



**Symantec Backup Exec™ 11d**  
***for Windows® Servers***  
New Encryption Capabilities

# Symantec Backup Exec 11d *for Windows Servers*

## **Contents**

<b>Executive summary</b> .....	<b>4</b>
Need for encryption .....	4
<b>Safe, secure, and easy encryption with Backup Exec</b> .....	<b>5</b>
Cost versus protection .....	5
Complexity .....	5
Lack of flexibility .....	6
Lengthened backup process .....	6
<b>Product highlights</b> .....	<b>7</b>
<b>How it works</b> .....	<b>8</b>
Creating and using encryption keys .....	8
Common and restricted keys for restores .....	9
Backup process with encryption .....	10
Managing encryption keys .....	11
Deleting encryption keys .....	13
Tracking changes to encryption keys .....	14
Restore process with encryption .....	15
<b>Encryption best practices</b> .....	<b>15</b>
<b>System requirements</b> .....	<b>17</b>
Other encryption architectures .....	17
Software-based versus hardware-based encryption .....	18
<b>Summary</b> .....	<b>19</b>

## Executive summary

Security and compliance risks to businesses and their data are greater than ever. Businesses depend on their data being protected in a safe and secure manner when it is stored internally and taken offsite. With the emergence of new compliance regulations, any data loss can adversely impact the bottom line, including possible additional regulatory and compliance concerns. Implementation of an encryption strategy for your company's backups plays a vital role in safeguarding the integrity and availability of your data.

## Need for encryption

Headlines about data theft, tape loss, and compromised customer records containing unencrypted data are appearing more frequently. These events underscore the need to focus on securing critical and sensitive company data, including copies of data created during backup operations.

The window of risk to your sensitive data expands as the value of your data increases. Some of these risks include:

- Unencrypted removable media taken offsite for "security" is less secure than almost any other corporate data.
- Theft of a tape and removable media is a major risk that is difficult to track due to the size of the media.
- Data may become available to third parties if a tape is lost or left unprotected.
- There is no way to tell if a tape has been copied or duplicated for unauthorized purposes.
- Tapes are often taken offsite by the lowest cost method instead of the most secure method.
- Operators can initiate an unauthorized restore of a tape redirected to their system.

Encryption is the most effective method for securing data on portable media. Analysts, government, law enforcement, and regulatory agencies continue to advise on the criticality of encryption, and yet many companies have not yet implemented encryption as part of their backup process. The main reasons given for this decision are that encryption can add layers of complexity to their processes and that it will increase the time required to successfully complete the backup or restore process.

## Key Benefits

- Helps reduce security risks to your data through integrated 128-/256-bit AES industrial-strength encryption
- Integrated encryption key management system for easy setup and management
- Included with Backup Exec 11d *for Windows Servers* at no additional charge

## **Safe, secure, and easy encryption with Backup Exec**

Symantec™ Backup Exec 11d *for Windows Servers* now includes encryption capabilities that provide an additional layer of protection for your sensitive data, while helping to ensure that the use of encryption does not hinder the backup or restore process critical to safeguarding company assets. The new encryption capabilities of Backup Exec 11d attempt to address the concerns traditionally associated with backup encryption such as:

- Cost versus protection
- Complexity
- Lack of flexibility
- Lengthened backup process

### **Cost versus protection**

Backup Exec 11d uses industrial-strength, 128-/256-bit Advanced Encryption Standard (AES) encryption. This allows Backup Exec to provide one of the highest levels of encryption that meet or exceed strict U.S. government and corporate standards.

Backup Exec 11d encryption supports both files and databases. It provides security for your backup data regardless of where it resides or what happens to it after it leaves your site.

Unlike competing solutions, Backup Exec 11d includes these encryption capabilities at no additional charge. In this way, Symantec helps ensure that all organizations that use Backup Exec have access to safe, secure, and easily encrypted backups—regardless of their budget—to safeguard their important data.

### **Complexity**

In today's complex IT world, encryption must not only be industrial strength, but it also must be easy to manage so that it is used whenever possible. The Backup Exec 11d integrated encryption key management system helps ensure that encryption is easy to use and manageable—all from within the familiar Backup Exec console.

