



SmartSecure[™] Encryption Technical White Paper

Contents

Introduction.....	4
Audience.....	4
Feature Overview	5
Terminology.....	5
Master Encryption Key.....	6
Passphrases.....	6
Deployment Guidelines.....	9
Enable Encryption.....	9
Default Setting Parameter.....	10
Scope Parameter.....	11
New Volumes.....	11
System Startup Mode.....	12
Replication.....	15
Clones.....	15
Role-Based Administration Privileges.....	16
Alerts.....	16
Changing the Encryption State of Existing Volumes.....	18
Disabling Encryption.....	19
Shredding Data.....	20
Merging Groups.....	21
Summary.....	23
References.....	24
Version History.....	25

Legal Notices

Copyright 2010-2017 Nimble Storage, Inc. All rights reserved worldwide.

No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by electronic, mechanical, recording, photocopy, scanning or other means without prior written permission from Nimble Storage, Inc.

The product described in this documentation may be protected by US Patent 8,285,918, US Patent 8,832,330 US Patent 8,924,607, US Patent 8,949,502, US Patent 9,003,113, US Patent 9,015,406, US Patent 9,081,670, US Patent 9,098,405, US Patent 9,116,630 and other pending patent applications.

Nimble Storage, Incorporated (Nimble), has used the latest information that is available in producing this document. Nimble Storage makes no warranty, expressed or implied, with regard to accuracy and completeness.

Information in this document is subject to change without notice.

Nimble Storage, the Nimble Storage logo, CASL, InfoSight, and NimbleConnect are trademarks or registered trademarks of Nimble Storage. All brand names and product names mentioned in this document are trademarks of their respective owners. Where known, trademarked, registered trademarks, and service marks are designated as such.

InfoSight® is a registered trademark in Japan of Intage Inc. of Japan. Usage of InfoSight® in Japan is permitted pursuant to a trademark license agreement between Nimble Storage, Inc. and Intage Inc.

Nimble Storage, Inc.
211 River Oaks Parkway
San Jose, CA 95134
U.S.A.

Tel: +1 408.432.9600
Website: <http://www.nimblestorage.com>
Sales: sales@nimblestorage.com

Publication Date: Wednesday March 8, 2017 12:20:24

Support

All documentation and knowledge base articles are available on the Nimble Storage Support site at <https://infosight.nimblestorage.com>. To register on InfoSight, click the *Enroll Now* link on the main page.

Email: support@nimblestorage.com

For all other general support contact information, go to <http://www.nimblestorage.com/support>.

Introduction

This white paper describes the advantages of the integrated, software-based Nimble Storage® SmartSecure™ encryption feature. SmartSecure enables you to encrypt data and to shred it on a per-application basis. It saves storage capacity and operations time, and it requires no custom drives, dedicated firmware, or expensive licensing.

You can enable SmartSecure on any Nimble platform by simply activating the feature for the volumes that need it. SmartSecure uses existing drives, and it has minimal impact on performance. The encryption works seamlessly with other Nimble features such as snapshots, replication, and zero-copy cloning; it can also be implemented across SSDs and HDDs within the array and on external shelves.

In consolidated and multi-tenant storage environments, you can enable SmartSecure encryption on a per-application (volume) or per-array basis. You can also shred data on a per-volume basis, which is especially useful for compliance and sensitive data environments and for cloud service providers.

SmartSecure requires you to encrypt stored data only once. When data is compressed by the Nimble array, capacity savings are preserved because there is no need to reconstitute the data that you want to secure. Encrypted data that is replicated to another site remains encrypted during transfer and is stored securely on the target system.

Audience

Nimble Storage administrators and security administrators can use the recommendations presented in this white paper to help them deploy a supported, successful, and reliable solution.

The paper assumes that the audience has a general knowledge of and familiarity with Nimble products, the Nimble user interface, and basic setup tasks. Readers should also understand the encryption and security requirements for a given product deployment.

Feature Overview

The software-based Nimble SmartSecure encryption feature is available for arrays running NimbleOS version 2.3 or later. It offers numerous benefits:

- The data encryption process uses the AES-256-XTS cipher for cryptographic protection of data on block-oriented storage devices.
- The performance-optimized implementation leverages the Intel AES-NI instruction set on a variety of Nimble arrays:
 - Later-model arrays in the CS-Series
 - All Flash Arrays
 - Adaptive Flash Arrays
- Data compression occurs prior to encryption, which preserves capacity savings.
- The feature can be deployed selectively on a volume-by-volume basis or to an entire array group.
- Two modes of operation are available:
 - Secure system startup mode, which requires a passphrase after an array restart to access encrypted data
 - Available system startup mode, which does not require a passphrase
- Support is included for the following Nimble configurations and processes:
 - Scale-out configurations with multiple arrays in a group
 - Volume collection cloning
 - Volume collection replication
- Encryption is validated to Federal Information Processing Standards (FIPS) 140-2 level 1 certification.

The encryption feature provides secrecy for the data in the array by using the AES-256-XTS cipher to encrypt volumes. This encryption protects against the theft of the array itself or the theft of array components such as disk drives. The feature, which is implemented in the software of the Nimble operating system, takes advantage of the Intel AES-NI instruction set on later-model arrays in the Nimble CS-Series, on Nimble All Flash Arrays, and on Nimble Adaptive Flash Arrays.

At implementation, you have the flexibility of choosing between two levels of encryption. You can choose to encrypt only specific data volumes or to encrypt an entire array group.

