

# HP Data Protector Smart Plug-in

For the Linux and Microsoft Windows operating systems

Software Version: 9.00

## User's Guide

Document Release Date: December 2014

Software Release Date: December 2014



## Legal Notices

### Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

### Restricted Rights Legend

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

### Copyright Notice

© Copyright 2014 Hewlett-Packard Development Company, L.P.

### Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

## Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: <http://h20230.www2.hp.com/selfsolve/manuals>

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: <http://h20229.www2.hp.com/passport-registration.html>

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

## Support

Visit the HP Software Support Online web site at: <http://www.hp.com/go/hpsupport>

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

To find more information about access levels, go to:

[http://h20230.www2.hp.com/new\\_access\\_levels.jsp](http://h20230.www2.hp.com/new_access_levels.jsp)

**HP Software Solutions Now** accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is

<http://h20230.www2.hp.com/sc/solutions/index.jsp>

# Contents

Contents .....	3
Chapter 1: Introduction .....	5
About HP Operations Manager .....	5
About Data Protector .....	5
About Data Protector Smart Plug-in .....	6
Product Architecture .....	8
Chapter 2: Installation and Configuration .....	9
Adding Data Protector Cell Manager as a Managed Node .....	10
Installing HP Operations Agent on the Data Protector Cell Manager .....	10
Installing Data Protector SPI on HPOM Management Server .....	11
Assigning Data Protector SPI User Profiles .....	11
Distributing Data Protector SPI Configuration to the Cell Managers .....	12
What's Next? .....	13
Chapter 3: Removing Data Protector SPI .....	14
Chapter 4: Licensing .....	15
How Licensing Works .....	15
Configuring License Requests .....	16
Requesting and Retrieving Licenses .....	16
Activating Licenses .....	17
Verifying Licenses .....	17
Removing Licenses from the Monitored System .....	17
Chapter 5: Data Protector SPI Discovery and Monitoring .....	19
Discovered Objects .....	19
Data Protector SPI Tools .....	20
Data Protector SPI Actions .....	23
Update Service Navigator Graph .....	23
Data Protector SPI Messages .....	23
Data Protector Service Status - Generic .....	24
Data Protector Service Status - LIC .....	24

Data Protector Service Status - IDB .....	25
Data Protector Client Backup Status .....	25
Data Protector Client Recovery Point Objective .....	26
Data Protector Cell Client Group Backup Status .....	26
Data Protector Device Mount Request .....	27
Data Protector Device Operational State .....	27
Data Protector Smart Plug-in License Validation .....	28
We appreciate your feedback! .....	29

# Chapter 1: Introduction

This chapter introduces the Data Protector Smart Plug-in and explains how it interacts with HP Operations Manager and HP Data Protector.

## About HP Operations Manager

HP Operations Manager (HPOM) is a distributed client-server software solution designed to help system administrators detect, solve, and prevent problems occurring in networks, systems, and applications in any enterprise. Using HPOM, you can check health, performance, and availability for all monitored objects in the environment as well as identify and resolve problems. It also provides alerts generated according to availability, performance, configuration or security situations that are identified. HPOM provides information which monitored objects are not healthy, sends alerts when problems are identified, and provides information to help you identify the cause of a problem and possible solutions. HPOM helps you do the following:

- Maximize the availability of network components.
- Reduce the time lost by end-users as a result of system downtime.
- Reduce unnecessary user actions by automatically solving problems.
- Reduce the number of problems through preventive actions.
- Decrease the time needed to solve problems.
- Reduce the cost of managing the client-server environment.

HPOM is a scalable and flexible solution that can be configured to meet the requirements of any information technology (IT) organization and its users. System administrators can expand the applications of HPOM by integrating management applications from HPOM partners or other vendors.

For more information on HPOM, see the HPOM documentation, located at:  
<http://support.openview.hp.com/selfsolve/manuals>

## About Data Protector

HP Data Protector is a backup solution that provides reliable data protection and high accessibility for your fast-growing business data. Data Protector offers comprehensive backup and restore functionality specifically tailored for enterprise-wide and distributed environments. The major Data Protector features are:

- Scalable and highly flexible architecture
- Mixed environment support

- Easy central administration
- High performance backup
- Easy restore
- Data and control communication security
- High availability support
- Automated or unattended operation
- Monitoring, reporting, and notification
- Service management
- Integration with online database applications
- Integration with other products

For more information on Data Protector, see the Data Protector documentation, located at:  
<http://support.openview.hp.com/selfsolve/manuals>

## About Data Protector Smart Plug-in

Data Protector Smart Plug-in (Data Protector SPI) is an availability and performance management solution that extends the end-to-end service monitoring capabilities of HP Operations Manager to include the Data Protector infrastructure. It fully integrates topology, health, and performance data into the HP Service Navigator, providing the end-to-end operations overview across the entire Data Protector environment and enabling delivery of effective business service management.

