



USB 3.0 SSD の設定

- [USB 3.0 SSD に関する情報](#) (1 ページ)
- [USB 3.0 SSD の設定方法](#) (3 ページ)
- [USB 3.0 SSD のモニタリング](#) (6 ページ)
- [トラブルシューティングのヒント](#) (8 ページ)
- [USB 3.0 SSD の設定例](#) (10 ページ)
- [USB 3.0 SSD の機能履歴](#) (12 ページ)

USB 3.0 SSD に関する情報

USB 3.0 SSD

USB 3.0 SSD は、アプリケーションをホストするための追加の 120 GB ストレージを提供します。アプリケーションはカーネル仮想マシン (KVM)、Linux Containers (LXC)、または Docker コンテナでホストできます。ストレージドライブを使用して、パケットキャプチャ、オペレーティングシステムによって生成されたトレースログ、およびサードパーティアプリケーションを保存することもできます。USB 3.0 SSD は、汎用ストレージデバイスとして、およびアプリケーションホスティングデバイスとして同時に使用できます。Cisco USB ドライブのみを使用する必要があります。シスコ以外の USB ドライブはサポートされていません。



(注) USB 3.0 SSD は、イメージのブート、イメージの緊急インストール、またはソフトウェアメンテナンスアップデート (SMU) または `install` コマンドを使用した内部フラッシュのアップグレードには使用できません。USB 3.0 SSD のブートローダーサポートは使用できません。

USB 3.0 SSD は、ドライブのヘルスマニタリング用に Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T) 機能が有効になっています。S.M.A.R.T の目的は、ドライブの信頼性のモニタ、ドライブ障害の予測、さまざまなタイプのドライブセルフテストを実行することです。SMART Disk Monitoring Daemon (smartd) は、USB 3.0 SSD を挿入した直後に有効になり、`/crashinfo/tracelogs/smart_errors.log` に警告とエラーのロギングを開始します。これらの警告

とエラーは、コンソールにも表示されます。USB 3.0 SSD を取り外すと、`smartd` は動作を停止します。

USB 3.0 SSD は、柔軟なストレージ構成を提供する Field Replaceable Unit (FRU) としてサポートされています。最初に PC で SSD を使用する場合、USB 3.0 SSD のデフォルトパーティションが、すべてのファイルシステムをサポートする PC によって作成されます。スイッチで SSD を最初に使用する場合、EXT4 ファイルシステムをサポートするためにドライブの 1 つのパーティションが作成されます。

USB 3.0 SSD のファイルシステム

USB 3.0 SSD は raw デバイスとして出荷されます。デバイスが起動すると、Cisco IOS ソフトウェアは EXT4 をデフォルトのファイルシステムとしてパーティションを作成します。ただし、デバイスは、EXT2、EXT3、EXT4 などのすべての EXT ベースのファイルシステムをサポートします。VFAT、NTFS、LVM などの非 EXT ベースのファイルシステムはサポートされていません。

ドライブでは、次のファイルシステム操作がサポートされています。

- 読み取り
- 書き込み
- Delete
- Copy
- 書式

USB 3.0 SSD でのパスワード認証

不正アクセスからドライブを保護するには、ユーザパスワードを設定して USB 3.0 SSD のセキュリティを有効にする必要があります。USB 3.0 SSD は、次のセキュリティ状態をサポートします。

- セキュリティ無効：ユーザパスワードがドライブに設定されていません。これは、新しいドライブのデフォルトであるアウトオブボックス状態です。
- セキュリティ有効：ユーザパスワードがドライブに設定されています。
- ロック済み：セキュリティは有効で、ドライブにアクセスできません。
- ロック解除済み：セキュリティは有効または無効ですが、ドライブはアクセス可能です。

CLI およびプログラム可能な NETCONF/YANG 方式を使用してパスワード認証を設定できます。

USB 3.0 SSD の設定方法

USB 3.0 SSD のフォーマット

EXT ファイルシステムまたはドライブ全体をフォーマットするには、**format usbflash1:{ext2 | ext3 | ext4 | secure}** コマンドを使用します。

デバイススタックの USB 3.0 SSD ドライブをフォーマットするには、**format usbflash1-switch_num: {ext2 | ext3 | ext4 | secure}** コマンドを使用します。

スイッチまたはスイッチスタックからの USB 3.0 SSD のマウント解除

スイッチまたはスイッチスタックから USB 3.0 SSD を安全に取り外すには、特権 EXEC モードで **hw-module switch <switch_num> usbflash1 unmount** コマンドを使用します。このコマンドは、挿入時に作成されたファイルシステムをマウント解除し、システムに保留中の読み取りまたは書き込み操作があれば完了し、スイッチからドライブを安全に取り外すように通知します。

```
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
```

