IBM

Washington Systems Center - Storage

Accelerate with IBM Storage:

Spectrum Virtualize Encryption

Byron Grossnickle
Washington Systems Center
Spectrum Virtualize Specialist

Session objectives

- Spectrum Virtualize Encryption Overview
- USB Key Management
- SKLM Key Management
- Demo

Encryption Basics

- Encryption is the process of encoding data so that only authorized parties can read it
- Uses secret keys to encode the data according to well known algorithms
- “Data at rest” means the data is encrypted on the end device (disk drives)
  - In the Spectrum Virtualize implementation the drives themselves DO NOT do the encrypting
- Algorithm being used is AES: US government standard from 2001
  - XTS-AES 256 for data keys
  - AES 256 for master keys
- Algorithm is public, the only secrets are the keys
- Symmetric key algorithm (same key used to encrypt and decrypt data)

Importance of encryption

- Improves physical security of data
- Required by certain customers

Encryption Use Cases

- Encryption typically of interest to industries with high privacy concerns
    - Financial Services
    - Healthcare Providers
    - Federal/Defense Agencies
    - Any client concerned about possible disclosure of data
- Typical encryption use cases
    - Protection against disclosure of data when drives removed
        - Malicious removal of drives
        - Allows customers to send failed hardware back to IBM under warranty (secure erase)
    - Secure erasure of storage
        - Drives or arrays being reused for different data
        - System used in PoC, coming off lease, being sold or otherwise disposed of
- Encryption helps protect against disclosure as a result of access to drives storing data
    - Does not address other exposure such as unauthorized access to systems

Hardware Encryption for Data at Rest

Storwize V7000 Gen2/+ versions, Storwize V5020 (internal only), Storwize V5030 (internal and external), SAN Volume Controller DH8/SV1 and FlashSystem V9000 support encrypting data on internal drives

- HDD and SDD drives in control and expansion enclosures

Encryption is performed in the control enclosure node canister SAS chip

- Applies to all existing drives: *no need to buy new drives*
- SAS chip complies with FIPS-140-2 standard
  - http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html#3598
  - IBM uses FIPS compliant Technology
- RAID/DRAID arrays are encrypted
  - If all RAID/DRAID arrays in a pool are encrypted, by nature the pool is encrypted

Available on v7.4 and above

Operates with all existing functions including:

- Real-time Compression
- Easy Tier

No performance impact/considerations

Note: Encryption for Distributed RAID is supported on v7.7 and above.

Software Encryption for Data at Rest

Storwize V7000 Gen2/+ versions, Storwize V5030, SAN Volume Controller DH8/SV1 and FlashSystem V9000 support encrypting data on externally virtualized storage (Mdisks).

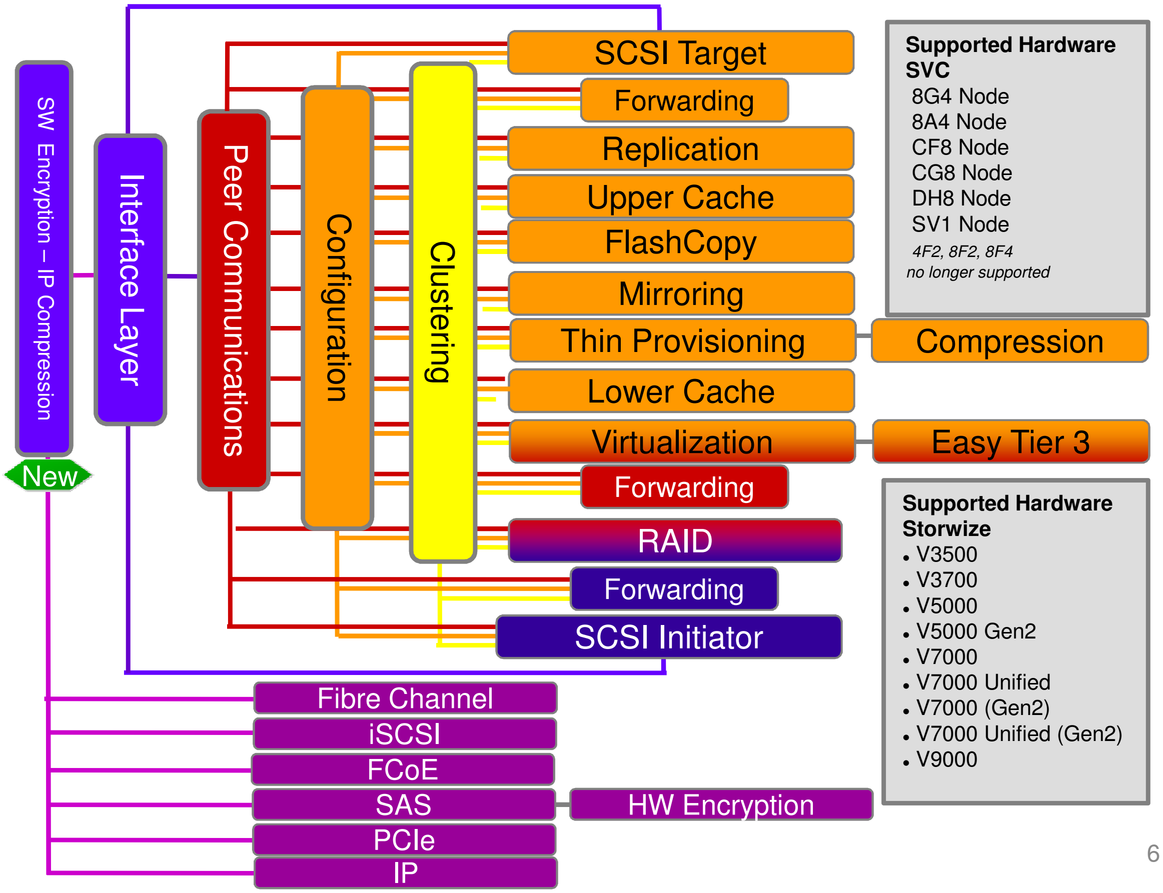
- **Encrypt data on external storage controllers with no encryption capability**
  - Encryption performed by software in the node/canister
  - For external encryption all I/O groups must be external encryption capable
  - Uses Intel AES_NI CPU instruction set and engines
  - AES 256-XTS Encryption, which is a FIPS 140-2 compliant algorithm
  - IBM uses FIPS compliant algorithms

Available on v7.6 and above

- **Encryption enabled at the storage pool level (per pool)**
  - A pool is therefore encrypting or not
  - All volumes created in an encrypted pool are automatically encrypted
  - MDisks now have an 'encrypted' or not attribute
  - Can mix external and internal encryption in same pool
    - If an MDisk is self-encrypting (and identified), then external encryption will **not** encrypt any data to be sent to that MDisk

When is Data Encrypted/Decrypted

- **Data is encrypted/decrypted when it is written to/read from external storage**
  - Encryption/decryption performed in software using Intel AES-NI instructions
  - Encryption/decryption performed by SAS Controller hardware
- **Data is stored encrypted in storage systems (SW) and/or drives (HW).**
- **Data is encrypted when transferred across SAN between IBM Spectrum Virtualize system and external storage (back end)**
- **Data is *not* encrypted when transferred on SAN interfaces in other circumstances (front end/remote system/inter node)**
  - Server connections
  - Remote mirror
  - Intra-system communication for clustered systems
- **If appropriate, consider alternative encryption for "on the fly" data**
  - Note though that Real-time Compression may be affected if you do so.



