Cisco Integrity Verification Application (Beta) on APIC-EM リリース 1.5.0.266 ユーザガイド

2017 年 8 月 1 日

Cisco Systems, Inc.
www.cisco.com

シスコは世界各国 200 箇所にオフィスを開設しています。
各オフィスの住所、電話番号、FAX 番号は
当社の Web サイトをご覧ください。
www.cisco.com/go/offices.

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries.シスコの商標の一覧は http://www.cisco.com/go/trademarks でご確認いただけます。Third-party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2017 Cisco Systems, Inc. All rights reserved.

目次

はじめに v

製品説明 v

マニュアルの構成 v

表記法 vi

関連資料 vii

マニュアルの入手方法およびテクニカル サポート vii

概要 1-1

Cisco IV アプリケーションについて 1-1

測定値の整合性と「No Detected Risk」 1-2

Cisco IV アプリケーション ワークフローの概要 1-3

導入 2-1

APIC-EM 向け Cisco IV アプリケーション 2-1

Cisco APIC-EM の導入 2-1

Cisco IV アプリケーションのインストールまたはアップグレード 2-2

Cisco IV アプリケーションへのアクセス 2-6

Cisco IV アプリケーションのホームページ 2-7

既知の適正な値（Known Good Values） 3-1

新しい KGV データのインストール 3-3

Cisco IV アプリケーションの設定 4-1

構成刻印値のリセット」 4-3

整合性モニタリング 5-1
デバイス ステータスの概要 5-2
リスク レベル フィルタの使用 5-3
リスク タイプ フィルタの使用 5-4
フィルタの削除 5-5
詳細なデバイス整合性測定結果の表示 5-5
整合性測定のタイプ 5-8
プラットフォームの整合性測定 5-8
ソフトウェアの整合性測定 5-12
ハードウェアの整合性測定 5-18
構成の整合性測定 5-20
サポート 6-1
システム要件 6-1
ハードウェアおよびソフトウェアの要件 6-1
テクニカル サポート 6-1
機能リクエスト 6-2
サポートされるプラットフォーム 6-2

はじめに

製品説明

Cisco Integrity Verification（IV）アプリケーションは、ネットワーク デバイスの整合性に関する測定値を自動的かつ継続的にモニタリングし、侵害の可能性を示唆する予期しない結果や不正な結果をすべて検知します。IV アプリケーションの目的は、侵害を早期に検出して、その影響を軽減することです。IV アプリケーションは、Cisco Application Policy Infrastructure Controller エンタープライズ モジュール（APIC-EM）内で動作します。

マニュアルの構成

このマニュアルの構成は、次のとおりです。

章	タイトル	説明
1	概要	IV アプリケーションに関する情報、関連するワークフロー、アプリケーションへのアクセス方法について説明します。
2	導入	APIC EM 環境内に IV アプリケーションを導入する方法を説明します。
3	既知の適正な値（Known Good Values）	デバイスから取得した整合性測定値を検証するために IV アプリケーション内で使用される既知の適正な値（ゴールデン ハッシュ）を保守する方法を説明します。
4	アプリケーションの設定	IV アプリケーションを構成してサービスやモニタリング機能を有効/無効にする方法を説明します。
5	整合性モニタリング	IV アプリケーションを導入して構成した後の使用方法を詳しく説明します。
6	サポート	サポートを受ける方法、サポートされているプラットフォーム、IV アプリケーションの新機能をリクエストする方法を説明します。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	コマンド、キーワード、およびユーザが入力するテキストは**太字**で記載されます。
イタリック体	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、*イタリック体*で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z }	必ずいずれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	いずれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
`courier` フォント	システムが表示する端末セッションおよび情報は、`courier` フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注）*読者に留意していただきたいこと*を示します。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

「注意：」は、*注意が必要なこと*を示しています。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

「警告：」は、安全上の重要事項です。

危険があることを示します。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。

これらの注意事項を保管しておいてください。

規制：追加情報および規制要件または顧客要件に準拠するために定められています。

関連資料

マニュアル	説明
Cisco APIC-EM Documentation Roadmap	すべての Cisco APIC-EM 製品のマニュアルの一覧が記載されています。このドキュメントは、コントローラとそのアプリケーションを最大限に活用できるようにすることを目的としています。次のリンク先のページに、Cisco IWAN を含め、すべてのドキュメントのリンクがあります。http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/tsd-products-support-series-home.html

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、Cisco Bug Search Tool（BST）の使用方法、サービス要求の送信方法、詳細情報の収集方法については、http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html で『What's New in Cisco Product Documentation』を参照してください。

『What's New in Cisco Product Documentation』は、シスコの新規および改訂版の技術ドキュメンテーションの一覧も示し、RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツをデスクトップに配信することもできます。RSS フィードは無料のサービスです。

概要

Cisco IV アプリケーションについて

Integrity Verification（IV）は、主要な製品データをモニタリングし、侵害の兆候（IOC）を表す予期しない変更や無効な値を検出します。その目的は、製品に対する不正な変更を検出するための時間を大幅に短縮し、侵害による影響を最小限に抑えることです。IV アプリケーションの主要なコンポーネントは次のとおりです。

- プラットフォーム内に組み込まれた、予期しない状況を検出するための技術と整合性測定機能
- 侵害の兆候に迅速に対応することを可能にする、実行時の整合性測定のモニタリングと可視性
- 攻撃を確認し、以降の攻撃を無効にできるよう、その攻撃元、目的、手段を判断するための詳細なオンライン/オフライン フォレンジック機能

IV アプリケーションは APIC-EM が提供する機能を利用してモニタリング対象のデバイスから整合性測定値を取得し、それらの測定値で正確さおよび予期しない変更の有無を評価して、その評価結果を詳しく確認できるようにします。表 1-1 に、IV アプリケーションでサポートしている整合性測定のタイプを記載します。また、詳細についての参照先も記載します。

表 1-1. 整合性測定のタイプ

測定のタイプ	機能	参照先
プラットフォーム	適正なデバイスであるかどうかを調べる機能。セキュア ブート プロセスの測定値およびデバイスのアイデンティティを検証します。	「プラットフォームの整合性」（5-8 ページ）
ソフトウェア	適正なデバイスで使用されるソフトウェアであるかどうかを調べる機能。ソフトウェア ファイルおよびメモリ内の内容をチェックします。	「ソフトウェアの整合性」（5-12 ページ）

ハードウェア	デバイスに含まれるハードウェア コンポーネントが期待されるものであるかどうかを調べる機能。ハードウェア インベントリをチェックします。	「ハードウェアの整合性」（5-18 ページ）
構成	デバイス構成に予期しない変更が加えられているかどうかを調べる機能。実行コンフィギュレーションをチェックします。	「構成の整合性測定」（5-20 ページ）

