manual:

- *HP OpenView Storage Data Protector Windows Integration Guide*

This manual describes integrations running the Windows operating systems, such as Microsoft Exchange, Microsoft SQL, Oracle, SAP R/3, Informix, Sybase, NetApp Filer, HP OpenView Network Node Manager and Lotus Domino R5 Server.

- *HP OpenView Storage Data Protector UNIX Integration Guide*

This manual describes integrations running on the UNIX operating system, such as: Oracle, SAP R/3, Informix, Sybase, NetApp Filer, HP OpenView Network Node Manager and Lotus Domino R5 Server.

### ***HP OpenView Storage Data Protector Concepts Guide***

This manual describes Data Protector concepts and provides background information on how Data Protector works. It is intended to be used with the task-oriented *HP OpenView Storage Data Protector Administrator's Guide*.

### ***HP OpenView Storage Data Protector EMC Symmetrix Integration Guide***

This manual describes how to install, configure, and use the EMC Symmetrix and EMC Fastrax integrations. It is intended for backup administrators or operators.

- The first part describes the integration of Data Protector with the EMC Symmetrix Remote Data Facility and TimeFinder features for Symmetrix Integrated Cached Disk Arrays. It covers the backup and restore of filesystems and disk images as well as online databases, such as Oracle and SAP R/3.
- The second part describes the integration of Data Protector with the EMC Fastrax. It covers the backup and restore of disk images as well as Oracle8i and SAP R/3 systems, using direct disk to tape technology.

### ***HP OpenView Storage Data Protector HP StorageWorks Disk Array XP Integration Guide***

This manual describes how to install, configure, and use the integration of Data Protector with HP StorageWorks Disk Array XP. It is intended for backup administrators or operators. It covers the backup and restore of Oracle, SAP R/3, Microsoft Exchange, and Microsoft SQL.

### ***HP OpenView Storage Data Protector HP StorageWorks Virtual Array Integration Guide***

This manual describes how to install, configure, and use the integration of Data Protector with HP StorageWorks Virtual Array. It is intended for backup administrators or operators. It covers the backup and restore of Oracle, SAP R/3 and Microsoft Exchange.



***HP OpenView Storage Data Protector Integration Guide for HP OpenView Service Information Portal***

This manual describes how to install, configure, and use the integration of Data Protector with HP OpenView Service Information Portal. It is intended for backup administrators. It discusses how to use the application for Data Protector service management.

***HP OpenView Storage Data Protector Integration Guide for HP OpenView Reporter***

This manual describes how to install, configure, and use the integration of Data Protector with HP OpenView Reporter. It is intended for backup administrators. It discusses how to use the application for Data Protector service management.

***HP OpenView Storage Data Protector Integration Guide for HP OpenView Service Desk***

This manual describes how to install, configure, and use the integration of Data Protector with HP OpenView Service Desk. It is intended for backup administrators. It discusses how to use the application for Data Protector service management.

***HP OpenView Storage Data Protector Software Release Notes***

This document gives a description of new features of HP OpenView Storage Data Protector A.05.10. It also provides information on supported configurations (devices, platforms and online database integrations, SAN configurations, EMC split mirror configurations, and HP StorageWorks XP configurations), required patches, limitations, as well as known problems and workarounds. An updated version of the supported configurations is available at <http://www.openview.hp.com/products/dataprotector/specifications/index.asp>.

**Online Help**

Data Protector provides online Help for Windows and UNIX platforms.



---

## In This Book

The *HP OpenView Storage Data Protector Integration Guide for HP OpenView Reporter* describes how to install, configure, and use the integration of Data Protector with HP OpenView Service Information Portal.

---

### NOTE

This manual describes Data Protector functionality without specific information on particular licensing requirements. Some Data Protector functionality is subject to specific licenses. The related information is covered in the *HP OpenView Storage Data Protector Installation and Licensing Guide*.

---

## Audience

This manual is intended for backup administrators or operators who plan to install and configure the integration of Data Protector with HP OpenView Service Information Portal, HP OpenView Service Desk, and HP OpenView Reporter.

Conceptual information can be found in the *HP OpenView Storage Data Protector Concepts Guide*, which is recommended in order to fully understand the fundamentals and the model of Data Protector.

## Organization

The manual is organized as follows:

- Chapter 1** “Introduction” on page 21.
- Chapter 2** “Data Protector-SIP Integration” on page 25.
- Chapter 3** “Data Protector-OVO-SIP Integration” on page 69.

The integrations of Data Protector with the following database applications are described in the *HP OpenView Storage Data Protector Integration Guide*:

- Microsoft SQL Server 7.0/2000
- Microsoft Exchange
- Microsoft Exchange 2000

The integrations of Data Protector with the following applications is described in the *HP OpenView Storage Data Protector Administrator's Guide*:

- OmniStorage
- Microsoft Cluster Server
- MC/ServiceGuard
- Data Source Integration
- Application Response Measurement
- ManageX

---

# **1 Introduction**

---

## **Overview**

This chapter provides a brief overview of Data Protector, the HP OpenView product integrated with it to create an enterprise-wide solution that provides service level management, and the integration itself.

### **Data Protector**

HP OpenView Storage Data Protector is a backup and recovery solution that provides reliability and protection for your fast growing business data. Data Protector offers comprehensive backup and restore functionality designed specifically for enterprise wide and distributed environments.

Data Protector also provides information that can be used, through reports and messaging tools, to help you monitor the status of your processes, in addition to providing backup and recovery functionality.

### **OpenView Products Integrated with Data Protector**

Data Protector is designed to allow the integration of other HP OpenView products, in order to provide you with an enterprise-wide solution for your IT environment. Integrations with HP OpenView Service Information Portal is described in this manual.

#### **OpenView Service Information Portal**

Service Information Portal (SIP) is a tool that lets you present data from your internal applications such as Data Protector, OVIS, OVR, and OVO as reports on custom web pages for each of your clients.

#### **OpenView Operations**

OpenView Operations is a central management point for various remote OpenView applications. Collects and analyzes data, automates critical response, as well as message forwarding to other services.

## **Service Level Management Integrations**

Data Protector and the HP OpenView products listed above are integrated to create an enterprise-wide solution that provides service level management. The integrations are introduced below:

### **Data Protector-SIP**

The integration of Data Protector with SIP helps you achieve a specific, consistent, measurable level of service by offering pertinent information to backup service managers. This integration provides additional network visibility to Data Protector and allows integration of Data Protector-specific information with other SIP services.

### **Data Protector-OVO-SIP**

The integration of Data Protector with SIP (via OVO) offers pertinent information to the managers of the backup service of a specific group. It provides additional network visibility to Data Protector and allows integration of Data Protector-specific data with other SIP services.





---

## **2 Data Protector-SIP Integration**

## Introduction

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

### Prerequisites

The integration requires the following licensed components:

- Data Protector
- OpenView Service Information Portal

### Product Capabilities and Integration Benefits

The integration of Data Protector and OpenView Service Information Portal helps enable Service Level Management (SLM) to help you achieve a specific, consistent, measurable level of service. In short, this integration helps you achieve maximum service availability by providing a simple, effective way to:

- 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 the 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.

## 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.
- OV SIP (OpenView 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.

## Dependencies

- Sun's Java Developer's Kit 1.3 is required for SIP.
- Some OpenView components require that Netscape Navigator 4.7 be installed. This step is unnecessary and may be skipped as long as alternative means of browsing HTML pages is available (e.g., a web browser on a separate machine, or an alternative compatible web browser).
- Successful configuration must also comply with the software requirements as described in the table below.
- The environment must be properly set and configured prior to the installation of the integration components. This may include patches, environment variables, kernel parameters, and other software components as required. For detailed information about the specific requirements, please refer to the installation guides for those components.
- This integration uses Data Protector backup specification groups. Refer to the *HP OpenView Storage Data Protector Administrator's Guide* and the Data Protector online help for more information about backup specification groups and how to configure them.

**Table 2-1 Software Requirements**

Component	Version	Operating System
Data Protector	5.1	HP-UX 11.0, 11.11 Solaris 8 Windows NT 4.0, Windows 2000
SIP	3.0, 3.1	HP-UX 11.0 Solaris 8 Windows 2000

**Table 2-2 Patch Requirements for SIP 3.0**

Platform	Patch Number	Description
HP-UX	PHSS_28254	SIP Server patch
	PHSS_28268	SIP Topology Module patch
Solaris	OVSIPSOL_00012	SIP Server patch
	OVSIPSOL_00013	SIP Topology Module patch
Windows 2000	OVSIPNT_00011	SIP Server patch
	OVSIPNT_00012	SIP Topology Module patch

## Data Protector/SIP Integration

The Data Protector/SIP integration consists of two major elements:

- The *Data Protector Integration module*, installed on the SIP server or on a separate web server.
- The *Cell Request Server process*, installed on the Data Protector cell server.

These elements are described in detail in the sections that follow.

## Data Protector Integration Module

The Data Protector Integration module components are automatically installed along with SIP, and are located either on your SIP web server or on a separate web server, depending on your deployment.

This integration module consists of two primary elements:

- SIP components, including SIP XML, XSL, and module definitions.
- SIP-Data Protector servlets, including the Java servlets described below, as well as the Configuration Specifications, `ConfigSpec.xml`.

This integration uses three Java servlets to communicate between SIP and Data Protector.

