Revised: September 29, 2025

USB 3.0 SSD storage device

Feature History for USB 3.0 SSD

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature Name and Description	Supported Platform
Cisco IOS XE 17.18.1	USB 3.0 SSD: You can perform operations such as formatting a storage device, unmounting a storage device, configure a password on a storage device, and so on.	Cisco C9350 Series Smart Switches

USB 3.0 SSD port on a switch

The USB 3.0 Solid State Drive (SSD) port on a switch supports either of the following storage devices:

- 120 GB USB 3.0 SSD (SSD-120G) and
- 240 GB USB 3.0 SSD (SSD-240G).

Uses of a USB 3.0 SSD storage device

A USB 3.0 SSD storage device serves as both a general-purpose storage device and an application-hosting device.

Note

An SSD-240G storage device is more suitable for application hosting.

For applications hosted in Kernel Virtual Machines (KVM), Linux Containers (LXC), or Docker containers, the storage drive saves packet captures, generates trace logs from the operating system and third-party applications, and captures Graceful Insertion and Removal (GIR) snapshots.

Detection and storage on a USB 3.0 SSD

A storage device is supported as a field-replaceable unit (FRU), which means it can be removed or replaced on-site with minimal downtime. The storage device is shipped as an unformatted (raw) device. When a storage device is initially inserted on the switch, one partition of the storage device is formatted to support the EXT4 file system.

Additionally, you can format the storage device with other EXT-based file systems, such as EXT2 and EXT4.

File permissions for USB 3.0 SSD storage device

The supported file permissions on a USB 3.0 SSD storage device are:

- Read

- Write
- Delete
- Copy
- Format

USB 3.0 SSD SMART functionality

USB 3.0 SSD support on a switch is also enabled with Self-Monitoring, Analysis, and Reporting Technology (S.M.A.R.T) functionality.

The purpose of S.M.A.R.T functionality is to

- monitor the reliability of the storage device,
- by executing different self-tests, and
- predicting storage device failures.

When a storage device is connected to a USB 3.0 SSD port, SMART Disk Monitoring Daemon (smartd) starts running by default. With smartd, errors and warnings are logged in the log file located at */crashinfo/tracelogs/smart_errors.log*, and also displayed on the console. When you remove the storage device, smartd stops running.

USB 3.0 SSD password authentication

You must enable security on the storage device by setting a user password to protect the storage device from unauthorized access.

The following security states are supported:

- Security disabled:

  User password has not been configured on the drive. This is the default for any new drive.

- Security enabled:

  User password has been configured on the drive.

- Locked:

  Security is enabled, and the drive is inaccessible.

- Unlocked:

  Security is enabled or disabled, but the drive is accessible.

You can configure password authentication using the CLI and the programmable NETCONF or YANG method.

Once a USB 3.0 SSD storage device is configured with the password, the password security will take effect only after Online Insertion and Removal (OIR) of the storage device or when a switch reloads. The storage device will be in a locked state. To unlock and access the drive, the switch prompts you to enter the USB 3.0 SSD password saved on the switch. The password is saved to the running configuration on the switch in type 6 encryption format.

Using the Encrypted Pre-shared Key feature, you can securely store plain text passwords in type 6 format in NVRAM using the CLI. Type-6 passwords are encrypted. Although the encrypted passwords can be viewed or retrieved, it is difficult to decrypt them to determine the actual password.

Guidelines for configuring USB 3.0 SSD storage device

- Only Cisco USB drives are supported on the USB 3.0 SSD port on the switch. •
- Non-EXT based file systems such as VFAT, NTFS, and LVM are not supported.
- The USB 3.0 SSD storage device cannot be used to boot images, install images, or upgrade the internal flash using software maintenance update (SMU) or install commands. The storage device is not available for bootloader support.
- If you run the **hw-module switch** *switch_num* **usbflash1 unmount** command on a switch or switch stack without inserting the storage device, the following error message is displayed.

```
Device# hw-module switch 1 usbflash1 unmount
*Jun 20 22:50:40.321:
ERROR: USB Not Present in this Slot 1
```

How to setup USB 3.0 SSD storage device

The following sections provide configuration information on how to format a storage device, unmount a storage device, enable and disable password security on a storage device.

