

# Hitachi Application Protector Quick Install & Configuration Guide for Oracle® Database Server

## FASTFIND LINKS

- Document organization
- Product version
- Getting help
- Table of contents

© 2014 Hitachi Data Systems Corporation. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for any purpose without the express written permission of Hitachi Data Systems Corporation.

Hitachi Data Systems Corporation reserves the right to make changes to this document at any time without notice and assumes no responsibility for its use. This document contains the most current information available at the time of publication. When new or revised information becomes available, this entire document will be updated and distributed to all registered users.

Some of the features described in this document might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Data Systems Corporation at <https://portal.hds.com>.

**Notice:** Hitachi, Ltd., products and services can be ordered only under the terms and conditions of the applicable Hitachi Data Systems Corporation agreements. The use of Hitachi, Ltd., products is governed by the terms of your agreements with Hitachi Data Systems Corporation.

Hitachi is a registered trademark of Hitachi, Ltd., in the United States and other countries. Hitachi Data Systems is a registered trademark and service mark of Hitachi, Ltd., in the United States and other countries.

Archivas, Essential NAS Platform, HiCommand, Hi-Track, ShadowImage, Tagmaserve, Tagmasoft, Tagmasolve, Tagmastore, TrueCopy, Universal Star Network, and Universal Storage Platform are registered trademarks of Hitachi Data Systems Corporation.

AIX, AS/400, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, ESCON, FICON, FlashCopy, IBM, Lotus, MVS, OS/390, RS/6000, S/390, System z9, System z10, Tivoli, VM/ESA, z/OS, z9, z10, zSeries, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

All other trademarks, service marks, and company names in this document or website are properties of their respective owners.

Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

**Notice Export Controls.** The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.



# Contents

## Contents

Preface . . . . .	V
Intended audience. . . . .	vi
Product version . . . . .	vi
Related documents . . . . .	vi
Document organization . . . . .	vi
Document revision level . . . . .	vii
Document conventions. . . . .	vii
Getting help . . . . .	viii
Comments . . . . .	viii
<b>1 Introduction . . . . .</b>	<b>1-1</b>
Application Protector overview . . . . .	1-2
Supported database server. . . . .	1-3
Configuring the Oracle database . . . . .	1-4
Oracle database configuration. . . . .	1-4
Configuring non-ASM Oracle database with LVM devices . . . . .	1-6
Configuring non-ASM Oracle database with multipath devices . . . . .	1-6
Supported storage arrays . . . . .	1-8
Firmware version for storage array . . . . .	1-8
Storage prerequisites . . . . .	1-8
VSP storage prerequisites. . . . .	1-9
HUS storage prerequisites . . . . .	1-11
Application Protector prerequisites . . . . .	1-12
System requirements . . . . .	1-12
Application Protector Server prerequisites . . . . .	1-13
Application Protector Server for SLES platform . . . . .	1-13
Application Protector Server for RHEL platform . . . . .	1-14
Application Protector Server for Solaris platform . . . . .	1-15

Application Protector Client prerequisites . . . . .	1-16
Application Protector Client for SLES platform . . . . .	1-16
Application Protector Client for RHEL platform . . . . .	1-16
Application Protector Client for Solaris platform . . . . .	1-17
<b>2 Installing Application Protector . . . . .</b>	<b>2-1</b>
Installing the Application Protector Server . . . . .	2-2
Application Protector Server installer syntax . . . . .	2-3
Installing the Application Protector Client . . . . .	2-5
Application Protector Client installer syntax . . . . .	2-6
Removing the Application Protector Server . . . . .	2-7
Removing the Application Protector Client . . . . .	2-8
<b>3 Configuring Application Protector . . . . .</b>	<b>3-1</b>
Accessing Application Protector . . . . .	3-2
Configuring the database service account . . . . .	3-2
Setting the database service account . . . . .	3-2
Modifying the database service account . . . . .	3-3
Service account user privileges . . . . .	3-3
Configuring the ASM service account . . . . .	3-4
Setting the ASM service account . . . . .	3-4
Modifying the ASM service account . . . . .	3-4
Licensing Application Protector . . . . .	3-5
Activating the Application Protector license . . . . .	3-5
Listing the Application Protector licenses . . . . .	3-6

## Glossary



# Preface

This document provides information about installing Hitachi Application Protector (Application Protector) for Oracle® Database Server (Oracle Database) on Linux® and Solaris® (Solaris) platform.

This chapter includes the following information:

- [Intended audience](#)
- [Product version](#)
- [Related documents](#)
- [Document organization](#)
- [Document revision level](#)
- [Document conventions](#)
- [Getting help](#)
- [Comments](#)

**Notice:** The use of all Hitachi Data Systems products is governed by the terms of the agreement(s) with Hitachi Data Systems.

## Intended audience

This document is intended for customers, application backup administrators, and Hitachi Ltd. partners involved in installing, configuring, and using Application Protector. Readers of this document should be familiar with the following:

- Oracle® Database administration
- Linux® and Solaris® operating system
- Storage administration
- Backup and recovery concepts

## Product version

This document revision applies to Hitachi Application Protector v1.2 release.

## Related documents

- *Hitachi Application Protector CLI Guide for Oracle® Database Server* MK-91HAP023-00
- *Hitachi Application Protector User Guide for Oracle® Database Server* MK-91HAP011-00
- *Hitachi Application Protector Troubleshooting Guide for Oracle® Database Server* FE-91HAP015-00

## Document organization

The following table provides an overview of the content and organization of this document. [Click the chapter title](#) in the first column to go to that chapter. The first page of every chapter contains a brief list of its content with links to the pages where the information is located.

Chapter title	Description
<a href="#">Chapter 1, Introduction</a>	Provides an introduction, installation requirements, supported databases and storage subsystems, and Application Protector prerequisites.
<a href="#">Chapter 2, Installing Application Protector</a>	Provides the details of installing and removing Application Protector Server and Client.
<a href="#">Chapter 3, Configuring Application Protector</a>	Provides information about mandatory configuration (first time) after installing Application Protector.
<a href="#">Glossary</a>	Defines acronyms and terms used in the document.

## Document revision level

This section provides a history of the revision changes in this document.



Revision	Date	Description
MK-91HAP013-00	July 2014	Initial release

## Document conventions

This document uses the following typographic conventions.

Convention	Description
<b>Bold</b>	Indicates text on a window, other than the window title, including menus, menu options, buttons, fields, and labels. Example: Click <b>OK</b> .
<i>Italic</i>	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: <i>copy source-file target-file</i> . <b>Note:</b> Angled brackets (< >) are also used to indicate variables.
screen/code	Indicates text that is displayed on screen or entered by the user. Example: # <code>pairdisplay -g oradb</code>
< > angled brackets	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: # <code>pairdisplay -g &lt;group&gt;</code> Note: <i>Italic</i> font is also used to indicate variables.
[ ] square brackets	Indicates optional values. Example: [a   b] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: {a   b} indicates that you must choose either a or b.
vertical bar	Indicates that you have a choice between two or more options or arguments. Examples: [a   b] indicates that you can choose a, b, or nothing. {a   b} indicates that you must choose either a or b.
<u>underline</u>	Indicates the default value. Example: [ <u>a</u>   b]

This document uses the following symbols to draw the attention to certain information.