このコマンドを実行すると、USB にアクセスできなくなります。USB を再度使用するには、スイッチに再度挿入します。

USB を挿入せずにスイッチまたはスイッチスタックで **hw-module switch <switch_num> usbflash1 unmount** コマンドを実行すると、次のエラーメッセージが表示されます。

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

```
*Jun 20 22:50:40.321:
ERROR: USB Not Present in this Slot 1
```

USB 3.0 SSD でのパスワードセキュリティの有効化

パスワード認証機能を使用すると、USB 3.0 SSD のセキュリティを設定して、不正アクセスや関連するリスクからドライブを保護できます。USB 3.0 SSD のセキュリティを有効にするには、次の手順に従ってドライブにパスワードを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 :	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	Device>enable	<ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	hw-module switch switch-number usbflash1 security enable password usb-password 例： Device#hw-module switch 1 usbflash1 security enable password 1234	USB 3.0 SSD でユーザ定義のパスワードを設定します。 (注) パスワードセキュリティは、USB の活性挿抜 (OIR) またはスイッチのリロード後にのみ有効になります。

USB の活性挿抜 (OIR) またはスイッチのリロード後、USB は *Enabled and Locked* 状態になります。USB のロックを解除して USB にアクセスするには、このタスクで作成した USB 3.0 SSD パスワードを使用するようにスイッチを設定する必要があります。

次のタスク

スイッチの USB 3.0 SSD パスワードを設定するには、[スイッチでの USB 3.0 SSD パスワードの設定 \(4 ページ\)](#) を参照してください。

スイッチでの USB 3.0 SSD パスワードの設定

スイッチを使用してパスワードで保護された USB 3.0 SSD にアクセスするには、スイッチで同じ USB 3.0 SSD パスワードを設定する必要があります。ドライブのスイッチリセットまたは OIR 後、USB 3.0 SSD はロック状態になります。ドライブのロックを解除してアクセスするために、スイッチに保存されている USB 3.0 SSD パスワードを入力するように求められます。この手順では、パスワードをタイプ 6 暗号化形式でスイッチの実行コンフィギュレーションに保存します。

暗号化事前共有キー機能を使用すると、コマンドラインインターフェイス (CLI) から、プレーンテキストのパスワードをタイプ 6 形式で NVRAM へセキュアに保存できます。タイプ 6 パスワードは暗号化されます。暗号化されたパスワード自体を、確認したり取得したりすることは可能ですが、それを復号化して実際のパスワードを特定することは困難です。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device>enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	(任意) key config-key password-encrypt password 例： Device (config)# key config-key password-encrypt 123456789	スイッチのマスターキーを設定します。 このコマンドを使用して設定されたパスワードは、スイッチ内のその他すべてのキーを暗号化するマスター暗号キーとして使用されます。 (注) スイッチにマスターキーがすでに設定されている場合は、この手順をスキップします。
ステップ 4	[no] hw-module switch switch-number usbflash1-password usb-password 例： Device (config)# hw-module switch 1 usbflash1-password 1234	(注) セキュリティを有効にするために、パスワードが USB 3.0 SSD で設定したパスワードと一致することを確認します。 タイプ 6 暗号化を使用してパスワードを内部的に暗号化します。 コマンドの no 形式を使用して、スイッチの実行コンフィギュレーションから USB 3.0 SSD パスワードを削除します。
ステップ 5	end 例： Device (config)# end	特権 EXEC モードに戻ります。

USB 3.0 SSD のロック解除

USB 3.0 SSD のロックを解除するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	hw-module switch switch-number usbflash1 security unlock password usb-password 例： Device#hw-module switch 1 usbflash1 security unlock password 1234	ドライブのロックを解除し、一時的にアクセスできるようにします。ドライブでパスワードセキュリティが有効になっていることに注意してください。ドライブを他のスイッチに挿入すると、ドライブはロックされた状態になります。

USB 3.0 SSD でのパスワードセキュリティの無効化

セキュリティを無効にする、または USB 3.0 SSD に設定されているパスワードを変更するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	hw-module switch switch-number usbflash1 security disable password usb-password 例： Device #hw-module switch 1 usbflash1 security disable password 1234	USB 3.0 SSD のセキュリティを無効にし、ドライブにアクセスできるようにします。変更を有効にするために、スイッチをリロードしたり、ドライブの OIR を実行したりする必要はありません。 <p>(注) スイッチスタックで、USB 3.0 SSD を挿入したスイッチのスイッチ番号を入力します。</p>