Data Protector SPI provides the following major features:

### **Discovery and visualization**

- Automatic discovery and visualization of the Data Protector environment using topology view and health perspectives.
- Centralized monitoring of the Data Protector infrastructure (multiple Cell Managers) via the HP Service Navigator.

### **Health, availability, and performance monitoring**

- Monitoring of the Data Protector environment health and state from connectivity issues to utilization, load, and availability.
- Detection of performance degradation before it affects end users.

### **Monitoring Data Protector components and tasks**

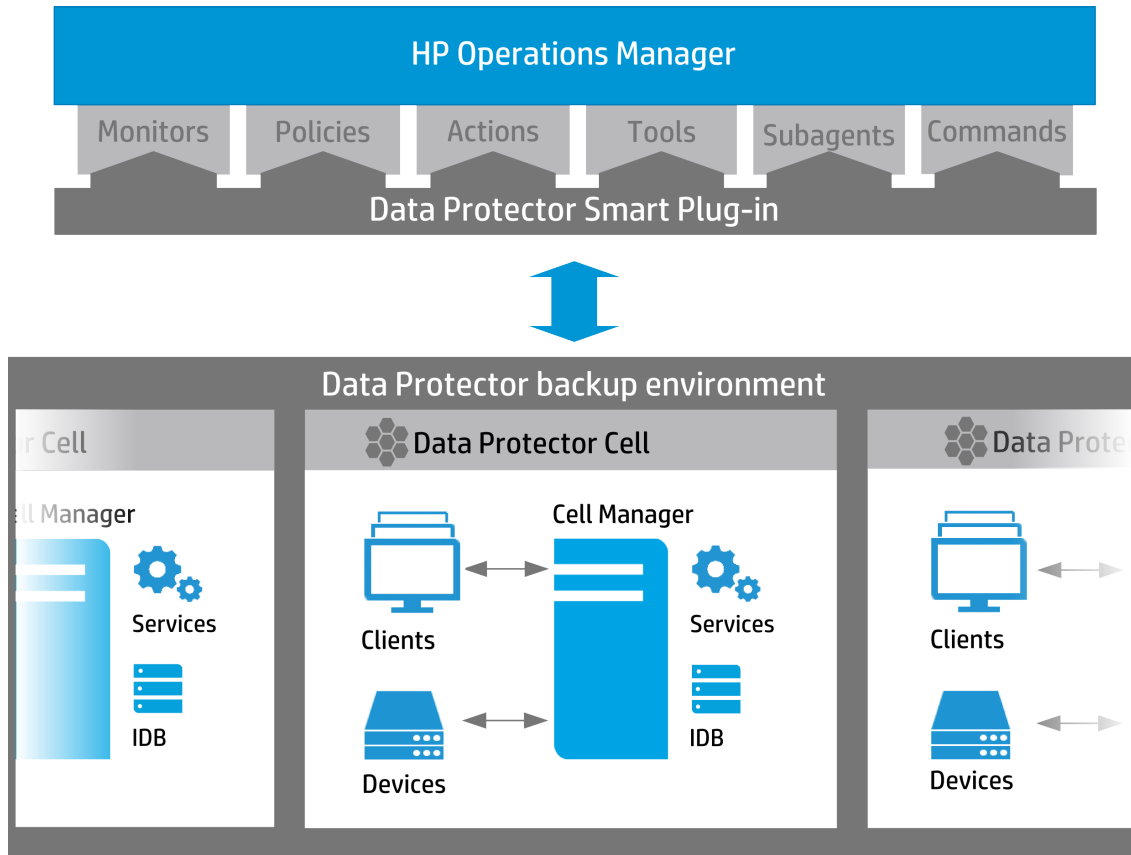
- Automatic detection of the Data Protector cell and its parts, such as servers (Cell Managers), services, clients, virtual environments, devices.
- Monitoring of the Data Protector backup sessions.
- A central data repository for storing event records and action records for all Data Protector managed nodes.

### **Problem identification and resolving mechanism**

- Generating messages according to different availability, performance, configuration, or security problems and sorting them by users-profiles, so that the users see only messages they need..
- Providing information that can help you identify the cause of a problem and possible solutions with instructions.
- Automatic actions that address frequent Data Protector operations.

## Product Architecture

The following high-level diagram displays how Data Protector SPI connects to the HP Operations Manager and Data Protector infrastructure.