注：現時点では、Cisco IV アプリケーションは概念検証用およびトライアルとしてベータ版で提供されています。このソフトウェアは現在の形で綿密に開発およびテストされていますが、今後はこのリリースに含まれるコア機能に加え、他の機能も追加される予定です。IV アプリケーション（ベータ版）には以下の目的があります。

- Cisco の中核的な整合性検証機能の可用性を広め、お客様のネットワーク保護を強化すること
- この新しいセキュリティ ツールの有効性を高めるために今後必要となる機能を特定し、開発を推進できるよう、お客様からフィードバックをいただくこと

測定値の整合性と「No Detected Risk」

IV アプリケーションは、デバイスから整合性測定値を取得し、それらの値を期待される値または既知の適正な値と比較します。Cisco の新製品には、測定値の収集および取得プロセスの整合性を保護する技術が組み込まれていますが、すべての製品にこれらの技術が導入されているわけではありません。デバイスが侵害されていて、実際の測定値ではなく期待される測定値を提供するリスクは常にあります。

注：整合性検証ステータスが「No Detected Risk」となっている場合、以下のいずれかのシナリオを示唆します。

- デバイスから取得した整合測定値が、期待された値である。
- デバイスが整合性測定をサポートしていない。
- アプリケーションの [IV Settings] オプションを使用して整合性アセスメントが有効にされていない。

「No Detected Risk」ステータスは、必ずしもデバイスが侵害されていないことを示すわけではありません。侵害されたデバイスが誤解を招く測定値を提供するリスクを軽減するために、レガシー システムを Cisco のより新しい、よりセキュアな製品で更新してください。

Cisco IV アプリケーション ワークフローの概要

表 1-2. Cisco IV にアクセスするための基本的なワークフロー

番号	アクション	参照先
1	Cisco APIC-EM を導入する。	「Cisco APIC-EM の導入」（2-1 ページ）
2	IV アプリケーションの最新バージョンをインストールする。	「Cisco IV アプリケーションのインストールまたはアップグレード」（2-2 ページ） **注：**Cisco IV アプリケーションのダウンロード、インストール、有効化を行う前に、Cisco APIC-EM コントローラを導入する必要があります。
3	Cisco APIC-EM にログインして Cisco IV アプリケーションにアクセスする。	「Cisco IV アプリケーションへのアクセス」（2-6 ページ）
4	IV アプリケーションを構成して有効にする。	o 「既知の適正な値のインストール」（3-1 ページ） o 「IV アプリケーションの設定」（4-1 ページ）
5	デバイスの整合性をモニタリングする。	o 「整合性モニタリング」（5-1 ページ）

導入

APIC-EM 向け Cisco IV アプリケーション

「概要」で説明したように、Cisco IV アプリケーション（IV アプリ）は、Cisco APIC-EM を介して、APIC-EM ブラウザベースのインターフェイス内でツールとして動作します。APIC-EM コントローラまたは IV アプリケーションを導入して構成する際は、以下の考慮事項に注意してください。

Cisco IV アプリ固有のリリース スケジュールおよびリリース番号

Cisco IV アプリケーションについては、以下の点に注意してください。

- IV アプリは APIC-EM のリリース スケジュールから切り離され、APIC-EM のインストールやアップグレードのプロセスからも切り離されました。
- IV アプリのリリース番号は、APIC-EM のリリース番号とは関係がなくなりました。
- IV アプリを APIC-EM とは別にダウンロードし、APIC-EM の [App Management] ページを使用してインストールまたはアップグレードします。「Cisco IV アプリケーションのインストールまたはアップグレード」（2-2 ページ）を参照してください。

システム要件

IV アプリケーションには Cisco APIC-EM リリース 1.5.0.x が必要です。APIC-EM のシステム要件は、IV アプリに適用されます。リリース ノートに、APIC EM を含め、IV アプリのリリースと互換性のあるソフトウェアが記載されています。

Cisco APIC-EM の導入

Cisco IV アプリケーションには Cisco APIC-EM のグラフィカル ユーザ インターフェイス（GUI）からアクセスします。IV アプリを使用するには、まず Cisco APIC-EM を導入する必要があります。

Cisco APIC-EM は、サーバ（ベアメタル ハードウェア）または VMware vSphere 環境の仮想マシンに導入できます。Cisco APIC-EM はシングル ホストとして導入することも、複数ホスト環境に導入することもできます。

APIC-EM のインストレーション ガイドの手順に従って Cisco APIC-EM を導入してください。インストレーション ガイドは APIC-EM の [Install and Upgrade Guides] ページで入手できます。

Cisco IV アプリケーションのインストールまたはアップグレード

IV アプリケーションをインストールまたはアップグレードする前に

IV アプリをインストールする前に、以下の作業を行ってください。

- APIC-EM をまだインストールしていない場合は、APIC-EM のインストレーション ガイドの手順に従って Cisco APIC-EM をインストールします。インストレーション ガイドは APIC-EM の [Install and Upgrade Guides] ページで入手できます。必要に応じて、必要なパッチをインストールして APIC-EM を適切なリリースにアップグレードします。
- Cisco APIC-EM のリリース（リリース 1.5.0.x が必要）およびネットワーク内の他の要素のソフトウェア バージョンに、インストールする IV アプリのバージョンとの互換性があることを確認します。詳細については、リリース ノートを参照してください。

注：IV アプリを以前のリリースからアップグレードする場合、アップグレード後の IV アプリには、以前のリリースで実行した操作のログは引き継がれません。

推奨事項

- 現在の APIC-EM 設定のバックアップを作成してください。バックアップおよび復元の詳細については、APIC-EM のマニュアルを参照してください。基本的な手順は以下のとおりです。
  1. APIC-EM で、[Settings]（歯車ボタン）> [App Management] を選択します。
  2. [Backup & Restore] タブを選択します。
  3. [Create New Backup] ボタンをクリックします。
- 以前のリリースの IV アプリからアップグレードする場合は、アップグレードする前に IV の設定のバックアップを実行します。「バックアップと復元、リカバリ、および削除」を参照してください。

