



# BackBox<sup>®</sup> E4.13 Tape Encryption Option

Abstract

This Tape Encryption Option document is for BackBox<sup>®</sup> E4.13

Published: July 2024



## Legal Notice

© Copyright 2013, 2024 ETI-NET Inc. All rights reserved.

Confidential computer software. Valid license from ETI-NET Inc. required for possession, use or copying.

The information contained herein is subject to change without notice. The only warranties for ETI-NET- 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. ETI-NET shall not be liable for technical or editorial errors or omissions contained herein.

BackBox is registered trademark of ETI-NET Inc.

StoreOnce is a registered trademark of Hewlett Packard Development, L.P.

Microsoft, Windows, and Windows NT are U.S. registered trademarks of Microsoft Corporation. Tivoli Storage Manager (TSM) is a registered trademark of IBM Corporation.

QTOS is a registered trademark of Quality Software Associates Inc.

All other brand or product names, trademarks or registered trademarks are acknowledged as the property of their respective owners.

This document, as well as the software described in it, is furnished under a License Agreement or Non- Disclosure Agreement. The software may be used or copied only in accordance with the terms of said Agreement. Use of this manual constitutes acceptance of the terms of the Agreement. No part of this manual may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, and translation to another programming language, for any purpose without the written permission of ETI-NET Inc.

Copyright © 2013, 2024 ETI-NET Inc. All rights reserved.

# Table of Contents

---

<b>INTRODUCTION</b> .....	<b>4</b>
Supported Operational Environments .....	4
BackBox VTC Encryption .....	4
Key Manager Server .....	4
Key Manager Client .....	4
<b>VLE SETUP</b> .....	<b>6</b>
VLE Key Generation Policy .....	6
KeyPerTape vs. KeyPerDrive .....	8
VTC Client (Non-VLE) Setup .....	8
BackBox Domain .....	10
<b>BACKBOX ENCRYPTION CONFIGURATION</b> .....	<b>12</b>
Enabling Encryption .....	12
Nonatomic License (License version prior to 4.09) .....	12
Atomic License (License version 4.09 and later) .....	12
VLE Configuration .....	13
VLE Virtual Tape Drives Topology .....	13
Enabling LTO 4 Virtual Tape Emulation in a VTC .....	14
Enabling VLE on Tapes in SCF .....	17
Replacement of FC HBA Card Emulating LTO 4 .....	18
Adding Key Manager in BackBox Configuration .....	18
<b>NON-VLE CONFIGURATION</b> .....	<b>20</b>
Key Manager Configuration .....	20
VTC Configuration .....	20
Generate RSA Key and Certificate Request .....	21
Sign Client Certificate and CA Certificate .....	22
Add the Key Manager in the BackBox Configuration .....	24
Add VTC Client Information in the BackBox Key Manager .....	25
Encryption in a Volume Group .....	32
Test BackBox Software Encryption Configuration .....	33
<b>USER INTERFACE CONFIGURATION</b> .....	<b>34</b>
VT Controller .....	34
Key Manager .....	34
ESKM only .....	34
KMIP only .....	35
Key Manager – VLE CLIM Clients .....	35
Volume Group .....	36
Encryption .....	36
VLE Setup .....	36
Report OBB038 – List of Encrypted Volumes .....	37
Volume .....	38
Volume Details .....	38
Volume Edition .....	38

# INTRODUCTION

This [Tape Encryption Option Manual](#) documents the tape encryption provided by the BackBox software running on VTC servers. The information provided in this manual and the following manuals listed below can provide useful information during the configuration and operation of the tape encryption:

[BackBox User Manual](#)

[BackBox Messages Manual and Troubleshooting](#)

Tape volumes can be encrypted by the BackBox VTC software or by the storage subsystem where the media is written by BackBox. This manual considers only the encryption provided by the BackBox VTC software.

## Supported Operational Environments

BackBox encryption is available for Windows File System Data Stores and for all NonStop systems supported by BackBox: H06.xx, J06.xx, and L06.xx.

The data is encrypted using IEEE 1619.1 (tape) industry standard algorithms before being sent to the Data Store.

The encryption algorithm uses a 256-bit encryption key stored on an external Key Management Server.

Encryption by BackBox software can be used with an Enterprise Security Key Manager (ESKM) and can optionally be fully integrated with the NonStop Volume Level Encryption (VLE) product. The backups created from Blade systems with LTO4 and VLE can be restored by older systems with LTO3 or CART3480 emulations, and vice-versa. When emulating LTO3 or CART3480, the BackBox VTC creates and retrieves in an ESKM the same encryption keys as would a CLIM implementing VLE.



For storage subsystems that implement data deduplication, such as StoreOnce, BackBox, data encryption avoids the deduplication.

Encryption or compression prevents deduplication algorithms from matching re-occurring data “chunks” which makes deduplication ineffective. For these subsystems, BackBox encryption should be performed only for a subset of the most sensitive volumes in distinct Volume Groups. Otherwise, all volumes should be encrypted by the storage subsystems themselves.



For QoreStor data stores, Key Manager encryption is not supported.

## BackBox VTC Encryption

The BackBox VTC tape emulation performs block level encryption. Block level encryption permits compression of each clear block of data before encrypting it. This improves the utilization of the storage while keeping the data-at-rest secure.

The BackBox tape emulation implements IEEE P1619.1 standard for tape-based encryption using the Advanced Encryption Standard algorithm and the Galois Counter Mode (known as AES-GCM) algorithm.

The AES Encryption algorithm uses a secret key. This key is suitable for block-mode encryption and it has an optional length of 164, 192, and 256 bits. BackBox tape emulation encryption implementation uses a 256-bit key.

The GCM provides an authentication algorithm that allows computing 16 bytes MAC for each tape block encrypted. This algorithm ensures strong authentication and block integrity.

The BackBox tape emulation software encryption can take advantage of the Intel processor AES-NI instruction set (if available) to accelerate execution of the AES algorithm and to reduce the CPU load when encrypting/decrypting data.

## Key Manager Server

As mentioned above, BackBox tape emulation encryption implementation uses a 256-bit key to encrypt or decrypt data. The key must be secured in a Key Manager server and must be available for the lifetime of the data stored in the virtual media.

The privacy of the data depends on the security of the key. The Key Manager server protects access to keys by allowing only authenticated users. Once both server and user digital certificates are authenticated by a certificate authority (CA), a secure communication channel (using TLS/SSL) is established between the server and the client, making any exchange private.

The Key Manager server can take care of a huge number of keys, which allows sharing key management infrastructure between NonStop systems and other platforms to take advantage of infrastructure investment and minimize management costs. There is no need for a separate infrastructure to generate, store, and protect tape volume keys for BackBox.

BackBox currently supports the following kinds of Key Manager servers:

- The Utimaco Enterprise Security Key Manager (ESKM).

In the BackBox configuration, depending on the type of client interface with the Key Manager, Key Manager Servers can be defined as distinct logical views with different configurations.

Each view is identified by an arbitrary Key Manager ID used by the BackBox domains. Such a view contains:

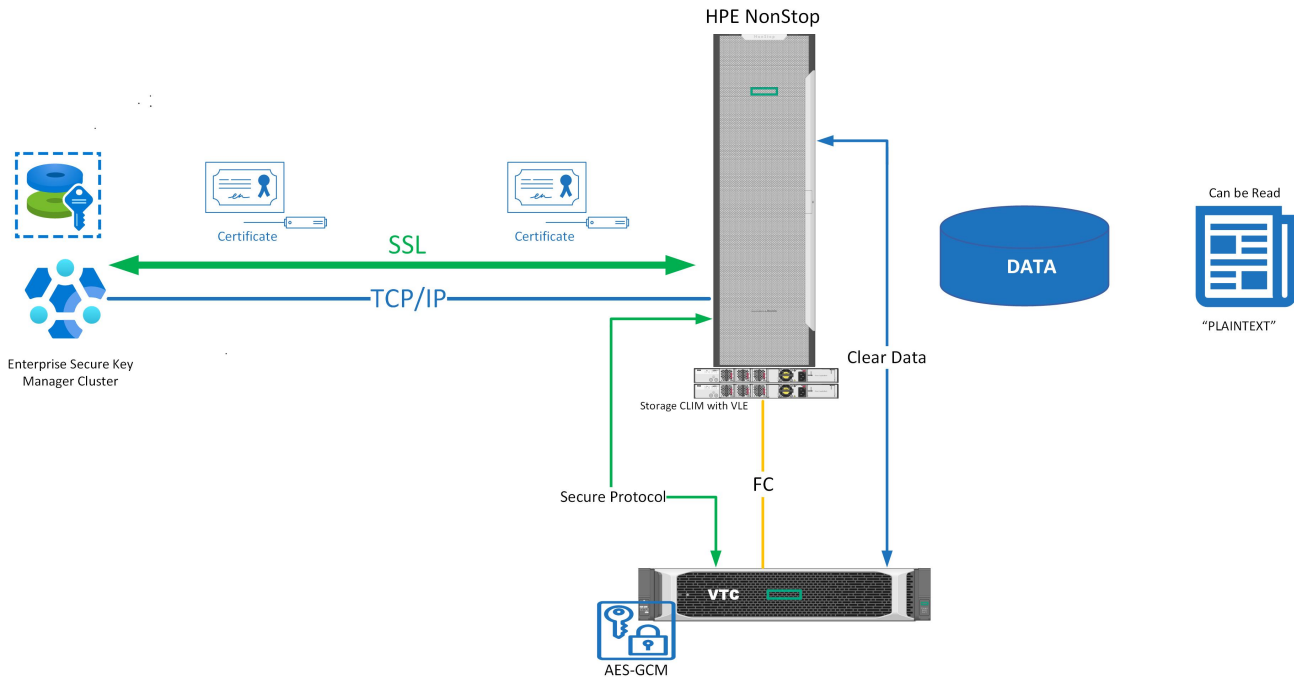
- general information, such as the server type (ESKM)
- the server's associated IP port and address(es)
- common Client Attributes, such as the possible connected Client Type and the Local Group.
- the list of possible clients able to reach the Key Manager server

## Key Manager Client

BackBox tape emulation software can interact with Key Management in one way:

- For a VLE setup, the client to the Key Manager is the CLIM (for ESKM only).

# VLE SETUP



For NonStop Volume Level Encryption (VLE), the Key Management appliance used is the Enterprise Secure Key Manager (ESKM), which is accessed via Storage CLIMs. This means that only NonStop systems supporting CLIMs (NonStop Blade systems and certain NS-series models) are supported.

The ESKM server generates and stores the keys, usually in a cluster of ESKM servers, replicating the keys on each server. The ESKM clusters can be split across multiple sites for site diversity.

Each Storage CLIM with the VLE option implements an ESKM Client that obtains keys from the ESKM and forwards them to the devices through the T10 SCSI Security Protocol command set that manages Encryption aware tape devices.

The BackBox tape emulation implements the T10 SCSI Security Protocol command set to integrate enterprise-class Key Management appliances. When emulating LTO 4 tape drives, BackBox virtual tape devices notify the CLIM that it can be used for encryption. In the BackBox configuration, CLIM and LTO 4 tape emulation configured for VLE usage is named VLE-CLIM Client and must be assigned to an ESKM Key Manager ID with Client type set to "VLEINTEROPERABILITY".

All LTO 4 virtual tape devices configured for VLE are dedicated for encryption/decryption purposes. Only LTO 4 media types can be presented to the Storage CLIM and \$ZSRV server in VLE encryption mode.

When attaching a VLE-CLIM Client to a Key Manager ID, it is necessary to identify the list of CLIMs that can be used to reach the ESKM server.

Encryption key rotation frequency is based on the VLE key generation policy (KeyPerTape or KeyPerDrive) set in SCF.

## VLE Key Generation Policy

When an LTO 4 tape drive is configured as an encryption device, VLE records a Drive Encryption context for it. This context holds information as the MasterKeyName (that identifies the tape drive by the tape drive

identifier and the CLIM number it connects to), the encryption algorithm used by the tape drive, the key size needed by the tape drive, and the key generation policy: KeyPerTape or KeyPerDrive.

To work with VLE, most of the BackBox encryption configuration consists of making LTO 4 tape drives available to NonStop systems and enabling VLE in the NonStop environment.

