Hewlett Packard
Enterprise

Data Protector Management Pack

Software Version: 10.00
Microsoft Windows operating systems

User's Guide

Document Release Date: June 2017
Software Release Date: June 2017

Legal notices

Warranty

The only warranties for Hewlett Packard Enterprise Development LP 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. HPE 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 HPE 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

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 software updates, go to https://softwaresupport.hpe.com/patches.

To verify that you are using the most recent edition of a document, go to https://softwaresupport.hpe.com/manuals.

This site requires that you register for an HPE Passport and sign in. To register for an HPE Passport ID, go to https://hpp12.passport.hpe.com/hppcf/login.do.

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

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 software updates, go to https://downloads.autonomy.com/productDownloads.jsp.

To verify that you are using the most recent edition of a document, go to https://softwaresupport.hpe.com/group/softwaresupport/search-result?doctype=online help.

This site requires that you register for an HPE Passport and sign in. To register for an HPE Passport ID, go to https://hpp12.passport.hpe.com/hppcf/login.do.

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

For information and details about the products, services, and support that HPE Software offers, contact your

Client Director.

Support

Visit the HPE Software Support Online web site at https://softwaresupport.hpe.com.

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

HPE 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
- Access product documentation
- Manage support contracts
- Look up HPE 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 HPE Passport user and sign in. Many also require a support contract.

To register for an HPE Passport ID, go to https://hpp12.passport.hpe.com/hppcf/login.do.

To find more information about access levels, go to https://softwaresupport.hpe.com/web/softwaresupport/access-levels.

Visit the HPE Software Support Online web site at https://softwaresupport.hpe.com.

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

HPE 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
- Access product documentation
- Manage support contracts
- Look up HPE 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 HPE Passport user and sign in. Many also require a support contract.

To register for an HPE Passport ID, go to https://hpp12.passport.hpe.com/hppcf/login.do.

To find more information about access levels, go to https://softwaresupport.hpe.com/web/softwaresupport/access-levels.

To check for recent software updates, go to https://downloads.autonomy.com/productDownloads.jsp.

To check for recent updates or to verify that you are using the most recent edition of a document, contact your Client Director.

Contents

Chapter 1: Introduction

This chapter introduces the Data Protector Management Pack and explains how it interacts with System Center Operations Manager and HPE Data Protector.

About System Center Operations Manager

System Center Operations Manager (SCOM), a component of Microsoft System Center, is a cross-platform data center management system that helps you monitor services, devices, and operations for many systems from a single console. Using SCOM, 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. SCOM 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.

For more information on Operations Manager, see the Microsoft System Center related documentation.

About Data Protector

HPE 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: https://softwaresupport.hpe.com/manuals

About Data Protector Management Pack

Data Protector Management Pack (Data Protector MP) is an availability and performance management solution that extends the end-to-end service monitoring capabilities of Microsoft System Center Operations Manager to include the Data Protector infrastructure. It fully integrates topology, health, and performance data into the Microsoft System Center Operations Manager console, providing the end-to-end operations overview across the entire Data Protector environment and enabling delivery of effective business service management.

Data Protector MP 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 via the Microsoft System Center Operations Manager console.

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

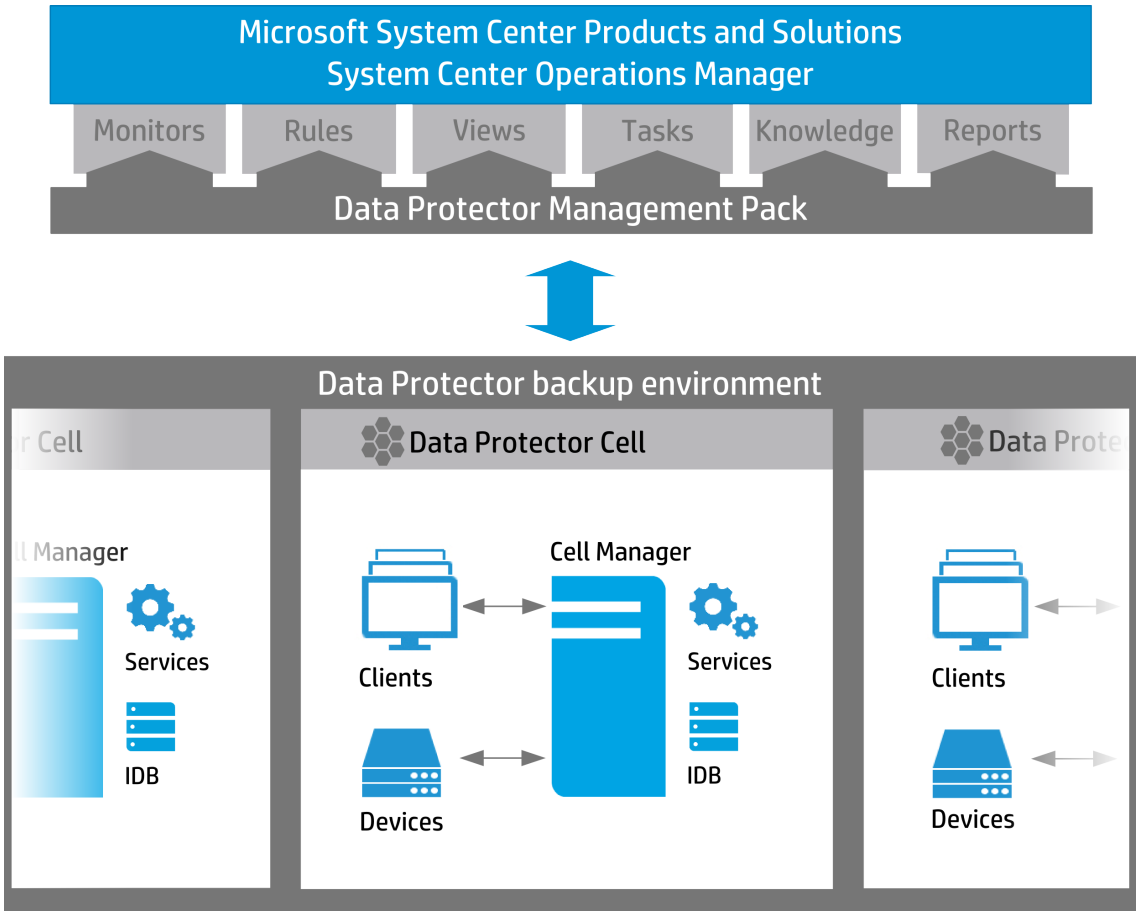
- Automatic detection of the Data Protector cell and its parts, such as servers (Cell Managers), services, clients, virtual environments, devices.
- Monitoring of the Data Protector backup sessions.