Cisco IV アプリケーションの導入手順

IV アプリケーションをダウンロード、インストール、有効化するには、以下の手順で説明するステップに従います。

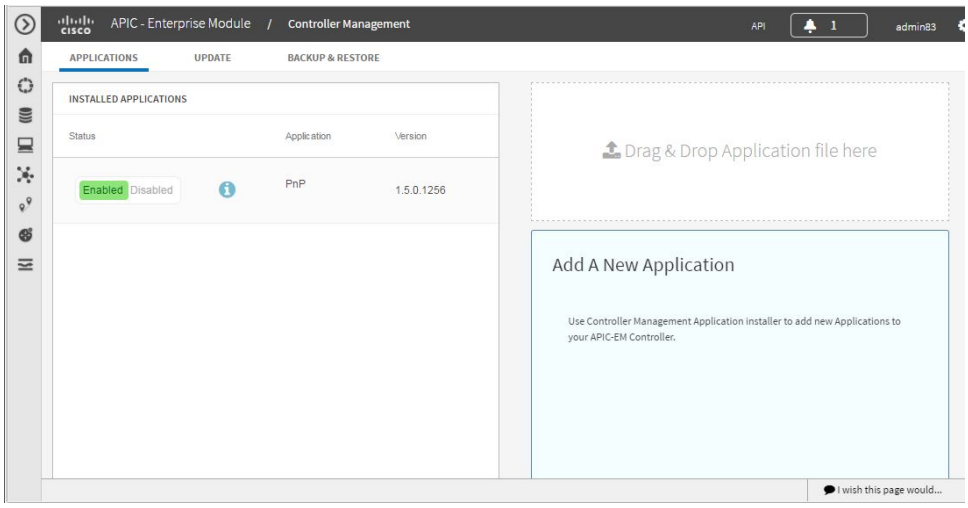
	手順
ステップ 1	シスコの [Download Software] ツールを使用して [Policy and Automation Controllers] に移動して APIC-EM を選択するか、または次の直接リンクを使用します。 https://software.cisco.com/download/type.html?mdfid=286208072&flowid=77162
ステップ 2	Cisco Integrity Verification アプリケーション（ベータ版）のソフトウェア オプションを見つけます。IV アプリケーションをダウンロードします。ダウンロードしたファイルの場所をメモします。

ステップ 3　APIC-EM を起動し、[APIC-EM Applications] ページを開きます。

a. [Settings]（歯車ボタン）> [App Management] を選択します。

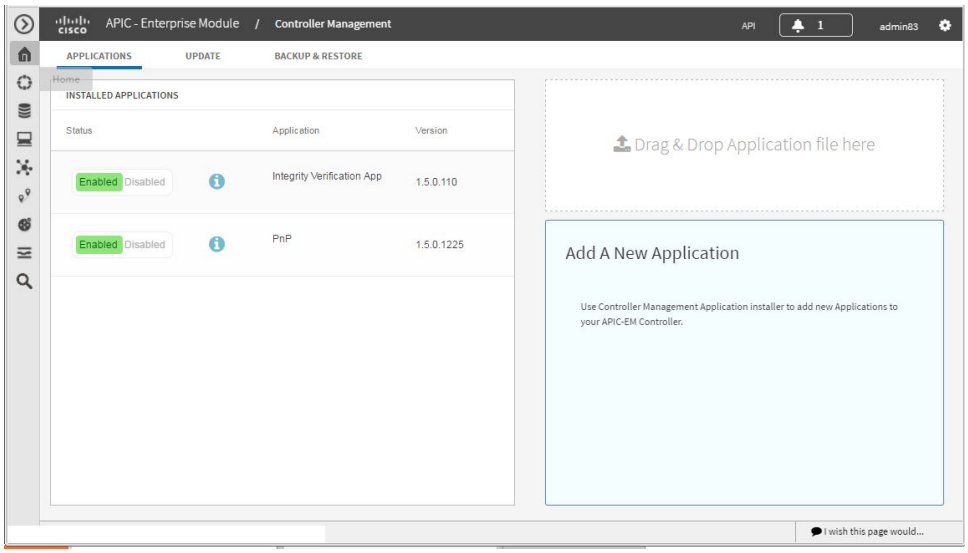
b. [Applications] タブが表示されることを確認します。

（以下の例は、APIC-EM にインストール済みの PnP アプリケーションを示しています。）



IV アプリがインストールされている場合は、そのバージョンが [Installed Applications] リストに表示されます。

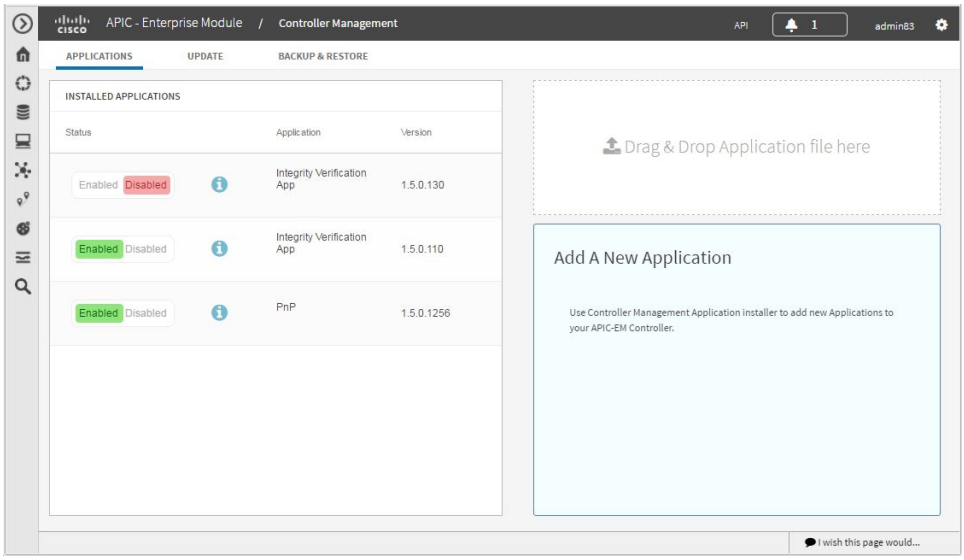
（下記の例に示されているのは、IV アプリケーションの旧リリースです）。



c. [APIC-EM Applications] ページの右側にある [Drag&Drop Application file here] ボックスに注目してください。

ステップ 4 ダウンロードした IV アプリ インストール ファイルを [Drag&Drop Application file here] ボックスにドラッグアンドドロップします。新しい IV アプリがアプリケーションのリストに示され、[Disabled] と表示されます。