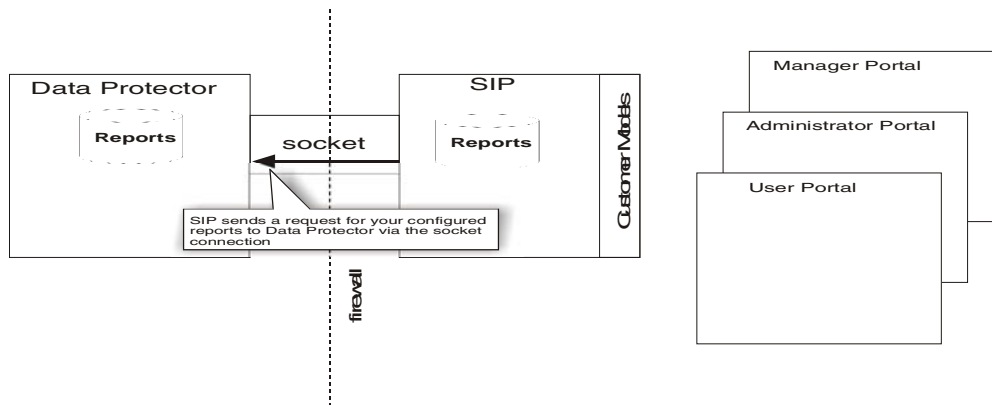
- The `CustomerGroup` servlet provides the customer model to the SIP Management Data Filter.
- The `Reporter` servlet generates and creates XML reports, and also includes a configurable threading option.
- The `StatusGauge` servlet generates status gauges.

## Cell Request Server (CRS)

The other main element of the Data Protector-SIP integration is the Cell Request Server (CRS) process in Data Protector cell server. The CRS serves reports to SIP via the socket. For information on configuring this module, see “Setup Process” on page 34.

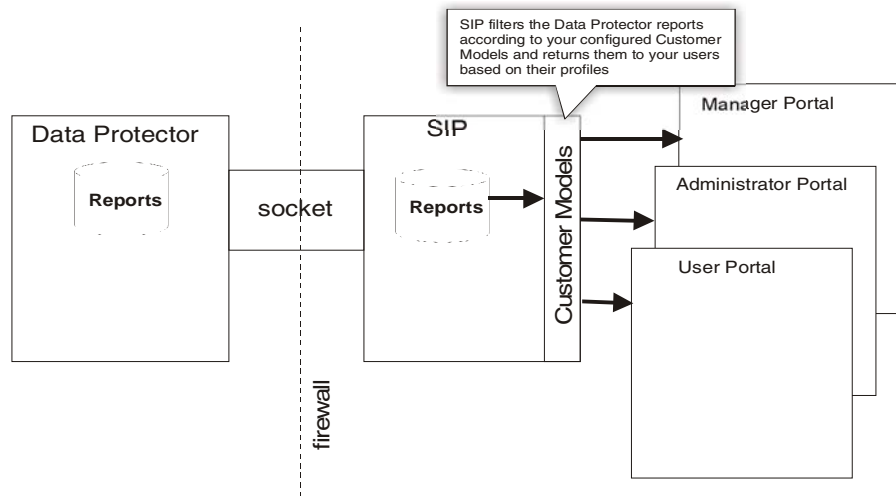
## How Data Protector Integrates with SIP

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



When a user requests a report, as in the illustration above, the request goes to the Customer Group servlet, which then maps that user to the group or groups in his or her customer profile. The Customer Group servlet then sends the request to Data Protector's report database via the socket connection between the SIP portal and Data Protector.

After Data Protector receives the user request for data, it sends report data via the socket connection to the Docs servlet and/or the Gauges servlet to be formatted.



Finally, the information is formatted, then the final reports and gauges pass through the security filter, and are returned to the user who initially requested them.

See “Deployments” on page 31 for more detailed information about how SIP and Data Protector work together.

## Deployments

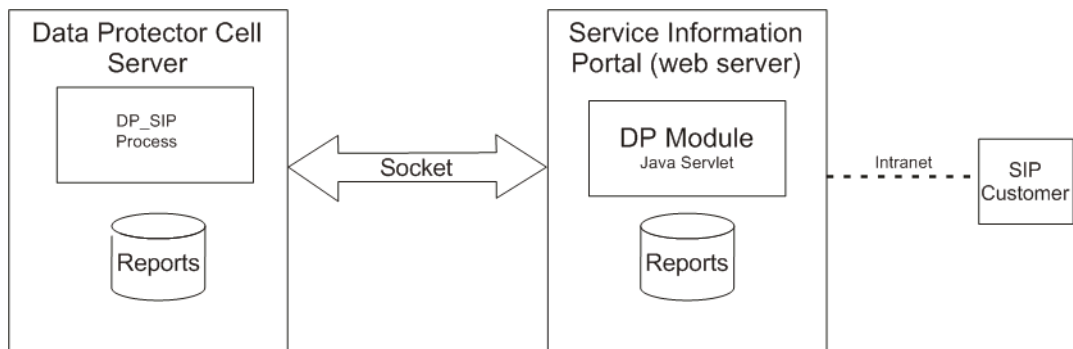
The first step in setting up your Data Protector cell server with SIP is to determine which deployment model to use. There are three basic models you can use to deploy your services, each of which is described in this chapter.

- Deployment A describes a deployment option in which 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.
- Deployment B describes a deployment option in which the Data Protector integration module resides on a web server, which then communicates with SIP via HTTP through the firewall.
- Deployment C describes an option in which Data Protector and SIP communicate through a socket completely contained within the firewall.

### Deployment A

This option can be implemented either completely behind a firewall or with access to SIP via port 8080 to a user portal outside the firewall.

**Figure 2-1**      **Deployment A**

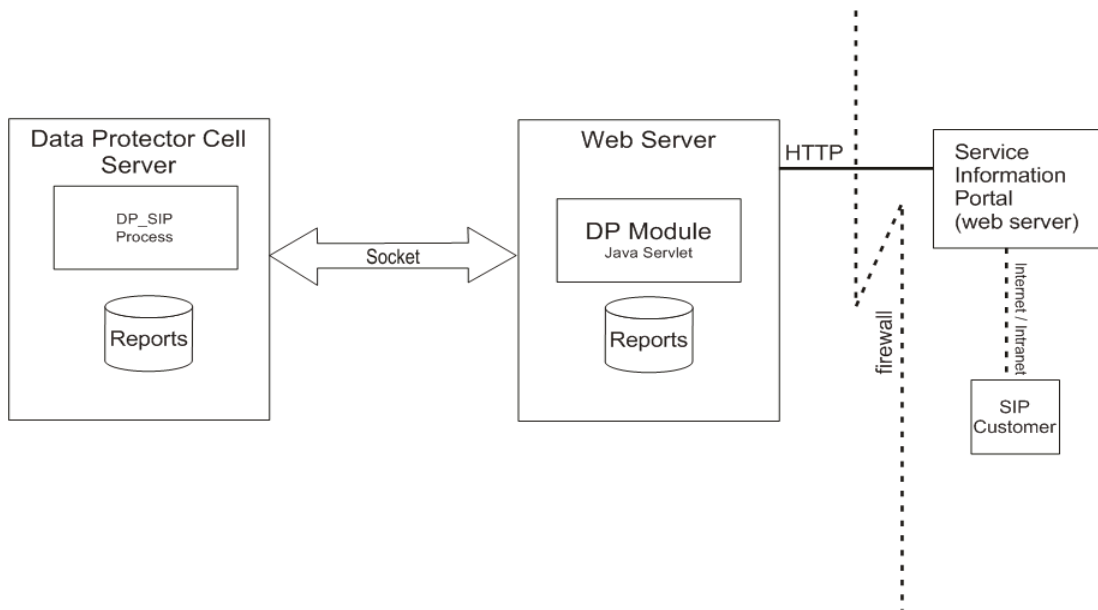


This option is for cases in which all customers are internal. In this model, the Data Protector module runs on the SIP server and communicates with the cell server and intranet users via socket. The SIP portal host may also be exposed through the firewall via the web server's port (i.e., 8080) and accessed by an external customer.

### Deployment B

In this deployment option, 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 server through sockets that are completely contained within the firewall.

Figure 2-2 Deployment B



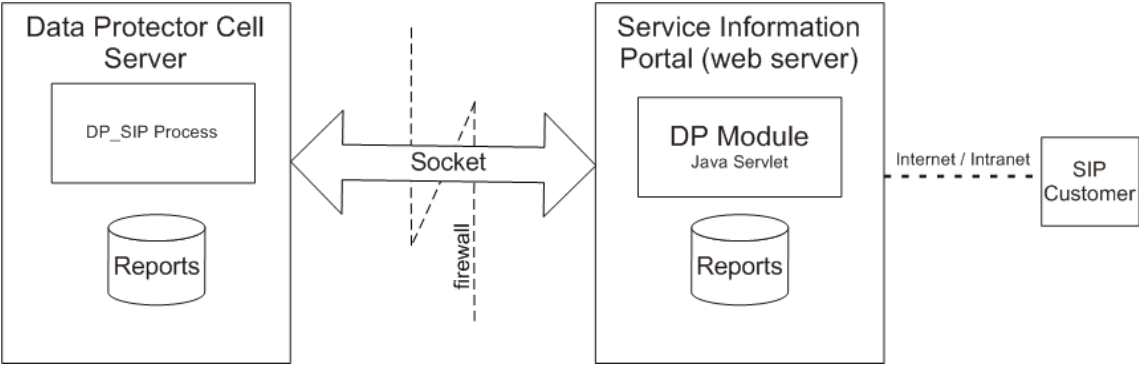
The benefits of this model are that socket connections are secured and deployment functions are compartmentalized. It does, however, require that you run a separate web server for the Data Protector module.



### Deployment C

In this deployment, the Data Protector module for SIP is run on the SIP server, outside of the corporate firewall, and it communicates with the Data Protector cell server via socket on port 5555 through the firewall.

