

Dell™ NetVault™ Backup Plug-in for Standard Encryption 2.2

User's Guide



© 2014 Dell Inc.
ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Dell Inc.

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Dell Inc.
Attn: LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656

Refer to our web site (software.dell.com) for regional and international office information.


Patents


This product is protected by U.S. Patents # 7,814,260; 7,913,043; 7,979,650; 8,086,782; 8,145,864; 8,171,247; 8,255,654; 8,271,755; 8,311,985; and 8,452,731. Protected by Japanese, E.U., French, and UK patents 1615131 and 05250687.0, and German patent DE602004002858. Additional patents pending. For more information, go to <http://software.dell.com/legal/patents.aspx>.


Trademarks

Dell, the Dell logo, and NetVault are trademarks of Dell Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims any proprietary interest in the marks and names of others.

Legend

 **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

 **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

 **IMPORTANT NOTE, NOTE, TIP, MOBILE,** or **VIDEO:** An information icon indicates supporting information.

Plug-in for Standard Encryption User's Guide
Updated - April 2014
Software Version - 2.2
NVG-122-2.2-EN-01

Contents

Introduction	4
About Dell™ NetVault™ Backup Plug-in for Standard Encryption	4
Target audience	5
Recommended additional reading	5
Defining a backup strategy	6
Encryption strategy overview	6
Selecting which backups to encrypt	6
Selecting the encryption algorithm	7
Encrypting primary or secondary backups	7
Encrypting all or specific backups	8
Installing the plug-in	9
Deployment overview	9
Installing the plug-in	10
Removing the plug-in	10
Configuring the plug-in	11
Configuring default settings	11
Using the plug-in	12
Encrypting all backups	12
Performing job-level encryption	12
Encrypting primary backup	12
Encrypting a Secondary Copy	12
About Dell	14
Contacting Dell	14
Technical Support Resources	14

Introduction

- [About Dell™ NetVault™ Backup Plug-in for Standard Encryption](#)
- [Target audience](#)
- [Recommended additional reading](#)

About Dell™ NetVault™ Backup Plug-in for Standard Encryption

Dell™ NetVault™ Backup (NetVault Backup) offers two encryption products:

- **Dell™ NetVault™ Backup Plug-in for Standard Encryption (Plug-in for Standard Encryption)** - The Plug-in for Standard Encryption provides support for CAST-128 algorithm to protect your data and meet the regulatory requirements.

CAST-128 is a 12- or 16-round Feistel network with a 64-bit block size and a key size of between 40 to 128 bits, but only in 8-bit increments.
- **Dell™ NetVault™ Backup Plug-in for Advanced Encryption (Plug-in for Advanced Encryption)** - The Plug-in for Advanced Encryption provides support for AES-256 and CAST-256 algorithms to protect your data and meet the regulatory requirements.
 - **CAST-256** - CAST-256 uses the same elements as CAST-128, but it is adapted for a block size of 128 bits - twice the size of its 64-bit predecessor. Acceptable key sizes are 128, 160, 192, 224 and 256 bits. CAST-256 is composed of 48 rounds, sometimes described as 12 "quad-rounds", arranged in a generalized Feistel network.
 - **AES-256** - Advanced Encryption Standard (AES) is an encryption standard adopted by the U.S. government. The standard comprises three block ciphers, AES-128, AES-192 and AES-256. Each AES cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively.

NOTE: The CAST-128 and CAST-256 encryption algorithms do not comply with the requirements of the United States Federal Information Processing Standard (FIPS). These algorithms are provided for the restoration of legacy data. For FIPS compliance, use the AES-256 algorithm.

When installed on the NetVault Backup Client, these plug-ins encrypt and transfer data across the network to the backup device, where the data remains encrypted until restored to the client. If encryption is only required for secondary storage, job-level encryption offers the choice of encrypting only the secondary copy while the primary backup remains unencrypted to shrink the backup window. When using disk-based storage devices, job-level deduplication allows you to separate deduplicated from non-deduplicated unencrypted data for optimal deduplication ratios and performance.

The Plug-in for Standard Encryption and the Plug-in for Advanced Encryption are installed and licensed separately. For a list of NetVault Backup Plug-ins that are incompatible with the Plug-in for Standard Encryption and Plug-in for Standard Encryption, refer to the respective Release Notes.

NOTE: The NetVault Backup encryption architecture only supports the Electronic Code Book (ECB) mode of operation. This means that every data block is encrypted individually. If two or more consecutive blocks contain identical data, the encrypted forms of these blocks will also be identical.