Problem identification and resolving mechanism

- Generating alerts according to different availability, performance, configuration, or security problems.
- Providing information that can help you identify the cause of a problem and possible solutions.
- Automatic actions that address frequent Data Protector operations.

Product Architecture

The following high-level diagram displays how Data Protector MP connects to the System Center Operations Manager management platform and Data Protector infrastructure.


Microsoft System Center Products and Solutions
System Center Operations Manager
Monitors
Rules
Views
Tasks
Knowledge
Reports
Data Protector Management Pack
Data Protector backup environment
Data Protector Cell
Cell Manager
Services
IDB
Clients
Devices
Data Prote
Clients
Devices

Chapter 2: Installation and Configuration

This chapter summarizes procedures to install and configure the Data Protector MP on the SCOM and the Data Protector sides:

1. Check system requirements. For more information, see Installation Requirements, below.
2. Install the Data Protector MP on the SCOM management server. For a detailed procedure, see Installing Data Protector MP on the SCOM Management Server, on the next page.
3. Import the Data Protector MP to SCOM. For a detailed procedure, see Importing Data Protector MP to SCOM, on the next page.
4. Install the SCOM agent on the Data Protector Cell Manager that you want to monitor. If you installed a SCOM agent to monitor this system before, you can also use it for the Data Protector MP. For a detailed procedure, see Installing SCOM Agent on the Data Protector Cell Manager, on page 13.
5. Install the Data Protector MP agent on a Data Protector Cell Manager to enable sending data from a Data Protector cell to SCOM. For a detailed procedure,see Installing Data Protector MP Agent on the Data Protector Cell Manager, on page 15.

Installation Requirements

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

- System Center Operations Manager is installed and configured.

  For supported version, see the *Data Protector Management Pack Support Matrix* at: https://softwaresupport.hpe.com/manuals
- The supported versions of the Data Protector Cell Managers that you want to monitor are: 8.1x, 9.xx, and 10.00.

  For information on the Data Protector hardware and software requirements as well as installation procedure, see the Data Protector documentation at: https://softwaresupport.hpe.com/manuals
- The Data Protector Cell Managers that you want to monitor are installed on Microsoft Windows Server 2008, Microsoft Windows Server 2012, and Microsoft Windows Server 2016.
- .NET 3.5 is installed on the Data Protector Cell Managers that you want to monitor.
- 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 MP installation. For information on the Data Protector users configuration, see the Data Protector documentation at: https://softwaresupport.hpe.com/manuals

Installing Data Protector MP on the SCOM Management Server

To install the Data Protector MP on the SCOM management server, perform the following steps:

1. Log in to the SCOM management server with an account that is a member of the Operations Manager Administrators role.
2. Insert the Data Protector MP installation DVD-ROM or mount the ISO image.
3. Follow the installation wizard to install the package.
4. After you completed the wizard, the following files and folders are created on the system:
   - *%ProgramFiles%*\Hewlett Packard Enterprise\Data Protector MP
   - *%ProgramData%*\Hewlett Packard Enterprise\Data Protector MP

Importing Data Protector MP to SCOM

For the up-to-date instructions about importing a management pack, see the web page How to Import a Management Pack in Operations Manager and follow the **Importing from disk** related procedure.

