VERITAS The truth in information.

# Veritas Backup Exec

## Security and Encryption

## VERITAS BACKUP EXEC

Veritas Backup Exec™ is the backup solution without barriers, delivered your way. You choose what to back up, where to store it and how to pay for it. Your data remains secure and available at every stage—whether backing up on-premises to the cloud, protecting workloads within the cloud, recovering from the cloud or connecting to on-prem storage. With Backup Exec you can connect with an ever-expanding family of solutions to help you to run your business confidently.

Backup Exec is available for purchase in either perpetual or term subscription licensing, with the level of functionality you require—Bronze, Silver or Gold. Bronze edition offers the most economic option. Silver edition offers the most-used features. Gold edition includes all features and functionality available in Backup Exec. Your purchase is based on the amount of front-end data you need to back up. Your chosen license-set is available in whatever quantities you require.

Backup Exec gives you comprehensive protection against external threats. So if the unthinkable happens, your critical data is backed up and ready to be recovered, quickly and easily.

## 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, ransomware, 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.

## KEY BENEFITS

- Helps reduces security risks to your data through integrated 128/256-bit AES industrial-strength encryption
- Data transfer over Secure Sockets Layer (SSL) connection between Backup Exec and cloud targets
- Integrated encryption key management system for easy setup and management
- Secure Console Management enhances the security of the Backup Exec console.
- Support for Payment Card Industry Data Security Standard (PCI DSS) 3.1/3.2 standard
- FIPS 140-2 compliant software encryption
- Supports TLS 1.2
- 256-bit AES symmetric encryption algorithm used in protecting the sensitive contents of the Backup Exec database
- Supports hardware encryption for any storage devices that use the T10 encryption standard
- Complete data security with data encrypted in transit and at rest
- Included with Backup Exec at no additional charge

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

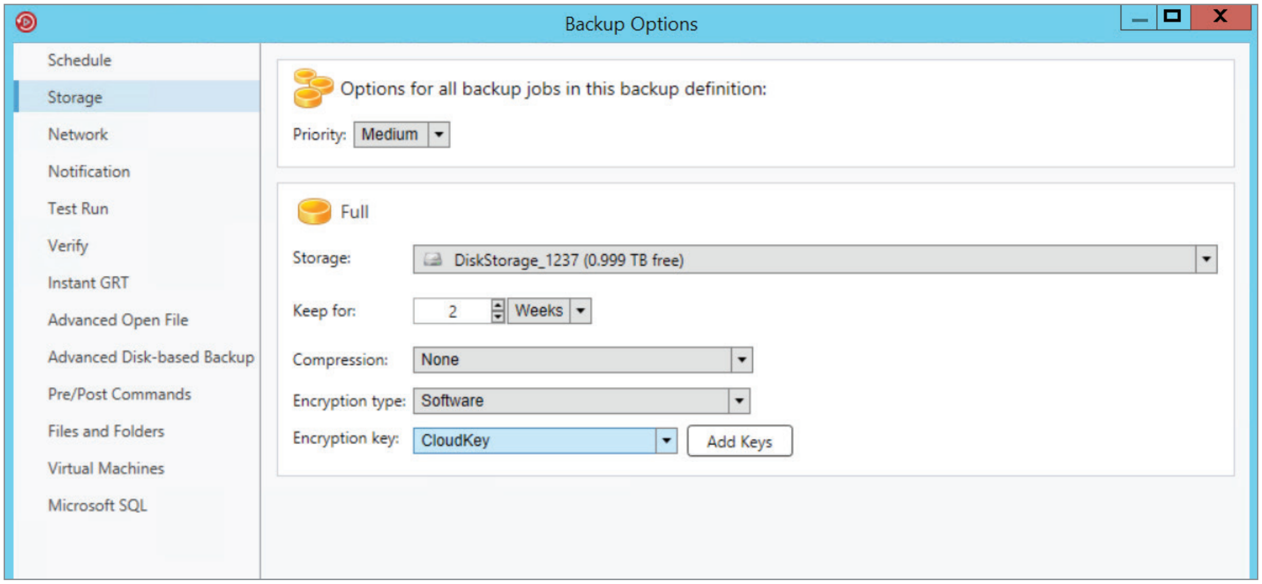
- Unencrypted removable media taken offsite for “security” is less secure than almost any other corporate data.
- Theft of a tape and removable media is a major risk that is difficult to track due to the size of the media.
- Data may become available to third parties if a tape is lost or left unprotected.
- 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 advice 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.

## USING ENCRYPTION WITH BACKUP EXEC

Backup Exec provides you with the ability to encrypt data. When you encrypt data, you protect it from unauthorized access. Anyone that tries to access the data has to have an encryption key that you create. Backup Exec provides software encryption, but it also supports some devices that provide hardware encryption with the T10 standard. Backup Exec configures encryption when you specify which storage devices that you want to use for a backup job.

Backup Exec supports two security levels of encryption: 128-bit Advanced Encryption Standard (AES) and 256-bit AES. The 256-bit AES encryption provides a stronger level of security because the key is longer for 256-bit AES than for 128-bit AES.