Figure 2-3 Deployment C



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

## Setup Process

This section describes how to install and configure the integration modules that let Data Protector 5.1 and Service Information Portal communicate and work together.

The following sections are included in this chapter:

- Installation Procedures
- Customization

### Installation Procedures

The Data Protector server and the SIP server communicate by way of a socket connection, which provides a dedicated two-way channel through which SIP can request reports from the Data Protector cell server, and Data Protector can send them. See “Deployments” on page 31 for more information on the architecture of a Data Protector-SIP integration.

This section describes the procedures for installing the integration modules that let Data Protector and SIP communicate and work together.

For instructions on installing SIP, refer to the Service Information Portal Installation Guide.

For instructions on installing Data Protector, refer to the *HP OpenView Storage Data Protector Installation and Licensing Guide*.

### Prerequisite Information

Before you begin the installation (on any platform or server), you should be sure that you know the following:

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

## On the Data Protector 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, you must associate the Data Protector organizations (imported via the customer model) with Roles. Refer to the *SIP Deployment and Integration Guide* for more information.

## Installing on a SIP Server

To install the Data Protector integration servlets on a SIP server, follow the steps below. Note that the steps are different depending on the operating system of the server.

### Installing on a Windows NT SIP Server

1. Insert the Data Protector Windows installation CD-ROM.
2. CD to DP\_Service\_Mgmt\_Integr.
3. Run DP-SIP-WIN.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 45
6. Create users and user roles, as described in the *SIP Deployment and Integration Guide*.
7. Customize ConfigSpec.xml as described in “Customization” on page 40.

## Installing on a UNIX SIP Server

1. Insert the Data Protector HP-UX/Solaris installation CD-ROM.
2. On HP-UX:       As root, use `swinstall` to install the following depot:  
  
                  `DP-SIP-HPUX.depot`  
  
On Solaris:       As root, use `pkgadd` to install the following package:  
  
                  `DP-SIP-SUN.pkg`
3. Select and install SIP components, Java Servlets, and Setup Script 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 45
6. Create users and user roles, as described in the *SIP Deployment and Integration Guide*.
7. Customize `ConfigSpec.xml` as described in “Customization” on page 40.
8. 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. Find the line:  
  
          `JkMount /ovportal/* ajp12`
  - c. Add the following lines:  
  
          `JkMount /dpreporter/* ajp12`  
  
          `JkMount /dpreporter ajp12`
  - d. 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 below. The steps are different depending on 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 UNIX. 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 the web server and the application server. These special configuration steps are not addressed in this installation. Refer to your application server and web server documentation.

---

## Installing on a Windows Web Server

1. Insert the Data Protector Windows installation CD-ROM.
2. CD to `DP_Service_Mgmt_Integr.`
3. Run `DP-SIP-WIN.exe`.
4. Follow the steps in the Setup Wizard. From the Select the type of Installation screen, select Java Servlets.

On the SIP portal machine, insert the Data Protector Windows installation CD.

1. CD to `DP_Service_Mgmt_Integr.`
2. Run `DP-SIP-WIN.exe`.
3. Follow the steps in the Setup Wizard. From the Select the type of Installation screen, select SIP (Direct) Components.

4. Import the Customer Model, as described in “Creating Customer Models and Portal Views” on page 45
5. Create users and user roles, as described in the *SIP Deployment and Integration Guide*.
6. Customize `ConfigSpec.xml` as described in “Customization” on page 40.

### Installing on an UNIX Web Server

To install the integration on an UNIX web server:

1. Insert the Data Protector HP-UX/Solaris installation CD-ROM.
2. On HP-UX: As root, use `swinstall` to install the following depot:

```
DP-SIP-HPUX.depot
```

- On Solaris: As root, use `pkgadd` to install the following package:

```
DP-SIP-SUN.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` as described in “Customization” on page 40.
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. Find the line:

```
JkMount /ovportal/* ajp12
```

- c. 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/Solaris CD.

1. On HP-UX: As root, use `swinstall` to install the following depot:

`DP-SIP-HPUX.depot`

- On Solaris: As root, use `pkgadd` to install the following package:

`DP-SIP-SUN.pkg`

2. Select and install the SIP component.
3. Import the Customer Model, as described in “Creating Customer Models and Portal Views” on page 45
4. Create users and user roles, as described in the *SIP Deployment and Integration Guide*.

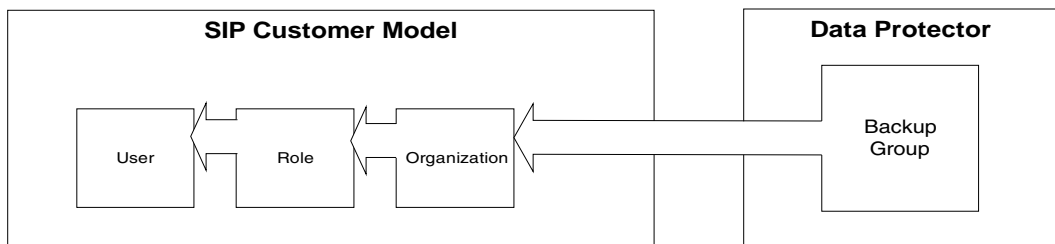
## Customization

This section describes how to customize the integration.

### Setting Up Backup Groups on Data Protector

In order to receive reports via SIP, you must 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 2-4. For more information about configuring groups, refer to the *HP OpenView Storage Data Protector Administrator's Guide*.

**Figure 2-4 Backup Group Mappings**



---

#### IMPORTANT

Use the following guidelines when setting up Data Protector backup specification groups:

1. Backup specification group names may NOT include periods (.) or question marks (?).
  2. If you define a role containing overlapping backup groups, users with that role will see redundant data in their reports.
-



## Editing ConfigSpec.xml

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), provides you with several options for customizing your integration. The following sections describe these options.

**Log Location, Log Level** The log level you set in your configuration determines the level at which events will be logged. In the example below, the log level is 3, so events with a severity of 3, 2, or 1 will be logged. Valid event severities are 1 - 5.

The log location parameter determines the name and location of your log file. You must specify an existing directory. To set the refresh rate, edit the following line:

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

In the example below, the log file msgtxt is located in the directory d:/tmp/logging/.

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

**Filter Level** The filter level you set in your SIP configuration determines which types of messages are delivered. You must set each of the message types as true (delivered) or false (not delivered).

In the following example, messages tagged as Major and Critical are delivered, while messages tagged as Minor and Warning are not.

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

---

**NOTE** Message filters in the ConfigSpec.xml file are applied at the system level. That is, any message levels you choose to filter out here will not be logged to your SIP or web server.

---

**Refresh Rate** By default, Data Protector reports refresh when SIP requests a report from the servlet (which it does every time a user logs on). You can, however, set the refresh rate variable so that reports refresh automatically at specified intervals. In this case, the reports are

gathered at each refresh interval and are archived on the system. Note that this is a universal parameter, so setting a value for it will cause all reports to refresh and expire at the specified rate.

To set the refresh rate, edit the following line:

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

Note that this variable has three parameters:

- **update\_rate** determines the refresh rate for the report, in minutes. It is recommended that you refresh reports no more than once every ten minutes.
- **archive\_rate** determines the rate at which archived reports are expired from the system. The value you enter here is the amount of time, in minutes, that a recently accessed report will be maintained on your system. The recommended minimum is five minutes. `Archive_rate` should be greater than `update_rate`.
- **file\_loc** specifies the location of the files that are gathered and archived to support `RefreshRate`. The location you specify must be a valid, existing directory. Note that this repository may need to be very large if you anticipate large numbers of users to be logging on at the same time.

In the example below, 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 your Data Protector system's health graphically using a gauge that has three ranges: green, yellow, and red, indicating the status of backup health.

You may, however, choose to change the default settings to reflect the sensitivity of your data or the critical nature of the systems you are backing up. To do this, change the ranges according to the health percentage you would like to fit into each range.

To set the gauges, edit the following line:

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

Note that you must not overlap different color bands, so if the green band ranges from 0 to 70, you must also change the lower value for the yellow band range in order not to overlap. For example:

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

---

**NOTE**

Gauge settings in `ConfigSpec.xml` are applied at the system level. That is, any gauge settings you enter here will be applied to your entire system. If you want some settings to be specific to a given module view, see “Editing the Backup Health Module” on page 57 for instructions. You may still change the bands for each gauge that you create.

---

**Cell Server Setting** The `CellServer` variable provides the integration with information about your Cell Servers, including the language, the port number, and the Java user password. If the Data Protector Administrator has changed either the Data Protector port or added a password for a Java user, you must edit this variable in order for the integration servlets to communicate with Data Protector.

To identify a cell server, edit the following line:

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

where:

- *locale* is a required parameter that specifies the language of the cell server.
- *port* identifies the port the integration will use to communicate with the cell server. Port defaults to 5555 if there isn't a specified number.
- *password* is an optional parameter necessary only if the Data Protector Administrator wants to create a Java user account. The parameter defaults to no password.
- *host\_name* is a required value that identifies the cell server using a fully qualified host name or IP address.

---

**NOTE**

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

---

In the following 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>
```

## Creating Customer Models and Portal Views

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

This chapter provides a brief overview of the concept of customer models, and a description of how SIP uses these models to filter the data a user sees.

For more information on customer models, see the SIP Deployment and Integration Guide.

This section discusses:

- “Customer Models”

This section describes the concept of customer models and how they are used within Data Protector and SIP.

- “Management Data Filter”

This section describes the Management Data Filter and how it is used to serve the appropriate information to your users.

- “Adding and Removing Services in a Portal View”

This section describes how to configure Data Protector services for display within a SIP portal view.