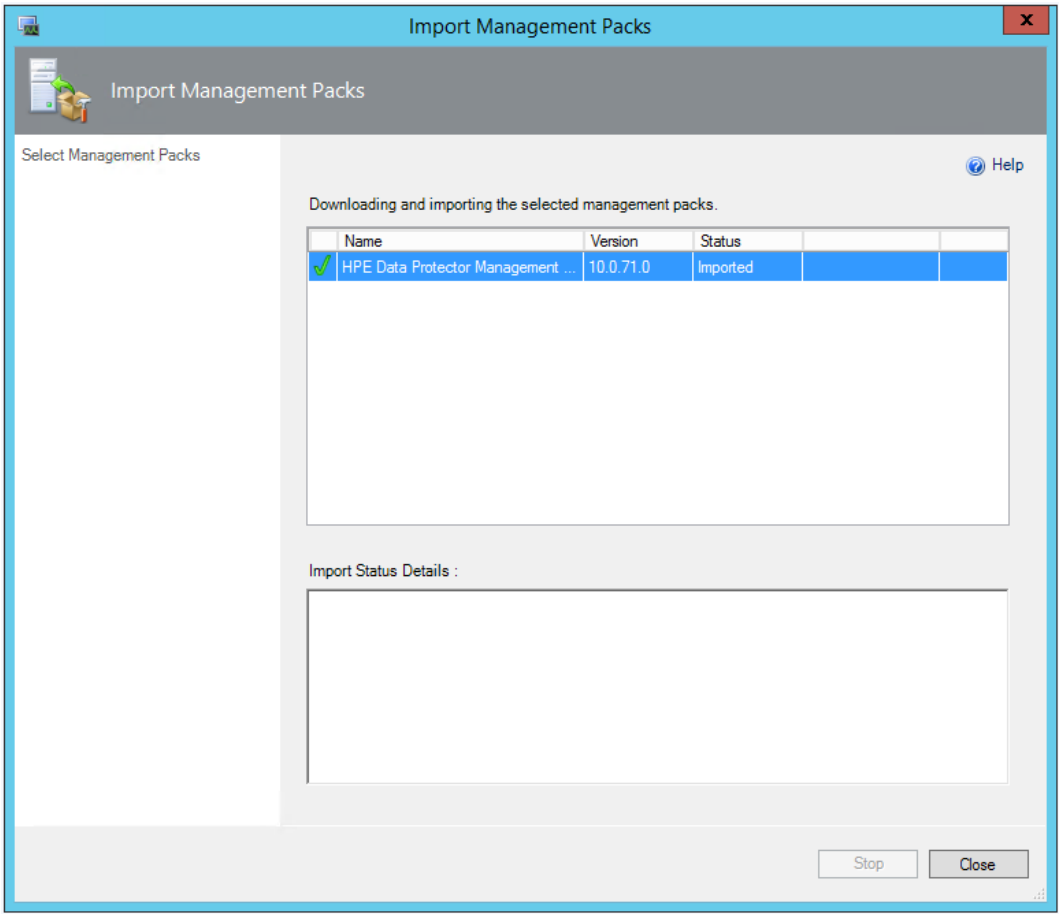
To import the Data Protector MP to SCOM, perform the following steps:

1. Log in to the SCOM management server with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Administration**.
3. Right-click **Management Packs**, and then click **Import Management Packs**.
4. The Import Management Packs wizard opens. Click **Add**, and then click **Add from disk**.

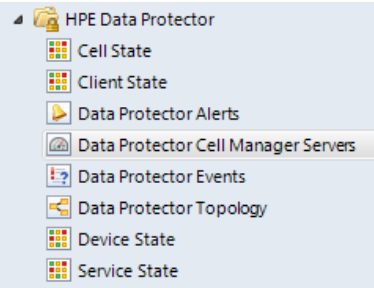
   When prompted to search the online catalog for dependencies, click **No**.
5. The Select Management Packs to import dialog box appears. Locate and select the Data Protector MP and click **Open**. The default location of the Data Protector MP is:

   %ProgramFiles%\Hewlett Packard Enterprise\Data Protector MP \ManagementPacks\SCOM2012\HPE.DataProtector.mp
6. On the Select Management Packs page, select Data Protector MP and click **Install**.
7. The Import Management Packs page appears and shows the progress. If there is a problem at any stage of the import process, select the management pack to view the status details. When the Import process is complete, the status of the management pack changes to **Imported**. Click

Close.



After the import procedure is complete, the following elements are visible in the Monitoring view of the System Center Operations Manager console:



Installing SCOM Agent on the Data Protector Cell Manager

If you used the SCOM agent to monitor the system with the Data Protector Cell Manager installed, you can use this agent also for the Data Protector MP. If the SCOM agent is already installed, skip this

procedure and continue with the Data Protector MP agent installation. See Installing Data Protector MP Agent on the Data Protector Cell Manager, on the next page.

Prerequisite

A user account with administrator's rights should be created on the Data Protector Cell Manager, where you want to install the SCOM agent. For information on the Data Protector users configuration, see the Data Protector documentation at: https://softwaresupport.hpe.com/manuals

> **IMPORTANT:** If you want to monitor the Cell Manager installed on cluster, you need to perform discovery for all cluster nodes with the installed Cell Manager.

To discover the Data Protector Cell Managers in SCOM and install the SCOM agent on the Cell Manager that you want to monitor using the Data Protector MP, perform the following steps:

1. Log in to the SCOM management server with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Administration**. In the navigation pane, expand **Device Management** and select **Agent Managed**.
3. At the bottom of the navigation pane, click **Discovery Wizard** to discover the Data Protector Cell Managers where you want to install the Data Protector MP agent. Follow the procedure on the Microsoft System Center website in the article: To install an agent on a computer running Windows by using the Discovery Wizard.

   Make sure to perform the following steps as they are specified below:

   a. On the Auto or Advanced? page, select **Advanced discovery**.
   b. In the Computer and Device Classes list, select **Servers and Clients**.
   c. On the Administrator Account page, select **Other user account**, type the user name and password, and then select the domain from the list. Click **Discover**.

      > **NOTE:**
      > Use the user account with administrator's rights that created on the Data Protector Cell Manager where you want to install the SCOM agent.

   The discovered Cell Managers are listed in the Results Area.
4. Select the devices you want to manage. Ensure that the management mode is set to `Agent`. Click **Next**. Finish the wizard.
5. Right-click the Cell Manager where you want to install the Data Protector MP agent and select **Properties**.
6. In the Properties dialog box, click the **Security** tab and select the following agent proxy security setting: `Allow this agent to act as a proxy and discover managed objects on other computers`.