Backup Options

Options for all backup jobs in this backup definition:

Priority: Medium

Full

Storage: DiskStorage_1237 (0.999 TB free)

Keep for: 2 Weeks

Compression: None

Encryption type: Software

Encryption key: CloudKey

*Figure 1: Encryption Key Options under Backup Options*

However, 128-bit AES encryption enables backup jobs to process more quickly. Hardware encryption using the T10 standard requires 256-bit AES. When you run a duplicate backup job, any backup sets that are already encrypted are not re-encrypted. However, you can encrypt any unencrypted backup sets.

To learn more about the Advanced Encryption Standard (AES) that Backup Exec uses for software encryption, review the following document: http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

## SOFTWARE ENCRYPTION

When you install Backup Exec, the installation program installs encryption software on the Backup Exec server and on any remote computers that use a Backup Exec agent. Backup Exec can encrypt data at a computer that uses a Backup Exec agent, and then transfer the encrypted data to the Backup Exec server. Backup Exec then writes the encrypted data on a set-by-set basis to public cloud storage targets (AWS, Azure, Google, and others), tape or to disk storage.

Backup Exec encrypts the following types of data:

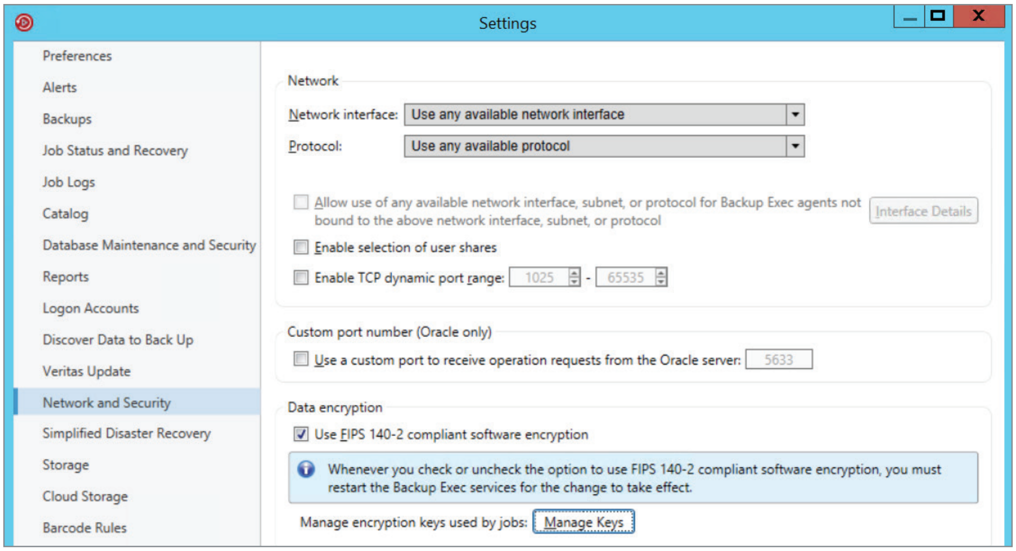
- User data, such as files and Microsoft Exchange databases.
- Metadata, such as file names, attributes, and operating system information.
- On-tape catalog file and directory information.

Backup Exec does not encrypt Backup Exec metadata or on-disk catalog file and directory information. 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 complete when you use both encryption compression and software compression.

Veritas recommends that you avoid using hardware compression with software encryption. Hardware compression is performed after encryption. Data becomes randomized during the encryption process. Compression does not work effectively on data that is randomized.

### Federal Information Processing Standard (FIPS) 140-2 compliant software encryption

Backup Exec lets you enable software encryption that complies with FIPS 140-2 standards. If you select this option, you must use a 256-bit AES encryption key. This option is available only for Windows computers.



Network

Network interface: Use any available network interface

Protocol: Use any available protocol

□ Allow use of any available network interface, subnet, or protocol for Backup Exec agents not bound to the above network interface, subnet, or protocol

□ Enable selection of user shares

□ Enable TCP dynamic port range: 1025 - 65535

Custom port number (Oracle only)

□ Use a custom port to receive operation requests from the Oracle server: 5633

Data encryption

☑ Use FIPS 140-2 compliant software encryption

Whenever you check or uncheck the option to use FIPS 140-2 compliant software encryption, you must restart the Backup Exec services for the change to take effect.

Manage encryption keys used by jobs: Manage Keys

*Figure 2: FIPS 140-2 compliant software encryption option under Network and Security*

Some agencies of the government (both US and foreign) as well as contractors who work with the government (e.g. defence contractors) often need the FIPS 140-2 assurance that the cryptography has been implemented correctly and that it has not been tampered with.

Refer to the following article for more information on FIPS: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

