



August 2020

**IBM® Virtualization Engine TS7770 Series  
Disk Encryption Overview for 3956-CSB  
Version 1.0**

By: Ramón A. Minjares Campos  
IBM Software Engineer  
Guadalajara, México

## Contents

<b>List of figures .....</b>	<b>4</b>
<b>Introduction .....</b>	<b>5</b>
<b>Summary of changes .....</b>	<b>5</b>
<b>Overview .....</b>	<b>5</b>
Introducing encryption.....	6
Encryption technology .....	7
Other important considerations .....	7
<b>Code requirements .....</b>	<b>8</b>
<b>Required TLS version for external encryption.....</b>	<b>8</b>
<b>Encryption .....</b>	<b>8</b>
<b>Defining encryption of data at rest.....</b>	<b>9</b>
<b>Encryption using USB flash drives (Local encryption).....</b>	<b>10</b>
<b>Features .....</b>	<b>10</b>
Local encryption enablement.....	10
EKM Migration Support .....	10
Regeneration of keys support (Rekeying) .....	11
Always-on Encryption .....	11
Cryptographic Disk Erase .....	11
<b>Prerequisites.....</b>	<b>11</b>
TS7700 Virtualization Engine Microcode .....	11
TS7700 Virtualization Engine Hardware.....	12
<b>Installation .....</b>	<b>12</b>
<b>Maintenance .....</b>	<b>12</b>
<b>Encryption using key servers (External encryption) .....</b>	<b>12</b>
<b>Supported key server versions for 3956-CSB .....</b>	<b>13</b>
<b>Features .....</b>	<b>13</b>
On Demand Enablement .....	13
Locally Managed Keys Migration.....	13
Regeneration of keys (Rekeying) and Key Backup .....	13
Single ISKLM Primary Key Store.....	14
Always-on Encryption.....	14
Cryptographic Disk Erase .....	14
<b>Prerequisites.....</b>	<b>14</b>
TS7700 Virtualization Engine Microcode .....	15
TS7700 Virtualization Engine Hardware.....	15
ISKLM Microcode .....	15

August 2020

<b>Encryption of Disk Storage using External Key Management .....</b>	<b>15</b>
<b>General configuration for external encryption key server (ISKLM) .....</b>	<b>15</b>
<b>ISKLM configuration.....</b>	<b>16</b>
<b>TS7700 Management Interface configuration .....</b>	<b>19</b>
<b>Adding the EKM's public certificate into the TS7700 trust store. ....</b>	<b>22</b>
<b>Installing the TS7700 HTTPS certificate into the ISKLM trust store .....</b>	<b>23</b>
Downloading the TS7700 HTTPS certificate using TS7700 Management Interface .....	23
Installing the TS7700 certificate into an ISKLM trust store .....	24
<b>Final TS7700 configuration, completing the external encryption enablement .....</b>	<b>25</b>
<b>Maintenance .....</b>	<b>26</b>
<b>TS7700 Proxy diagram.....</b>	<b>26</b>
<b><i>References.....</i></b>	<b><i>27</i></b>
<b>IBM TS7700 5.1.0 Knowledge Center .....</b>	<b>27</b>
<b>IBM Storwize V5000E documentation.....</b>	<b>27</b>
<b>IBM Security Key Lifecycle Manager V4.0.0 documentation.....</b>	<b>27</b>
<b>IBM TS7700 Full Disk Encryption (FDE) V1.3 for 3956-CSA and before .....</b>	<b>27</b>
<b>IBM TS7700 Release 5.0 Guide – Redbook .....</b>	<b>27</b>
<b>IBM TS7700 Virtualization Engine Information Center .....</b>	<b>27</b>
<b><i>Disclaimers.....</i></b>	<b><i>28</i></b>

## List of figures

Figure 1 - Creating device group in the ISKLM.....	17
Figure 2 - Displaying the device groups and device family .....	17
Figure 3 - Welcome page displaying the key and device management .....	18
Figure 4 - Menu to add new authorized devices to a device group .....	19
Figure 5 - Feature Licenses panel displaying external feature codes .....	20
Figure 6 - Data at Rest Encryption configuration .....	20
Figure 7 - ISKLM welcome page to display Available Protocols .....	21
Figure 8 - Security Settings panel to display SSL/TLS level in the TS7700.....	21
Figure 9 - Add a certificate to the TS7700 Trust Store.....	22
Figure 10 - Fill the retrieve signer information of the EKM server(s) .....	22
Figure 11 - Assigning an alias if the connection was succeeded .....	23
Figure 12 - Downloading and saving the TS7700 certificate .....	24
Figure 13 - Importing the TS7700 certificate into the ISKLM trust store.....	25
Figure 14 - Imported TS7700 certificate .....	25
Figure 15 - TS7700 eidaemon proxy diagram to support 3956-CSB .....	26

August 2020

## Introduction

The IBM Virtualization Engine TS7700 Series is the latest in the line of tape virtualization products that has revolutionized the way mainframe customers utilize their tape resources. Security of the information stored on the internal disk subsystem used to virtualize tape has become important to many customers. The TS7770 (collectively called TS7700 hereon) internally use a disk encryption to store or cache virtual tape volumes. The IBM TS7700 disk subsystem model 3956-CSB have been enhanced to support disk encryption, 3956-CSB was introduced from TS7700 8.50.0.134. Additionally, these subsystem model support externally managed disk encryption of data at rest. This support protects against the potential exposure of sensitive user data and user metadata that is stored on discarded, lost, or stolen storage devices. The 3956-CSB supports IBM Security Key Lifecycle Manager server to handle key management on the cache (called External Encryption enablement) and USB flash drives to enable encryption and copy a key to the cache (called Local Encryption enablement). This white paper describes the general use of the data encryption on 3956-CSB disk storage subsystem when used in the TS7700 Virtualization Engine (VE).

## Summary of changes

Version 1.0 – August 2020    This is the initial version of this document.

## Overview

The importance of data protections has become increasingly apparent with new reports of security breaches, loss and theft of personal and financial information, and government regulation. Encryption of the disk internal to the TS7700 helps control the risks of unauthorized data access without excessive security management burden or subsystem performance issues.

The 3956-CSB supports two methods of configuring encryption. Disk cache storage subsystem can use a centralized key server that simplifies creating and managing encryption keys on the cache subsystem. This method of encryption key management is preferred for security and simplification of key management. In addition, the disk cache storage subsystem also supports storing encryption keys on USB flash drives. USB flash drive-based encryption requires physical access to the disk cache storage subsystem. For organizations that require strict security policies regarding USB flash drives, the 3956-CSB supports the change of encryption type Local USB to External encryption key management via TS7700 service menus.

When encryption is activated and enabled on the 3956-CSB, valid encryption keys must be present on the disk cache storage subsystem when the cache unlocks the drives, or the user generate a new key. If the key server is enabled on the 3956-CSB, the key is retrieved from the

key server. If USB encryption is enabled on the 3956-CSB, the encryption key must be stored on the USB flash drives that contain a copy of the key that was generated when encryption was enabled.

Encryption is a licensed feature that requires a license key to enable it before it can be used.

The 3956-CSB disk cache storage subsystem requires an encryption key to be present during the following operations:

- Cache power-on
- Cache restart
- User initiated rekey operations
- Cache recovery

### Introducing encryption

The following is the information related to the encryption type methods used in 3956-CSB:

- **Hardware encryption:** SAS hardware encryption is specific to the 3956-CSB hardware. After encryption is enabled, all internal storage array objects are created as hardware that is encrypted, by default. Hardware is encrypted within the SAS chip, and the hardware encryption does not consume any additional resources.
- **Software encryption:** Software encryption is specific to the 3956-CSB, and the software is encrypted on external, attached storage at the pool level. Software encryption uses the CPU and the AES\_NI CPU instruction set and engines.

Both methods of encryption protect against the potential exposure of sensitive user data and user metadata that are stored on discarded, lost or stolen storage devices. Both methods of encryption use the same encryption algorithm, the same key management. And, they use the same license.

**Note:** The design for encryption is based on the concept that a 3956-CSB cache is fully encrypted or not encrypted. Encryption implementation is intended to encourage solutions that contain only encrypted volumes or only unencrypted volumes.

The following list of encryption key server and USB flash drive characteristics provide guidance to choose the type of encryption enablement customer want to use.

Key servers can have the following characteristics:

- Physical access to the 3956-CSB is not required to process rekeying operation.
- Support for businesses that have requirements not to use USB ports.