Symbol	Meaning	Description
	Note	Note emphasize or supplement important points of the main text.
	WARNING	Warning indicate that failure to take a specified action could result in loss of data or serious damage to the hardware.

This document uses the following conventions for the support matrix.

Convention	Description
√	Features that are fully functional and available in Application Protector.
x	Features that are not functional or are not available in Application Protector.
-	Features that are not supported by Application Protector.

## Getting help

The Hitachi Data Systems customer support staff is available 24 hours a day, seven days a week.

If you need technical support, log on to the Hitachi Data Systems support portal for contact information: <https://hdssupport.hds.com>.

If you purchased this product from an authorized HDS reseller, contact that reseller for support. For the name of your nearest HDS authorized reseller, refer to the HDS support portal for locations and contact information.

## Comments

Your comments and suggestions to improve this document are greatly appreciated. Please send your comments on this document to [doc.comments@hds.com](mailto:doc.comments@hds.com). Include the document title, number, and revision. Please refer to specific sections and paragraphs whenever possible.

**Thank you!** (All comments become the property of Hitachi Data Systems.)



# Introduction

Hitachi Application Protector (Application Protector) is a snapshot-based backup and recovery software. It is based on client-server architecture. The Application Protector Client can be installed on the same or a remote server on the same network or accessible to the Application Protector Server network.

This chapter describes the following topics:

- ❑ [Application Protector overview](#)
- ❑ [Supported database server](#)
- ❑ [Supported storage arrays](#)
- ❑ [Application Protector prerequisites](#)

## Application Protector overview

Backup and storage administrators can use Application Protector to create snapshots of the storage logical units (LU)s hosting the supported Oracle® Database (Oracle Database). Application Protector facilitates creation of snapshots of the Oracle Database on the Linux and Solaris platform.

Application Protector uses the following approach:

1. Install and activate the Application Protector license, as applicable.
2. Register the supported storage arrays.
3. Configure the Application Protector Server, Client, and scripts as required.
4. Create snapshots. In addition, you can schedule snapshots.
5. Recover database and tablespace from the snapshots. In addition, you can revert database using a snapshot.
6. View progress and logs of the operations.

Application Protector supports the following.

- Register the supported Hitachi storage arrays.
- Set policy to configure snapshot retention count at server level.
- Create, list, modify, and delete snapshot schedules.
- Create, list, mount, unmount, and delete ShadowImage® (SI), Hitachi Thin Image (HTI), and Tree Clone snapshots.
- Restore, point-in-time (PIT), and complete recovery of the selected database at database or tablespace level.
- Revert snapshot of database.
- Native Device-Mapper Multipath environment for Red Hat® Enterprise Linux® (RHEL) and SUSE® Linux Enterprise Server (SLES) platform.
- Protect databases hosted on the Logical Volume Manager (LVM) devices for SLES platform.
- Supports Automatic Storage Management (ASM) setup on RHEL platform and non-ASM setups on SLES and Solaris platform.

Application Protector has a Java™ based graphical user interface (GUI) and command line interface (CLI).

## Supported database server

Application Protector supports the following versions of Oracle database on the supported operating system.

**Table 1-1: Supported Oracle database versions**

Operating system	32 bit	64 bit	Oracle database version
SLES 11 SP3	√	√	<ul style="list-style-type: none"> <li>Oracle® 10g Release 2 (10.2.0.4 and 10.2.0.5) (non-ASM)</li> <li>Oracle® 11g Release 2 (11.2.0.3 and 11.2.0.4) (non-ASM)</li> </ul>
	√	√	
<ul style="list-style-type: none"> <li>RHEL 5.7 (for ASM setups)</li> <li>RHEL 6.3 (for non-ASM setups<sup>1</sup>)</li> </ul>	√	√	<ul style="list-style-type: none"> <li>Oracle® 10g Release 2 (10.2.0.4 and 10.2.0.5) (ASM)</li> <li>Oracle® 11g Release 2 (11.2.0.3 and 11.2.0.4) (ASM and RAC-ASM)</li> </ul>
	√	√	
<ul style="list-style-type: none"> <li>Solaris 10 u11</li> <li>Solaris 11</li> </ul>	√	√	<ul style="list-style-type: none"> <li>Oracle® 10g Release 2 (10.2.0.4 and 10.2.0.5) (non-ASM) on Solaris 10 u11</li> <li>Oracle® 11g Release 2 (11.2.0.3 and 11.2.0.4) (non-ASM)</li> </ul>

1. For RHEL 6.3 platform, HNAS and Oracle 11gR2 is only supported.

## Configuring the Oracle database

This section provides details to configure Oracle database for various setups:

- ❑ [Oracle database configuration](#)
- ❑ [Configuring non-ASM Oracle database with LVM devices](#)
- ❑ [Configuring non-ASM Oracle database with multipath devices](#)

### Oracle database configuration

The following configurations are required after installing the Oracle database.

1. The Application Protector user must be in the Oracle user group.
2. The databases must be in open state.
3. The database instances must be running in the `ARCHIVELOG` mode.
4. The database data files must be on a different volume from database archive log, redo log, and control files.
5. For Oracle 11gR2 tablespace recovery, install Oracle® patch – 17011832. For details to install the patch, see [Installing the Oracle patch for tablespace recovery](#).



#### NOTE:

- For RHEL setup, in a database, the data files must not be in the same ASM diskgroup as control files or archive log file. Control files and archive log files can be on the same ASM diskgroup.
  - It is recommended to turn on the control file AUTOBACKUP feature.
  - The verbosity of the multipath daemon must not be changed by editing the multipath configuration file (`/etc/multipath.conf`). Use the default value (2).
- 

6. For RAC setups, during the database installation, single entry is written in `tnsnames.ora` with the database name. Application Protector checks the database status of the connected instance using SQL queries to list a database. This query fails if `tnsnames.ora` do not have an entry with the instance names. So, you must add one entry for each instance.

For example, if the database name is OORCL. To list database in Application Protector, add one entry for each instance of OORCL in `tnsmaes.ora` as follows.

```
OOORCL =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP) (HOST = Cal64-178-scan) (PORT
= 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
```

```

        (SERVICE_NAME = OORCL.hap.cal.hds.com)
    )
)

OORCL1 =
    (DESCRIPTION =
        (ADDRESS = (PROTOCOL = TCP) (HOST = Cal64-178-scan) (PORT
= 1521))
        (CONNECT_DATA =
            (SERVER = DEDICATED)
            (SERVICE_NAME = OORCL.hap.cal.hds.com)
            (INSTANCE_NAME = OORCL1)
        )
    )

OORCL2 =
    (DESCRIPTION =
        (ADDRESS = (PROTOCOL = TCP) (HOST = Cal64-178-scan) (PORT
= 1521))
        (CONNECT_DATA =
            (SERVER = DEDICATED)
            (SERVICE_NAME = OORCL.hap.cal.hds.com)
            (INSTANCE_NAME = OORCL2)
        )
    )

```

## Installing the Oracle patch for tablespace recovery

Install the Oracle 17011832 patch as follows.

