user manual

AES Encryption for HP Data Protector 6.0

December 2006

Legal and notice information

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

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

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for Hewlett-Packard Company products are set forth in the express limited warranty statements for such products. Nothing herein should be construed as constituting an additional warranty.

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

UNIX® is a registered trademark of The Open Group.

Linux is a U.S. registered trademark of Linus Torvalds.

This product includes software developed by the OpenSSL Project for use in the openSSL Toolkit (http://www.openssl.org/)

Contents

About this guide 7
Intended audience 7
Related documentation 7
Document conventions and symbols 8
Abbreviations 9
HP technical support 9
HP-authorized reseller 10

1 Introduction 11
AES encryption overview 12
Modules of HP Data Protector’s that use AES encryption 12
Support matrices for AES encryption on HP Data Protector 6.0 13

2 Using AES encryption 15
Enabling encryption for a backup specification 16
Enabling encryption for an Internal Database (IDB) backup 17
Backing up data using AES encryption on a client 18
Using omnikeystore 19
Restoring data using AES encryption on a client 20

3 Additional Backup and Restore Scenarios 21
Backing up data using XOR encoding on a client 22
Restoring data that is already backed up using XOR encoding or custom built encryption 23
Restoring encrypted backups performed on host A to another host B 25
Using the custom built encryption or XOR encoding instead of AES encryption 26
Using a new key for all backups from a given host 26
Using a common omnikeystore file across hosts A and B 27

4 Best Practices 29
Backing up the omnikeystore file 30
Managing keys in the omnikeystore file 30
The omnikeystore file size 30
Using AES Encryption in the simplest way 30

5 Limitations 31

6 Troubleshooting 33

7 Frequently asked Questions (FAQs) 35

A omnikeytool 37

Glossary 39

Figures

1 Selecting the encode option in backup specification 16
2 Selecting the encode option in IDB 17
3 Backup with AES encryption 19
4 Restore with AES encryption 20
5 Backup with XOR encryption 23
6 Restoring with XOR encryption or a custom built encryption 24

Tables

1 Document conventions 8
2 Terms and Abbreviations 9
3 Support matrix for IDB backup with AES encryption 13
4 Support matrix for Raw Disk and file system backup with AES encryption 13
5 Platform restrictions for supported operating systems 14
6 Omnikeystore file locations 19
7 Recommended steps for using XOR encoding or custom built encryption 26
8 Common issues 33

About this guide

This guide discusses the following topics:

- AES encryption
- Using the product
- Best Practices
- Limitations

Intended audience

This guide is intended for the following types of users:

- Administrators
- Any one who needs to use encryption for backing up and restoring data.

Related documentation

In addition to this guide, following are the other documents available for this product:

- *HP Data Protector Help*
- *Advanced Encryption Standard* at the website:

  http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
- *Federal Information Processing Standards Publication 197* at the website:

  http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
- *NIST Special Publication 800-38A 2001 Edition* at the website:

  http://csrc.nist.gov/CryptoToolkit/modes/800-38_Series_Publications/SP800-38A.pdf
- *Comments to NIST concerning AES Modes of Operations* at the website:

  http://csrc.nist.gov/CryptoToolkit/modes/workshop1/papers/lipmaa-ctr.pdf
- *The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)* at the website:

  http://csrc.nist.gov/cryptval/aes/AESAVS.pdf

NOTE:

One or more of the links above will take you outside the Hewlett-Packard website. HP does not control and is not responsible for information outside of the HP website.

Any further information on HP Data Protector can be found at the HP website:

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

Document conventions and symbols

Table 1 lists the conventions and symbols used in this document.

Table 1 Document conventions

Convention	Element
Medium blue text: Related documentation	Cross-reference links and e-mail addresses
Medium blue, underlined text (http://www.hp.com)	Website addresses
Bold font	• Key names • Text typed into a GUI element, such as into a box • GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes
Italic font	Text emphasis
`Monospace font`	• File and directory names • System output • Code • Text typed at the command line
`Monospace, italic font`	• Code variables • Command-line variables
`Monospace, bold font`	Emphasis of file and directory names, system output, code, and text typed at the command line

△ CAUTION:

Indicates that failure to follow directions can result in damage to equipment or data.

IMPORTANT:

Provides clarifying information or specific instructions.

NOTE:

Provides additional information.

Abbreviations

Table 2 lists the abbreviations and definitions used in the document.

Table 2 Terms and Abbreviations

Abbreviation	Expansion	Description
AES	Advanced Encryption Standard	Encryption algorithm to encrypt the data using a key.
DA	Disk Agent	The module that reads data from and writes to the disk devices viewed as file systems or raw disks.
MA	Media Agent	The module that reads data from and writes to a backup device.
IDB	Internal Database	Stores information regarding the backup data, such as: • Media on which the data resides • The result of backup • Restore • Copy • Object consolidation • Media management sessions • Configuration of devices and libraries
FIPS	Federal Information Processing Standards	Publicly announced standards developed by the United States Federal government for use by all non-military Government agencies and by government contractors. Many FIPS standards are modified versions of standards used in the wider community (ANSI, IEEE, and ISO).

HP technical support

Telephone numbers for worldwide technical support are listed on the HP support website: http://www.hp.com/support/

Collect the following information before calling:

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

HP recommends that customers sign up online using subscriber's choice website: http://www.hp.com/go/e-updates

- Subscribing to this service provides you with e-mail updates on the latest product enhancements, newer versions of drivers, and firmware documentation updates, as well as instant access to numerous other product resources.
- After signing up, you can quickly locate your products by selecting **Business support** and then **Storage** under Product Category.

HP-authorized reseller

For the name of your nearest HP-authorized reseller:

- In the United States, call 1-800-345-1518.
- In Canada, call 1-800-263-5868.
- Elsewhere, visit the HP web site: http://www.hp.com, and click **Contact HP** to find locations and telephone numbers.

1 Introduction

This chapter discusses the following topics:

- AES encryption overview
- Modules of HP Data Protector's that use AES encryption
- Support matrices for AES encryption on HP Data Protector 6.0

AES encryption overview

The Advanced Encryption Standard (AES), also known as Rijndael, is a block cipher adopted as an encryption standard by the US government. AES was adopted by the National Institute of Standards and Technology (NIST) as US FIPS PUB 197 in November 2001, after a 5-year standardization process (Advanced Encryption standards process).

The AES specifies an FIPS-approved cryptographic algorithm that can be used to protect electronic data. This algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back to its original form, called plaintext.

With this release, HP Data Protector 6.0 includes 256–bit AES encryption to secure backup data.

This user manual discusses HP Data Protector's 256–bit AES encryption functionality. It also discusses the implications of the AES encryption for system and backup administrators. For more information on HP Data Protector, see *HP Data Protector Concepts Guide*. For information on HP Data Protector commands, see the UNIX manpages or the *HP Data Protector Command Line Interface Reference*.