August 2020

- Strong key generation.
- Key self-replication and automatic backups (ISKLM feature functionalities).
- Implementations follow an open standard that aids in interoperability.
- Audit detail.
- Ability to administer access to data separately from storage devices.

USB flash drives have the following characteristics:

- Physical access to the 3956-CSB required to process a rekeying operation.
- No mechanical components to maintain with almost no read operations or write operations to the USB flash drive.
- Inexpensive to maintain and use.
- Convenient and easy to have multiple identical USB flash drives available as backups. (Default are 4 copies, 2 connected to each node canisters, and 2 as backups).

## **Encryption technology**

Data encryption is protected by the Advanced Encryption Standard (AES) algorithm that uses a 256-bit symmetric encryption key in XTS mode, as defined in the IEEE 1619-2007 standard and NIST Special Publication 800-38E as XTS-AES-256. The data encryption key is itself protected by a 256-bit AES key wrap of a key derived from the access key stored on the USB flash drive or a key server. The wrapped key is stored in the disk subsystem controllers in non-volatile form.

## **Other important considerations**

The disk drive encryption is at the cluster level (disk cache controller) and whether the cluster is in a Grid or not, does not matter. The grid boxes support any type of combination of TS7700's: No Encryption / Local Encryption / External Encryption (Key Servers) / Tape Encryption.

Regarding the 3956-CSB disk encryption, it supports encryption for data at rest. That means, encryption is performed by the controller enclosures for data stored within the entire 3956-CSB/XSB system (the controller enclosure and all attached expansion enclosures). So, unlike 3956-CSA, 3956-CSB perform the encryption by controller enclosures. And 3956-CSA and before use SDE/FDE.

August 2020

When drive encryption is written to the disk, it is encrypted. When data is read from the disk, it is decrypted. The data on the fly in the Grid network is not encrypted by the disk cache encryption. If required, another feature, Secure Data Transfer, is required.

## Code requirements

Disk encryption was first introduced with the TS7700 Virtualization Engine microcode version 8.21.0.19 in January 2012. The first version only supported Local key encryption management. Starting with microcode version 8.50.0.134 introduced in November 2019, the TS7700 add support for 3956-CSB model, with two types of encryption enablement: Internal (USB flash drive based) and External (Key server managed based). The external key management function requires an ISKLM server.

## Required TLS version for external encryption

IBM Security Key Lifecycle Manager key servers supports Key Management Interoperability Protocol (KMIP), which is a standard for encryption of stored data and management of cryptographic keys. This version supports SSL/TLS, IBM Security Key Lifecycle Manager use Transport Layer Security version 1.2 (TLS v1.2).

## Encryption

The 3956-CSB storage subsystem supports local and external disk encryption. Unlike the 3956-CSA model however, encryption needs to be pre-set from the beginning in manufacturing. This is because the 3956-CSB system needs to start encryption as soon as the arrays are created. If any array is created without encryption and a customer decides it now wants encryption, the array will have to get deleted and recreated but with encryption enabled. This will be very inconvenient to the customers as it will result in the loss of any existing non-migrated data because of the array deletions.

The encryption solution for 3956-CSB requires its enablement pre-set in manufacturing. This encryption enablement setting will be stored in TS7700 vital product data (VPD). As mentioned before, there are two types of encryption that the 3956-CSB supports: Local or External. Local encryption requires at least one USB drive be present in the node canisters. This USB drive contains the obfuscated encryption key which is needed by the canisters. If the USB key is not present / missing or if it's corrupted/invalid, the data will not be accessible, and the disk subsystem will not fully power on / initialize. Another solution which does not require USB drives is External management. External key management removes the need for a USB key

because it instead obtains/stores the encryption key from an IBM Secure Key Lifecycle Manager (ISKLM) server. The 3956-CSB system allows for the migration from Local to External key management on-demand, concurrently, and without having to erase the array configuration. Because manufacturing needs to ship the disk storage system with arrays created, all the TS7700 with 3956-CSB's systems that are encryption enabled will be shipped with Local encryption, but with a EKM certificate in place. The EKM certificate is currently getting installed by manufacturing for CSA external encryption and this will continue for 3956-CSB storage subsystem model. The EKM certificate allows secure communication to/from the encryption setting just like manufacturing does in 3956-CSA. If customer want to move from Internal to External encryption they can do that at any time after the TS7700 has been installed at the customer's site and the TS7700 has been activated. The move from Local to External will be done using the same TS7700 service menus mechanism as for the older 3956-CSA systems. This mechanism employs a TS7700 service menu option where an SSR initiates Local to External migration and then performs the needed steps. The panel asks for the External Key Manager (EKM) information such as Ips and ports and issues the needed commands to migrate from Local to External disk encryption in all applicable strings.

## Defining encryption of data at rest

Encryption is the process of encoding data so that only authorized parties can read it. Secret keys are used to encode the data according to well-known algorithms.

Encryption of data at rest is defined by the following characteristics:

- “Data at Rest” means that the data is encrypted on the end device (drives).
- The algorithm that is used is the Advanced Encryption Standard (AES) US government standard from 2001.
- Encryption of data at rest complies with the Federal Information Processing Standard 140 (FIPS-140) standard, but it not certified.
- Ciphertext stealing (XTS)-AES 256 is used for data keys.
- AES 256 is used for master keys.
- The algorithm is public. The only secrets are the keys.
- The symmetric key algorithm is used. (The same key used to encrypt and decrypt data).

Encryption for data at rest is full data encryption on data storage (that is, at storage system). *Host to storage communication is not encrypted.*

## Encryption using USB flash drives (Local encryption)

The 3956-CSB can use USB flash drives to enable disk encryption and copy a key to the disk storage system. Encryption process create system encryption keys and write those keys to all USB flash drives.

Two options are available for accessing key information on USB flash drives.

- USB flash drives left inserted in the disk storage system at all times (recommended option). If restart operation is requested to be done automatically, minimum of one USB flash drive must be left inserted in the canisters on the disk storage system. When it is powered on, all canisters then have access to the encryption key. This method requires physical environment where the disk storage system is located is secure. If the location is secure, it prevents an unauthorized person from making copies of the encryption keys, stealing the disk storage system, or accessing data that is stored on the disk storage system. If a USB flash drive that contains valid encryption keys is left inserted in both of the two canisters, the disk storage systems always has access to the encryption keys and the user data on the drives is always accessible.
- USB flash drives are not left inserted into the disk storage system except as required. For the most secure operation, do not keep the USB flash drives inserted into the canisters on the disk storage system. However, this method requires that you manually insert the USB flash drives that contains copies of the encryption key in the canister during operations that requires an encryption key to be present. USB flash drives that contain keys must be stored securely to prevent theft or loss. During operations that the disk storage system requires an encryption key to be present, the USB flash drives must be inserted manually into each canister so data can be accessed. After the disk storage system completes unlocking the drives, the USB flash drives must be removed and stored securely to prevent theft or loss.

## Features

### *Local encryption enablement*

Disk-encryption is enabled with Local Managed Encryption Keys at manufacturing. This needs to be pre-set from the beginning. The 3956-CSB needs to be encrypted before creating array disk configuration.

### *EKM Migration Support*

Any TS7700 configured with Local Key Management can be easily migrated to External Key Management for future needs. Migration to External Key Management is concurrent with customer operations.

### ***Regeneration of keys support (Rekeying)***

Any TS7700 configured with Local Key Management encryption can be re-keyed with new encryption keys on-demand with no downtime and no performance loss during or after the re-key operation. The re-key operations can be initiated from the TS7700 service menus, strictly physical access to the disk storage system is required to process a rekeying operation.

Rekeying is the process of creating a new key for the disk storage system. Before creating a new key, ensure that at least one USB port contains a USB flash drive that contains the current and valid key. During the rekey process, a new key is generated and copied to the USB flash drives (default rekey generation is four new copies, which two are expected to be connected and two more as backup drives). The new key is then used instead of the current key. The rekey operation fails unless at least one USB flash drive contains the current key. To rekey the disk storage system, you need at least four USB flash drives to store the copied key material.

### ***Always-on Encryption***

Once encryption is enabled it cannot be disabled unless Cryptographic Disk Erase is performed.

### ***Cryptographic Disk Erase***

Cryptographic Disk Erase allows customers to erase the disk subsystem by securely erasing all copies of the encryption keys only. This feature does not do Secure Data Overwrite as actual data is not erased. Instead, this feature code securely erases only the encryption keys such that any knowledge of such keys is forgotten. Without any means of retrieving the encryption key. Cryptographic Disk Erase is meant to complement the Cluster Cleanup feature code (4017). Cryptographic Disk Erase in conjunction with Cluster Cleanup is the only way available of disabling encryption and returning the disk storage system to its un-encrypted state.