Supported Hardware SVC

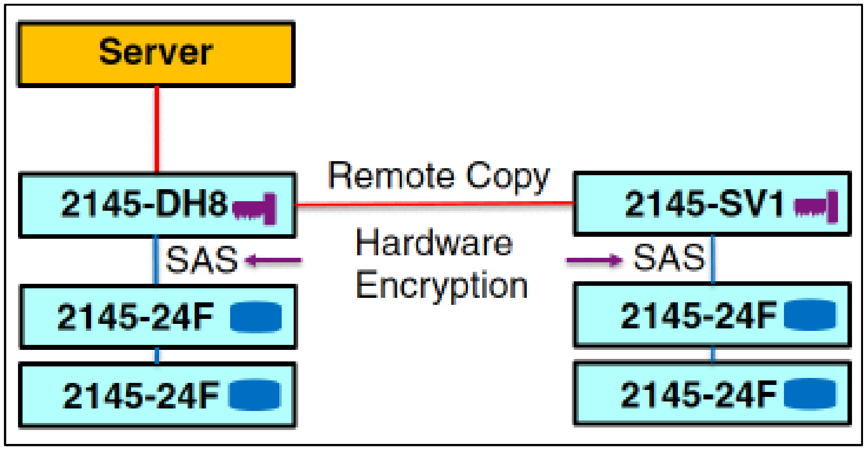
8G4 Node
8A4 Node
CF8 Node
CG8 Node
DH8 Node
SV1 Node

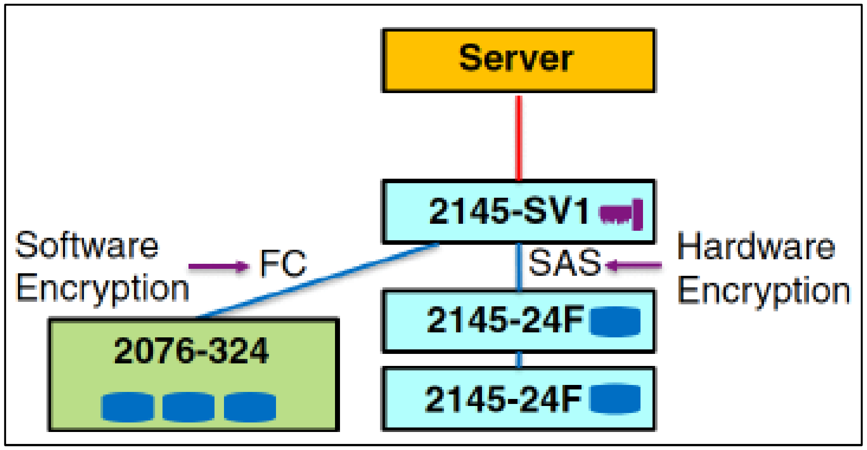
4F2, 8F2, 8F4 no longer supported

Supported Hardware Storwize

- V3500
- V3700
- V5000
- V5000 Gen2
- V7000
- V7000 Unified
- V7000 (Gen2)
- V7000 Unified (Gen2)
- V9000

Software Encryption for Data at Rest





🟩 Encrypted disks and data paths

🟥 Unencrypted disks and data paths

Encryption Key Management

- **IBM Spectrum Virtualize has built-in key management**
  - **Types of keys**
    - Master key (one per system/cluster)
    - Pairwize Master Key (PMK) - Generated by the system and encrypted with the master key
    - Data encryption key
      - One for encrypted pool using external encryption
      - One for each RAID/DRAID array using internal encryption
- **Master key is created when encryption enabled**
    - Stored on USB devices or on a Security Key Lifecycle Manager (SKLM) server
    - Required to use a system with encryption enabled
    - Required on boot (system power-on, system restart) or re-key process, stored in volatile memory on system
    - May be changed
- **Data encryption key is used to encrypt data and is created automatically when an encrypted pool/array is created**
    - Stored encrypted either in the SAS chip for internal encryption or in the quorum disk
    - No way to view data encryption key
    - Cannot be changed
    - Discarded when an array/pool is deleted (secure erase)

Master Key – Internal (USB) Key Management

- **Master key is persistently stored on USB devices**
  - At least 3 devices required when encryption enabled
  - They are also stored in volatile memory in a Key Manager on every node
- **Stored as a simple file**
  - May be copied or backed up as necessary
- **Should be stored securely**
  - Enables access to encrypted data
- ***Master key is required on boot for a system with encryption enabled***
  - System will not access data without contact to master key – handled by the key manager
  - Protect the USB devices holding the master key and consider secure backup copies
- **When a node/controller restarts, software obtains master key**
  - From other node in control enclosure if operational
  - From other nodes in a clustered system
  - From a USB device plugged into the canister

Treatment of USB Devices Holding Master Key

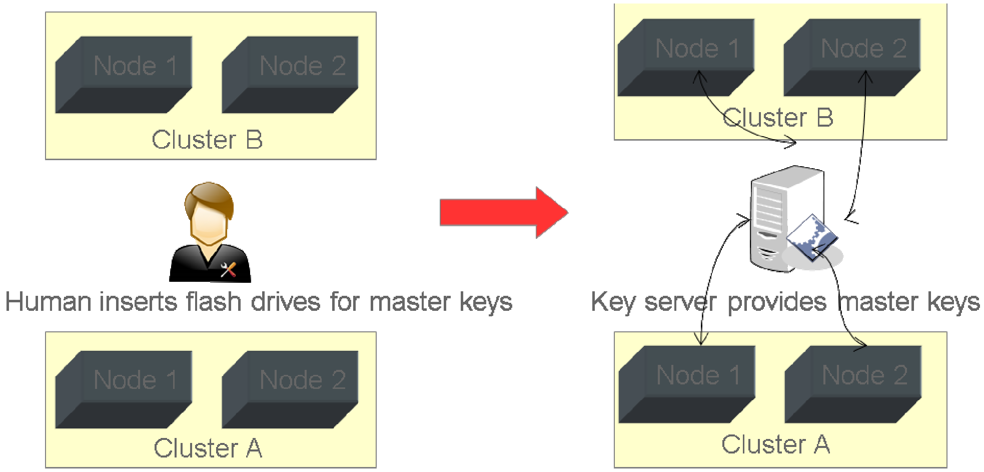
- **USB devices may be permanently plugged into node canisters**
  - Ensures master key will be available in event of a system restart
  - Eliminates any delay
  - Enables access to data if malicious individual removes entire system
- **USB devices may be stored securely apart from system running Spectrum Virtualize**
  - At least one will be required in event of system restart (but not for a node restart)
  - May cause delay in access to data
  - Eliminates risk of access to data if system removed
- USB devices not plugged into node canisters and any backup copies of master key file should be stored securely
- Only IBM USB devices supported for encryption key use so order them in eConfig
  - Others may work, but could be "hit and miss"