Modules of HP Data Protector's that use AES encryption

The following modules of HP Data Protector use AES encryption:

- Volume Backup Disk Agent (VBDA) or Volume Restore Disk Agent (VRDA)
- Raw Backup Disk Agent (RBDA) or Raw Restore Disk Agent (RRDA)
- Data Protector Internal Database Backup Disk Agent (DBBDA)

Support matrices for AES encryption on HP Data Protector 6.0

This section discusses the support matrices for AES encryption on HP Data Protector 6.0.

Table 3 lists the support matrix for IDB backup with AES encryption.

Table 3 Support matrix for IDB backup with AES encryption

Data Protector modules using encryption	Supported operating systems
Data Protector Internal Database (IDB) Backup Disk Agent (on Cell Manager)	• Windows 2003 (32-bit) [1] • HP-UX (PA-RISC) - 11.11 [2] • HP-UX (PA-RISC) - 11.23 [3] • HP-UX (Itanium) - 11.23 [3] • SuSe Linux Enterprise Server 9 (64-bit) (x64) • RedHat Enterprise Linux 4.0 (64-bit) (x64)

NOTE:

1. Includes support for Windows 2003 R2 and Windows Storage Server 2003 R2, where applicable.
2. HP-UX 11.11 is HP-UX 11i Version 1.0.
3. HP-UX 11.23 is HP-UX 11i Version 2.0

Table 4 lists the support matrix for Raw Disk and file system backup with AES encryption.

Table 4 Support matrix for Raw Disk and file system backup with AES encryption

Data Protector modules using encryption	Supported operating systems
Volume Backup or Restore Disk Agent Raw Disk Backup or Restore Disk Agent (disk agents)	• Windows XP Pro • Windows 2003 (32-bit) [1] • Windows 2003 (64-bit) (Itanium and x64) [4] • HP-UX (PA-RISC) - 11.11 [2] • HP-UX (PA-RISC) - 11.23 [3] • HP-UX (Itanium) -- 11.23 [3] • Linux (64-bit): • Red Hat Enterprise Linux – Adv. Server 2.1, 3.0, 4.0 [5] • SuSE Linux Enterprise Server (SLES) 8, 9

NOTE:

1. Includes support for Windows 2003 R2 and Windows Storage Server 2003 R2, where applicable.
2. HP-UX 11.11 is HP-UX 11i Version 1.0.
3. HP-UX 11.23 is HP-UX 11i Version 2.0.
4. Reflection X Version 9 and later are supported.
5. Includes support for Red Hat Enterprise Linux Advanced Workstation and Enterprise Server, where applicable.

Table 5 lists the platform restrictions for the supported operating systems.

Table 5 Platform restrictions for supported operating systems

Operating system	Supported processor platform
HP-UX	PA-RISC (HP-UX 11.0, 11.11, 11.23) Itanium (HP-UX 11.23)
Windows	x86 and x86_64 (for 32-bit Windows) Itanium and x86_64 (for 64-bit Windows)
Linux	x86 and x86_64 (for 32-bit Linux) Itanium and x86_64 (for 64-bit Linux)

2 Using AES encryption

This chapter discusses the following topics:

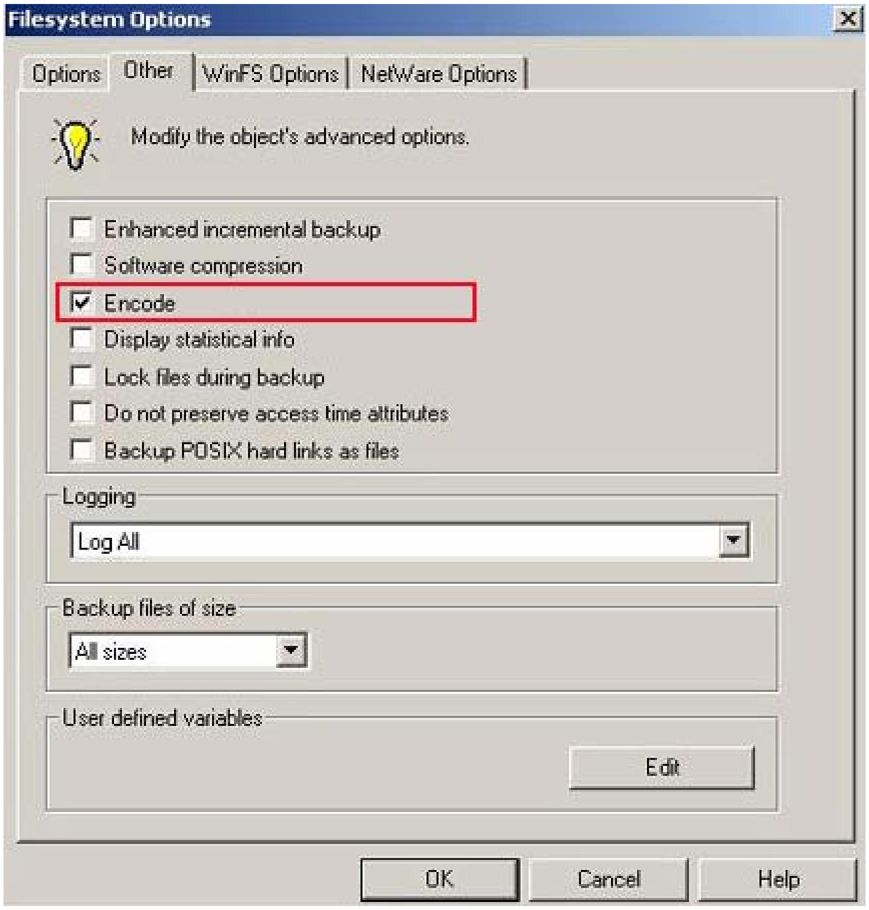
- Enabling encryption for a backup specification
- Enabling encryption for an Internal Database (IDB) backup
- Backing up data using AES encryption on a client
- Using omnikeystore
- Restoring data using AES encryption on a client

Enabling encryption for a backup specification

To enable encryption for a backup specification, complete the following steps:

1. In the backup context, select the backup specification to be encrypted.
2. In the results area, click **Options**.
3. Click the **Advanced** button in the Filesystem Options category. The Filesystem Options window appears.

   Figure 1 shows the Filesystem Options window.



Filesystem Options

Modify the object's advanced options.