## **Prerequisites**

The feature for disk encryption support local encryption needs to be pre-set at manufacturing. Local encryption enablement should be requested when an order is placed for TS7770. If they are correctly ordered in place, these machines arrive with Local Encryption already enabled and installed.

### ***TS7700 Virtualization Engine Microcode***

The Virtualization Engine (VE) must be running microcode level 8.50.0.134 or higher for the cache model 3956-CSB. The disk encryption feature code is installed and configured at manufacturing.

August 2020

### ***TS7700 Virtualization Engine Hardware***

All TS7770 with 3956-CSB are totally hardware compatible for encryption configuration.

## **Installation**

Local encryption enablement should be requested when an order is placed for TS7700 with 3956-CSB. Local encryption is pre-set at a manufacturing line. The feature code is installed and configured in manufacturing line.

The USB encryption keys will be attached to the side of the 3956-CSB cache controller rail. The ship will come with USB cache encryption keys. And prior to activate microcode in the TS7700 for First Time Install process, USB flash drives containing the encryption keys are expected to be connected.

Encryption is completely transparent operation of the TS7700. Once activated, encryption cannot be disabled. However, keys can be re-generated or backed up to external media at any time by IBM service representative from the VE service menu.

## **Maintenance**

There are no additional maintenance requirements with locally managed disk encryption.

## **Encryption using key servers (External encryption)**

Encryption key servers create and manage encryption keys that are used by the 3956-CSB. Key servers distribute keys remotely without requiring physical access to the disk storage systems. For security and simplification of key management, key servers are the preferred method of managing encryption keys on the disk storage system.

A key server is a centralized system that generates, stores, and send encryption keys to the disk storage system. The TS7700 with 3956-CSB supports IBM Security Key Lifecycle Manager to handle key management on the disk storage system. ISKLM is a management application that creates and manage cryptographic keys for the disk storage system and provide access to these keys through a certificate. Authentication takes place when certificates are exchanged between the disk storage system and the key server. Certificates must be managed closely because expired certificates can cause disk storage system outages. Key servers must be installed and configured before they are defined on the 3956-CSB storage subsystems.

IBM Security Key Lifecycle Manager key server support Key Management Interoperability Protocol (KMIP), which is a standard for encryption of stored data and management of cryptographic keys.

August 2020

Externally managed encryption stores the lock key to the encryption key inside an IBM Secure Key Lifecycle Manager (ISKLM) server. And ISKLM server is separate and independent from the TS7700 system. A minimum of one key server is required in order to enable the key server support.

## **Supported key server versions for 3956-CSB**

The 3956-CSB model does not support IBM Security Key Lifecycle Manager versions older than 2.7.

The following are the supported version of IBM SKLM:

- IBM SKLM 2.7
- IBM SKLM 3.0
- IBM SKLM 4.0

## **Features**

### ***On Demand Enablement***

Disk-encryption can be enabled with Externally Managed Encryption Keys concurrent with customer operations. This ensures no customer downtime. Additionally, there is no performance degradation during or after encryption enablement even on systems with large amounts of active stored data in the disk subsystem.

### ***Locally Managed Keys Migration***

Migrating from External to Local Key Management is not supported.

### ***Regeneration of keys (Rekeying) and Key Backup***

If external encryption enablement is configured to manage encryption keys, 3956-CSB can generate new keys with the encryption key servers.

Rekeying is the process of creating a new key for the disk storage system. To create a new key, encryption must be enabled on the disk storage system.

During the rekey process, the key server generates a new key and the existing key becomes obsolete. In configurations with a single primary key server and multiple secondary key servers, only the primary key server is updated during the rekey operation.

Any TS7700 configured with External Key Management Encryption will depend on the ISKLM server to manage the encryption keys. The TS7700 does not support backing up the encryption keys to external media such as DVD discs, USB flash drives, etc. Instead, the ISKLM itself must be used to perform key backups. The TS7700 support re-key, however. From the TS7700 service menu, a request can be sent to the ISKLM to issue a new key to the disk subsystem for the re-key. The TS7700 does not store any encryption key permanently. All copies of the encryption keys will remain only in the ISKLM indefinitely. The TS7700 supports up to two synchronized ISKLM servers for redundancy.

### ***Single ISKLM Primary Key Store***

The disk cache model 3956-CSB used by the TS7700 are assigned encryption keys by the ISKLM primary key store using sequential key labels. Two or more independent primary key stores connected to two or more TS7700 cluster can be used, but their key stores must remain independent forever. Any future merging of primary key stores when two or more key stores have assigned keys to different TS7700's can lead to key label collisions. Though the actual encryption keys are unique, the labels associated with them can conflict. Therefore, it's best to use a single primary key store, which can have many synchronized children, secondaries or clones. If two primary key stores are required, the keys handed out to the attached TS7700's can never be consolidated through key store merging.

### ***Always-on Encryption***

Once encryption is enabled it cannot be disabled unless Cryptographic Disk Erase is performed via Manufacturing Cluster Cleanup.

### ***Cryptographic Disk Erase***

Cryptographic Disk Erase allows customers to erase the disk subsystem by securely erasing all copies of the encryption keys only. This feature does not do Secure Data Overwrite as actual data is not erased. Instead, this feature code securely erases only the encryption keys such that any knowledge of such keys is forgotten. Without any means of retrieving the encryption key all previously written data inside every DDM will be undifferentiated from random or meaningless data. Cryptographic Disk Erase is meant to complement the Cluster Cleanup feature code. Cryptographic Disk Erase in conjunction with Cluster Cleanup is the only way available of disabling encryption and returning the disk storage system to its un-encrypted state.

### **Prerequisites**

In order to enable external encryption in 3956-CSB, local encryption enablement should be present in the TS7700. That means if a TS7700 with 3956-CSB is ordered to be External Encryption:

- Manufacturing will prepare the TS7700 installing Local encryption enablement.

August 2020

- Customer install the box via First Time Install in customer's site.
- Once box is activated, the feature for disk encryption support is customer-installable, actual enablement may require configuration by an IBM Service representative.

### ***TS7700 Virtualization Engine Microcode***

The Virtualization Engine (VE) must be running microcode level 8.50.0.134 or higher for the cache model 3956-CSB. The disk encryption feature code must be installed to access the encryption settings on service panels. Additionally, a second feature code that install an ISKLM communication certificate in the TS7700 may be needed as well.

### ***TS7700 Virtualization Engine Hardware***

All TS7770 with 3956-CSB are totally hardware compatible for encryption configuration.

### ***ISKLM Microcode***

The TS7700 currently only supports ISKLM running on Linux or Windows. ISKLM for z/OS is not currently supported. The minimum version of supported ISKLM is 2.7.

IBM Security Key Lifecycle Manager key server supports Key Management Interoperability Protocol (KMIP), which is a standard for encryption stored data and management of cryptographic keys.

TS7700 vital product data (VPD) can be analyzed by IBM service representatives to ensure existing hardware, software and feature codes meet the above requirements.

## **Encryption of Disk Storage using External Key Management**

In order to enable external encryption in 3956-CSB using IBM Security Key Lifecycle Manager key server, user must create a device group, in addition to name, IP address, port and certificate information. The *device group* is a collection of security credentials (including keys and group of keys) that allows for restricted management of subsets of devices with a larger pool. The 3956-CSB disk storage system must be defined on the key server to the **SPECTRUM\_VIRT** device group. If the **SPECTRUM\_VIRT** device groups does not exist on the key server, it must be created based on the GPFS device family. This needs to be defined as well in the additional key servers.

## **General configuration for external encryption key server (ISKLM)**

August 2020

Ensure that the following tasks are completed on the IBM Security Key Lifecycle Manager before performing external encryption enablement:

1. Define the IBM Security Key Lifecycle Manager to use Transport Layer Security version 1.2 (TLS V1.2). The default setting on IBM Security Key Lifecycle Manager is TLSv1, but the 3956-CSB only supports version 1.2. On the IBM Security Key Lifecycle Manager, set the values to **SSL\_TLSv2**, which is a set of protocols that includes TLSv1.2.
2. Ensure that the database service is started automatically.
3. Ensure that a valid SSL certificate from IBM Security Key Lifecycle Manager is installed on the system and in use. If automatic replication is configured on IBM Security Key Lifecycle Manager, then this certificate needs to be uploaded to the system once. However, if automatic replication is not configured on the IBM Security Key Lifecycle Manager, a certificate for the additional key server must be uploaded to the system.
4. Specify the **SPECTRUM\_VIRT** device group for the system definition. If you are configuring multiple key servers, the **SPECTRUM\_VIRT** device group must be defined on the primary and the secondary key server.
5. If the TS7700 + 3956-CSB currently have encryption enabled with USB flash drives, at least one of the USB flash drives must be inserted into the disk storage system before key servers can be configured for managing keys.