Terminology

Portions of the encryption terminology used in this document might introduce new or unfamiliar concepts for some readers. To help provide a high-level understanding, the following list briefly defines encryption-related terminology:

Cipher

An algorithm for performing encryption or decryption. For example, Advanced Encryption Standard (AES) is a cipher. Additional examples of ciphers include Data Encryption Standard (DES), Rivest Cipher 5 (RC5), and Blowfish.

AES-256-KeyWrap

An algorithm that provides security to protect encryption keys in the context of a key management architecture. For example, AES-256-KeyWrap is used for secure transmission of encryption keys over a network connection.

AES-256-XTS

A block cipher-based disk encryption scheme that uses two different keys of 256 bits, each resulting in a combined 512-bit key.

OpenSSL

An open source implementation of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols that is designed to provide secure communications over a network connection.

Secure Hash Algorithm-256 (SHA-256)

A cryptographic hash function that is used to determine data integrity by comparing a known hash value to the computed hash value of a given file.

Passphrase

A phrase that, similar to a password, is used to control access to encrypted data residing on a Nimble Storage array that has the encryption feature enabled. A passphrase may consist of 8 to 64 printable ASCII characters. The passphrase is used to encrypt the master key.

Master key

A 256-bit encryption key generated by seeding the OpenSSL random number generator. The master encryption key is used to encrypt or decrypt all other encryption keys.

Volume key

A 256-bit encryption key generated by seeding the OpenSSL random number generator. New encrypted volumes, or volumes cloned from snapshots of encrypted volumes, are assigned new volume encryption keys.

Key table

A table structure internal to the Nimble Storage array in which all keys are encrypted with the master key by using the AES-256-KeyWrap algorithm.

Master Encryption Key

The master encryption key plays an important role in encryption. It is used to encrypt or decrypt all of the other encryption keys. The passphrase also plays an important role because it is used to encrypt the master key. It is important to understand how the master encryption key value is generated, how it is protected from unauthorized access, and how it is recovered after an array restart.

The master encryption key is generated when the Nimble encryption feature is enabled. At initialization, the user must enter a passphrase that consists of 8 to 64 printable ASCII characters. The passphrase is used to generate an SHA-256 hash. The master encryption key generation process seeds the OpenSSL random number generator by using 256 bits of pseudo-random data output from `/dev/urandom`. The resulting master encryption key is then encrypted with AES-256-KeyWrap by using the passphrase hash.

The passphrase is never stored in the Nimble array. It is the responsibility of the array administrative team to keep track of the passphrase. The master encryption key is stored in an encrypted state in the key table, a PostgreSQL table internal to the Nimble operating system, NimbleOS. To allow key access during normal operations or during a failover event, pieces of the master key can exist in array RAM that is allocated to certain processes.

Passphrases

It is the user's responsibility to maintain the passphrase forever. Regardless of which encryption settings you select to use, you will require access to the passphrase at some point in the future.

The passphrase is not stored in the array. It is not transmitted to Nimble Storage technical support through the AutoSupport process. The array does not generate copies of the passphrase in email alerts, SNMP, or Syslog.

It is very important to understand the implications of losing or forgetting a passphrase:

- If the passphrase is lost and the array is configured to use the secure system startup mode, then power cycling or rebooting the array will place all encrypted volumes into an offline state. If the passphrase is lost, the data in these volumes becomes permanently inaccessible. Consider changing to the available

system startup mode to mitigate this problem if a power cycle or reboot event occurs. Plan to copy or migrate data on encrypted volumes to new unencrypted volumes. To create a new passphrase, you must set the encryption feature to its uninitialized state.

- If the passphrase is lost, there is no ability to modify it to a known value. To modify the passphrase, you must provide the current passphrase. Plan to copy or migrate data on encrypted volumes to new unencrypted volumes. To create a new passphrase, you must set the encryption feature to its uninitialized state.

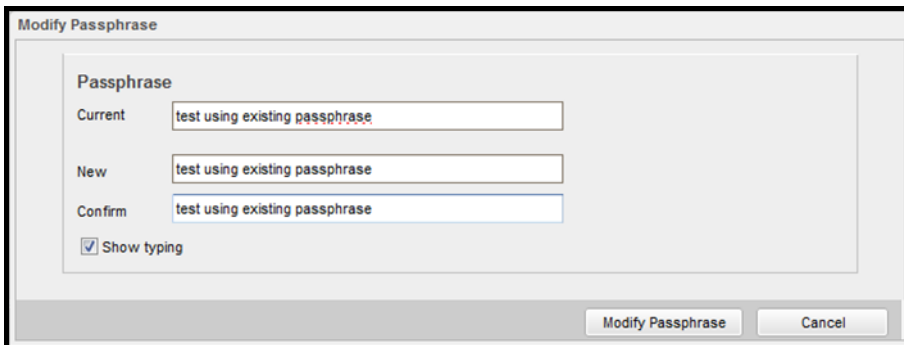
Modify Passphrase

Some passphrase storage utilities might be incapable of accommodating up to 64 ASCII characters. If you plan to use a passphrase storage utility, Nimble strongly recommends that you test the utility's ability to recover the passphrase before you create encrypted volumes. For instance, try to modify the existing passphrase.

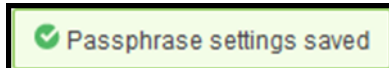
Note You can also use the steps provided in this procedure to change the existing passphrase in response to site requirements. When you change the passphrase, use the current passphrase to decrypt the master key and then use the new passphrase to reencrypt it.