- ☐ Enhanced incremental backup
- ☐ Software compression
- ☑ Encode
- ☐ Display statistical info
- ☐ Lock files during backup
- ☐ Do not preserve access time attributes
- ☐ Backup POSIX hard links as files

Logging: Log All

Backup files of size: All sizes

User defined variables

Figure 1 Selecting the encode option in backup specification

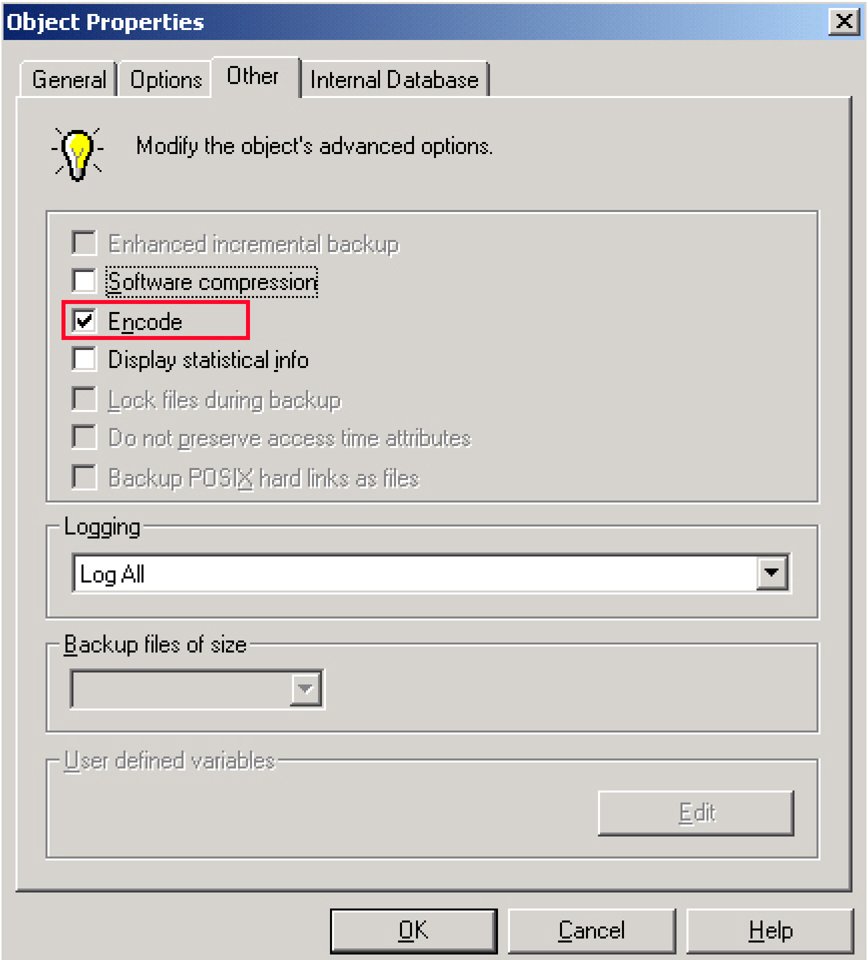
4. Click **Other**.
5. Select **Encode**.
6. Click **OK**.

Enabling encryption for an Internal Database (IDB) backup

To enable encryption for an IDB backup, complete the following steps:

1. In the backup context, click on the backup specification that you created for backing up IDB.
2. In the results area, click **Backup Object Summary**.
3. Right-click on any of the backup specification summary listed in the results area, and select **Properties**. The Object Properties window appears.

   Figure 2 shows the Object Properties window.



Modify the object's advanced options.

□ Enhanced incremental backup
□ Software compression
☑ Encode
□ Display statistical info
□ Lock files during backup
□ Do not preserve access time attributes
□ Backup POSIX hard links as files

Logging: Log All

Backup files of size

User defined variables

Figure 2 Selecting the encode option in IDB

4. Click **Other**.
5. Select **Encode**.
6. Click **OK**.

Backing up data using AES encryption on a client

To back up data using AES encryption on a client, complete the following steps:

1. Enter the following command to create a new key with type 3 (AES encryption) in the `omnikeystore` file:

   ```
   $omnikeytool -create
   ```

   A `Successfully created a key` message is displayed.

   For information on the `omnikeytool` command, see omnikeytool.
   For information on the `omnikeystore` file location, see Using omnikeystore.

> NOTE:
>
> In the above command, –type 3 or AES encryption is used by default. New keys are created in the `omnikeystore` file by the `omnikeytool` command. If there is no `omnikeystore` file, a new file is created with a new key. The newly created key is the active key and is used automatically for backup. A time stamp is also added to this new key.

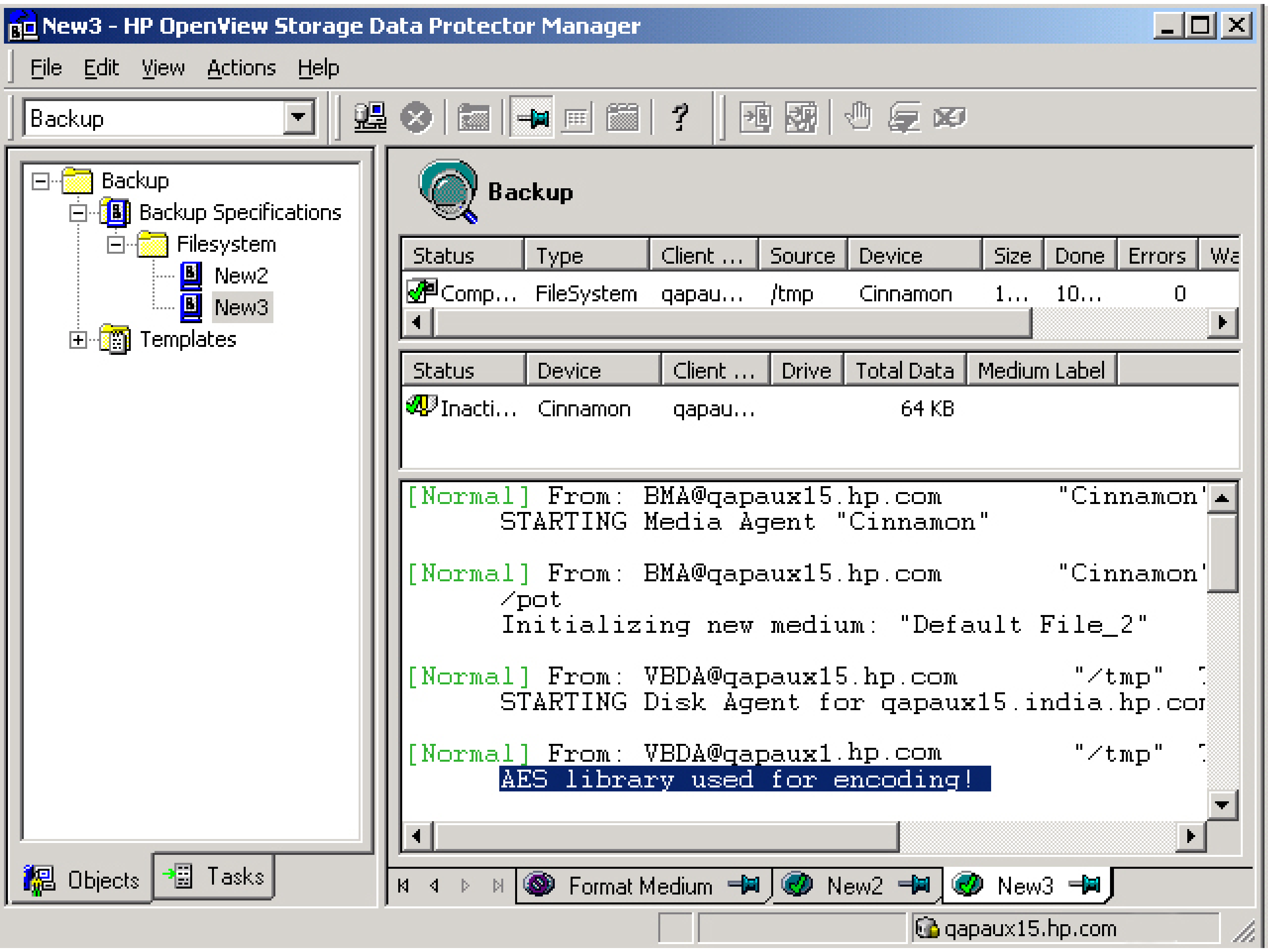
2. Either enable encryption in every backup specification by selecting the **Encode** option, or set the omnirc variable `OB2ENCODE` to `1` if you want to use encryption for every backup on this client.