# Chapter 2: Installation and Configuration

This chapter summarizes procedures to install and configure the Data Protector SPI on the HPOM and the Data Protector sides:

1. Check system requirements. For more information, see "[Installation Requirements](#)" below.
2. Before installing Data Protector SPI, add Data Protector Cell Managers as managed nodes to the HPOM environment and then install the HPOM agent on the Data Protector Cell Manager that you want to monitor. If you installed an HPOM agent to monitor this system before, you can also use it for the Data Protector SPI. For detailed procedures, see "[Adding Data Protector Cell Manager as a Managed Node](#)" on the next page and "[Installing HP Operations Agent on the Data Protector Cell Manager](#)" on the next page.
3. Install the Data Protector SPI. For a detailed procedure, see "[Installing Data Protector SPI on HPOM Management Server](#)" on page 11.
4. Assign the Data Protector SPI profiles to the users that will use the Data Protector SPI functionality. For a detailed procedure, see "[Assigning Data Protector SPI User Profiles](#)" on page 11.
5. Distribute the Data Protector SPI configuration to the HPOM managed nodes with the Data Protector Cell Managers. For a detailed procedure, see "[Distributing Data Protector SPI Configuration to the Cell Managers](#)" on page 12.

## Installation Requirements

For detailed information on HP Operations Manager and Data Protector including hardware and software requirements, operating systems support, installation and configuration procedures, see the product related documentation at: <http://support.openview.hp.com/selfsolve/manuals>

Before you start with Data Protector SPI installation, make sure that the following requirements are met:

- HP Operations Manager for Linux 9.xx is installed and configured.
- The supported versions of the Data Protector Cell Managers that you want to monitor are 7.xx, 8.xx, and 9.0x.
- The Data Protector Cell Managers that you want to monitor are installed on the Microsoft Windows or Linux operating systems.
- Make sure, that the HPOM agent is supported on the operating systems where Data Protector Cell Managers are installed.
- On the Data Protector Cell Managers that you want to monitor, a user account with administrator's rights exists. This account is used during the Data Protector SPI installation.

- **On Linux:** Check that the local root user is in the Data Protector admin user group.
- **On Windows:** Add the local HPOM account user to Data Protector admin user group.

## Adding Data Protector Cell Manager as a Managed Node

For detailed and up-to-date information on the HP Operations Manager related procedures including hardware and software requirements, operating systems support, installation and configuration procedures, see the product related documentation at:

<http://support.openview.hp.com/selfsolve/manuals>

Perform this procedure for every Data Protector Cell Manager that you want to monitor using HPOM.

1. Log in to the HPOM Administration UI as user `admin`.
2. Click the **HPOM** icon in the tool bar to set the data context to HPOM for UNIX Configuration.
3. In the Edit menu, click **Add Node**.
4. In the Add Node window, select the Node type depending on the operating system of the Data Protector Cell Manager, which you are adding as a managed node. Then enter the label and hostname of the new node, click **Save**.

## Installing HP Operations Agent on the Data Protector Cell Manager

For detailed and up-to-date information on the HP Operations Manager related procedures including hardware and software requirements, operating systems support, installation and configuration procedures, see the product related documentation at:

<http://support.openview.hp.com/selfsolve/manuals>

If you used the HPOM agent to monitor the managed nodes with the Data Protector Cell Manager installed, you can use this agent also for the Data Protector SPI. If the HPOM agent is already installed, skip this procedure and continue with the Data Protector SPI installation. See "[Installing Data Protector SPI on HPOM Management Server](#)" on the next page.

To discover the Data Protector Cell Managers in HPOM, install the HPOM agent on the Cell Manager that you want to monitor using the Data Protector SPI. You should perform this procedure for every Data Protector Cell Manager that you want to monitor using HPOM.

1. Log in to the HPOM Administration UI as user `opc_admin`.
2. Click the **HPOM** icon in the tool bar to set the data context to HPOM for UNIX Configuration.
3. In the Deployment menu, click **(De)Install Agent**.
4. In the (De)Install Agent window, select the **Installation** Install type.

Then, specify the managed nodes with the Data Protector Cell Manager where you want to install the HPOM agents. You can do this by typing in the node hostname in the Nodes text box or by clicking the [...] button to browse for the available managed nodes, which you can then select as destinations for the new agent installation. The nodes you select appear in a list in the Nodes box.

Click **Preinstall Check**.

5. Verify the summary for the agent installation, enter the password for the user whose account will be used to perform the installation, update, or removal and then click **Install on Selected Nodes**. Agent installation starts. You can review the installation status by clicking the **Agent Installation Logs** link.

Make sure that the messages from this managed node arrive to the HPOM management server.

## Installing Data Protector SPI on HPOM Management Server

Run the installation of the Data Protector SPI on the HPOM management server.

