Configuring USB 3.0 SSD

Information about USB 3.0 SSD

The following sections provide information about USB 3.0 SSD.

USB 3.0 SSD

In Cisco IOS XE Fuji 16.9.1, support for USB 3.0 SSD is enabled on Cisco Catalyst 9300 Series Switches. USB 3.0 SSD provides extra 240 GB storage for application hosting. Applications can be hosted in Kernel Virtual Machines (KVM), Linux Containers (LXC), or Docker containers. The storage drive can also be used to save packet captures, trace logs generated by the operating system and third-party applications. USB 3.0 SSD can be used simultaneously as a general-purpose storage device and as an application-hosting device. You must use only Cisco USB drives; non-Cisco USB drives are not supported.

Note USB 3.0 SSD cannot be used to boot images, emergency install the images, or upgrade internal flash using (software maintenance update (SMU or **install** commands. Bootloader support for USB 3.0 SSD is not available.

USB 3.0 SSD is enabled with Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T) functionality for health monitoring of the drive. The purpose of S.M.A.R.T is to monitor the reliability of the drive and predict drive failures, and to carry out different types of drive self tests. SMART Disk Monitoring Daemon (smartd) is enabled immediately after the insertion of a USB 3.0 SSD and starts logging warnings and errors in the /crashinfo/tracelogs/smart_errors.log. These warnings and errors are also displayed on the console. On removing the USB 3.0 SSD, smartd stops running.

USB 3.0 SSD is supported as a field-replaceable unit (FRU) that offers flexible storage configurations. If SSD is used initially on a PC, the default partition on USB 3.0 SSD is created by the PC supporting all the file systems. If SSD is used initially on the switch, one partition of the drive is created to support EXT4 file system.

File System on USB 3.0 SSD

USB 3.0 SSD is shipped as a raw device. When the device boots up, Cisco IOS software creates a partition with EXT4 as the default file system. However, the device supports all EXT-based file systems such as EXT2, EXT3, and EXT4. Non-EXT based file systems such as VFAT, NTFS, LVM, and so on are not supported.

The following file system operations are supported on the drive:

- Read
- Write
- Delete
- Copy
- Format

Password Authentication on USB 3.0 SSD

To protect the drive from unauthorized access, you must enable security on USB 3.0 SSD by setting a user password. A USB 3.0 SSD supports the following security states:

- Security disabled — User password has not been configured on the drive. This is the out-of-box state which 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 as well as programmable NETCONF/YANG method.

How to Configure USB 3.0 SSD

The following sections provide information about configuring USB 3.0 SSD:

Formatting USB 3.0 SSD

Use the **format usbflash1:** {**ext2** | **ext3** | **ext4** | **secure**} command to format the EXT file systems or the entire drive.

To format the USB 3.0 SSD drive in a device stack, use **format usbflash1**-*switch_num***:** {**ext2** | **ext3** | **ext4** | **secure**} command.

Unmounting USB 3.0 SSD from a Switch or a Switch Stack

To safely remove the USB 3.0 SSD from a switch or a switch stack, use the **hw-module switch** <*switch_num*> **usbflash1 unmount** command in privileged EXEC mode. This command unmounts the filesystem created

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

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

      *Jan  5 22:21:32.723: %IOSXE-0-PLATFORM: Switch 1 R0/0: SSD_UNMOUNT_LOG: usbflash1:
has been unmounted. All the usbflash1 entries in    IOS will now be cleared until the SSD
is plugged back into the switch.
      *Jan  5 22:21:32.729: %IOSD_INFRA-6-IFS_DEVICE_OIR: Device usbflash1 removed
```

After you run this command, you will not be able to access the USB anymore. To use the USB again reinsert it into the switch.

If you run the **hw-module switch** <*switch_num*> **usbflash1 unmount** command on a switch or switch stack without inserting the USB, 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
```

Enabling Password Security on USB 3.0 SSD

The password authentication feature enables you to configure security on a USB 3.0 SSD in order to protect the drive from unauthorized access and associated risks.To enable security on a USB 3.0 SSD, follow these steps to set a password on the drive.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device>enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**hw-module switch** *switch-number* **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. **Note** Password security will take effect only after after Online Insertion and Removal (OIR) of the USB or a switch reload.