Procedure

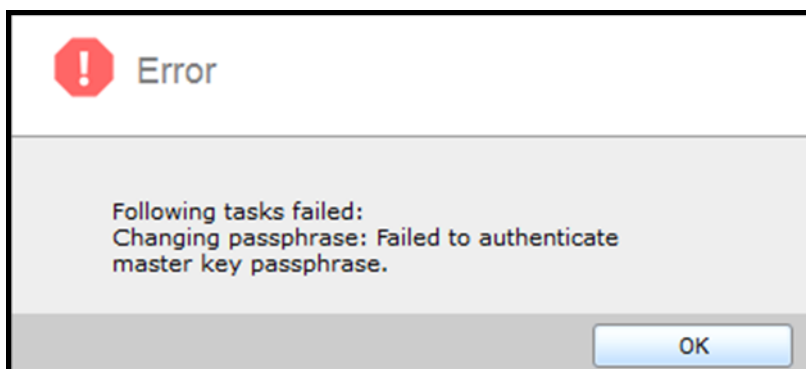
- 1 In the **Modify Passphrase** dialog box, enter the existing passphrase in the **Current**, **New**, and **Confirm** fields and click **Modify Passphrase**.



- 2 If the passphrase successfully retrieved, a message indicates that the passphrase settings were saved.



If the retrieval was unsuccessful, a message warns that the attempt to change the passphrase failed.



Note If the attempt to change the passphrase failed, indicating that passphrase retrieval was unsuccessful, see [Disabling Encryption](#) on page 19 later in this document. Disabling encryption returns the encryption feature to its uninitialized state. Starting over from the uninitialized state allows you to set a new passphrase.

Deployment Guidelines

To deploy the software-based SmartSecure encryption feature, you must first enable encryption and then configure the parameters for the default setting and the scope.

The encryption feature also affects the following operations:

- New volumes
- System startup mode
- Replication
- Clones
- Role-based administration privileges
- Alerts

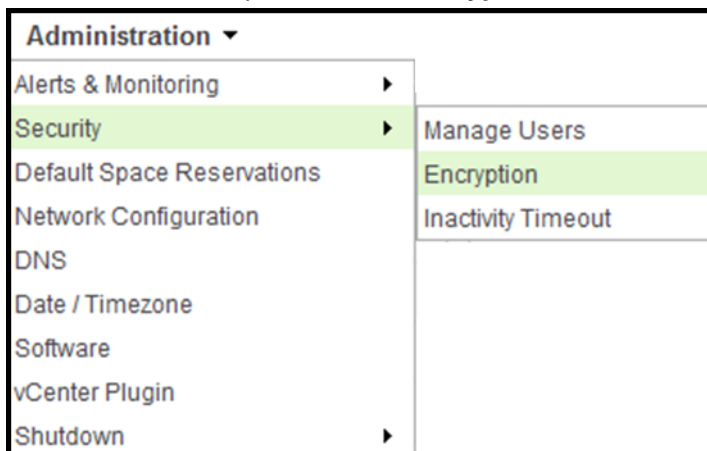
For more information about encryption, see the *NimbleOS Release Notes* document associated with your version of the Nimble operating system. The document is available for download on the Nimble Storage [InfoSight](#) web portal.

Enable Encryption

By default, encryption is disabled. To enable it, you must have the administrator role privilege set.

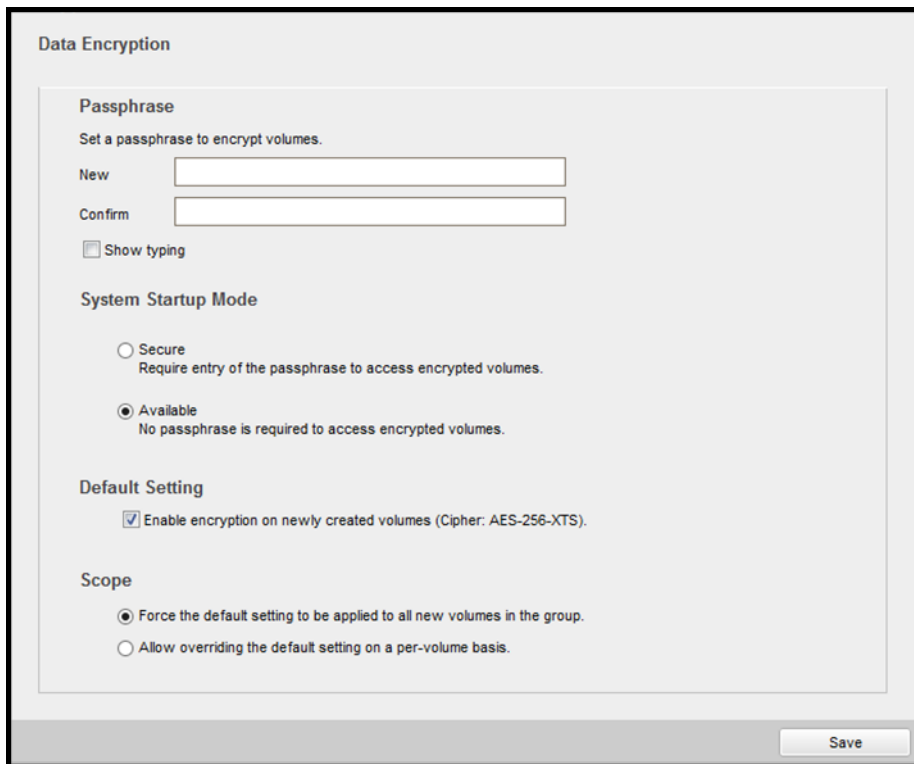
Procedure

- 1 Click the **Administration** menu item.
- 2 From the pull-down menu, select **Security**.
- 3 From the available options, select **Encryption**.