1. Log in to the HPOM management server as `root`.
2. Insert the Data Protector SPI installation DVD-ROM or mount the ISO image.
3. In the command-line console, run the following command:

```
# rpm -ivh hdpdspi-9.00.x86_64.rpm
```

After the installation completes, the following changes occur on HPOM management server:

- Data Protector SPI service is created: `hpdaprotector`
- Data Protector SPI related files and folders are located at: `/opt/hdpdspi/`

## Assigning Data Protector SPI User Profiles

During the installation, two Data Protector SPI specific user profiles are created, HP DP Administrator and HP DP Operator. These profiles grant the Data Protector and Data Protector SPI

specific rights and responsibilities to the users they are assigned to. The user profiles grant access to the following tool groups:

- HP DP Administrator:


HP Data Protector

HP Data Protector SPI

- HP DP Operator:

HP Data Protector SPI

Assign the Data Protector SPI specific user profiles to the users that will use the Data Protector SPI functionality.

1. Log in to the HPOM Administration UI as user `admin`.
2. Click the **HPOM** icon in the tool bar to set the data context to HPOM for UNIX Configuration.
3. In the Browse menu, click **All User Profiles**.
4. In the All User Profiles window, locate one of the Data Protector SPI specific user profile (HP DP Administrator or HP DP Operator).
5. Click the actions button () and select **Assign to user/profiles...**
6. In the Selector dialog, select the users, to which you want to assign the profile and then click **OK**.

The profile is assigned to the selected users.

## Distributing Data Protector SPI Configuration to the Cell Managers

Distribute the Data Protector SPI configuration to the HPOM managed nodes with the Data Protector Cell Managers using the HPOM Java GUI.

1. Log in to Java GUI as user `opc_adm`.
2. In the Object Pane, expand **Holding Area**, then expand **Nodes**, and select the nodes, to which you want to distribute the Data Protector SPI configuration.
3. Right-click the selected nodes and select **Start -> HP Data Protector -> SPI -> Add Cell Manager**.
4. Expand Services, then right-click **HP Data Protector**, and select nodes and select **Start -> Update service tree**.

After the task completes, the HPOM managed nodes are added to the HP DP nodes group, the following files and folders are created on the HPOM managed nodes with Cell Managers:

**On Windows:**

- *%ProgramFiles%\HP\HP BTO Software\bin\win64\dpspi*
- *%ProgramData%\HP\HP BTO Software\bin\win64\dpspi*

**On Linux:** */opt/OV/bin/dpspi/*

## What's Next?

After you installed Data Protector SPI, you can continue with the following:

- Start using the product. You can use it without a license for 60 days. For Data Protector SPI specifics, see "[Data Protector SPI Discovery and Monitoring](#)" on page 19.
- Purchase the Data Protector SPI permanent license. For licensing related tasks, see "[Licensing](#)" on page 15.

## Chapter 3: Removing Data Protector SPI

To completely remove Data Protector SPI from your HPOM environment you should remove it from the HPOM managed nodes and from the HPOM management server.

1. Remove the Data Protector SPI configuration from the managed nodes. Perform this procedure for each managed node
  - a. Log in to Java GUI as user `opc_admin`.
  - b. In the Object Pane, expand the **Nodes** hierarchy and select the node, from which you want to remove the Data Protector SPI configuration.
  - c. Right-click the selected node and select **Start -> HP Data Protector -> SPI -> Remove Cell Manager**.
2. Remove the Data Protector SPI from the HPOM management server.
  - a. Log in to the HPOM management server as `root`.
  - b. In the command-line console, run the following command:

```
# rpm -e hpdp-spi
```

# Chapter 4: Licensing

After you installed and configured Data Protector SPI on the HPOM management server, you can start using it immediately. An Instant-On password is built in the product when first installed. You are able to use the software for 60 days and buy a permanent license within this period. If you don't buy a permanent license, only a limited functionality will be available after 60 days.

## How Licensing Works

Data Protector SPI provides the `LicTool.exe` licensing tool to request and monitor Data Protector SPI licenses for your monitored environment. The `LicTool` licensing tool is distributed to each Data Protector Cell Manager during the installation procedure and can be found at the following location:

- **On Windows:** `%ProgramFiles%\HP\HP BTO Software\bin\win64\dpspi`
- **On Linux:** `/opt/OV/bin/dpspi/`

You can run the `LicTool` licensing tool using the following options:

To generate a license request file:

```
--generate-request productId requestfilename company
```

To verify if the Data Protector SPI license is valid and is applicable for the current system:

```
--check-license productId licensefilename
```

To verify the license format and to view the content of the Data Protector SPI license:

```
--read-license productId licensefilename
```

where:

*productId* is the abbreviated product name, `dpspi` for Data Protector SPI.

*requestfilename* is the name of the request file with the `DAT` extension, for example, `dpspi_license_request.dat`.

*company* is your company name.

*licensefilename* is the name of the license file you received from the licensing portal, `license.dat`.

### Prerequisite

You have already bought the Data Protector SPI license and have an entitlement order.