   > **NOTE:** In the Cell Manager cluster, ensure that the `Allow this agent to act as a proxy and discover managed objects on other computers` proxy is configured for all cluster nodes.

Installing Data Protector MP Agent on the Data Protector Cell Manager

Prerequisite

A user account with administrator's rights should be created on the Data Protector Cell Manager, where you want to install the Data Protector MP agent. For information on the Data Protector users configuration, see the Data Protector documentation at: https://softwaresupport.hpe.com/manuals

To install the Data Protector MP agent, perform the following steps:

1. In the Operations console, click **Monitoring**.
2. In the navigation pane, locate **Data Protector Cell Manager Servers**, select the Data Protector Cell Manager, where you want to install the Data Protector MP agent, and then run the **Install DPMP Agent** task.

   > **IMPORTANT:** If you want to monitor the Cell Manager installed on cluster, you need to install Data Protector MP Agent on all cluster nodes with the installed Cell Manager.

   When the task is finished, the `Agent Installed` status of the Cell Manager changes from `false` to `true`.

After the installation is complete, the following changes occur on the Data Protector Cell Manager:

- In Windows Control Panel > Programs and Features:
  `HPE Management Pack Agent for HPE Data Protector`
- New files and folders:
  `%ProgramFiles%``\Hewlett Packard Enterprise\Data Protector MP Agent\MPDPMonitorSvc.exe`
- New service: HPE `MPDP Agent`

What's Next?

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

- Start using the product. You can use it without a license for 60 days. For Data Protector MP specifics, see Data Protector MP Discovery and Monitoring, on page 24.
- Purchase the Data Protector MP permanent license. For licensing related tasks, see Licensing, on page 19.

Chapter 3: Upgrading Data Protector MP

To upgrade Data Protector MP from the previous version, perform the following steps:

1. Upgrade the Data Protector MP from the previous version on the SCOM management server:
   a. Log in to the SCOM management server with an account that is a member of the Operations Manager Administrators role.
   b. Insert the Data Protector MP installation DVD-ROM or mount the ISO image.
   c. Follow the installation wizard to upgrade the Data Protector MP.
   d. After you completed the wizard, the upgrade is performed.
2. Import a new version of the Data Protector MP. The procedure is the same as if you import the management pack for the first time. The Data Protector MP is upgraded to a new version during the import procedure. See Importing Data Protector MP to SCOM, on page 12.
3. Upgrade Data Protector MP Agents on the Data Protector Cell Managers. The procedure is the same as if you install a Data Protector MP Agent on the Data Protector Cell Manager for the first time:
   a. In the Operations console, click **Monitoring**.
   b. In the navigation pane, locate **Data Protector Cell Manager Servers**, select the Data Protector Cell Manager, where you want to install the Data Protector MP agent, and then run the **Install DPMP Agent** task.

When the upgrade is finished, you can see the new version features after a discovery.

Chapter 4: Removing Data Protector MP

To completely remove Data Protector MP from your SCOM environment, perform the following procedures:

1. Removing the Data Protector MP Agent from the Cell Manager, below.
2. Removing the Data Protector MP from the SCOM Console, below.

Removing the Data Protector MP Agent from the Cell Manager

You can remove the Data Protector MP agent from a Data Protector Cell Manager using the SCOM console or locally, from the Cell Manager where it is installed.

To remove the Data Protector MP agent using the SCOM console, perform the following steps:

1. Log in to the SCOM management server with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Monitoring**. In the navigation pane, locate **Data Protector Cell Manager Servers**, select the Data Protector Cell Manager, from which you want to remove the Data Protector MP agent, and then start the **Uninstall DPMP Agent** task.

Alternatively, you can remove the Data Protector MP agent locally on the Cell Manager system. Perform the following steps:

1. In the Windows Control Panel > Programs and Features, locate Hewlett Packard Enterprise MPDP Agent.
2. Right-click **Hewlett Packard Enterprise MPDP Agent** and then click **Uninstall**.

   A warning dialog may appear informing you that other users are logged on to this computer. The program might not be removed completely, if another user is running it.Click **Continue**.
3. Follow the Data Protector MP Install Shield Wizard to remove the product.

After the task is complete, the following is removed from the Data Protector Cell Manager:

- In Windows Control Panel > Programs and Features the following program is not visible:
  `Hewlett Packard Enterprise MPDP Agent`
- The files and folders created during the installation are deleted. Note, that the generated files, such as log files or data files can remain on the system.
- The `HPEMPDPAgent` service is not present on the system.

Removing the Data Protector MP from the SCOM Console

To remove the Data Protector MP from the SCOM console, perform the following steps:

1. Log in to the SCOM management server with an account that is a member of the Operations Manager Administration role.
2. In the Operations console, click **Administration** and then click **Management Packs**.
3. In the Management Packs pane, right-click the **Data Protector MP** and then click **Delete**.

Chapter 5: Licensing

After you installed and configured Data Protector MP on the SCOM 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

Use the Data Protector MP Licensing Tool located on the SCOM management server to request and manage the Data Protector MP license for your monitored environment.

Prerequisite

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

Perform the following licensing tasks:

1. Configure a license request. See Configuring License Requests, below.
2. Request and obtain licenses from the web licensing portal. See Requesting and Retrieving Licenses, on the next page.
3. Activate the licenses to start using Data Protector MP. See Activating Licenses, on page 21.
4. Update the license information on the monitored Cell Managers. See Updating License Information on the Monitored Systems, on page 22.
5. You can always verify the licensing related information. See Verifying Licenses, on page 22.