STORAGE - Status TAPE \NSBLDE4.\$VTE400, ENCRYPTION

Media

Not present or encryption status unknown

Drive

MasterKeyName.....N2108001086022114\_S066666C1002541

KeyAlgorithm.....GCM-AES

KeySize.....256

KeyGenPolicy.....KeyPerTape

**When the KeyPerTape key generation policy is set (via SCF), each tape written by the tape drive will use a unique encryption key. Each time data is rewritten on the media, (when the media state changes from state SCRATCH to SELECT), the tape drive will use a new key to encrypt the data. In this case, the key is automatically renewed and the key is identified by a key name associated with the media. In some situations, such as the need to restore the media's data on a remote NonStop system using another ESKM Cluster, it will be necessary to export the media key in the other ESKM Cluster using the Media KeyName.**

STORAGE - Status TAPE \NSBLDE4.\$VTE400, ENCRYPTION

Media

KeyName.....N7566B3CCLAB035D873833A969D0008\_BBBBBBBB\_1911112107

KeyAlgorithm.....GCM-AES

KeySize.....256

Drive

MasterKeyName.... N2108001086022114\_S066666C1002541

KeyAlgorithm.....GCM-AES

KeySize.....256

KeyGenPolicy.....KeyPerTape

**When the KeyPerDrive key generation policy is selected, each tape written by the tape drive will use the current tape drive Encryption Key. Each time media data is rewritten, (when the media state changes from state SCRATCH to SELECT), the tape drive will use the key identified by its Drive context. The key is not renewed (or changed) automatically. If the user wants to change the drive key, it will be necessary to ALTER the tape drive in SCF using the NEWENCRYPTIONKEY attribute.**

STORAGE - Status TAPE \NSBLDE4.\$VTE400, ENCRYPTION

Media

Not present or Encryption status unknown

Drive

MasterKeyName. ... N2108001086022114\_S066666C1002541

KeyName..... N2108001086022114\_2011023101234

KeyAlgorithm. .... GCM-AES

KeySize. .... 256

KeyGenPolicy. .... KeyPerDrive

As with KeyPerTape, when the media's data is rewritten, a Media Key Name is used to identify the key that was used by the tape drive at encryption time. Even in a case where a user renews the Drive Encryption key and changes the drive key context, the Media Key Name will still be available. The key most recently used to write data on each media is retained to facilitate later decryption, regardless of whether the key associated with the drive has been changed some time after the media was written.

```
STORAGE - Status TAPE \NSBLDE4.$VTE400, ENCRYPTION
```

```
Media
```

```
KeyName.....N7566B3CCLAB035D873833A969D0008_BBBBBBBB_1911112113
KeyAlgorithm.....GCM-AES
KeySize.....256
```

```
Drive
```

```
MasterKeyName.... N2108001086022114_S066666C1002541
KeyName..... N2108001086022114_2011023101234
```

The samples above show examples of drive status of media backup with current Drive key context. Below are examples for the same media after renewal of the drive Encryption key.

Since media is usually written, read and rewritten by different tape drives, a Media Key Name will always be generated to identify the encryption key of the media, regardless of which key generation policy has been used. Key management actions, such as export, delete or query should be performed using the Media Key Name.

```
STORAGE - Status TAPE \NSBLDE4.$VTE400, ENCRYPTION
```

```
Media
```

```
KeyName..... N7566B3CCLAB035D873833A969D0008_BBBBBBBB_1911112113
KeyAlgorithm..... GCM-AES
KeySize.....256
```

```
Drive
```

```
MasterKeyName.... N2108001086022114_S066666C1002541
KeyName..... N2108001086022114_20111118134512
KeyAlgorithm..... GCM-AES
KeySize.....256
KeyGenPolicy..... KeyPerDrive
```

## KeyPerTape vs. KeyPerDrive

The nature of the tape media is used to hold different data generations for specific periods of time (retention).

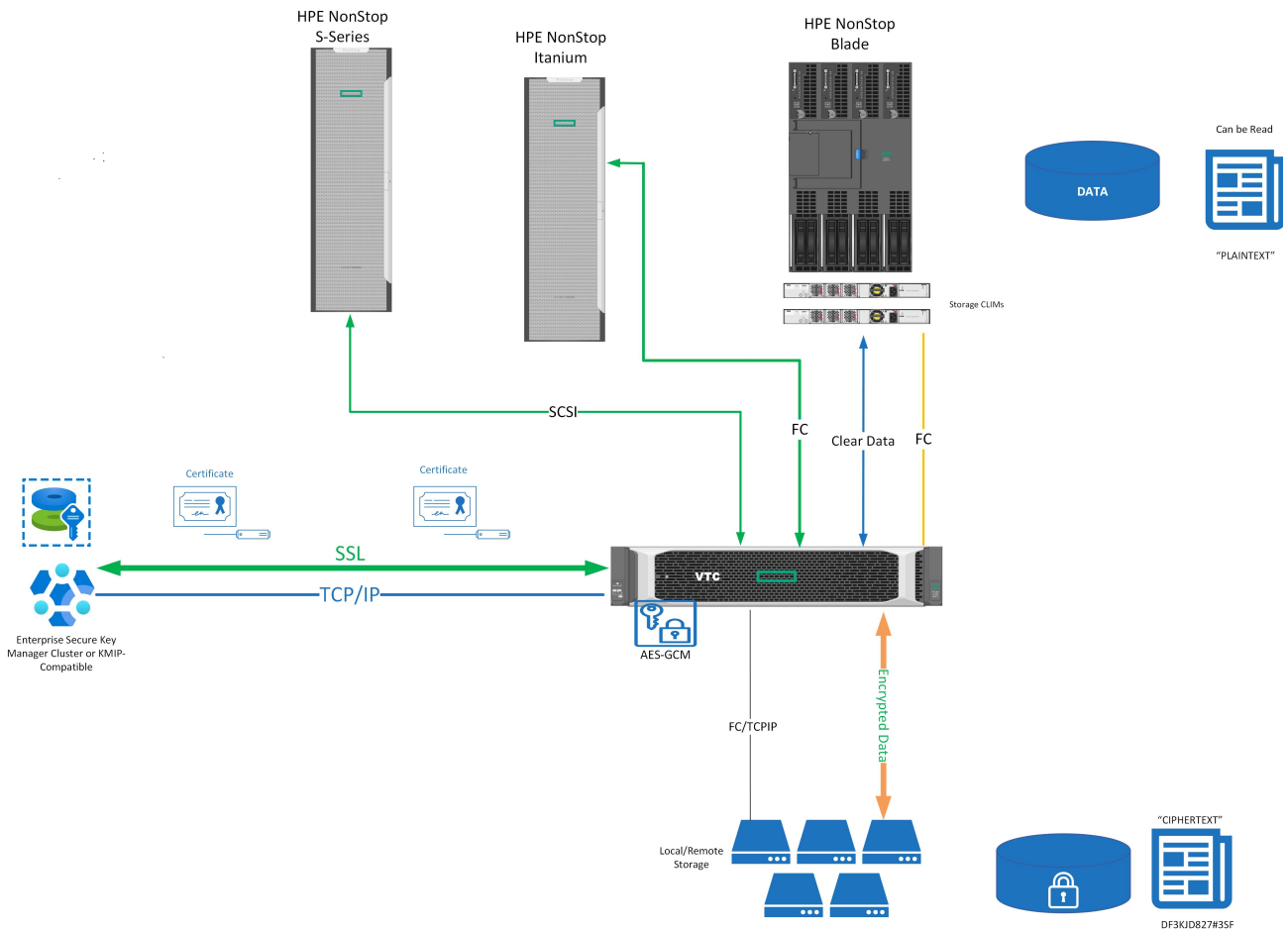
The fact that KeyPerTape policy generates a new key when a virtual tape is rewritten makes its usage more secure.

If a virtual volume were tampered with, only the data on that specific virtual volume would be compromised. The ESKM administrator can delete the key to avoid a security breach. Also, key renewal is performed automatically and doesn't require manual intervention at the TAPE device level: there is no need to STOP and ALTER the device.

The [KeyPerDrive](#) policy is less secure, since multiple virtual volumes will all be encrypted using the same key. Having one virtual volume tampered with would be more critical, as data on all virtual volumes encrypted with that key could be compromised. Deleting that key would affect much more data, as none of the other virtual volumes encrypted with that key would be retrievable thereafter. We highly recommend using the policy with less exposure: [KeyPerTape](#) policy.

## VTC Client (Non-VLE) Setup





BackBox software includes a key management client to interface with Key Manager server. This allows tape encryption to the whole range of NonStop systems. All tape device types supported by BackBox, CART3480, LTO 3 and LTO 4, can encrypt. VTCs are registered as clients to the Key Manager Server.

In the BackBox configuration, VTC with encryption devices licensed are named VTC Client and can be assigned to an ESKM or a KMIP Key manager ID. For each VTC Client attached, we will need to define information related to the TLS/SSL communication required to connect to the Key Manager server.

When an ESKM Key manage is set to used "VLE INTEROPERABILITY" Client type,

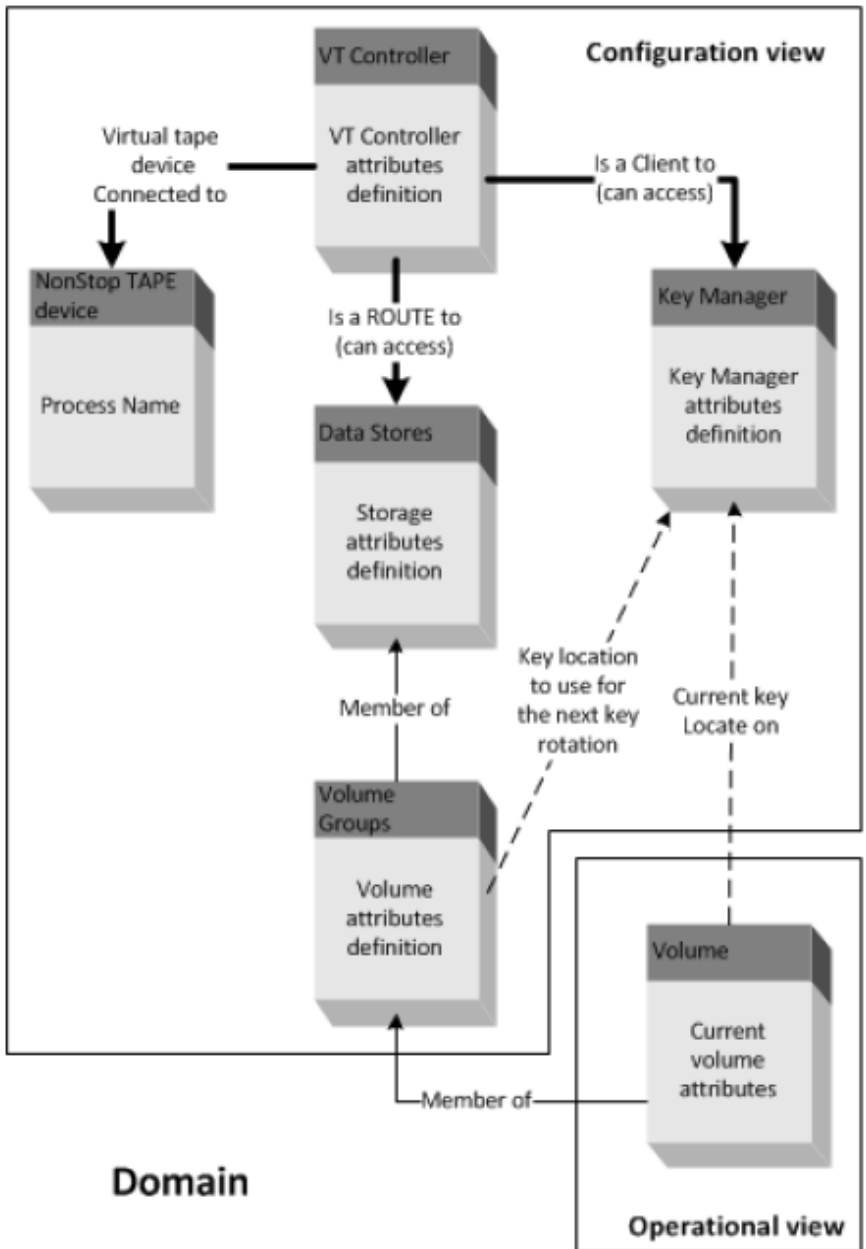
- VLE key naming convention will be used :

**NXXXXXXXXXXXXXXXXXXXXXXXXXXXXX\_BBBBBBBB\_ZZZZZZZZ**

- Access to encrypted virtual volume can be made across NonStop node not supporting Storage CLIM and Storage CLIM configure with VLE.
- VTC Client can be used by any available virtual tape drive. Virtual tape drives are not dedicated to encryption.
- Usage of encryption is not restricted to LTO 4 media type. LTO 3 and CART3480 can also be used.
- VTC Client will use KeyPerTape method when requesting a new key even VLE the key generation policy KeyPerDevice is used for VLE managed LTO 4 devices.

A VTC Client can be assigned to an ESKM or KMIP Key manager ID when the Client type is set to "VTC ONLY":

- In this mode, BackBox key naming convention would be used:
- **BBOX\_XXXXXXXXXXXXXXXXXXXXXXXXXXXXX\_AAAAAAAAAA**
- Access to encrypted virtual volume can be made across any type of NonStop node.
- VTC Client can be used by any available virtual tape drive. Virtual tape drives are not dedicated to encryption (except LTO 4 configured for VLE.)
- Usage of encryption is not restricted to LTO 4 media type. LTO 3 and CART3480 can also be used.
- When data retention date expired for specific volumes, encrypted data still remains on them. A simple way to make sure expired encrypted data can't be recoverable is to delete the encryption key associated to it from the Key Manager server. Doing so, protected data will be secured, even if expired data can be found in several copies (on a DR site, vault in Backup Enterprise, etc...). The VTC client can help automate deletion of encryption key when data has expired. VTC client can request Key Manager server to delete old key when virtual tape volume is SCRATCHED by rewriting data or by freeing expired volumes when running the daily cleanup job (OBB017.)
- It is also possible to virtualize and encrypt data of non-encrypted legacy physical tape media.
- Each virtual volume will be encrypted with a different key and will be rotate each time the volume is rewritten (same has VLE KeyPerTape.)