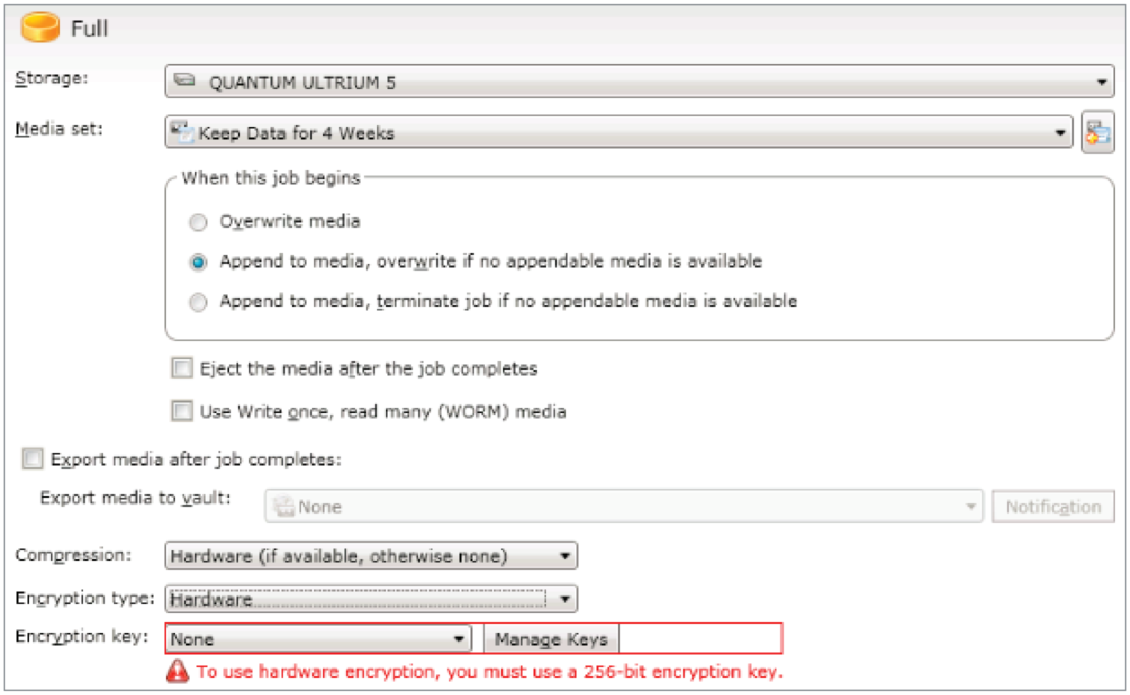
You can view the OpenSSL/FIPS version in the About Veritas Backup Exec dialog box, as displayed in figure 3.

## HARDWARE ENCRYPTION

Backup Exec supports hardware encryption for any storage devices that use the T10 encryption standard. When you use hardware encryption, the data is transmitted from the host computer to the storage device and then encrypted on the device. Backup Exec manages the encryption keys that are used to access the encrypted data.

Backup Exec only supports approved devices for T10 encryption.

You can find a list of compatible devices at the following URL: https://www.veritas.com/support/en_US/article.000017788



Full

Storage: QUANTUM ULTRIUM 5

Media set: Keep Data for 4 Weeks

When this job begins

○ Overwrite media

● Append to media, overwrite if no appendable media is available

○ Append to media, terminate job if no appendable media is available

□ Eject the media after the job completes

□ Use Write once, read many (WORM) media

□ Export media after job completes:

Export media to vault: None

Compression: Hardware (if available, otherwise none)

Encryption type: Hardware

Encryption key: None

To use hardware encryption, you must use a 256-bit encryption key.

*Figure 3: Hardware Encryption*

Note: Hardware encryption that uses the T10 standard requires 256-bit AES. Backup Exec does not let you enable hardware encryption for a job unless it uses at least a 16-character pass phrase.

## ENCRYPTION KEYS

You must create encryption keys to use encryption in Backup Exec. When a user creates an encryption key, Backup Exec marks that key with an identifier based on the logged-on user's security identifier. The person who creates the key becomes the owner of the key.

If you use encryption for synthetic backups, all of the associated backups must use the same encryption key. Do not change the encryption key after the baseline is created. The encryption key that you select for the baseline backup is automatically applied to all associated backups.

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 recreate 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 running, Backup Exec sends an alert. You can then recreate the missing encryption key if you know the pass phrase. Simplified Disaster Recovery supports the recovery of computers with previously encrypted backup sets. If you have Simplified Disaster Recovery backups that are encrypted during backup, the Recover This Computer wizard prompts you for the pass phrase of each encrypted backup set that is required to complete the recovery.

## RESTRICTED KEYS AND COMMON KEYS

Backup Exec has the following types of encryption keys:

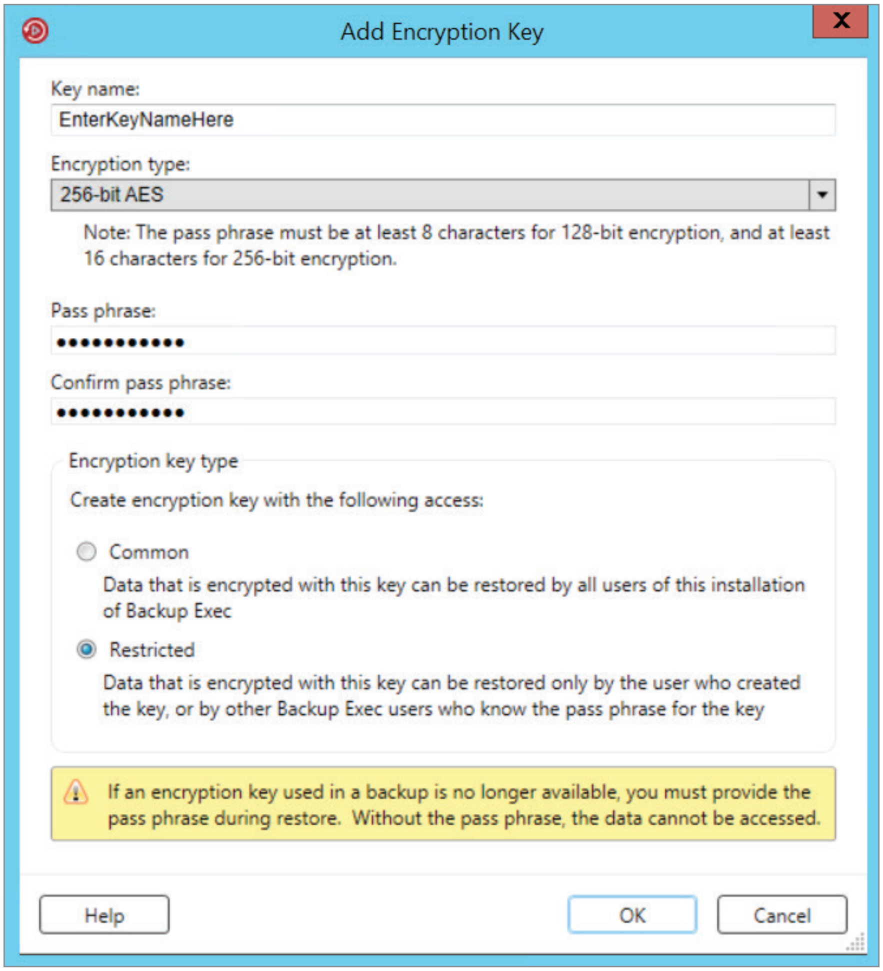
| Encryption Key Type | Description |
|---|---|
| Common | Anyone can use the key to encrypt data during a backup job and to restore encrypted data. |
| Restricted | Anyone can use the key to encrypt data during a backup job, but users other than the key owner must know the pass phrase. If a user other than the key owner tries to restore the encrypted data, Backup Exec prompts the user for the pass phrase. If you cannot supply the correct pass phrase for the key, you cannot restore the data. |

## PASS PHRASES

Encryption keys require a pass phrase, which is similar to a password. Pass phrases are usually longer than passwords and are comprised of several words or groups of text. A good pass phrase is between 8 and 128 characters. The minimum number of characters for 128-bit AES encryption is eight. The minimum number of characters for 256-bit AES encryption is 16. Veritas recommends that you use more than the minimum number of characters.

Note: Hardware encryption that uses the T10 standard requires 256-bit AES. Backup Exec does not let you enable hardware encryption for a job unless it uses at least a 16-character pass phrase.

Also, a good pass phrase contains a combination of upper and lower case letters, numbers, and special characters. You should avoid using literary quotations in pass phrases.



Add Encryption Key

Key name:
EnterKeyNameHere

Encryption type:
256-bit AES

Note: The pass phrase must be at least 8 characters for 128-bit encryption, and at least 16 characters for 256-bit encryption.

Pass phrase:
●●●●●●●●●●●●

Confirm pass phrase:
●●●●●●●●●●●●

Encryption key type

Create encryption key with the following access:

○ Common
Data that is encrypted with this key can be restored by all users of this installation of Backup Exec

● Restricted
Data that is encrypted with this key can be restored only by the user who created the key, or by other Backup Exec users who know the pass phrase for the key

If an encryption key used in a backup is no longer available, you must provide the pass phrase during restore. Without the pass phrase, the data cannot be accessed.

*Figure 4: Adding Encryption Key*

A pass phrase can include only printable ASCII characters, which are characters 32 through 126. ASCII character 32 is the space character, which is entered using the space bar on the keyboard. ASCII characters 33 through 126 include the following:

!″#$%&′()*+,-./0123456789:;<=>?@
ABCDEFGHIJKLMNOPQRSTUVWXYZ

[\]^_‘abcdefghijklmnopqrstuvwxyz{|}

## ENCRYPTION KEY MANAGEMENT

When a user creates an encryption key, Backup Exec marks that key with an identifier based on the logged-on user's security identifier. The person who creates the key becomes the owner of the key.

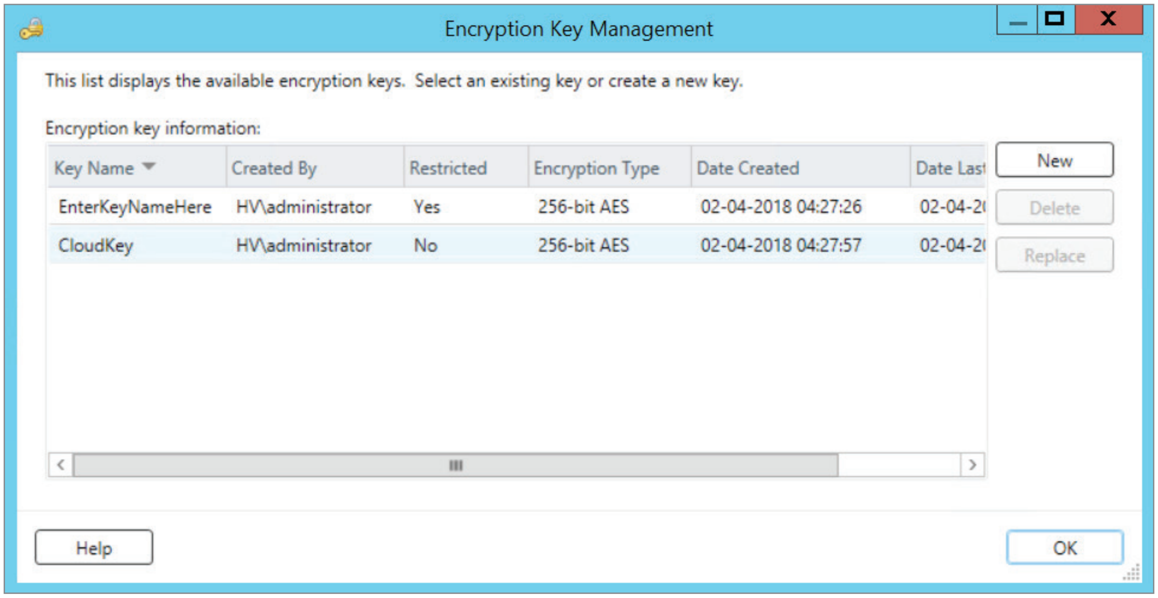
Backup Exec stores the keys in the Backup Exec database. However, Backup Exec does not store the pass phrases for the keys. The owner of each key is responsible for remembering the pass phrase for the key.