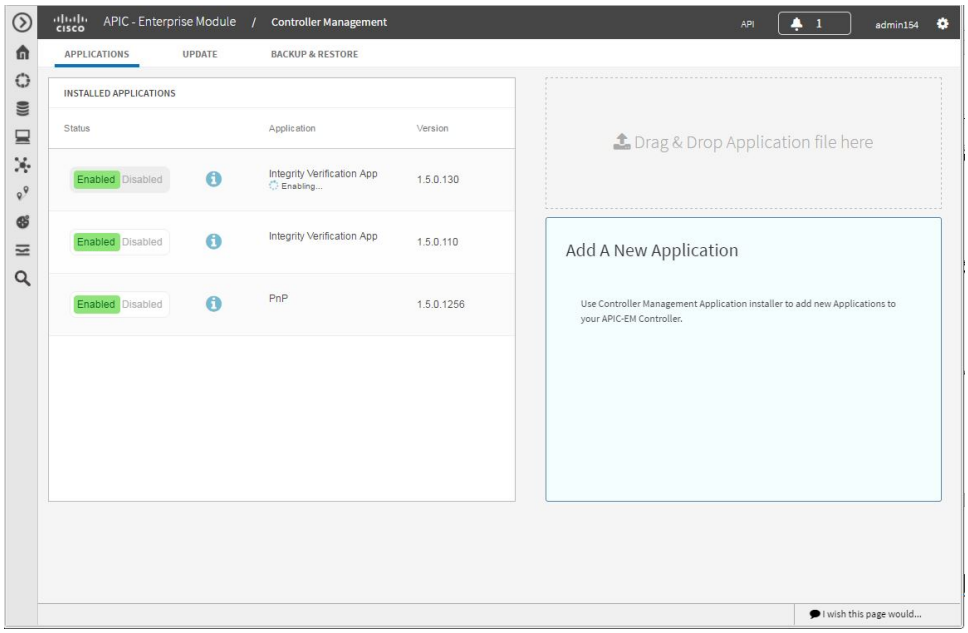
（下記の例に示されているのは、IV アプリケーションの旧リリースです）。

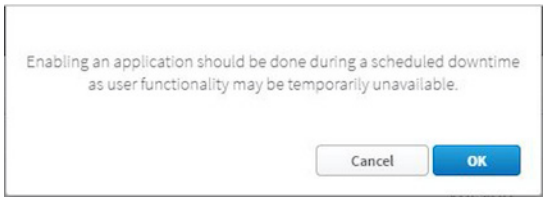


IV アプリの以前のバージョンからアップグレードする場合、インストールのこの時点では、IV の以前のバージョンが引き続きリストに表示されます。

ステップ 5　新しい IV アプリケーションの [Enabled] をクリックします。APIC-EM で新しいバージョンが有効になります。IV アプリの以前のバージョンからアップグレードする場合、APIC-EM は IV の既存の設定を保持します。ページには、有効化プロセスが進行中であることが示されます。処理が完了するまで待ちます。インストールの所要時間は、クラスタ サイズや他の要因に応じて異なります。

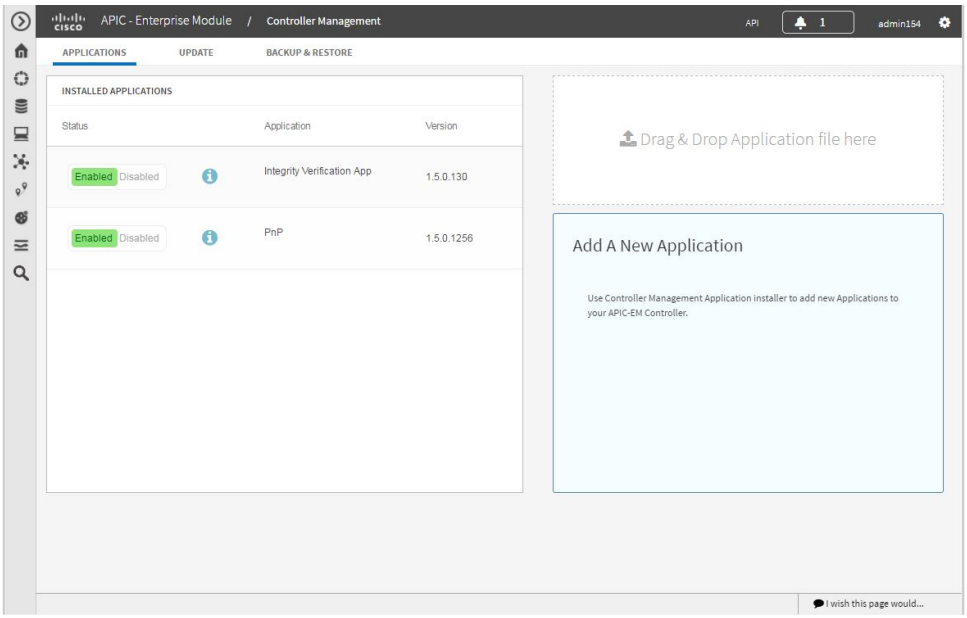
（下記の例に示されているのは、IV アプリケーションの旧リリースです）。





注：IV アプリケーションを有効にする際は、ポップアップ警告に十分注意してください。このプロセスには時間がかかることがあり、一時的に APIC-EM のユーザ機能に影響を及ぼす可能性があります。IV アプリケーションのインストールと有効化のプロセスは、予定されているダウンタイム時に実行してください。

ステップ 6 インストールと有効化が完了したら、ブラウザのキャッシュをクリアして [APIC-EM Applications] ページを更新します。[Status] 列に新しい IV アプリが有効であることが示され、[Version] 列に新しい IV アプリのバージョンが示されます。IV アプリの以前のバージョンはすべて、リストから削除されます。



Cisco IV アプリケーションへのアクセス

Cisco APIC-EM の GUI から Cisco IV アプリケーションにアクセスします。

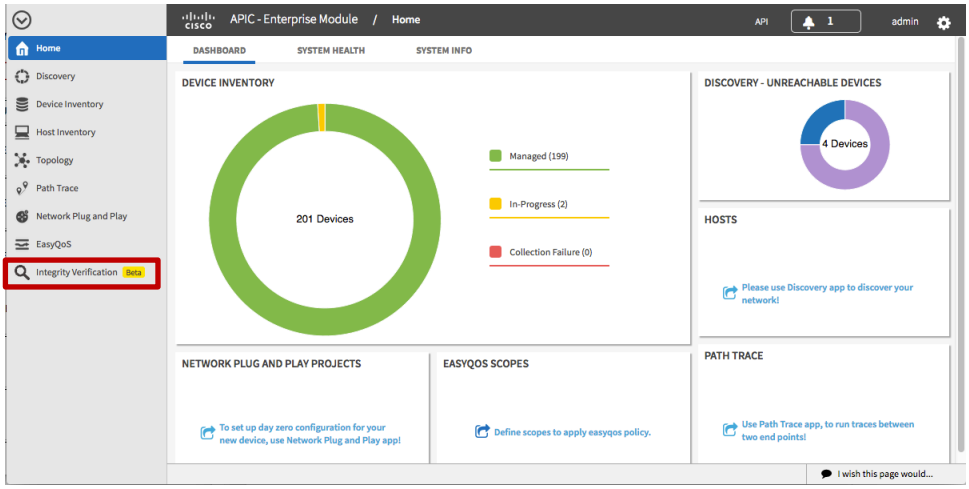
手順

ステップ 1 Google Chrome または Mozilla Firefox を使用して、Cisco APIC-EM の IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。