Target audience

This guide is intended for Backup Administrators and other technical personnel who are responsible for designing and implementing a backup strategy for the organization. Familiarity with encryption solutions is assumed.

Recommended additional reading

- *Dell NetVault Backup Installation Guide* - This guide provides information about installing the NetVault Backup Server and Client software.
- *Dell NetVault Backup Administrator's Guide* - This guide provides information about configuring and using NetVault Backup to protect your data. It provides comprehensive information about all NetVault Backup features and functionality.
- *Dell NetVault Backup Command Line Interface Reference Guide* - This guide provides information about using the NetVault Backup command line utilities.

You can download these guides from <https://support.software.dell.com/>.

- ① **IMPORTANT:** Starting with 10.0, NetVault Backup provides a web-based user interface to configure, manage, and monitor your NetVault Backup system and installed plug-ins. The procedures described in the user's guide for this version of the plug-in are intended for the new NetVault WebUI. For procedures based on the NetVault Backup Console (user interface available with NetVault Backup 9.x and 8.x), refer to the documentation for an earlier version of the plug-in.

Defining a backup strategy

- [Encryption strategy overview](#)

Encryption strategy overview

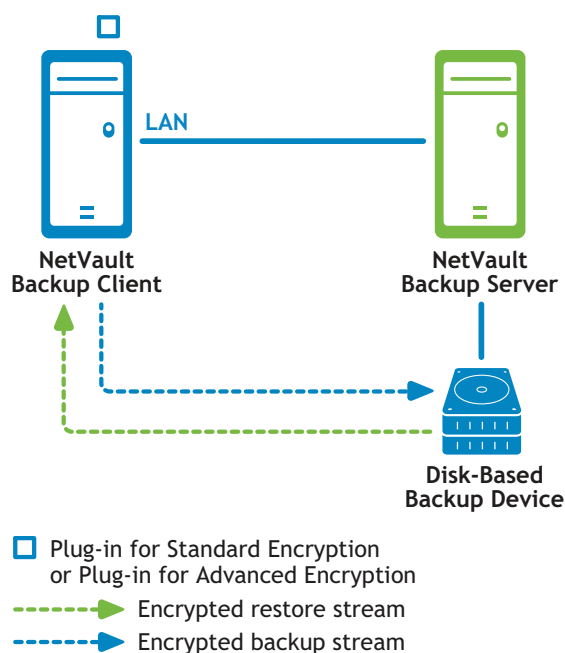
When defining an encryption strategy, you must determine the following:

- Which backups will be encrypted.
- Which encryption algorithm is required.
- Whether encryption is required for primary backups or secondary backups.
- Whether encryption will be enabled for all backups or on a per-job basis.

Selecting which backups to encrypt

NetVault Backup performs software-based encryption. The backup stream is encrypted using the selected algorithm by the NetVault Backup Server or Client where the plug-in is installed. The encrypted data stream is transferred over the network to the backup device where it remains encrypted. During restore, the encrypted backup is transferred from the backup device to the targeted NetVault Backup client, where the plug-in installed on the client completes the decryption.

Figure 1. Encrypted backup and restore path



NOTE: Installing the Plug-in for Standard Encryption or Plug-in for Advanced Encryption on the NetVault Backup Server is only required to encrypt the backups that originate from the server, such as NetVault Database backups. It is not required to encrypt backups that originate on a client running any built-in or licensed plug-in.

The backup encryption and decryption processes are performed by the plug-in installed on the NetVault Backup Server or Client. These processes use resources on the machine. The encryption process lengthens the time it takes to perform backups, while the decryption process lengthens the time it takes to perform restores. The impact to the performance of the client, backup window, and restore time should be considered when deciding which backups need to be encrypted. In summary, backups should only be encrypted when security requirements outweigh the impact to performance, backup windows, and restore times.

Selecting the encryption algorithm

NetVault Backup provides multiple algorithms that can be used to encrypt and decrypt backups. While each NetVault Backup client can use a different encryption algorithm, all backups from a particular client must use the same algorithm.

The same encryption algorithm that was used during backup must be used during restores. It is possible to utilize a different algorithm from this point forward than was previously used. However, when restoring backups that used the previous algorithm, the NetVault Backup Server or Client must be configured to specify the algorithm used by the backup to restore data successfully. For example, if previous backups used the CAST-128 algorithm while current backups are using the AES-256 algorithm, the plug-in must be configured on the server or client to utilize the CAST-128 algorithm when restoring a backup that was taken using that algorithm; otherwise, restore will fail.