Encryption Key Management - External

Security Key Lifecycle Manager Support (SKLM)

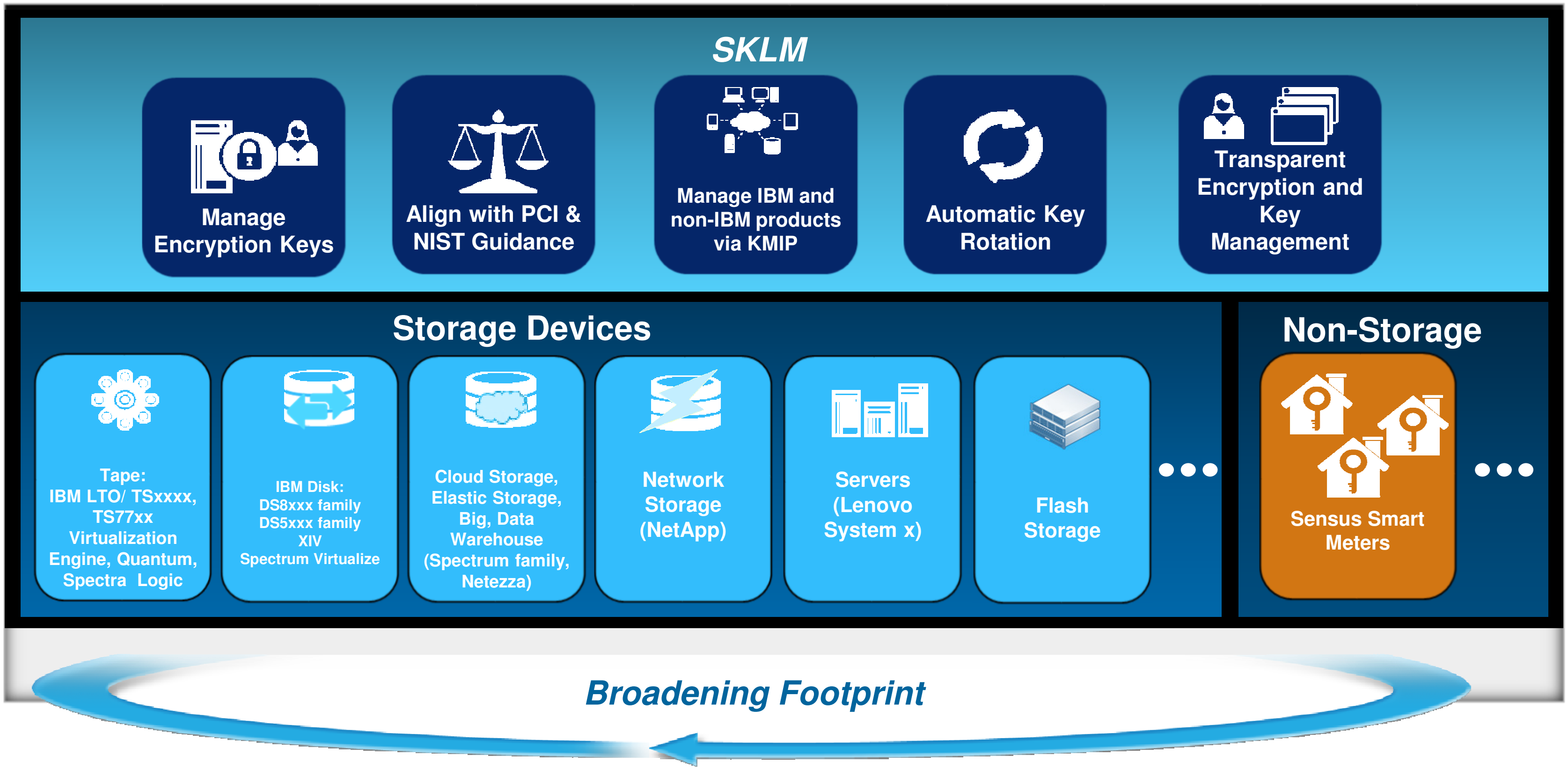
- Spectrum Virtualize now supports SKLM for managing the master encryption key on the system.
  - USB key is no longer a requirement but is still an option.
- **Why is SKLM support important?**
  - Some customers have “no flash drive” policy
  - Allows changing of the master key without physical access to equipment
  - Allows for a central point of key management for the entire organization and across all platforms (server, tape, storage, etc.)

Available on v7.8



Security Key Lifecycle Manager

IBM's centralized key management solution for all encryption solutions



SKLM

- Manage Encryption Keys
- Align with PCI & NIST Guidance
- Manage IBM and non-IBM products via KMIP
- Automatic Key Rotation
- Transparent Encryption and Key Management

Storage Devices

- Tape: IBM LTO/ TSxxxx, TS77xx Virtualization Engine, Quantum, Spectra Logic
- IBM Disk: DS8xxx family DS5xxx family XIV Spectrum Virtualize
- Cloud Storage, Elastic Storage, Big, Data Warehouse (Spectrum family, Netezza)
- Network Storage (NetApp)
- Servers (Lenovo System x)
- Flash Storage
- ● ● ●