### **Lack of flexibility**

Backup Exec 11d encryption implementation offers the flexibility to encrypt only the data you want—when you want and where you want. Encryption can be enabled:

- On a per-backup-job basis
- On a per-policy basis for increased automation of policy-based protection
- On a global basis to help ensure all backups are encrypted per company standards
- On tape and/or disk backups

By using software as the controller of encryption rather than media hardware, administrators gain a heterogeneous security option that allows them to encrypt and decrypt data regardless of the hardware platform used for backup or recovery.

### **Lengthened backup process**

Backup Exec 11d encryption is flexible, which allows it to occur only during a particular stage of a backup. For example, companies using disk staging or disk-to-disk-to-tape (D2D2T) can enable encryption only on the tape portion of the backup. Companies that are concerned about the performance impact of software-based encryption on production systems can now perform fast, unencrypted backups to secure disk locations using the included backup-to-disk (B2D) technology. They can then configure a duplication job to run immediately after the initial disk-based backup or at a later scheduled time regardless of the backup window. This portion of the backup can be done to another disk location or to removable media, such as tape, for offsite storage where encryption is most critical. This avoids lengthening the initial backup process and also avoids any encryption-related performance impact on production systems, as the duplication job involves only data movement on the Backup Exec server.

## Product highlights

Feature	Description	Benefit
128-/256-bit Symmetric Encryption	<ul style="list-style-type: none"> <li>Provides data encryption using either 128-bit or 256-bit OpenSSL ciphers</li> </ul>	<ul style="list-style-type: none"> <li>Meets both U.S. government and corporate standards of encryption quality</li> </ul>
Integrated Encryption Key Management	<ul style="list-style-type: none"> <li>Create both common and restricted encryption keys</li> <li>Integrated into Backup Exec's console</li> <li>Checksum validation of encryption keys</li> <li>Key regeneration</li> <li>Designed for future hardware-based tape encryption standards</li> </ul>	<ul style="list-style-type: none"> <li>Restricts access to encryption keys to the proper personnel in your organization to help ensure only the proper personnel have access to critical or sensitive backup data</li> <li>No need for separate encryption key management application or hardware</li> <li>Encryption keys are checksum validated on restore operations to prevent any tampering of keys in the Backup Exec database</li> <li>If the encryption key gets deleted or destroyed, the key can be regenerated using the pass phrase</li> <li>Allows Backup Exec to manage encryption keys for future hardware-based tape encryption devices</li> </ul>
File System and Database Support*	<ul style="list-style-type: none"> <li>Provides encryption support for file systems and databases including Windows, Linux®, Macintosh®, UNIX, and Microsoft® Exchange and SQL Server</li> </ul>	<ul style="list-style-type: none"> <li>Provides security for all of your backup data regardless of what it is, where it lives, or what happens to it</li> </ul>
Flexible Encryption Configuration	<ul style="list-style-type: none"> <li>Encryption can be enabled on a per-job, per-policy, or global default basis for backups</li> </ul>	<ul style="list-style-type: none"> <li>Provides flexibility to back up and encrypt only the data you want, when you want, and where you want based on your established policies</li> </ul>
Client, Network, and Storage-Level Encryption	<ul style="list-style-type: none"> <li>Encryption occurs on the source client as the backup occurs</li> <li>Data is encrypted over the network in transit to the Backup Exec server</li> <li>Data is written to tape or disk in an encrypted format by Backup Exec for long-term storage</li> </ul>	<ul style="list-style-type: none"> <li>Protects your backup data at all times during the backup process from start to finish, beginning at the protected server</li> <li>Prevents network access to the data during the backup process over the network</li> <li>Prevents unauthorized access, tampering, or duplication of backup data while it is stored onsite or offsite on tapes or removable media</li> </ul>
Tape- and Disk-based Backup Support**	<ul style="list-style-type: none"> <li>Backups can be written to tape or disk in an encrypted format by Backup Exec 11d</li> </ul>	<ul style="list-style-type: none"> <li>Provides the flexibility to choose where data is stored in an encrypted format</li> </ul>
Limited Performance Impact	<ul style="list-style-type: none"> <li>Backups can be written to disk locations in an unencrypted format for best possible raw performance and later duplicated to tape for offsite storage</li> </ul>	<ul style="list-style-type: none"> <li>Helps ensure there is no performance impact on the source production server during the duplication process of a backup where data is encrypted from disk to tape for offsite storage</li> </ul>
Integrated Audit Logging	<ul style="list-style-type: none"> <li>Built-in Audit Log to track any changes to encryption keys, including username, time/date, and change description</li> <li>Ability to save and export Audit Logs</li> </ul>	<ul style="list-style-type: none"> <li>Increases security for compliance, and regulatory concerns of any and all changes made to encryption keys</li> <li>Helps ensure that any and all changes made to encryption keys are recorded, saved, and exported for auditing purposes</li> </ul>

\* See the table in the "System requirements" section for a complete listing of all agents supported with encryption.