Perform the following licensing tasks on *each* Data Protector Cell Manager that you want to monitor:

1. Configure a license request. See ["Configuring License Requests" on the next page](#).
2. Request and obtain licenses from the web licensing portal. See ["Requesting and Retrieving](#)

Licenses" on the next page "Configuring License Requests" below.

3. Activate the licenses to start using Data Protector SPI. See "Activating Licenses" on the next page.
4. You can always verify the licensing related information. See "Verifying Licenses" on the next page.

**Note:** If you add a new Cell Manager after performing all licensing tasks, you should repeat the whole licensing procedure for this newly added Cell Manager.

When you do not want to monitor any of the Cell Managers with the Data Protector SPI license deployed, you can remove the license from this Cell Manager and use it later on other systems. See "Removing Licenses from the Monitored System" on the next page.

## Configuring License Requests

To request your Data Protector SPI licenses, run the following command on the Data Protector Cell Manager that you want to monitor:

```
LicTool --generate-request productId requestfilename company
```

**For example:**

```
LicTool --generate-request dpspi CM1_license_request.dat LITEHOUSE
```

Example of the CM1\_license\_request.dat license request file:

```
CN MyCompany  
PID dpspi  
ND LITEHOUSE  
HSUD DB2FBE444DE05E2AB9CB899AD92D269C  
NEXT NODE
```

## Requesting and Retrieving Licenses

After you created a license request file, you can obtain the licenses from the licensing portal. Perform the following steps for every Data Protector Cell Manager that you want to monitor:

1. Connect to the web licensing portal at: <http://hp-licensing.comtrade.com>
2. If you already have a licensing portal account, click **Sign in**, enter your user name and password, and then click **Login**. Otherwise, create an account and then sign in with a newly created user account.
3. Click the **License Activation** link and then enter the Entitlement Order in the text box. Click



**Next.**

4. Select **HP Data Protector Smart Plug-in**, browse for your license request file, and then click **Send Request**.

Within a few minutes, you should receive an email with a license activation file `dpspi_licact_new.dat` attached.

## Activating Licenses

After you submit your license request for Data Protector SPI licenses to the web licensing portal, you get an email with a product license activation file (`license.dat`) attached. To activate the licenses, copy this file to the following location on the Data Protector Cell Manager that you want to monitor:

- **On Windows:** `%ProgramFiles%\HP\HP BTO Software\bin\win64\dpspi`
- **On Linux:** `/opt/OV/bin/dpspi/`

## Verifying Licenses

To check the state of your Data Protector SPI license and verify whether it is valid for the current Cell Manager, run the following command the Data Protector Cell Manager:

```
LicTool --check-license productId requestfilename
```

**For example:**

```
LicTool --check-license dpspi license.dat
```

To verify whether the license format is valid and to view the content of your Data Protector SPI license, run the following command on the Data Protector Cell Manager:

```
LicTool --read-license productId requestfilename
```

Example of the Data Protector SPI license file:

```
Node: HRIB  
Company: LITEHOUSE  
Is valid: Yes  
Days to expire: 99999  
License type: Permanent  
Num licenses: 1  
Action: None
```

## Removing Licenses from the Monitored System

You can remove a license from the Cell Manager using the web licensing portal.

1. Connect to the web licensing portal at: <http://hp-licensing.comtrade.com>
2. Sign in to the web licensing portal.
3. Click the **License Redesignation** link and follow the instructions to complete the procedure.

The system will automatically process your request and send you the updated licensing information by email. You can later use the released licenses on other Cell Managers that you want to monitor.

# Chapter 5: Data Protector SPI Discovery and Monitoring





The functionality of the Data Protector SPI is comparable to the functionality of other smart plug-ins used with HPOM. You can monitor and manage Data Protector environment from the HPOM Java GUI. For more information on using HPOM Java GUI, see the *HPOM Java UI Operator's guide*.









This chapter describes specifics of the Data Protector SPI features set and advises on available configuration options. The following topics are described:

- ["Discovered Objects" below](#).
- ["Data Protector SPI Tools" on the next page](#).
- ["Data Protector SPI Actions" on page 23](#).
- ["Data Protector SPI Messages" on page 23](#).

## Discovered Objects

Data Protector SPI discovers the object types described in the following table:

Icon	Object Type	Description
	Data Protector cell	A set of systems that are under the control of a Cell Manager. Central control is available to administer the backup and restore policies and tasks.
	Data Protector Cell Manager	The main system in the cell where the essential Data Protector software is installed and from which all backup and restore activities are managed. Each cell has one Cell Manager system.
	Data Protector IDB	The Data Protector Internal Database. IDB is an embedded database located on the Cell Manager and keeps information regarding which data was backed up, to which media it was backed up, how backup, restore, and other sessions were run, which devices, libraries, and disk arrays are configured, and so on.
	Data Protector client	Any system configured with any Data Protector component and configured in a cell.