> **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 MP 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 page 23.

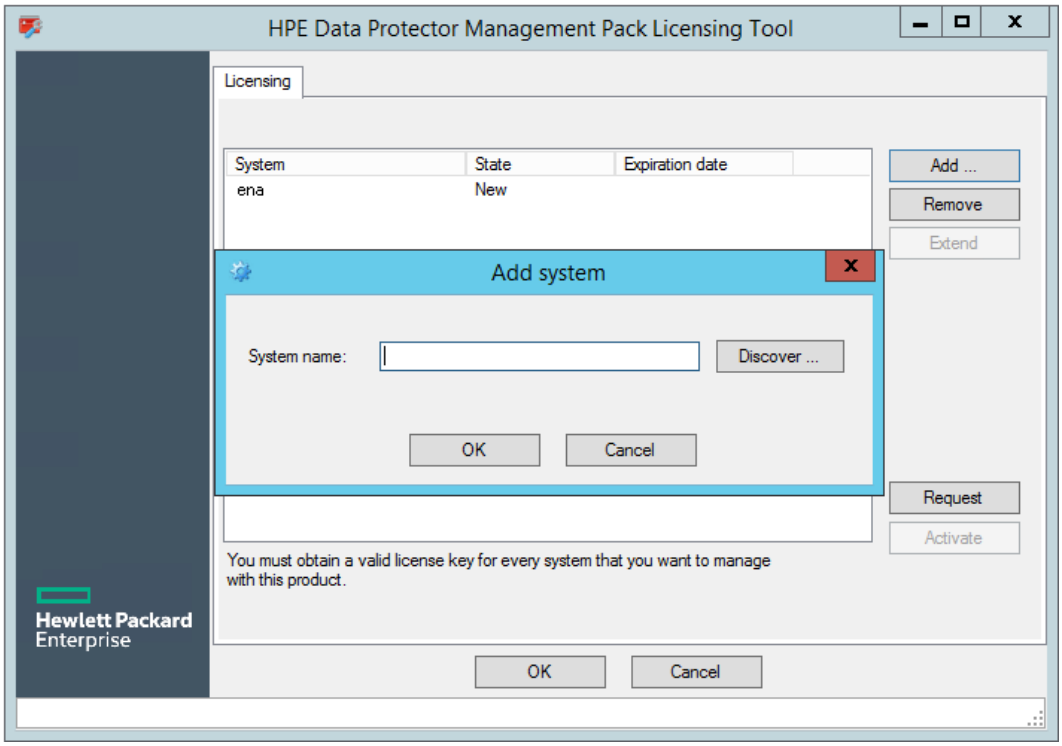
Configuring License Requests

To obtain a Data Protector MP license, submit a request form to the web licensing portal located at: http://hp-licensing.comtrade.com

To request your Data Protector MP licenses, perform the following steps:

1. On the SCOM management server, use the Start menu to navigate to Programs > Hewlett Packard Enterprise > Data Protector Management Pack > Licensing Tool.
2. Click **Licensing Tool**.
3. In the Data Protector Management Pack Licensing Tool, click **Add** to add a system to the license request list.

4. In the Add system dialog, you can do one of the following:
   - Enter the Cell Manager name manually and then click **OK** to add the system to a list.
   - Click **Discover** to get a list of systems, for which you can send a license request. In the Discovered systems dialog, select the discovered systems that you want to add to the license request list and then click **OK**.



5. In the Data Protector Management Pack Licensing Tool, click **Request**, enter your company name, and then click **OK**.

   A message box appears, specifying the location of the `dpmp_license_requests.dat` license request file for the discovered Cell Managers. The state of the systems in the list changes to `Requested`.

   Example of the `dpmp_license_requests.dat` license request file:

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

Requesting and Retrieving Licenses

After you created a license request file, perform the following steps to obtain the licenses:

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.

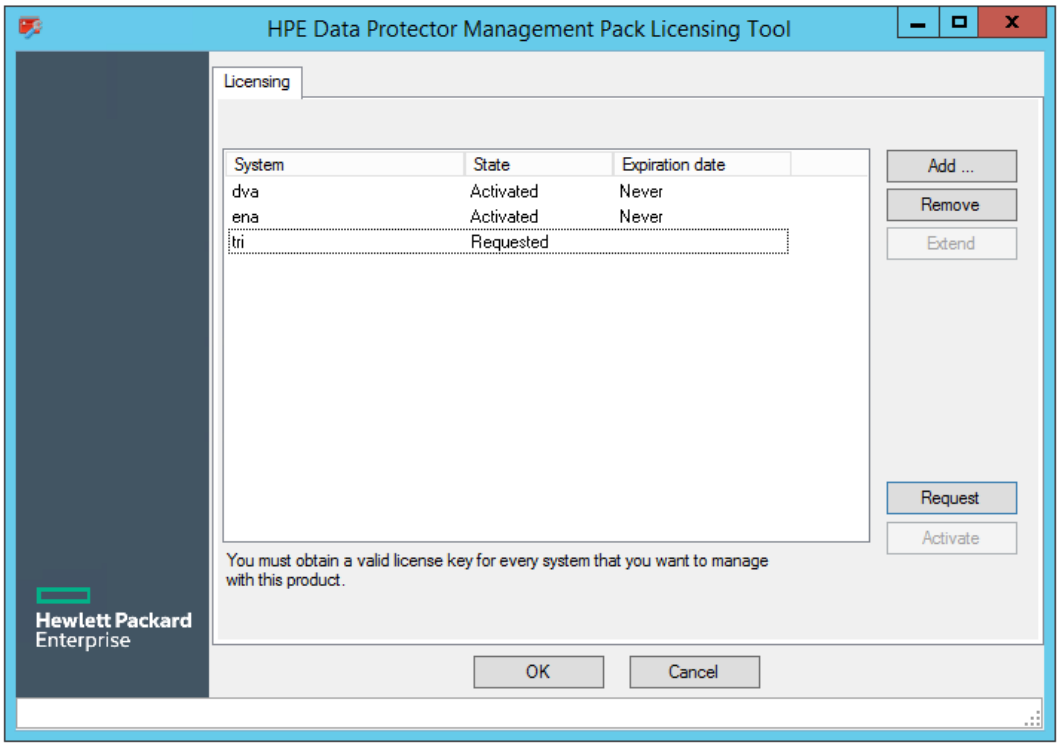
3. Click the **License Activation** link and then enter the Entitlement Order in the text box. Click **Next**.
4. Select **HPE Data Protector Management Pack**, browse for your license request file, and then click **Send Request**.