\*\* Backups enabled for encryption and sent to a disk-based backup target with Backup Exec 11d for Windows Servers new Granular Recovery Technology (GRT) are not stored in an encrypted format. GRT allows individual object-level recovery for Microsoft Exchange, SharePoint, and Active Directory objects. GRT-enabled backups targeted to B2D devices are encrypted at the source server during the network transit, but they are stored in an unencrypted format on the final B2D target location. Tape-based GRT-enabled backups are stored on tape in an encrypted format and so do not have this limitation.

## **How it works**

Backup Exec 11d encryption is designed to be a comprehensive and integrated solution that works seamlessly with your normal backup operations.

## **Creating and using encryption keys**

The process of applying and managing encryption keys is simplified through integration with Backup Exec. Simply select the level of encryption you want, create the encryption key pass phrase you want when configuring backup jobs, and leave the rest to Backup Exec (see Figure 1).

Encryption keys are safely stored inside of the Backup Exec database (BEDB) in an encrypted format. The pass phrase itself is not stored in the database; only the key generated by the pass phrase is stored. Once created, encryption keys can be reused by Backup Exec for other jobs. You can set a default encryption key to use when you create:

- Backup jobs
- Templates
- Duplicate backup set jobs
- Backup policies
- Policy-based backup templates
- Policy-based duplicate backup set templates
- Policy-based synthetic full-backup policies

However, you can also override the default key for any specific job.

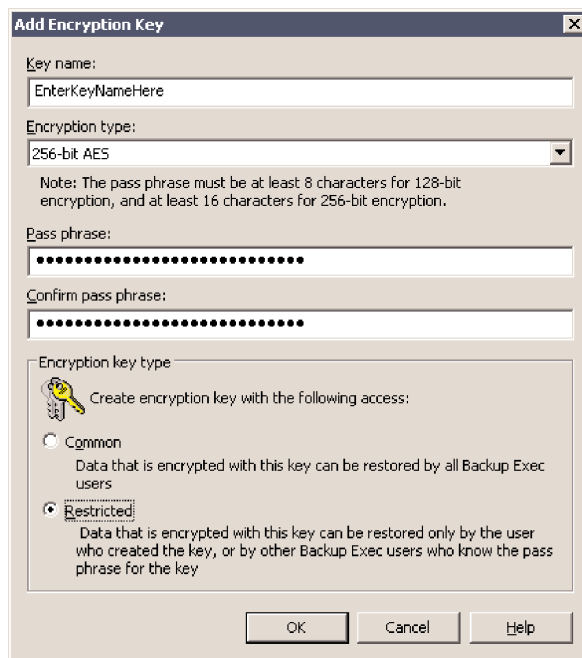


Figure 1. Creating an encryption key

### Common and restricted keys for restores

The encryption key can be either common (making it shareable) or restricted (making it private to that user). For backup jobs, any user can use any key available, regardless of whether it is common or restricted. The job log of the backup will indicate if encryption was used. The pass phrase is not included in the job log.

If a user creates a backup job using another user's restricted key, the user will get a prompt warning that the data can only be restored if the user knows the correct pass phrase for the key. For restore jobs, key validation is performed based on ownership:

- **Common keys:** Anyone can use the key to encrypt data during a backup job and to restore encrypted data. If a common key exists in the database, any user can use the key for restores.
- **Restricted keys:** Anyone can use the key to encrypt data during a backup job. If a user other than the key owner tries to restore data that was encrypted with a restricted key, Backup Exec prompts the user for the key's pass phrase. If the user cannot supply the correct pass phrase for the key, the user cannot restore the data.