Format a storage device from a switch or a switch stack

You need to format a new USB 3.0 SSD storage device. This procedure shows you how to format a storage device from a switch or switch stack.

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 Configure one of these commands based on the switch configuration:
Choose from:

- On a switch:

  format usbflash1: {**ext2** | **ext3** | **ext4** | **secure**}
- On a switch stack:

  format usbflash1-*switch-num*: {**ext2** | **ext3** | **ext4** | **secure**}

Example:

```
Device# format usbflash1: ext2
```

Format the storage device in a switch or switch stack using the EXT file systems.

switch-num: Enter the switch number of the switch on which you want to insert the storage device.

Unmount a storage device from a switch or a switch stack

You need to perform this task only if you want to remove a storage device plugged into a switch or switch stack.

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 Configure one of these commands based on the switch configuration:
Choose from:

- On a switch:

  hw-module switch usbflash1 unmount
- On a switch stack:

  hw-module switch *switch-num* **usbflash1 unmount**

Example:

```
Device# hw-module switch 1 usbflash1 unmount
```

Safely removes the USB 3.0 SSD storage device from a switch or a switch stack.

switch-num: Enter the switch number of the switch on which you want to insert the storage device.

This command unmounts the file system created upon insertion, and notifies the system to complete pending read or write operations, if any, to safely remove the drive from the switch.

How to configure password security on a storage device

The following sections provide configuration information on how to enable and disable password security, configure password, and unlock a storage device.

Enable password security on a storage device

You can perform this task if you want to enable password security on a storage device.

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 Configure one of these commands based on the switch configuration:
Choose from:

- On a switch:

  hw-module switch usbflash1 security enable password *usb-password*

- On a switch stack:

  hw-module switch *switch-num* **usbflash1 security enable password** *usb-password*

Example:

```
Device# hw-module switch 1 usbflash1 security enable password 1234
```

Configures a user-defined password on the USB 3.0 SSD storage device.

switch-num: Enter the switch number of the switch on which you want to insert the storage device.

Configure a password on a storage device

Perform this task only if you want to configure a password after enabling password security.

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **key config-key password-encrypt** *password*

Example:

```
Device(config)# key config-key password-encrypt 123456789
```

(Optional) Configures the master key on the switch.

The password configured using this command is the master encryption key that is used to encrypt all the other keys in the switch.

Skip this step if you have already configured the master key on the switch.

Note

Step 4 Configure one of these commands based on the switch configuration:
Choose from:

- On a switch:

  [**no**] **hw-module switch usbflash1-password** *usb-password*
- On a switch stack:

  [**no**] **hw-module switch** *switch-num* **usbflash1-password** *usb-password*

Example:

```
Device(config)# hw-module switch 1 usbflash1-password 1234
```

Encrypts the password internally using type-6encryption.

switch-num: Enter the switch number of the switch on which you want to insert the storage device.

Use the **no** form of the command to remove the password from the storage device.

Note Enter the same password as the one you configured in the Enable password security on a storage device, on page 4.

Step 5 **end**

Example:

```
Device(config)#  end
```

Exits interface configuration mode, and returns to privileged EXEC mode.

Unlock a locked storage device

Perform this task only if you want to temporarily unlock a locked storage device.

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 Configure one of these commands based on the switch configuration:
Choose from:

- On a switch:

  hw-module switch usbflash1 security unlock password *usb-password*
- On a switch stack:

  hw-module switch *switch-num* **usbflash1 security unlock password** *usb-password*

Example:

```
Device# hw-module switch 1 usbflash1 security unlock password 1234
```

Unlocks the drive and make the drive available for temporary access.

switch-num: Enter the switch number of the switch on which you want to insert the storage device.

Note Password security is still enabled on the drive and if you insert the drive on any other switch, the drive will be in locked state.

Disable password security on a storage device

Perform this task only if you want to disable password security on a storage device.

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 Configure one of these commands based on the switch configuration:
Choose from:

- On a switch:

  hw-module switch usbflash1 security disable password *usb-password*
- On a switch stack:

  hw-module switch *switch-num* **usbflash1 security disable password** *usb-password*

Example:

```
Device# hw-module switch 1 security disable password 1234
```

Disables security on a storage device and makes the drive accessible. You do not have to reload the switch or perform OIR of the drive for the changes to take effect.

switch-num: Enter the switch number of the switch on which you want to insert the storage device.