   For information on enabling encryption, see Enabling encryption for a backup specification. For information on using the omnirc variables, see *HP Data Protector Help*.

3. Start backup.

   The key generated is used automatically to encrypt the backup data.

   Figure 3 shows a backup with AES encryption.



Status	Type	Client ...	Source	Device	Size	Done	Errors	Wa
Comp...	FileSystem	qapau...	/tmp	Cinnamon	1...	10...	0	

Status	Device	Client ...	Drive	Total Data	Medium Label
Inacti...	Cinnamon	qapau...		64 KB	

```
[Normal] From: BMA@qapaux15.hp.com         "Cinnamon'
      STARTING Media Agent "Cinnamon"

[Normal] From: BMA@qapaux15.hp.com         "Cinnamon'
      /pot
      Initializing new medium: "Default File_2"

[Normal] From: VBDA@qapaux15.hp.com         "/tmp"
      STARTING Disk Agent for qapaux15.india.hp.cor

[Normal] From: VBDA@qapaux1.hp.com          "/tmp"
      AES library used for encoding!
```

Figure 3 Backup with AES encryption

Using omnikeystore

The `omnikeytool` command creates new keys in the `omnikeystore` file. When a new key is created, it is made the current active backup key and is stored in the `omnikeystore` file. All previously used keys are retained for later use during restore. For information on the `omnikeytool` command, see omnikeytool. Table 6 lists the location of the `omnikeystore` file.

Table 6 Omnikeystore file locations

Operating system	Locations
Windows	`<Data_Protector_home>\omnikeystore`
HP-UX and Linux	`/opt/omni/omnikeystore`

NOTE:

The `omnikeystore` file locations can be overridden using the `OB2ENCODE_KEYSTORE` variable. Only the administrator can access or change the location of the `omnikeystore` file.

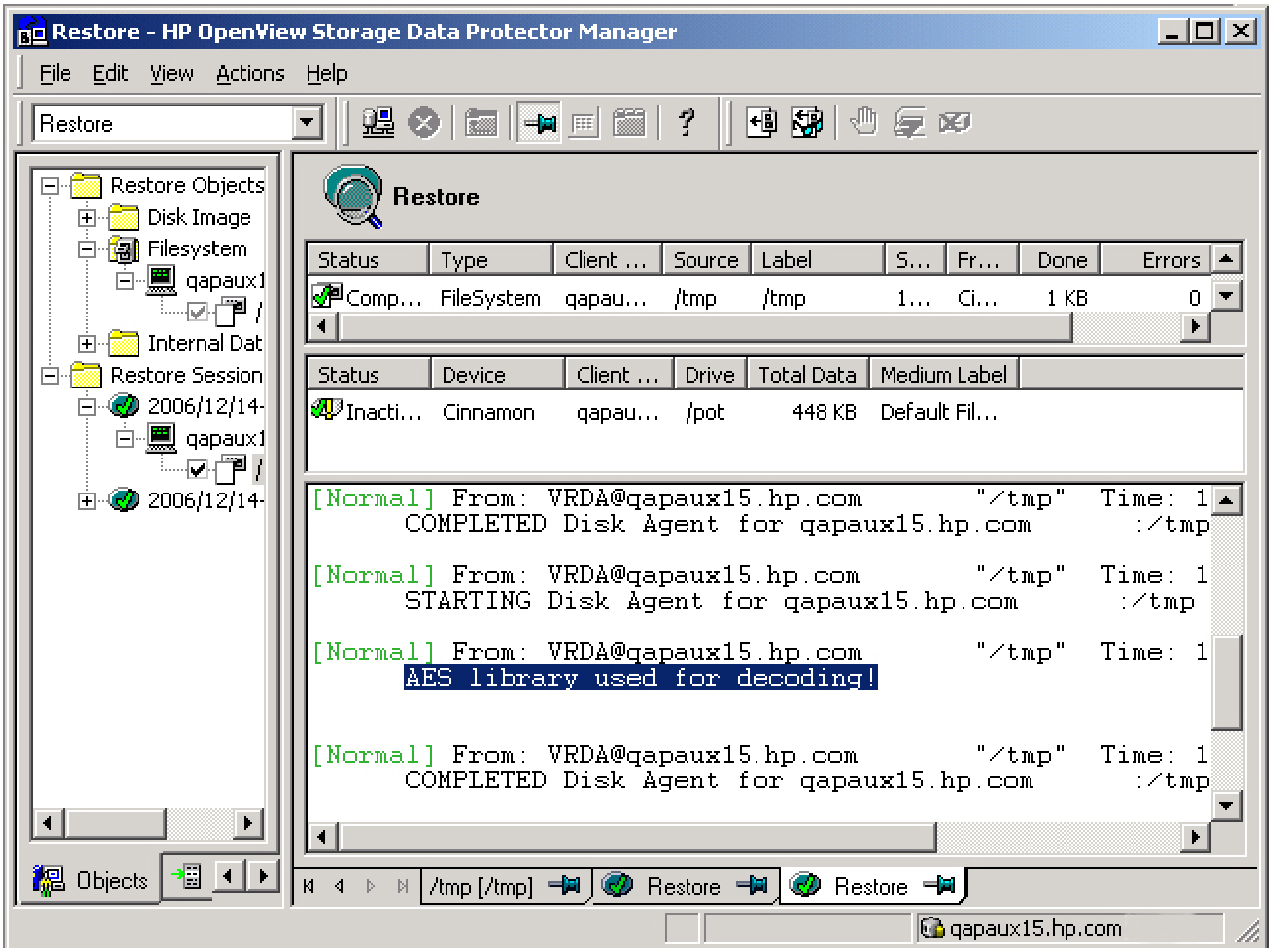
For more information on `omnikeystore` file handling, see Backing up the omnikeystore file, Managing keys in the omnikeystore file, and The omnikeystore file size.

Restoring data using AES encryption on a client

Ensure that the `omnikeystore` file is present on the host system before restoring data. If the `omnikeystore` file is not available on the host, it must be manually migrated or the key must be imported to the host before performing a restore. The `omnikeystore` file must be on a shared disk for clustered nodes. This provides the user with a common `omnikeystore` file, instead of multiple copies of the `omnikeystore` files on different nodes.

Restore data using the HP Data Protector Graphical User Interface (GUI). The key used for encryption in the corresponding backup session is automatically assigned to the restore session for decryption.

Figure 4 shows the restore operation with AES encryption.



