



# ハードウェアの完全性の検証

• [ハードウェアの完全性の検証 \(1 ページ\)](#)

## ハードウェアの完全性の検証

このアラームは、Cisco Secure Unique Device Identifier (SUDI) 証明書のエラー数をモニターします。SUDI は、構成、セキュリティ、監査、および管理用の変更できないデバイスアイデンティティとして使用できるため、資産管理、プロビジョニング、バージョンの可視性、サービス権限付与、品質フィードバック、およびインベントリ管理のために、シスコ製品の正確で一貫性のある電子的な識別が可能になります。

アラームをトリガーする SUDI エラーの数を指定します。このアラームを設定するには、次の手順を実行します。

- ステップ 1 メインウィンドウで、 > [設定 (Configure)] > [ポリシー (Policies)] の順にクリックします。
- ステップ 2 [ポリシーを追加 (Add Policy)] をクリックします。
- ステップ 3 [名前 (Name)] フィールドでポリシー名を入力します。
- ステップ 4 [トリガー (Triggers)] で、[ルールを追加 (Add Rules)] をクリックします。
- ステップ 5 [ハードウェアの完全性の検証 (Hardware Integrity Validation)] をクリックします。
- ステップ 6 [次へ (Next)] をクリックします。
- ステップ 7 デフォルトでは、ルールが有効になっています。ルールをまだ使用しない場合は、スイッチを [無効 (DISABLED)] に切り替えます。
- ステップ 8 スライダーを使用して、このアラームをトリガーする SUDI エラーの数を示します。
- ステップ 9 [重大度 (Severity)] ドロップダウンリストで、このアラームに定義する重大度を選択します。
- ステップ 10 その他の必要なインターフェイスおよびエンドポイント通知の設定を行い、[保存 (Save)] をクリックします。



## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。