



Enable Encryption on Self Encrypting Disks

CE1300 ships with **UCS-HD12T10NK9**, which are FIPS140-2 compliant Self Encrypting Disks. However, this is not shipped with encryption enabled by default.

This section describes enabling Drive Security for the individual disks and securing the RAID 1 Array. Users can apply these without data loss. But, if this is done on an active machine in service, follow the instructions in the [Cisco Expressway Administrator Guide](#) to back up the machine configuration.



Note If the Expressway has option keys installed, ensure these are safely copied in the unlikely event there are issues enabling security.

Perform these steps to encrypt the hardware in the disks and to secure the array after backing up the Expressway backup (if required):

1. Log into the CIMC, and from the top left menu icon, select **Storage/Cisco 12G SAS RAID Controller with 4GB FBWC (16 drives) (MRAID)**.
2. Select the **Controller Info** tab and click **Enable Drive Security**.
3. Select **Local Key Management**; either enter a **Security Key Identifier** or **Security Key** or press the **Suggest** button to generate values and select any one of them.
4. Record the values in a secure location if they are required again.
5. Click **Save** the disks to enable the SED functionality.
6. Click the **Virtual Drive Info** tab.
7. Check the **RAID 1 disk** checkbox.
8. Select **Secure Virtual Drive** and confirm if you want to secure the virtual drive at the prompt.