To protect your keys, Veritas recommends the following:

- Maintain a written log of the pass phrases. Keep the log in a safe place in a separate physical location from the encrypted backup sets.
- Back up the Backup Exec database. The database keeps a record of the keys.

Caution: If you do not have a backup of the Backup Exec database and do not remember your pass phrases, you cannot restore data from the encrypted media. In addition, Veritas cannot restore encrypted data in this situation.

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



This list displays the available encryption keys. Select an existing key or create a new key.

Encryption key information:

| Key Name | Created By | Restricted | Encryption Type | Date Created | Date Last |
|---|---|---|---|---|---|
| EnterKeyNameHere | HV\administrator | Yes | 256-bit AES | 02-04-2018 04:27:26 | 02-04-2 |
| CloudKey | HV\administrator | No | 256-bit AES | 02-04-2018 04:27:57 | 02-04-2 |

*Figure 5: Encryption Key Management*

If a Backup Exec database becomes corrupted on a Backup Exec server and is replaced by a new database, you must manually recreate all of the encryption keys that were stored on the original database.

If you move a database from one Backup Exec server to another Backup Exec server, the encryption keys remain intact as long as the new Backup Exec server meets the following criteria:

- Has the same user accounts as the original Backup Exec server.
- Is in the same domain as the original Backup Exec server.

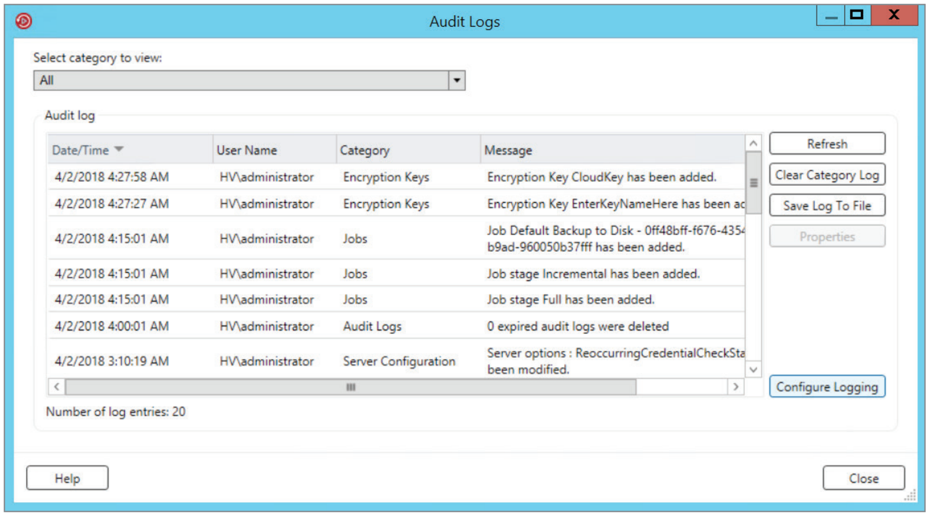
## TRACKING CHANGES TO ENCRYPTION KEYS

Backup Exec 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 console's Tools/Audit Log menu (see Figure 5).

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

The audit log displays the date and time of the activity, who performed it, what the activity was, and a description of the activity.



Select category to view: All

Audit log

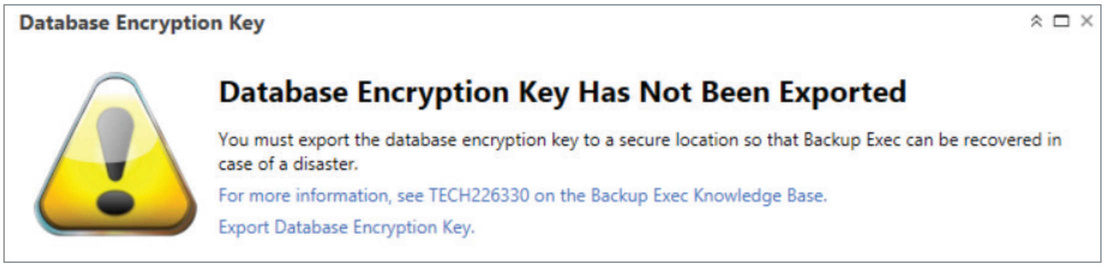
| Date/Time | User Name | Category | Message |
|---|---|---|---|
| 4/2/2018 4:27:58 AM | HV\administrator | Encryption Keys | Encryption Key CloudKey has been added. |
| 4/2/2018 4:27:27 AM | HV\administrator | Encryption Keys | Encryption Key EnterKeyNameHere has been ac |
| 4/2/2018 4:15:01 AM | HV\administrator | Jobs | Job Default Backup to Disk - 0ff48bff-f676-4354 b9ad-960050b37fff has been added. |
| 4/2/2018 4:15:01 AM | HV\administrator | Jobs | Job stage Incremental has been added. |
| 4/2/2018 4:15:01 AM | HV\administrator | Jobs | Job stage Full has been added. |
| 4/2/2018 4:00:01 AM | HV\administrator | Audit Logs | 0 expired audit logs were deleted |
| 4/2/2018 3:10:19 AM | HV\administrator | Server Configuration | Server options : ReoccurringCredentialCheckSta been modified. |