Status	Type	Client ...	Source	Label	S...	Fr...	Done	Errors
Comp...	FileSystem	qapau...	/tmp	/tmp	1...	Ci...	1 KB	0

Status	Device	Client ...	Drive	Total Data	Medium Label
Inacti...	Cinnamon	qapau...	/pot	448 KB	Default Fil...

```
[Normal] From: VRDA@qapaux15.hp.com       "/tmp"   Time: 1
      COMPLETED Disk Agent for qapaux15.hp.com       :/tmp

[Normal] From: VRDA@qapaux15.hp.com       "/tmp"   Time: 1
      STARTING Disk Agent for qapaux15.hp.com       :/tmp

[Normal] From: VRDA@qapaux15.hp.com       "/tmp"   Time: 1
      AES library used for decoding!


[Normal] From: VRDA@qapaux15.hp.com       "/tmp"   Time: 1
      COMPLETED Disk Agent for qapaux15.hp.com       :/tmp
```

Figure 4 Restore with AES encryption

3 Additional Backup and Restore Scenarios

This chapter discusses the following topics:

- Backing up data using XOR encoding on a client
- Restoring data that is already backed up using XOR encoding or custom built encryption
- Restoring encrypted backups performed on host A to another host B
- Using the custom built encryption or XOR encoding instead of AES encryption
- Using a new key for all backups from a given host
- Using a common omnikeystore file across hosts A and B

Backing up data using XOR encoding on a client

XOR encoding is the default encryption algorithm used with HP Data Protector.

To back up data using XOR encoding on a client, complete the following steps:

1. Enter the following command to use XOR encoding on a client:

   ```
   $omnikeytool -create –type 1
   ```

   A `Successfully created a key` message is displayed.

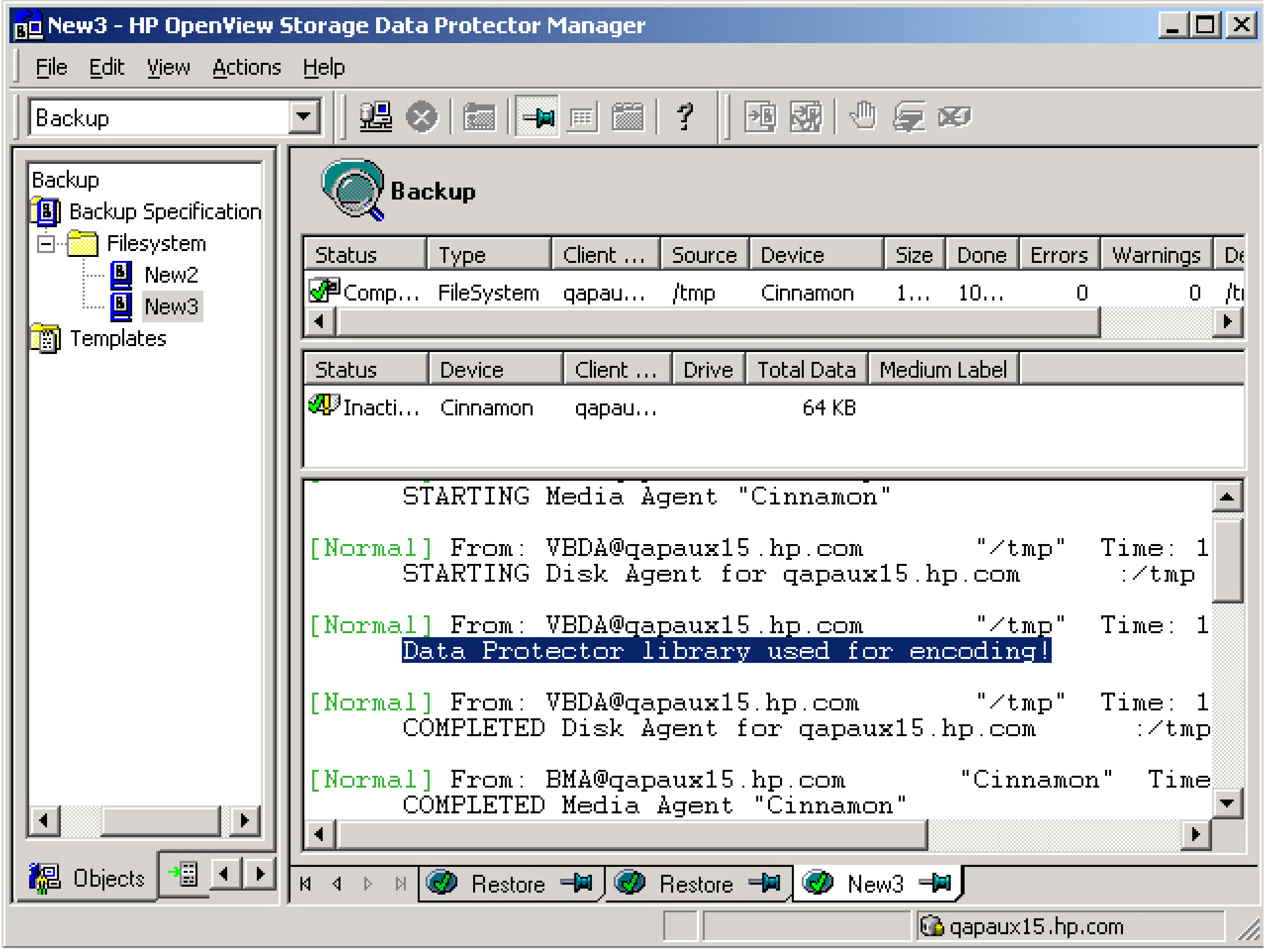
2. Either enable encryption in every backup specification by selecting the **Encode** option, or set the omnirc variable `OB2ENCODE` to `1` if you want to use encryption for every backup on this client.

   For information on enabling encryption, see Enabling encryption for a backup specification. For information on using the omnirc variables, see *HP Data Protector Help*.

3. Start backup.

   The key generated is automatically used to encrypt the data to be backed up.

   Figure 5 shows a backup with XOR encryption.