ステップ 2 ユーザ名とパスワードを入力して、[Log In] をクリックします。

ステップ 3 初めてログインした場合、テレメトリ情報の開示について確認し、[Confirm] をクリックします。Cisco APIC-EM GUI が表示されます。

ステップ 4 Cisco APIC EM GUI の左側のナビゲーション ペインで、[Integrity Verification Beta] アイコン をクリックします。Cisco IV アプリケーションのホームページが開きます。以下の Cisco IV アプリケーションのホームページを参照してください。



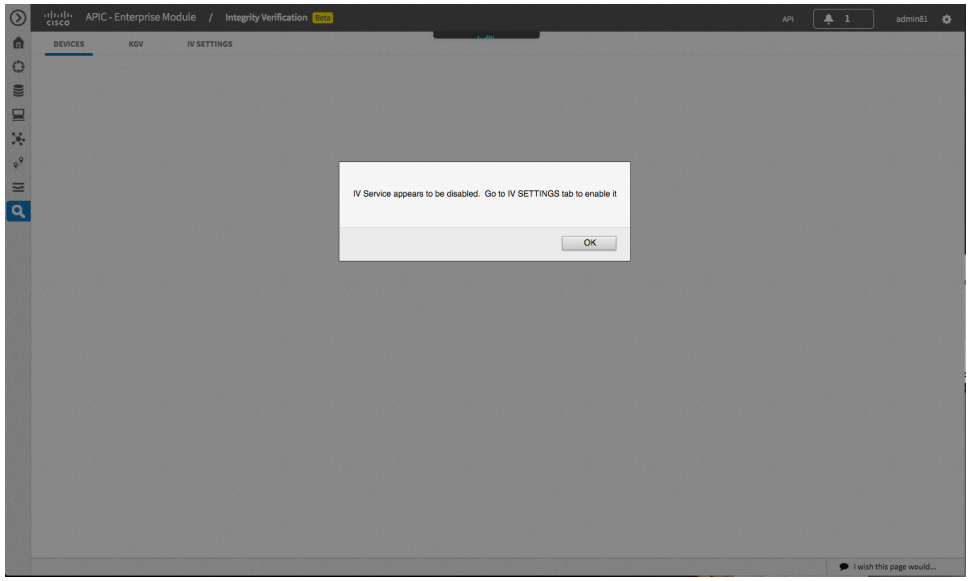
Cisco IV アプリケーションのホームページ

初期セットアップでは、Cisco IV アプリケーションのホーム ページに、IV サービスがまだ有効にされていないことが示されます。IV アプリケーションを構成して有効にする手順は次のとおりです。

1. IV アプリケーションに、最新の既知の適正な値（KGV）をロードします。「既知の適正な値（Known Good Values）」（3-1 ページ）を参照してください。

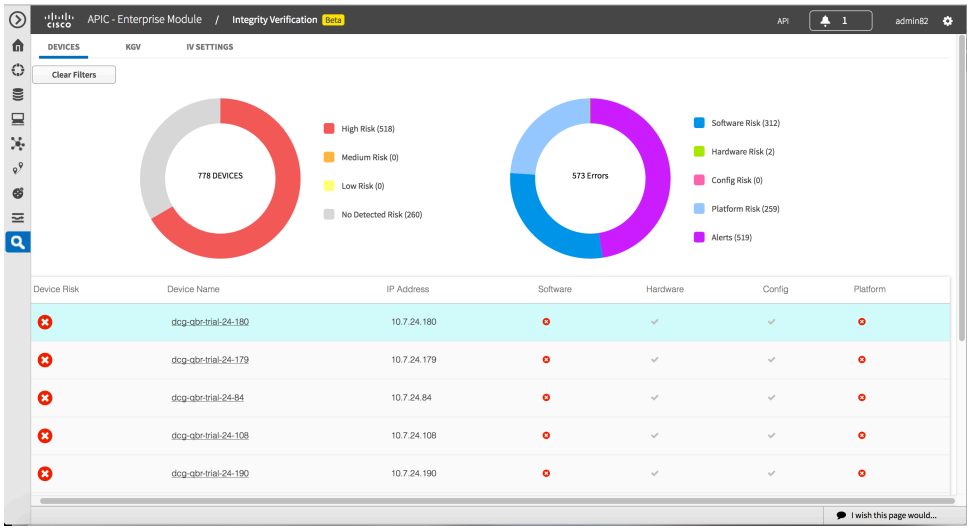
2. モニタリング対象の整合性測定のタイプを選択し、IV サービスを有効にします。「Cisco IV アプリケーションの設定」（4-1 ページ）を参照してください。

図 2-1. Cisco IV アプリのホーム ページ：新しいシステムへの最初のログイン



Cisco IV を設定してプロビジョニングすると、ホームページに追加情報が表示されます。たとえば、次の図に示すように、デバイス、デバイスの全体的なリスク、整合性測定のタイプ別リスクが表示されます。

図 2-2. Cisco IV アプリのホームページ：プロビジョニング後



タスク エリア	機能	参照先
DEVICES	侵害の兆候を表示および管理します。	「整合性モニタリング」(5-1 ページ)
KGV	既知の適正な値 (Known Good Values、KGV) をインストールおよび管理します。	「既知の適正な値」（3-1 ページ）
IV SETTINGS	IV アプリケーションのオプションを有効化および選択します。	「IV アプリケーションの設定」（4-1 ページ）

既知の適正な値（Known Good Values）

一定レベルのセキュリティの整合性を確保するためには、Cisco デバイスが適正かつ有効なソフトウェアを実行していることを検証する必要があります。現在、実際に運用されている Cisco デバイスには、適正な Cisco ソフトウェアを実行していることを確認するための評価基準がありません。Cisco IV アプリケーションが使用するシステムは、収集されたイメージ整合性データを Cisco ソフトウェアの既知の適正な値（Known Good Values、KGV）に照合します。

Cisco では、多くの Cisco 製品の KGV を含む KGV データ ファイルを作成して公開しています。標準の JSON 形式で作成されたこの KGV ファイルは、Cisco の署名が付けられた上で他のファイルと併せて KGV Combo Bundle にバンドルされ、Cisco から入手できるようになっています。