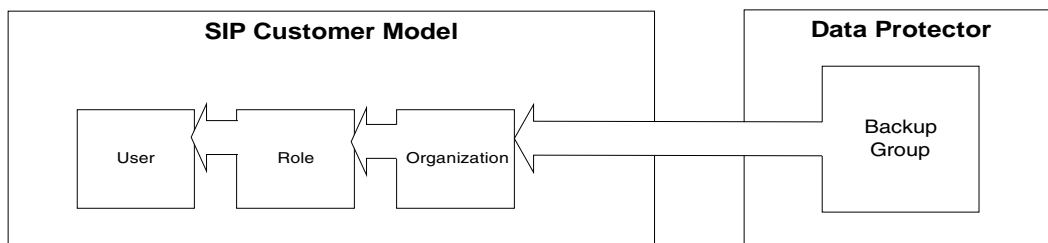
### Customer Models

To help you present exactly the right information to all of your users, SIP employs an expandable concept of customer models, which allows you to create and fine-tune different portals for users according to the department they work in, their job functions, security considerations, or anything else you would like to sort by.

Each cell server is used to create a basic organization where the host is specified; the name of the organization is group@cellserver. This mapping is required to properly generate reports. For detailed instructions for segmenting data and creating customer models, refer to the SIP Deployment and Integration Guide.

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

**Figure 2-5**      **Customer Model**



### Importing the Customer Model

Import the customer model from the SIP servlet by following these steps:

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 the following:

*http://servlet\_host.com/dpreporter/customer*

where

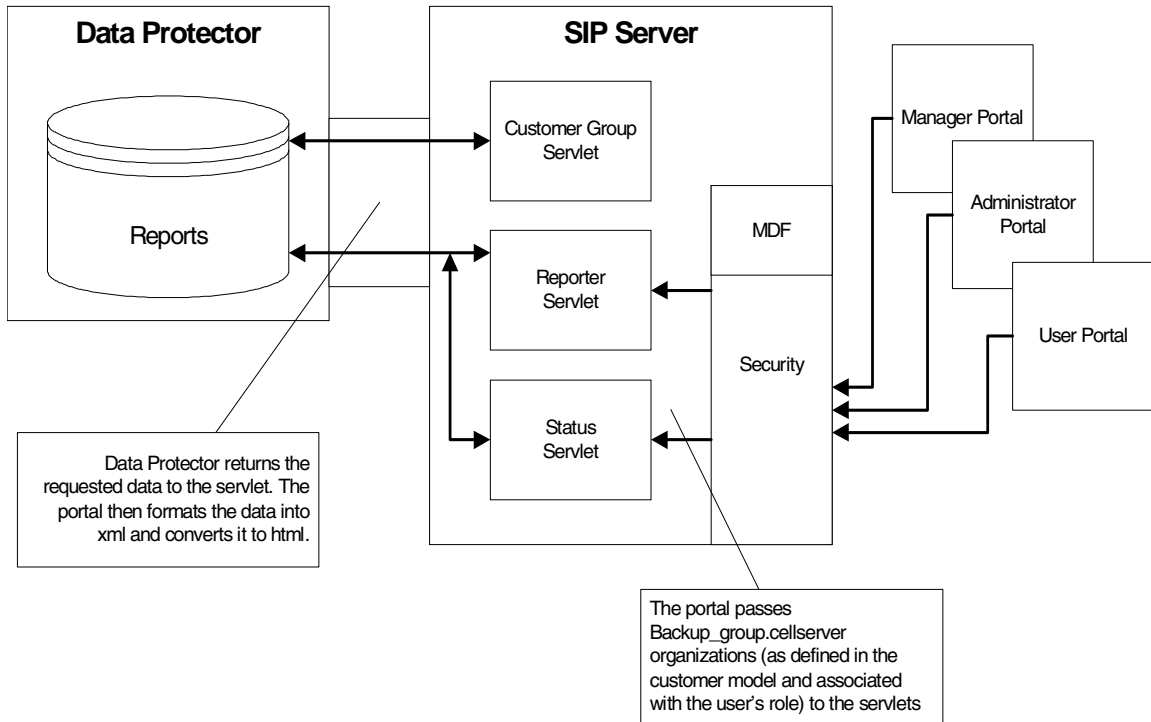
*servlet\_host.com* is the fully qualified host name of the web server on which the servlets are installed.

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 2-6** 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 server. The role can include multiple organizations.

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

For a more detailed explanation 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 the appropriate role (one 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 you chose is inserted into your PortalView.xml file and is displayed in the portal view. For instructions on how to edit the modules, refer to “Error Messages Module” on page 49, “Protection Status Module” on page 52, or “Data Protector Reports Module” on page 59.



## Error Messages Module

This chapter provides an overview of what Data Protector Messages are and how to configure and use them.

This chapter contains the following sections:

- “Understanding Data Protector Error Messages”  
This section describes what Data Protector Messages are and how you can use them in your organization.
- “Editing Data Protector Message Modules”  
This section describes how to set up new Data Protector message modules, as well as how to edit and eliminate existing messages.

### Understanding Data Protector Error Messages

The Messages module presents backup and recovery process messages from Data Protector running on one or more Data Protector stations within your management domain.

This 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

The Data Protector Error Messages 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 the chapter “Monitoring, Reporting, Notifications and the Event Log” in the *HP OpenView Storage Data Protector Administrator’s Guide*.

### **Adding a Data Protector Error Message Module to your Portal View - GUI**

To add a Data Protector message module to a SIP portal, follow the steps below.

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 the appropriate role (one with ViewAdmin editing permissions).
2. Navigate to the Storage tab.
3. At the bottom of the right column, either:
  - Select Data Protector 5.1 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 5.1 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.

If the timeframe you select does not provide any messages, a message appears indicating that no messages were available for that timeframe.

## Editing Data Protector Message Modules

To modify the Message module in your SIP portal, follow the steps below.

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 the appropriate role (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 on the upper right corner of the module.
5. From the Over the last: menu, choose a timeframe.
6. In the Data Protector Servlet host: field, enter the qualified host name and port of the appropriate servlet.
7. Click OK to apply the changes and return to the main portal view.

### Editing the PortalView.XML File Directly

Refer to the *SIP Deployment and Integration Guide* for more information.

---

## Protection Status Module

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

### Understanding the Protection Status Module

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

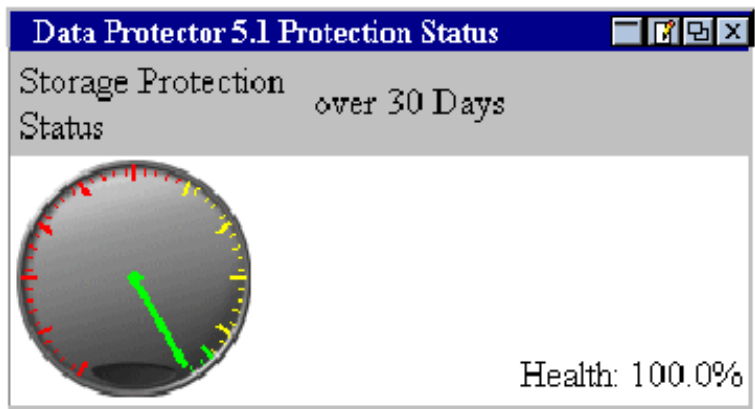
This module has two components: Protection Status gauge and Host Status report.

Gauges appear when the tab first displays in your portal. They indicate the overall health rating for selected or all services that are being monitored by that particular gauge. You can view the details by clicking on a gauge or a health title link to display information about the backups.

### Protection Status Gauge

The Protection Status Gauge provides a visual depiction of the status of the backup statistics for all organizations associated with the current role. This is calculated by averaging information from all the organizations.

**Figure 2-7** Protection Status Gauge



**All Hosts Backup Statistics Report**

If you click on a Protection Status Gauge from the main portal window, you can see the All Hosts Backup Statistics report, a detailed listing of information about your system’s backup health.

**Figure 2-8 All Hosts Report**

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

Table 2-3 describes the fields displayed on this screen.


**Table 2-3 Fields in the All Hosts Backup Statistics Report**

Client Host	The name of the cell server.
User Group	The name of the customer group.
% Success	The percentage of successful backup requests. The number in this field is expandable. See the following section for detailed information about this expanded information.
Data Written	The amount of backup data written (in gigabytes).
# Completed Objects	The number of completed backup jobs.
# Failed Objects	The number of failed backup jobs.
# Running DA	The number of disk agents currently running.
# Pending Objects	The number of backup jobs that are pending.

### Client Host Backup Report

When you click on the % Success field in the All Hosts Backup Statistics page, you can see the Client Host Backup Report, an expanded detail view of the backup health for the selected customer group on the selected cell server.

**Figure 2-9 Client Host Backup Report**

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

The fields on this screen are described in Table 2-4.

**Table 2-4 Client Host Backup fields**

Details:	The name of the cell server to which the report applies.
Group	The name of the customer group.
% Success	The percentage of successful backup requests. The number in this field is expandable. See the following section for detailed information about this expanded information.
Data Written	The amount of backup data written.
# Files	The number of files backed up.
# Backup Objects	The number of objects backed up. A <b>backup object</b> is any data selected for a backup, such as a disk, a file, a directory, a database, or a part of the database.

**Table 2-4 Client Host Backup fields (Continued)**

# Completed Jobs	The number of completed backup jobs.
# Failed Objects	The number of failed backup jobs.
# Running DA	The number of disk agents currently running.
# Pending Objects	The number of backup jobs that are pending.