For example:

- If User B tries to restore a set that was encrypted with User A's restricted key, User B will be prompted for the pass phrase. If the pass phrase is validated, User A's key will be used for restore, and no new key will be created in the database.
- If User B tries to edit a restore job that uses User A's restricted key, User B will be prompted for the pass phrase.

**Important Note:** Backup Exec 11d utilizes industrial-strength 128-/256-bit AES encryption that meets both U.S. government and corporate standards of encryption quality. Once data has been encrypted, it cannot be recovered by anyone without the encryption key pass phrase, including Symantec.

You will be prompted with a warning message when creating a new encryption key to remember the pass phrase or store it in a secure location (see Figure 2).

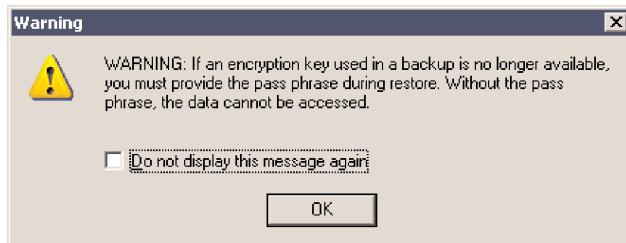


Figure 2. Pass phrase warning

## Backup process with encryption

When you install Backup Exec, the installation program installs the necessary encryption software on the Backup Exec media server and on remote computers that use the Remote Agent.

Backup Exec software performs the data encryption on the client via the Remote Agent, transfers the data across the network, and then stores it on tape or disk in the encrypted format. The backup process follows this sequence:

1. The Backup Exec 11d media server sends the encryption keys to the Backup Exec Remote Agent installed on the client system. The keys are protected via asymmetric encryption during this transfer.

2. Data is encrypted at the Backup Exec 11d Remote Agent client with symmetric encryption using the specified AES 128-bit or 256-bit key.
3. Data is sent encrypted over the network to the Backup Exec 11d media server and written to the backup device specified in the backup job.

Figure 3 shows the data flow of Backup Exec 11d encryption from original source servers, to network, to final storage location using the Backup Exec 11d Remote Agent and media server.

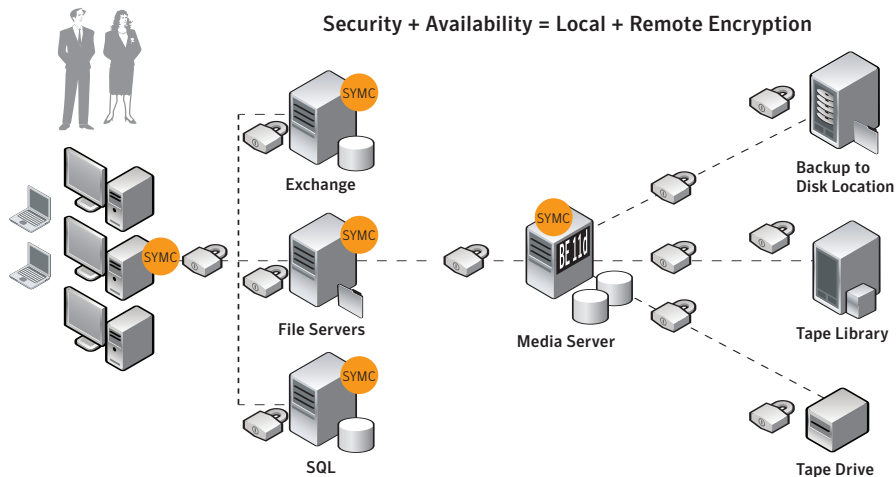


Figure 3. Data flow of Backup Exec 11d encryption

### Managing encryption keys

Organizations often have a difficult time identifying and tracking which data should be encrypted. Should the whole backup database be encrypted or only part of it? Should all the data on the network be encrypted? Should all backups be encrypted or only a portion of them?

Backup Exec 11d provides flexible methods for configuring backups to include encryption on a per-backup-job basis, per-policy basis, or as a global default setting for all backups. This allows you to encrypt data based on established policies in your company. To assist with this process, Backup Exec 11d includes an integrated Encryption Key Management feature that is accessible from the Backup Exec 11d Tools/Encryption Keys menu or from within any backup job or policy (see Figure 4).