## ISKLM configuration

An administrator of the ISKLM server is required to enable and setup the ISKLM in order for key exchanges to be handled by the ISKLM. The TS7700 has no control of the ISKLM configuration. The TS7700 simply act as a proxy to pass internal request for keys by the controllers to the ISKLM and vice versa. Therefore, the first step is to setup the ISKLM server for key exchanges. The actual steps to configure the ISKLM can vary based on the operating system or ISKLM version. Because of that reason, please consult with an ISKLM administrator for the correct or updated instructions.

As a general guideline, the following instructions can be used to configure an ISKLM server:

1. Open the ISKLM management window and log in using and Admin ID
2. Create a new key-store if not done already (expected and normal case is that it is already created). “Click here to create the master keystore”.
3. Click on Advanced Configuration > Device Group > Create, to create a new device group based on an existing device family. For device group: **SPECTRUM\_VIRT**. And for device family: **GPFS**

IBM Security Key Lifecycle Manager

Welcome | Configuration | **Advanced Configuration** | Administration | Clients | Search

You can create a new device group based on an existing device family.

You cannot delete a device group if there are cryptographic objects or devices associated with it.

Create | Delete

No filter applied

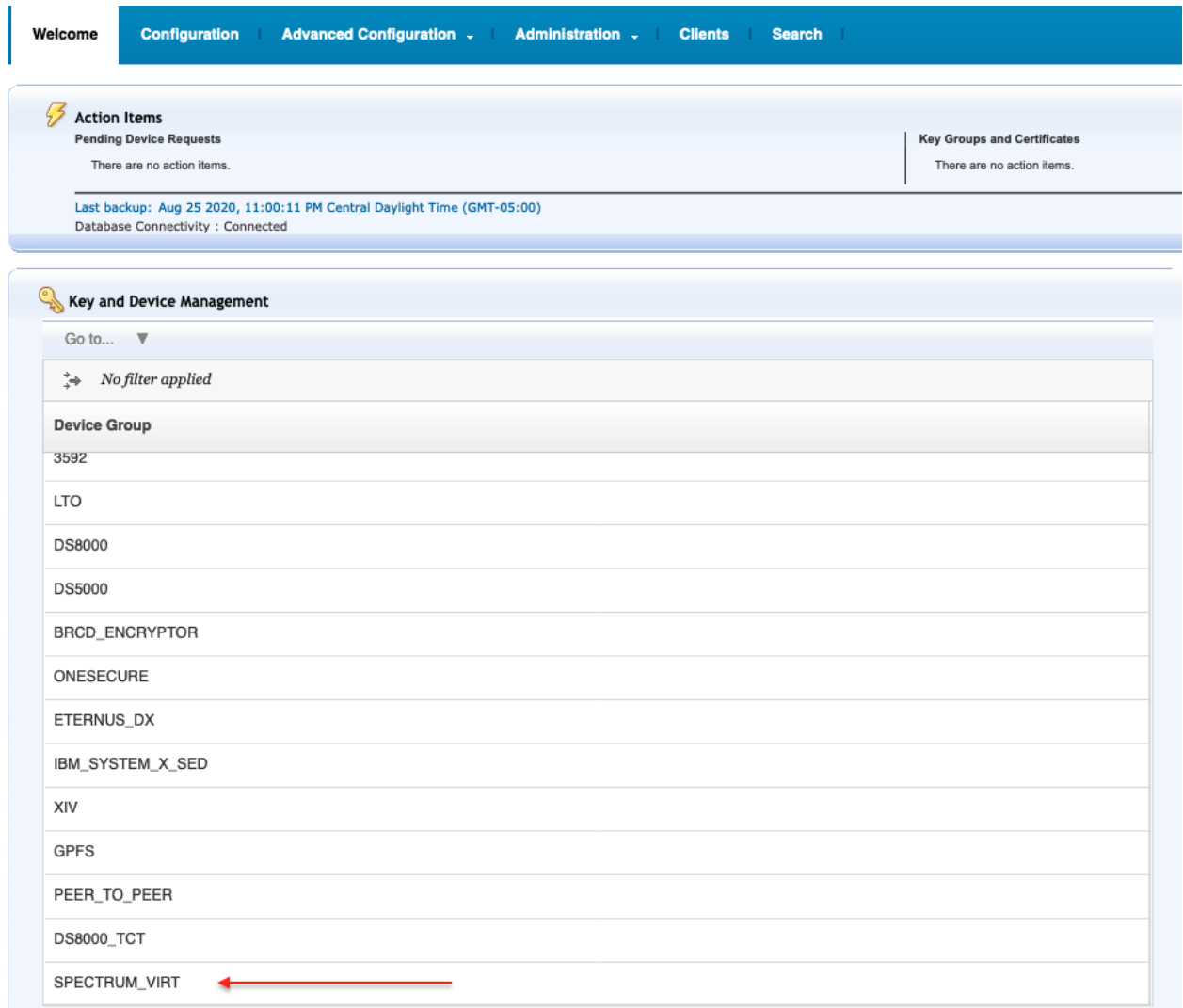
Device Group	Device family:
<b>Create Device Group</b>	
<p>*Device family:</p> <p> <input type="radio"/> Many asymmetric keys to many devices (3592)  <input checked="" type="radio"/> Many devices to many keys with access via certificate (GPFS)  <input type="radio"/> Many symmetric keys to many devices (LTO)  <input type="radio"/> Symmetric Keys directly tied to a single device (DS5000) <input type="checkbox"/> Enable machine affinity  <input type="radio"/> Two devices and many symmetric keys (PEER_TO_PEER)         </p> <p>*Device group name:</p> <p><input type="text" value="SPECTRUM_VIRT"/></p> <p> <input type="button" value="Create"/> <input type="button" value="Cancel"/> </p>	

Figure 1 - Creating device group in the ISKLM

Device Group	Device family:
BRCD_ENCRYPTOR	LTO
ONESECURE	DS5000
ETERNUS_DX	DS5000
IBM_SYSTEM_X_SED	DS5000
XIV	DS5000
DS8000_TCT	GPFS
SPECTRUM_VIRT	GPFS

Figure 2 - Displaying the device groups and device family

Contents of a specific device group can be displayed by selecting the target group from the list displayed in the Key and Device Management section under the Welcome page.



**Welcome** | **Configuration** | **Advanced Configuration** | **Administration** | **Clients** | **Search**

**Action Items**  
 Pending Device Requests  
 There are no action items.

**Key Groups and Certificates**  
 There are no action items.

Last backup: Aug 25 2020, 11:00:11 PM Central Daylight Time (GMT-05:00)  
 Database Connectivity : Connected

**Key and Device Management**


Go to... ▼

✚ No filter applied



Device Group
3592
LTO
DS8000
DS5000
BRCD_ENCRYPTOR
ONESECURE
ETERNUS_DX
IBM_SYSTEM_X_SED
XIV
GPFS
PEER_TO_PEER
DS8000_TCT
SPECTRUM_VIRT

Figure 3 - Welcome page displaying the key and device management

- In the Key and Device Management from Welcome panel, right click on **SPECTRUM\_VIRT** and select “**Manage key and devices**”. Then, in the drop-down menu at the bottom of the window, select either the option to **Automatically accept new device requests** or select the option to **Hold new device requests pending my approval**.