1. Login to **My Oracle Support**, click **Patches & Updates**, provide **17011832**, and click the **Search** button. Click **17011832** in the left column for the platform and the Oracle version you need to install.
2. You must have **My Oracle Support** access to download the patch. If the patch does not show for the required platform and Oracle version combination, create a SR to request a patch.
3. You cannot apply the patch for 11.2.0.3 against an 11.2.0.4 installation. If the patch was not applied on 11.2.0.3, and then the database had the 11.2.0.4 patchset applied, apply the 11.2.0.4 version of the patch.
4. Patch for 11.2.0.4 on Linux x86-64 is available. For any other platform using 11.2.0.4, submit a patch request.

## Configuring non-ASM Oracle database with LVM devices

This section provides the mandatory details required while configuring non-ASM Oracle database with the LVM devices for SLES platform.

1. Create physical volumes (PVs) using any of the following type of devices:
  - a. SCSI Block Device  
For example: `/dev/sdx`
  - b. SCSI Block Device Partition  
For example: `/dev/sdx1`
  - c. Multipath device or partition. For details, see [Configuring non-ASM Oracle database with multipath devices](#).



**NOTE:** The physical device and multipath device can have only one partition.

---

2. A PV must be a part of a single volume group (VG) only.
3. Create only one logical volume (LV) for each VG.
4. The LV should not have any partitions (the ext3 filesystem must be created directly on the LV).
5. The DATA, REDO, and ARCHIVE files must reside on different LVs. For example, DATA on LV1 and VG1 and REDO on LV2 and VG2.

## Configuring non-ASM Oracle database with multipath devices

For RHEL and SLES platform, when configuring the non-ASM Oracle database with multipath devices, the following variations of multipath device configurations are supported:

1. A multipath device is mounted using any of the following representations:
  - a. WWID of the multipath device.  
For example: ``/dev/mapper/<wwid>``.
  - b. Friendly name for a multipath device, obtained by making an entry in the multipath configuration file (`/etc/multipath.conf`).  
For example: ``/dev/mapper/mpatha``.
  - c. Alias defined for a multipath device by making of an entry in the multipath configuration file (`/etc/multipath.conf`).  
For example: ``/dev/mapper/AliasName``.
2. A single partition created on a multipath device is mounted using any of the following representations:
  - a. WWID of the multipath device partition. For example: ``/dev/mapper/<wwid>_part1``.
  - b. Friendly name for the multipath device partition, obtained by making an entry in the multipath configuration file (`/etc/multipath.conf`).

For example: ``/dev/mapper/mpatha_part1``.

- c. Alias defined for the multipath device partition by making an entry in the multipath configuration file (`/etc/multipath.conf`).

For example: ``/dev/mapper/AliasName_part1``.



**WARNING!** Mounting snapshot fails for the following:

- Mounting the PVs as physical devices with the multipath daemon service in the running state.
  - Blacklisting the devices by adding an entry in the multipath configuration file (`/etc/multipath.conf`).
- 



**NOTE:** To use physical device names such as ``/dev/sdx``, stop the multipath daemon service.

---



**NOTE:** DATA, REDO, and ARCHIVE files for non-ASM Oracle database must be stored on devices of the same configuration. For example, if DATA files are stored on a multipath device with one partition, then store ARCHIVE and REDO files on multipath devices with one partition each.

---

## Supported storage arrays

Application Protector supports the following storage arrays.

**Table 1-2: Supported storage configurations**

Storage	Snapshot type	Protocol	SLES 11 SP3	RHEL 5.7	Solaris 10 u11 and Solaris 11
VSP (RAID 700)	ShadowImage and HTI snapshots	FC	√	√	X
		iSCSI	X	X	X
HUS (DF850)	ShadowImage and HTI snapshots	FC	X	√	X
		iSCSI	X	√	X
HNAS (3090)	Tree Clone snapshots	NFS v3	√	√ <sup>1</sup>	√
		DNFS	X	X	√

1. RHEL 6.3 is supported.

## Firmware version for storage array

Application Protector supports the following firmware version.

**Table 1-3: Firmware version**

Storage subsystem	Microcode/Firmware version
VSP RAID 700	70-06-04-00/00
HUS DF850	0915/B-S
HNAS 3090	NAS Platform (M1SEKW0933273)

## Storage prerequisites

You must set the following storage prerequisites to use Application Protector. For details about supported storage prerequisites, see the following.

- [VSP storage prerequisites](#)
- [HUS storage prerequisites](#)
- [Application Protector prerequisites](#)



## VSP storage prerequisites

This section provides the prerequisites required for using VSP storage with Application Protector.

- Configure the RAID Manager (HORCM instance) prior to the Application Protector server configuration and storage registration. For details about CCI configuration, see [Installing and configuring command control interface](#).
- Create a staging hostgroup with the name, `HITACHI-HAPRO-HG` on the VSP storage to stage the V-VOLs created by Application Protector. It is recommended that no hosts are added to this host group.



**NOTE:** World Wide Name (WWN)s belonging to any of the host machines using Application Protector must not be a part of this host group.

---

- To create Full Copy (ShadowImage) snapshots using Application Protector, create a pair relationship of P-VOL and S-VOL prior to creating a snapshot. For VSP storage, add this S-VOL to the staging host group. Best practice suggests to add it to the `HITACHI-HAPRO-HG` host group that does not contain any host WWNs. After creating a new pair, split the pair to avoid revert failure.

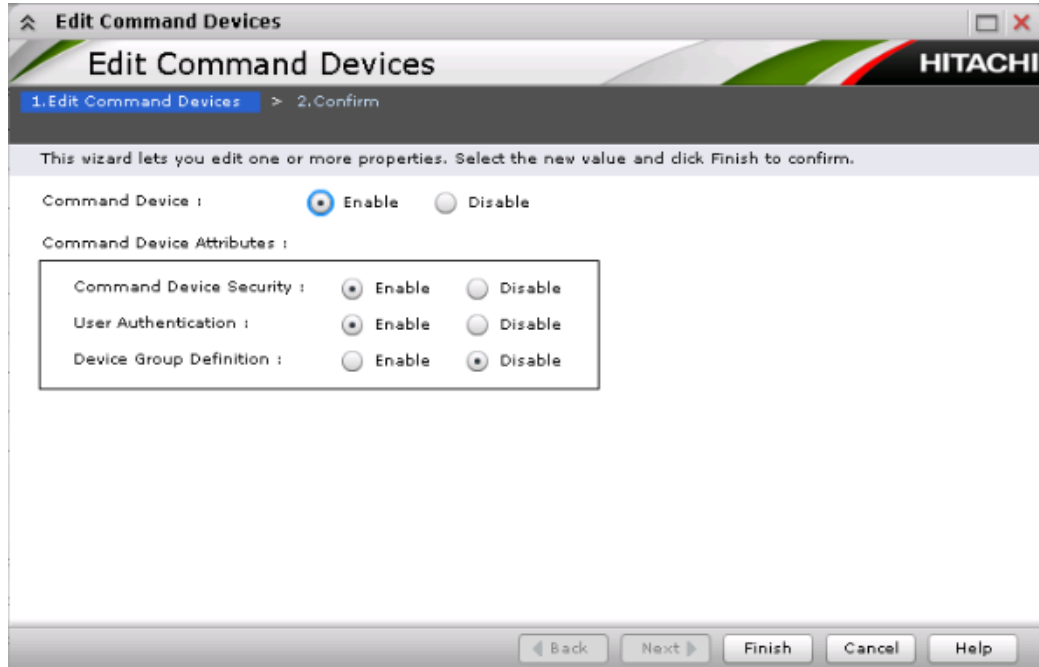
## Installing and configuring command control interface

This section provides the details to install and configure the command control interface (CCI).