Number of log entries: 20

*Figure 6: Audit Logs*

## BACKUP EXEC DATABASE ENCRYPTION KEY.

Backup Exec stores sensitive information in the Backup Exec Database using encryption. When you install or upgrade Backup Exec, it automatically creates a database encryption key. The database encryption key is used to encrypt information such as login account credentials and the keys that are used for encrypted backup jobs, for example. It is stored in the Data folder in the Backup Exec installation directory.



Database Encryption Key

**Database Encryption Key Has Not Been Exported**

You must export the database encryption key to a secure location so that Backup Exec can be recovered in case of a disaster.

For more information, see TECH226330 on the Backup Exec Knowledge Base.

Export Database Encryption Key.

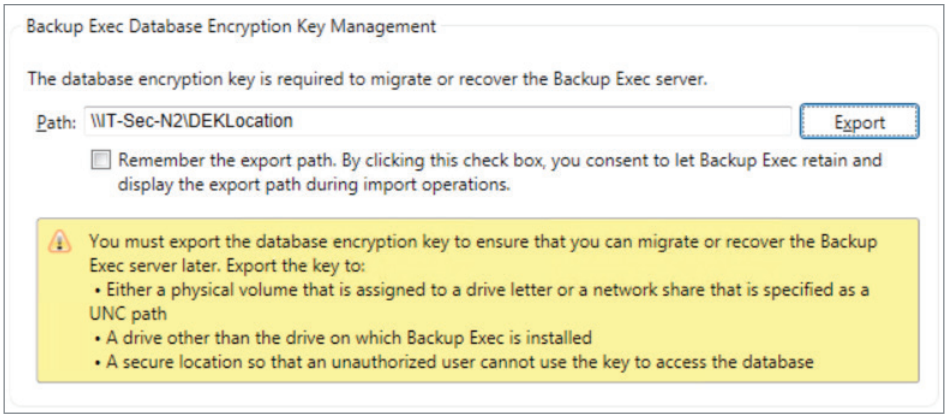
*Figure 7: Database Encryption Key on the Home screen*

You are required to provide the Backup Exec Database encryption key for each of the following scenarios:

- Performing a manual disaster recovery of a Backup Exec server
- Performing a disaster recovery of a Backup Exec server using Simplified Disaster Recovery (SDR)
- Migrating Backup Exec from one computer to another computer
- Resolving any situations in which the database encryption key on the Backup Exec server is corrupted or goes missing

Veritas recommends that you export the Backup Exec Database encryption key to a secure location so that you can access it later if it is needed. Make sure that you export the database encryption key to a location that meets the following criteria:

- The destination is either on a physical volume that is assigned to a drive letter or a network share that is specified by a UNC path (network shares that are mapped to drive letters are not supported)
- The destination has enough disk space
- The destination is accessible from the Backup Exec server
- Backup Exec has permission to write to the destination



Backup Exec Database Encryption Key Management

The database encryption key is required to migrate or recover the Backup Exec server.

Path: \\IT-Sec-N2\DEKLocation

□ Remember the export path. By clicking this check box, you consent to let Backup Exec retain and display the export path during import operations.

You must export the database encryption key to ensure that you can migrate or recover the Backup Exec server later. Export the key to:
- Either a physical volume that is assigned to a drive letter or a network share that is specified as a UNC path
- A drive other than the drive on which Backup Exec is installed
- A secure location so that an unauthorized user cannot use the key to access the database

*Figure 8: Backup Exec Database Encryption Key management*

## SECURE SQL CONNECTIONS TO THE BACKUP EXEC DATABASE

The Backup Exec Database contains sensitive information about your organization, including user account credentials and backed up data. Securing Microsoft SQL Server's connection to the Backup Exec Database is an important step in protecting your network from outside access. Microsoft recommends that you use SSL encryption any time data that is transmitted between SQL Server and an application travels across a network.

Data transmission between the Backup Exec services and the SQL instance can travel across the network in the following scenarios:

- You configure the Backup Exec Database as a centralized database and it is located on a central administration server in a CASO environment. Data can also travel across the network in variations of this scenario, for example when you use a managed Backup Exec server or when you use shared storage.
- You use a remote SQL instance for the Backup Exec Database so that the Backup Exec services must access the database across the network.

Backup Exec automatically enables SSL encryption if you use the default, local SQL Express instance called "BKUPEXEC". If you configure Backup Exec to use any other SQL Server instance, you must configure encryption yourself.

SQL Server uses certificates to encrypt data. You can generate your own certificates or you can let SQL Server use an automatically generated, self-signed certificate. By default, Backup Exec uses the self-signed certificates that SQL Server automatically generates. However, Veritas recommends that you create and use your own certificates for additional security.