**SPECTRUM\_VIRT**

The screen below allows you to add or delete certificate and their associated node name. As well as, modify the node name associated with a certificate. New



Add ▼ Modify Delete

No filter applied		
Certificate UUID:	Name	Endpoint Count
CERTIFICATE-e097e87-70838392-5b01-4318-8988-aa2931689be3	hydra	18

Total: 1 Selected: 0

10 25 50 100 +

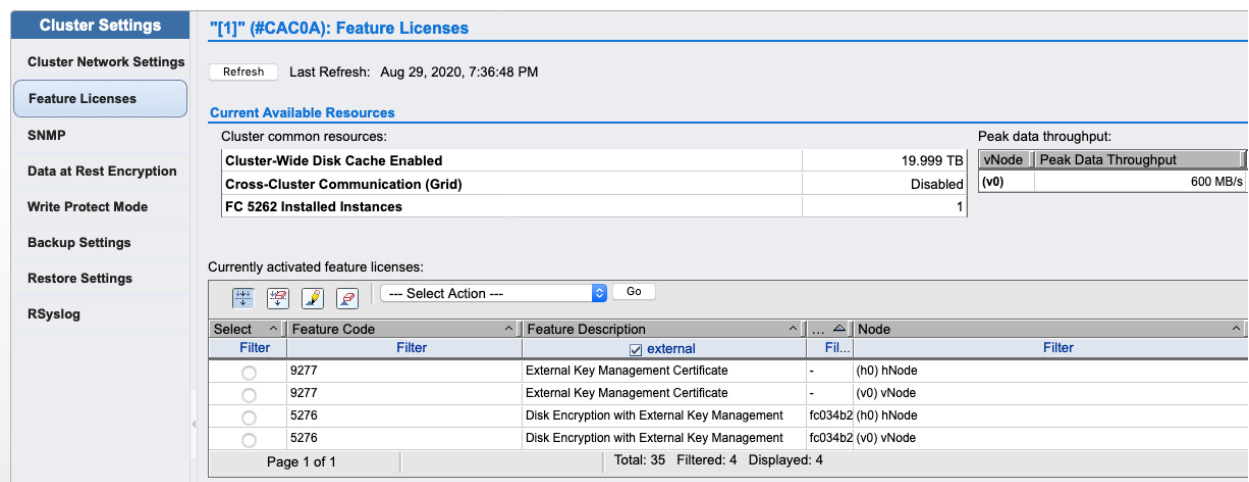
Hold new certificate requests pending my approval

Figure 4 - Menu to add new authorized devices to a device group

## TS7700 Management Interface configuration

As a general guideline, the following instructions can be used to configure an TS7700 Management Interface.

1. All TS7700's coming from manufacturing has installed the External Key Management Certificate (normal process if the machine was first ordered with feature code 9277). In order cases, have an IBM Service representative to install the certificate on-site 5277 using TS7700 Management Interface. If not previously installed, have the IBM Service representative to install feature code 5276 Disk Encryption with External Key Management using TS7700 Management Interface.



**Cluster Settings**

**Cluster Network Settings**

**Feature Licenses**

**SNMP**

**Data at Rest Encryption**

**Write Protect Mode**

**Backup Settings**

**Restore Settings**

**RSyslog**

**"[1]" (#CAC0A): Feature Licenses**

Refresh Last Refresh: Aug 29, 2020, 7:36:48 PM

**Current Available Resources**

Cluster common resources:

Resource	Value
Cluster-Wide Disk Cache Enabled	19.999 TB
Cross-Cluster Communication (Grid)	Disabled
FC 5262 Installed Instances	1

Peak data throughput:

vNode	Peak Data Throughput
(v0)	600 MB/s

**Currently activated feature licenses:**

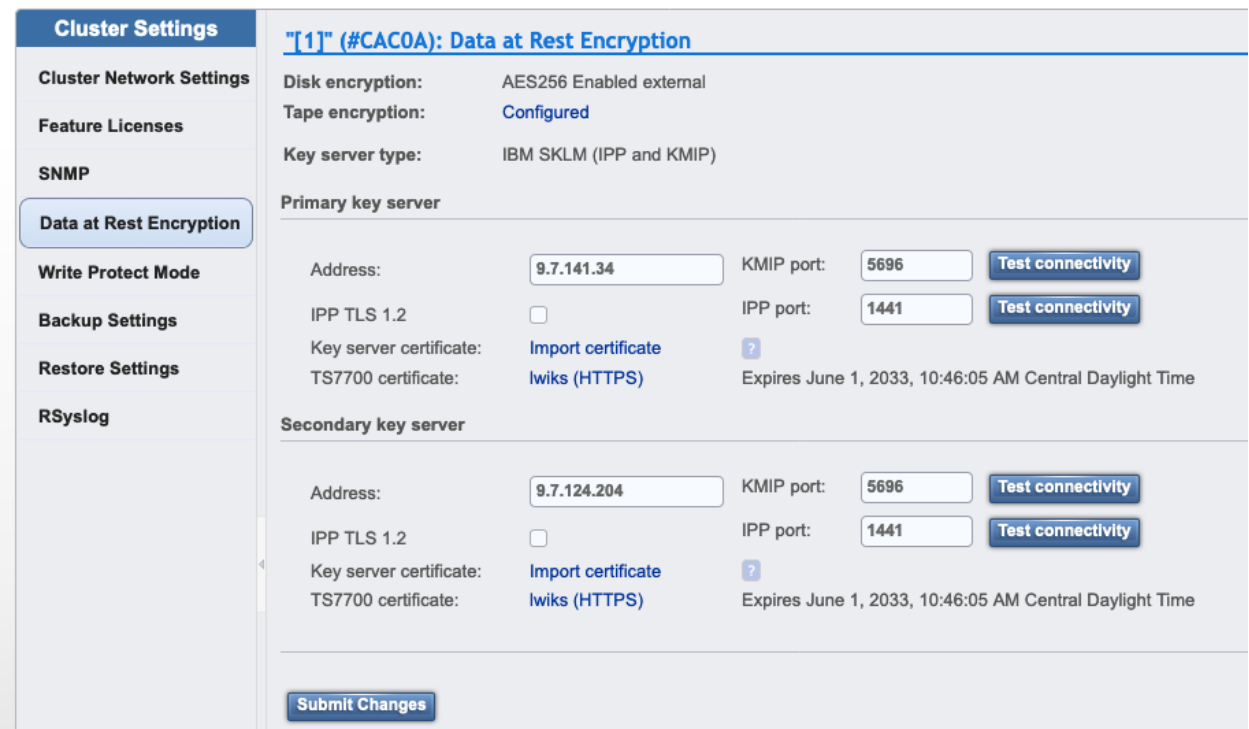
Select Action Go

Select	Feature Code	Feature Description	external	Node
<input type="radio"/>	9277	External Key Management Certificate	<input checked="" type="checkbox"/>	(h0) hNode
<input type="radio"/>	9277	External Key Management Certificate	<input checked="" type="checkbox"/>	(v0) vNode
<input type="radio"/>	5276	Disk Encryption with External Key Management	<input type="checkbox"/>	fc034b2 (h0) hNode
<input type="radio"/>	5276	Disk Encryption with External Key Management	<input type="checkbox"/>	fc034b2 (v0) vNode

Page 1 of 1 Total: 35 Filtered: 4 Displayed: 4

Figure 5 - Feature Licenses panel displaying external feature codes

- Configure the TS7700 to see at least one Encryption Key manager (EKM) server through the same network infrastructure used by the TS7700 Management Interface. This panel is located in **Cluster Settings > Data at Rest Encryption** in the TS7700 Management interface. The communication uses the KMIP protocol for 3956-CSB storage subsystems. It is strongly recommended to have two configured EKM's, which should be replicas of each other for redundancy. You need to submit Network addresses of the target EKM's, and the port configuration.



**Cluster Settings**

**Cluster Network Settings**

**Feature Licenses**

**SNMP**

**Data at Rest Encryption**

**Write Protect Mode**

**Backup Settings**

**Restore Settings**

**RSyslog**

**"[1]" (#CAC0A): Data at Rest Encryption**

Disk encryption: AES256 Enabled external

Tape encryption: Configured

Key server type: IBM SKLM (IPP and KMIP)

**Primary key server**

Address: 9.7.141.34 KMIP port: 5696 Test connectivity

IPP TLS 1.2 ☐ IPP port: 1441 Test connectivity

Key server certificate: Import certificate ?