### Configuring the command device

Use the Hitachi Storage Navigator to configure the Command Device (CMD). Refer the following screenshot to set the CMD attributes.

**Figure 1-1: Configuring CCI**



**NOTE:** In the preceding figure, **Enable** the user authentication.

### Configuring the command control interface

Configure the CCI HORCM instance on the host server. Brief instructions for configuring the CCI on a Linux server follows.

For detailed instructions, see the *Hitachi Command Control Interface Installation and Configuration Guide*.

### Configuring CCI on a Linux server

1. Confirm the CCI version:

```
# raidqry -h
Model : RAID-Manager/Linux
Ver&Rev: 01-29-03/06
```

2. In the `/etc` folder, create or link to an instance configuration file for a subsystem. The configuration file must be named as `horcm<instance number>.conf`. For example, the `/etc/horcm0.conf` configuration file is for the instance "0".
3. Edit the configuration file as follows:

```
HORCM_CMD
#dev_name dev_name dev_name
/dev/sdf #VSP 66033
```

```
/dev/sde #VSP 66034
```

4. Start an instance by executing `horcmstart.sh <horcm instance number>`:

```
>horcmstart.sh 0
```

confirm the instance working:

```
#raidcom get command_status -I0 -s 66033 -login <uid>  
<password>
```

HANDLE	SSB1	SSB2	ERR_CNT	Serial#	Description
00c9	-	-	0	66033	-

```
#raidcom get command_status -I0 -s 66034 -login <uid>  
<password>
```

HANDLE	SSB1	SSB2	ERR_CNT	Serial#	Description
00c4	-	-	0	66034	-

For details about command line options, see the following guide.

<http://www.hds.com/assets/pdf/cci-user-and-reference-guide.pdf>

## HUS storage prerequisites

This section provides the prerequisites required for using HUS storage on RHEL setup with Application Protector.

1. Enable the iSCSI target security on the port on which Application Protector server is connected. The iSCSI host initiator name of the machine hosting the Application Protector server must be a part of the iSCSI target that contains the P-VOLs hosting the Oracle database.
2. To create Full Copy (ShadowImage) snapshots using Application Protector, create a pair relationship of P-VOL and S-VOL prior to creating a snapshot.

# Application Protector prerequisites

This section provides the details of Application Protector system requirements and Application Protector Server and Client prerequisites.

## System requirements

The following table provides the Application Protector minimum system requirements.

**Table 1-4: System requirements**

Item	Description
System memory	Minimum 1GB and recommended 4GB+
Free disk space required for installation	100MB minimum and recommended 500MB
Operating system	Any one for the following supported operating system: <ul style="list-style-type: none"><li>• SLES 11 SP3 (32-bit and 64-bit)</li><li>• RHEL 5.7 (32-bit and 64-bit) for ASM setups</li><li>• RHEL 6.3 (32-bit and 64-bit) for non-ASM setups</li><li>• Solaris 10 update 11x86 and Solaris 11x86 (32-bit and 64-bit)</li></ul>
Networking	Gigabit Ethernet recommended
Application software	<b>For SLES platform:</b> Oracle® Database 11g Release 2 (11.2.0.3 and 11.2.0.4) (non-ASM) OR Oracle® Database 10g Release2 (10.2.0.4 and 10.2.0.5) (non-ASM) <b>For RHEL platform:</b> Oracle® Database 11g Release2 (11.2.0.3 and 11.2.0.4) (ASM and RAC-ASM) OR Oracle® Database 10g Release2 (10.2.0.4 and 10.2.0.5) (ASM) <b>For Solaris platform:</b> Oracle® Database 11g Release2 (11.2.0.3 and 11.2.0.4) (non-ASM) OR Oracle® Database 10g Release2 (10.2.0.4 and 10.2.0.5) (non-ASM)

## Application Protector Server prerequisites

After you have installed and configured Oracle database, install the following Application Protector Server prerequisites. For details about Application Protector Server prerequisites for supported operating system, see the following.

- ❑ [Application Protector Server for SLES platform](#)
- ❑ [Application Protector Server for RHEL platform](#)
- ❑ [Application Protector Server for Solaris platform](#)

### Application Protector Server for SLES platform

The following table provides the Application Protector Server prerequisites for SLES platform.

**Table 1-5: Application Protector Server prerequisites**

Software version	Package/RPM	Details
SLES 11 SP3	-	32/64-bit operating system supported.
Oracle Database 11gR2 (11.2.0.3 and 11.2.0.4)	-	Non-ASM configuration Oracle database is supported.
SBLIMB SFCB	sblim-sfcb 32 bit	Install 32-bit <sup>1</sup> for both 32/64-bit operating system. For 64-bit, comment out the following line: <pre>preload_pam_misc_so" in "/etc/init.d/sfcb</pre>
Parted	parted-2.3-10.38.16	Shipped with the operating system install media and used to detect partitions on the device.
CCI RAID-Manager/Linux version 01-29-03/06	-	VSP storage prerequisite.

1. Application Protector user must be in the sfcb user group.  
# usermod -A sfcb <HAPRO-user>

## Application Protector Server for RHEL platform

The following table provides the Application Protector Server prerequisites for RHEL platform.

**Table 1-6: Application Protector Server prerequisites**

Software version	Package/RPM	Details
<ul style="list-style-type: none"> <li>RHEL 5.7 for ASM setups with VSP and HUS storage</li> <li>RHEL 6.3 for non-ASM setups with HNAS</li> </ul>	-	32/64-bit operating system supported.
OpenSSL 0.9.8e	-	Required for secure communication with the client.
Oracle 11gR2 version 11.2.0.3/4	-	Supported Oracle database.
Oracle 10gR2 version 10.2.0.4/5	-	Supported Oracle database.
Open Pegasus	tog-pegasus	Install 32-bit RPM in 64-bit operating system that is shipped with the system install media. <sup>1</sup>
Oracle 10gR2 patchset version 10098816	p10098816_112020_Linux-x86-64_3of7.zip	Install the patchset for 64-bit operating system from the grid folder.* <sup>2</sup>
	p10098816_112020_Linux-i386_3of7.zip	Install the patchset for 32-bit operating system.*
Oracle patch: 9316059	-	Install the patch for Oracle 11gR2 ASM support only.*
Oracle Opatch ID 17011832	-	This patch is required for TSPITR on Oracle 11gR2.
CCI RAID-Manager/Linux version 01-29-03/06	-	For VSP only.

1. Do not install 64-bit RPM.

2. Note: "\*" indicates, log in user should be an "Oracle user".

After you have installed and configured Oracle database, install the prerequisites mentioned in [Table 1-6](#), and perform the following tasks prior to installing the Application Protector Server.

- Application Protector user must be in the Pegasus user group:

```
usermode -aG pegasus <HAPRO-user>
```

- Create a pair relationship of S-VOL and P-VOL prior to creating snapshot for the VSP or HUS full copy type of snapshots. You must add this S-VOL to the staging host group. Best practice suggests to add it to the HITACHI-HAPRO-HG host group that does not contain any host WWNs. After creating a new pair, split the pair to avoid revert failure.
- Install the following:
  - For RHEL 6.3, install parted-2.3-10.38.16

- For RHEL 5.7, install parted-1.8.1-28.el5
4. Move the `ASMPARAMFILE` to perform the snapshot management operations. For instructions about how to move the `SPFILE`, see [Backing Up, Copying, and Moving an Oracle ASM Initialization Parameter File](#).