View information on a storage device

View the contents of the USB 3.0 SSD before working on its contents. For example, before copying a new configuration file, verify that the file system does not already contain a configuration file with the same name.

To display information about files on a filesystem, use one of the privileged EXEC commands listed in the following table:

Command Name	Description
dir usbflash1:	Displays the list of files on the USB flash filesystem on an active switch.
dir usbflash1-*switch-num*:	Displays the list of files on the file system in a stack setup. *switch-num* is the standby switch number or the stack member number.
dir stby-usbflash1:	Displays the list of files on the file system on the standby switch in a stack setup.
show usbflash1:filesystem:	Displays more information about the file system.
show inventory	Displays the physical inventory information for the USB hardware. After multiple switchovers, the **show inventory** command output might display the USB flash filesystem (usbflash1) for the active switch with the switch number. **Note** The **show inventory** command displays *usbflash1* in the output only when the device is in *Disabled and Unlocked* state or *Enabled and Unlocked* state.
more *file-url*	Displays the logs with SMART errors and overall health of the drive.
show hw-module usbflash1 security status	Displays the authentication status.

Errors and how to troubleshoot

Insertion and removal of a storage device

Error that you may encounter	Troubleshooting
Storage device not detected after insertion	• Check if you are using a USB 3.0 SSD storage device. If not, remove the drive from the device, and replace it with a Cisco USB 3.0 SSD storage device. • If you are using a Cisco USB 3.0 SSD storage device and the system is unable to detect the device, remove and reinsert the storage device. If it continues to fail, the USB is defective.

Error messages displayed on the console after removing the storage device:
`*Mar 20 00:48:16.353: %IOSXE-4-PLATFORM: Switch 1 R0/0: kernel: xhci_hcd 0000:00:14.0: Cannot set link state.`
`*Mar 20 00:48:16.353: %IOSXE-3-PLATFORM: Switch 1 R0/0: kernel: usb usb4-port1: cannot disable (err = -32)`
`*May 10 01:12:49.603: %IOSXE-3-PLATFORM: Switch 3 R0/0: kernel: JBD2: Error -5 detected when updating journal superblock for sda1-8.`
	Remove the storage device from the switch using the **unmount** command. For more information, see Unmount a storage device from a switch or a switch stack, on page 4

Error message displayed on the console on inserting a non-Cisco USB 3.0 SSD storage device: `%IOSXEBOOT-4-SSD_MOUNT_LOG: (local/local): ***INFO: Not a CISCO SSD - Cannot be used***`	Remove the USB from the device, and replace it with a Cisco USB 3.0 SSD storage device.

Password authentication

Error that you may encounter	Troubleshooting
Storage device not detected after insertion	Run the **show hw-module usbflash1 security status** command and check for USB Authentication Status fields in the output. If the USB Authentication Status field in the output displays Enabled and Locked, perform one of the following: • Unlock the drive temporarily using the **hw-module switch** *switch-num* **usbflash1 security unlock password** *usb-password* command. • Configure USB 3.0 SSD password on the switch. For more information, see Configure a password on a storage device, on page 5

Error that you may encounter	Troubleshooting

USB 3.0 SSD password does not match the password saved in the running configuration of the switch. The switch displays the following error messages:
`*Oct 19 19:32:04.094: %IOSD_INFRA-6-IFS_DEVICE_OIR: Device usbflash1 added`
`*Oct 19 19:32:04.138: Warning: Configured password on SWITCH does not match with that on DRIVE.`
`Please remove password from SWITCH first and then from DRIVE to re-configure.`
	Remove the password from the switch and reconfigure the switch to use the correct password. For more information, see Configure a password on a storage device, on page 5.

USB 3.0 SSD without a password inserted on a switch that has the drive password configured. An attempt to unlock the disk using the password configured on the switch fails and the switch displays the following messages:
`*Dec 14 00:01:00.374: %IOSD_INFRA-6-IFS_DEVICE_OIR: Device usbflash1 added`
`*Dec 14 00:01:00.430: ERROR: No password configured on DRIVE. Remove password from SWITCH to re-configure.`
	Perform the following steps:
	1. Enable security on the drive USB 3.0 SSD. See Enable password security on a storage device, on page 4.
	2. Reconfigure the password on the switch. See Configure a password on a storage device, on page 5.