After Online Insertion and Removal (OIR) of the USB or a switch reload, the USB will be in *Enabled and Locked* state. To unlock and access the USB, you must configure the switch to use the USB 3.0 SSD password that you create in this task.

What to do next

To configure the USB 3.0 SSD password on the switch, see Configuring USB 3.0 SSD Password on a Switch, on page 4.

Configuring USB 3.0 SSD Password on a Switch

To access a password protected USB 3.0 SSD using a switch, you must configure the same USB 3.0 SSD password on the switch. USB 3.0 SSD will be in locked state after a switch reset or OIR of the drive. To unlock and access the drive, the switch prompts you to enter the USB 3.0 SSD password saved on the switch. This procedure saves the password to the running configuration on the switch in type-6 encryption format.

Using the Encrypted Preshared Key feature, you can securely store plain text passwords in type-6 format in NVRAM using the command-line interface (CLI). Type-6 passwords are encrypted. Although the encrypted passwords can be seen or retrieved, it is difficult to decrypt them to find out the actual password.

Procedure

	Command or Action	Purpose
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	(Optional) **key config-key password-encrypt** *password* **Example:** `Device(config)#key config-key password-encrypt 123456789`	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. **Note** Skip this step if you have already configured the master key on the switch.
Step 4	[**no**] **hw-module switch** *switch-number* **usbflash1-password** *usb-password* **Example:** `Device(config)#hw-module switch 1 usbflash1-password 1234`	**Note** Ensure the password matches the one that you have configured on the USB 3.0 SSD to enable security. Encrypts the password internally using type-6 encryption. Use the **no** form of the command to remove the USB 3.0 SSD password from the running configuration of the switch.
Step 5	**end** **Example:** `Device(config)#end`	Returns to privileged EXEC mode.

Unlocking USB 3.0 SSD

Follow these steps to unlock a USB 3.0 SSD:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**hw-module switch** *switch-number* **usbflash1 security unlock password** *usb-password* **Example:** `Device#hw-module switch 1 usbflash1 security unlock password 1234`	Unlocks the drive and makes the drive available for temporary access. Note that 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.

Disabling Password Security on USB 3.0 SSD

Follow these steps to disable security or to change the password configured on a USB 3.0 SSD.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**hw-module switch** *switch-number* **usbflash1 security disable password** *usb-password* **Example:** `Device #hw-module switch 1 usbflash1 security disable password 1234`	Disables security on USB 3.0 SSD 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. **Note** On a switch stack, enter the switch number of the switch on which you have inserted the USB 3.0 SSD.

Monitoring USB 3.0 SSD

You can view the contents of the USB 3.0 SSD before working on its contents. For example, before copying a new configuration file, you might want to verify that the filesystem 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:

Table 1: Commands to Display Files on a Filesystem

Command Name	Description
dir usbflash1:	Displays the list of files on the USB flash filesystem on an active switch. To access flash partitions of a standby switch or the device members in a stack, use **usbflash1**–*n* where *n*, is the standby switch number or the stack member number.
dir usbflash1-*switch_num***:**	Displays the list of files on the filesystem in a stack setup.
dir stby-usbflash1:	Displays the list of files on the filesystem on the standby switch in a stack setup.
show usbflash1: filesystem	Displays more information about the filesystem.
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 USB 3.0 SSD authentication status.

Troubleshooting Tips

The following sections provide troubleshooting tips:

Troubleshooting USB 3.0 SSD Insertion and Removal

Table 2: Errors and Troubleshooting

Error That You May Encounter	Troubleshooting
USB3.0 SSD not detected after insertion	• Check if you are using a Cisco USB 3.0 SSD. If not, remove the drive from the device, and replace it with a Cisco USB 3.0 SSD. • If you are using a Cisco USB 3.0 SSD and the system is unable to detect the drive, remove and reinsert the USB 3.0 SSD. If it continues to fail, the USB might be defective.