## Application Protector Server for Solaris platform

The following table provides the Application Protector Server prerequisites for Solaris platform.

**Table 1-7: Application Protector Server prerequisites**

Software version	Details
<ul style="list-style-type: none"> <li>• Solaris 10</li> <li>• Solaris 11</li> </ul>	32/64-bit operating system supported.
<ul style="list-style-type: none"> <li>• Oracle 10g Release 2 (10.2.0.4 and 10.2.0.5) (non-ASM)</li> <li>• Oracle 11g Release 2 (11.2.0.3 and 11.2.0.4) (non-ASM)</li> </ul>	Non-ASM configuration Oracle database is supported.
Oracle Opatch ID 17011832	This patch is required for TSPITR on Oracle 11gR2.



**NOTE:** The root user and the Application Protector login user must be in the user group owning the database install location.

**NOTE:** The root user is added to the `hapro` user group on installation. To add more users, you must add them to the `hapro` user group to perform Application Protector operations. For example, `usermod -G hapro <user>`.

## Application Protector Client prerequisites

Perform the following tasks prior to installing the Application Protector Client. For details about Application Protector Server prerequisites for supported operating system, see the following.

- [Application Protector Client for SLES platform](#)
- [Application Protector Client for RHEL platform](#)
- [Application Protector Client for Solaris platform](#)

### Application Protector Client for SLES platform

The following table provides the Application Protector Client prerequisites for SLES platform.

**Table 1-8: Application Protector Client prerequisites**

Software version	Package/RPM	Details
SLES 11 SP3	-	32/64-bit operating system supported
Oracle JRE 1.6 +	JRE 1.6	For 32-bit/64-bit operating system
SBLIM CIM Client	sblim-cim-client2	For 32-bit and 64-bit operating system
Log4j	log4j	For 32-bit and 64-bit operating system

### Application Protector Client for RHEL platform

The following table provides the Application Protector Client prerequisites for RHEL platform.

**Table 1-9: Application Protector Client prerequisites**

Software version	Package/RPM	Details
<ul style="list-style-type: none"><li>• RHEL 5.7 for ASM setups</li><li>• RHEL 6.3 for non-ASM setups</li></ul>	-	32/64-bit operating system
Oracle JRE 1.6+	JRE 1.6	For 32-bit and 64-bit operating system
SBLIM CIM Client	sblim-cim-client	For 32-bit and 64-bit operating system
Log4j	log4j	For 32-bit and 64-bit operating system



## Application Protector Client for Solaris platform

The following table provides the Application Protector Client prerequisites for Solaris platform.

**Table 1-10: Application Protector Client prerequisites**

Software version	Package/RPM	Details
<ul style="list-style-type: none"><li>Solaris 10 u11</li><li>Solaris 11</li></ul>	-	32/64-bit operating system
Log4j	CSWlog4j	For 32-bit and 64-bit operating system
Oracle JRE 1.6+	JRE 1.6	For 32-bit/64-bit operating system



**NOTE:** For Solaris operating system, if the Application Protector Server does not respond to the Client request in 30 minutes, then the operation fails and an error displays.

---



# Installing Application Protector

This chapter guides you through the installation and removal of the Application Protector Server and Client.

This chapter describes the following topics:

- ❑ [Installing the Application Protector Server](#)
- ❑ [Installing the Application Protector Client](#)
- ❑ [Removing the Application Protector Server](#)
- ❑ [Removing the Application Protector Client](#)

# Installing the Application Protector Server

The Application Protector Server self extracting installer is distributed in the shell script (.sh) file format. You must accept the end user license agreement and then perform actions based on the provided command and option.

Application Protector is a 32-bit application that is installed on both 32-bit and 64-bit systems.



**NOTE:** Make sure that the **/var/tmp** directory has more than 1GB of free space.

The following table provides the Application Protector installer names for the supported platform.

**Table 2-1: Supported platform and installers**

Platform	Application Protector Server	Application Protector Client
Solaris	<ul style="list-style-type: none"><li>HAPRO-Oracle-Server-&lt;v1.2.0.x&gt;-Solaris-10-x86.sh</li><li>HAPRO-Oracle-Server-&lt;v1.2.0.x&gt;-Solaris-11-x86.sh</li></ul>	<ul style="list-style-type: none"><li>HAPRO-Client-&lt;v1.2.0.x&gt;-Solaris-10-x86.sh</li><li>HAPRO-Client-&lt;v1.2.0.x&gt;-Solaris-11-x86.sh</li></ul>
RHEL	HAPROSetup_Server_x86_RHEL.sh	HAPROSetup_Client_noarch_RHEL.sh
SLES	HAPROSetup_Server_x86_SLES.sh	HAPROSetup_Client_noarch_SLES.sh

## To install the Application Protector Server

1. Extract the installer as follows.

```
tar -xzvf HAPROInstaller.tar.gz
```

2. The **HAPROInstaller** directory contains the **<HAPRO Server<sup>1</sup>>.sh** installer script. Use the following commands to install the Application Protector Server for the supported platforms.

```
./HAPROSetup_Server_x86_SLES.sh -t <Block (VSP/HUS)/  
HNAS*2> install
```

```
./HAPROSetup_Server_x86_RHEL.sh install
```

```
./HAPRO-Oracle-Server-<v1.2.0.x>-Solaris-<10/11>-x86.sh  
install
```



**NOTE:** Provide permission to the installer script using the `chmod 777 <thesetup.sh>` command if you do not have permission for installation.

3. Accept **End User License Agreement (EULA)** to proceed with the installation.

1. <HAPRO Server> refers to the Server installer for supported platform.

Solaris: HAPRO-Oracle-Server-<v1.2.0.x>-Solaris-<10/11>-x86.sh

RHEL: HAPROSetup\_Server\_x86\_RHEL.sh

SLES: HAPROSetup\_Server\_x86\_SLES.sh

2. "\*" indicates: Provide "HNAS" for HNAS storage, else provide "Block (VSP/HUS)" for other storages.

On installing the Application Protector Server successfully, the executable files are copied to the **/opt/Hitachi/HAPRO/server/bin** directory.

Logs are generated in the **/opt/Hitachi/HAPRO/sever/logs** directory.

For details about the Application Protector Server command and actions, see [Application Protector Server installer syntax](#).

## Application Protector Server installer syntax

The following table provides the Application Protector Server installer commands and parameters.