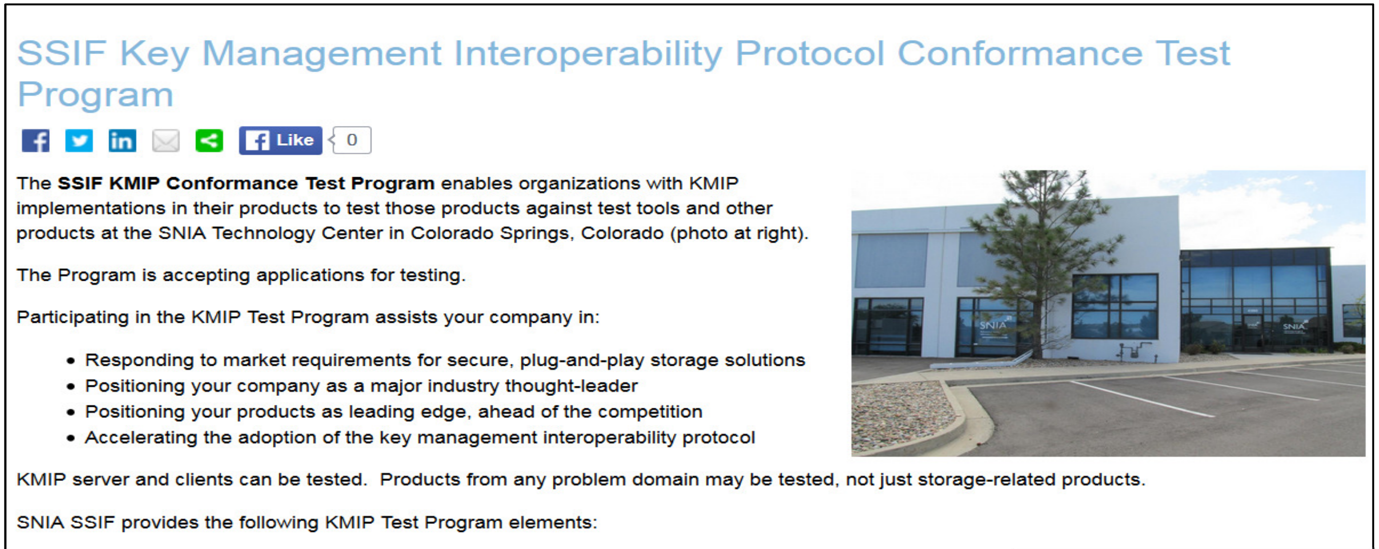
Non-Storage

- Sensus Smart Meters
- ● ● ●

Broadening Footprint

Security Key Lifecycle Manager

SKLM is independently-certified as KMIP-compliant



SSIF Key Management Interoperability Protocol Conformance Test Program

The **SSIF KMIP Conformance Test Program** enables organizations with KMIP implementations in their products to test those products against test tools and other products at the SNIA Technology Center in Colorado Springs, Colorado (photo at right).

The Program is accepting applications for testing.

Participating in the KMIP Test Program assists your company in:

- Responding to market requirements for secure, plug-and-play storage solutions
- Positioning your company as a major industry thought-leader
- Positioning your products as leading edge, ahead of the competition
- Accelerating the adoption of the key management interoperability protocol

KMIP server and clients can be tested. Products from any problem domain may be tested, not just storage-related products.

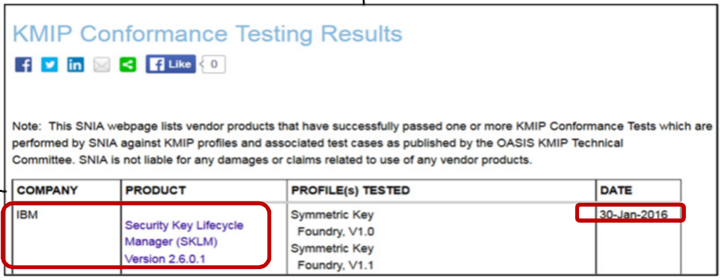
SNIA SSIF provides the following KMIP Test Program elements:

- KMIP test harness to execute tests based on published OASIS KMIP Profile test cases
- Secure, vendor-neutral test lab environment
- VPN access into secure environment
- Formal test execution and monitoring
- Results auditing
- Results reporting
- Results archiving

http://www.snia.org/forums/ssif/kmip

IBM is *only one of three* companies that have passed the rigid SNIA-SSIF Conformance Test:

- IBM
- HP
- CryptSoft



KMIP Conformance Testing Results

Note: This SNIA webpage lists vendor products that have successfully passed one or more KMIP Conformance Tests which are performed by SNIA against KMIP profiles and associated test cases as published by the OASIS KMIP Technical Committee. SNIA is not liable for any damages or claims related to use of any vendor products.

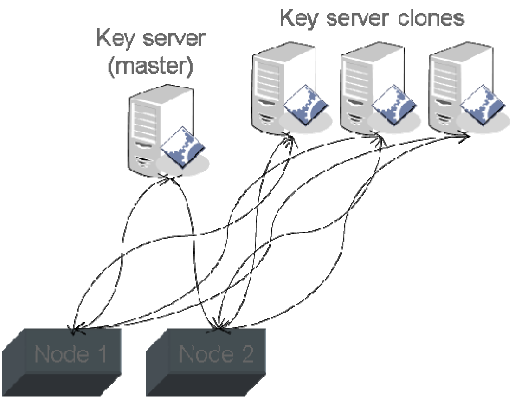
COMPANY	PRODUCT	PROFILE(s) TESTED	DATE
IBM	Security Key Lifecycle Manager (SKLM) Version 2.6.0.1	Symmetric Key Foundry, V1.0 Symmetric Key Foundry, V1.1	30-Jan-2016

Security Key Lifecycle Manager

What It Requires

- Each node/controller needs the ability to talk with the key management server(s) through the service IP address
- Key server software requirements
  - SKLM 2.6.0.0 or higher
  - KMIP Protocol
    - Key Management Interoperability Protocol (KMIP) is a standardized protocol for key servers
    - May support more key managers in the future – have the IBM accou team use SCORE to request
  - Up to 1 master and 3 clones

  (1 Master, no clones at GA, ability will be added soon)



NOTES:

USB **or** Key Server (Not Both)

- Intention is to support both simultaneously
  - ○ Gives a conversion mechanism
  - ○ No easy way to convert at GA

Software Encryption

Performance Overview

- Will not double encrypt – use external / hardware encryption on
  - Virtualized FlashSystems
  - SAS hardware encryption on internal storage (drives) on V7k Gen2/+, DH8/SV1, V5020/V5030 and V9000
  - External MDisks manually defined as encrypted
- Industry Standard XTS-AES256 with AES_NI CPU instruction set
- Software Performance impact 10 – 20% **off top end** worst case on systems under maximum load

- For externally virtualized mdisks encryption is performed in software by the CPU so this can limit total IOPS and/or MBps of the system but expected to have minimal impact to latency

Software Encryption

Performance measured

SVC DH8 over FlashSystem (SW encryption), 1 I/O group, 8Gb FC, cache miss

	encrypted	unencrypted	% performance
4k random read (IOPs)	520k	600k	86%
4k random write (IOPs)	168k	185k	90%
256k random read (MB/s)	10700	13000	82%
256k random write (MB/s)	2900	3100	93%

Storwize V7000 Gen2 over 50% FlashSystem (SW encrytion) / 50% SSD RAID5 (HW encryption), 1 I/O group, 8Gb FC, cache miss

	encrypted	unencrypted	% performance
4k random read (IOPs)	270k	316k	85%
4k random write (IOPs)	74k	83k	89%
256k random read (MB/s)	7200	9200	78%
256k random write (MB/s)	2600	3100	83%

Resources Designated for External Encryption

Encryption runs inside the normal IO process - there's no CPU’s dedicated for encryption.