Status	Type	Client ...	Source	Device	Size	Done	Errors	Warnings	De
Comp...	FileSystem	qapau...	/tmp	Cinnamon	1...	10...	0	0	/t

Status	Device	Client ...	Drive	Total Data	Medium Label
Inacti...	Cinnamon	qapau...		64 KB	

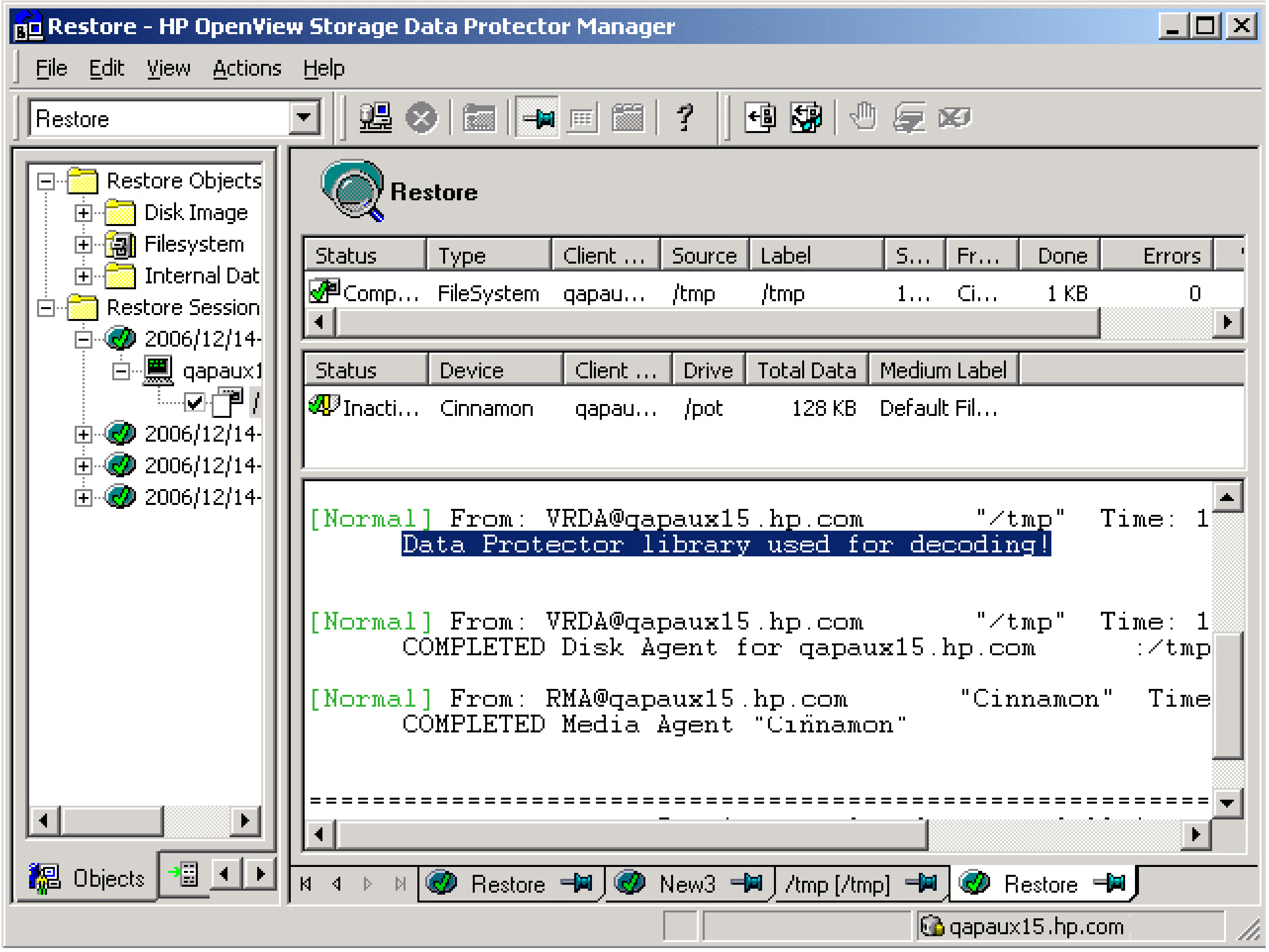
```
      STARTING Media Agent "Cinnamon"

[Normal] From: VBDA@qapaux15.hp.com       "/tmp"  Time: 1
      STARTING Disk Agent for qapaux15.hp.com      :/tmp

[Normal] From: VBDA@qapaux15.hp.com       "/tmp"  Time: 1
      Data Protector library used for encoding!

[Normal] From: VBDA@qapaux15.hp.com       "/tmp"  Time: 1
      COMPLETED Disk Agent for qapaux15.hp.com      :/tmp

[Normal] From: BMA@qapaux15.hp.com      "Cinnamon"  Time
      COMPLETED Media Agent "Cinnamon"
```

Figure 5 Backup with XOR encryption

Restoring data that is already backed up using XOR encoding or custom built encryption

To restore backed up data using XOR encoding or custom built encryption, you need not modify the keys in the `omnikeystore` file. HP Data Protector automatically determines the XOR or custom library used for encryption, and the same library is used for decryption.

Figure 6 shows the restore operation with XOR encryption.



Status	Type	Client ...	Source	Label	S...	Fr...	Done	Errors
Comp...	FileSystem	qapau...	/tmp	/tmp	1...	Ci...	1 KB	0

Status	Device	Client ...	Drive	Total Data	Medium Label
Inacti...	Cinnamon	qapau...	/pot	128 KB	Default Fil...

```
[Normal] From: VRDA@qapaux15.hp.com        "/tmp"   Time: 1
      Data Protector library used for decoding!


[Normal] From: VRDA@qapaux15.hp.com        "/tmp"   Time: 1
      COMPLETED Disk Agent for qapaux15.hp.com        :/tmp

[Normal] From: RMA@qapaux15.hp.com       "Cinnamon"   Time
      COMPLETED Media Agent "Cinnamon"


=================================================================
```

Figure 6 Restoring with XOR encryption or a custom built encryption

NOTE:

The `libde` library used for encryption during backup must not be replaced, because the same file is used for decryption during restore.

Restoring encrypted backups performed on host A to another host B

To restore any encrypted backups performed on host A to another host B, complete the following steps:

1. On host A, check the key number (KEY NO) of the key to be imported by entering the `omnikeytool -print` command. Note the key number given in the `KEY NO` field that is used for backup.

   Example:

   On host A, enter the following command:

   ```
   #omnikeytool -print
   ```

   ```
   *********************************OMNIKEYSTORE*********************************
   ------------------------------------------------------------------------------
   |KEY NO|  |TYPE| |STATUS|               |KEY ID|                |START TIME|
   ------------------------------------------------------------------------------
   1          1     INACTIVE  --------------------------------  10:32 27-Oct-2006
   2          3     INACTIVE  d08840ac28b361f02b3530514b505cc2  10:34 27-Oct-2006
   3          1     INACTIVE  --------------------------------  10:35 27-Oct-2006
   4          3     INACTIVE  dc7d01a744e8c89433f93b4d235f6c68  10:35 27-Oct-2006
   5          1     INACTIVE  --------------------------------  10:41 27-Oct-2006
   6          3     ACTIVE    7ba3b522ba3c66ad73e8b411d6f5a997  10:42 27-Oct-2006
   ```

   In this output, if the key with the key number (KEY NO) 2 is used to take a backup of the file on host A, then import key 2 after performing step 2.

2. Copy the `omnikeystore` file from host A to host B on any location other than `/opt/omni`.

   Example:

   You can copy the file to the `/tmp` directory using ftp or rcp.

3. Import the key with the key number (KEY NO) to the host B's `omnikeystore` file by entering the following command:

   ```
   #omnikeytool -import -keyno <KEY_NO> -file <SOURCE_KEYSTORE>
   ```

   Example:

   Import the key with the key number (KEY NO) 2 into host B's `omnikeystore` file by using the following command:

   ```
   #omnikeytool -import -keyno 2 -file /tmp/omnikeystore
   ```

   A `Successfully imported the record` message is displayed.