### Syntax

**./<HAPRO Server>.sh <command> <parameter>**

**Table 2-2: Command and parameter description**

Command	Parameter <sup>1</sup>	Description
<ul style="list-style-type: none"> <li>HAPROSetup_Server_x86_RHEL.sh -t &lt;Block (VSP/HUS)/HNAS&gt; install</li> <li>HAPROSetup_Server_x86_SLES.sh -t &lt;Block (VSP/HUS)/HNAS&gt; install</li> <li>HAPRO-Oracle-Server-&lt;v1.2.0.x&gt;-Solaris-&lt;10/11&gt;-x86.sh install</li> </ul>	--accept_eula   -e	Installs the Application Protector Server without user confirmation.
<ul style="list-style-type: none"> <li>HAPROSetup_Server_x86_RHEL.sh -t &lt;Block (VSP/HUS)/HNAS&gt; install</li> <li>HAPROSetup_Server_x86_SLES.sh -t &lt;Block (VSP/HUS)/HNAS&gt; install</li> <li>HAPRO-Oracle-Server-&lt;v1.2.0.x&gt;-Solaris-&lt;10/11&gt;-x86.sh install</li> </ul>	--help   -h	Displays the help for the install command.
<ul style="list-style-type: none"> <li>HAPROSetup_Server_x86_RHEL.sh -t &lt;Block (VSP/HUS)/HNAS&gt; uninstall</li> <li>HAPROSetup_Server_x86_SLES.sh -t &lt;Block (VSP/HUS)/HNAS&gt; uninstall</li> <li>HAPRO-Oracle-Server-&lt;v1.2.0.x&gt;-Solaris-&lt;10/11&gt;-x86.sh uninstall</li> </ul>	--complete   -c  --silent   -s  --help   -h	Removes Application Protector cache and temporary files associated with Application Protector, in addition to normal uninstall.  Uninstall without user confirmation.  Displays the help.
<ul style="list-style-type: none"> <li>HAPROSetup_Server_x86_RHEL.sh version</li> <li>HAPROSetup_Server_x86_SLES.sh version</li> <li>HAPRO-Oracle-Server-&lt;v1.2.0.x&gt;-Solaris-&lt;10/11&gt;-x86.sh version</li> </ul>	Not required	Displays version of the installed Application Protector Server.
<ul style="list-style-type: none"> <li>HAPROSetup_Server_x86_RHEL.sh help</li> <li>HAPROSetup_Server_x86_SLES.sh help</li> <li>HAPRO-Oracle-Server-&lt;v1.2.0.x&gt;-Solaris-&lt;10/11&gt;-x86.sh help</li> </ul>	Not required	Prints help for the installer.
<ul style="list-style-type: none"> <li>HAPROSetup_Server_x86_RHEL.sh update</li> <li>HAPROSetup_Server_x86_SLES.sh update</li> <li>HAPRO-Oracle-Server-&lt;v1.2.0.x&gt;-Solaris-&lt;10/11&gt;-x86.sh update</li> </ul>	Not required	Updates to newer version or newer release.

1. The Application Protector Server installer parameters are optional.

## Sample commands

### To install the Application Protector Server for SLES

```
./HAPROSetup_Server_x86_SLES.sh -t <Block (VSP/HUS)/HNAS>  
install
```

### To install the Application Protector Server for SLES by accepting EULA

```
./HAPROSetup_Server_x86_SLES.sh -t <Block (VSP/HUS)/HNAS>  
install --accept_eula
```

### To display the Application Protector Server help for SLES

```
./HAPROSetup_Server_x86_SLES.sh -t <Block (VSP/HUS)/HNAS>  
help
```

# Installing the Application Protector Client

The Application Protector Client self extracting installer is distributed in the shell script (.sh) file format. You must accept the end user license agreement and then perform actions based on the command and option provided.



**NOTE:** Make sure the **/var/tmp** directory has more than 1GB of free space.

---

## To install the Application Protector Client

1. Extract the installer as follows.

**tar -xzvf HAPROInstaller.tar.gz**

2. The **HAPROInstaller** directory contains the **<HAPRO Client<sup>1</sup>>.sh** installer script. For Application Protector Server and Client installer names, see [Supported platform and installers](#). Use the following commands to install the Application Protector Client for the supported platforms:

**./HAPROSetup\_Client\_noarch\_SLES.sh install**

**./HAPROSetup\_Client\_noarch\_RHEL.sh install**

**./HAPRO-Client-<v1.2.0.x>-Solaris-<10/11>-x86.sh install**

3. Accept **End User License Agreement (EULA)** to proceed with the installation.

On successful installation of Application Protector Client, the following files are copied:

- Executable files are copied into the following directory.
  - CLI executable: **/opt/Hitachi/HAPRO/client/bin**
  - UI executable: **/opt/Hitachi/HAPRO/client/oracle/bin**
- Logs are generated in the **/opt/Hitachi/HAPRO/client/logs** directory.

---

1. <HAPRO Client> refers to the Application Protector Client installer for the supported platform.

Solaris: HAPRO-Client-<v1.2.0.x>-Solaris-<10/11>-x86.sh

RHEL: HAPROSetup\_Client\_Oracle\_noarch\_RHEL.sh

SLES: HAPROSetup\_Client\_Oracle\_noarch\_SLES.sh

## Application Protector Client installer syntax

The following table provides the Application Protector Client installer commands and parameters.

### Syntax

**./<HAPRO Client>.sh <command> <parameter>**

**Table 2-3: Command and parameter description**

Command	Parameter	Description
<ul style="list-style-type: none"> <li>HAPROSetup_Client_Oracle_noarch_RHEL.sh install</li> <li>HAPROSetup_Client_Oracle_noarch_SLES.sh install</li> <li>HAPRO-Client-&lt;v1.2.0.x&gt;-Solaris-&lt;10/11&gt;-x86.sh install</li> </ul>	--accept_eula  -e  --help  -h	Installs the Application Protector Client without user confirmation.  Displays help for install command.
<ul style="list-style-type: none"> <li>HAPROSetup_Client_Oracle_noarch_RHEL.sh uninstall</li> <li>HAPROSetup_Client_Oracle_noarch_SLES.sh uninstall</li> <li>HAPRO-Client-&lt;v1.2.0.x&gt;-Solaris-&lt;10/11&gt;-x86.sh uninstall</li> </ul>	--silent  -s	Uninstall without user confirmation.
<ul style="list-style-type: none"> <li>HAPROSetup_Client_Oracle_noarch_RHEL.sh version</li> <li>HAPROSetup_Client_Oracle_noarch_SLES.sh version</li> <li>HAPRO-Client-&lt;v1.2.0.x&gt;-Solaris-10-x86.sh version</li> </ul>	Not applicable	Displays version of the installed Application Protector Client.
<ul style="list-style-type: none"> <li>HAPROSetup_Client_Oracle_noarch_RHEL.sh help</li> <li>HAPROSetup_Client_Oracle_noarch_SLES.sh help</li> <li>HAPRO-Client-&lt;v1.2.0.x&gt;-Solaris-&lt;10/11&gt;-x86.sh help</li> </ul>	Not applicable	Prints help message.
<ul style="list-style-type: none"> <li>HAPROSetup_Client_Oracle_noarch_RHEL.sh update</li> <li>HAPROSetup_Client_Oracle_noarch_SLES.sh update</li> <li>HAPRO-Client-&lt;v1.2.0.x&gt;-Solaris-&lt;10/11&gt;-x86.sh update</li> </ul>	Not applicable	Updates the application.