A BackBox license key must be installed to allow VTCs encryption.

If the Client uses to the Key Manager, CLIM for VLE, the user must configure the BackBox domain in the same way:

- The encryption is enabled in the Volume Group configuration by choosing an encryption algorithm (AES-GCM 256 bits).
- The Key Manager must be registered under an arbitrary Key Manager ID and all its clients defined.
- The setup must be verified by the Test Function available on the Key Manager configuration page.
- The BackBox license key contains a maximum number of encryption drives concurrently active. The tape workload requiring encryption should be anticipated, especially in the case of a VLE setup where VLE drives cannot be used to write non-encrypted backups.

The Key Manager ID and the encryption algorithm are saved in the BackBox catalog of virtual volumes to know how to decrypt each volume, independently of configuration changes to the Volume Group or to the Key Manager server.

The Key Manager ID is a logical identifier that becomes important when there are more than one operational Key Manager servers on a site and for D/R operations where three duplications are to be managed:

- The replication of encrypted virtual volumes.
- The replication of catalogs (BackBox, DSM/TC and TMF catalogs).




The Key Manager ID, which is an arbitrary BackBox ID, is part of the BackBox replicated catalog. The Key Manager IDs must be planned from an enterprise point of view.

- The replication of keys from the Key Manager server of the Primary site to the Key Manager server on the Secondary site.

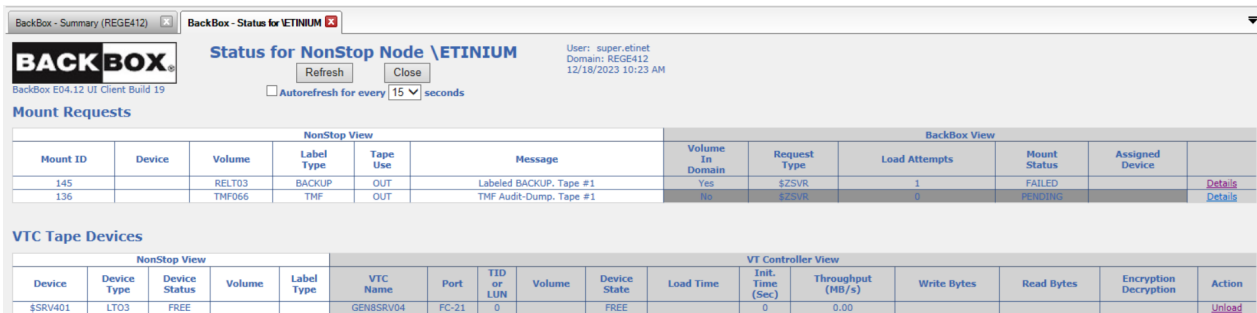
Once the system is configured, the encryption functionality is totally transparent and automated. Once a NonStop tape mount requests to mount a volume from an encrypted Volume Group is recognized, the BackBox Domain will find a free virtual tape drive connected to this NonStop system which allows it to receive the encryption key from the Key Manager server (via the appropriate Key Manager Client) and access the storage location of the virtual volume.

When the virtual device is found, the BackBox Domain will request it in order to load the volume and put it online. Once the volume is online, a request will be generated through a secure TLS/SLL session between the Key Manager server and Client to obtain the Encryption Key (identified by the Encryption Key ID) needed by the virtual tape device to encrypt or decrypt the virtual tape volume data.



When errors related to encryption happen, any attempt to use the drives will fail with Error 101 (“tape is write-protected”), and a descriptive message should be logged in the EMS. In such a case, refer to [BackBox Messages Manual and Troubleshooting](#) and [Guardian Procedure Errors and Messages Manual](#)

To see the encryption/decryption status while a tape is being written/read: the encryption/decryption status for each drive is displayed on the BackBox UI status page.



The screenshot shows the BackBox Status for NonStop Node \ETINIUM interface. It includes a 'Mount Requests' table and a 'VTC Tape Devices' table.

NonStop View					BackBox View					
Mount ID	Device	Volume	Label Type	Tape Use	Message	Volume In Domain	Request Type	Load Attempts	Mount Status	Assigned Device
145		REL03	BACKUP	OUT	Labeled BACKUP, Tape #1	Yes	\$ZSVR	1	FAILED	
136		TMF066	TMF	OUT	TMF Audit-Dump, Tape #1	No	EEZSVR	0	PENDING	

NonStop View					VT Controller View											
Device	Device Type	Device Status	Volume	Label Type	VTC Name	Port	TID or LUN	Volume	Device State	Load Time	Init. Time (Sec)	Throughput (MB/s)	Write Bytes	Read Bytes	Encryption Decryption	Action
\$SRV401	LTO3	FREE			GEN8SRV04	FC-21	0		FREE		0	0.00				Unload

# BACKBOX ENCRYPTION CONFIGURATION

## Enabling Encryption

BackBox Tape Encryption is a licensed option. You will have to license virtual tape encryption devices per VTC regardless of the VLE setup. Make sure to specify the quantity of encryption devices (BBENCR) for each VTC server in the license order.

## Nonatomic License (License version prior to 4.09)

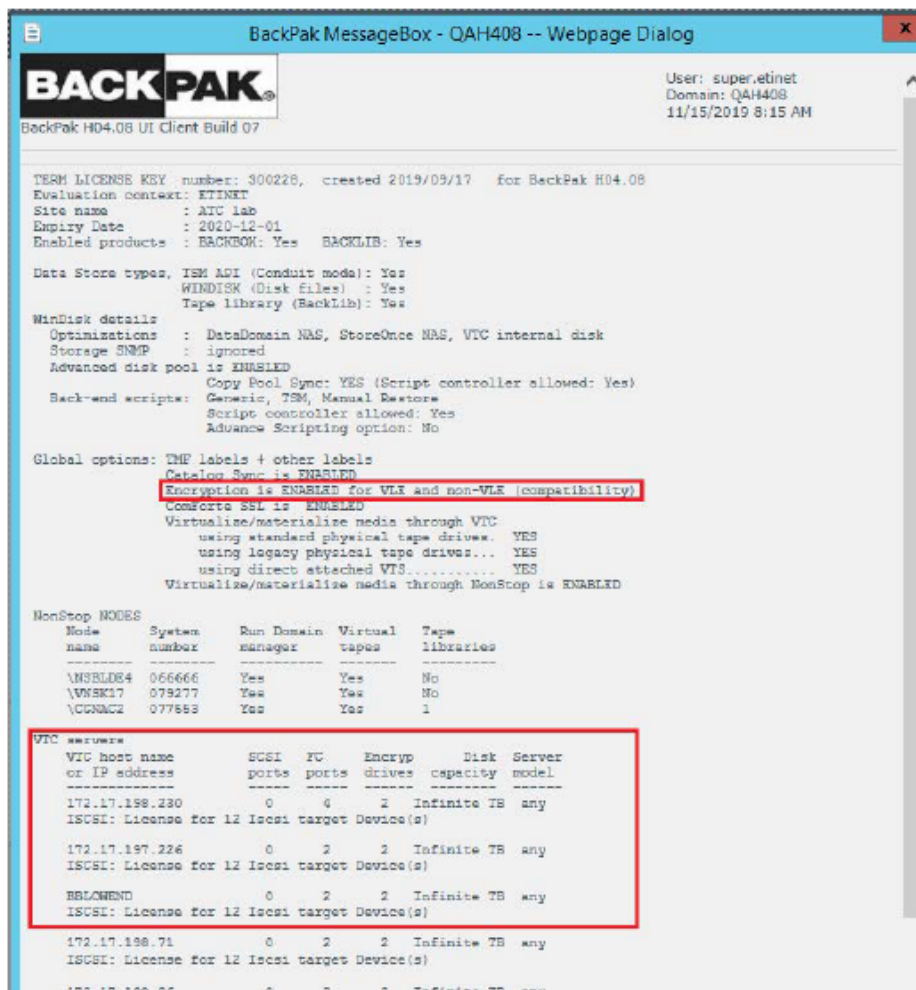
Without the encryption license option, the Key Manager tab does not appear on the Configuration page and, therefore, the encryption cannot be configured.

The encryption is controlled at two levels in the BackBox license key:

- Global control by the encryption option.
- In each VTC, the maximum number of virtual drives operating concurrently with encryption is limited. This number can be smaller than the actual number of drives when some tape volumes are not to be encrypted.

To verify the license control levels, go to Configuration > Domain > License Options

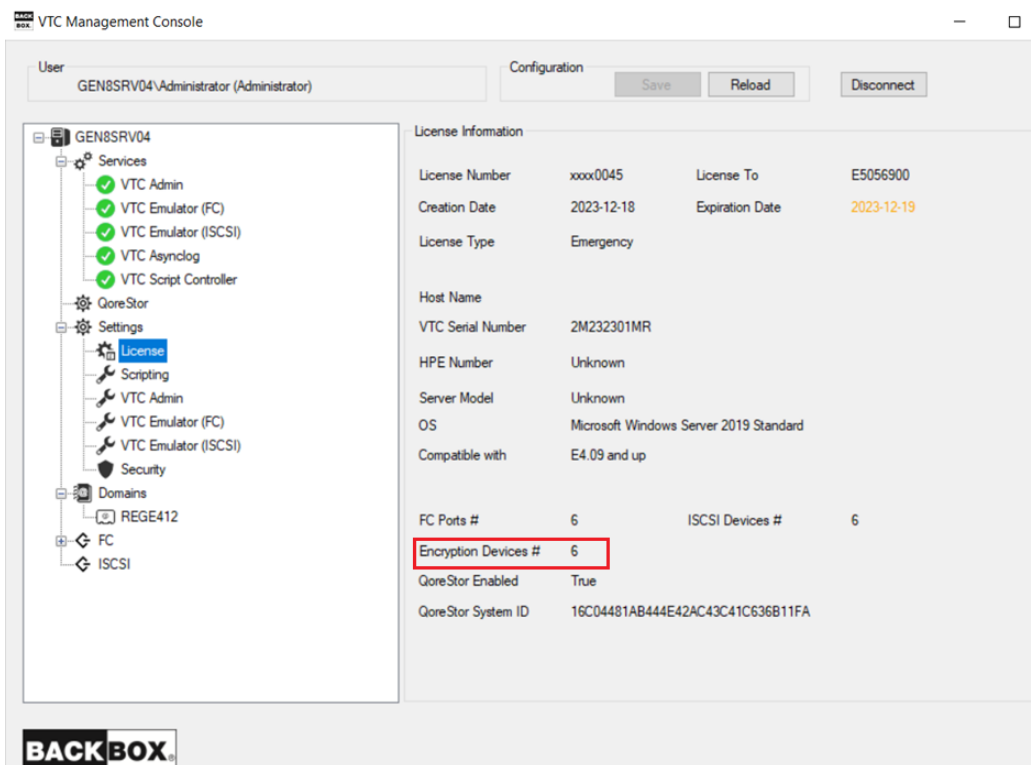
A demo license has generally no limitation on the number of drives concurrently encrypting or decrypting.



## Atomic License (License version 4.09 and later)

For domain license 4.09 and higher, the encryption devices are controlled by VTC license version.

Check the VTC Management Console > Settings > License for the info regarding the number of encryption devices.



## VLE Configuration

Volume Level Encryption requires the creation of a security officer that allows a member of the SUPER group to perform VLE operations and configuration tasks.

For more information about VLE requirements, installation and other product references, see [NonStop Volume Level Encryption Guide](#).

## VLE Virtual Tape Drives Topology

- Identify CLIMs that support VLE

The first step is to identify CLIMs supporting encryption, by determining which of them have VLE installed.

If it is not already known, the easiest way to verify that a given CLIM is ready for encryption is by using the SCF command:

```
STATUS CLIM $ZZSTO.*, KEYMANAGER
```

This command will list all CLIMs that have access to the ESKM Key Manager.

```
1- > status clim $zzsto.*, keymanager
```

```
STORAGE - KeyManager Status CLIM \NSBLDE4.$ZZSTO.#S1002531
```

```
CLIM not registered with Key Manager
```

```
STORAGE - KeyManager Status CLIM \NSBLDE4.$ZZSTO.#S1002533
```

```
CLIM not registered with Key Manager
```

```
STORAGE - KeyManager Status CLIM \NSBLDE4.$ZZSTO.#S1002541
```

```
KeyManager 10.10.10.54 OK
```

```
KeyManager 10.10.10.55 OK
```

```
STORAGE - KeyManager Status CLIM \NSBLDE4.$ZZSTO.#S1002543
```

```
CLIM not registered with Key Manager
```

```
STORAGE - KeyManager Status CLIM \NSBLDE4.$ZZSTO.#S1002561
```

```
CLIM not registered with Key Manager
```

In this example the only CLIM with VLE Encryption support is S1002541.