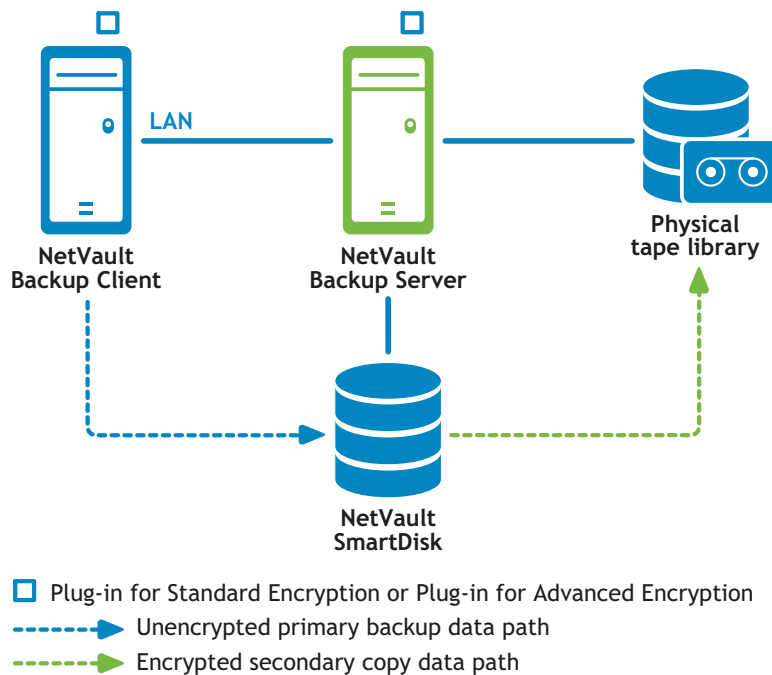
Encrypting primary or secondary backups

A backup job consists of one or optionally two phases - Primary Backup and Secondary Copy. The primary backup is the backup of data stream to the selected backup device. These backups are generally performed to local storage devices to enable faster restores. The Secondary Copy is a Duplicate or Data Copy of the primary backup to a different backup device. These backups are usually targeted to remote disk-based storage devices or physical tape libraries whose tapes are stored offsite for disaster recovery purposes.

Your security requirements will dictate whether you require encryption for both the primary backups and the secondary copies. For example, if the security requirements dictate that only the backups that leave the corporate network require encryption (such as those stored on physical tapes in a remote location), you just need to encrypt the secondary copy backups that target the physical tape libraries. However, if the security requirements dictate that data must be encrypted while it transfers across the network or while it is stored on a disk-based backup device - even if the disk-based backup device is located within the corporate network - you need to encrypt both the primary backup and secondary copy.

Encrypted data does not deduplicate well. Therefore, encrypting only the secondary copy backup is beneficial when the primary backups are performed to storage devices that support deduplication. This allows you to take advantage of both encryption and deduplication by deduplicating the primary backup and encrypting the secondary copy.

Figure 2. Unencrypted primary backups and encrypted secondary copy backups



Encrypting all or specific backups

Once the Plug-in for Standard Encryption or Plug-in for Advanced Encryption is installed, you can enable encryption for all backups on the NetVault Backup Server or Client where the plug-in is installed, or enable encryption only for specific jobs. Encryption can also be enabled only for the primary backup or the secondary copies. This allows you to take advantage of both encryption and deduplication. For example, you can deduplicate the primary backup and encrypt the secondary copy.

The job-level encryption option can be used in the following situations:

- When any plug-in installed on the server or client is incompatible with the Plug-in for Standard Encryption or Plug-in for Advanced Encryption.
- Only specific backups on the server or client require encryption.
- Primary backups do not require encryption while secondary backups for offsite protection require encryption.
- Primary backups are targeted to storage devices that support deduplication.

The NetVault Backup Server and Client should only be configured to encrypt all its backups in the following situations:

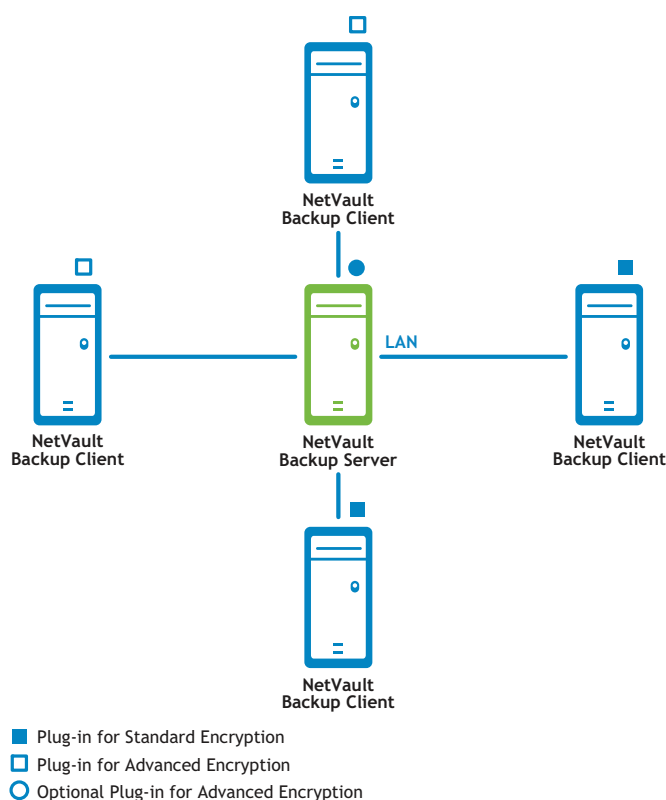
- All plug-ins installed on the server or client are compatible with the Plug-in for Standard Encryption or Plug-in for Advanced Encryption.
- All backups from the server or client require encryption.
- Both primary and secondary backups require encryption.
- Backups are not selected for deduplication.

Installing the plug-in

- Deployment overview
- Installing the plug-in
- Removing the plug-in

Deployment overview

Figure 1. Deployment overview




The Plug-in for Standard Encryption or Plug-in for Advanced Encryption must be installed on all NetVault Backup clients on which the backups will be encrypted. For each client, you must obtain a separate permanent license key. The server and clients can be configured to use different encryption algorithms, except when using the server or client to create encrypted secondary copies.

For example, if a client is configured to use the AES-256 algorithm, and the server is used to create the encrypted secondary copy, the server must also be configured to use the AES-256 algorithm to ensure that the secondary copy backups can be restored by the client.


Installing the plug-in

To install plug-in

- 1 In the Navigation pane, click **Guided Configuration**, and then in the **NetVault Configuration Wizard** page, click **Install Plugins**. In the **NetVault Backup Clients** list, select the clients on which you want to install the plug-in. This method allows you to select multiple clients.

 **NOTE:** When you select multiple clients, ensure that the plug-in binary file is compatible with the OS and platforms of the target clients.

- or -

In the Navigation pane, click **Manage Clients**. In the **NetVault Backup Clients** list, select the client on which you want to install the plug-in, and click **Manage**. At the lower-right corner of the **Installed Software** table, click the **Install Plugin** button ().

- 2 Click **Choose Plug-in File**, and in the browse window, navigate to the location of the “.npg” installation file for the plug-in (on the installation CD or the directory to which the file was downloaded from the web site).
- 3 Select the platform-specific binary file for the plug-in. The files names listed in the following table (where x-x-x-x represent the version, build, and platform numbers).

Table 1. Binary files for supported encryption algorithms

Encryption algorithm	Binary file name
CAST-128	cst-x-x-x-x.npk
CAST-256	cst2-x-x-x-x.npk
AES-256	aes-x-x-x-x.npk

click **Next** to begin installation

- 4 When the installation completes successfully, a message is displayed.

Removing the plug-in

To remove the plug-in

- 1 In the Navigation pane, click **Manage Clients**.
- 2 In the **NetVault Backup Clients** list, select the client, and click **Manage**.
- 3 In the **Installed Pug-ins** table, select the algorithm that you want to remove. The options include:
 - CAST-128 Encryption
 - CAST-256 Encryption
 - AES-256 Encryption

Click the **Remove Plugin** button ().

- 4 In the **Confirm** dialog box, click **Remove**.

Configuring the plug-in

- [Configuring default settings](#)

Configuring default settings

To configure default settings for the plug-in

- 1 In the Navigation pane, click **Change Settings**, and then on the **Configuration** page, click **Server** or **Client Settings**, as applicable.
- 2 Under **Plugins**, click **Encryption**.
- 3 Configure the following settings.