## Sample commands

### To install the Application Protector Client for SLES

```
./HAPROSetup_Client_noarch_SLES.sh install
```

### To install the Application Protector Client for SLES by accepting EULA

```
./HAPROSetup_Client_noarch_SLES.sh install --accept_eula
```

### To display the Application Protector Client help for SLES

```
./HAPROSetup_Client_noarch_SLES.sh help
```

### To update the Application Protector Client for SLES

```
./HAPROSetup_Client_noarch_SLES.sh update
```

## Removing the Application Protector Server

You can remove the Application Protector Server by using one of the following commands.

```
./HAPROSetup_Server_x86_RHEL.sh -t <Block (VSP/HUS)/  
HNAS>1 uninstall
```

```
./HAPROSetup_Server_x86_SLES.sh -t <Block (VSP/HUS)/HNAS>  
uninstall
```

```
./HAPRO-Oracle-Server-<v1.2.0.x>-Solaris-<10/11>-x86.sh  
uninstall
```

```
./<HAPRO Server2>.sh uninstall --complete
```

```
./<HAPRO Server>.sh uninstall --silent
```



**NOTE:** The `-s` | `--silent` option uninstalls Application Protector without user confirmation, else you are prompted to provide the input to uninstall Application Protector Server.

---

For details about <HAPRO Server> installer for the supported platform, see [Supported platform and installers](#).



**WARNING!** The `--complete` option removes the Application Protector metadata cache and temporary files associated with Application Protector.

---

1. Provide “HNAS” for HNAS storage, else provide “Block (VSP/HUS)” for other storages.
2. <HAPRO Server> refers to the Application Protector Server installer for supported platform.

## Removing the Application Protector Client

You can remove the Application Protector Client by using the following commands.

```
./<HAPRO Client1>.sh uninstall
```

```
./<HAPRO Client>.sh uninstall -s
```



**NOTE:** The `-s` | `--silent` option uninstalls Application Protector without user confirmation, else you are prompted to provide the input to uninstall Application Protector Client.

---

For details about <HAPRO Client> installer for the supported platform, see [Supported platform and installers](#).

---

1. <HAPRO Client> refers to the Application Protector Client installer for the supported platform.

# Configuring Application Protector

This chapter guides you to setup the user account and activate license for Application Protector.

This chapter describes the following topics:

- ❑ [Accessing Application Protector](#)
- ❑ [Configuring the database service account](#)
- ❑ [Configuring the ASM service account](#)
- ❑ [Licensing Application Protector](#)

## Accessing Application Protector

You can invoke the Application Protector GUI using the credentials provided by the administrator.

### To access the Application Protector GUI

1. Click the **HAPRO Client** desktop icon to launch the **Application Protector** login page.  
Else, use the `./HAPROOracleUI` command in the `/opt/Hitachi/HAPRO/client/oracle/bin` directory.  
Else, launch the login page by executing the `haproui` command from anywhere on the terminal.
2. Enter the server name, FQDN or server IP address in the **Server** field. You can provide the server name as "localhost" if the client and server are installed on the same server.
3. Enter the user credentials in the **Username** and **Password** fields. You must have access to the Oracle database.
4. Click **Login**.

### To access the Application Protector CLI

You can use the CLI interface to perform the Application Protector operations. For details, see *Hitachi Application Protector CLI Guide for Oracle® Database Server*.

## Configuring the database service account

After installing Application Protector, set the database service account credentials. The service account is used as the login credential for an Oracle Database user. Each Application Protector user has a service account and all databases that you intend to work with must be accessible with the service account credentials.

For details on user privileges to perform the Application Protector tasks, see [Licensing Application Protector](#). You can set and modify the database service account as follows.

## Setting the database service account

The Oracle Database credentials having `SYS` privileges are used as service account to access the Oracle Database. You must set the service account credentials while using Application Protector Server for the first time.

### To set the database service account

1. Click **Configuration** and then click **Server**.
2. Click **Set** in the **Database Service Account** field.
3. Enter the Oracle database credentials in the **Username** and **Password** fields.
4. Click **Save** to setup the database service account credentials and click **OK**.

## Modifying the database service account

As a best practice, you should not change the database service account credentials when snapshot operations are in progress.

You cannot modify the database service account credentials, if you are connected to the database.

### To modify the database service account

1. Click **Configuration** and then click **Server**.
2. Click **Set** in the **Database Service Account** field.
3. Modify the details.
4. Click **Save** to modify the service account credentials and click **OK**.



**NOTE:** To remove the specified service account credentials, click **Clear**.

---

## Service account user privileges

You must have the service account user privileges to perform operations such as Create Snapshot, Delete Snapshot, Create Snapshot Schedule, or Recovery. The following table lists the service account privileges you must have to perform the Application Protector operations.

**Table 3-2: Service account user privileges**

Application Protector operation	OS user	Privileges	Details
Create snapshot	Oracle	SYSDBA	RMAN requires SYSDBA privilege to connect to target DB.
Delete snapshot	-	-	SYSDBA privilege
Mount snapshot	Oracle	SYSDBA	SYSDBA privilege
Unmount snapshot	Oracle	SYSDBA	SYSDBA privilege
Revert snapshot	Oracle	SYSDBA	RMAN requires SYSDBA privilege to connect to target DB.
Recover snapshot	Oracle	SYSDBA	RMAN requires SYSDBA privilege to connect to target DB.

## Configuring the ASM service account

After installing Application Protector, set the ASM service account. Set the ASM service account credentials while using Application Protector Server for the first time.

### Setting the ASM service account

#### To set the ASM service account

1. Click **Configuration** and then click **Server**.
2. Click **Set** in the **ASM Service Account** field.
3. Enter the Oracle ASM instance credentials in the **Username** and **Password** fields.
4. Click **Save** to setup the ASM service account credentials and click **OK**.



**NOTE:** This field is applicable to ASM database on RHEL platform only.

---

### Modifying the ASM service account

This field is applicable to ASM databases on RHEL platform only.

#### To modify the ASM service account

1. Click **Configuration** and then click **Server**.
2. Click **Set** in the **ASM Service Account** field.
3. Modify the details.
4. Click **Save** to modify the ASM service account credentials and click **OK**.



**NOTE:** To remove the specified ASM service account credentials, click **Clear**.

---

## Licensing Application Protector

After installing Application Protector, register a valid license key on the server.

The following is applicable for the Application Protector license key:

- The Application Protector license is node-locked. A license is generated for a given server and you can install it on that server only.
- The license is a perpetual license.

For example, license keys purchased and installed for version 1.0 continues to function for all 1.x releases. Upgrading to 2.x requires an updated license key.

The Application Protector license must be activated to use the snapshot-based backup and recovery features for the supported storage array and application.



**NOTE:** You must generate and activate the Application Protector license for SLES and RHEL platforms.

**NOTE:** For RHEL platform, in a RAC setup, register the key on each node on which Application Protector Server is installed.

---

### To install and activate the production license

1. Create a capability license request based on information provided while purchasing the product license from HDS.
2. Provide the Activation ID for the supported storage.
3. Install the license response file reverted by the [HDSLicensing@hds.com](mailto:HDSLicensing@hds.com) team as a part of production license activation.

## Activating the Application Protector license

Activate the license to perform the snapshot management tasks. Application Protector is available with the following license types:

- Trial License (30 days)
- Production License (unlimited)

### To activate the Application Protector trial license

Perform the following, on successful installation of Application Protector.

1. Enter the user credentials in the login page. A trial license activation dialog box appears.
2. Click **Yes** in the confirmation box to install trial license.
3. Click **OK**.

After 30 days, the trial license expires and you cannot use the Application Protector features. You must activate the production license to use Application Protector further.

## To activate the Application Protector production license

1. Click **Configuration**.
2. Click **Licenses** and then **Activate** in the action pane, else select **Activate** in the **Action** menu.