Then, for each VLE-supporting CLIM identified in the previous step, display all of the WWN port names available on that specific CLIM by using the TACL command:

```
climcmd <clim-name> lunmgr -wwns
```

```
$SAS22 ETINET 4> climcmd S1002541 lunmgr --wwns
```

```
slot port wwn speed
```

```
1 1 5001438001336F40 4 Gbit
```

Termination Info: 0

- Identify VTC Ports Connected to the VLE-Supporting CLIMs

For each CLIM identified to be used for BackBox VLE virtual tape drives, determine the VTC Server, the FC ports and the tape drives that will be used for VLE.

Log on to the BackBox UI interface and navigate to the VT Controller configuration page. A list of each VTC available port is shown in VTC Ports table. The Host WWN column displays the WWN of the host port connected to the VTC port.

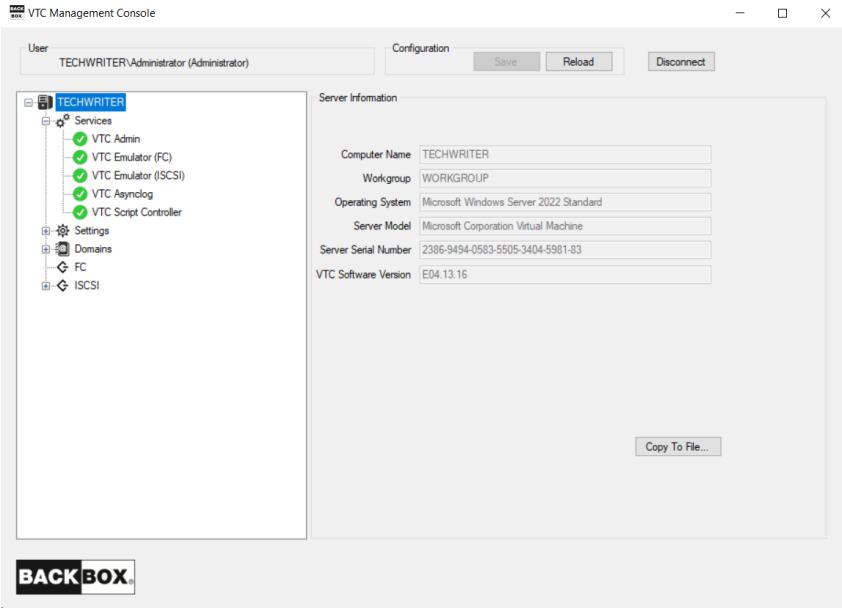
Port	Port WWN/Serial #	Status	Speed	Card Module	Card Slot Id/Target IP	Card Channel Id	Host WWN
FC-21	1000001086053700	UP	16-Gb	FC-162P	2	1	50014380331312E8
FC-22	1000001086053701	UP	16-Gb	FC-162P	2	2	21FDC4F57C40A0E6

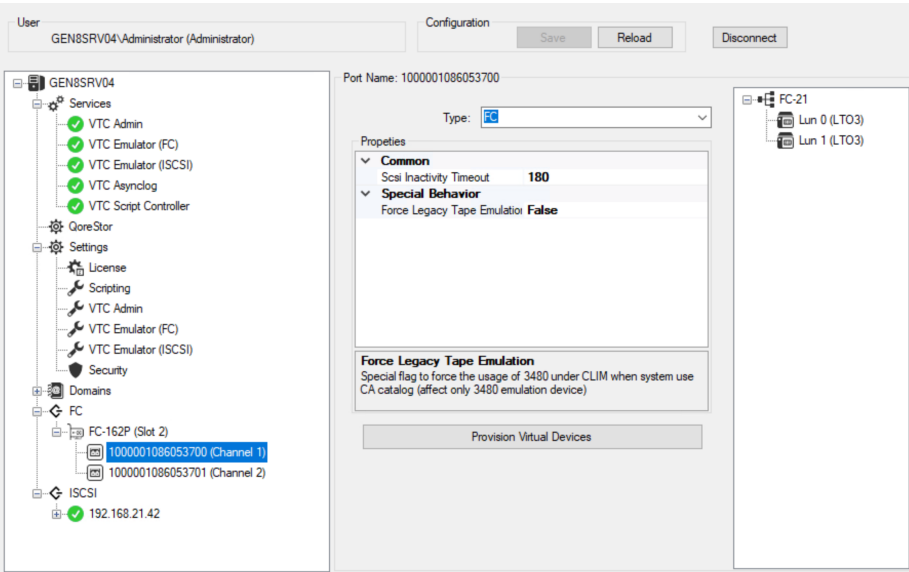
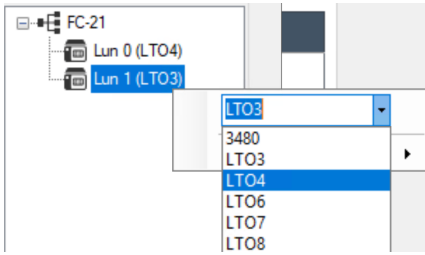
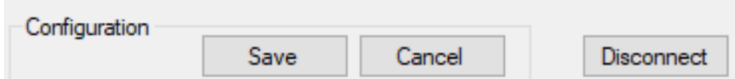
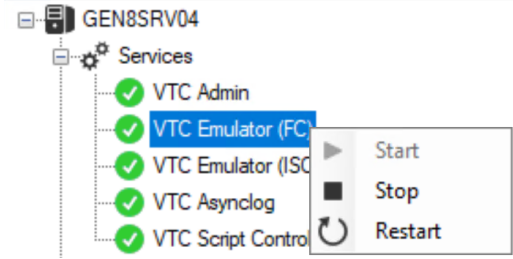
### Enabling LTO 4 Virtual Tape Emulation in a VTC

The VTC is internally configured by default for LTO 3 media type. To enable the LTO 4 emulation required by VLE, the tape drives must be stopped and reconfigured in SCF, in CLIM, and in VTC.

For a VTC, there might be several entities involved: several BackBox domains, several NonStop nodes, and more than one CLIM per node.

Step	Description																																																																	
1. Take note of the location (CLIM # and LUN #) of the tape drives to be changed to LTO4	<p>At the TACL prompt:                      SCF INFO CLIM &lt;clim-id&gt;,DETAIL                      STORAGE - Detailed Info CLIM \NSBLDE4.\$ZZST0.#C1002561</p> <p>Configured Devices:</p> <table border="1"> <thead> <tr> <th>Type</th> <th>Name</th> <th>Primary CPU</th> <th>Backup CPU</th> <th>Lun</th> </tr> </thead> <tbody> <tr><td>TAPE</td><td>\$LW2131</td><td>0</td><td>1</td><td>1</td></tr> <tr><td>TAPE</td><td>\$LW2132</td><td>0</td><td>1</td><td>2</td></tr> <tr><td>TAPE</td><td>\$LW2133</td><td>0</td><td>1</td><td>3</td></tr> <tr><td>TAPE</td><td>\$LW2134</td><td>0</td><td>1</td><td>4</td></tr> <tr><td>TAPE</td><td>\$G86130</td><td>3</td><td>0</td><td>17</td></tr> <tr><td>TAPE</td><td>\$G86131</td><td>3</td><td>0</td><td>18</td></tr> <tr><td>TAPE</td><td>\$G86132</td><td>3</td><td>0</td><td>19</td></tr> <tr><td>TAPE</td><td><b>\$G86133</b></td><td>3</td><td>0</td><td>20</td></tr> <tr><td>TAPE</td><td>\$G86140</td><td>0</td><td>1</td><td>29</td></tr> <tr><td>TAPE</td><td>\$G86141</td><td>1</td><td>2</td><td>30</td></tr> <tr><td>TAPE</td><td>\$G86142</td><td>2</td><td>3</td><td>31</td></tr> <tr><td>TAPE</td><td>\$G86143</td><td>3</td><td>0</td><td>32</td></tr> </tbody> </table>	Type	Name	Primary CPU	Backup CPU	Lun	TAPE	\$LW2131	0	1	1	TAPE	\$LW2132	0	1	2	TAPE	\$LW2133	0	1	3	TAPE	\$LW2134	0	1	4	TAPE	\$G86130	3	0	17	TAPE	\$G86131	3	0	18	TAPE	\$G86132	3	0	19	TAPE	<b>\$G86133</b>	3	0	20	TAPE	\$G86140	0	1	29	TAPE	\$G86141	1	2	30	TAPE	\$G86142	2	3	31	TAPE	\$G86143	3	0	32
Type	Name	Primary CPU	Backup CPU	Lun																																																														
TAPE	\$LW2131	0	1	1																																																														
TAPE	\$LW2132	0	1	2																																																														
TAPE	\$LW2133	0	1	3																																																														
TAPE	\$LW2134	0	1	4																																																														
TAPE	\$G86130	3	0	17																																																														
TAPE	\$G86131	3	0	18																																																														
TAPE	\$G86132	3	0	19																																																														
TAPE	<b>\$G86133</b>	3	0	20																																																														
TAPE	\$G86140	0	1	29																																																														
TAPE	\$G86141	1	2	30																																																														
TAPE	\$G86142	2	3	31																																																														
TAPE	\$G86143	3	0	32																																																														
2. Stop all tape drives emulated by the VTC to update	<p>NonStop, at the SCF command prompt:  <b>RESET TAPE \$G8*, FORCE</b></p>																																																																	
3. Delete the tape drives to change to LTO4 (List in Step 1)	<p>NonStop, at the SCF command prompt:  <b>DELETE TAPE \$G86133</b></p>																																																																	

Step	Description
<p>4. Stop the VTC Emulator (FC) Service</p>	<p>In a Remote Desktop session to the VTC</p> <p>Open the Search dialog and type VTC Management Console and click on the executable to start it.</p>  <p>Right-click on the VTC Emulator (FC) of the Services node and click on the Stop action.</p> 
<p>5. In the CLIM, remove the entries to change to LT04 (List in Step 1)</p>	<p>At the TACL prompt:</p> <pre>climcmd C1002561 lunmgr --scan climcmd C1002561 lunmgr --delete 20</pre> <p>Are you sure you want to delete lun 20 (tape HPE M8505 #BB030FA705)? y Termination Info: 0</p>

Step	Description
<p>6. Update the VTC internal configuration</p>	<p>Using the VTC Management Console, expand the FC and HBA Card node and click on the identified Port connected to the VLE CLIM.</p>  <p>Replace the emulation type LTO3 by LTO4 on the devices that will be VLE.</p>  <p>If all devices are designated to be VLE, right-click on the Port ID node and select the LTO4 emulation to change all devices at once.  <b>Note:</b> Additional LUN can be added by clicking on the Provision Virtual Devices button.  Save changes by clicking on the Save button.</p> 
<p>7. Restart the VTC Emulator FC Service</p>	<p>Using the VTC Management Console, right-click on the VTC Emulator (FC) of the Services node and click on Start.</p>  <p>If there is a syntax error, the service will stop immediately.  If the service stops, check the reason in the Event log:  In the MS-Windows menu, Administrative Tools, select Event Viewer &gt; Applications and Services Logs &gt; Virtual Tape Controller.</p>



Step	Description																																
8. Rescan the CLIM and approve the new LTO4 tape drives	<p>At the TAEL prompt:</p> <pre>climcmd C1002561 lunmgr -scan</pre> <p>Termination Info: 0</p> <pre>climcmd C1002561 lunmgr --approve</pre> <p>OK to assign lun 20 to tape HPE Ultrium4-SCSI #BB030FA705? <b>y</b></p> <p>Termination Info: 0</p>																																
9. Re-add the LTO4 tape drives in SCF (List in Step 1)	<p>Adjust the SCF command to add the tapedrives, the LUN # might be changed.</p> <p>Then execute the command:</p> <pre>ADD TAPE \$G86133, SENDTO STORAGE, &amp; PRIMARYCPU 2, BACKUPCPU 3, &amp; CLIM S1002531, &amp; LUN 20</pre>																																
10. Restart the tape drives emulated by the VTC	<p>At the SCF command prompt:</p> <pre>START TAPE \$&lt;tape-name-pattern&gt;</pre> <p>Check in EMS the messages reporting the tape drives starting.</p> <p>Verify the NonStop systems recognized by the LTO4 media type:</p> <pre>MEDIACOM INFO TAPEDRIVE</pre> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Tape Drive Name</th> <th>Device Type</th> <th>NL Check</th> <th>BLP Check</th> </tr> </thead> <tbody> <tr> <td>\$G64131</td> <td>LT03</td> <td>OFF</td> <td>ON</td> </tr> <tr> <td>\$G64140</td> <td>LT04</td> <td>OFF</td> <td>ON</td> </tr> <tr> <td>\$G66130</td> <td>LT03</td> <td>OFF</td> <td>ON</td> </tr> <tr> <td><b>\$G66133</b></td> <td><b>LT04</b></td> <td><b>OFF</b></td> <td><b>ON</b></td> </tr> <tr> <td>\$G66140</td> <td>LT04</td> <td>OFF</td> <td>ON</td> </tr> <tr> <td>\$G64141</td> <td>LT04</td> <td>OFF</td> <td>ON</td> </tr> <tr> <td>\$G66141</td> <td>LT04</td> <td>OFF</td> <td>ON</td> </tr> </tbody> </table>	Tape Drive Name	Device Type	NL Check	BLP Check	\$G64131	LT03	OFF	ON	\$G64140	LT04	OFF	ON	\$G66130	LT03	OFF	ON	<b>\$G66133</b>	<b>LT04</b>	<b>OFF</b>	<b>ON</b>	\$G66140	LT04	OFF	ON	\$G64141	LT04	OFF	ON	\$G66141	LT04	OFF	ON
Tape Drive Name	Device Type	NL Check	BLP Check																														
\$G64131	LT03	OFF	ON																														
\$G64140	LT04	OFF	ON																														
\$G66130	LT03	OFF	ON																														
<b>\$G66133</b>	<b>LT04</b>	<b>OFF</b>	<b>ON</b>																														
\$G66140	LT04	OFF	ON																														
\$G64141	LT04	OFF	ON																														
\$G66141	LT04	OFF	ON																														

