Securing your data in Block Storage

To ensure that you can securely manage your data when you use Block Storage, it's important to know exactly what data is stored and encrypted and how you can delete any stored personal data.

**How your data is stored and encrypted in Block Storage**

IBM Cloud™ Block Storage that is provisioned with either Endurance or Performance option is secured with provider-managed encryption, at no extra cost and no impact to performance.

The provider-managed encryption-at-rest feature uses the following industry standard protocols:

* Industry-Standard AES-256 encryption
* Keys are managed in-house with industry standard Key Management Interoperability Protocol (KMIP)
* Storage is validated for Federal Information Processing Standard (FIPS) Publication 140-2, Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA). Storage is also validated for Payment Card Industry (PCI), Basel II, California Security Breach Information Act (SB 1386), and EU Data Protection Directive 95/46/EC compliance.

**Encryption-at-Rest for Snapshots or Replicated storage**

All snapshots and replicas of encrypted Block Storage are also encrypted by default. This feature can't be turned off on a volume basis.

**Provisioning Storage with Encryption**

The provider-managed encryption-at-rest feature is available for Block Storage that is provisioned in [most data centers](https://cloud.ibm.com/docs/BlockStorage?topic=BlockStorage-selectDC). All storage that is ordered in these data centers is automatically provisioned with encryption.

When you order Block Storage, select a data center noted with an asterisk (\*). You can see a lock icon to the right of the LUN/Volume Name field that indicates that the volume is encrypted.

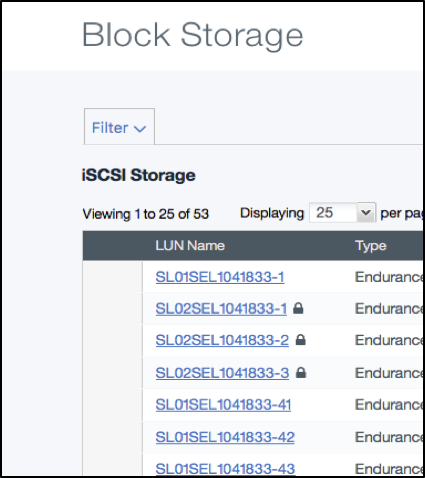


Figure 1. Example of the lock icon that shows that the LUN is encrypted.

Non-encrypted storage that was provisioned before the data center was upgraded **isn't** automatically encrypted. If you own non-encrypted storage in an upgraded data center and you want encrypted storage, then you need to create a new volume and migrate your data. For more information, see [Block Storage Migration in Upgraded Data Centers](https://cloud.ibm.com/docs/BlockStorage?topic=BlockStorage-migratestorage).

**Deleting Block Storage instances**

If you no longer need a specific LUN, you can cancel it at any time. IBM Cloud™ Block Storage presents Block volumes to customers on physical storage that is wiped before any reuse. Customers with special requirements for compliance such as NIST 800-88 Guidelines for Media Sanitization must perform the data sanitization procedure before they delete their storage.

To delete a storage LUN, it's necessary to revoke access from any hosts first. Active replicas and dependent duplicates can also block reclamation of the Storage volume. Make sure that the volume is no longer mounted, host authorizations are revoked, replication is canceled, and no dependent duplicates exist before you attempt to cancel the original volume.

1. Click **Storage**, **Block Storage**.
2. Select the volume to be canceled, click **Actions**, and select **Cancel Block Storage**.
3. Confirm if want to cancel the LUN immediately or on the anniversary date of when the LUN was provisioned.

If you select the option to cancel the LUN on its anniversary date, you can void the cancellation request before its anniversary date.

1. Click **Continue** or **Close**.
2. Click the **Acknowledgment** check box and click **Confirm**.

You can expect the LUN to remain visible in your Storage list for at least 24 hours (immediate cancellation) or until the anniversary date. Certain features aren't going to be available any longer, but the volume remains visible until it's reclaimed. However, billing is stopped immediately after you click Delete/Cancel.

After the Storage LUN is reclaimed, the disk is wiped and data can't be restored. When drives are decommissioned, IBM destroys them before they are disposed of. The drives become unusable. Any data that was written to that drive becomes inaccessible