Icon	Object Type	Description
	Hypervisor host	ESX(i) Server system or Hyper-V system configured within the Data Protector Virtual Environment integration. To check the hypervisor type, right-click the icon and then select <b>Instance properties</b> . The application server type <code>esx</code> or <code>hyperv</code> is specified.
	Managing software for virtual environment	VMware vCloud Director or VMware vCenter Server that manages resources (datacenters, resource pools, virtual machines) in the VMware virtual environment within the Data Protector Virtual Environment integration.
	VMware datacenter	An organizational unit that consists of one or more ESX(i) Server systems and the related storage for virtual machines (datastores) and that is configured within the Data Protector Virtual Environment integration.
	VMware resource pool	A VMware resource pool (the aggregated physical compute hardware allocated to virtual machines) configured in a VMware virtual infrastructure within the Data Protector Virtual Environment integration.
	Virtual machines	Virtual machines configured within the Data Protector Virtual Environment integration.
	Data Protector devices	A device configured for use with Data Protector, which can write data to and read data from storage media.
	Data Protector services	Data Protector services: Cell Request Server (CRS), Inet, Application Server (HPDP AS), IDB connection pool (IDBCP).
	Data Protector services	Data Protector services: Key Management Server (KMS), License Service (LIC), Media Management Daemon (MMD).

## Data Protector SPI Tools

Besides the default tools available within HPOM, Data Protector SPI provides the Data Protector specific tools. The Data Protector specific tools are visible in the **Tools -> HP Data Protector** hierarchy, in the Java GUI Object pane. For the ease of use, the tools are logically distributed into tool groups of different object types. For more information on using tools, see the *HPOM Java UI Operator's guide*.

To start a tool from the Object Pane, expand the Tool hierarchy and then click the needed tool. To start a tool from a specific object, right-click the object and then select **Start->Tools->HP Data Protector -> tool group -> tool of your choice**. To start a tool that requires input parameters (for example, Cell Manager hostname), right-click the tool or the object and select **Start Customized...** Such tools can be recognized by three dots ("...") in the name, for example, `Import Client...`

If you start a tool from a specific object, consider to start the tool from the related object group. For example, if you start a tool from a device, the tool should be of a Devices tool group; if you start a tool from a client, the tool should be of a Clients tool group. However, the tools of the Services and Reports tool groups, can be started from any object.

See a list of the Data Protector specific tasks, their short descriptions, and other related information in the following table:

Tool groups and tools	Description
<b>Clients</b>	
Client Backup Report	Provides all end-user backup related information for the selected client.
Client statistics	Lists the clients from the selected cell and their backup related statistics, such as backup size, number of objects, backup success rate, and so on.
Disable Client Updates	Disables the Data Protector SPI agent to update the client's health status. Note, when disabled, the client's health status is always OK (green).
Enable Client Updates	Enables the Data Protector SPI agent to update the client's health status.
Export Client	Exports the client from the cell. This enables you to remove a client from the cell without uninstalling its Data Protector components.
Import Client...	Imports the client to a cell. This allows you to move a client between two cells without reinstalling the Data Protector components.
Get Session Report	Provides the session report for the last backup session.
Patch Status	Lists Data Protector patches installed on the Data Protector clients.
Restart Backup	Restarts the last failed backup session.
<b>Devices</b>	
Cancel Mount Request	Cancels the mount request and stops the backup session.
Confirm Mount Request	Confirms the mount request to continue the backup session. A medium should be inserted into device.
Show Unused Devices	Lists the configured destination devices that are not used for backup, object copy, or object consolidation.
<b>Reports</b>	
Show Cell Information	Shows the Data Protector cell related information (number of clients, backup specifications, Media Management server, Licensing service).