USB 3.0 SSD configured with a password inserted on a switch that does not have the drive password configured. An attempt to unlock the disk fails and the switch displays the following messages:
`Oct 19 19:36:18.003: %IOSD_INFRA-6-IFS_DEVICE_OIR: Device usbflash1 added`
`*Oct 19 19:36:18.028: Warning: No password configured on SWITCH. Remove password from DRIVE to re-configure`
	Do one of the following:
	• Disable the password configured on the drive. See Disable password security on a storage device, on page 6.
	• Configure password on the switch. See Configure a password on a storage device, on page 5.

A USB 3.0 SSD in Disabled and locked state indicates that the USB drive has become unusable because of corrupted hardware.	To unlock and enable the drive, contact TAC.

Configuration examples for USB 3.0 SSD

You can refer to the following sections to view the authentication status of a storage device, verify the file system, view the file system information, verify physical inventory information, and verify the health of the storage device.

Example: View the authentication status of a storage device

The following example is a sample output for the **show hw-module usbflash1 security status** command executed on a switch stack with 4 switches:

```
Device# show hw-module usbflash1 security status
Device#   USB Authentication        Status
-----------------------------------------------------
1         USB Not Present         USB 3.0 is not present
```

```
2         Disabled and Unlocked  □ Security is disabled & the drive in unlocked state (Default state if USB is
  present)
3         Enabled and Locked     □ Security Enabled and the drive in locked state
4         Enabled and Unlocked   □ Security Enabled and the drive in unlocked state
```

When the drive is in *Enabled and Unlocked* or *Disabled and Unlocked* state, you can format a drive and perform normal file system operations like read, write, delete, and copy.

Example: Verify the file system

The following example is a sample output of the **dir usbflash1:** command:

```
Device# dir usbflash1:

Directory of usbflash1:/
11  drwx            16384   Oct 9 2015 01:49:18 +00:00  lost+found
3145729  drwx             4096   Oct 9 2015 04:10:41 +00:00  test
118014062592 bytes total (111933120512 bytes free)
```

The following example is a sample output of the **dir usbflash1-** *switch_num*: command in a switch stack:

```
Device# dir usbflash1-2:
Directory of usbflash1-2:/
11 drwx 16384 Jun 8 2018 21:35:39 +00:00 lost+found
118014083072 bytes total (111933390848 bytes free)
```

The following example is a sample output of the **dir stby-usbflash1:** command:

```
Device# dir stby-usbflash1:

Directory of usbflash1-3:/
11  drwx            16384  May 16 2018 23:32:43 +00:00  lost+found
118014083072 bytes total (110358429696 bytes free)
```

Example: View the file system information

The following example is a sample output of the **show usbflash1: filesystem** command:

```
Device# show usbflash1: filesystem

Filesystem: usbflash1
Filesystem Path: /vol/usb1
Filesystem Type: ext4
```

Example: Verify physical inventory information

The following example is a sample output of the **show inventory** command on a switch:

```
Device# show inventory

NAME: "usbflash1", DESCR: "usbflash1"
PID: SSD-240G          , VID: V01, SN: STP21460FN9
```

The following example is a sample output of the **show inventory** command on a switch stack:

```
Device# show inventory

NAME: "usbflash1", DESCR: "usbflash1"
PID: SSD-240G          , VID: V01, SN: STP21460FN9

NAME: "usbflash1-3", DESCR: "usbflash1-3"
PID: SSD-240G          , VID: V01, SN: STP21310001
```

Example: Verify the health of the storage device

The following example is a sample output of the **more flash:smart_overall_health.log** command:

```
Device# more flash:smart_overall_health.log

=== START OF READ SMART DATA SECTION ===
SMART overall-health self-assessment test result: PASSED
```

The following example is a sample output of the **more crashinfo:tracelogs/smart_errors.log** command:

```
Device# more crashinfo:tracelogs/smart_errors.log

%IOSXEBOOT-4-SMART_LOG: (local/local): Mon Jan 4 00:13:10 Universal 2016 INFO: Starting SMART daemon
```

 **Note**

The system might display warnings in the `smart_errors.log`. You can ignore these if the overall health self assessment in the `flash/smart_overall_health.log` displays `PASSED`.