   NOTE:

   Imported keys are used only for restore.

   For information on managing keys, see Managing keys in the omnikeystore file.

You can now restore data on host B for the encrypted file backed up on host A.

Using the custom built encryption or XOR encoding instead of AES encryption

Table 7 lists the use of custom built encryption or XOR encoding, instead of AES encryption for backups and restore.

Table 7 Recommended steps for using XOR encoding or custom built encryption

Condition	Steps to be performed
If the `omnikeytool` command is not used to create the `omnikeystore` file.	Set the encode option in the HP Data Protector GUI or set the omnirc variable `OB2ENCODE` set to `1`, so that backups are encoded using XOR/custom library for encoding. For information on enabling encryption, see Enabling encryption for a backup specification. For information on using the omnirc variables, see *HP Data Protector Help*.
If the `omnikeytool` command is already used to create the `omnikeystore` file.	• Use the `omnikeytool -create -type -1` command in the HP Data Protector Command-Line Interface (CLI) to indicate that you want to use XOR encoding. • To select the custom built encryption, use the command `omnikeytool -create -type -<type no>`, where:-<*type no*> is the number used for the custom built encryption. NOTE: Here, the -<*type no*> is greater than or equal to 50, and depends on the custom built encryption being used. • To deactivate AES encryption, use the command `omnikeytool -deactivate -keyno <KEY_NO>`. For more information, see Deactivating the backup key to a key with a serial number. To reactivate AES encryption, use the command `omnikeytool -activate -keyno <KEY_NO>`. For more information, see Setting the backup key to a key matching a key number.

Using a new key for all backups from a given host

Enter the `omnikeytool -create` command to create a new key for all backups from a given host.

The newly generated key is automatically used as the backup key. No other configuration is required.

All disk agents (even from existing sessions) that start after the new key creation use the new key for backups.

Using a common omnikeystore file across hosts A and B

To use a common `omnikeystore` file across hosts A and B, complete the following steps:

1. Use the omnirc variable `OB2ENCODE_KEYSTORE` to specify the location of the shared `omnikeystore` file on host A and B.
2. Use the `omnikeytool -create` command to create an AES backup key and activate it.
3. On hosts A and B, set up backup specifications with the encode option turned on, or set the `OB2ENCODE` variable to `1`. For information on enabling the encode option, see Enabling encryption for a backup specification. For information on using the omnirc variables, see *HP Data Protector Help*.

Restore operation performed on the hosts automatically determines the key for decryption.

4 Best Practices

This chapter discusses the following best practices for using AES encryption:

- Backing up the omnikeystore file
- The omnikeystore file size
- Managing keys in the omnikeystore file
- Using AES Encryption in the simplest way

Backing up the omnikeystore file

Ensure that the `omnikeystore` file is backed up.

IMPORTANT:

If the `omnikeystore` file is not backed up and if this file is corrupt, you cannot restore the backed up files. If HP Data Protector is used for `omnikeystore` file backup, do not use backup encryption.

The user must not add a key, activate or deactivate a key, or import a key on the `omnikeystore` file when a backup of the `omnikeystore` file is in progress. This can corrupt the `omnikeystore` file, and a corrupt `omnikeystore` file results in loss of backup data. HP recommends that you backup the `omnikeystore` file every time a new key is added or imported to it.

Managing keys in the omnikeystore file

You must keep track of the keys used for `omnikeystore` file, so that you can import it easily while using it on any other client. You can do this by noting the key number (KEY NO) of the key used to back up specific files. If you have not kept track of the keys, you must either change the location of the `omnikeystore` file to the copied `omnikeystore` file location and change it back to the pre-existing location, or import all keys as described in the Restoring encrypted backups performed on host A to another host B section.

The omnikeystore file size

The maximum possible file size for the `omnikeystore` file depends on the file system properties of the operating system. For proper usage of the keys in the `omnikeystore` file, ensure that the `omnikeystore` file size does not exceed 2 GB.

Using AES Encryption in the simplest way

To use AES encryption in the simplest way, complete the following steps:

1. Create one `omnikeystore` file with only one encryption key.
2. Copy the `omnikeystore` file on all the clients.

5 Limitations

Following are the limitations of using AES encryption on HP Data Protector 6.0:

- Backed up data **cannot be restored** without the `omnikeystore` file.
- Disaster recovery is not supported with encrypted backups. Therefore, you must not encrypt backups used for Disaster Recovery restore.
- Keys can be managed only from the HP Data Protector CLI only.
- Key management is not centralized.
- A key that is accidentally created and not used in any of the backups cannot be deleted.
- Synthetic full and Virtual full backups are not supported.
- Encrypted backup of Integration Agents is not supported.

6 Troubleshooting

This chapter discusses some of the common issues encountered while using AES encryption for HP Data Protector 6.0:

Table 8 lists the common issues encountered while using AES encryption for HP Data Protector 6.0.

Table 8 Common issues

Error message	Possible cause	Recommended steps
AES library initialization failed! during backup	• The `omnikeystore` file is not present. • The key for AES encryption is deactivated. • The `OB2ENCODE_KEYSTORE` variable contains a path where the `omnikeystore` file may not be present. • XOR encoding or a custom built encryption is used.	1. In the HP Data Protector CLI, enter the `omnikeytool -print` command and check if a key of type 3 exists and its status is active. 2. If an active key of type 3 exists, then ensure that the path mentioned for the `omnikeystore` file in the omnirc variable `OB2ENCODE_KEYSTORE` is correct. For information on using the omnirc variables, see *HP Data Protector Help*. 3. If there are no keys listed as active in the status column, activate the key using the `omnikeytool -activate -keyno` *<KEY_NO>* command. For more information, see Setting the backup key to a key matching a key number. 4. If you get the message `Not able to open the Keystore`, see Not able to open the Keystore. 5. If a key other than type 3 is listed as active, create the AES encryption key using the `omnikeytool -create` command. 6. If you intended to use the XOR encoding or custom built encryption, then ignore this message, if the `Data Protector Library used for Encoding` message is present. 7. If you still get this message after completing all the above steps, contact your HP support representative.

Error message	Possible cause	Recommended steps
AES library initialization failed! during restore	The AES key used for backup may not be present in the omnikeystore file.	If you are restoring the file from another host that was not used to perform backups, then ensure that you follow the steps described in the Restoring encrypted backups performed on host A to another host B section. In addition, you must also ensure that you imported the appropriate key. For more information, see Managing keys in the omnikeystore file. If you still get this message after performing the above step, contact your HP support representative.
	omnikeystore file on the host is corrupt.	Restore the omnikeystore file from the backup media. If you still get this message after restoring the omnikeystore file, contact your HP support representative.
	The omnikeystore file is not present in the location specified by the OB2ENCODE_KEYSTORE variable, or the OB2ENCODE_KEYSTORE variable contains a path where the omnikeystore file may not be present.	If the OB2ENCODE_KEYSTORE variable is explicitly used in the omnirc file ensure that the PATH is set correctly. Example: OB2ENCODE_KEYSTORE=/home/enc/omnikeystore If you still get this message after correcting the path, contact your HP support representative.
Not able to open the Keystore message when the omnikeytool -print command is executed.	The omnikeystore file is not present.	Create the AES encryption key using the omnikeytool -create command. If you still get this message after creating the omnikeystore file, contact your HP support representative.