注：KGV データは次の URL に掲載されます。
https://tools.cisco.com/cscrdr/security/center/files/trust/Cisco_KnownGoodValues.tar

KGV ファイルを IV アプリケーションにロードして、ネットワーク デバイスから取得した整合性測定値を検証するために使用します。**注：**デバイス整合性測定値は、IV アプリケーションで利用でき、IV アプリケーション内でのみ使用されます。IV アプリケーションと cisco.com が接続されている必要はありません。KGV ファイルは保護された環境にエアギャップで転送して IV アプリケーションにロードすることができます。詳細については、新しい KGV データのインストール 下のを参照してください。

図 3-1.既知の適正な値フローの概要に、開発プロセスで KGV の初期収集を行うところから、cisco.com に KGV を掲載し、最終的に IV アプリケーションで KGV を使用するまでの流れを示します。

注：デバイス整合性測定値は、IV アプリケーションで利用でき、IV アプリケーション内でのみ使用されます。IV アプリケーションと cisco.com が接続されている必要はありません。KGV ファイルは保護された環境にエアギャップで転送して IV アプリケーションにロードすることができます。詳細については、新しい KGV データのインストール 下のを参照してください。

図 3-1.既知の適正な値フローの概要

現在 Cisco が作成している KGV データ ファイルには、以下のカテゴリのコンポーネント測定値が含まれます。

- ブート整合性の可視性ハッシュ
  - ブート 0
  - ブートローダ/ROMMON
  - OS イメージ
- 実行中イメージ ファイルのハッシュ

注：サービスをアクティブにする前に、KGV データを IV アプリケーションにロードする必要があります。

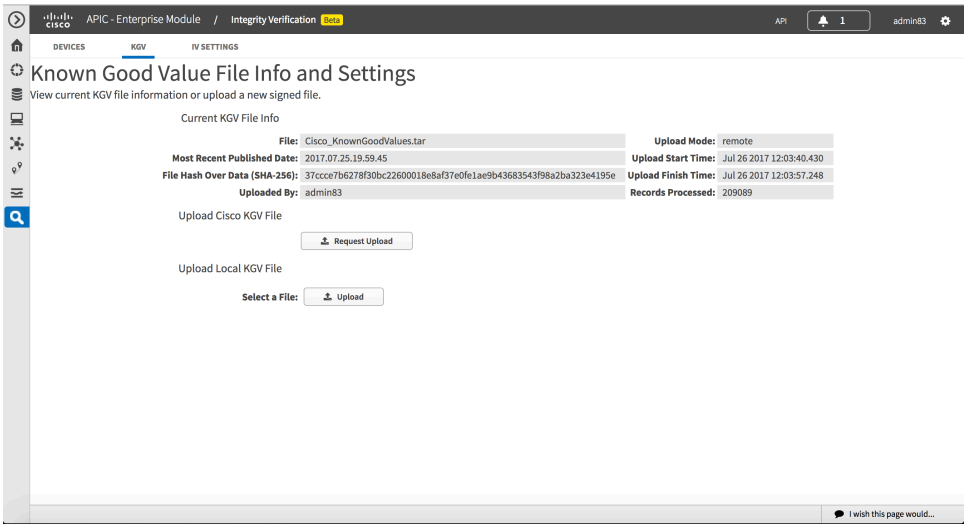
KGV システムにアクセスするには、IV アプリケーション画面の上部にある **[KGV]** をクリックします。これにより、現在ロードされている KGV に関する情報を示す KGV 画面が表示されます（図 3-2 を参照）。この画面上に、新しい KGV データを IV アプリケーションにアップロードするためのボタンがあります。

この画面に表示される主要な情報は以下のとおりです。

- **Most Recent Published Date:** 2017.06.14.18.54.51

これは、KGV データのスナップショットが取得されて公開された日時を示します。この日付が、IV アプリケーションのモニタリング対象デバイス上で使用されているすべてのソフトウェアの公開日よりも後になっていることが重要です。KGV の公開日以降に公開されたソフトウェアを使用していると、そのソフトウェアの KGV は IV アプリケーションで既知となっていないため、検証チェックは「**Failure**」の結果になります。

図 3-2. KGV 画面の情報



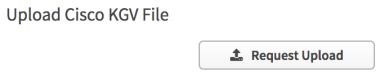
KGV の更新は定期的に行う必要があります。少なくとも、ソフトウェアの新しいバージョンをシステムに導入する際は、必ず KGV を更新してください。

注：KGV データを最新の状態に維持しておかないと、新しくインストールしたソフトウェアの KGV が IV アプリケーションで使用できないため、誤検出によるエラーが示される可能性があります。

新しい KGV データのインストール

新しい KGV データを IV アプリケーションにインストールするには 2 つの方法があります。

1. APIC-EM コントローラをインターネットに接続できる場合、[Request Upload] ボタンをクリックすることで、Cisco からの最新の KGV ファイルのダウンロードとインストールを同時に行うことができます。



2. または、最新の KGV データをシステムにダウンロードしてから、IV アプリケーションにインストールすることもできます。この方法では、APIC-EM コントローラをインターネットに接続する必要はありません。この方法を使用する場合は、表 3-1. KGV のアップロード手順に記載されている手順に従ってください。

表 3-1. KGV のアップロード手順

	手順
ステップ 1	以下のリンクを使用して、最新の KGV データをローカル システムにダウンロードします。 https://tools.cisco.com/cscrdr/security/center/files/trust/Cisco_KnownGoodValues.tar ファイルの保存先を覚えておいてください。ステップ 3 でその情報が必要になります。
ステップ 2	[Upload] ボタンをクリックします。
ステップ 3	お使いのシステムのファイル ブラウザ ウィンドウが表示されたら、ステップ 1 で KGV データを保存したディレクトリに移動します。 Cisco_KnownGoodValues.tar ファイルを選択し、[Open] をクリックします。
ステップ 4	KGV ファイルが IV アプリケーションに正常にアップロードされると、正常にアップロードされた KGV ファイルがウィンドウの上部に表示されます。