TS7700 certificate: Iwks (HTTPS) Expires June 1, 2033, 10:46:05 AM Central Daylight Time

**Secondary key server**

Address: 9.7.124.204 KMIP port: 5696 Test connectivity

IPP TLS 1.2 ☐ IPP port: 1441 Test connectivity

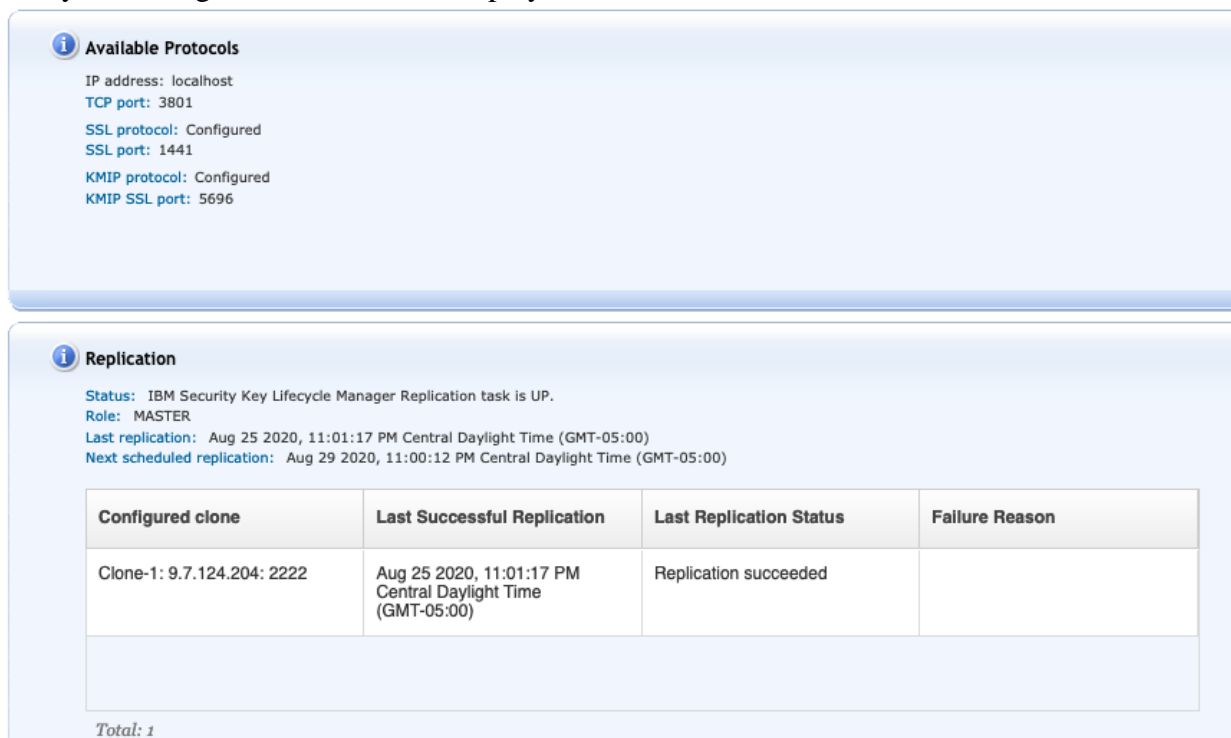
Key server certificate: Import certificate ?

TS7700 certificate: Iwks (HTTPS) Expires June 1, 2033, 10:46:05 AM Central Daylight Time

Submit Changes

Figure 6 - Data at Rest Encryption configuration

You can use the **Welcome Page > Available Protocols** panel in the IBM Security Key Lifecycle Manager GUI in order to display the Available Protocols information:



**Available Protocols**

IP address: localhost  
 TCP port: 3801  
 SSL protocol: Configured  
 SSL port: 1441  
 KMIP protocol: Configured  
 KMIP SSL port: 5696

---

**Replication**

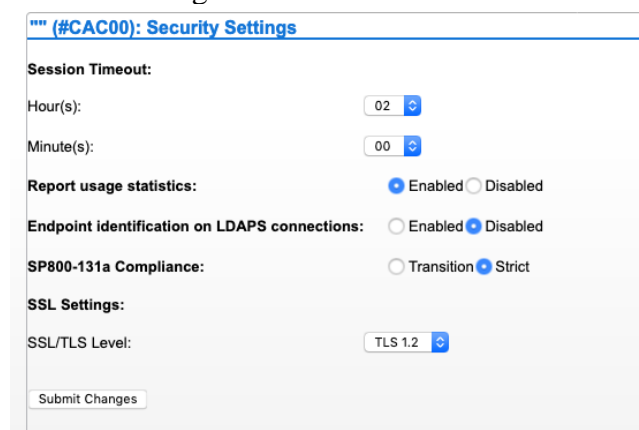
Status: IBM Security Key Lifecycle Manager Replication task is UP.  
 Role: MASTER  
 Last replication: Aug 25 2020, 11:01:17 PM Central Daylight Time (GMT-05:00)  
 Next scheduled replication: Aug 29 2020, 11:00:12 PM Central Daylight Time (GMT-05:00)

Configured clone	Last Successful Replication	Last Replication Status	Failure Reason
Clone-1: 9.7.124.204: 2222	Aug 25 2020, 11:01:17 PM Central Daylight Time (GMT-05:00)	Replication succeeded	

Total: 1

Figure 7 - ISKLM welcome page to display Available Protocols

- TLS v1.2 is the one used by 3956-CSB. It is required when enabling external disk encryption in the TS7700. By default, TS7700 Management Interface is configured to use TLS 1.2, user can easily verify this in the panel: **Access > Security Settings**, using TS7700 Management Interface.



**Security Settings**

Session Timeout:  
 Hour(s): 02  
 Minute(s): 00

Report usage statistics: ☒ Enabled ☐ Disabled

Endpoint identification on LDAPS connections: ☐ Enabled ☒ Disabled

SP800-131a Compliance: ☐ Transition ☒ Strict

SSL Settings:  
 SSL/TLS Level: TLS 1.2

Submit Changes

Figure 8 - Security Settings panel to display SSL/TLS level in the TS7700

## Adding the EKM's public certificate into the TS7700 trust store.

Perform the following steps for each EKM (Encryption Key Manager) to be attached to the TS7700 using a TLS/SSL connection:

1. Log into the TS7700 Management Interface and open the Access > SSL Certificates panel.
2. Select **New certificate**, which will open the **Add certificate** wizard, then select *Retrieve a certificate from server* as method to trust a public key certificate in the **Method to add a certificate** tab

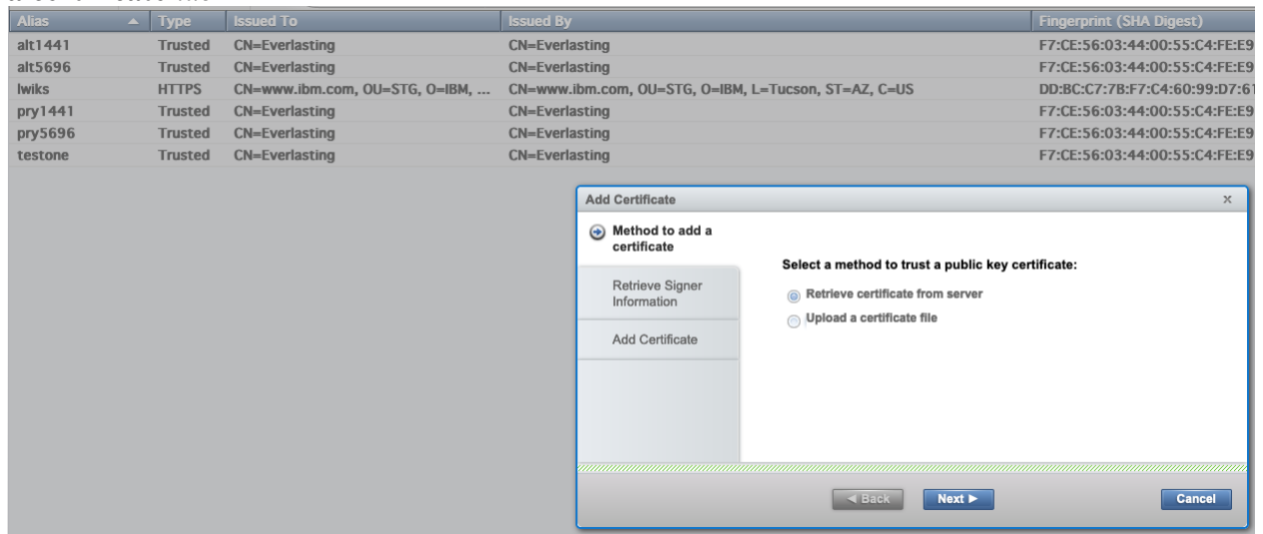


Figure 9 - Add a certificate to the TS7700 Trust Store

3. Fill the information to retrieve the signer information of the EKM's. The default value (port 443) may not be the correct for most of the cases. The correct values are commonly (port 1441 or port 5696).