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

Activating Licenses

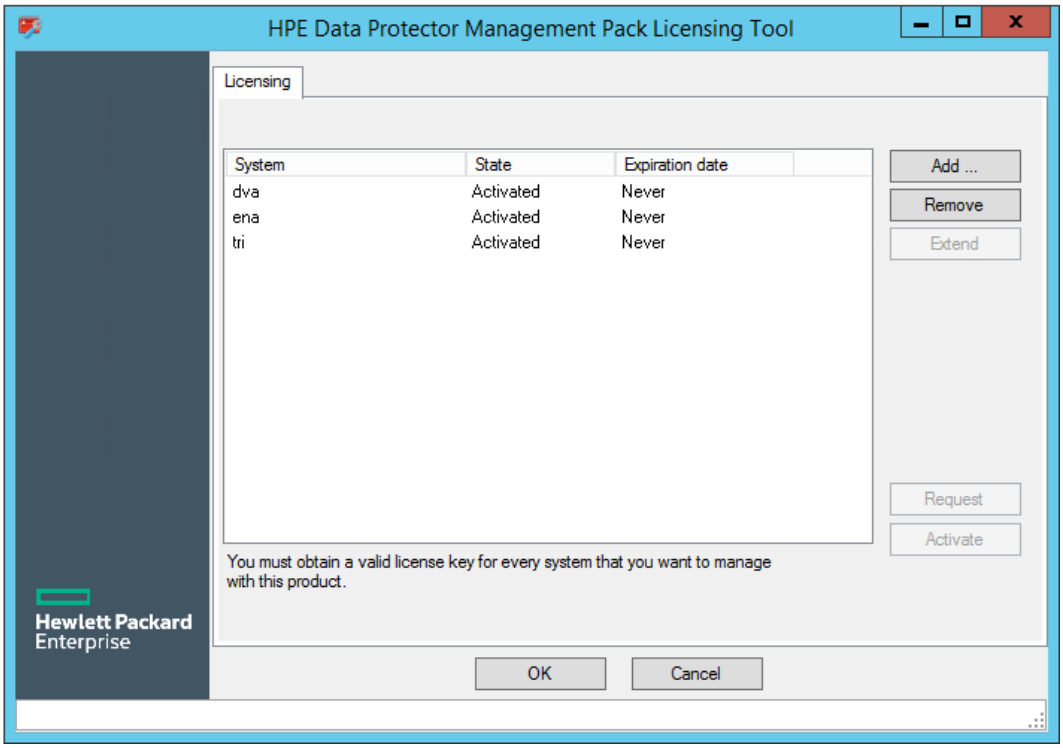
After you submit your license request for Data Protector MP licenses to the web licensing portal, you get an email with a product license activation file attached. To activate the licenses, perform the following steps:

1. On the SCOM management server copy the license activation file `dpmp_licact_new.dat` to *`%ProgramData%`*`\Hewlett Packard Enterprise\MPShare\Data Protector MP`.
2. Use the Start menu to navigate to **Programs > Hewlett Packard Enterprise > Data Protector Management Pack > Licensing Tool**.
3. Click **Licensing Tool**.



NOTE:
If the Activate button is not enabled, make sure that you completed step 1.

4. Click **Activate**. A confirmation of a successful license activation appears. Click **OK**.



Updating License Information on the Monitored Systems

As you deployed the Data Protector MP agent to a Cell Manager before the licensing procedure, you should update the license information on all monitored systems. Otherwise, the Data Protector MP will not collect any information from the system with the installed Data Protector MP agent. Deploy the license files from the SCOM management server to make them effective on the monitored Cell Managers. Perform the following steps:

1. Log in to the SCOM management server with an account that is a member of the Operations Manager Administrators role.
2. In the Operations console, click **Monitoring**. In the navigation pane, locate **Data Protector Cell Manager Servers**, select the Data Protector Cell Manager, where you want to update the license information, and then start the **Update DPMP Agent License** task.

Verifying Licenses

You can check the state of your licenses at any time by starting the Data Protector MP Licensing Tool on the SCOM management server:

Use the Start menu to navigate to **Programs > Hewlett Packard Enterprise > Data Protector Management Pack > Licensing Tool**.

