



ファブリック セキュリティ

この章は、次の項で構成されています。

- [連邦情報処理標準 \(FIPS\) について \(1 ページ\)](#)
- [注意事項と制約事項 \(1 ページ\)](#)
- [GUI を使用した Cisco APIC の FIPS の設定 \(2 ページ\)](#)
- [NX-OS スタイル CLI を使用した Cisco APIC の FIPS 設定 \(2 ページ\)](#)
- [REST API を使用した Cisco APIC の FIPS の設定 \(3 ページ\)](#)

連邦情報処理標準 (FIPS) について

連邦情報処理標準 (FIPS) 発行 140-2、暗号化モジュールのセキュリティ要件では、暗号化モジュールの米国政府要件が詳述されています。FIPS 140-2 では、暗号モジュールがハードウェア、ソフトウェア、ファームウェア、または何らかの組み合わせのセットで、暗号機能またはプロセスを実装し、暗号アルゴリズムおよび任意のキー生成機能を含み、明確に定義された暗号境界の内部に位置しなければならないと定義しています。

FIPS は特定の暗号アルゴリズムがセキュアであることを条件とするほか、ある暗号モジュールが FIPS 準拠であると称する場合は、どのアルゴリズムを使用すべきかも指定しています。

注意事項と制約事項

次の注意事項と制約事項に従ってください。

- FIPS を有効にすると、Cisco APIC 全体に適用されます。
- Cisco APIC ソフトウェアのダウン グレードを実行しているときに FIPS を最初に無効にする必要があります。
- パスワードは最小限 8 文字の長さで作成してください。
- Telnet をディセーブルにします。ユーザのログインは SSH だけで行ってください。
- SSH サーバの RSA1 キー ペアすべてを削除してください。

- RADIUS/TACACS+によるリモート認証をディセーブルにしてください。ローカルとLDAP ユーザのみを認証できます。
- セキュア シェル (SSH) および SNMP がサポートされます。
- SNMPv1 およびv2をディセーブルにしてください。SNMPv3に対して設定された、スイッチ上の既存ユーザ- アカウントのいずれについても、認証およびプライバシー用 AES3 は SHA でのみ設定されていなければなりません。
- リリース 2.3(1x) で始まる、FIPS は、スイッチのレベルで設定できます。
- リリース 3.1(1x) から始まる FIPs を有効にすると、NTP が FIPSモードの動作は、HMAC SHA1 による認証と認証なしで FIPSモード NTP をサポートしています。

GUI を使用した Cisco APIC の FIPS の設定

FIPS を有効にすると、Cisco APIC 全体に適用されます。

手順

- ステップ1 メニュー バーで、**[Admin] > [AAA]** の順に選択します。
- ステップ2 **[ナビゲーション]** ペインで、**[AAA] > [ファブリック セキュリティ]** を展開します。
- ステップ3 **[作業]** ペインの **[プロパティ]** 領域で、目的の FIPSモードを選択します。

FIPSモードのオプションは、**[無効化]** と **[有効化]** です。デフォルト値は **[Disable]** です。

(注) 設定を完了するには再起動する必要があります。モードを変更すると、設定を完了するため必ず再起動する必要があります。

NX-OS スタイル CLI を使用した Cisco APIC の FIPS 設定

FIPS を有効にすると、Cisco APIC 全体に適用されます。

手順

	コマンドまたはアクション	目的
ステップ1	configure 例： apic1# configure	コンフィギュレーションモードに入ります。

	コマンドまたはアクション	目的
ステップ 2	fips mode enable 例 : <pre>apic1(config)# fips mode enable</pre>	FIP を有効にします。 no fips mode enable コマンドにより FIPS が無効になります。 設定を完了するには再起動する必要があります。モードを変更すると、設定を完了するため必ず再起動する必要があります。

REST API を使用した Cisco APIC の FIPS の設定

FIPS を有効にすると、Cisco APIC 全体に適用されます。

手順

すべてのテナントの FIPS を設定します。

例 :

```
https://apic1.cisco.com/api/node/mo/uni/userext.xml
<aaaFabricSec fipsMode="enable" />
```

(注) 設定を完了するには再起動する必要があります。モードを変更すると、設定を完了するため必ず再起動する必要があります。