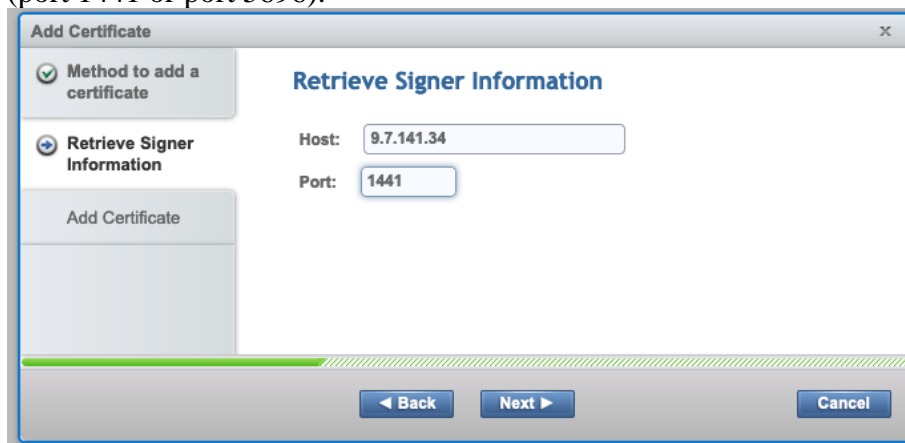


Figure 10 - Fill the retrieve signer information of the EKM server(s)

4. If connection succeeds, the certificate will be retrieved. Select an **Alias** to identify the retrieved certificate. And click **Finish** to complete the process.

Figure 11 - Assigning an alias if the connection was succeeded

**Note:** The EKM trust can also be added manually if you have available the certificate file of the EKM, or its signing Certificate Authority (CA) trust available. You would follow the same steps, but use the Upload Certificate File option when manually adding the trust using the option **Upload a certificate file** from this figure: Figure 9 - Add a certificate to the TS7700 Trust Store

## Installing the TS7700 HTTPS certificate into the ISKLM trust store

By default, the TS7700 uses a self-signed certificate to handle secure HTTPS connections to the Management Interface identified by the LWIKS alias (Lightweight Infrastructure Key Store certificate) included in the TS7700 trust store. However, users of the TS7700 have the option to replace this certificate with a customer-provided one, so make sure that you are using the correct HTTPS certificate for your environment when performing this procedure.

### *Downloading the TS7700 HTTPS certificate using TS7700 Management Interface*

1. Select Cluster Settings > Data at Rest Encryption panel. Click on the **TS7700 certificate / Iwiks (HTTPS)** to save and download the certificate.

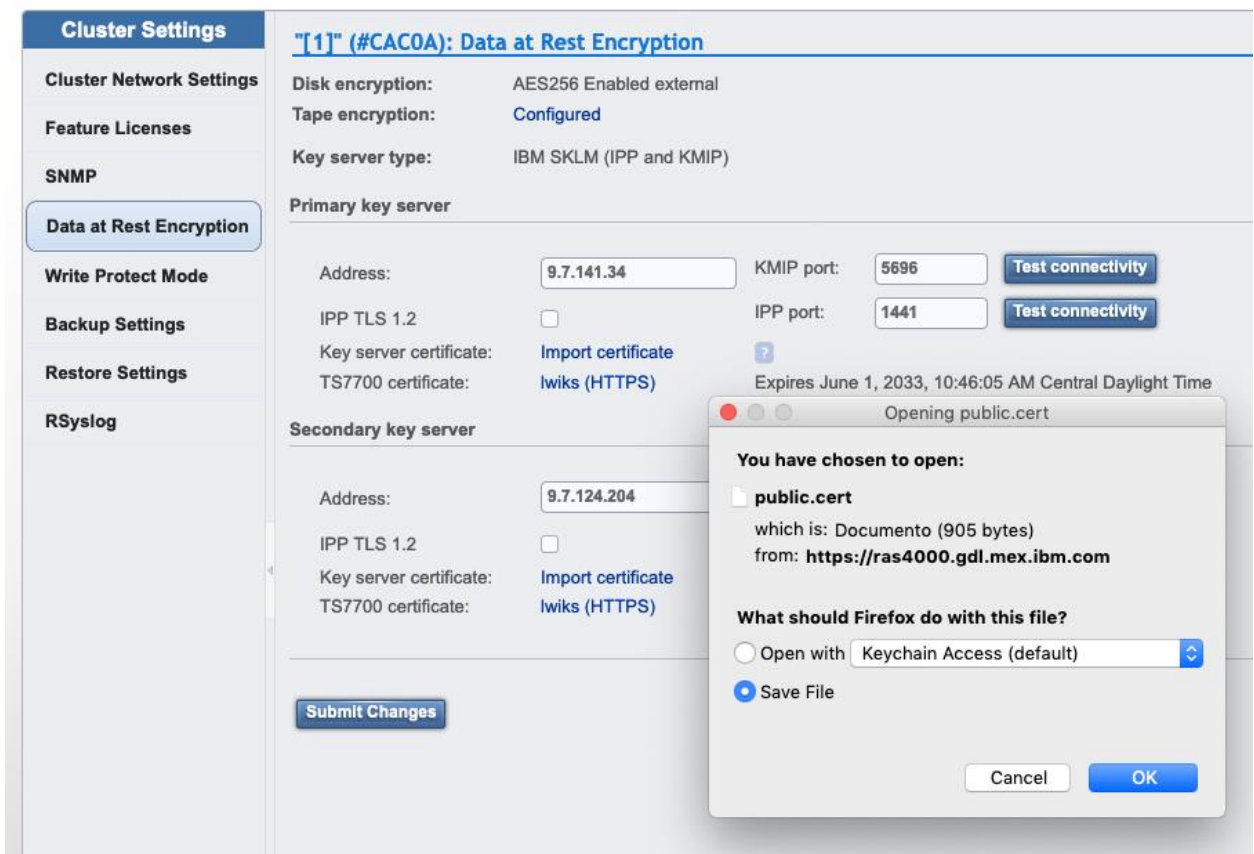


Figure 12 - Downloading and saving the TS7700 certificate

**Note:** If the organization installed a customer-provided certificate on the TS7700 to replace the default Iwiks self-signed certificate, you need to use the organization’s CA’s trust certificate available, and use that directly instead of completing previous steps to download the HTTPS TS7700 Iwiks certificate.

### *Installing the TS7700 certificate into an ISKLM trust store*

1. First recommendation is to rename the “**public.cert**” TS7700 certificate downloaded in previous steps to better identify the certificates in the ISKLM side.
2. Open the ISKLM management window and log in using an Admin ID. Then, select the **Advanced Configuration > Client Device Certificates** panel, then click the **Import** option. Fill the **Certificate name**, and click on **Browse** file to **Select** and upload the certificate. Click on **Allow the server to trust this certificate and communicate with the associated client device**. Final step is just click on **Import** dialog window.