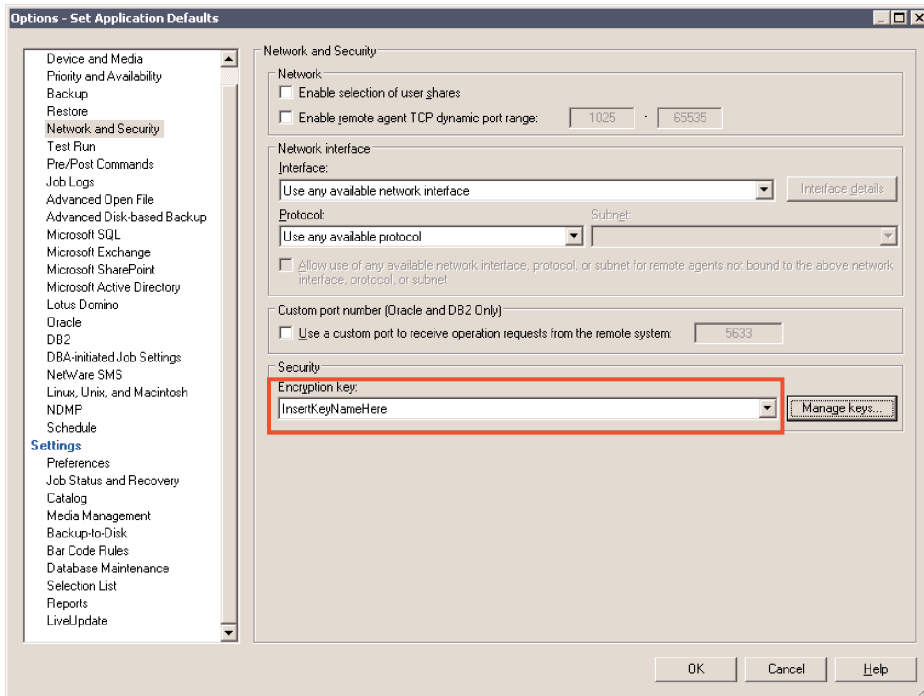


Figure 4. Accessing Encryption Key Management

The Encryption Key Management screen allows you to view, manage, create, and delete encryption keys available for use by Backup Exec 11d. These keys are managed in a manner similar to the Backup Exec logon accounts that are used for providing authentication to network resources to back them up. Keys can also be set as default keys to be used for a job, a policy, or all jobs (see Figure 5).

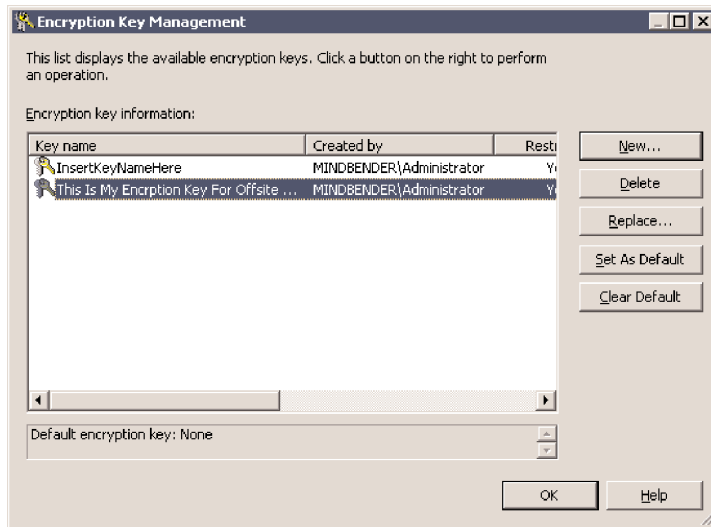


Figure 5. Encryption Key Management

A key that is created on a media server is specific to that media server. You cannot move keys between media servers. However, you can create new keys on a different media server by using existing pass phrases. A pass phrase always generates the same key. In addition, if you delete a key accidentally, you can re-create it by using the pass phrase.

If a Backup Exec database becomes corrupted on a media server and is replaced by a new database, you must manually re-create all of the encryption keys that were stored on the original database. If you move a database from one media server to another, the encryption keys remain intact as long as the new media server has the same user accounts and is in the same domain as the original media server.