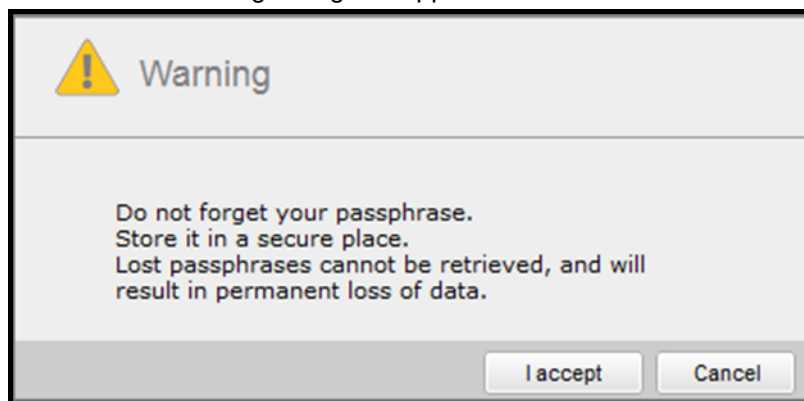
- 4 In the **Encryption** dialog box, enter a passphrase and click **Save** to enable data encryption.

Note Select the **Show typing** checkbox to see the passphrase characters (8 to 64 printable ASCII characters) as you type them.



The image shows a 'Data Encryption' configuration window. It has a title bar 'Data Encryption'. Inside, there's a section 'Passphrase' with the instruction 'Set a passphrase to encrypt volumes.' Below this are two text input fields labeled 'New' and 'Confirm'. A checkbox labeled 'Show typing' is below the input fields. The next section is 'System Startup Mode' with two radio button options: 'Secure' (with subtext 'Require entry of the passphrase to access encrypted volumes.') and 'Available' (with subtext 'No passphrase is required to access encrypted volumes.'). The 'Available' option is selected. Below this is a 'Default Setting' section with a checked checkbox labeled 'Enable encryption on newly created volumes (Cipher: AES-256-XTS)'. The final section is 'Scope' with two radio button options: 'Force the default setting to be applied to all new volumes in the group.' (selected) and 'Allow overriding the default setting on a per-volume basis.' At the bottom right is a 'Save' button.

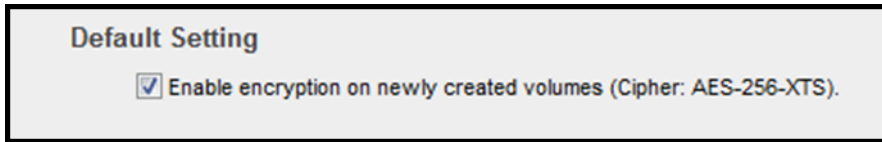
- 5 Click Save. A warning dialog box appears.



- 6 Take the warning seriously. Click **I accept** to enable encryption or click **Cancel** to leave the encryption feature in an uninitialized state.
- 7 Record the passphrase and retain it in a secure location as determined by your site procedures.

Default Setting Parameter

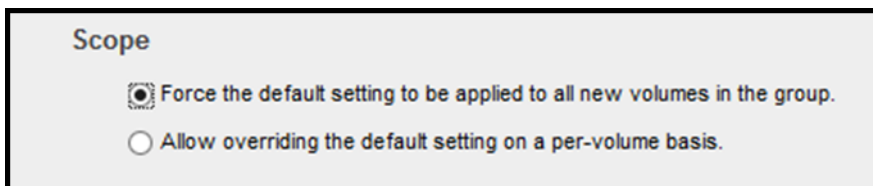
The default setting parameter defines the default encryption setting to be used on all newly created volumes. To enable encryption, select **Enable encryption on newly created volumes (Cipher: AES-256-XTS)**.

Figure 1: Default setting

In its default state, this parameter is enabled (with the checkbox selected).

Scope Parameter

The scope parameter allows you to either enforce the default setting or allow it to be overridden.

Figure 2: Scope

You must select one of the two scope parameter options:

- **Force the default setting to be applied to all new volumes in the group** enforces the default encryption setting (enabled or disabled) on all newly created volumes.
- **Allow overriding the default setting on a per-volume basis** allows encryption to be selectively enabled or disabled on a new volume when it is created.

The following table clarifies the possible interactions between the default setting parameter and the scope parameter.

Table 1: Default setting/scope matrix

Default Setting	Scope	Result
Enable encryption	Allow override	Encryption is enabled by default and can be disabled at volume creation time.
Enable encryption	Force default setting	Encryption is enabled by default and cannot be disabled at volume creation time.
Disable encryption	Allow override	Encryption is disabled by default and can be enabled at volume creation time.
Disable encryption	Force default setting	Encryption is disabled by default and cannot be enabled at volume creation time.

New Volumes

You can enable or disable data encryption on a volume only when it is first created. You cannot enable encryption on an existing unencrypted volume or disable encryption on an existing encrypted volume.

Each new encrypted volume is assigned a new volume key at the time of its creation.

When you create a new volume, the data encryption property is enabled or disabled based on the value of the default setting parameter. Your ability to enable or disable encryption when you create a new volume depends on the value selected for the scope parameter.

In the following example, the default setting parameter is enabled; therefore, encryption is enabled on new volumes by default. The scope parameter is set to the value **Force the default setting to be applied to all new volumes**. The result is that the data encryption parameter is enabled, and it cannot be altered.

Figure 3: Create volume with encryption enabled and force default setting

The screenshot shows the 'Create a volume' dialog box with tabs for General, Space, Protection, and Performance. The 'Data Encryption' section is highlighted with a green box, showing the 'Enable encryption' checkbox checked and the 'Cipher' set to 'AES-256-XTS'.