## Enabling VLE on Tapes in SCF

Step	Description
11. Enable VLE on the selected tape drives	<p>At the SCF command prompt:</p> <pre>STOP \$&lt;tape-name&gt; ALTER \$&lt;tape-name &gt;, KeyGenPolicy KeyPerTape START \$&lt;tape-name &gt; STATUS \$&lt;tape-name &gt;, ENCRYPTION</pre> <p>Sample drive with enabled VLE:</p> <pre>l-&gt; status\$G64141,Encryption STORAGE - Status TAPE \NSBLDE4.\$G64141, ENCRYPTION Media Not present or Encryption status unknown Drive MasterKeyName. . . N2103001086022117_S066666C1002541 KeyAlgorithm GCM-AES KeySize. . . 256 KeyGenPolicy KeyPerTape</pre>
12. Update the Domain configuration with the new drive attributes	<p>Log in to the BackBox UI, go to the Configuration, VTC page.</p> <p>Select the VTC.</p> <p>Switch to the configuration Edit mode.</p> <p>Select the Refresh tab, select the Guardian node and click the Refresh button; the response time might take up to one minute.</p> <p>The already configured drives will be updated to LTO4 and VLE.</p> <p>Save the configuration.</p>

The resulting BackBox UI should show the VLE indication on the updated drives:

VTC Ports <span style="float:right">Refresh</span>							
Port	Port WWN/Serial #	Status	Speed	Card Module	Card Slot Id/Target IP	Card Channel Id	Host WWN
FC-21	1000001086053700	UP	16-Gb	FC-162P	2	1	50014380331312E8
FC-22	1000001086053701	UP	16-Gb	FC-162P	2	2	21FDC4F57C40A0E6

Virtual Devices												
Node	Guardian Device	Device Type	Serial Number	Port	Target	Lun	VLE	Explicit Only	Reserved For	Host WWN	Status	Guardian Port
NETINIUM	\$SRV401	LTO3	BB05370000	FC-21	0	0		False	...	50014380331312E8	FREE	\$ZZSTO.#S100231

Copyright ETI-NET, 2003-2023

## Replacement of FC HBA Card Emulating LTO 4

Should an FC HBA card in a VTC fail, it may need to be replaced. Replacing the HBA of the CLIM connected to it will have the same functional impact as replacing a group of tape drives with new ones. All virtual LTO 4 tape drives emulated using the new HBA will be seen by the CLIM as different tape drives. Also, those tape drives will not, by default, be managed by the VLE for encryption, even if the prior tape drives were all set to encrypt or decrypt data.

Some pre- and post-card-replacement actions will be needed to achieve this task.

Important:

The following activity needs to be carried out by a local system user member of the SAFEGUARD encryption officer group:

Before replacing the HBA:

In SCF, perform the following actions on the affected (associated with the FC Ports of the failed FC HBA) LTO 4 tape drives individually by using the pattern process name (only for virtual tape drives connected to the port that needs to be replaced):

- Stop the tape drive.
- Alter the tape drive with the attribute: KEYGENPOLICY NOENCRYPTION.
- Start the tape drive.
- Status tape drive with attribute: ENCRYPTION, to validate the result.

When done, STOP all tape drives again and replace the failed FC HBA.

After the HBA is replaced, re-activate the key generation policy for the tape drives that use the new HBA.

- Stop the tape drive.
- Alter the tape drive with the attribute: KEYGENPOLICY KEYPERTAPE.
- Start the tape drive.
- Status tape drive with the attribute: ENCRYPTION, to validate the result.

## Adding Key Manager in BackBox Configuration

Attach the listed CLIM supporting the VLE to be able to reach the targeted ESKM Key Manager represented by a BackBox Key Manager's configuration entity (Key Manager ID).

Log on to the BackBox UI interface.

- Select the Configuration menu and select the Switch to Edit mode.
- Select the Key Manager tab.
- Select the targeted Key Manager ID.



A VLE-CLIM Client can be attached to an ESKM Key Manager Type only. If the Key Manager entity doesn't exist, create one.

Click on the Create Key Manager button and fill in the Key Manager information:

- Choose an alias name and type it in the Key Manager ID file.
- Server Type must be set to ESKM.
- Client Type must be set to VLE INTEROPERABILITY.
- Other fields can remain empty or filled in for self-configuration documentation or for future use.

**BACKBOX** Administration

BackBox E04.12 UI Client Build 19

Status | Domain | NSK Nodes | VT Controller | **Key Manager** | Data Store | Volume Group

**Configuration**

Save | Cancel | Create Key Manager

W3162 Domain license will expire on 2024-01-22.

Key Manager ID	Server Type	Client Type		
<a href="#">ESKMVTCONLY</a>	ESKM	VLE INTEROPERABILITY	Test	<a href="#">Delete</a>
<a href="#">KMIPVTCONLY</a>	KMIP	VTC ONLY	Test	<a href="#">Delete</a>

**Storage Admin**

**Volume**

EDIT MODE ACTIVE

You have to click the **Save** button to commit your changes to the Domain Manager.

**Key Manager Information**

Key Manager ID\*

Server Type\*

Client Type\*

ESKM Local Group  Required when there are any VTC Clients defined.

- Select the Add link from the VLE-CLIM Client Information section and:
  - Select a CLIM ID proposed in the drop down box.
  - Click on the ADD VLE-CLIM Client button. The selected entry will appear in a CLIM ID table below the button.
  - Repeat for each entry, as needed

**VLE-CLIM Client Information** [Hide](#)

CLIM ID\*

		CLIM ID*
<a href="#">Edit</a>	<a href="#">Delete</a>	\ETINIUM S100231

# NON-VLE CONFIGURATION

In this setup, the VTC is a client to the Key Manager. To be authenticated by the KeyManager, the VTC presents an account, a password, and a digital certificate signed by a Certificates Authority (most of the time a local one.)

For security reasons, tasks related to the generation, installation and configuration of certificate and authentication elements should be restricted to a Security Authority user.

Since there are many ways to generate a digital certificate and each of them may require specific certificate fields entries depending on Key Manager server used or enterprise security policies restrictions, following procedure would focus on IN and OUT needed to be produced and which one (role) should accomplish it. Method describes to produce requirements should be taken as guidelines and adapted to enterprise reality.

## Key Manager Configuration

- VT Controller (VTC) who will be used as client must be identified. Each VTC should be licensed for encryption support (Security Authority user role)
- Supplemental client licenses (1 per VTC identify) should be provisioned at the Key Manager server (KM Administrator role)
- A username with his password (1 per VTC identify) should be create according to the enterprise policy (KM Administrator role.) The VT Controller ID can be a good candidate for username
- All VTC's "username" should be configured as a group on the key manager server (KM Administrator role) and allow to:
  - Be able to request key generation
  - Be able to access key owned by VTC group member
  - Be able to delete key owned by VTC group member (if key deletion automation will be enabled for SCRATCH media)



If Key manager server type is ESKM and VTC Client are not intent to be used in collaboration with VLE, a local group named BackBox should be created and VTC's username added to it. If VTC Client are intent to be used in interoperability with VLE for tape, VTC's username should be added to same local group than CLIM (normally local group NonStop).

**IMPORTANT:** For Client Type VTC ONLY, the ESKM Local Group BackBox is only default suggestion and must be override by the group name configure in the ESKM server configuration else key will not be generated and access denied will be logged in the ESKM audit logs.

## VTC Configuration

- For a VTC digital certificate generation activity (for each VTC identified by the Third-Party Security Authority user role):
  - Generate a private key (normally an RSA key) for the Key Manager communication channel according to enterprise security policy (key length 1024 or 2048, passphrase).
  - Generate a certificate request with certificate fields set according to enterprise security policy and Key Manager server specific data (the username needs to be specified in the Common Name field or in another specific certificate field, in the Client IPaddress).
  - Submit the request certificate which is to be signed by the Key Manager Server local Certificate Authority (KM Administrator role).
  - Install the signed certificate file (must be named ClientCert.pem), the private key file (must be named ClientKey.pem), and the Local CA certificate (must be named CACert.pem) to authenticate the Key Manager server, into a specific folder on the local disk of the VTC. Access to these 3 files and to the folder should be restricted to only the Third Party Security Authority user and VTC services (LOCAL SERVICE account).  
Note: The 3 files must be in PEM format.
  - Keep and save (required for BackBox configuration):
    - The Key Manager VTC username.
    - The Key Manager VTC username password.
    - The ClientKey.pem passphrase.
    - The 3 file folder locations.

## Generate RSA Key and Certificate Request

Here is an example that can be adapted to the Key Manager server requirement and to the enterprise security policies. It will use openssl to generate a 1024-bit RSA key and a certificate request with a username in the Common Name field as a Key Manager ESKM requirement.

- 1- Download and install an openssl distribution package.
- 2- From a command console: `c:\OpenSSL-Win64\bin>openssl req -newkey rsa:1024 -keyout ClientKey.pem -out REQ-ClientCert.pem`

Loading 'screen' into random

state - done Generating a 1024-

bit RSA private key

..... ++++++

..... ++++++

Writing new private key to

'ClientKey.pem' Enter PEM pass

phrase:

Verifying - Enter PEM pass phrase:

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank

For some fields there will be a default value, If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:.

State or Province Name (full name)

[Some-State]:. Locality Name (E.g. city)

[:].

Organization Name (E.g. company) [Internet Widgets Pty Ltd]:.

Organizational Unit Name (E.g. section) [:].

Common Name (E.g. YOUR name)

[:BBOX1 Email Address [:].

Please enter the following 'extra' attributes to be sent with your certificate request

A challenge password [:].

An optional company name [:].

c:\OpenSSL-Win64\bin>

Please enter the following 'extra' attributes to be sent with your certificate request

A challenge password [:].

An optional  
company name []:  
c:\OpenSSL\bin>

## Sign Client Certificate and CA Certificate

- 3- Now that the private key has been generated, a certificate request needs to be sent. Once issued, the certificate has to be signed against a CA. Use a local CA installed on the Key Manager Server. In the command window, display the file containing the certificate request as follows:

```
c:\OpenSSL-Win64\bin>type REQ-ClientCert.pem
-----BEGIN CERTIFICATE REQUEST-----
MIIBTzCBuQIBADAQMq4wDAYDVQQDDAVCQk9YMTCBnzANBgkqhkiG9w0B
AQEFAAOB
jQAwwYkCgYEAWjT4SMRTJyMy2sMt4tn4t+1qurnpru99L4OHZknE6zw0akTkYEmV
YISYvKAt2nRVVejYYGul2VAisHiF6YkivRQi6nblVNC02fn8B2Zh6BGGeNzszWRN
ofpJ00q7505Ig3Rw9bqmV6wRICuN4kl0zW5Zxx25st+5uQ11xMzJzUCAwEAAaAA
MA0GCSqGSIb3DQEBBQUAA4GBAGkDaoqzBn65p3sebRDxR8zuh7T2eeuDY49/JASr
gvM7453rzrjfsx8mEdW8m7x2z6yWvwMMmUcxlDXm869sGIYAnaqK5oWsaYt+Tjj
9TvyUpQePnOfufiwj3+NznHhw0eMjygEQj6AWjPz4EeE6cGjDAmK6q5qm6JfJ2ac Oq3P
-----END CERTIFICATE REQUEST-----

c:\OpenSSL-Win64\bin>
```

- 4- Sign the certificate.
- Select and copy the Client certificate request text from -----BEGIN CERTIFICATE REQUEST--- -- through ---- END CERTIFICATE REQUEST ----.
  - Sign Client certificate request with the local CA:
    - Log onto the Enterprise Secure Key Manager UI as admin. On the Security tab, select Local CAs.
    - Select the trusted local CA and click Sign Request:

## Certificate and CA Configuration

**Local Certificate Authority List**
Help

CA Name	CA Information	CA Status
<input checked="" type="radio"/> <a href="#">atlab</a>	Common: atlab Issuer: atlab Expires: Oct 24 21:37:18 2019 GMT	CA Certificate Active

Edit
Delete
Download
Properties
Sign Request

Show Signed Certs

- Select Client as Certificate Purpose. Paste the copied certificate request into the Certificate Request box.