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 6: Data Protector MP Discovery and Monitoring

The functionality of the Data Protector MP is comparable to the functionality of other management packs used with the SCOM environment. This chapter describes specifics of the Data Protector MP features set and advises on available configuration options. The following topics are described:

Discovered Objects

Data Protector MP 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.
	Hypervisor host	Hyper-V system configured within the Data Protector Virtual Environment integration. To check the hypervisor type, right-click the icon and then select **Instance properties**. The application server type `hyperv` is specified.
	Hypervisor host	ESX(i) Server system configured within the Data Protector Virtual Environment integration. To check the hypervisor type, right-click the icon and then select **Instance properties**. The application server type `esx` is specified.

Icon	Object Type	Description
	Management host 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 MP Tasks

Besides the default tasks available within SCOM, Data Protector MP provides the Data Protector specific tasks. The Data Protector specific tasks are visible in the Monitoring context of the SCOM console, and depend on the monitor you are currently viewing. You can start a task from a respective monitor.

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

Task	Description	Location
Install MPDP Agent	Installs the Data Protector MP agent on the Data Protector Cell Managers, which you want to monitor. Parameters:`Upgrade=False|True` If `True`, the installed agent is upgraded to a newer version. If `False`, the installed agent is uninstalled and a new agent version is installed.	Data Protector Cell Manager Servers monitor > Cell Servers item
Uninstall MPDP	Removes the Data Protector MP agent from the Data	

Task	Description	Location
Agent	Protector Cell Managers, which you do not want to monitor anymore.	
Update MPDP Agent License	Updates the license information on the monitored Cell Managers with the Data Protector MP agent installed.	
Check Dependent NT Services	Checks the state of the services, which the target service depends on.	Data Protector Cell Manager Servers monitor > Agent Service State item
Set Agent Debugging	Enables or disables the Data Protector MP agent to write debug output into a log file. Enables debug level, directory, and the debug log suffix.	
Start NT Service	Starts Windows service.	
Stop NT Service	Stops Windows service.	
Update Agent Configuration	Enables the SCOM user to set time intervals for discovery, event check cycles, and health check cycles.	
Disable Client Updates	Disables the Data Protector MP agent to update the client's health status. Note, when disabled, the client's health status is always OK (green).	Client State monitor
Enable Client Updates	Enables the Data Protector MP agent to update the client's health status.	
Patch Status	Lists Data Protector patches installed on the Data Protector clients.	
Restart Backup	Restarts the last failed backup session. Parameters: `RestartSession=False|True` If `True`, session is resumed from where it failed. Supported only for `WinFS|Filesystem|Oracle8`. For other applications, an error is returned. If `False`, session starts from the beginning.	
Get Session Report	Provides the session report for the last backup session.	
Export Client	Exports the client from the cell. This enables you to remove a client from the cell without uninstalling its Data Protector components.	
Client Backup Report	Provides all end-user backup related information for the selected client.	
Confirm Mount Request	Confirms the mount request to continue the backup session. A medium should be inserted into device.	Device State monitor

Task	Description	Location
Cancel Mount Request	Cancels the mount request and stops the backup session.	
Get Device Error Report	Provides a report for the device with an error occurred.	
Check Service Status	Checks whether the services on the Cell Manager are running properly by running the `omnisv -status` command.	Server State monitor
Import Client	Imports the client to a cell. This allows you to move a client between two cells without reinstalling the Data Protector components.	
Show Cell Information	Shows the Data Protector cell related information (number of clients, backup specifications, Media Management server, Licensing service).	
Show Database Report	Checks the consistency of the Data Protector internal database (IDB) and displays the summary of the check.	
Show Unused Devices	Lists the configured destination devices that are not used for backup, object copy, or object consolidation.	
Start Service	Starts the services on the Cell Manager by running the `omnisv -start` command.	
Stop Service	Stops the services on the Cell Manager by running the `omnisv -stop` command.	
Show Licensing Information	Lists all licenses and the available number of licenses.	Data Protector Topology monitor > locate and select the Licensing service (LIC)

Data Protector MP Monitors

Besides the default monitors available within SCOM, Data Protector MP provides the Data Protector specific monitors. For each Data Protector specific monitor, a knowledge article is provided. If you want to view monitors and knowledge articles for a specific object, select this object in the SCOM console, and open the SCOM Heath Explorer.

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

> **NOTE:**
> You cannot click the links to the SCOM tasks or views that are provided in the knowledge articles in the sections below, they are only for your information. You can use these links only

from the SCOM Health Explorer.

Data Protector Cell Server ComputerRole MPAgentInstallState Monitor

Summary

This monitor is a Data Protector Cell Manager Servers monitor. This monitor is in error state, if no Data Protector MP agent is installed on the discovered Data Protector Cell Manager system. An alert also appears in the Alert view.

Causes

The problem occurs, when a Data Protector Cell Manager is discovered from SCOM, but no Data Protector MP agent is installed on the Cell Manager system.

Resolutions

You can install the Data Protector MP agent on the discovered Data Protector Cell Manager by using the following task:

Install MPDP Agent

Data Protector Service Status Monitor - Generic

Summary

This monitor is a Data Protector service monitor. It checks the status of the following Data Protector services: CRS, IDBCP, OmniInet. If a service is set to automatic start and it is not currently running, an alert is raised. If the service is set to manual start or it is disabled, and it is not currently running, no alert is raised.

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 view all collected events for this service using the following link:

View all events

You can try to restart the service by using the following link:

Start the Service

Data Protector Service Status Monitor - LIC

Summary

This monitor is a Data Protector service monitor. It checks, whether the Data Protector licensing is covered or not. If the check succeeds, but some licensing related information is not covered, a warning is issued. If the check fails, an alert is raised.