After activating the license for a supported storage such as VSP, you can activate the license for other supported storages as well.

Application Protector supports creating single request file per storage.
3. Click **Skip** if you already have a license response file, else provide the following in the **License Activation Wizard** and click **Next**.

**First Name:** Enter the first name. Maximum 64 characters are supported.

**Last Name:** Enter the last name. Maximum 64 characters are supported.

**Activation ID:** Enter the activation ID provided to you with the product.

**Email ID:** Enter the valid email ID. Maximum 32 characters are supported.

**Company Name:** Enter the company name. Maximum 32 characters are supported.

**Site ID:** Enter the company site ID. Maximum 64 characters are supported.

**Address:** Enter the company address. Maximum 256 characters are supported.

**Country:** Enter the country. Maximum 64 characters are supported.
4. Click **Next**, to generate the **License Request**.
5. Click **Browse** in the **License File** to add the **License Response** file and click **Install**.
6. Click **OK**.

For more details about activating license by using CLI, see *Hitachi Application Protector CLI Guide for Oracle Database Server*.

## Listing the Application Protector licenses

After activating the production license, you can list the Application Protector license details.

### To list the Application Protector license

1. Click **Configuration**.
2. Click **Licenses**.
3. Click **Details** in the action pane, else select **Details** in the **Action** menu to view the Application Protector license details with the expiry details (in days).

You can perform snapshot management operations for the activated production license only.





# Glossary

This glossary provides definitions of general storage terms as well as specific terms related to the technology that supports Hitachi Application Protector. Click the letter of the glossary section to display that page.

## A

### **Application Protector**

Hitachi Application Protector.

### **ASM**

Automatic Storage Management.

## C

### **CCI**

Command Control Interface.

### **CIM**

Common information model.

### **CLI**

Command line interface.

### **Complete recovery**

Complete recovery involves using redo data or incremental backups combined with a backup of database, tablespace, or datafile to update it to the current point-in-time. The recovery is called complete recovery because all redo changes contained in the archived and online logs are overwritten completely. Complete recovery is generally performed after a control file or data file damage.

#	<a href="#">A</a>	<a href="#">B</a>	<a href="#">C</a>	<a href="#">D</a>	<a href="#">E</a>	<a href="#">F</a>	<a href="#">G</a>	<a href="#">H</a>	<a href="#">I</a>	<a href="#">J</a>	<a href="#">K</a>	<a href="#">L</a>	<a href="#">M</a>	<a href="#">N</a>	<a href="#">O</a>	<a href="#">P</a>	<a href="#">Q</a>	<a href="#">R</a>	<a href="#">S</a>	<a href="#">T</a>	<a href="#">U</a>	<a href="#">V</a>	<a href="#">W</a>	<a href="#">X</a>	<a href="#">Y</a>	<a href="#">Z</a>
---	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------

## **Control file**

The control file is a binary file that records the physical structure of the database. Every Oracle database has a control file. It includes the database name, names and locations of associated datafiles and redo log files, database creation timestamp, current log sequence number, and checkpoint information.

## **CSV**

Comma separated value.

## **F**

### **FQDN**

Fully qualified domain name.

### **Full copy snapshot**

Full copy (ShadowImage) type of snapshots backup complete database and enable restoring the data without referring to any other snapshot copies. A complete copy of the original database is created using full copy snapshot technology that can be replicated to other sites or backed up.

## **G**

### **GUI**

Graphical user interface.

## **H**

### **HAPRO**

Hitachi Application Protector.

### **HNAS**

Hitachi Network Attached Storage.

### **HTI**

Hitachi Thin Image.

### **HUS**

Hitachi Unified Storage.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

## **Glossary–2**

## **I**

### **I/O**

Input/output.

## **L**

### **LV**

Logical volume.

### **LVM**

Logical volume manager.

### **LU**

Logical unit.

## **M**

### **Mount tool path**

The mount tool path is configurable for Oracle 10gR2. You can set the mount tool path to the path where the patch set is installed. This parameter is applicable for mount, recovery and revert operations.

## **O**

### **OCI**

Oracle call interface.

## **P**

### **PL**

Perl script.

### **PV**

Physical volumes.

### **Point-in-time recovery**

Application Protector uses the log files generated by the application server, to replay the log operation to recover the data to the point-in-time (PIT).

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

## **Prescripts**

Executed prior to snapshot management operations in a synchronous manner. If the prescript fails, the snapshot creation fails, and you can refer the error log for failure details.

## **Postscripts**

Executed after snapshot management operations in a synchronous manner. If the postscript fails, the snapshot is created and you need to check the process ID to decide whether you want to keep the snapshot.

## **PSUS**

PAIR suspended.

## **P-VOL**

A volume that consists of a production volume containing the original data is called the primary volume (P-VOL).

# **R**

## **Recovery**

Recovery is the process of copying data from the backup or the snapshot data and then applying logs to roll forward the recovered database up to the point of failure or to any point-in-time. Recovery can be performed on the host that has the current active database and has access to the snapshot volumes.

## **Restore**

Restore is a process of copying a database from a snapshot copy to the original LUN or to a new LUN. On restoring a snapshot, only data files are restored from the snapshot.

## **Revert**

The database is overwritten completely and is performed on the same host only.

## **RMAN**

Oracle Recovery Manager.

## **RPO**

Recovery point objective.

## **RTO**

Recovery time objective.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

## **Glossary-4**

## S

### SI

ShadowImage®

### Session

A series of communications or exchanges of data between two end points that occurs during the span of a single connection. The session begins when the connection is established at both ends, and terminates when the connection is ended.

### SH

Shell script.

### SLES

SUSE Linux Enterprise Server.

### Snapshot

Snapshot is a point-in-time copy of the data of an application database. The data files, control files, and archive log files are backed-up while creating a snapshot.

### Snapshotable instance

The database instance that resides on a Hitachi supported storage device such as VSP. You must move the database to VSP arrays for protection.

### Space efficient

Space efficient snapshots are created using space efficient snapshot technologies. These are transient copies that allow quick recovery of the database. Application Protector supports Hitachi Thin Images (HTI) snapshots.

### SPFile

Server parameter file.

### S-VOL

Secondary volumes contain copies of the P-VOL.

## T

### Tablespace

A tablespace is a logical storage unit within an Oracle database. It consists of at least one datafile that is physically located in the file system of the server.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

**Target**

Devices that receive iSCSI requests that originate from an iSCSI initiator.

**Tree Clone**

Tree Clone is a cloning method for NAS based storages. It recreates the source directory structure at the destination and clones contained files.

**V****VG**

Volume group.

**VSP**

Virtual Storage Platform.

**V-VOL**

Virtual volumes contain virtual copies on the P-VOL.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

**Glossary–6**



## **Hitachi Data Systems**

### **Corporate Headquarters**

2845 Lafayette Street, Santa Clara,  
California 95050-2629, U.S.A.

[www.hds.com](http://www.hds.com)

### **Regional Contact Information**

#### **Americas**

+1 408 970 1000

[info@hds.com](mailto:info@hds.com)

#### **Europe, Middle East, and Africa**

+44 (0)1753 618000

[info.emea@hds.com](mailto:info.emea@hds.com)

#### **Asia Pacific**

+852 3189 7900

[hds.marketing.apac@hds.com](mailto:hds.marketing.apac@hds.com)



MK-91HAP013-00