# Certificate and CA Configuration

**Sign Certificate Request**Help

---

**Sign with Certificate Authority:** atlab (maximum 2837 days) ▼

---

**Certificate Purpose:**

Server

Client

---

**Certificate Duration (days):** 100

---

**Certificate Request:**

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBTzCBuQIBADAQMq4wDAYDVQQDDAVCQk9YMTCBnzANBgkqhkiG9w0BAQEFAAOB
jQAwgYkCgYEAwjT4SMRtJyMy2sMt4tn4t+1qurnpru99L4OHZknE6zwOakTkyEmV
YISYvKAt2nRVVeJYYGuI2VAisHiF6YkivRQi6nb1VNC02fn8B2Zh6BGeNzszWRN
ofpJ00q7505Ig3Rw9bqmV6wRICuN4k1OzW5Zxx25st+5uQ11xMzJz1UCAwEAAA
MA0GCSqGSIb3DQEBBQUAA4GBAGkDaoqzBn65p3sebRDxR8zuh7T2eeuDY49/JASr
gvM74S3rzrjfjsx8mEdW8m7x2z6yWvwMMmUcx1DXm869sGIYAnaqK5oWsaYt+Tjj
9TvyUpQePnOfufIwj3+NznHhw0eMjygeQj6AWjPz4EeE6cGjDAmK6q5qm6JfJ2ac
Oq3P
-----END CERTIFICATE REQUEST-----|
```

---

Sign Request Back

- d. Click Sign Request. The Key Manager signs the Client certificate request with the Local CA and displays the signed Client certificate:

# Certificate and CA Configuration

## CA Certificate Information

Help ?

<b>Key Size:</b>	1024
<b>Start Date:</b>	Jan 16 18:57:35 2012 GMT
<b>Expiration:</b>	Apr 26 18:57:35 2012 GMT
<b>Issuer:</b>	C: US ST: ca L: cupertino O: atlab OU: atlab CN: atlab
<b>Subject:</b>	CN: BBOX1

-----BEGIN CERTIFICATE-----

```
MIICqDCCA2CgAwIBAgIBNjANBgkqhkiG9w0BAQUFADCBgDELMAkGA1UEBhMCVVMx
CzAJBgNVBAGTAMNhMRlWYAYDVQQLHEw1jdXB1cnRpbm8xDjAMBGNVBAoTBWFObGFi
MQ4wDAYDVQQLEwVhdGxhYjEOMAwGA1UEAxMFYXRyYWIxIDAeBgkqhkiG9w0BCQEW
EWhpZ3V5Z3V5ZW5AaHauY29tMB4XDTEyMDExNjE4NTczNVoXDTEyMDQyNjE4NTcz
NVowEDEOMAwGA1UEAwwFQkJPWDEwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGB
AMI0+EjEbScjMtrDLZ+Lftarq56a7vfS+Dh2ZJxOs8DmpE5GBJlWCEmLygLXtp
0VVXo2GBriN1QIrB4hemJIr0UIup25VTQtNn5/AdmYegRnjc7M1kTaH6STtKu+Tu
SIN0cPW6plesESArjeJTTs1uWccubLfubkNdcTMyC5VAgMBAAGjIDAEMAkGA1Ud
EwQCMAAwEQYJYIZIAAYb4QgEBBAQDAgeAMA0GCSqGSIb3DQEBBQUAA4IBAQAByKSS
wslJmcPG7mPIImThBio708IbWf1gC4JiRsr16SL7ujEu5JSdWTwiqrIO1AEzH2fZd
v/0+lx8aAKNu2SrcCckzoo8LzzzQtRsiS1LzSxxKCxflwmuxrgzaGvviMpb1aXJ9
zHioCjciIfRyfgfQqo53nLDJve+AlzzSKzW9cDUL1UW6cGpOuYQnqklsNbYW0YQw
7Rfn1SAK8d3CMIAIMAMBZaEYXhmo72BsV00Q9IPyvcNULW0umj9gHaEiv21w5oj
/KBoTBPQRagCPDBQ8K2joc3gLKt18ra7CeJyAyAT0tQiNi9wV+qGrNX0yvFiYWji2
OiU9TKmbPI5nbvm8
```

-----END CERTIFICATE-----

Download

Back

- C) Select and copy the signed Client Certificate text from -----BEGIN CERTIFICATE ----- through -----END CERTIFICATE ----- (Or use download).
1. Create a file named ClientCert.pem and paste the signed certificate containing ..... (or rename the downloaded file).
2. Download the CA certificate and name the file CACert.pem.
3. Move the 3 files: ClientKey.pem, ClientCert.pem and CACert.pem to the designated TSL configuration file locations.
4. The file REQ-ClientCert.pem can be deleted.

## Add the Key Manager in the BackBox Configuration


This activity should be accomplished by the (Third Party) Security Authority user. The Security Authority user should have a NonStop user account with enough privilege to modify the BackBox Domain configuration. Log on to the BackBox UI interface.

- Select the Configuration menu and select the Switch to Edit mode.
- Select the Key Manager tab.
- Select the targeted Key Manager ID. If the Key Manager entity doesn't exist, you will need to create one first. Click on the Create Key Manager button and fill in Key Manager information:
  - Choose an alias name and type it in the Key Manager ID file.
  - Set the Server Type in accordance with the Key Manager model. (ESKM or KMIP).
  - Set the Client Type according to Client connectivity purpose and Key Manager model. For Server Type



ESKM, the Client type can be either VTC ONLY or VLE INTEROPERABILITY. For Server Type KMIP, Client Type: VTC ONLY.

- Enter the Key Manager IP port where the VTC Client can reach the server (KMIP only).
- Add all IP Addresses that the VTC Client can use to reach the server. If a connection fails using the first address, the VTC Client will attempt to connect using the next one, until the list is exhausted (KMIP only).



Some Key Manager servers, work in cluster mode. IP addresses of each member of the cluster can be added to the list.

- When Client Type is VTC ONLY, the optional check box Delete old key id is available. This optional field enable/disable automation of deletion of encryption key when data expired.
- When Server Type is ESKM, a supplemental field must be provided (ESKM Local Group.) Enter the Local Group name that the VTC Client is part of. Depending on the Client Type value set, the field will be set with a default name to NonStop (VLE INTEROPERABILITY) to be able to work with NonStop VLE. The value entered could be changed if other group names are used instead of a default name.

Key Manager ID	Server Type	Client Type		
<a href="#">ESKMVTCONLY</a>	ESKM	VLE INTEROPERABILITY	<a href="#">Test</a>	<a href="#">Delete</a>
<a href="#">KMIPVTCONLY</a>	KMIP	VTC ONLY	<a href="#">Test</a>	<a href="#">Delete</a>

**Key Manager Information**

Key Manager ID\*

Server Type\*

Client Type\*

ESKM Local Group  Required when there are any VTC Clients defined.

ESKM VLE Key Manager Information

Key Manager ID	Server Type	Client Type		
<a href="#">ESKMVTCONLY</a>	ESKM	VLE INTEROPERABILITY	<a href="#">Test</a>	<a href="#">Delete</a>
<a href="#">KMIPVTCONLY</a>	KMIP	VTC ONLY	<a href="#">Test</a>	<a href="#">Delete</a>

**Key Manager Information**

Key Manager ID\*

Server Type\*

Client Type\*   Delete old key

ESKM Local Group  Required when there are any VTC Clients defined.

ESKM VTC ONLY Key Manager Information

**Key Manager Information**

Key Manager ID\*

Server Type\*

Client Type\*   Delete old key

Key Manager IP Port  Required when there are any VTC Clients defined.

**Key Manager IP List**

IP Address   Required when there are any VTC Clients defined

		IP Address
<a href="#">Edit</a>	<a href="#">Delete</a>	192.168.21.31

KMIP VTC ONLY Key Manager Information

## Add VTC Client Information in the BackBox Key Manager



You need to have configured Data Store WINDISK with VTC Route to be able to add VTC Client in the Key Manager Configuration.

- ESKM VTC Client (VTC ONLY or VLE INTEROPERABILITY)

**VTC Client Information** [Hide](#)

VT Controller ID\*

User ID

User Password  Confirm

ESKM Configuration File

Switch to **Edit Mode** and select the **Add** link from the VTC Client Information section and:

- Select a VT Controller ID in the drop-down list.
- Attention: Check the displayed number of Encryption Devices: a VTC must be licensed for at least one encryption device to be functional.
- Enter the User ID to be used by the VTC to log in to the Key Manager.
- Key Manage Configuration Info, such as IP address and Port number of the Key Manager) need to be defined inside the ESKM Configuration File
- Repeat for all other VTC Clients that need to be attached to the Key Manager ID.
- Click on the Save configuration when done.

User can define the parameters for the communication between the client and the Key Manager server in the ESKM Configuration File `IngrianNAE`. See the properties below:

#### ESKM Configuration File

```
#
# NOTE: Do not use quotes when specifying values in
this file. #

#[Version]
# Version of the properties file for the Ingrian
PKCS#11/ICAPI/MSCAPI/.NET # providers.
#
# Do not modify this
property. #
Version=2.4

#[Network
Configuration] #
[NAE Server IP]
# The IP address and port of the NAE
server. #
# Multiple IPs can be specified when load balancing is used. The
port must # be the same on all NAE servers. You can configure up
to three tiers of
# NAE servers. Tiers are numbered 1-3. If all servers in the primary
tier 1 # become unreachable, the client will switch to tier 2. If all
servers
# in tier 2 become unreachable, the client will switch to tier
3. When # using an alternate tier, the client will periodically
try to switch
# back to tier 1 (after Connection_Retry_Interval has
expired). #
# For all tier-aware parameters, the tier is indicated with a
trailing # .n after the parameter name, i.e.
NAE_IP.1=127.0.0.1
# Setting the parameter with no tier sets the default value for all
tiers. # i.e. Connection_Timeout=600000 sets Connection_Timeout for
all tiers while # Connection_Timeout.1=700000 sets
Connection_Timeout for tier 1.
# A tier-specific setting will
override #
# For NAE_IP, IPs are separated by
colons, e.g., #
192.168.1.10:192.168.1.11:192.168.1.12
#
```

NAE\_IP=63.80.93.150

```
##[Network
Configuration] #
[NAE Server Port]
# NAE_Port is tier-aware
# Do not set the port value to 9443 because this is the port
typically used # to connect to the management console.
NAE_Port=9000
```

```
#[Network
Configuration] #
[Protocol]
# The protocol used between the client and the NAE
server. #
# If you are load balancing across multiple NAE servers, the
protocol must # be the same for each server.
# Protocol is
tier-aware. #
# Valid values:
tcp, ssl. #
Default: tcp
#
Recommend
d: ssl #
Protocol=tcp
```

```
#[Connection
Configuration] #
[Persistent
Connections]
# Enable or disable persistent
connections. #
# If enabled, the client will use a pool of persistent connections
to the # NAE server. If disabled, a new connection will be created
and then
# closed for each
request. #
# Valid values:
yes, no. #
Default: yes
#
Recommend
d: yes #
Use_Persistent_Connections=yes
```

```
#[Connection
Configuration] #
[Connection Pooling]
# The maximum number of connections in the persistent
connection pool. #
# This value is used only when persistent connections are
enabled. # Size_of_Connection_Pool is tier-aware.
#
#
Default
: 300 #
Size_of_Connection_Pool=300
```

```
#[Connection
Configuration] #
[Connection Timeout]
# The timeout when connecting to the NAE
server. #
# The timeout is specified in milliseconds. The client will wait
for the # specified number of milliseconds when trying to
connect to each NAE
#
#
# Setting this value to 0 uses the system connect()
timeout. #
# Caution: Setting this value too low may cause connections to
fail when # the NAE servers and/or network are under load. Do
```

```

not change it unless # you really need to.
# Connection_Timeout is
tier-aware. #
#
Default:
60000 #
Connection_Timeout=60000

#[Connection
Configuration] #
[Connection Idle
Timeout]
# The time a connection is allowed to be idle in the
connection pool # before it gets closed automatically by the
client.
#
# The timeout is specified in milliseconds. The client will check
how long # each connection has been idle for. If the time has
passed the value
# specified here, the client will close the connection and remove
it from # the connection pool. To be effective, this setting must
be less than the # Connection Timeout setting in the NAE Server
Settings section in the
# Management Console of the NAE
server. #
# Setting this value to 0 is equivalent to an infinite
timeout. # Connection_Idle_Timeout is tier-aware.
#
# Default:
600000 #
Connection_Idle_Timeout=60

0000 #[Connection

Configuration]