### Host Statistics Report

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

**Figure 2-10 Host Statistics Report**

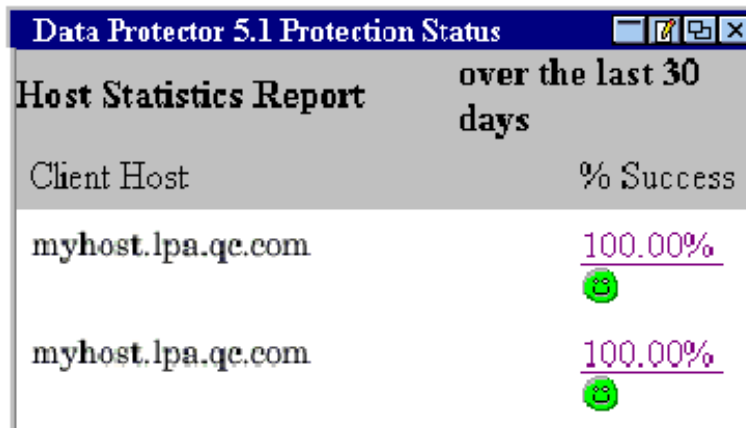


Table 2-5 describes the fields displayed on this screen.

**Table 2-5 Host Statistics fields**

Host Statistics Report	The name of the report.
------------------------	-------------------------

**Table 2-5**                      **Host Statistics fields (Continued)**

Time Frame (i.e., over the last 30 days in Figure 2-10)	The time frame for which data is collected/displayed.
Client Host	The qualified host name of the cell server.
% Success	The percentage of successful backup requests. The number in this field is expandable. See the following section for information about the detailed view.

**Detail View**

If you click on a percentage in the main portal window, you can see the All Hosts Backup Statistics report, a detailed listing of information about your system’s backup health. Refer to “All Hosts Backup Statistics Report” on page 53 for more information about this report.

Clicking on a percentage in the All Hosts Backup Statistics report displays the Client Host Backup Report and a further level of detail. Refer to “Client Host Backup Report” on page 54 for more information about this report.



## Editing the Backup Health Module

The Backup Health 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. You can use the Edit page to customize the Backup Health module.

### Using the Backup Health - Edit page



To customize the Backup Health module, click on the Edit button in the title bar. The Data Protector 5.1 Protection Status - Edit pane is displayed.

**Figure 2-11** Data Protector 5.1 Protection Status - Edit

**Table 2-6** Edit Fields

Data Protector Servlet host:	The fully qualified name of the host on which the servlets are running and the port on which the servlets are communicating.
Module	A drop down menu from which you can choose which version of the module to display, Status Gauge or Host Status.
Over the last:	The time frame from which to display results.
Warning % At and Below:	The success percentage at (and below) which the protection status is considered to be warning. Anything above this is considered to be normal/successful.
Critical % At and Below:	The success percentage at (and below) which the protection status is considered to be critical.

### Backup Health Criteria

The criteria for gauging backup health have been pre-configured in this system, so no additional steps are necessary for you to configure these gauges. You can, however, configure the thresholds for the general backup health status, or severity.

Backup health statuses are generally defined as described in Table 2-7.

**Table 2-7 Backup Health Status**

Normal	A safe health range, in which the 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 likely imminent, and the situation should be resolved immediately.

You can change the thresholds for these statuses globally based on factors within your unique environment. See “Editing ConfigSpec.xml” on page 41 for more information on setting these thresholds.

### Directly Editing the PortalView.xml File

You can edit the PortalView.xml file directly. You should be careful, if you choose to edit directly, as incorrect editing may cause anomalous results in the integration. Refer to the *SIP Deployment and Integration Guide* for more information about direct editing.

## Data Protector Reports Module

This chapter provides an overview of what Data Protector Reports are and how to configure and use them.

This chapter contains the following sections:

- “Understanding Data Protector Reports”
- “Editing the Data Protector Reports Module”
- “Establishing Global Settings for Reports”

### Understanding Data Protector Reports

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

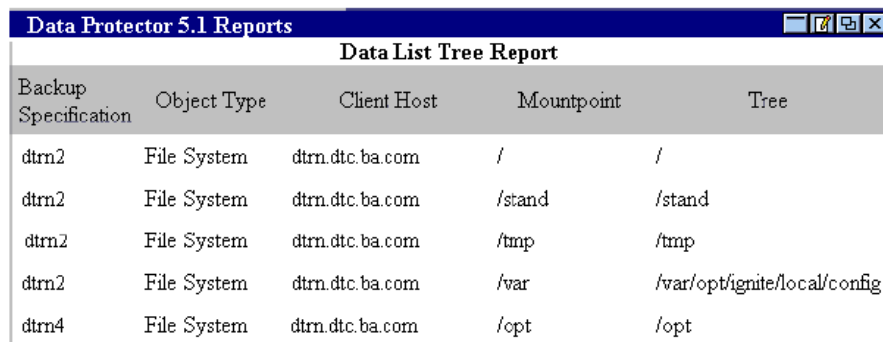
#### Data Protector Reports

The following Data Protector reports are pre-configured for SIP:

**Data List Trees** This basic report has information on all directory trees backed up by the cell server, but is limited to the directories of the groups associated with the SIP customer. Note that this option provides one report per group; customers with multiple groups get multiple reports.

Figure 2-12

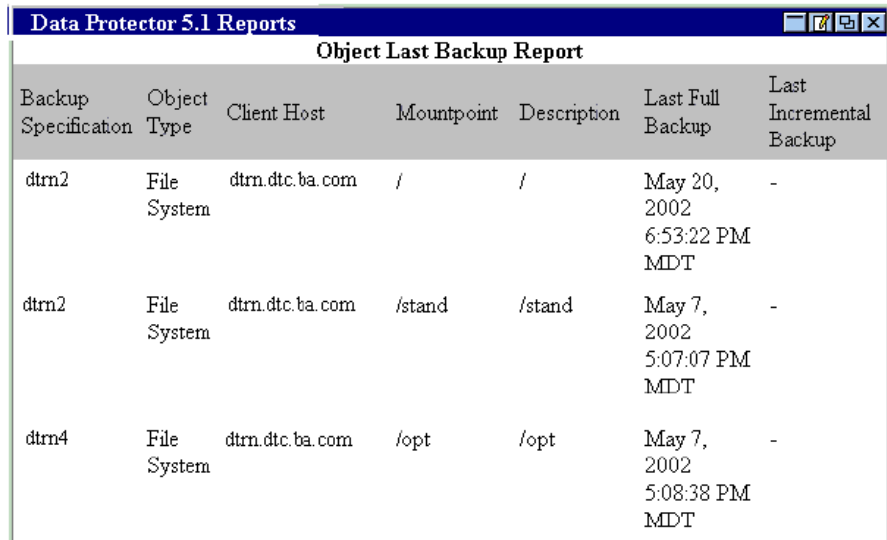
#### Data List Tree Report



Data Protector 5.1 Reports				
Data List Tree Report				
Backup Specification	Object Type	Client Host	Mountpoint	Tree
dtrn2	File System	dtrn.dtc.ba.com	/	/
dtrn2	File System	dtrn.dtc.ba.com	/stand	/stand
dtrn2	File System	dtrn.dtc.ba.com	/tmp	/tmp
dtrn2	File System	dtrn.dtc.ba.com	/var	/var/opt/ignite/local/config
dtrn4	File System	dtrn.dtc.ba.com	/opt	/opt

**Object Last Back Up** This is a basic report showing all objects owned by a group and the data of the last full and partial backup for that group. Note that this option provides one report per group, so customers with multiple groups get multiple reports.

**Figure 2-13** Object Last Back Up Report




The screenshot shows a window titled "Data Protector 5.1 Reports" with a sub-header "Object Last Backup Report". The window contains a table with the following data:

Backup Specification	Object Type	Client Host	Mountpoint	Description	Last Full Backup	Last Incremental Backup
dtrn2	File System	dtrn.dtc.ba.com	/	/	May 20, 2002 6:53:22 PM MDT	-
dtrn2	File System	dtrn.dtc.ba.com	/stand	/stand	May 7, 2002 5:07:07 PM MDT	-
dtrn4	File System	dtrn.dtc.ba.com	/opt	/opt	May 7, 2002 5:08:38 PM MDT	-

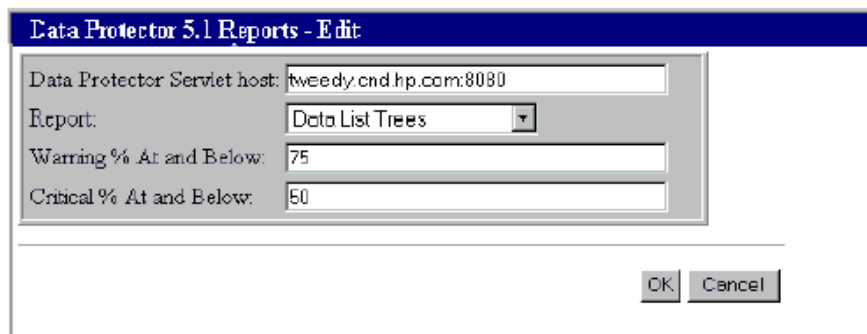
## Editing the Data Protector Reports Module

You can use the Edit page to customize the Reports module.

### Using the Reports - Edit page

 To customize the Reports module, click on the Edit button in the title bar. The Data Protector 5.1 Reports - Edit pane is displayed.

**Figure 2-14** Data Protector 5.1 Reports - Edit



**Table 2-8** Edit Fields

Data Protector Servlet host:	The fully qualified name of the host on which the servlets are running and the port on which the servlets are communicating.
Report	A drop down menu from which you can choose which report to display, Data List Trees or Object Last Backup.
Warning % At and Below:	The success percentage at (and below) which the protection status is considered to be warning. Anything above is considered to be normal/successful.
Critical % At and Below:	The success percentage at (and below) which the protection status is considered to be critical.

