Note: IPv4 and IPv6 addresses are supported.

For configuration and management, you must allocate an IP address to the Ethernet management port of each canister, which is referred to as the *management IP address*. If both IPv4 and IPv6 operate concurrently, an address is required for each protocol.

You can configure the enclosure for event notification by using SNMP, syslog, or email. To configure notification, you must ensure that the SNMP agent, syslog IP addresses, or SMTP email server IP addresses can be accessed from all management addresses.

The system does not use name servers to locate other devices. You must supply the numeric IP address of the device. To locate a device, the device must have a fixed IP address.

For example, when you click **GUI** → **Settings** → **General** → **Upgrade Software**, the software level is checked. This check is done by the GUI by using the specific URL, as shown in the following example:

`https://public.dhe.ibm.com/storage/flash/9840.js`

To perform this check, the system that runs the GUI must have access to this URL by using target port 443.

3.8 Planning for encryption

Planning for encryption involves purchasing a licensed function and then, activating and enabling the function on the system.

To encrypt data that is stored on drives, they must contain an active license and be configured to use encryption. When encryption is activated and enabled on the system, a valid encryption key must be present on the system when the system unlocks the drives or the user generates a new key.

The encryption key must be stored on USB flash drives that contain a copy of the key that was generated when encryption was enabled or be available at an SKLM server, or both, depending on the method that is configured. Without these keys, user data on the drives cannot be accessed.

The encryption key is read from the USB flash drives that were created during system initialization or fetched from the SKLM server in your environment that must be running. The use of both methods (USB keys and SKLM server) in parallel is also supported.

Note: The system supports IBM Security Key Lifecycle Manager version 2.7.0.1 or later for enabling encryption with up to four key servers.

Before activating and enabling encryption, determine which method to use for accessing key information during times when the system requires the presence of an encryption key. The system requires an encryption key to be present during the following operations:

- System power-on
- System restart
- User initiated rekey operations
- Firmware update