### Deleting encryption keys

Be cautious when you delete encryption keys. When you delete an encryption key, you cannot restore the backup sets that you encrypted with that key unless you create a new key that uses the same encryption key and pass phrase as the original key. You can delete encryption keys if:

- The encrypted data on the tape has expired or if the tape is retired.
- The encryption key is not the default key.

- The encryption key is not being used in a job or a template. If the key is being used, you must select a new key for the job or template.
- The encryption key is not being used in a selection list for restore jobs and for verify duplicate backup set jobs. If you delete a key that is being used in one of the listed job types, the selection list can no longer be used.

If you delete an encryption key that is being used in a scheduled restore job, you cannot replace the key. Therefore, any scheduled restore job in which you delete an encryption key fails.

### Tracking changes to encryption keys

Backup Exec 11d includes comprehensive audit logging capabilities to track most configuration changes made to Backup Exec settings, including changes made to encryption keys. The Audit Log is easily accessible via the Backup Exec 11d console's Tools/Audit Log menu (see Figure 6).

The Backup Exec Audit Log tracks:

- Creation of new encryption keys
- Deletion of encryption keys
- Modification of encryption keys
- User name of user who made change
- Date/time of change
- Description of change

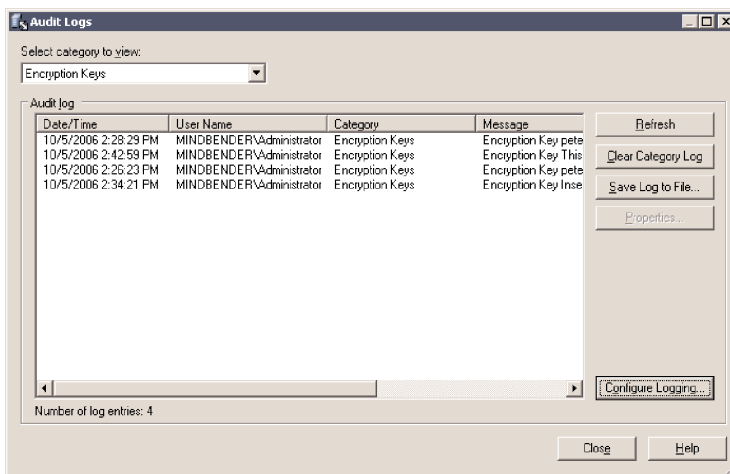


Figure 6. Audit Logs

The Backup Exec 11d Audit Log can be saved and exported to help ensure compliance with government and corporate requirements. This Audit Log can also be used to provide key documentation in audit situations. In addition, the contents of the Audit Log can be included in the Backup Exec 11d Audit Log Report. This report can be scheduled to run just like any other job within Backup Exec and can be automatically distributed to key compliance-focused personnel via email. See the *Backup Exec 11d Administrator's Guide*, Chapter 14, "Reports in Backup Exec," for more information on running and configuring Backup Exec reports.

### Restore process with encryption

Restores of encrypted data with Backup Exec 11d are just as easy as the backup, provided that you have the necessary pass phrase for the encryption key needed for the restore. Encrypted backup sets are identified in the restore selection list by an icon with a lock on it. The restore process of encrypted data follows this sequence:

1. When you select encrypted data for restore, Backup Exec verifies that encryption keys for the data are available in the database. If you use encryption keys with the Intelligent Disaster Recovery Option, the wizard prompts you for the pass phrase of each encrypted backup set that is required to complete the recovery.
2. If any of the keys are not available, Backup Exec prompts you to re-create the missing keys. Anyone can generate keys or restore any tape provided they have the pass phrase used for the original encryption key.
3. Once the key has been re-created or the pass phrase provided, the encrypted data is read from media and transferred across the network to the client before decryption.

### Encryption best practices

- Protect your pass phrases: Be sure to keep track of your pass phrases when you create encryption keys. This is the single most important step to remember when using Backup Exec 11d encryption. Pass phrases can be written down and stored in secure locations such as safes or safe deposit boxes, or they can be stored electronically in other secure locations.
- Backup Exec supports two types of encryption: 128-bit and 256-bit AES. The 256-bit AES encryption provides stronger security because the key is longer for 256-bit AES than it is for 128-bit AES. However, 128-bit AES encryption enables backup jobs to process more quickly.