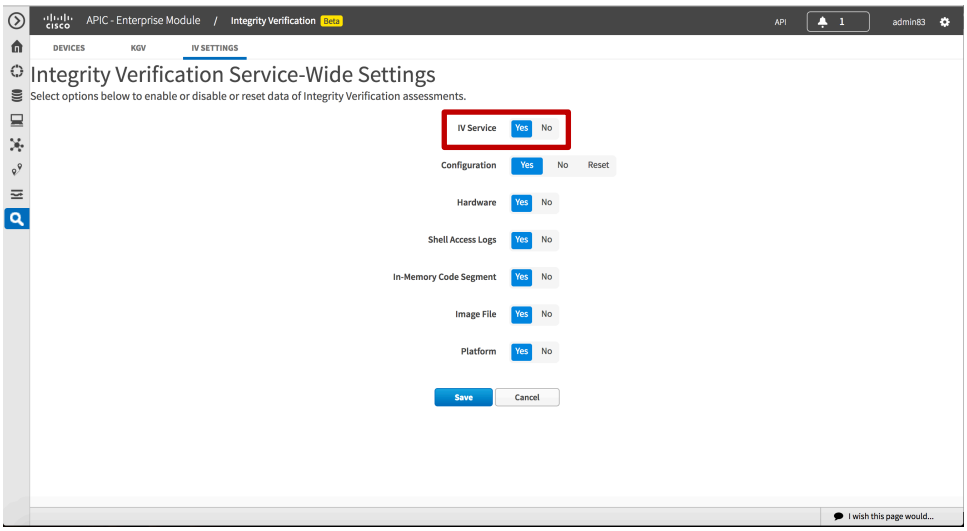
初期セットアップでは、KGV データのインストールが完了したら、「Cisco IV アプリケーションの設定」に進んで IV サービスを構成し、有効化します。

Cisco IV アプリケーションの設定

IV サービスは、デフォルトでは無効になっています。IV サービスを有効にするには、[IV Service] に対して [Yes] をクリックしてから、[Save] をクリックします。使用可能な設定については、表 4-1 で説明します。すべての設定に共通して、[Yes] をクリックするとその機能が有効になり、[No] をクリックすると無効になります。

注：IV サービスを有効にする前に、KGV 値がインストールされている必要があります。手順については、「既知の適正な値（Known Good Values）」（3-1 ページ）を参照してください。

図 4-1. IV 設定 - 初期の選択内容



注：IV アプリケーションを初めてアクティブ化すると、APIC がポーリングするデバイスのそれぞれに対して IV アセスメントが行われます。したがって、IV デバイス テーブルにすべてのデバイスが表示されるまでには、ポーリング期間の分だけ時間がかかります（ポーリング期間は、[APIC-EM Settings] ページの [DISCOVERY CREDENTIALS] セクションにある [Polling Interval] で [Polling Time] 値として定義されます）。

最も CPU 使用率が高いのは、IV アプリケーションがデバイスを初めて認識した時点、およびデバイスのリブートが検出された時点でのみ実行される IV アセスメントであるため、この最初のポーリング期間では IV アプリケーションでもデバイスでも追加処理能力が最も多く必要になります。以降のポーリング期間では、IV サービスが使用する処理能力は大幅に減ります。

図 4-2. IV 設定 - デフォルトの選択で有効にされるサービス

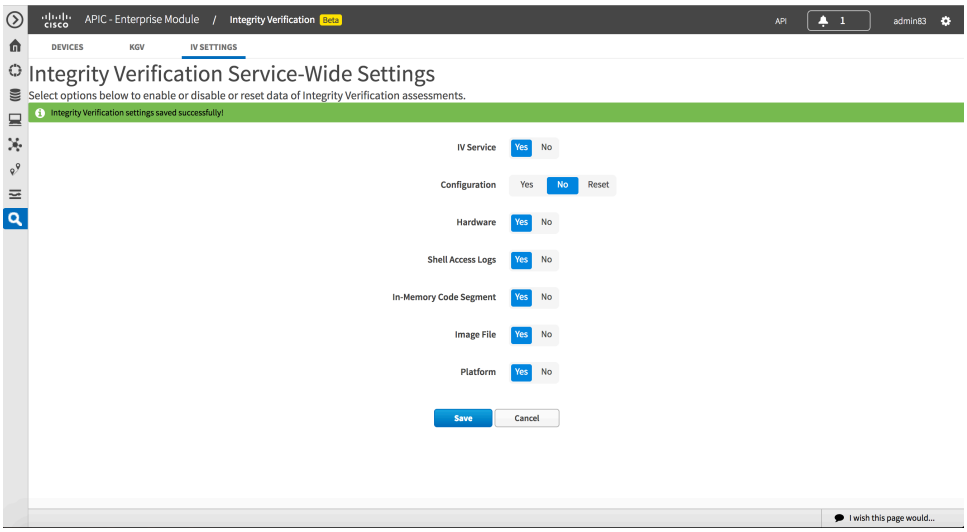


表 4-1. 整合性検証サービス全体の設定

設定	機能	参照先
IV Service	IV サービスのマスター オン/オフ スイッチ。すべての設定に共通して、[Yes] をクリックするとその機能が有効になり、[No] をクリックすると無効になります。	該当なし
Configuration	実行コンフィギュレーションの予期しない変更をモニタリングします。APIC-EM には同様の機能が備わっているため、このサービスはデフォルトで無効にされています。	「構成の整合性測定」（5-20 ページ）
Hardware	ハードウェア インベントリの予期しない変更をモニタリングします。	「ハードウェアの整合性」（5-18 ページ）
Shell Access Logs	シェル アクセスをサポートするデバイス上で、通常の運用中にシェル アクセスが行われることはありません。シェルへのアクセスを示すログ エントリの存在は、侵害の兆候です。	「ソフトウェアの整合性」（5-12 ページ）
In-Memory Code Segment	メモリ内のプログラム内容の予期しない変更をモニタリングします。	「ソフトウェアの整合性」（5-12 ページ）

Image File	KGV を使用して、ファイルに含まれるプログラム内容を検証します。	「ソフトウェアの整合性」（5-12 ページ）
Platform	KGV を使用してセキュア ブートの結果を検証し、プラットフォーム アイデンティティの有効性を確認します。	「プラットフォームの整合性」（5-8 ページ）

構成刻印値のリセット」

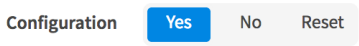
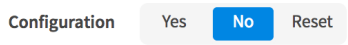
構成検証チェックでは、実行コンフィギュレーションを初期刻印値と照合します。初期刻印値は、IV アプリケーションによるデバイスの初期ディスカバリで取得されますが、 現在の構成に基づき、刻印値を再取得しなければならない場合もあります。その場合に考えられるシナリオは 2 つあります。

1. 現在、IV アプリケーションは APIC-EM 構成機能と統合されていません。APIC-EM が多数のデバイスに変更をプッシュした場合、IV アプリケーションはそれらの変更に予期しない変更としてフラグを立てるため、IV アプリケーション ユーザは個々のデバイスで変更を確認して個別に変更を承認しなければなりません。このような場合には、すべてのデバイスの刻印値を更新するために、リセット機能を使用できます。