In the next example, the default setting parameter is enabled, so encryption is enabled on new volumes by default. However, the scope parameter is set to **Allow overriding the default setting on a per-volume basis**. The result is that the data encryption parameter is enabled, but it can be overridden for new volumes.

Figure 4: Create volume with encryption enabled and allow override setting

The screenshot shows the 'Create a volume' dialog box with tabs for General, Space, Protection, and Performance. The 'Data Encryption' section is highlighted with a green box, showing the 'Enable encryption' checkbox checked and the 'Cipher' set to 'AES-256-XTS'.

System Startup Mode

When you restart or power on an array, your access to the master encryption key depends on how the system startup mode setting is configured. By default, the available system startup mode is enabled; however, this default does not negate the requirement to maintain the passphrase forever.

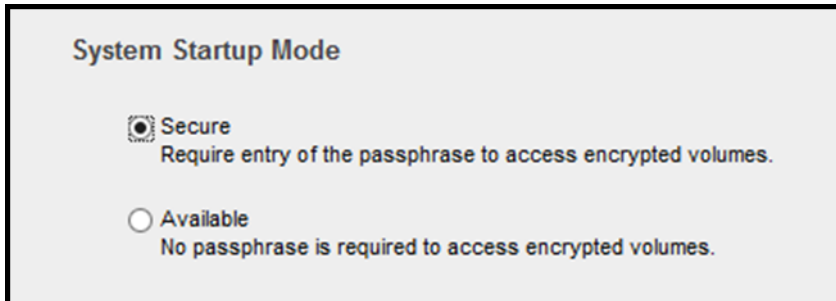
In the available system startup mode, restarting or powering on the array causes all encrypted volumes to be set to an online state, with the following known exceptions:

- **Controller upgrades:** If controllers are being swapped, you must enter the passphrase to enable access to encrypted volumes.

- **NVRAM loss:** In the rare scenario of NVRAM loss, which includes component failure or complete battery discharge, you must enter the passphrase to enable access to encrypted volumes.

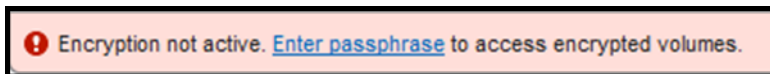
If the secure system startup mode is enabled, you must enter the passphrase so that the system can decrypt the master key. There is no access to encrypted volumes on the array until the passphrase is entered.

Figure 5: System startup mode



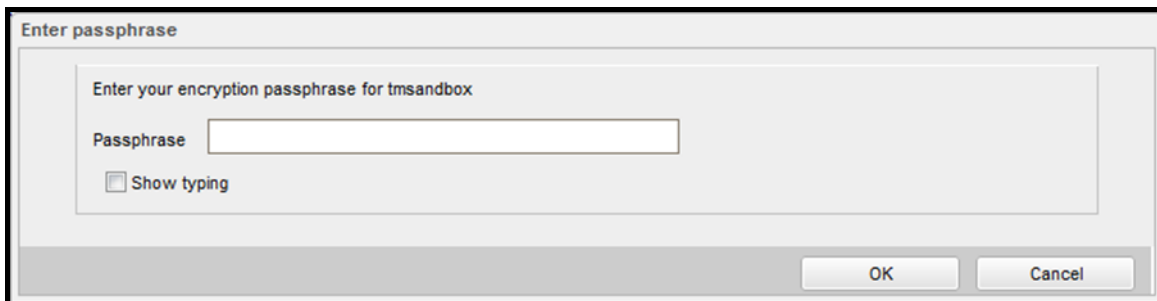
After you restart an array in the secure system startup mode, a message displays to indicate that encryption is not active. Clicking the highlighted **Enter Passphrase** portion of the message allows you to enter the passphrase.

Figure 6: Encryption not active message



After you click **Enter Passphrase**, a dialog box opens where you can enter the passphrase.

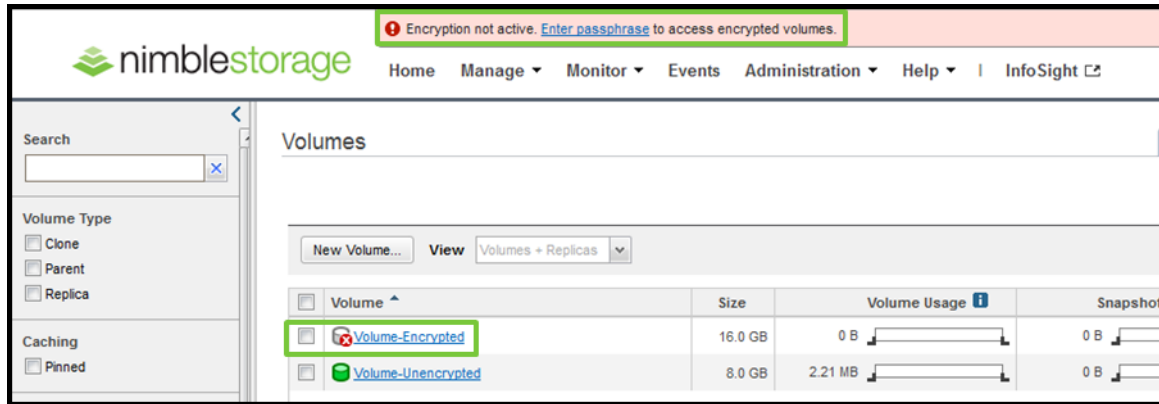
Figure 7: Enter passphrase



Alternatively, you can enter the passphrase through the command line interface (CLI). Use the syntax **encryptkey –enable_master**. After you enter this command, you are prompted for the passphrase.

