Before the TS7700-VED server and 3956-CSB cache model, the cache models 3956-CC9, 3956-CS9, and 3956-CSA encrypted their data at rest by using the full data encryption (FDE) DDMs, with local or external management of the encryption key (only the IBM Security Key Lifecycle Manager, SKLM, supported). Both cache models 3956-CC9/CS9 and 3956-CSA required IPP key servers for encryption; likewise, the tape encryption. Figure 9-79 shows an example of the *Data at rest Encryption* window.

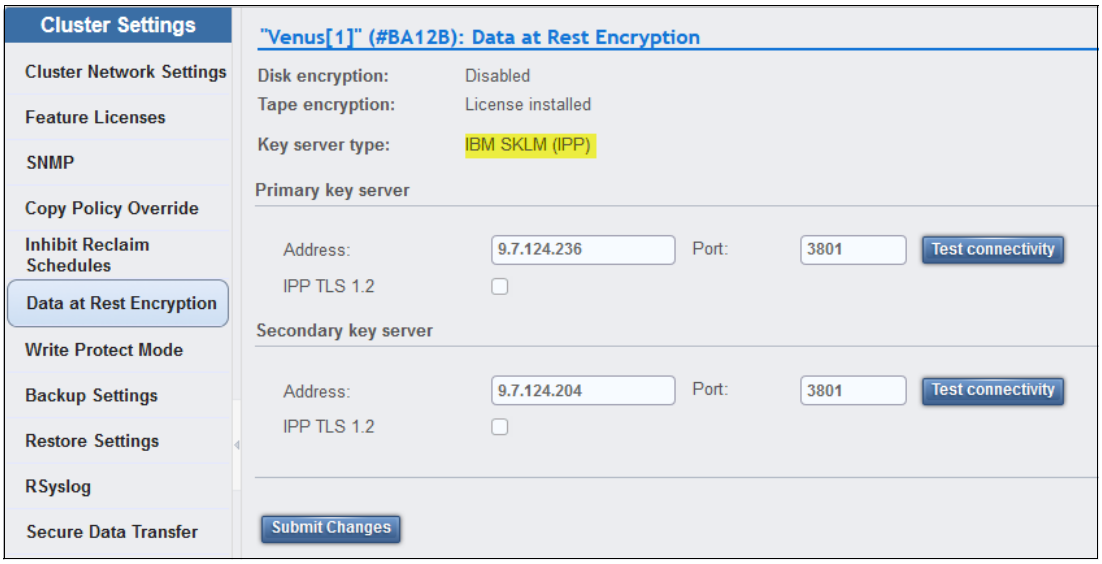

Figure 9-79 Data at rest Encryption using ISKLM (IPP)

The TS7770-VED features a new type of cache, the 3956-CSB. In this cache model, the encryption is performed by the CSB processor at the nodes on control enclosure, which is a different approach from previous models in which the encryption is performed on the FDE-DDMs. In the 3956-CSB, the encrypted data is written into regular DDMs (non-FDE) in the drawers. The DRAID arrays in the CSB cache must be encrypted at creation time at manufacturing.

Consider the following points regarding the CSB cache model:

- FC 5272 Disk Enabled Encryption is not available for field installations on the TS7770. It must be shipped from manufacturing for any encryption.
- FC 7405 must be ordered on every 3956-CSB in the TS7770 configuration.
- FC 7405 provides four USB sticks per 3956-CSB used to store the local encryption keys

Therefore, the External Key Encryption (FC 5276) requires that FC 5272 is installed on the TS7770 server before initial installation. All TS7770 configurations with 3956-CSB /XSB ordered for encryption cache data is always shipped from manufacturing with local key management enabled (FC 5272).

After a TS7770 with FC 5272 is configured in a client environment and can communicate with an external key server, FC 5276 can be activated to transition to external key management.

CSB cache model requires KMIP key servers for encryption. Figure 9-80 on page 493 shows an example of an ISKLM key server configuration for CSB cache encryption (KMIP portion, port 5696) and tape encryption (IPP portion, port 441). The IPP portion uses port 441 because the IPP TLS 1.2 option is selected; otherwise, the default port is still 3801. With the TLS option, we display the option to import a Key Server certificate.