### **Directly Editing the PortalView.xml File**

It is possible to edit the PortalView.xml file directly. You should be careful, if you choose to edit directly, as incorrect editing may cause anomalous results in the integration. Refer to the *SIP Deployment and Integration Guide* for more information about direct editing.

### **Establishing Global Settings for Reports**

For more information about establishing global settings for reports, refer to “Editing ConfigSpec.xml” on page 41.

---

## Backup Sessions Module

This section provides an overview of Data Protector Backup Sessions and how to configure and use them. This information is divided into the following sections:

- **Understanding Data Protector Backup Sessions Module**  
This section describes what Data Protector Backup Sessions are and how you can use them in your organization.
- **Setting Up New Data Protector Backup Sessions Modules**  
This section describes how to set up new Data Protector Backup Session modules.
- **Editing Data Protector Backup Sessions Module**  
This section describes how to edit and delete Data Protector Backup Session modules.

### Understanding Data Protector Backup Sessions Module

The Backup Sessions module presents backup session information from Data Protector running on one or more Data Protector stations within your management domain.

This module displays changes each time the portal view is displayed or refreshed. The Session lists are continually updated in SIP memory.

The Backup Sessions Module consists of the fields described Table 2-9.

**Table 2-9 Backup Session Module Fields**

<b>Fields</b>	<b>Description</b>
Client Host	The Name of the Cell Server
Backup Specification	The Name of the Backup Specification
Status	Final status of the Session. . i.e. Completed, Failed ,Completed with Errors etc

**Table 2-9 Backup Session Module Fields**

<b>Fields</b>	<b>Description</b>
Schedule Type	Schedule Type of the Backup Session. . i.e. Full, incremental, incremental1 etc
Start Time	Start Time of the Backup Session.
End Time	End Time of the Backup Session.
Duration (hours:mins)	Duration of the Backup Session in hours:minutes
Queuing (hours:mins)	Amount of Time, the Backup Session waited in the queue in hours:minutes
GB Written	The amount of backup data written (in giga bytes).
# Media	No of Media used for backing up the data.
# Errors	No of Errors occurred during the Session.
# Warnings	No of Warnings displayed during the Session.
# Files	No of Files backed up
% Success	Success Percentage of the Session
Session ID	ID of the backup session.

### **Setting Up New Data Protector Backup Sessions Modules**

To add a Data Protector Backup Sessions Module to an SIP portal, complete the following steps:

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 the appropriate role (one with ViewAdmin editing permissions).
2. Navigate to the Storage tab.
3. At the bottom of the right column, either:



- Select Data Protector 5.1 Backup Sessions from the Select Module to Add list box, and click Add.

or

  - Click Edit to access the Modify Column window. Choose Data Protector 5.1 Backup Sessions from the Available Modules list 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 backup sessions, 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. If the timeframe you select does not have any backup sessions, a message appears indicating that no backup sessions were available for that timeframe.

## Editing Data Protector Backup Sessions Module

To modify the Backup Sessions module in your SIP portal, complete the following steps:

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 the appropriate role (one with ViewAdmin editing permissions).
2. Navigate to the Storage tab.
3. Scroll to the Backup Sessions module that you want to edit.
4. Click on the Edit button on the upper right corner of the module.
5. From the Over the last: menu, choose a timeframe.
6. In the Data Protector Servlet host: field, enter the qualified hostname and port of the appropriate servlet.
7. Click OK to apply the changes and return to the main portal view.

## Internationalization Issues

This chapter describes internationalization issues with the Data Protector-SIP integration.

### Language Support

Both Data Protector and SIP offer multi-language support for English, Japanese, and German.

### Internationalization Issues

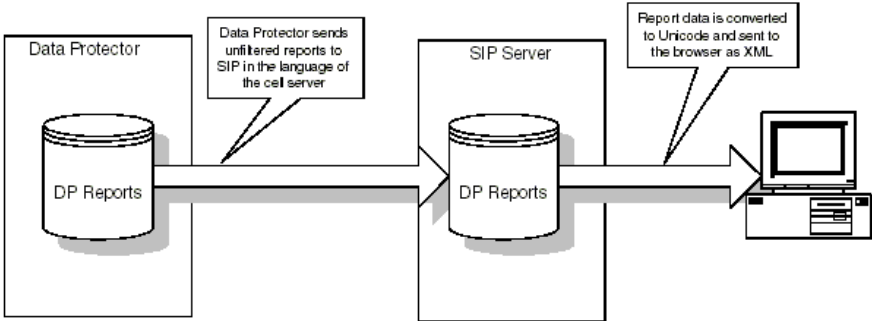
Because of the multiple languages supported, and because of the distributed nature of computer networks, there are potential internationalization issues with the Data Protector-SIP integration.

**Wide Bit vs. Single Bit Character Sets** The Data Protector-SIP integration is currently available in three languages: English, German, and Japanese. In most cases, these integrations should work without difficulty.

However, a problem may be presented if your cell, or Data Protector, server and your web, or SIP, server use different languages. German and English both use the Latin alphabet, which is rendered as a single-bit character set. Japanese, however, is rendered as a wide-bit character set. This may cause readability issues when your cell server is in one character set and your web server in another.

If the cell server is in Japanese, your reports may not display correctly on a non-Japanese browser; and if your cell server is in German or English, your reports may not display correctly on a Japanese browser.

**How the Cell Server and the Web Server Communicate** The illustration below shows how the cell server (Data Protector 5.1) and the web, or SIP, server communicate.



All Data Protector reports are generated and sent to SIP in the language of the cell server. The reports are then converted to Unicode, which recognizes a wide range of character sets, and sent to the browser as XML. Because of this configuration, if your cell server is in a language with a wide-bit character set (Japanese), and your SIP server or the end user’s web browser is in a language with a single-bit character set (English or German), or vice versa, there may be problems displaying your reports.

Whenever possible, the report headers will be in the language of the end-user’s browser, if that language is supported. If the browser’s preferred language is not supported, the title lines will default to English. Some examples of this are shown in Table 2-10.

**Table 2-10 Internationalization Scenarios**

Cell Server	Web Server	Browser	Report
Japanese	French	German	Title lines in German
			Body of report in Japanese
German	English	Japanese	Title lines in Japanese
			Body of report in German
German	French	Korean	Title lines in English
			Body of report in German

## Troubleshooting

### Error Messages

This section lists some error messages you may see while using this integration and discusses how to respond to them.

#### Data Unavailable

If, while viewing reports, you get a *Data Unavailable* error message after adding a module, 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 reasonable in size to have data.

#### Parse Rest of Config

If, while using this integration, you get 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.

---

# **3 Data Protector-OVO-SIP Integration**

## Introduction

The integration of Data Protector with the OpenView Service Information Portal (SIP) offers pertinent information to the managers of the backup service of a specific group. The portal allows for tailoring of the page for each user.

This chapter describes how SIP and OpenView Operations integrate with Data Protector to provide additional network visibility to Data Protector and to allow integration of Data Protector-specific information with other SIP services.

## Prerequisites

The integration requires the following licensed components:

- Data Protector
- OpenView Operations
- OpenView Service Information Portal
- Supported Oracle Database (third party software)
- Data Protector Integration for OVO for UNIX

## Product Capabilities and Integration Benefits

This integration provides the following capabilities:

- Convenient data protection service monitoring through web access from any machine.
- Various forms of data presentation: service health gauges, service graphs, service cards, and a service browser.
- The specification of resource in terms of machine and backup specification group names.
- Segmentation of accessible data by the different backup administrators.
- Support for various authentication mechanisms including a generic authentication mechanism.

- Information aggregation from other services (not related to Data Protector) to the portal, using SIP's configuration mechanisms. A single presentation format for all modules.
- Easy configuration: GUI configuration editor and XML document editing only.

## Component List

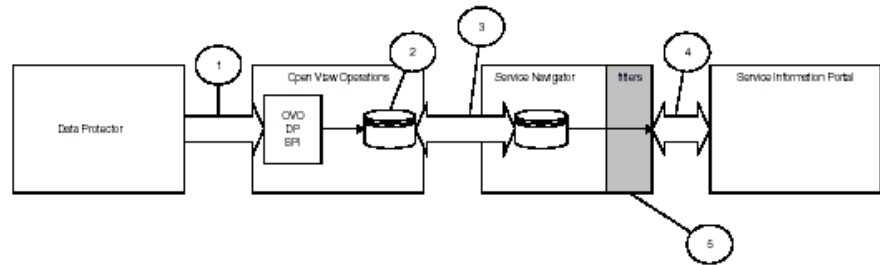
- Data Protector - A backup solution that provides reliable data protection and maximum accessibility for your business data. Data Protector offers comprehensive backup and restore functionality specifically tailored for enterprise-wide and distributed environments.
- OpenView Operations (OVO) - A central data collection and management point capable of reading messages from a variety of modules on various machines, acting on them when such action is defined, and transmitting them (the messages) further if asked. OVO has the potential of serving as a central management point for various remote systems. OVO offers both command line and graphical user interfaces for local and remote administration.
- Data Protector Integration for OVO for UNIX - A component that implements the data passing interface between Data Protector and OVO. This component resides on both ends and is integrated into both products.
- OpenView Service Navigator - A system that maps messages to services to ease the control of complicated systems.
- OpenView Service Information Portal (OV SIP) - 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.



---

## Data Mappings

The illustration below shows the data mappings for this integration.