Consider your choice of system startup mode very carefully. If you enable the secure system startup mode, all encrypted volumes will be in the offline state after an array restart or a power-on event. After you enter the passphrase, the encrypted volumes will change to the online state on the array. On the hosts to which they are normally connected, however, these volumes might still be in the disconnected state.

The following example shows an encrypted volume in the offline state. The system startup mode was set to enable secure mode, and the array was rebooted. An alert message displays to indicate that encryption is not active.

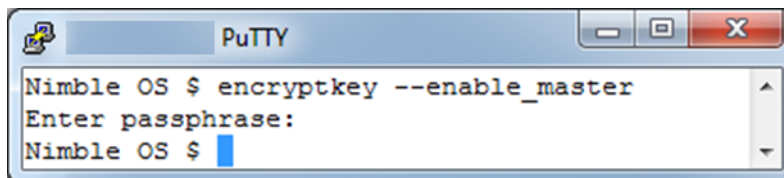
Figure 8: Encrypted volume offline

Moving the cursor over the offline volume displays additional detail, which indicates that the encryption key is not active.

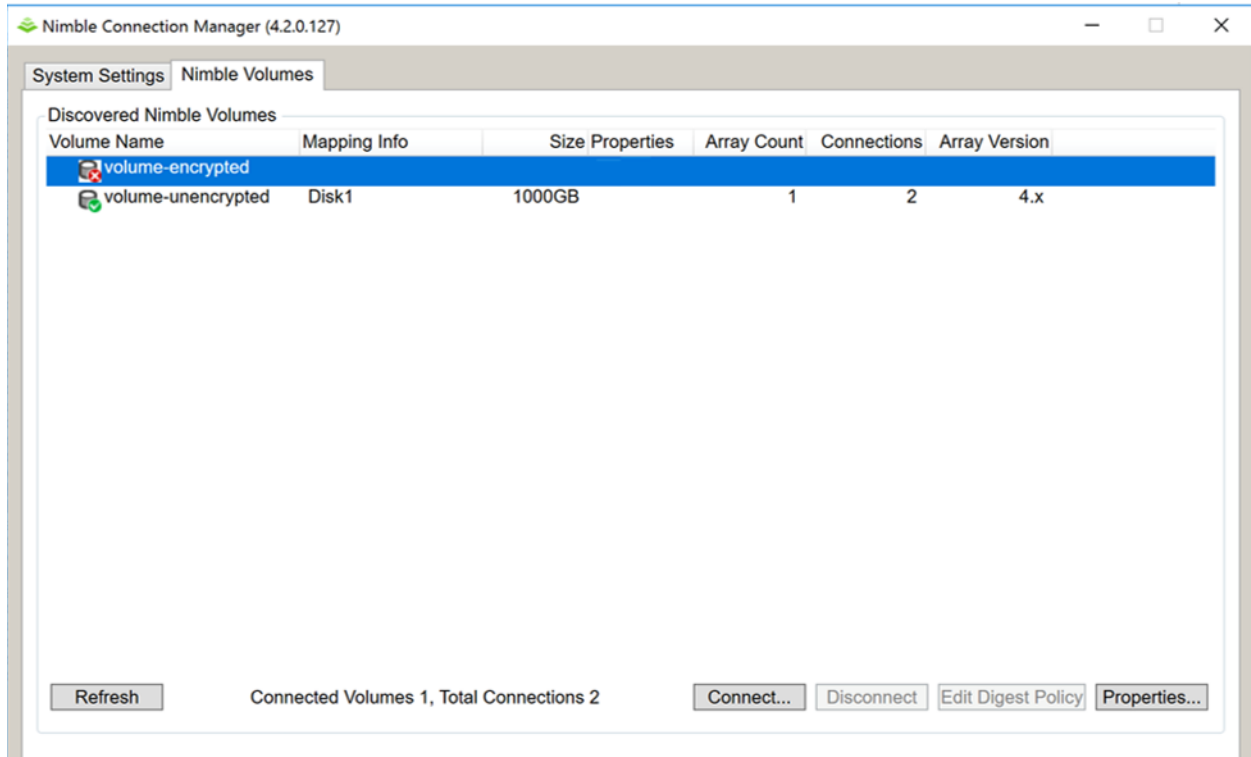
Figure 9: Encryption key inactive

Volume Name	Volume-Encrypted
Status	Encryption key inactive.
Performance Policy	default (Block size: 4096 bytes, Compress: Yes, Cache: Yes)
Volume Collection	
Connected Initiators	0
Replication Partners	
Description	
Storage Pool	default
Caching	Standard

Entering the passphrase changes the state of encrypted volumes to online from the perspective of the array.

Figure 10: Enable master key

On the host that uses this volume, the Nimble Connection Manager (NCM) shows that the encrypted volume is no longer connected to the host.

Figure 11: Nimble Connection Manager

In this example, the encrypted volume must be manually reconnected to the host after the array is rebooted in the secure system startup mode. The effect of using the secure system startup mode might vary depending on the type of connection (Fiber Channel or iSCSI), the type of host operating system, and the version in use.

Replication

To replicate encrypted volumes, you must enable data encryption on both replication partners. Data blocks are replicated in their compressed and encrypted state.

Volume keys for the encrypted volumes that are to be replicated are transmitted to the partner array securely by first being encrypted with AES-256-KeyWrap. The wrapping key is generated through a secure SSL transaction that is authenticated by using the partner array's shared secret.

The volume collection replication of encrypted volumes is administered in the same way as the volume collection replication of unencrypted volumes. A volume collection may contain both encrypted and unencrypted volumes.

A replica volume maintains its original encrypted or unencrypted property.

Clones

When encrypted volumes are cloned, the new cloned volume is also encrypted.