- If you use encryption in a synthetic backup policy, all the templates in the policy must use the same encryption key. You should not change the key after you create the policy.
- The minimum number of characters for 128-bit AES encryption is 8. The minimum number of characters for 256-bit AES encryption is 16. Symantec recommends that you use more than the minimum number of characters.
- Symantec recommends that you avoid using hardware compression with encryption. Hardware compression is performed after encryption. Data becomes randomized during the encryption process, and compression does not work properly on data that is randomized.
- You can use software compression with encryption for a backup job. First, Backup Exec compresses the files and then encrypts them. However, backup jobs take longer to be completed when you use both encryption and software compression.
- To catalog a tape on a different media server, you need to know the key and the encryption method (128/256 bit).
- Do not delete keys without first considering which backup jobs are currently scheduled and configured to use those keys.
- When you create a duplicate backup set template or a duplicate backup set job, backup sets that are already encrypted are not reencrypted. However, you can encrypt any unencrypted backup sets.
- If you use encryption in a synthetic backup policy, all the templates in the policy must use the same encryption key. You should not change the key after you create the policy.
- For the synthetic backup template, Backup Exec automatically uses the encryption key that you select for the other templates in the policy. When you select encrypted data for restore, Backup Exec verifies that encryption keys for the data are available in the database. If any of the keys are not available, Backup Exec prompts you to re-create the missing keys. If you delete the key after you schedule the job to run, the job fails.
- If Backup Exec cannot locate an encryption key while a catalog job is processing, Backup Exec sends an alert. You can then re-create the missing encryption key if you know the pass phrase. If you use encryption keys with the Intelligent Disaster Recovery Option, special considerations apply.

## System requirements

To use the new encryption capabilities of Backup Exec 11d for Windows Servers, the Backup Exec server must have the following items installed:

- Windows 2000, Windows XP, or Windows Server 2003
- Backup Exec for Windows Servers 11d or later

In addition, Backup Exec 11d or later Remote Agents must be used.

Platform Agents Supported*	Application Agents Supported	Database Agents Supported
<ul style="list-style-type: none"><li>• Backup Exec Remote Agent for Windows Servers (RAWS)</li><li>• Backup Exec Agent for Linux and UNIX Servers (RALUS)</li><li>• Backup Exec Agent for Macintosh Systems (RAMS)</li><li>• Backup Exec Desktop and Laptop Option (DLO)</li></ul>	<ul style="list-style-type: none"><li>• Agent for Microsoft Exchange Server**</li><li>• Agent for Microsoft SharePoint**</li><li>• Agent for Lotus Domino®</li><li>• Agent for Microsoft DPM</li><li>• Agent for Microsoft Active Directory*</li></ul>	<ul style="list-style-type: none"><li>• Agent for Microsoft SQL Server</li><li>• Agent for Oracle® Servers</li><li>• Agent for IBM® DB2® Servers on Windows</li><li>• Agent for SAP Applications</li></ul>

Backups enabled for encryption and sent to a disk target with new GRT for individual object-level recovery for Microsoft Exchange, SharePoint, and Active Directory are encrypted at the source during the network transit, but they are stored in an unencrypted format on the final backup disk target location. Tape-based GRT-enabled backups do not have this limitation and are stored on tape in an encrypted format.

## Other encryption architectures

Encryption for backup purposes can be done in both hardware and software. Each has its own advantages and disadvantages.

Backup Exec 11d provides powerful software-based encryption at no additional charge. However, some companies may want to take advantage of the features that a dedicated hardware-based encryption solution provides. Companies need to evaluate their environment and decide which method works best for them. The following table provides some guidance on the various advantages and disadvantages of software-based and hardware-based encryption. As the world's leading storage and security-focused company, Symantec is not recommending one type of encryption over the other. We simply believe in providing the highest level of security possible that best meets an organization's needs, regardless of whether or not it is hardware or software based.

\* The following Backup Exec Agents do not support encryption: Backup Exec Continuous Protection Agent (CPA) and Backup Exec Remote Agent for NetWare® (RANW).  
\*\* The following Backup Exec Agents do not support encrypted disk-based backups when enabled with GRT: Backup Exec Agent for Microsoft Exchange Server, Backup Exec Agent for Microsoft SharePoint, and Backup Exec Agent for Microsoft Active Directory.