1. OVO receives information from Data Protector via the Data Protector Integration for OVO for UNIX.
2. OVO stores the information locally in its database.
3. Service Navigator receives the Data Protector records from OVO.
4. SIP queries Service Navigator about the OVO information.
5. Service Navigator filters the records received from OVO by service name, according to the SIP query.

If the customer also integrates OV Reporter in this configuration, SIP may provide URLs to the reports as generated by Reporter. It is up to the administrator to configure the links. The Reporter-Data Protector integration generates these reports as statically linked HTML documents.

## Dependencies

- If Reporter is included in the integration, the configuration of the URL links for the reports depend on the names that Reporter gives to those reports.
- The Backup Service pie chart module will only be available if the OpenView Reporter integration is installed.
- If you choose to use the Backup Service pie chart module, the Data Protector backup specification group names must be names that Windows NT accepts for file names. A folder named “machinename.DPServiceName” is created for them on the Reporter machine, which is a Windows machine. The names must contain only ASCII characters.
- OVO requires a supported Oracle database to be installed. The exact version depends on the OVO version. For more information, refer to the OVO Installation Guide.
- Sun's Java Developer's Kit 1.3 is required for SIP, OVO, and Service Navigator.
- Some OpenView components require that Netscape Navigator 4.7 be installed. This step is unnecessary and may be skipped as long as alternative means of browsing HTML pages is available (e.g., a web browser on a separate machine, or an alternative compatible web browser).
- Successful configuration must also comply with the software requirements as described in the table below.
- The environment must be properly set and configured prior to the installation of the integration components. This may include patches, environment variables, kernel parameters, and other software components as required. For detailed information about the specific requirements, please refer to the installation guides for those components.
- This integration uses Data Protector backup specification groups. Refer to the *HP OpenView Storage Data Protector Administrator's Guide* and the Data Protector online help for more information about backup specification groups and how to configure them.

**Table 3-1 Software Requirements**

<b>Component</b>	<b>Version</b>	<b>Operating System</b>
OVO	6.0, 7.0, 7.10	HP-UX 11.0
Data Protector	5.1	HP-UX 11.0, 11.11 Solaris 8 Windows NT 4.0, Windows 2000
OVO Agent	6.05, 7.0, 7.10	HP-UX 11.0, 11.11 Windows NT 4.0, Windows 2000
OVO Database	Oracle 8i	HP-UX 11.0, 11.11
SIP	3.0, 3.1	HP-UX 11.0 Solaris 8 Windows 2000
Service Navigator	6.0	HP-UX 11.0

## Setup Process

The setup process for this integration consists of two main procedures:

- Installation of the components
- Configuration of those components

### Installation

Service Navigator, OVO, SIP, and Data Protector can be installed on a mix of UNIX and Windows machines. All the necessary and required components should be installed and working.

1. Data Protector 5.1 should be installed on the data protection cell manager. If the cell manager is an HP-UX machine, the DCE-KT-Tools component must also be installed.

See the Data Protector 5.1 Installation Guide for detailed instructions.

2. Install the following Oracle products, version 8.1.6.0.0, on the management station:

- Oracle8i Server (Optional components not required)
- Net8 Products (All components are required)
- Oracle Utilities (All components are required)
- Oracle Installation Products (All components are required)

3. Use `swinstall` to install the ITOEngDoc and ITOEngOraAll OVO components (assuming the chosen language is English) on the management station. See the *OpenView Operations Installation Guide* for detailed instructions.

4. Install Service Navigator on the management station. See the *HP OpenView Operations and Service Navigator Integration with SIP* document for detailed instructions.

5. Install Data Protector Integration for OVO for UNIX on the management station. This component is located on the Data Protector CD. (This step includes various related patches for Service

Navigator and OVO.) See the *HP OpenView Storage Data Protector Integration Guide for HP OpenView Operations* for detailed instructions.

6. Install the OVO agent on the cell server. See the OpenView Operations Installation Guide for detailed instructions.
7. Install SIP on the portal server. See the Service Information Portal Installation Guide for detailed instructions.
8. Install the integration package (listed below) on the SIP server.
  - Windows
    - a. Insert the Windows installation CD.
    - b. Run the following executable:

```
\DP_SERVICE_MANAGEMENT_INTEGR\DP-SIP-WIN.exe
```
    - c. Follow the on-screen instructions and from the Select the type of Installation screen, select SIP (OVO) Components .
  - UNIX
    - a. Insert the HP-UX/Solaris installation CD.
    - b. On HP-UX: As root, use `swinstall` to install the following depot:

```
/OV_INTEGRATIONS/DP-SIP-HPUX.depot
```

On Solaris: As root, use `pkgadd` to install the following package:

```
/OV_INTEGRATIONS/DP-SIP-SUN.pkg
```
    - c. Follow the on-screen instructions and select the DP-OVO-SIP component.

## Configuration

SIP maintains its configuration documents in XML format. The XML must be modified to present customized portal views, implement user data segmentation and separation, and map resources to the users.

### Sample Configuration Files

The integration package will place sample configuration files in the following directory:

Windows 2000 <SIP>\ovo\SIP\integration\DP

UNIX <SIP>/ovo/SIP/integration/DP

See the readme file for details about the sample files.

### Editing Configurations

There are three basic ways to create and update the configuration. You can use any of the following methods:

- The SIP Administrator view can be used to restart the engine, to accept new customer models, and to help design the portal page when viewing a role with ViewAdmin.
- The configuration editor is a Java tool supplied with SIP that guides the user through the process of configuration, including user/role mapping and management station declarations.
- The XML files can be edited by hand. The customer model must be defined via manual XML editing. You can also perform any other configuration tasks by editing the XML files directly.

### Configuring the Management Stations

1. On the portal machine, use the SIP configuration editor to select and right click the ManagementStation folder. From the shortcut menu, click New...
2. Type the fully qualified hostname in the New Management Station Window.
3. Select the OVO tab and check the "OVO Is Installed On This System" and "Service Navigator Is Installed On This System" boxes.
4. Accept the default values, or change the values and continue.

The configuration file is located as follows:

Windows 2000 SIP\conf\...

UNIX /SIP/conf/share/stations/mgmtStations.xml

Following is an example of a management station element in the `mgmtStations.xml` file. Notice that it contains the definitions of all the OVO stations SIP communicates with.

```
<ManagementStation hostname="ovo.example.com">
  <OVOSTation
    serviceNavPort="7278"
    serviceDataSource="yes"
    dbPort="1521"
    dbUser="opc_op"
    dbPassword="OpC_op"
    maxConnections="10"
    minConnections="5"
    maxCachedStmts="10"/>
</ManagementStation>
```

For more information about management stations, refer to `mgmtStations.dtd`, `ovoConfig.dtd`, and the online help in the SIP configuration editor.

## Updating the Customer Model

The customer model is where Organizations are defined in terms of accessible resources. The file that describes the model is:

Windows 2000    <SIP>\conf\share\CustomerModel.xml

UNIX            <SIP>/conf/share/CustomerModel.xml

Make a copy of the existing model and amend `CustomerModel.xml` to include the organization you want your users to access. Add `<Organization>` tags as an element in `<SimpleCustomerModel>`. The specification of backup services requires neither `<NodeList>` nor `<InterfaceList>`, so those tags will be empty if present at all. If you include resources other than Data Protector backup services as described in this integration, you may need to use the `<NodeList>` and `<InterfaceList>` tags.

For more information, consult the chapter “Segmenting Data by Customer Organization” in the SIP Deployment and Integration Guide.

The example below shows a description of a backup service. The <ServiceLevel> tag is used to describe the service level. The <Service> tag is where the backup service is referenced. Its name must be specified as software name (e.g., "Data Protector"), fully qualified machine name, backup specification group name (if defined in Data Protector), and service name with full hierarchy (full hierarchy means the path in the service graph starting at the root and ending in the required node). The service navigator requires a format of a service description to be topnode separated by a dot followed by its child node, and so on till the last node to be described. All items should be separated by a dot.

```
<Organization name="firstOrg" type="customer">           <ServiceLevel>Gold
Service</ServiceLevel>

  <NodeList/>
  <InterfaceList/>
  <ServiceList>
    <Service name="Data Protector.example.com.group1.BackupSessions"
      type="server"/>
    <Service name="Data Protector. ..." type="server"/>
  </ServiceList>
</Organization>
```

### Creating a SIP User/Role Package

The SIP security model is based on segmentation. Services are mapped to roles (not necessarily uniquely) and users are given access to those roles (each user may have more than one role). The information about the user/role model is then processed and saved in a format SIP can use.

To create a new user/role package:

1. Highlight User Role Packages
2. Select New in the drop down menu in the Configuration Editor

The list of active user/role packages is located in:

```
Windows 2000  <SIP>\conf\share\roles\index.xml
UNIX          <SIP>/conf/share/roles/index.xml
```



---

**NOTE**

---

Remove any packages you do not use. Each package contains doors through which one may enter your system. Leaving unused packages on your system can create unnecessary risk by introducing security holes.

To define a SIP user/role package, follow the steps below. In this example, the SIP configuration editor is used.

For more information about user role/model and definition, use the online help in the SIP configuration editor.

**Define the management data**

1. Create the managementData items in the package you defined.
2. Select the “Show Data for the Following Organizations:” button, select the name for the management data, and click Add.
3. The list of available organizations is displayed in a new window. Select all organizations (previously defined in the customer model) and click OK. (You may later remove organizations from the management data, e.g. for security purposes.)
4. Repeat the previous steps for each group of resources.