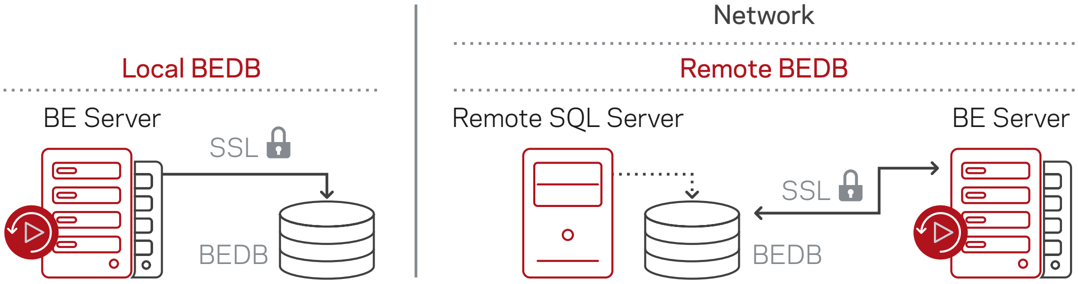


*Figure 9: Secure SQL Connections*

**Note:** Using encryption may affect the performance of communications between SQL Server and the Backup Exec Database. It involves an extra round trip across the network as well as time to encrypt and decrypt the data.

Refer to the Microsoft knowledge base for more information about Secure Sockets Layer (SSL) and encrypting connections to SQL Server.

Microsoft has requirements that must be followed when you use your own certificates for SQL Server. Certificates can be either self-signed or issued from a certification authority. Certification authorities can be either a local authority in your organization's domain or a known third-party authority.

For more information about Microsoft's certification requirements, refer to the following Microsoft article: Encrypting Connections to SQL Server

Before you configure encryption, you must import the certificates that you want to use into the local certificate store of the computer that hosts the Backup Exec Database.

For more information about importing and installing a certificate on the server, refer to the following Microsoft article: How to: Enable Encrypted Connections to the Database Engine (SQL Server Configuration Manager)

When you import certificates, you should use the same user account under which the SQL Server service runs

## NETWORK SECURITY LAYER (NSL) UTILIZING SSL

Backup Exec provides SSL support from the agent to the Backup Exec server, providing an extra layer of security for companies that transmit backup data across the WAN, public cloud, or to a private cloud. The added security features help you ensure that backed up data sent over a public Internet connection is secure.

Certificates are now used in conjunction with SSL to ensure any communication between Remote Agents and Backup Exec Media Servers is secure over WANs, LANs, or other Internet-based connections.

Backup Exec establishes trust between the Backup Exec remote agent and Backup Exec server before exchanging any sensitive information to avoid any Man-in-The-Middle (MiTM) issues. This minimizes risk of transporting data across networks from agent to Backup Exec server.

MiTM exploitation may result in privilege escalation enabling an attacker to execute post authentication NDMP commands. Successful exploitation requires the attacker to be an authorized user on the network or have unauthorized presence on an authorized system on the network.

Backup Exec uses the Transport Layer Security (TLS) 1.2 protocol for its SSL control connection over NDMP between the Backup Exec server and the agent on a protected server (supported for Backup Exec Servers, Agent for Windows, and Agent for Linux).

For increased security, customers use strong ciphers for SSL enabled control connection over NDMP between the Backup Exec Server and Agents. The TLS connection works well with security scanners, which provides customers continued confidence in using Backup Exec. TLS 1.2 supports AES-GCM cipher suites that are not prone to the weaknesses of cipher block chaining, or CBC and RC4.

Also, Backup Exec used SHA-2 certificates for the Backup Exec Server and Agents SSL communications. SHA-2 SSL certificates are supported with the Backup Exec Server, Central Admin Server, Managed Backup Exec Server, Agent for Windows, and the Agent for Linux. SHA-2 Certificates offers immediate benefits with higher levels of security.

As opposed to using intermediate certificates signed by a real CA (such as Verisign which will cost money), each Backup Exe Server can be made its own Certificate Authority (CA). It has the ability to sign certificates which are then deployed to Remote Agents. Once the trust between the Backup Exec Server and remote agents is established using these certificates, it can prevent a Man-In-The-Middle (MITM) attack on the NDMP connections that Backup Exec server and Remote Agents use to talk to each other.

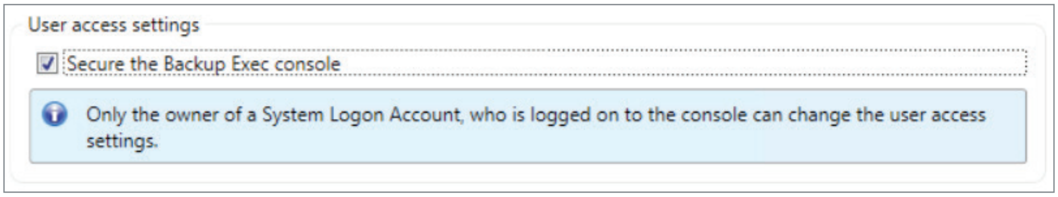
## USING ENCRYPTION WITH COMPRESSION

If you use software compression and software encryption for a backup job, Backup Exec first compresses the files and then encrypts them. This results in a slower backup.