USB 3.0 SSD のモニタリング

USB 3.0 SSD の格納ファイルを操作する前に、その格納ファイルを確認できます。たとえば、新しいコンフィギュレーションファイルをコピーする前に、ファイルシステムに同じ名前のコンフィギュレーションファイルが格納されていないことを確認できます。ファイルシステムのファイルに関する情報を表示するには、次の表に記載する特権 EXEC コマンドのいずれかを使用します。

表 1: ファイルシステム上のファイルを表示するコマンド

コマンド名	説明
dir usbflash1:	<p>アクティブスイッチ上の USB フラッシュファイルシステム上のファイルのリストを表示します。</p> <p>スタックのスタンバイスイッチまたはデバイスメンバのフラッシュパーティションにアクセスするには、usbflash1-n を使用します (<i>n</i> はスタンバイスイッチ番号またはスタックメンバ番号です)。</p>
dir usbflash1-switch_num:	スタックセットアップのファイルシステム上のファイルのリストを表示します。
dir stby-usbflash1:	スタックセットアップのスタンバイスイッチのファイルシステム上のファイルのリストを表示します。
show usbflash1: filesystem	ファイルシステムに関する詳細情報を表示します。
show inventory	<p>USB ハードウェアの物理インベントリ情報を表示します。</p> <p>複数のスイッチオーバー後、show inventory コマンドの出力には、アクティブスイッチの USB フラッシュファイルシステム (usbflash1) とスイッチ番号が表示されることがあります。</p> <p>(注) show inventory コマンドの出力に「usbflash1」と表示されるのは、デバイスが「Disabled and Unlocked」状態または「Enabled and Unlocked」状態の場合のみです。</p>
more file-url	SMART エラーおよびドライブの全体的な正常性を示すログを表示します。
show hw-module usbflash1 security status	USB 3.0 SSD 認証ステータスを表示します。

トラブルシューティングのヒント

USB 3.0 SSD の挿入および取り外しのトラブルシューティング

表 2: エラーとトラブルシューティング

発生する可能性のあるエラー	トラブルシューティング
挿入後に USB3.0 SSD が検出されない	<ul style="list-style-type: none"> • Cisco USB 3.0 SSD を使用しているかどうかを確認します。使用していない場合は、デバイスからドライブを取り外し、Cisco USB 3.0 SSD と交換します。 • Cisco USB 3.0 SSD を使用していて、システムがドライブを検出できない場合は、USB 3.0 SSD を取り外して再度挿入します。それでも障害が発生する場合は、USB が不良品である可能性があります。
<p>USB 3.0 SSD の取り外し後にコンソールに表示されるエラーメッセージ:</p> <pre>*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.</pre>	<p>umount コマンドを実行した後、デバイスから USB 3.0 SSD を取り外します。詳細については、スイッチまたはスイッチスタックからの USB 3.0 SSD のマウント解除 (3 ページ) を参照してください。</p>
<p>シスコ以外の USB 3.0 SSD を挿入すると、コンソールに次のエラーメッセージが表示されます。</p> <pre>%IOSXEBOOT-4-SSD_MOUNT_LOG: (local/local): ***INFO: Not a CISCO SSD - Cannot be used***</pre>	<p>デバイスから USB を取り外し、Cisco USB 3.0 SSD と交換します。</p>

パスワード認証に関するトラブルシューティング

表 3: エラーとトラブルシューティング

発生する可能性のあるエラー	トラブルシューティング
<p>挿入後に USB3.0 SSD が検出されない</p>	<p>show hw-module usbflash1 security status コマンドを実行し、出力の [USB Authentication Status] フィールドを確認します。出力の [USB Authentication Status] フィールドに [Enabled and Locked] が表示されている場合は、次のいずれかを実行します。</p> <ul style="list-style-type: none"> • hw-module switch 1 switch-number usbflash1 security unlock password usb-password コマンドを使用して、ドライブを一時的にロック解除します。 • スイッチで USB 3.0 SSD パスワードを設定します。 スイッチでの USB 3.0 SSD パスワードの設定 (4 ページ) を参照してください。
<p>USB 3.0 SSD のパスワードが、スイッチの実行中のコンフィギュレーションに保存されているパスワードと一致しません。スイッチに次のエラーメッセージが表示されます。</p> <pre>*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.</pre>	<p>次の手順を実行します。</p> <ul style="list-style-type: none"> • スイッチからパスワードを削除し、正しいパスワードを使用するようにスイッチを再設定します。 スイッチでの USB 3.0 SSD パスワードの設定 (4 ページ) を参照してください。