<b>Tool groups and tools</b>	<b>Description</b>
Show IDB Size	Provides a table that contains information about the MMDB, CDB, archived log files, datafiles, and information for DCBF and SMBF.
Show Licensing Information	Lists all licenses and the available number of licenses.
<b>Services</b>	
Check DP Services	Checks whether the services on the Cell Manager are running properly by running the <code>omnisv -status</code> command.
Check IDB Health	Checks the entire IDB with the exception of the SMBF and displays the summary of the check.
Start Services	Starts the services on the Cell Manager by running the <code>omnisv -start</code> command.
Stop Services	Stops the services on the Cell Manager by running the <code>omnisv -stop</code> command.
Restart Services	Stops the services on the Cell Manager by running the <code>omnisv -stop</code> command and then starts them by running the <code>omnisv -start</code> command.
<b>SPI</b>	
Add Cell Manager	Adds Data Protector Cell Manager as a managed node to the HPOM environment.
Get Agent Settings	Provides the information on configuration settings of the Data Protector SPI agent (specified intervals, thresholds, and so on) running on the selected Cell Manager.
Remove Cell Manager	Removes the Data Protector Cell Manager, which you do not want to monitor anymore, from the HPOM environment.
Set Agent Debug...	Specifies the debug related settings, such as debug level: 'ERROR', 'WARN', 'INFO' (default), 'DEBUG', or 'DUMP', debug size: in KB, MB (default), GB, TB, or PB), and the debug log filename (by default, <code>dspiagt.log</code> ). Note, when the debug size is exceeded, the "old" suffix is added to the debug filename and a new debug file is created.
Set Discovery Interval...	Specifies interval for discovering topology (by default, 15 min).
Set Event Interval...	Specifies interval for sending messages on Data Protector specific events (by default, 3 min).
Set Health Interval...	Specifies interval for checking health of discovered objects (by default, 5 min).

Tool groups and tools	Description
Set Health RPO...	Specifies the recovery point objective. After the specified number of days (by default, 7 days) without successful backup for a particular client is exceeded, a message is sent.
Set Monitor Interval...	Specifies interval for sending Data Protector SPI specific messages listed in " <a href="#">Data Protector SPI Messages</a> " below (by default, 3 min).
Set RPO Error Threshold...	Specifies percentage of clients with failed backups before a message of the <code>Major</code> severity is sent (by default, 60).
Set RPO Warning Threshold...	Specifies percentage of clients with failed backups before a message of the <code>Minor</code> severity is sent (by default, 40).
Set Service Tree Update Mode...	Specifies the service tree update mode: <code>manual</code> - no messages about topology change, operator must update service tree manually, <code>auto</code> - update service tree automatically if topology changes, <code>notify</code> (default) - only sends message about topology change, <code>periodic</code> - update service tree every interval seconds
Set Service Tree Update Interval...	In case of periodic update mode (by default, 12 h), specifies the service tree update interval.
Show Agent Status	Shows the Data Protector SPI agent status (running or not running) and processes.
Start Agent	Starts the Data Protector SPI agent.
Start Agent	Stops the Data Protector SPI agent.

## Data Protector SPI Actions

Besides the default actions available within HPOM, Data Protector SPI provides a specific one. To start the Data Protector SPI specific action from the Object Pane, expand the Services hierarchy, right-click **HP Data Protector**, and select **Update Service Navigator Graph**.

### Update Service Navigator Graph

Updates the Service Navigator Graph with the latest data. Use this action every time when you change the configuration, for example, add new Cell Managers.

## Data Protector SPI Messages

Besides the default messages available within HPOM, Data Protector SPI provides the Data Protector specific ones. For each Data Protector specific message, a knowledge article (instructions) is provided. If you want to view instructions for a specific object, in the Java GUI

Message browser, select the associated message, right-click on it, and then click the **Instructions** tab.

Data Protector SPI messages are acknowledged automatically.

See a list of the Data Protector specific product knowledge articles below:

## Data Protector Service Status - Generic

### Summary

A Data Protector service (CRS, IDBCP, Omnilnet) set to automatic start is not currently running.

### Causes

A service can stop for many reasons, including:

- The service was stopped by an administrator.
- The service was prevented from starting because the user account could not be authenticated.
- The service encountered an exception that stopped it.
- The service was configured inappropriately, which prevented it from starting.
- Another service that this service is dependent on was stopped.

### Resolutions

You can try to restart the service by stating the `Start DP Services` tool from the `Tools -> HP Data Protector -> Services` hierarchy.

## Data Protector Service Status - LIC

### Summary

The Data Protector licensing or some licensing related information is not covered.

### Causes

Licensing check can fail for the following reasons:

- Some licensing related information is not covered. For example, license server is not available or some licenses are missing.
- Some unexpected licensing related information is encountered.

### Resolution

Run the `omnicc -check_licenses` command on the Data Protector Cell Manager to see the specific reasons for the sent messages in the command output.

### External Knowledge Sources

For more information, see the *HP Data Protector Installation and Licensing Guide* located at:



<http://support.openview.hp.com/selfsolve/manuals>

## Data Protector Service Status - IDB

### Summary

Any of the following Data Protector IDB status and consistency parameters is unavailable or inconsistent:

- database connection
- database schema consistency
- datafiles consistency
- DCBF presence and size

### Causes

Any of the verified IDB parameters is unavailable or inconsistent.

### Resolutions

Run the `omnidbcheck` command on the Data Protector Cell Manager to see the exact reasons for the issued errors in the command output.