**Define user roles**

1. Select Roles from the package you created. Right click and select New from the shortcut menu.
2. In the General tab, choose a Role Name (the name used in the configuration to reference the role) and a Display Name (the name appearing on SIP for that role).
3. Select a setting from the drop down menu for the Edit Permissions field. User Preferences is the recommended setting, as it allows users to select their own skins--or predefined display settings--for their pages.
4. Select Portal View File. This file may be any portal view you have already defined or one of the demo portal views, such as samples/liveDemo.xml (Use the browse button to help you navigate through these files.)

5. Type a new name in Modified View File field. The name should have the extension .xml. When you do this, the file used in the Portal View File is copied and the role has its own portal view. If you do not want to do this (for example if you would like any change to a portal view of one role to be reflected by all roles who share that view), do not specify a Modified View File.
6. Click the Management Data tab and select “Use specific management data.”
7. Choose the management data you would like to associate with the role.
8. Click OK.

You now have a new role.

### **Define a User**

1. Select Users in the package, right click and select “New...” from the shortcut menu to add the user. Choose the user login name (the name used to refer to that user in the configuration) and display name.
2. Click the Roles tab and choose the user's roles and initial role. You may override the edit preferences of a role for a user by specifying the role in the Other Roles block, adding the role there and editing its “Override Permissions” field.
3. To allow easy editing of the portal views for all roles, you may want to either give an existing administrator access to those roles or create a new portal view administrator. To create a new portal view administrator, create a new user with access to all the Roles you want the user to be able to configure portals for. Make sure the Override Permission field for these roles is set to ViewAdmin for this user. (See the Roles tab in the user definition window).
4. Click the save button in the SIP portal configuration editor.

The configuration is saved.

## Design portal views

1. Now that your users are set, you must restart the SIP engine before the changes take effect.
2. To design portal views, log in as a portal views administrator (a user with ViewAdmin permission to the configured role) and design the portal views for the various roles. You may add, remove, and edit any module that has access to the information spanned by the role's management data. When finished, log out, then log back on as a user with access to the role to view your new view as users will see it.
3. Please refer to the “Designing a Custom Look and Feel to Your Portals” section of the “Customizing Portal View” chapter in the SIP Deployment and Integration Guide for more details on customizing your portal view.

## Add Password Authentication (optional)

The system configured so far offers little security. Access to a user's view is given upon request with only a user name.

To add a level of security to the system, you can configure password authentication to the portal.

This step is optional as the customer may choose to have a different security model, or no security at all.

## Enable password authentication

Follow the steps below to add a user/password authentication scheme to the portal. For all other authentication options, or for further information, refer to the “Configuring Authentication” chapter in the SIP Deployment and Integration Guide.

Enable user password authentication in SIP. Authentication is a portal-wide setting configured in the OVPortalConfig.xml file, located in the following directory:

Windows 2000    <SIP>\conf\framework\

UNIX            <SIP> /opt/OV/SIP/conf/framework/

Find the Authentication element and change it as shown below:

```
<Authentication LoginPage="/ovportal/jsp/security/login_html.jsp"
    AuthenticationProviderClass=
        "com.hp.ov.portal.security.FileAuthenticationProvider"
    ShowLogoutButton="yes"
    LogoutPage="/ovportal/jsp/security/logout_html.jsp"/>
```

Once you enable password authentication you can begin to add authorized users to SIP.

### Add authorized users to SIP

SIP provides a program, `htpasswd`, for configuring user logins. It also comes with a password file containing one user:

```
username: ovuser
```

```
password: ovuser
```

1. The password file is manipulated the same way a UNIX password file is. You must add a user and its password to the password file to allow users access their SIP accounts. To add a user:

Windows 2000:

```
%SIP_HOME%\bin\htpasswd
%SIP_HOME%\etc\passwd <username>
```

UNIX: (as root)

```
/opt/OV/SIP/bin/htpasswd
/opt/OV/SIP/etc/passwd <username>
```

where *<username>* is the user you want to add to the portal.

2. Enter a password for the user when prompted.

The location of the default password file is:

Windows 2000: %SIP\_HOME%\etc\passwd

UNIX: <SIP>/etc/passwd

Once you have created new user accounts, you may remove `ovuser` from the password file by deleting its entry and saving the file.

## Finalize the Configuration

1. If an authentication module was configured, restart the engine.
2. Log on to the system from the web and access the admin view for the configured role.
3. If the reporting system (OVR) is integrated into the system, you should now associate users with reports.

---

### NOTE

It is important to note that only the Backup Health Report is currently customized per group. None of the other included OVR reports have been customized and so will contain information regarding all groups. Users who have access to these reports can easily gain information regarding other services. It is recommended, in the interest of segmentation, that you do not give regular users not designated as administrators links to the non-customizable reports. You should give these users a link to their respective group report only.

---

Backup Administrators with jurisdiction over all backups may be given a link to all reports. These references are represented as URL links in the portal.

4. To add a reference, log in as a user with ViewAdmin privilege for the role you want to add a report for.
5. In the new window, click the Add Bookmark button.
6. Complete the following fields:

**Bookmark Name** The name the portal will display for the link. In most cases, you can use Backup Health Report (unless it is a different report you give a link to).

**HREF** The URL itself.

**Window Name (optional)** A title for the new window the user will open by clicking that link.

7. Click OK.
8. Return to the bookmarks window and click OK again.

The bookmark will now display in the portal view for this role.

---

**NOTE**

---

OVR reports are not secured, and unless special actions are taken, can be accessed by any user who has the link names. If there is a concern about the security and sensitivity of the displayed information, OVR should not be integrated with SIP

SIP is delivered with a generic demo portal that includes graphics files of sample logos. You may want to remove these samples.

To remove these files, follow the procedure below.

1. On the machine with the web server installed, go to the directory where the default header is stored.

Windows 2000    <SIP>\webapps\ovportal\jsp\core

UNIX            <SIP>/webapps/ovportal/jsp/core

2. Save a copy of `header.jsp` and edit `header.jsp` to eliminate the link to `generic_net.gif` or `hplogo.gif` or, alternatively, replace them with links to your favorite logos.

The portal view has many details that can be customized. For more information on this, refer to the *SIP Deployment and Integration Guide*.

If the OVR Data Protector integration has also been installed, then there is a Backup Service Health pie chart module available. The following steps will activate the module.

1. Verify that the OVR Data Protector integration is installed correctly by locating <...>HP OpenView\bin\split.exe on the OVR machine.
2. Open the file <SIP>/registration/defaults/OVDefaultOVRRep.xml. It should contain the following content and can be found in the release package:

```
<Generic>
  <Submodule>
    <Url href="http://<reporterAddress>/hpov_reports/DP/
      SessionHealthStatus_m/SIP_USERS/$OVROLE[OVName].jpg"
      displayMethod="inline" inlineHeight="400"
      anchorText="Backup Service Health Status"/>
  ...</Submodule>
</Generic>
```

---

**NOTE**

The “\_m” that precedes `SessionHealthStatus` in the link above specifies the 30 days period report. If you want the daily or weekly period report, you can redefine the link to `SessionHealthStatus_d` or `SessionHealthStatus_w` *provided* that the corresponding steps on the OVR side are taken, too. By default, OVR is only configured to split the monthly report.

---

Substitute `<reporterAddress>` with the machine name and the port number, if required, of your reporting station.

3. Restart the SIP engine. Verify that the configuration of the Backup Service Health pie chart module is correct by viewing the log file as a SIP administrator. The log should show details if the configuration has problems.
4. You can now add the Backup Service Health pie chart module by modifying a Data Protector user's portal view. If the pie chart does not appear and an error message is displayed, please refer to the Troubleshooting section.

## Troubleshooting

**Table 3-2**

### Troubleshooting

<b>Problem</b>	<b>Resolution</b>
The module in the portal displays an error description.	Click the refresh button.
The module displays a message: Currently not configured - the management station is not connected to SIP or attempt to use information from service outside the resources defined for the given role.	Reconfigure and reprocess configuration. (Run <code>create_role_db</code> if the customer model changed. Otherwise, restart the engine.)



**A**

All Hosts Backup Statistics Report, 53

**B**

Backup groups, 40

Backup Health

    criteria, 58

    status, 58

Backup Health Module, 57

**C**

Cell request server, 28, 29

Client Host Backup Report, 54

conventions, 11

Customer models, 45

    importing, 46

Customization

    Data Protector-SIP, 40

**D**

Data Protector

    error messages, 49

    reports, 59

        understanding, 59

Data Protector Integration module, 29

Data Protector-SIP

    cell server, 43

    customer models, 45

    filter level, 41

    gauge settings, 42

    logging, 41

    management data filter, 47

    portal views, 45

    refresh rate, 41

    troubleshooting, 68

Data Protector-SIP deployments, 31

Deployments

    Data Protector-SIP, 31

**E**

Error messages

    module, 49

        adding, 50

        editing, 51

    understanding, 49

**G**

Gauges

    protection status, 52

**H**

Hosts Statistics Report, 55

**J**

Java Developer's Kit, 27

**L**

Logging, 41

**M**

Management data filter, 47

**N**

Netscape Navigator, 27

**O**

OpenView

    Service Information Portal, 22, 26, 28

    Service Navigator, 22

OpenView Operations, 22

**P**

Portal view

    services, 48

Portal views, 45

Protection status

    gauge, 52

    module, 52

**R**

Reports, 59

    All Hosts Backup Statistics, 53

    Client Host Backup, 54

    Data List Trees, 59

    global settings, 62

    Host Statistics, 55

    module, 59

        editing, 61

    Object Last Backup Up, 60

    understanding, 59

**S**

Service Information Portal, 22

Service Navigator, 22

SIP, 22, 26, 28

---

# Index

Status gauges, 29

## T

Troubleshooting

    Data Protector-SIP, 68

typographical conventions, 11