A new volume key is generated for the cloned volume. Cloned volumes are given access to their ancestor's volume key so that they can read shared data blocks. New data blocks that are written to an encrypted cloned volume are encrypted by using the new volume key.

Role-Based Administration Privileges

Administrative capabilities for the data encryption feature vary based on the role of the user. The following table defines the capabilities available for the administrator, power user, operator, and guest roles.

Table 2: Administrative privileges

Role	View Info	Create Master	Enable Master	Disable Master	Delete Master
Administrator	Yes	Yes	Yes	Yes	Yes
Power user	Yes	No	Yes	No	No
Operator	Yes	No	Yes	No	No
Guest	No	No	No	No	No

Important

Each role has its own distinct privileges and limitations:

- The administrator role has full privileges for the encryption feature, including the ability to delete the master key.
- The power user and operator roles can enter the passphrase after a system restart in secure system startup mode.
- The guest role has no privileges.

Alerts

Alerts are generated automatically under certain circumstances:

- When the data encryption feature is enabled
- When the encryption configuration is altered
- After the system is restarted in the secure system startup mode

The following examples show alerts that appear after encryption is deactivated and after the configuration is changed.

Figure 12: Alert – Encryption deactivated

Time: Wed May 6 13:07:55 2015			
Type: 10267			
Id: 31040			
Message: Encryption deactivated. Encrypted volumes cannot be accessed or created. Enter encryption passphrase to reactivate.			
Group Name: tmsandbox			
Group ID: 5818601046605818563			
Version: 2.3.0.0-229814-opt			
Arrays in the group:			
-----+-----+-----+-----			
Name	Serial	Model	Version
-----+-----+-----+-----			
tmsandbox	AA-100471	CS220G-X2	2.3.0.0-229814-opt

Figure 13: Alert – Configuration altered

Time: Wed May 6 06:59:41 2015
Type: 10270
Id: 31005
Message: Encryption mode was changed to available mode.
An array reboot will not require passphrase entry.

Group Name: tmsandbox
Group ID: 5818601046605818563
Version: 2.3.0.0-229814-opt

Arrays in the group:

Name	Serial	Model	Version
tmsandbox	AA-100471	CS220G-X2	2.3.0.0-229814-opt

Changing the Encryption State of Existing Volumes

For existing volumes, you cannot change an unencrypted volume to an encrypted one or an encrypted volume to an unencrypted one. A volume's encryption state is configurable only when the volume is first created.

One way to change the encrypted state of data is to copy the existing volume to a newly created volume that has the desired encryption state. For example, you might copy an unencrypted volume to a new encrypted volume. The copy operation uses a host system that is connected to both the old and the new volumes.

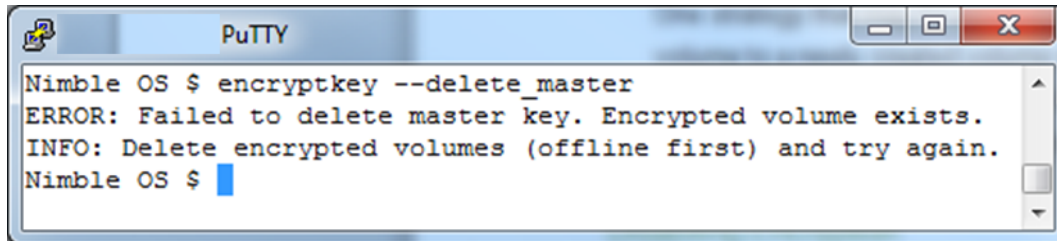
You might also use data migration tools such as VMware vSphere® Storage vMotion® to relocate data from a source volume to a destination volume.

Disabling Encryption

After you enable data encryption, you can disable it only through the command line interface. The **encryptkey --master_delete** command deletes the master encryption key and restores the encryption feature to its uninitialized state.

Before you can disable encryption, you must delete all existing encrypted volumes. If any encrypted volume remains, its presence prevents the deletion of the master key.

Figure 14: Delete master key failure

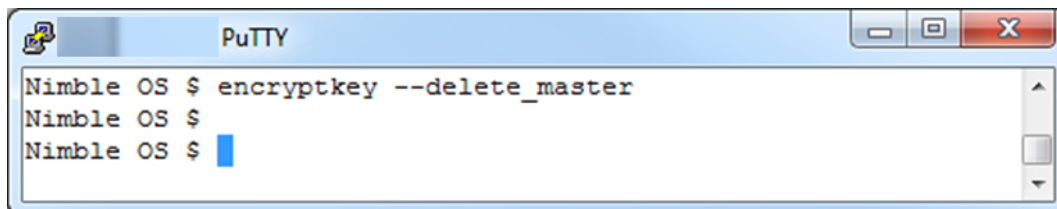


If you have a business requirement to disable encryption, you should copy all encrypted volumes that contain valuable or important data to unencrypted volumes. The tasks necessary to copy data from an encrypted volume to an unencrypted one vary depending on the file system and data type.

For example, you might use Storage vMotion to migrate guests in a VMware® datastore. You might also copy data by mounting encrypted and unencrypted volumes to a host and manually initiating a copy operation. Alternatively, if you have encrypted volumes that do not contain valuable or important data, you might set them to the offline state and delete them to disable the data encryption feature.

If no error message displays in response to the delete command, then the attempt to delete the master key was successful.

Figure 15: Delete master key success



Shredding Data

When an encrypted volume is set offline and deleted, the corresponding volume key is marked inactive. The Nimble operating system does not permit access to inactive keys.