### External Knowledge Sources

For more information, see the *HP Data Protector Command Line Interface Reference* located at:

<http://support.openview.hp.com/selfsolve/manuals>

## Data Protector Client Backup Status

### Summary

Monitoring is not started for this client, the status of the last backup is unknown, or no policy is defined for this configuration. In the Data Protector virtual environments, this applies to the status of the ESX(i) Server systems, Microsoft Hyper-V systems, vCloud Director systems and vCenter Server systems.

### Causes

There was an error during the last backup on this client. In the Data Protector virtual environments, error state is caused by errors during the last backup of the VMware datacenter, VMware resource pool, or virtual machines residing on the ESX(i) Server systems and Microsoft Hyper-V systems or being managed by vCloud Directors and vCenter Servers.

### Resolutions

Find out the cause of the unhealthy state by starting the `Get Session Report` tool from the `Tools -> HP Data Protector -> Clients` hierarchy (right-click on the tool and select **Start customized...**).

### External Knowledge Sources

For more information, see the *HP Data Protector Troubleshooting Guide* located at:

<http://support.openview.hp.com/selfsolve/manuals>

## Data Protector Client Recovery Point Objective

### Summary

The configured recovery point objective for this client is exceeded, monitoring is not started for this client, the status of the last successful backup is unknown, or no policy is defined for this configuration.

### Configuration

The default RPO value is 7 days. You can override this value (number of days) by starting the Set Health RPO... tool from the Tools -> HP Data Protector -> SPI hierarchy (right-click on the tool and select **Start customized...**).

### Causes

The configured recovery point objective for this client is exceeded. This means that there is no successful backup for this client in the specified number of days.

### Resolutions

Troubleshoot and fix the problem for this client and perform a successful backup of this client.

### External Knowledge Sources

For more information, see the *HP Data Protector Troubleshooting Guide* located at:

<http://support.openview.hp.com/selfsolve/manuals>

## Data Protector Cell Client Group Backup Status

### Summary

The configured thresholds (allowed percentage of the failed client backups) are exceeded, monitoring is not started for this client group or no policy is defined for this configuration.

### Configuration

There are two configurable thresholds for this policy:

- **Warning Threshold** – Specifies percentage of clients with failed backups before a message of the **Minor** severity is sent. Default value: 40
- **Error Threshold** – Specifies percentage of clients with failed backups before a message of the **Major** severity is sent. Default value: 60

You can override this values (percentage) by starting the Set RPO Error Threshold... or Set RPO Warning Threshold... tool from the Tools -> HP Data Protector -> SPI hierarchy (right-click on the tool and select **Start customized...**).

### **Causes**

The configured thresholds (allowed percentage of the failed client backups) are exceeded.

### **Resolutions**

Troubleshoot and fix the problem in the backup environment.

### **External Knowledge Sources**

For more information, see the *HP Data Protector Troubleshooting Guide* located at:

<http://support.openview.hp.com/selfsolve/manuals>

## **Data Protector Device Mount Request**

### **Summary**

Mount request is issued for this device during the backup session.

### **Causes**

Mount request is issued, when one or more media are missing in the device, which is used for the currently running backup session.

### **Resolutions**

To continue the backup session, follow these steps:

1. View the Data Protector Events to identify the device with missing media.
2. Insert one or more media to the device.
3. Confirm the mount request by starting the Confirm Mount Request tool from the Tools -> HP Data Protector -> Devices hierarchy.

To stop the backup session, start the Cancel Mount Request tool from the Tools -> HP Data Protector -> Devices hierarchy.

## **Data Protector Device Operational State**

### **Summary**

An error is issued for the monitored device.

### **Causes**

An error for the monitored device can be issued for such reasons as poor condition of media in the device or dirty drive.

### **Resolutions**

Troubleshoot and fix the device related problem in the backup environment.

### **External Knowledge Sources**

For more information, see the *HP Data Protector Troubleshooting Guide* located at:

<http://support.openview.hp.com/selfsolve/manuals>

## Data Protector Smart Plug-in License Validation

### Summary

The Data Protector SPI license for a Data Protector Cell Manager is not available or is not valid.

### Causes

The problem may occur for the following reasons:

- You did not obtain a valid Data Protector SPI license from the web licensing portal.
- You did not deploy the Data Protector SPI license to the Cell Manager.

### Resolutions

Check whether you obtained a valid Data Protector SPI license for the Data Protector Cell Manager and deployed it appropriately. For licensing related procedures, see "[Licensing](#)" on page 15.

### Additional Information

Every Data Protector Cell Manager, which you want to monitor using the Data Protector SPI, can be used without a license for 60 days. If you want to continue monitoring Cell Manager with the Data Protector SPI, you should buy a permanent license.

## We appreciate your feedback!

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

**Feedback on User's Guide (Data Protector Smart Plug-in 9.00)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to [AutonomyTPFeedback@hp.com](mailto:AutonomyTPFeedback@hp.com).