Causes

A warning is issued, if some licensing related information is not covered. For example, license server is not available or some licenses are missing.

An alert is raised, when the check fails because of unexpected licensing related information.

Resolution

You can view all collected events for this service using the following link:

View all events

You can run the `omnicc -check_licenses` command on the Data Protector Cell Manager to see the specific reasons for the issued warnings or alerts in the command output.

External Knowledge Sources

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

https://softwaresupport.hpe.com/manuals

Data Protector Service Status Monitor - IDB

Summary

This monitor is a Data Protector service monitor. It checks the status and consistency of the Data Protector IDB. The following information is verified:

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

If any of these parameters is unavailable or inconsistent, an error is issued.

Causes

Any of the verified IDB parameters is unavailable or inconsistent.

Resolutions

You can view all collected events for this service using the following link:

View all events

You can 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 *HPE Data Protector Command Line Interface Reference* located at:

https://softwaresupport.hpe.com/manuals

Data Protector Client Backup Status Monitor

Summary

This monitor is a Data Protector client backup monitor. The monitor is in error state, if monitoring is not started for this client, the status of the last backup is unknown, or no monitor is defined for this monitor configuration. In the Data Protector virtual environments, this monitor applies to the status of the ESX (i) Server systems, Microsoft Hyper-V systems, vCloud Director systems, and vCenter Server systems.

Causes

This monitor is in error state, if there was any 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 virtual machines residing on the ESX(i) Server systems and Microsoft Hyper-V systems or being managed by vCloud Directors and vCenter Servers.You can view all current alerts from this client using this link:

View Alerts

Resolutions

You can find out the cause of the unhealthy state by using the following Data Protector task:

Get Session Report

External Knowledge Sources

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

https://softwaresupport.hpe.com/manuals

Data Protector Object Backup Status Monitor

Summary

This monitor is a Data Protector backup monitor for the virtual environment objects (VMware datacenter, VMware resource pool, and virtual machines). The monitor is in error state, if monitoring is not started for this object, the status of the last backup is unknown, or no monitor is defined for this monitor configuration.

Causes

This monitor is in error state, if there was any error during the last backup of this object. You can view all current alerts from this virtual machine using this link:

View Alerts

Resolutions

You can find out the cause of the unhealthy state by using the following Data Protector task:

Get Session Report

External Knowledge Sources

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

https://softwaresupport.hpe.com/manuals

Data Protector Client Recovery Point Objective Monitor

Summary

This monitor is a Data Protector client recovery point objective monitor. The monitor is in error state, if monitoring is not started for this client, the status of the last successful backup is unknown, or no monitor is defined for this monitor configuration.

Configuration

The default RPO value is 7 days. You can override this value by setting another number of days for the `Recovery Point Objective` parameter in the Override dialog.

Causes

This monitor is in unhealthy state, if 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.

View all current alerts from this client using this link:

View Alerts

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 *HPE Data Protector Troubleshooting Guide* located at:

https://softwaresupport.hpe.com/manuals

Data Protector Cell Client Group Backup Status Monitor

Summary

This monitor is a Data Protector client group monitor. The monitor is in error state, if monitoring is not started for this client group or no monitor is defined for this monitor configuration.

Configuration

There are several configurable thresholds for this monitor:

- `Warning Threshold` – Specifies percentage of clients with failed backups before monitor enters a `Warning` state. Default value: `40`
- `Error Threshold` – Specifies percentage of clients with failed backups before monitor enters an `Error` state. Default value: `60`
- `Accept Faulty Backups` – Specifies, whether the client with `Completed with errors` state

considered `Successful` or not.
Default value: `false`

Causes

This monitor is in error state, if the configured thresholds (allowed percentage of the failed client backups) are exceeded.

View all current alerts from this client using this link:

Data Protector Alerts

Resolutions

Troubleshoot and fix the problem in the backup environment.

External Knowledge Sources

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

https://softwaresupport.hpe.com/manuals

Data Protector Device Mount Request Monitor

Summary

This monitor is a Data Protector device state monitor. This monitor is in error state, if a 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 using the following task:

   Confirm Mount Request

To stop the backup session, use the following task:

Cancel Mount Request

Data Protector Device Operational State Monitor

Summary

This monitor is a Data Protector device state monitor. This monitor is in error state, if an error is issued for the monitored device.

Causes

An error for the monitored device can be issued for several reasons, for example, poor condition of media in the device or dirty drive.

Resolutions

Run the Device Error Report to get more information on the specific problem and then troubleshoot it accordingly. Use the following link:

Get Device Error Report

External Knowledge Sources

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

https://softwaresupport.hpe.com/manuals

Data Protector MP Rules

Besides the default rules available within SCOM, Data Protector MP provides the following specific rule:

Data Protector Management Pack License Validation Rule

Verifies the status of the Data Protector MP license for a Data Protector Cell Manager.

Summary

The Data Protector MP 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 MP license from the web licensing portal.
- You did not deploy the Data Protector MP license to the Cell Manager.

Resolutions

Check whether you obtained a valid Data Protector MP license for the Data Protector Cell Manager and deployed it appropriately. For licensing related procedures, see Licensing, on page 19.

Additional Information

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

Tuning Thresholds for Performance Monitors and Rules

Some monitors and rules have default thresholds that might need additional tuning to suite your environment. Evaluate the monitors and rules to determine whether the default thresholds are appropriate or should be adjusted to meet your specific needs. You can override such thresholds with new values.

Send documentation 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 Management Pack 10.00)

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.

We appreciate your feedback!