7 Frequently asked Questions (FAQs)

Following are some of the common questions and answers:

What is encryption?

Encryption is a way to make data unreadable to others while still allowing authorized users to access it. It requires the user or system to have a specific key and software to encrypt and decrypt the data. It utilizes various mathematical algorithms for transforming clear text into cipher text and then back again.

Encryption is the process of changing data into a form that can be read only by the intended receiver. To decipher the message, the receiver of the encrypted data must have the proper decryption key (acts like a password). In traditional encryption schemes, the sender and the receiver use the same key to encrypt and decrypt data.

In this case the key is generated by the `omnikeytool` command and stored in the `omnikeystore` file. This key is used to encrypt the data to be backed up and the same key is retrieved from the `omnikeystore` file used for decrypting data.

Why do you need to encrypt data while you backup or restore?

There are numerous ways of accessing data when it is backed up on the disks or tapes. One such way of accessing data is to physically remove the disks from the existing library or the servers and access it by connecting the same to another system.

Hence, the data that is protected on the disk or tapes is insecure this way. To ensure that there is no such problem of data being stolen from the tapes; we need to encrypt the data to prevent data access to any unauthorized personnel.

Why should I use AES encryption?

As the name suggests it is an Advanced Encryption Standard (AES) used to produce random keys which encrypts the existing data to make it cryptic. AES is an efficient encryption algorithm and is ranked as secure for the next 30 years. AES with 192 bit and 256 bit is approved for encryption of US-secret and top-secret classified data.

What are the advantages of using the AES encryption over other encryption types?

AES is a cryptographic algorithm that protects sensitive, unclassified information. The National Security Agency (NSA) reviewed all the AES finalists, including Rijndael, and stated that all of them were secure enough for US Government non-classified data. In June 2003, the US Government announced that AES may be used for classified information by stating the following:

"*The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths. The implementation of AES in products intended to protect national security systems and/or information must be reviewed and certified by NSA prior to their acquisition and use.*"

When to encrypt backup data?

You can encrypt backup data under any of the following circumstances:

- When the backup data is treated as confidential.
- When the backup data is of high value for criminals.

  For example, following data is of high value to the criminals:

  - Credit card information
  - Account information

- When backing up any customer related data, for example customer contact information.
- When the tapes containing backup information is moved off site.
- Backup to remote disk hosted by a service provider.
- Backup to removable disk.

Do I need the omnikeystore file for media copy/object copy?

No, because the DA is not involved in the media copy.

Can I specify within a backup specification two different objects with different encryption methods?

Yes, if you are using different omnirc files (on different clients).

Is media copy possible from a tape with unencrypted content?

Media copy uses MA only, therefore no DA-encryption is possible from a tape.

Why do we have a support matrix for AES encryption but not for the old XOR-encoding?

XOR encoding is supported with all DAs.

A omnikeytool

Name:

`omnikeytool` - enables the user to manage keys used for AES encryption.

Synopsis:

omnikeytool -help

omnikeytool -create [-type <*ENCR_TYPE*> (1-255 Default=3)]

omnikeytool -activate -keyno <*KEY_NO*>

omnikeytool -deactivate -keyno <*KEY_NO*>

omnikeytool -print [-file <*KEYSTORE*>]

omnikeytool -import -keyno <*KEY_NO*> -file <*SOURCE_KEYSTORE*>

Description:

This command enables the user to manage keys used for AES encryption. You must generate the key using `omnikeytool` command before using AES encryption. Before starting a restore operation, you must set the appropriate key in order to obtain the correct decrypted data.

Options:

`-help`	Displays the usage synopsis for the `omnikeytool` command.
`-create`	Creates a new key record and also updates the backup offset to point to this record.
`-activate -keyno` <*KEY_NO*>	Sets the key matching the key number as the backup key.
`-deactivate -keyno` <*KEY_NO*>	Deactivates the backup key that matched the key number.
`-print`	Prints the key records stored in the `omnikeystore` file. You can obtain the date or key number that you require for restore by viewing the records printed.
`-import -keyno` <*KEY_NO*> `-file` <*SOURCE_KEYSTORE*>	Imports the record matching the key number from the target `omnikeystore` file.

Example 1. Creating a new key and setting it as an active key for subsequent backup sessions

To create a new key and set it as an active key for subsequent backup sessions, enter the following command:

```
omnikeytool -create
```

Example 2. Setting the backup key to a key matching a key number

To set the backup key to a key whose key number (KEY NO) is 3, enter the following command:

```
omnikeytool -activate -keyno 3
```

NOTE:

The activate option sets the encryption key for the subsequent backup sessions. However during restore, the key that was used during backup is identified and used automatically for decryption.

Example 3. Deactivating the backup key to a key with a serial number

To deactivate the backup key to a key with key number (KEY NO) 3, enter the following command:

```
omnikeytool -deactivate -keyno 3
```

NOTE:

The deactivate option deactivates all the keys in the `omnikeystore` file and ensures that no AES encryption key is active. If the encode option is still selected, the backup sessions use XOR encoding by default.

Example 4. Printing the contents of the omnikeystore file

To print the contents of the `omnikeystore` file, enter the following command:

```
omnikeytool -print
```

The following output is displayed:

```
*********************************OMNIKEYSTORE*********************************
------------------------------------------------------------------------------
|KEY NO|  |TYPE| |STATUS|              |KEY ID|                |START TIME|
------------------------------------------------------------------------------
1          1     INACTIVE  --------------------------------  10:32 27-Oct-2006
2          3     ACTIVE    d08840ac28b361f02b3530514b505cc2  10:34 27-Oct-2006
3          1     INACTIVE  --------------------------------  10:35 27-Oct-2006
4          3     INACTIVE  dc7d01a744e8c89433f93b4d235f6c68  10:35 27-Oct-2006
5          1     INACTIVE  --------------------------------  10:41 27-Oct-2006
6          3     INACTIVE  7ba3b522ba3c66ad73e8b411d6f5a997  10:42 27-Oct-2006
7          1     INACTIVE  --------------------------------  10:44 27-Oct-2006
8          3     INACTIVE  9b41b91fa3279e0f58cd3920ef3586d3  10:44 27-Oct-2006
9          3     INACTIVE  10424a3a72f4367bb72c8a2728d1533d  10:20 23-Oct-2006
10         3     INACTIVE  386cde669350806ecabe014723e0bd3c  14:44 27-Oct-2006
******************************************************************************
```

Example 5. Importing a key from another omnikeystore

To import a particular key from another `omnikeystore` file into the current `omnikeystore` file, enter the following command:

```
omnikeytool -import -keyno 3 -file <SOURCE_KEYSTORE>
```

Glossary

Cipher An algorithm to encrypt and decrypt data.

libde File used for encryption in XOR encoding and custom built encryption.