# [Connection Retry]
# The amount of time to wait before trying to reconnect to a
disabled # server.
#
# The retry interval is specified in milliseconds. If one of the NAE
# servers in a load balanced configuration is not reachable,
the client # will disable this server, and then wait for the
specified number of # milliseconds before trying to connect to
it again.
#
# Setting this value to 0 is equivalent to an infinite retry
interval # (meaning the disabled server will never be brought
back into use). # Connection_Retry_Interval is tier-aware.
#
# Default:
600000 #
Connection_Retry_Interval=600000

#[Connection
Configuration] #
[Unreachable Server
Retry]
# The amount of time to try establishing a connection if all
servers # in the pool become unreachable.
#
# The retry period is specified in milliseconds. An error is returned
# after the specified period if no server in the pool becomes
reachable. # If logging is enabled, error messages will be
logged to the log file. #
# Setting this value to -1 is equivalent to an infinite retry
period. The # client will keep trying to connect to a server in
the current tier
# until a connection is
established. #
# Setting this value to -1 is not compatible with multi-tier load
# balancing because the load balancer will never switch to the
secondary # or tertiary pools. If multi-tier load balancing is
enabled (i.e., if # NAE_IP[2] is set to one or more IP
addresses) then set this value

```

```

# to a number between one and two times the
Connection_Retry_Interval. #
# Unreachable_Server_Retry_Period is
tier-aware. #
#
Default
:60000 #
Unreachable_Server_Retry_Period=60000

#[Connection Configuration]
# [Maximum_Server_Retry_Period]
# The total amount of time to spend trying to make connections on
all tiers. # This value only has meaning when using multi-tiered
load balancing.
#
# If this value is set to -1 (try forever), the connection manager
will try # every server on every tier continually, until one
answers.
#
# If set to 0, it is
disabled. #
# If this value is enabled, the connection manager will try to make
connections # for at least Maximum_Server_Retry_Period milliseconds but
will return
# an error if no connection can be made on the tier in
use when # Maximum_Server_Retry_Period expires.
#
# In all cases, the Unreachable_Server_Retry_Period for a given
tier must # expire before the connection manager switches to the
next tier.
#
# Default: 0
(disabled) #
Maximum_Server_Retry_Period=0

#[Connection Configuration]
# [Cluster_Synchronization_Delay]
# The total amount of time to spend trying to make requests
on keys # go to the same device the key create or latest key
modify went to. #
# A device tries to replicate key information to other
devices in the # cluster after it completes a key create or
modify request. Until # that replication completes, requests
on the key need to go to the

# device pushing the
replication. #
# If replication fails, the device waits for 30 seconds, then
# tries again. If three replications fail, the device stops
trying # to replicate data.
#
# The default is 100 seconds: 3 times 30 seconds plus a few extra
# seconds per try for network latency. For larger clusters
additional # time may be needed.
#
# Disable the function: 0
seconds #
# Default: 100
seconds #
Cluster_Synchronization_Delay=100

#[Connection
Configuration] #
[EdgeSecure Name]
# Name of device or file containing the name of an EdgeSecure
device. #
# The name of an EdgeSecure device is a unique value
assigned # by the administrator to define a single
device.
#
# If the name refers to a readable file, then the first line in
the file # defines the name of an EdgeSecure device. This
allows all properties # files stored on different platforms to
be the same and still allow
# each platform to refer to a different EdgeSecure
device. #
#
Default
: none #

```

#EdgeSecure\_Name=

```
#[SSL/TLS
Configuration] #
[Cipherspec]
# The SSL/TLS protocol and encryption algorithms
to use. #
# Default is "HIGH:!ADH:!DH:!DSA:!EXPORT:RSA+RC4:RSA+3DES:RSA+AES"
# which translates to high-strength RSA key exchange and RC4,
triple DES, # or AES.
# Cipher_Spec is
tier-aware. #
# Default:
HIGH:!ADH:!DH:!DSA:!EXPORT:RSA+RC4:RSA+3DES:RSA+AES #
#Cipher_Spec=HIGH:!ADH:!DH:!DSA:!EXPORT:RSA+RC4:RSA+3DE
S:RSA+AES
```

```
#[SSL/TLS Configuration]
# [CA Certificate for Server Authentication]
# The CA certificate that signed the NAE server certificate
presented to # clients to establish SSL connections.
#
# If you are using SSL between the client and server, you must
specify a # path to the CA certificate that signed the NAE
server certificate. If # the client cannot validate the
certificate presented by the NAE server,
# the client will not be able to establish an SSL connection with
the NAE # server.
#
# You should provide the path and file name of the CA
certificate. The # path can be absolute or relative to the
application. Do not use quotes # when specifying the path, even
if it contains spaces.
# CA_File is
tier-aware. #
# No
defau
lt. #
CA_File=
```

```
#[SSL/TLS
Configuration] #
[Client
Certificate]
# The client certificate to present to the NAE
server. #
# This value is required when client certificate authentication is
enabled # on the NAE server. The certificate must be in PEM
format. If this value # is set, the certificate and private key
must be present even if the NAE # server is not configured to
request a client certificate.
#
# You should provide the path and file name of the client
certificate. The # path can be absolute or relative to the
application. Do not use quotes
# when specifying the path, even if it contains
spaces. # Cert_File is tier-aware.
#
# No
defau
lt. #
Cert_File=
```

```
#[SSL/TLS
Configuration] #
[Client Private
Key]
# The private key associated with the client certificate
specified in # Cert_File.
#
# This value is required when client certificate authentication is
enabled # on the NAE server. The client private key must be in
PEM-encoded PKCS#12 # format. If this value is set, a correctly
formatted key and certificate # must be present.
#
```

```

# You should provide the path and file name of the private key.
The path # can be absolute or relative to the application. Do
not use quotes when # specifying the path, even if it contains
spaces.
# Key_File is
tier-aware. #
# No
defau
lt. #
Key_File=

#[SSL/TLS Configuration]
# [Client Private Key Passphrase]
# The passphrase to unlock the client private key specified in
Key_File. #
# This value is required when client certificate authentication is
enabled # on the NAE server. Since the value is in the clear, this
properties file # must have its permission restricted so that it
can be read only by the
# applications that are to have legitimate
access to it. # Passphrase is tier-aware.
#
# No
defau
lt. #
Passphrase=

#[Logging
Configuration] #
[Log Level]
# The level of logging that will be performed by the
client. #
# The log level determines how verbose your client logs are. You can
# disable logging by selecting NONE; however, it is recommended
that you # set the log level to MEDIUM. A log level of HIGH can
create a very large # log file. Set the log level to HIGH to
troubleshoot configuration
#
prob
lems
. #
# Valid values:
#     NONE      - nothing is logged
#     LOW       - only essential events are
logged #     MEDIUM  - some events
are logged
#     HIGH      - many events are
logged #
# Default:
MEDIUM #
Log_Level=MEDIUM

#[logging
configuration] #
[log file]
# the location of the log file the client will
create. #
# you should provide the path and file name of the log file. the
path can # be absolute or relative to the application. do not use
quotes when
# specifying the path, even if it contains
spaces. #
# default: logfile (created in the current
directory) #
Log_File=logfile

#[Logging
Configuration] #
[Log Rotation]
# The log rotation
method. #
# This value specifies how frequently the log file is
rotated. #
# Valid values:
#     Daily     - log file is rotated once a day
#     Size      - log file is rotated when it exceeds

```

```

Log_Size_Limit #
#
Default:
Daily #
Log_Rotation=Daily

#[Logging
Configuration] #
[Log Size]
# The maximum log
file size. #
# If Log_Rotation=Size, the log will be rotated after it
reaches the # specified size. This value is only used when
Log_Rotation=Size.
#
# The size may be specified in bytes, kilobytes (using 'k' or
'K'), or # megabytes (using 'm' or 'M'). One kilobyte is 1024
bytes, and one
# megabyte is 1048576
bytes. #
#
Default
: 100k #
Log_Size_Limit=100k

```

## KMIP VTC Client

Switch to **Edit Mode** and select the **Add** link from the VTC Client Information section and:

- Select a VT Controller ID in the drop-down list.
- **Attention:** Check the displayed number of Encryption Devices: a VTC must be licensed for at least one encryption device to be functional.
- Enter the User ID to be used by the VTC to log in to the Key Manager.
- Enter the Password to be used by the VTC to log in to the Key Manager.
- Enter the Key Pass-phrase required by the VTC to access the private key for the TLS/SSL communication channel with the Key Manager.
- Enter the TLS Configuration File Locations where the digital certificate and private key have been installed. (ClientCert.pem, ClientKey.pem and CACert.pem).
- Repeat for all other VTC Clients that need to be attached to the Key Manager ID.
- Click on the Save configuration when done.

## Encryption in a Volume Group

**Attention:** Toggling encryption ON and OFF affects subsequent usage of the virtual volume member of the Volume Group. To avoid disabling the tape encryption by mistake it is recommended that the number of users who can update the BackBox configuration be kept to a minimum.

**Attention:** Encrypting data will protect the data from external system access, but it will not protect the access to media from a tape application running in the NonStop. If user segregation needs to be carried out, Control Access from the Volume Group with advanced attributes should be enabled.

Log on to the BackBox UI interface.

- Select the Configuration menu and select the Switch to Edit mode.
- Select the Volume Group tab.
- Select or Create a Volume Group ID.
- In the Class Information:
  - Select the AES-GCM-256 in the Encryption Algorithm drop down list box.



- Select the target Key Manager ID from its drop down list box.

Guardian Node Owner\*

Guardian User ID Owner\*

Encryption Algorithm

Key Manager ID

Comment

- If the setup is for VLE, the Volume Group Media Type must be LTO 4.

**Important:** If you already have a Volume Group that you have been using and want to encrypt the content on its media from now on using VLE-CLIM Client, you can simply modify its Media Type to LTO 4.

From that point on, all new uses of SCRATCH volumes in the Volume Group (such as for new backups) will mount as LTO 4 media to be encrypted. Existing ASSIGNED media will also be mounted as LTO 4 and be read by NonStop applications, such as RESTORE, even if not encrypted. If the Volume Group uses the DSM/TC tape catalog, the following MEDIACOM command must be performed on the Pool associated with that Volume Group:

```
MEDIACOM
>ALTER POOL vt-pool-name, TYPE ANY
>ALTER TAPEVOLUME *, POOL vt-pool-name, TYPE LTO 4
```

- Click on the Update Volume Group button at the very bottom of the page.
- Repeat for other required Volume Groups.
- Click on the Save link.

## Test BackBox Software Encryption Configuration

Good Practice: Validate encryption configuration before trying to do the real encryption. For a Key Manager ID, the overall configuration and the connectivity to the key server is verified by clicking the Test link on the Configuration Key Manager page.

Status	Domain	NSK Nodes	VT Controller	Key Manager	Data Store	Volume Group															
<p><b>Configuration</b></p> <p>Save Cancel</p> <p><b>Storage Admin</b></p> <p><b>Volume</b></p> <p><b>EDIT MODE ACTIVE</b></p> <p>You have to click the Save button to commit your changes to the Domain Manager.</p>																					
<p>Select, Delete or Create a Key Manager</p> <p>Create Key Manager</p> <p>W3162 Domain license will expire on 2024-01-22.</p> <table border="1"> <thead> <tr> <th>Key Manager ID</th> <th>Server Type</th> <th>Client Type</th> <th></th> <th></th> </tr> </thead> <tbody> <tr> <td><a href="#">ESKMVTCONLY</a></td> <td>ESKM</td> <td>VLE INTEROPERABILITY</td> <td>Test</td> <td><a href="#">Delete</a></td> </tr> <tr> <td><a href="#">KMIPVTCONLY</a></td> <td>KMIP</td> <td>VTC ONLY</td> <td>Test</td> <td><a href="#">Delete</a></td> </tr> </tbody> </table>							Key Manager ID	Server Type	Client Type			<a href="#">ESKMVTCONLY</a>	ESKM	VLE INTEROPERABILITY	Test	<a href="#">Delete</a>	<a href="#">KMIPVTCONLY</a>	KMIP	VTC ONLY	Test	<a href="#">Delete</a>
Key Manager ID	Server Type	Client Type																			
<a href="#">ESKMVTCONLY</a>	ESKM	VLE INTEROPERABILITY	Test	<a href="#">Delete</a>																	
<a href="#">KMIPVTCONLY</a>	KMIP	VTC ONLY	Test	<a href="#">Delete</a>																	

# USER INTERFACE CONFIGURATION

## VT Controller

Virtual Devices

Add Devices Automatically    Add Devices Manually

Guardian Node\*

VTC Port\*

Guardian Device\*

	Node	Guardian Device	Device Type	Serial Number	Port	Target	Lun	VLE	Explicit Only	Reserved For	Host WWN	Status	Guardian Port	
<a href="#">Edit</a>	<a href="#">Delete</a>	VETINIUM	\$TOUT01	LTO4	BB04AF6600	FC-21	0	0	VLE	False	...	50014380331312E8	FREE	\$ZZSTO.#S100231

## Key Manager

The Key Manager is an external server generating and storing encryption keys; the encryption itself being processed in the BackBox VTC for all configuration types.

The Key Manager must be configured even for VLE Encryption.

- For VLE, the Key Manager configuration is used to control the encryption configuration during Operations and to clearly identify the key server storing the encryption keys.
- For non-VLE Encryption, the Key Manager configuration is also used to identify and secure a network path to the key server.

It is possible to configure more than one Key Manager instance, each describing the server holding the encryption keys for different groups of tape volumes.

Domain    NSK Nodes    VT Controller    **Key Manager**    Data Store    Volume Group

W3162 Domain license will expire on 2024-01-22.

Key Manager ID	Server Type	Client Type		
<a href="#">ESKMVTCONLY</a>	ESKM	VLE INTEROPERABILITY	Test	<a href="#">Delete</a>
<a href="#">KMIPVTCONLY</a>	KMIP	VTC ONLY	Test	<a href="#">Delete</a>

Status

Domain    NSK Nodes    VT Controller    **Key Manager**    Data Store    Volume Group

Configuration

Storage Admin

Volume

EDIT MODE ACTIVE

You have to click the Save button to commit your changes to the Domain Manager.

Key Manager Information

Key Manager ID\*

Server Type\*

Client Type\*   Delete old key

Key Manager IP Port:  Required when there are any VTC Clients defined.

Key Manager IP List

IP Address:   Required when there are any VTC Clients defined

	IP Address	
<a href="#">Edit</a>	<a href="#">Delete</a>	192.168.21.31

VTC Client Information [Hide](#)

VT Controller ID\*

User ID

User Password  Confirm\*

Key Pass-Phrase  Confirm\*

KMIP Client Certificate File

CA Certificate File

Private Key File

	VT Controller ID*	User ID	Password	Key Passphrase	KMIP Client Certificate File	KMIP VTC Private Key File	KMIP CA Certificate File
<a href="#">Edit</a>	<a href="#">Delete</a>	VTC_MONTREAL	toutatis	*****	D:\Cert\veskma.pem	D:\Cert\toutatis.pem	D:\Cert\toutatis.pem

## ESKM only

- ESKM Configuration File – Path to the NAE properties configuration file that defined Certificate, CA, Private KEY and Pass-phrase.

## KMIP only

- Key Pass-Phrase - Enter the key passphrase for the private key file and confirm it by re-entering it in the field
- KMIP Client Certificate File – Certificate file used to establish the SSL connection and the Key Manager server (refer to your IT support team to have the file generated)
- CA Certificate File – Enter the CA Certificate File
- Private Key File – Private key file used for the SSL connection between the client and the Key Manager server.

Click [Add Key Manager Client](#) button at the bottom of the page to finish up the Key manager setting up. Details on the Key Manager setting will be displayed in a table like the one below.

	VT Controller ID*	User ID	Password	Key Passphrase	KMIP Client Certificate File	KMIP VTC Private Key File	KMIP CA Certificate File
<a href="#">Edit</a> <a href="#">Delete</a>	VTC_MONTREAL	toutatis	*****	*****	D:\Cert\eskmca.pem	D:\Cert\toutatis.pem	D:\Cert\toutatis.pem

## Key Manager – VLE CLIM Clients

When the Encryption keys are managed by the Storage CLIMs for VLE processing, the CLIMs hosting the LTO 4 virtual tape drives must be identified as Clients of the Key Manager in order to identify which Key Manager holds the Encryption key of each volume. The current list of VLE CLIM Clients is presented on the Key Manager page. New CLIMs can be added by clicking on the button Add VLE-CLIM Client.

VLE-CLIM Client Information [Hide](#)

CLIM ID\*

[Add VLE-CLIM Client](#)

	CLIM ID*
<a href="#">Edit</a> <a href="#">Delete</a>	\ETINIUM S100231

**CLIM ID:** Select a CLIM in the selection list. The selection list is based on information queried from the host during the VTC configuration of tape drives in the BackBox Domain. The list of proposed CLIMs is limited to those associated with a tape drive of the BackBox Domain, defined as LTO 4, and enabled for VLE by SCF.

If the proposed list is empty or unexpected, check that the tape devices are enabled for VLE in SCF, and refresh the host information in the VTC configuration page of the involved VTCs by the link Update devices based on the probe result from the VTC and all hosts.

The Key Manager connectivity should be tested before testing actual virtual tape Encryption, in any case of Encryption setup – including HPE VLE.

The Key Manager page is shown in the list of configured Key Managers, and the [Test](#) link is available when the Configuration tab is in the Browse mode.

The Test will execute several verifications and show the resulting report in a new window.

- The connectivity of all VTC Clients to the Key Manager, will be tested by a query to the Key Manager for its identification and for each of the IP addresses configured for the Key Manager.
- All VTCs in the domain having LTO 4 devices, will be tested to check if the LTO 4 devices are connected to a CLIM recognized as a VLE CLIM Client to the Key Manager.
- The LTO 4 drives must be started to allow BackBox to check the host WWN and compare it to the VLE CLIM Client configuration. If there is a match, the connectivity to the Key Manager from the CLIM will be assumed.
- The domain configuration will then be analyzed to:
  - Detect the Volume Groups using the Key Manager ID.
  - Verify that the VTC routed to the corresponding Data Stores, have the connectivity to the Key Manager.
  - Verify that the VTCs have the Encryption license option for at least one drive.

### Key Manager – Test Report

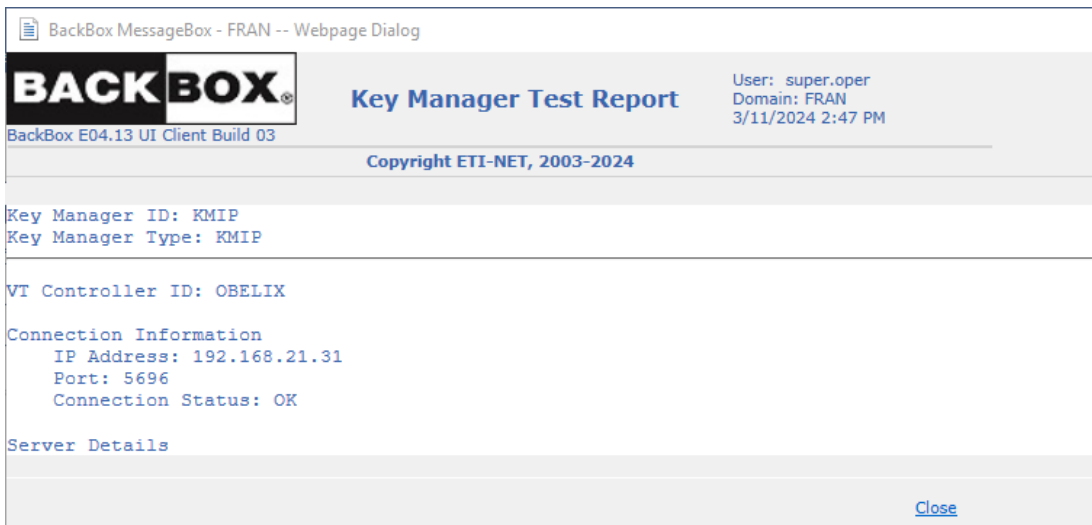
Only those VTCs that actually receive messages, will be shown in the Key Manager Test Report. For each VTC, there can be three sections:

- A section VTC Client showing the report generated by the VTC.
- The report is **green** for success, **orange** for any warning not preventing connectivity, and **red** for a complete lack of connectivity.
- A section VLE-CLIM Client showing a report of counts of FC LTO 4 drives per port and connected host WWN. The report is green for success, orange if no LTO 4 drive is currently connected to a recognized CLIM, and **red** for a complete lack of connectivity.

- A list of messages pertaining to the VTC.

The messages are explained in the [BackBox Messages Manual and Troubleshooting](#)

Three Test report samples are presented after the common underlying VTC configuration below, with each sample showing its specific Key Manager configuration page and the associated Test report page:



## Volume Group

### Encryption

For all setups, the Encryption must be enabled in the Class Information

- Select the AES-GCM-256 in the Encryption Algorithm drop down list box.
- Select the target Key Manager ID from its drop down list box.

Guardian Node Owner*	<input type="text" value="\CGNAC2"/>
Guardian User ID Owner*	<input type="text" value="255,144"/>
Encryption Algorithm	<input type="text" value="AES-GCM-256"/>
Key Manager ID	<input type="text" value="KMVLE"/>
Comment	<input type="text"/>

A change in this setup will affect further backups, not the restore of backups already written.

If the catalogs (BackBox, DSM/TC and TMF) are replicated on a DR site, it should be noted that the Key Manager ID registered for each volume, will be replicated. Also, the Key Manager IDs of both Primary and Secondary sites must be planned globally.

### VLE Setup

For encryption with VLE, the Volume Group Media Type must be LTO 4.

Tape Catalog	<input type="text" value="DSM/TC"/>
Auto Scratch at Load Time	<input type="text" value="YES - data discarded only for expired volumes"/>
Delete Expired Volumes	<input type="text" value="Yes"/>
Media Type	<input type="text" value="LTO4"/>
Warning Threshold (Min % Of Scratch Volumes)	<input type="text" value="0"/> %
Migration to BackBox	<input type="text" value="None"/> Switch to the BackBox storage is completed. Virtualization is still available, but Auto-import is disabled.

If there is a Volume Group that you have been using, and from now on, you want to encrypt the content of its media using the VLE-CLIM Client, you can simply modify its Media Type to become LTO.

4. From that point on, all new uses of SCRATCH volumes in the Volume Group (such as for new backups) will mount as LTO 4 media to be Encrypted. Existing ASSIGNED media will also be mounted as LTO 4 and be read by NonStop applications, such as RESTORE, even if not encrypted. If the Volume Group uses the DSM/TC tape catalog, the following MEDIACOM command must be performed on the Pool associated with that Volume Group:

```

MEDIACOM
>ALTER POOL vt-pool-name, TYPE ANY
>ALTER TAPEVOLUME *, POOL vt-pool-name, TYPE LTO 4

```

## Report OBB038 – List of Encrypted Volumes

OBB038 lists the Encrypted volumes whose label matches a volume label pattern.

### Syntax:

```
RUN OBB038 label-pattern
```

Where label-pattern is a specific label or a simple pattern ending by \*, ex:

```

RUN OBB038 *
RUN OBB038 PR*

```

### Content of OBB038:

```

?tacl macro
COMMENT
*****
***** COMMENT * Extract VOLEXT from
the BackBox catalog *
COMMENT * and list Encrypted volumes *
COMMENT * One positional parameter:
pattern of labels to select* COMMENT
*****
***** RUN BB010 %1%

COMMENT*****
***** COMMENT BB038: List the
BackBox Encrypted volumes * COMMENT
*
COMMENT Note: The Tandem ENFORM
reporting tool is required * COMMENT
*****
***** ASSIGN VOLEXT-REC, VOLEXT
PARAM LABELS
%1%
ENFORM /IN
BB038/

```

### Sample:

```

BB038 Encrypted volumes with label matching *2022-10-24 11:24
Last

DSMTC
Volume
write
or TMF
label date status Encryption key ID
Key Manager
id : KM-ESKM
Client type
: 1-VTC
ONLY
VE1001 2022/10/27 ASSIGNED BBOX_21F5BD27VE1001D68095D44B400008_111027202410
VE1015 2022/10/27 ASSIGNED BBOX_767FE574VE1015D5C6642F4B230008_111024144520
2 printed volumes for Key
Manager KM-ESKM End of report
BB038

```

### Report elements:

Volume label	Label of the virtual tape volume.
Last write date	Last date the volume was written by a tape application. DSM/TC - TMF Volume status in DSM/TC or TMF
Status	(when applicable). Encryption key ID Encryption key name instance.

## Volume

### Volume Details

The Encryption state of each volume is registered. The ID of the volume specific key in the Key Manager is included for support to access this key through the Key Manager user interface.

Encryption Algorithm	AES-GCM-256
Key Manager ID	KMVLE
Encryption Key ID	N12804D13CSW005A88CEEE0DD360008_BBBBBBBB_1903131332

### Volume Edition

The Encryption attributes of a volume can be updated. Example of use case:

- Volumes manually registered in a Restricted Data store accessing the images of volumes written encrypted in a different environment not linked by the BackBox catalog replication.

Guardian Node Owner*	<input type="text" value="\CGNAC2"/>
Guardian User ID Owner*	<input type="text" value="255,144"/>
Encryption Algorithm	<input type="text" value="AES-GCM-256"/> ▼
Key Manager ID	<input type="text" value="KMVLE"/> ▼
Comment	<input type="text"/>

#### Encryption related elements

- Encryption Algorithm (value AES-GCM-256 or None).  
In the case used above, changing None to AES-GCM-256 will enable the decryption when reading the tape volume.
- Key Manager ID: Appears only when the encryption is enabled and is mandatory in this case.  
This ID names the Key Manager, configured in the current BackBox domain, and this will provide the encryption context for accessing the tape volume.