発生する可能性のあるエラー	トラブルシューティング
<p>ドライブパスワードが設定されているスイッチにパスワードがない USB 3.0 SSD が挿入されています。スイッチで設定されたパスワードを使用したディスクのロック解除は失敗し、スイッチに次のメッセージが表示されます。</p> <pre>*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.</pre>	<p>次の操作を行ってください。</p> <ol style="list-style-type: none"> 1. ドライブ USB 3.0 SSD でセキュリティを有効にします。USB 3.0 SSD でのパスワードセキュリティの有効化 (3 ページ) を参照してください。 2. スwitchのパスワードを再設定します。スイッチでの USB 3.0 SSD パスワードの設定 (4 ページ) を参照してください。
<p>ドライブパスワードが設定されていないスイッチにパスワードが設定された USB 3.0 SSD が挿入されています。ディスクのロック解除は失敗し、スイッチに次のメッセージが表示されます。</p> <pre>*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</pre>	<p>次のいずれかを実行します。</p> <ul style="list-style-type: none"> • ドライブに設定されているパスワードを無効にします。USB 3.0 SSD でのパスワードセキュリティの無効化 (6 ページ) を参照してください。 • スwitchでパスワードを設定します。スイッチでの USB 3.0 SSD パスワードの設定 (4 ページ) を参照してください。
<p>Disabled and locked 状態の USB 3.0 SSD は、ハードウェアの破損により USB ドライブが使用できなくなったことを示します。</p>	<p>ドライブのロックを解除して有効にするには、TAC にお問い合わせください。</p>

USB 3.0 SSD の設定例

例：USB 3.0 SSD 認証ステータスの表示

この例では、4つのスイッチを備えたスイッチスタックの USB 3.0 SSD 認証ステータスを示します。

```
# 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

```

ドライブが *Enabled and Unlocked* または *Disabled and Unlocked* 状態の場合、ドライブをフォーマットし、読み取り、書き込み、削除、コピーなどの通常のファイルシステム操作を実行できます。

例：ファイルシステムの確認

次に、特権 EXEC モードでの **dir usbflash1:/** コマンドの出力例を示します。

```

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)

```

次に、デバイススタックでの **dir usbflash1:switch_num:** コマンドの出力例を示します。

```

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)

```

または、**dir stby-usbflash1:** コマンドを使用して、スタンバイスイッチのファイルシステムにアクセスできます。

```

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)

```

usbflash1 のファイルシステム情報を表示するには、特権 EXEC モードで **show usbflash1: filesystem** コマンドを使用します。

```

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

```

例：物理インベントリ情報の確認

USB 3.0 SSD ハードウェアの物理インベントリ情報を表示するには、**show inventory** コマンドを使用します。

```

Switch#show inventory

NAME: "usbflash1", DESCR: "usbflash1"
PID: SSD-120G           , VID: STP21460FN9, SN: V01

```

次に、デバイススタックの **show inventory** コマンドの出力例を示します。

```

Switch#show inventory

NAME: "usbflash1", DESCR: "usbflash1"
PID: SSD-120G           , VID: STP21460FN9, SN: V01

```

```
NAME: "usbflash1-3", DESCR: "usbflash1-3"
PID: SSD-120G          , VID: STP21310001, SN: V01
```

例：ドライブの正常性の確認

ドライブの全体的な正常性を確認するには、特権 EXEC モードで **more flash:smart_overall_health.log** コマンドを使用します。

```
Switch#more flash:smart_overall_health.log
```

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

正常性エラーログを確認するには、特権 EXEC モードで **more crashinfo:tracelogs/smart_errors.log** コマンドを使用します。

```
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
```



- (注) システムは、**smart_errors.log** に警告を表示することがあります。**flash/smart_overall_health.log** の全体的な正常性のセルフアセスメントに **PASSED** と表示されている場合は、これらを見逃すことができます。

USB 3.0 SSD の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Gibraltar 16.11.1	パスワード認証付き USB 3.0 SSD	<p>USB 3.0 SSD は、汎用ストレージデバイスおよびアプリケーションホスティングデバイスとして使用するための追加の 120 GB ストレージを提供します。</p> <p>パスワード認証機能を使用すると、USB 3.0 SSD デバイスにパスワードを設定して、不正アクセスや関連するリスクからドライブを保護できます。</p>

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。