If you use hardware compression and software encryption for a backup job, the data is encrypted before being compressed. Because encryption randomizes data, it cannot be properly compressed. Veritas recommends that you avoid using hardware compression with encryption.

## SECURE CONSOLE MANAGEMENT IN BACKUP EXEC

Secure Console Management enhances the security of the Backup Exec User Interface console.



User access settings

☑ Secure the Backup Exec console

Only the owner of a System Logon Account, who is logged on to the console can change the user access settings.

*Figure 10: Secure Console Management in Backup Exec*

As a part of Secure Console Management, Backup Exec provides:

### Identity Authentication

Enabling the Secure Console Management checkbox will enable Identity Authentication. Because of this, Backup Exec will no longer automatically attempt to login using the Windows logged-in user account when the BE User Interface is launched, but instead, Authentication credentials will be required to be entered each time, the user wants to login into the Backup Exec console.

### Session Locking

Enabling the Secure Console Management checkbox will enable Session Locking capability. Because of this, BE User Interface session will be locked and will need to re-authenticate to unlock BE UI.

## USING BACKUP EXEC WITH FIREWALLS

In firewall environments, Backup Exec provides the following advantages:

- The number of ports that are used for backup network connections is kept to a minimum.
- Open ports on the Backup Exec server and remote systems are dynamic and offer high levels of flexibility during browsing, backup, and restore operations.
- You can set specific firewall port ranges and specify backup and restore networks within these ranges. You can use specific ranges to isolate data traffic and provide high levels of reliability.

With 20.1 release, Backup Exec has enhanced the existing inbound firewall rules to provide access for only the required ports and restrict access to all other ports. This helps to minimize probability of a security lapse or violation.

## BEST PRACTICES

As a part of normal best practices, Veritas strongly recommends:

- Restrict access to administration or management systems to privileged users.
- Restrict remote access, if required, to trusted/authorized systems only.
- Run under the principle of least privilege where possible to limit the impact of exploit by threats.
- Keep all operating systems and applications updated with the latest vendor patches.
- Follow a multi-layered approach to security. Run both firewall and anti-malware applications, at a minimum, to provide multiple points of detection and protection to both inbound and outbound threats.
- Deploy network and host-based intrusion detection systems to monitor network traffic for signs of anomalous or suspicious activity. This may aid in detection of attacks or malicious activity related to exploitation of latent vulnerabilities

- Create strong pass phrases by doing the following:
  - Use more than the minimum number of characters that are required.
  - Use a combination of upper- and lower-case letters, numbers, and special characters.
  - Avoid literary quotations in pass phrases.
  - Keep your pass phrases secure.
- Run Backup Exec Services in FIPS mode and use 256-bit AES encryption to be FIPS compliant.
- If you do not use software encryption when you back up data to disk-based storage, use File System encryption to prevent unauthorized access.

## REPORTING VULNERABILITIES TO VERITAS

Veritas takes the security and proper functionality of our products very seriously. Veritas Technologies firmly believes in a proactive approach to secure software development and implements security review into various stages of the software development process. Additionally, Veritas is committed to the security of its products and services as well as to its customers' data. Veritas is committed to continually improving its software security process.

This document provides an overview of the security and encryptions capabilities within Veritas Backup Exec. This document is intended as a summary and does not represent a comprehensive list of security and encryption features in the Backup Exec software.

Please contact Veritas authorized reseller/partner or Veritas technical support if you believe you have discovered a security issue in Backup Exec or any other Veritas product.

## SUMMARY

With the new encryption and security capabilities offered by Backup Exec, your company's critical and sensitive data can be easily protected in a secure format from unauthorized access and security threats. 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—Cloud. Virtual. Physical.

## FOR MORE INFORMATION

| | |
|---|---|
| Backup Exec web page | www.backupexec.com |
| Backup Exec admin guide | www.backupexec.com/admin |
| Backup Exec resources | www.backupexec.com/resources |
| Backup Exec compatibility | www.backupexec.com/compatibility |
| Backup Exec support | www.backupexec.com/support |
| Backup Exec training | www.backupexec.com/training |
| Backup Exec user forum | www.backupexec.com/forum |
| Backup Exec blogs | www.backupexec.com/blogs |
| 60-day trialware for Backup Exec | www.backupexec.com/trybe |
| Backup Exec subscription | www.backupexec.com/subscription |
| Backup Exec promotions | www.backupexec.com/save |
| PartnerNet | https://partnernet.veritas.com/ |
| Find a Backup Exec Partner | http://veritas.force.com/public |

## ABOUT VERITAS TECHNOLOGIES LLC

Veritas Technologies empowers businesses of all sizes to discover the truth in information—their most important digital asset. Using the Veritas platform, customers can accelerate their digital transformation and solve pressing IT and business challenges including multi-cloud data management, data protection, storage optimization, compliance readiness and workload portability—with no cloud vendor lock-in. Eighty-six percent of Fortune 500 companies rely on Veritas today to reveal data insights that drive competitive advantage. Learn more at **www.veritas.com** or follow us on Twitter at **@veritastechllc**.

Veritas Technologies LLC
500 East Middlefield Road
Mountain View, CA 94043 USA
+1 (866) 837 4827
**veritas.com**

For specific country offices and contact
numbers, please visit our website.
**www.veritas.com/about/contact**

VERITAS™

The truth in information.