### Software-based versus hardware-based encryption

Considerations	Backup Exec 11d	Dedicated Hardware Encryption Solutions
<b>Cost</b>	Included with Backup Exec 11d at no additional charge	Varies, but always more costly
<b>Key Management</b>	Included and integrated with Backup Exec 11d	Varies, vendor supplied
<b>Configurability</b>	Can be enabled on/off on a per-job, per-policy, or global default basis from disk to disk to tape (D2D2T), tape to tape (T2T), and disk to tape (D2T)	Varies, but usually complete data path from source to network to final destination
<b>Performance Impacts on Backup</b>	Depends on type of encryption (128-bit versus 256-bit) and server hardware capabilities and performance	Varies, but usually minimal compared with software-based encryption
<b>Ease of Data Recovery</b>	Encryption is pass phrase based, allowing the encryption key to be re-created at any Backup Exec 11d server for recovery	Varies, but usually not portable; requires hardware replacement or cluster solution if encryption device is lost
<b>Encryption Type</b>	128-/256-bit AES encryption with OpenSSL ciphers	Similar
<b>Management</b>	No additional servers or hardware to manage for encryption capabilities	Additional hardware to manage, power, and cool within an environment

Hardware-based encryption devices provide performance advantages that only a dedicated hardware-based solution can provide (see Figure 7). In this topology, the security appliance for hardware-based encryption serves as the device responsible for managing and controlling all encryption activities, including data that is protected through Backup Exec. When a job is scheduled to run, Backup Exec is unaware that a hardware-based encryption solution is present on the network. The hardware-based encryption device is responsible for all encryption and decryption duties including key management. It is required to be present and available in order for the data to be accessible.

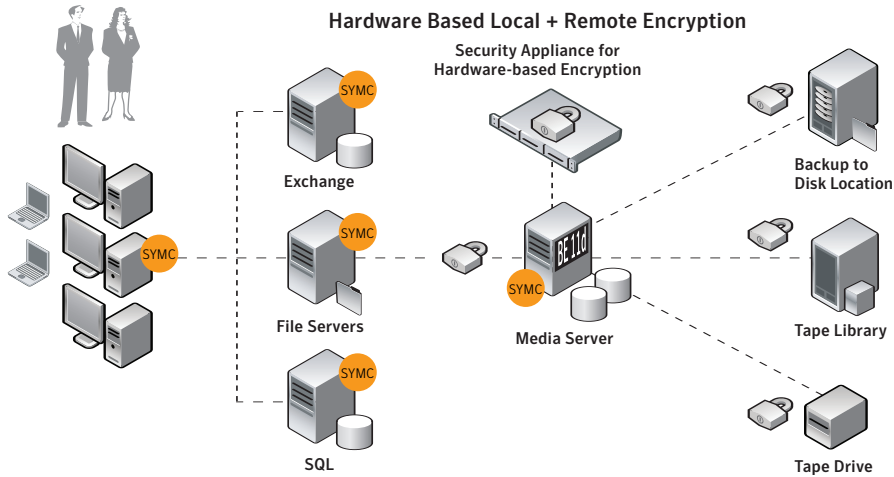


Figure 7. Hardware-based encryption

## Summary

With the new encryption capabilities offered by Backup Exec 11d for Windows Servers, your company's critical and sensitive data can be easily protected in a secure format from unauthorized access. By combining the industrial-strength encryption capabilities of 128-/256-bit AES OpenSSL encryption with Backup Exec software's ease of use and flexible implementation to encrypt what, when, and where you want, businesses that rely on Backup Exec can be confident that their critical data is secure wherever it may reside.

## About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information.

Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries.

More information is available at [www.symantec.com](http://www.symantec.com).

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation  
World Headquarters  
20330 Stevens Creek Boulevard  
Cupertino, CA 95014 USA  
+1 (408) 517 8000  
1 (800) 721 3934  
[www.symantec.com](http://www.symantec.com)

Copyright © 2006 Symantec Corporation. All rights reserved. Symantec, the Symantec logo, and Backup Exec are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Macintosh is a trademark of Apple Computer, Inc., registered in the United States and other countries. Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and other countries. Other names may be trademarks of their respective owners. Printed in the USA. 10/06 11305664