DH8/SV1//V9000

- 8 CPU cores on first CPU

V7000 Gen2

- No compression enabled – 8 of 8 cores
- Compression enabled – 4 of 8 cores

V7000 Gen2+

- No compression enabled – 10 of 10 cores
- Compression enabled – 6 of 10 cores

V5030

- No compression enabled – 6 of 6 cores
- Compression enabled – 4 of 6 cores

Encryption Recommendations

- If you can encrypt on the back end storage with no performance penalty or encrypt with data in place, take that option.
  - For example, an XIV can encrypt it's data without the need to move it
  - The DS8K, XIV and V7K Internal encryption can be done with no performance penalty
- If you need more granular key management or single methodology use external encryption
  - i.e. key per child pool
  - Single methodology for entire environment (i.e. encryption is done the same way for everything)
- Be careful when mixing types of encryption in the same pool, as different forms of encryption may have different security characteristics.
- Do not mix encrypted and unencrypted arrays in pools – It will result in an unencryped pool

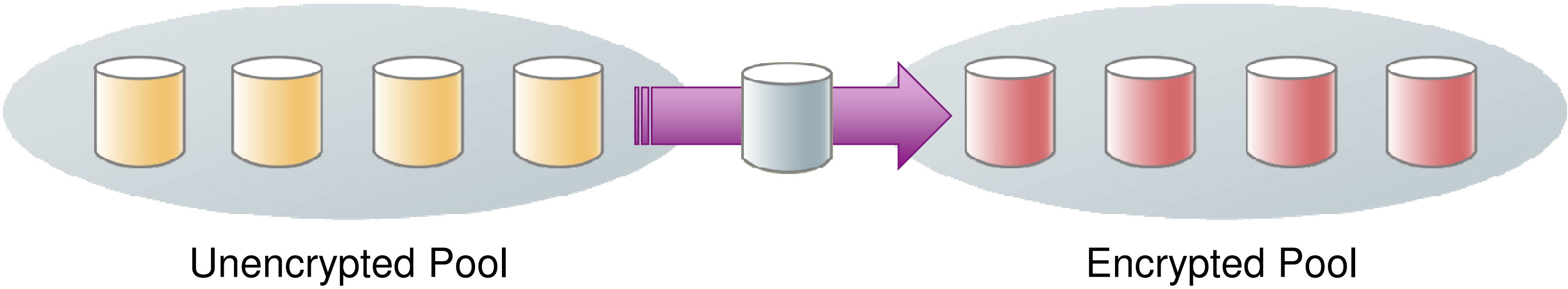
Implementing Encryption

Encryption method for existing systems

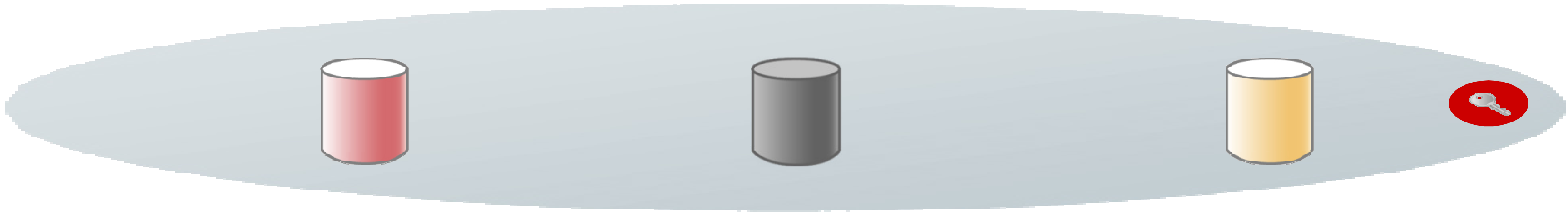
- Create new encrypted pool
  - Move volumes from existing pool to new pool

No “convert in place” function to encrypt existing pools

May require additional capacity



Mixed Encryption in a Pool



Data in this example is encrypted with 3 different keys

🟨 MDisk is created as an internal encrypted RAID array.
SAS Chip Encrypts on Storwize or DH8/SV1 SAS card (HW).

⬛ MDisk is external and declared self-encrypting.
Back end storage array encrypts. Security characteristics could be different.

🟥 MDisk is external and not self-encrypting
Software encryption is used to encrypt with the pool key (SW).

Activating encryption

- Can be performed in one of two ways, either *automatically* or *manually*.
- Both methods can be started during the initial system setup or while the system is running.

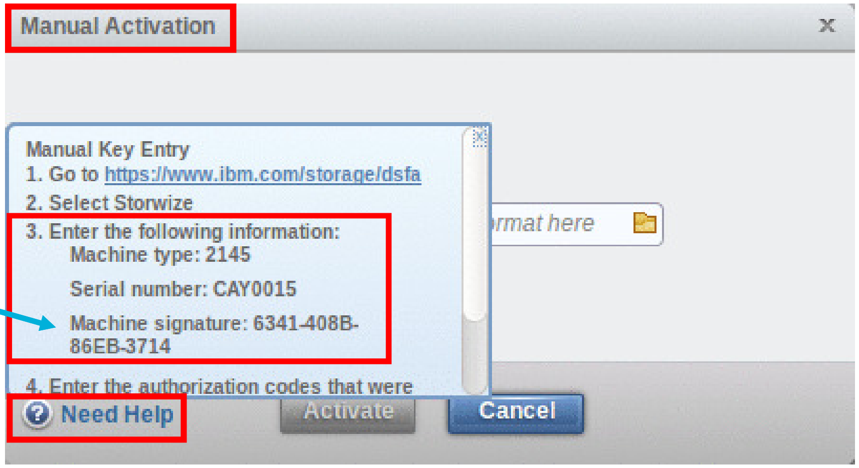
When you purchase a license you should receive a function authorization document with an **authorization code** printed on it. This code is enough to carry on with the automatic activation process.
If the automatic activation process fails or if you prefer using the manual activation process, use this page to retrieve your license keys:
https://www.ibm.com/storage/dsfa/storwize/selectMachine.wss
Ensure that the following information is available:

Machine type (MT)

Serial number (S/N)

Machine signature

Authorization code

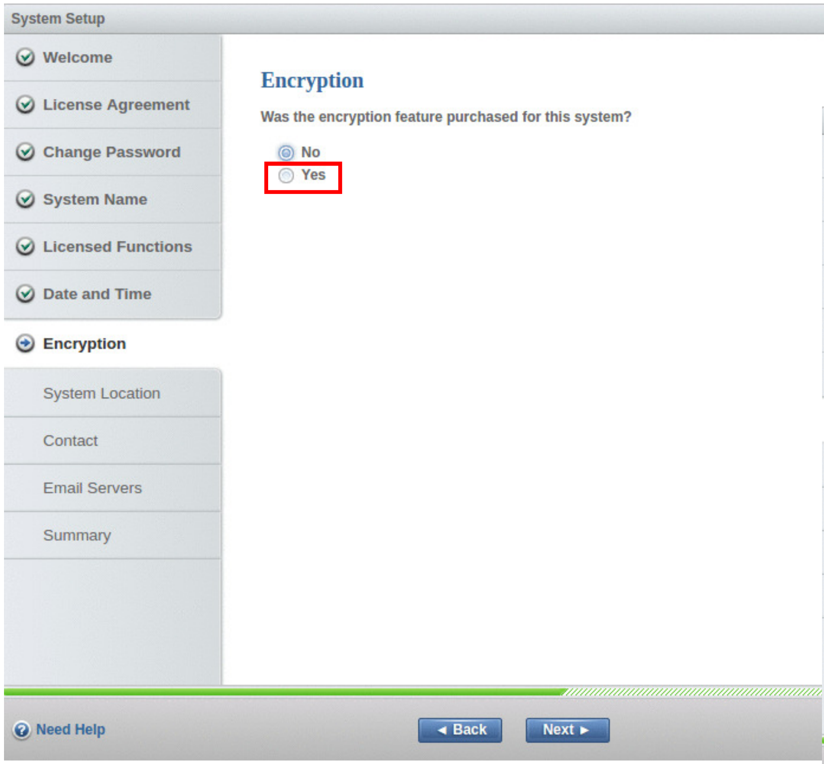


Manual Activation

Manual Key Entry
1. Go to https://www.ibm.com/storage/dsfa
2. Select Storwize
3. Enter the following information:
Machine type: 2145
Serial number: CAY0015
Machine signature: 6341-408B-86EB-3714
4. Enter the authorization codes that were

Activating encryption

Start activation process during initial system setup



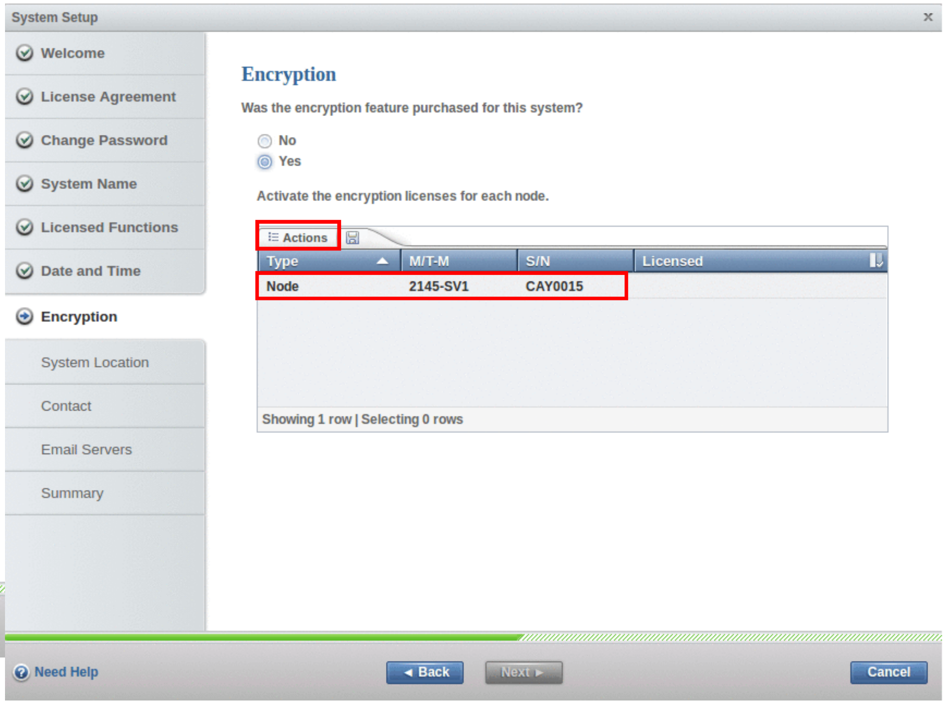
System Setup

- Welcome
- License Agreement
- Change Password
- System Name
- Licensed Functions
- Date and Time
- Encryption
- System Location
- Contact
- Email Servers
- Summary

Encryption

Was the encryption feature purchased for this system?

● No
○ Yes



System Setup

- Welcome
- License Agreement
- Change Password
- System Name
- Licensed Functions
- Date and Time
- Encryption
- System Location
- Contact
- Email Servers
- Summary

Encryption

Was the encryption feature purchased for this system?