August 2020

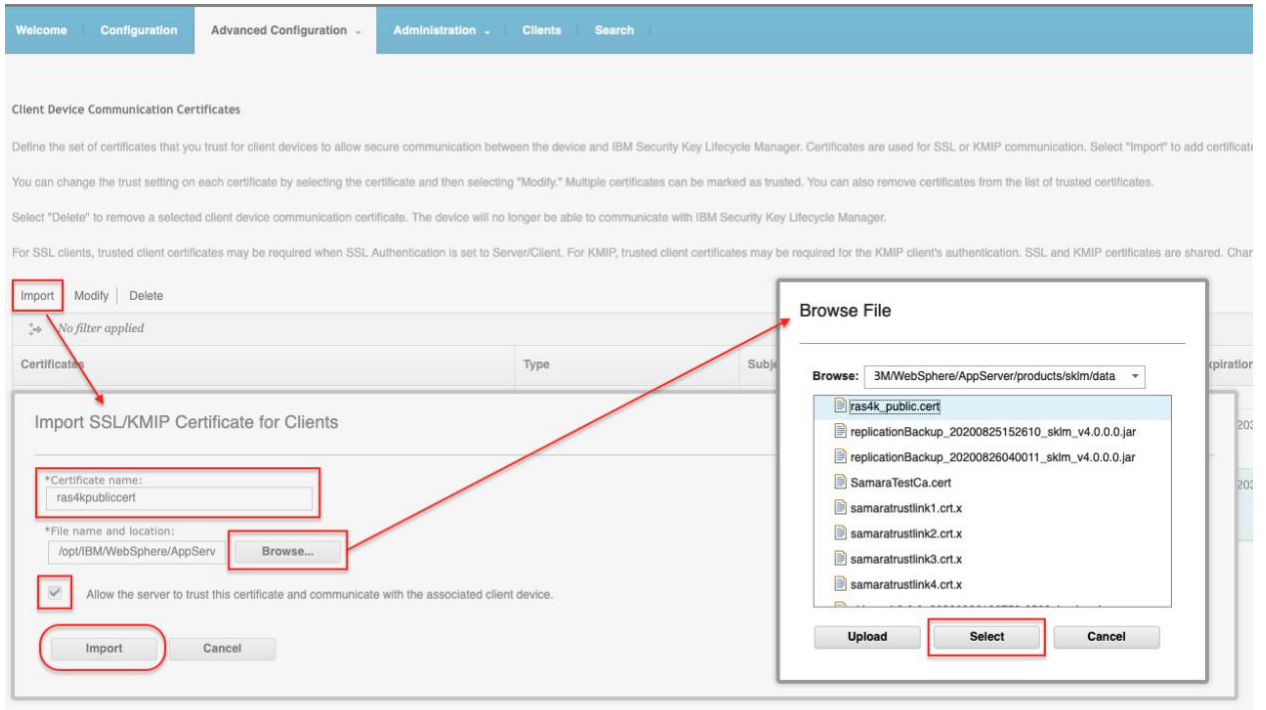


Figure 13 - Importing the TS7700 certificate into the ISKLM trust store

3. Verify the import completed successfully, listing and searching the recently new added certificate.

Certificates	Type	Subject Distinguished Name	Expiration Date
bobtailtest_tucson_ramon	SSL/KMIP	CN=www.ibm.com, OU=STG, O=IBM, L=Tucson, ST=AZ, C=US	Jun 01 2033, 10:46:05 AM Central Daylight Time (GMT-05:00)
ras4kpubliccert	SSL/KMIP	CN=www.ibm.com, OU=STG, O=IBM, L=Tucson, ST=AZ, C=US	Jun 01 2033, 10:46:05 AM Central Daylight Time (GMT-05:00)

Figure 14 - Imported TS7700 certificate

## Final TS7700 configuration, completing the external encryption enablement

Once the ISKLM server has been configured, and also the TS7700 Management Interface has been configured, last part is that an IBM Service representative must complete the enablement of external key Management using the TS7700 service menu.

## Maintenance

There are no additional maintenance requirements with externally managed disk encryption. Due to the transparency of the externally managed encryption, other TS7700 subcomponents upgrades, part replacements, etc. are not affected and will continue to work the same way as systems without disk encryption enabled. The ISKLM server, however, may require additional maintenance.

## TS7700 Proxy diagram

The following is a flow diagram of the TS7700 encryption key manager daemon in support of the 3956-CSB.

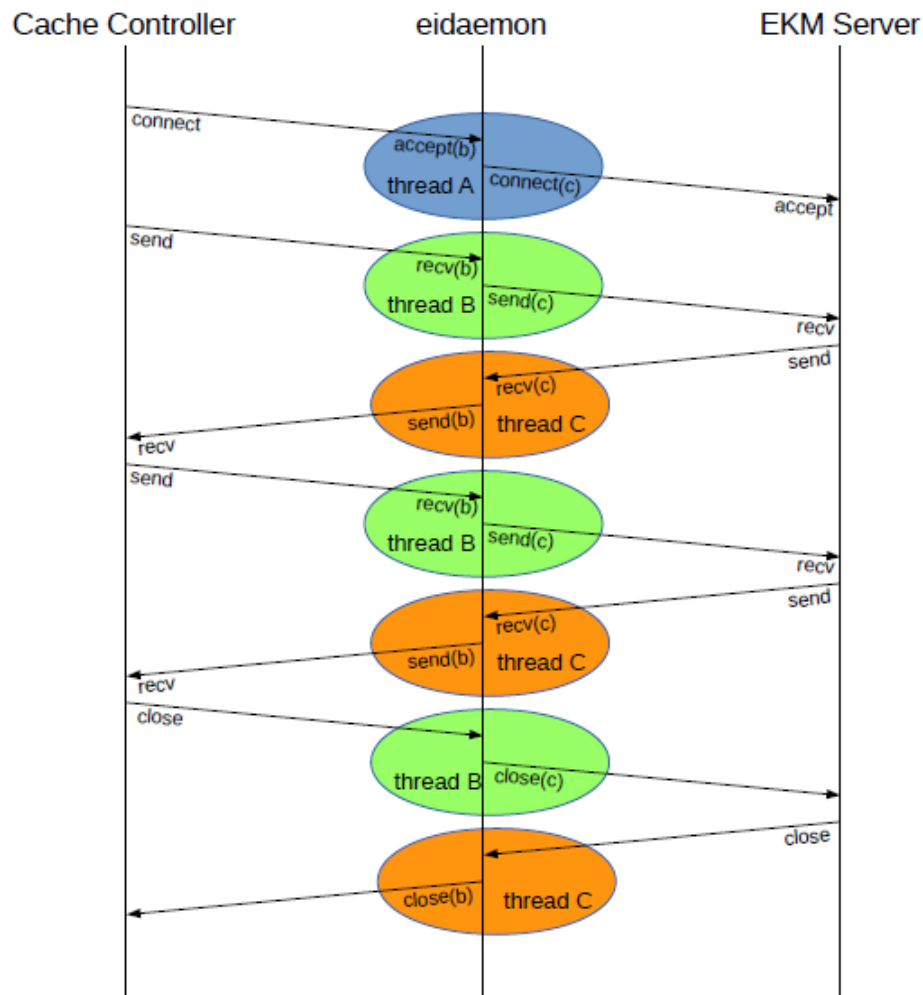


Figure 15 - TS7700 eidaemon proxy diagram to support 3956-CSB

August 2020

## References

### **IBM TS7700 5.1.0 Knowledge Center**

[https://www.ibm.com/support/knowledgecenter/STFS69\\_5.1.0/hydra\\_c\\_ichome.html](https://www.ibm.com/support/knowledgecenter/STFS69_5.1.0/hydra_c_ichome.html)

### **IBM Storwize V5000E documentation**

[https://www.ibm.com/support/knowledgecenter/STHGUI\\_8.2.1/com.ibm.storwize.v5000.821.doc/v5000\\_ichome.html](https://www.ibm.com/support/knowledgecenter/STHGUI_8.2.1/com.ibm.storwize.v5000.821.doc/v5000_ichome.html)

### **IBM Security Key Lifecycle Manager V4.0.0 documentation**

[https://www.ibm.com/support/knowledgecenter/SSWPVP\\_4.0.0/com.ibm.sk1m.doc/welcome.htm](https://www.ibm.com/support/knowledgecenter/SSWPVP_4.0.0/com.ibm.sk1m.doc/welcome.htm)

### **IBM TS7700 Full Disk Encryption (FDE) V1.3 for 3956-CSA and before**

<https://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP102200>

### **IBM TS7700 Release 5.0 Guide – Redbook**

<http://www.redbooks.ibm.com/abstracts/sg248464.html?Open>

### **IBM TS7700 Virtualization Engine Information Center**

<https://www.ibm.com/support/knowledgecenter?origURL=api/redirect/ts7700ic/v1r0/index.jsp>

August 2020

## Disclaimers

Copyright © 2020 by International Business Machines Corporation.

No part of this document may be reproduced or transmitted in any form without written permission from IBM Corporation.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This information could include technical inaccuracies or typographical errors. IBM may make improvements and/or changes in the product(s) and/or programs(s) at any time without notice.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectually property rights, may be used instead. It is the user's responsibility to evaluate and verify the operation of any non-IBM product, program or service.

**The information provided in this document is distributed "AS IS" without any warranty, either express or implied. IBM EXPRESSLY DISCLAIMS any warranties of merchantability, fitness for a particular purpose OR NON-INFRINGEMENT.** IBM shall have no responsibility to update this information. IBM products are warranted according to the terms and conditions of the agreements (e.g., IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. IBM is not responsible for the performance or interpretability of any non-IBM products discussed herein. The customer is responsible for the implementation of these techniques in its environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. Unless otherwise noted, IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

The provision of the information contained herein is not intended to, and does not grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785

August 2020

U.S.A.

#### Trademarks

The following are trademarks or registered trademarks of International Business Machines in the United States, other countries, or both.

IBM, TotalStorage, DFSMS/MVS, S/390, z/OS, and zSeries.

Other company, product, or service names may be the trademarks or service marks of others.