Although an inactive volume key can still be present in the key table, it is stored encrypted by the master key with the AES-256-KeyWrap algorithm. In effect, the data that is associated with the deleted volume is not accessible. Over time, inactive keys in the key table are removed.

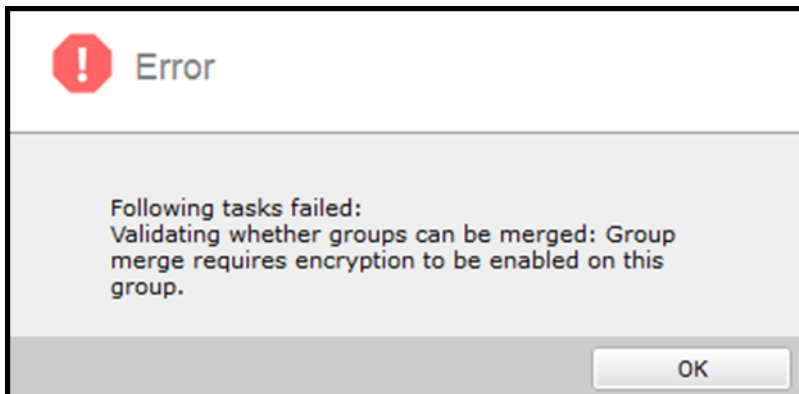
Merging Groups

The movement of pools and volumes can affect the behavior of the data encryption feature. Because encryption can be enabled at the group level or the volume level, and because the settings can be different in different groups, it is important to understand what happens when a pool or volume leaves one group and joins another.

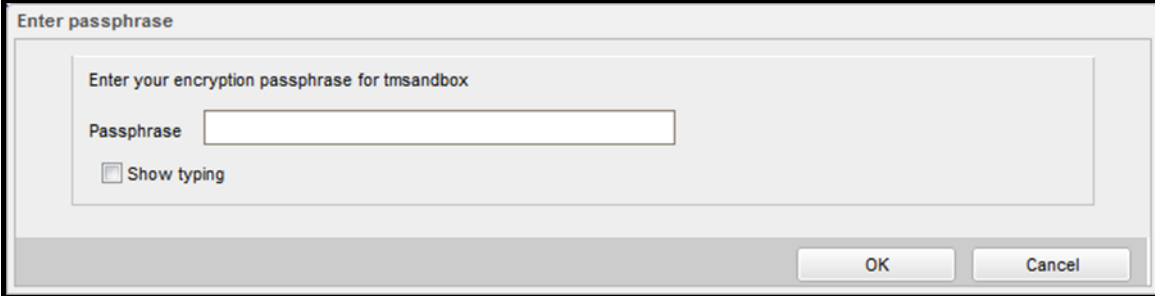
The following merge scenarios show what happens in each use case. In every case, group A is the source group and group B is the destination group.

- **Use case 1:** Group A (encryption enabled) is merged into group B (encryption disabled).
 - This use case is not supported. You must enable encryption in group B before you add group A.

Figure 16: Group merge error



- **Use case 2:** Group A (encryption disabled) is merged into group B (encryption enabled).
 - Pools or volumes on group A with encryption disabled remain unencrypted after they are merged into group B.
 - Pools or volumes on group B with encryption enabled remain encrypted.
 - After the merge, there is no passphrase on group A.
 - After the merge, the passphrase for group B becomes the active passphrase for all pools or volumes.
- **Use case 3:** Group A (encryption disabled) is merged into group B (encryption disabled).
 - Pools or volumes on group A with encryption disabled remain unencrypted after they are merged into group B.
 - Pools or volumes on group B with encryption disabled remain unencrypted.
 - After the merge, there is no passphrase on group A or group B.
- **Use case 4:** Group A (encryption enabled) is merged into group B (encryption enabled).
 - You must enter the passphrase for group A when you add the array to group B.

Figure 17: Enter passphraseA screenshot of a software dialog box titled "Enter passphrase". The dialog has a light gray background. Inside, there is a text input field with the placeholder text "Enter your encryption passphrase for tmsandbox". Below the input field, the label "Passphrase" is followed by the same input field. At the bottom left of the input area, there is a checkbox labeled "Show typing". At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

- Pools or volumes on group A with encryption enabled remain encrypted after they are merged into group B.
- Pools or volumes on group B with encryption enabled remain encrypted.
- After the merge, the passphrase for group A is no longer used.
- After the merge, the passphrase for group B becomes the active passphrase for all pools or volumes.

Summary

The software-based Nimble SmartSecure encryption feature provides data protection by using the AES-256-XTS cipher. It optimizes performance by leveraging the Intel AES-NI instruction set on later-model arrays in the Nimble CS-Series, on Nimble All Flash Arrays, and on Nimble Adaptive Flash Arrays. In addition, it enables you to encrypt data selectively on a volume-by-volume basis or to encrypt an entire array group.

The feature offers the flexibility of two operational modes: the secure system startup mode, which requires a passphrase after an array restart, and the available system startup mode, which does not.

Comprehensive support is included for Nimble scale-out configurations with multiple arrays in a group, for volume collection cloning, and for volume collection replication.

References

For more information about security, see the following Nimble Storage documents:

Version 2.3:

- [Administration Guide](#)
- [Command Reference](#)
- [Windows Integration Guide](#)

Version 3.x:

- [CLI Administration Guide](#)
- [GUI Administration Guide](#)
- [Command Reference](#)
- [Windows Integration Guide](#)

Version History

Version	Release Date	Description
2.0	March 2017	Updated to include Nimble All Flash Arrays and Adaptive Flash Arrays
1.4	August 2015	Second published release
1.3	July 2015	Initial published release
1.0, 1.1, 1.2	May–June 2015	Draft releases