○ No
● Yes

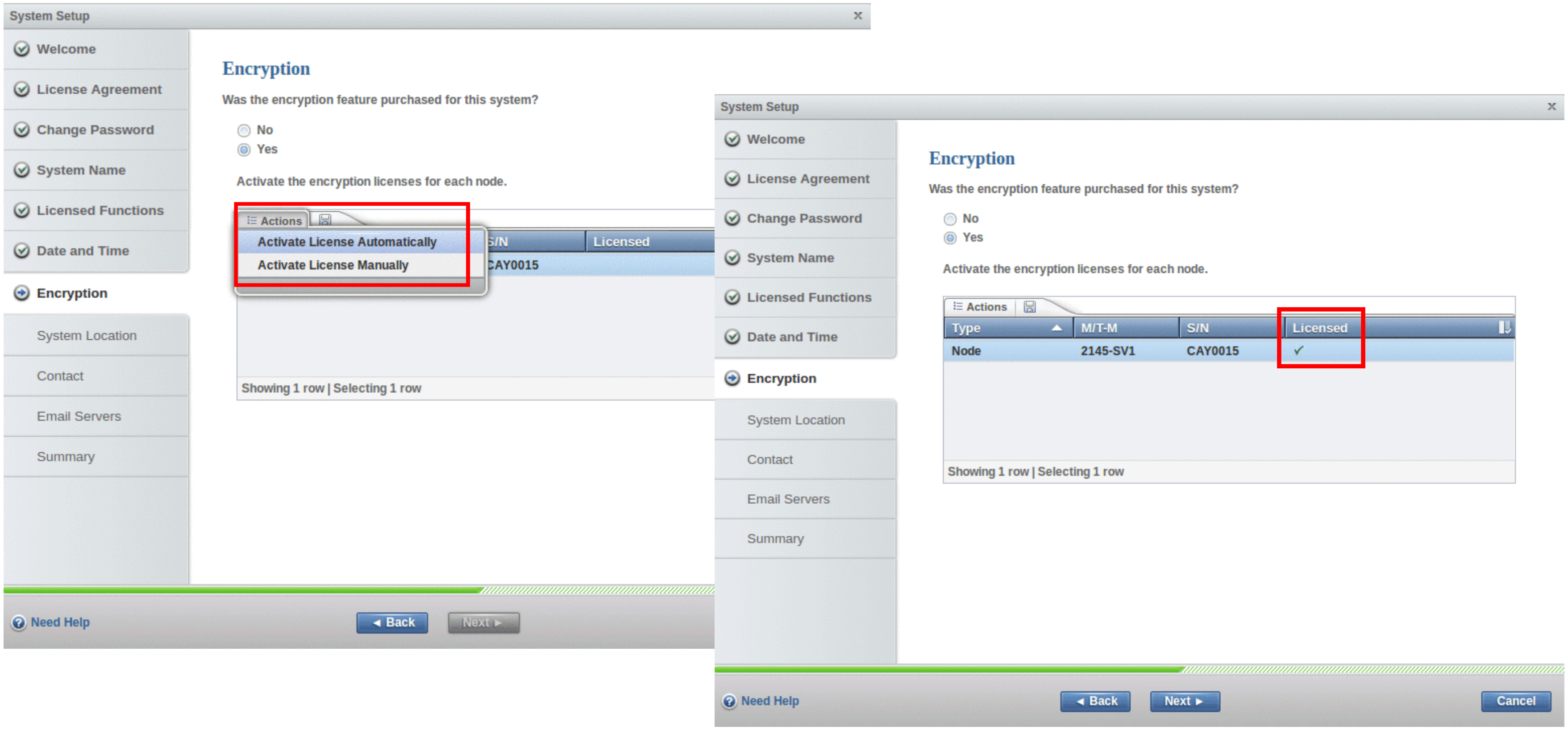
Activate the encryption licenses for each node.

Type	M/T-M	S/N	Licensed
Node	2145-SV1	CAY0015	

Showing 1 row | Selecting 0 rows

Activating encryption

Start activation process during initial system setup



Encryption

Was the encryption feature purchased for this system?

○ No
● Yes

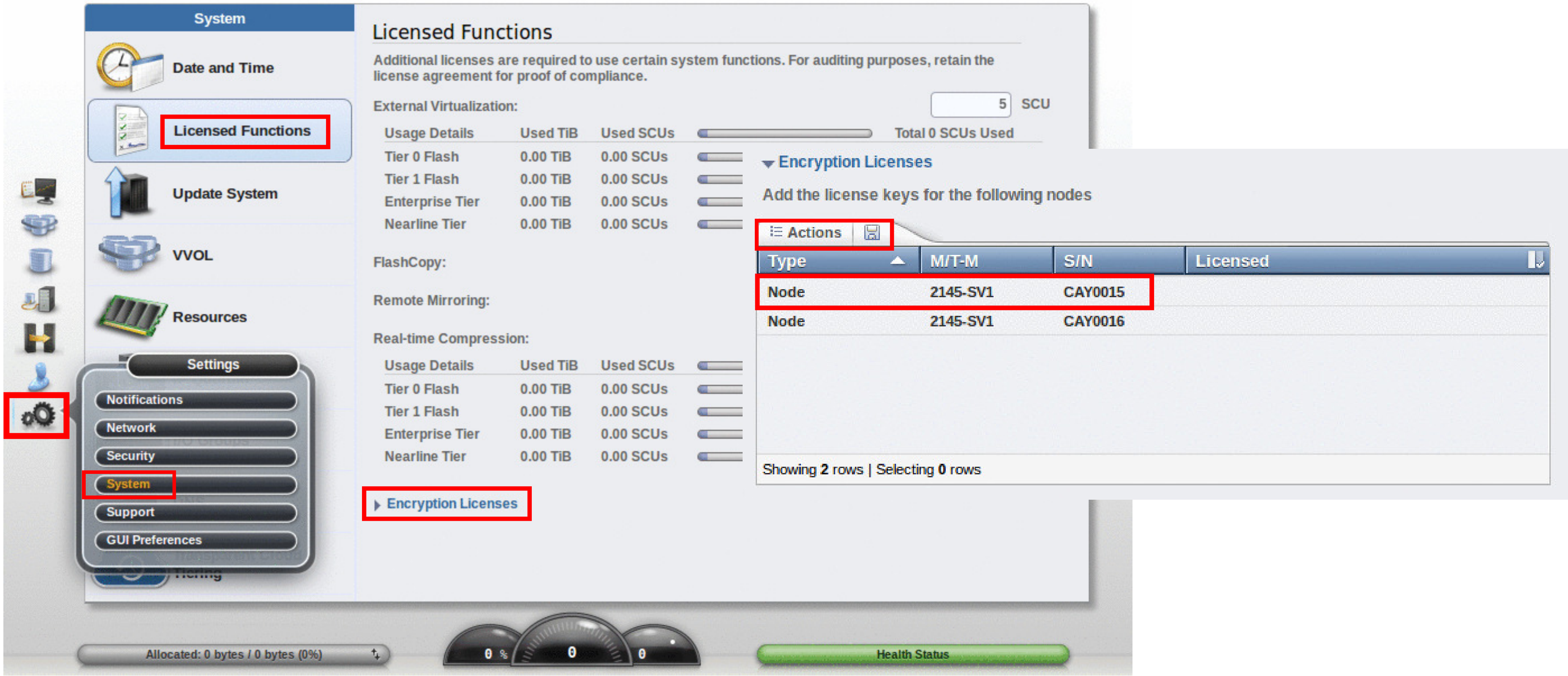
Activate the encryption licenses for each node.

Type	M/T-M	S/N	Licensed
Node	2145-SV1	CAY0015	✓

Showing 1 row | Selecting 1 row

Activating encryption on an Existing System

Navigate to **Settings** → **System** → **Licensed Functions** and click on **Encryption Licenses.**



Licensed Functions

Additional licenses are required to use certain system functions. For auditing purposes, retain the license agreement for proof of compliance.