Table 1. Plug-in default settings

Setting	Description
Encrypt ALL Backups on this Client	<p>Once the Plug-in for Standard Encryption or Plug-in for Advanced Encryption is installed on a client, you can do either of the following:</p> <ul style="list-style-type: none"> • Encrypt all backups performed for that client • Encrypt specific backups performed for that client <p>To enable encryption for all backups, select this check box. When you enable encryption for all backups, you cannot change the setting on a per-job basis. For more information about enabling encryption for specific backups, see Performing job-level encryption.</p> <p>NOTE: To perform job-level encryption for backups originating from a NetVault Backup Server or Client, the plug-in should not be configured for encrypting all backups.</p>
Encryption Key String	<p>Type the string that will serve as the encryption key for the NetVault Backup machine.</p> <p>Different platforms allow varying characters and password lengths. We recommend that you use passwords of 32 characters or less. You can use characters from the following set: "A-Z", "a-z", "0-9", and "_". Key strings that do not conform to these specifications may work on one platform but may be invalid in another environment.</p>
Available Encryption Algorithms	<p>Select the encryption algorithm that you want to use for backups and restores. Depending on the products that you have installed, the list includes the following options: CAST-128, CAST-256, and AES-256.</p>

- 4 Click **Apply** to apply the new settings and close the dialog box.

NOTE: An encrypted backup can be restored to either its original location or to a new target machine. In either event, the plug-in must be installed on the target machine and it must be configured as it was when the backup was performed - using the same **Encryption Key String** and **Encryption Algorithm**.

Using the plug-in

- [Encrypting all backups](#)
- [Performing job-level encryption](#)

Encrypting all backups

If encryption is enabled for all backups performed from a particular NetVault Backup Client, there are no additional requirements for encrypting backups. Refer to the backup and restore procedures in the User's Guide for the relevant plug-in.

Performing job-level encryption

The job-level encryption option can be used to encrypt the primary backup, secondary copy, or both. Encrypting both the primary backup and secondary copy is beneficial when security requirements dictate that the backup must be encrypted while it transfers across the network or while it is stored on a disk-based backup device even if the disk based backup device is located within the corporate network.

The job-level encryption setting is specified in the Backup Advanced Options Set. For more information about creating an Advanced Options Set for a backup job, refer to the *Dell NetVault Backup Administrator's Guide*.

Encrypting primary backup

To enable job-level encryption for a primary backup

- 1 Start the Backup Job Wizard, and open the **Advanced Options** page. For more information, refer to the *Dell NetVault Backup Administrator's Guide*.
- 2 Click **Additional Options**.
- 3 In the **Additional Options** dialog box, select the **Enable Encryption** check box.

Encrypting a Secondary Copy

NetVault Backup offers the following methods for creating Secondary Copies:

- **Duplicate** - This method creates an exact copy which is linked to the original backup. It breaks down the backup into segments and copies the segments to the storage device. During restore, the segments from the primary and secondary copy can be interchanged. As it is not possible to mix unencrypted segments with encrypted segments during restore, you cannot enable or disable encryption for a secondary copy created using the Duplicate method. If the original saveset is encrypted, the Duplicate method will create an encrypted secondary copy. If you have not encrypted the primary backup, the secondary copy will also be unencrypted.
- **Data Copy** - This method is recommended when you want to create a Secondary Copy for offsite storage. The Data Copy method breaks down the backup into segments and copies the segments to the backup device. During restore, either the primary or the secondary copy is used to recover data. The segments

from the primary and secondary copy are not interchanged. This allows you to encrypt the Data Copy when the primary copy is unencrypted. This is useful when you want to use the deduplication option for the primary backups.

To enable job-level encryption for a Secondary Copy

- 1 Start the Backup Job Wizard, and open the **Advanced Options** page. For more information, refer to the *Dell NetVault Backup Administrator's Guide*.
- 2 Click **Secondary Copy**.
- 3 In the **Secondary Copy** dialog box, select the **Create Secondary Copy** check box.
- 4 Select the **Encrypt Secondary Copy Only** check box. This option can only be used with the Data Copy method.

If the primary copy is encrypted, Data Copy will automatically create an encrypted saveset regardless of whether the **Encrypt Secondary Copy Only** check box is selected or not. Therefore, this option is only useful when you want to create an encrypted secondary copy from an unencrypted primary copy.

NOTE: Encrypted primary copies will not be encrypted again if you select the **Encrypt Secondary Copy Only** check box for a copy. For restoring data from such secondary copies, you must use the primary copy's Encryption Key.

Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.software.dell.com.

Contacting Dell

Technical Support:

[Online Support](#)

Product Questions and Sales:

(800) 306-9329

Email:

info@software.dell.com

Technical Support Resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions. To access the Support Portal, go to <https://support.software.dell.com/>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the portal provides direct access to product support engineers through an online Service Request system.

The site enables you to:

- Create, update, and manage Service Requests (cases)
- View Knowledge Base articles
- Obtain product notifications
- Download software. For trial software, go to [Trial Downloads](#).
- View how-to videos
- Engage in community discussions
- Chat with a support engineer