Error messages displayed on the console after removing USB 3.0 SSD:
`*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 USB 3.0 SSD from the device after running the **unmount** command. For more information, see Unmounting USB 3.0 SSD from a Switch or a Switch Stack, on page 2.

Error message displayed on the console on inserting a non-Cisco USB 3.0 SSD: `%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.

Troubleshooting Password Authentication

Table 3: Errors and Troubleshooting

Error That You May Encounter	Troubleshooting
USB3.0 SSD 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 1** *switch-number* **usbflash1 security unlock password** *usb-password* command. • Configure USB 3.0 SSD password on the switch. See Configuring USB 3.0 SSD Password on a Switch, on page 4.

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.`
	Perform the following:
	• Remove the password from the switch and reconfigure the switch to use the correct password. See Configuring USB 3.0 SSD Password on a Switch, on page 4.

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 Enabling Password Security on USB 3.0 SSD, on page 3.
	2. Reconfigure the password on the switch. See Configuring USB 3.0 SSD Password on a Switch, on page 4.

Error That You May Encounter	Troubleshooting

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 Disabling Password Security on USB 3.0 SSD, on page 5.
	• Configure password on the switch. See Configuring USB 3.0 SSD Password on a Switch, on page 4.

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

The following sections provide configuration examples for USB 3.0 SSD:

Example: Displaying USB 3.0 SSD Authentication Status

This example shows the USB 3.0 SSD authentication status on a switch stack with 4 switches.

```
# show hw-module usbflash1 security status

Switch#   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.

Examples: Verifying the Filesystem

The following example displays the output of the **dir usbflash1:/** command in privileged EXEC mode:

```
Switch#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 displays the output of the **dir usbflash1:***switch_num***:** command in a device stack:

```
Switch#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)
```

Alternately, you can use the **dir stby-usbflash1:** command to access the file system on a standby switch:

```
Switch#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)
```

To display the file system information for usbflash1, use the **show usbflash1: filesystem** command in privileged EXEC mode:

```
Switch#show usbflash1: filesystem
Filesystem: usbflash1
Filesystem Path: /vol/usb1
Filesystem Type: ext4
```

Examples: Verifying Physical Inventory Information

To display the physical inventory information for USB 3.0 SSD hardware, use the **show inventory** command:

```
Switch#show inventory

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

The following is a sample output of the **show inventory** command in a device stack:

```
Switch#show inventory

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

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

Examples: Verifying the Health of the Drive

To check the overall health of the drive, use the **more flash:smart_overall_health.log** command in privileged EXEC mode:

```
Switch#more flash:smart_overall_health.log

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

To check the health error logs, use the **more crashinfo:tracelogs/smart_errors.log** command in privileged EXEC mode:

```
Switch#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`.

Feature History for USB 3.0 SSD

This table provides release and related information for features explained in this module.

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

Release	Feature	Feature Information
Cisco IOS XE Fuji 16.9.1	USB 3.0 SSD	USB 3.0 SSD provides extra 120 GB storage to be used as a general-purpose storage device and as an application-hosting device.
Cisco IOS XE Fuji 16.9.6	USB 3.0 SSD storage	USB 3.0 SSD storage capacity increased to 240 GB in Cisco IOS XE Fuji 16.9.6 and later Cisco IOS XE Fuji 16.9 releases.
Cisco IOS XE Gibraltar 16.10.1	Password authentication	Password authentication feature enables you set a password on the USB 3.0 SSD device in order to protect the drive from unauthorized access and associated risks.
Cisco IOS XE Gibraltar 16.12.4	USB 3.0 SSD storage	USB 3.0 SSD storage capacity increased to 240 GB in Cisco IOS XE Gibraltar 16.12.4 and later Cisco IOS XE Gibraltar 16.12 releases.
Cisco IOS XE Amsterdam 17.3.1	USB 3.0 SSD storage	USB 3.0 SSD storage capacity increased to 240 GB in Cisco IOS XE Amsterdam 17.3.1 and all later releases.

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.