External Virtualization: 5 SCU

Usage Details	Used TiB	Used SCUs
Tier 0 Flash	0.00 TiB	0.00 SCUs
Tier 1 Flash	0.00 TiB	0.00 SCUs
Enterprise Tier	0.00 TiB	0.00 SCUs
Nearline Tier	0.00 TiB	0.00 SCUs

Total 0 SCUs Used

FlashCopy:

Remote Mirroring:

Real-time Compression:

Usage Details	Used TiB	Used SCUs
Tier 0 Flash	0.00 TiB	0.00 SCUs
Tier 1 Flash	0.00 TiB	0.00 SCUs
Enterprise Tier	0.00 TiB	0.00 SCUs
Nearline Tier	0.00 TiB	0.00 SCUs

▸ Encryption Licenses

▾ Encryption Licenses

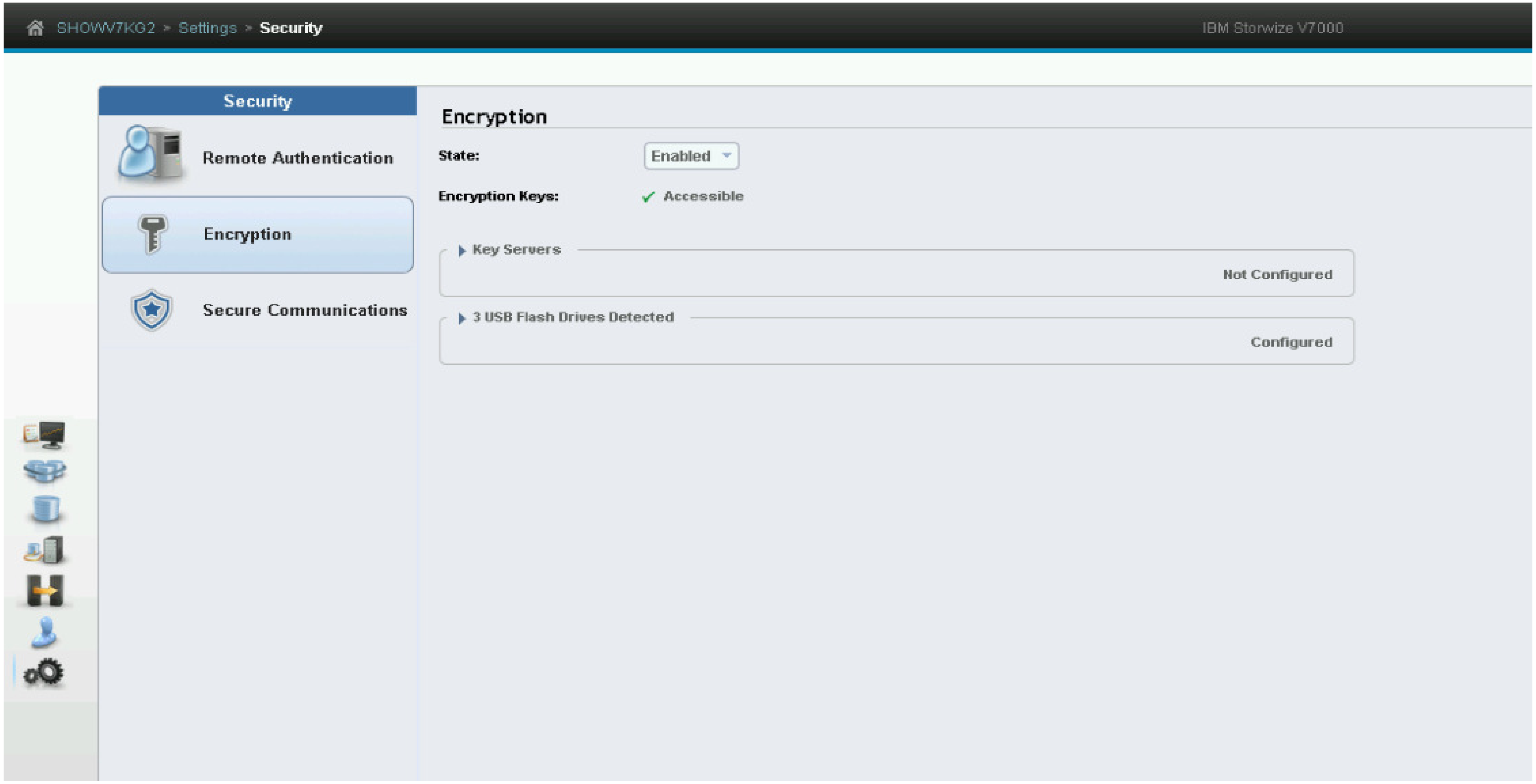
Add the license keys for the following nodes

Actions

Type	M/T-M	S/N	Licensed
Node	2145-SV1	CAY0015	
Node	2145-SV1	CAY0016	

Showing **2** rows | Selecting **0** rows

Enable Encryption From Here



Encryption

State: Enabled

Encryption Keys: ✓ Accessible

Key Servers — Not Configured

3 USB Flash Drives Detected — Configured

2017 Storage Masters

Demo

Enabling encryption (USB and Key Manager)
Using encryption

Accelerate with IBM Storage Webinars

The Free IBM Storage Technical Webinar Series Continues in 2017...

Washington Systems Center – Storage experts cover a variety of technical topics.

Audience: Clients who have or are considering acquiring IBM Storage solutions. Business Partners and IBMers are also welcome.

How to sign up? Information, schedules, and replays:

To automatically receive announcements of upcoming Accelerate with IBM Storage webinars, Clients, Business Partners and IBMers are welcome to send an email request to accelerate-join@hursley.ibm.com.

Located in the Accelerate with IBM Storage Blog:
https://www.ibm.com/developerworks/mydeveloperworks/blogs/accelerate/?lang=en

2017 Webinars:

Jan 19 - Spectrum Virtualize Updates Feb 2 - DS8000 Configuration and Monitoring using the GUI
Mar 9 - Elastic Storage Servers (ESS) and Spectrum Scale Software Solution
Mar 16 - TS7700 Management Classes and Copy Policies - What You Need to Know
Apr 27 - How to Develop a Workload Baseline to Evaluate Flash Storage
May 17 - DS8880 Storage Options for IBM i
June 21 – TS7700 BVIR What You Need to Know
June 22 – FlashSystem A9000 Update
June 29 – DS8880 Thin Provisioning
July 20 – Spectrum Virtualize Encryption
July 24 - Accelerate with Storage Advanced uses of IBM Storage for storage immutability, building air gapped storage and recovery from RansomWare attacks Speakers:

Register Here: https://ibm2.webex.com/ibm2/onstage/g.php?MTID=e5bba23ae811af13ded262deffa7303fd