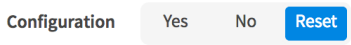
2. カスタマー フィードバックに応じて、IV アプリケーションは通常の期待される構成の変更（ntp クロック周期など）をマスクするように修正されています。リセット機能を使用することで、以前に予期しない変更としてフラグが立てられていたアイテムをクリアできます。

表 4-2. 構成のリセット手順で、リセット機能を使用するために必要な手順を説明します。このリセット機能を使用すると時間を節約できますが、既存の予期しない変更が隠れてしまうことがないよう、注意して使用してください。

表 4-2. 構成のリセット手順

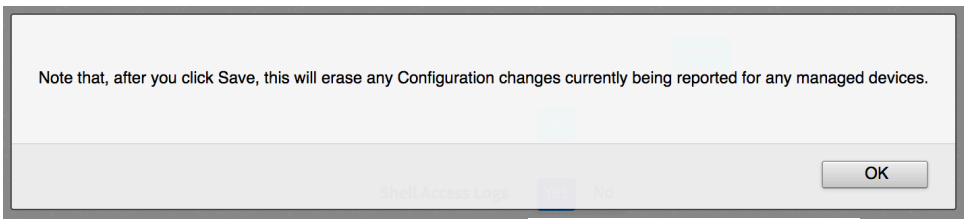
	手順
ステップ 1	現在の [Configuration] が [Yes] に設定されている場合：  設定を [No] に変更します。  [Save] をクリックします。 操作が完了したら、ステップ 2 に進みます。

ステップ 2



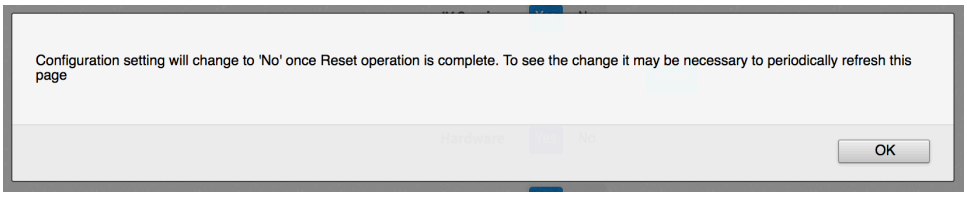
[Reset] をクリックします。

以下に示すポップアップ メッセージが表示されたら [OK] をクリックして、この操作によって、デバイス構成チェックに現在使用されている刻印値が消去されることを確認します。構成チェックでの次回のデバイス スキャンからは、新しい刻印値が使用されるようになります。

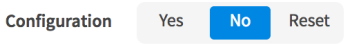


[Save] をクリックします。

以下に示すポップアップ メッセージが表示されたら [OK] をクリックします。「リセット」操作が完了すると [Configuration] 設定が [No] に変更されることを確認します。



操作が完了して [Configuration] が [No] に設定された状態になったら、ステップ 3 に進みます。



ステップ 3

構成チェックを再び有効にする場合は、設定を [Yes] に変更します。

[Save] をクリックします。

整合性モニタリング

IV アプリケーションは一連の検証テストを行う際に、デバイスから取得した情報を使用します。この情報を既知の適正な値または期待される値と比較して、その結果を記録します（表 5-3. 検証結果を参照）。各デバイスの結果は整合性測定タイプ（表 5-5. 整合性測定のタイプを参照）ごとのリスク レベル（表 5-1. IV リスク レベルを参照）に要約されます。全体的なリスク レベルもデバイスに割り当てられます。

「リスク レベル」は、デバイスの検証テストの不合格が侵害の兆候である可能性の高さを表します。IV アプリケーションではデバイスの整合性を確認できますが、デバイスが侵害されている、または侵害されていないと断言することはできません。また、そうすることもしません。

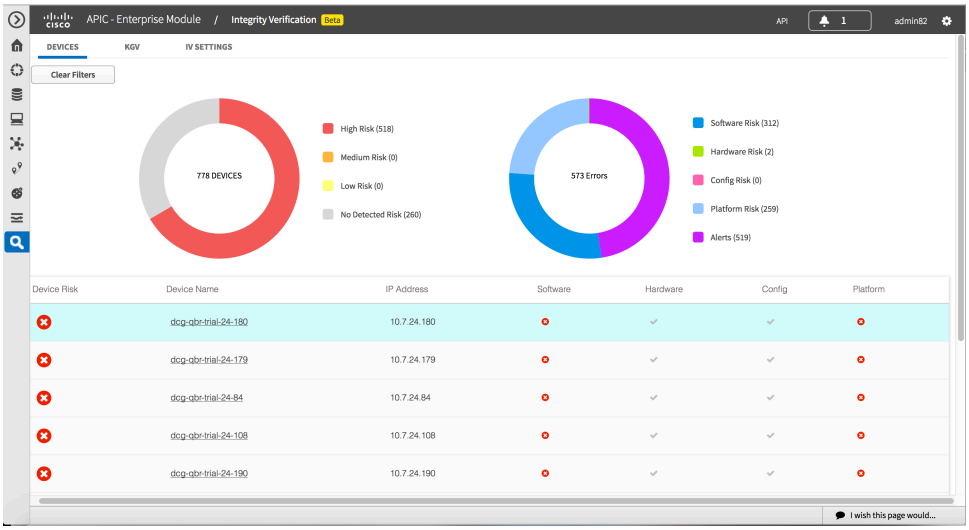
例えて言うなら、リスク レベルは自動車の燃料計のようなものです。私たちは燃料計を見て、燃料タンクにどれくらいの燃料が残っているのかを判断します。燃料計の情報を信じがちですが、燃料計が故障する可能性もあります。その場合、燃料計にはタンクが満タンであると示されていても、燃料切れになるでしょう。ドライバーによっては、燃料計が正しい情報を報告しているかどうかを判断するために他の情報も頼りにします。その一例は、タンクを満タンにしてからの走行距離です。通常タンクに燃料を補充する段階になるまでの走行距離に近づいてくると、ドライバーはアクションをとります。これと同様に、IV アプリケーションが提供する結果も、デバイスの整合性を示す多くの指標のうちの 1 つであると考えてください。燃料切れが発生する原因は、多くの場合、故障した燃料計よりも、燃料計に注意を払っていないことにあります。燃料計と同じく、IV アプリケーションが提供するデバイスの整合性についての洞察は、貴重ではあるものの、絶対に確実とは言えません。

整合性検証テストの結果は、Cisco IV アプリケーションの [DEVICES] タブに表示されます。[DEVICES] ウィンドウの上部には、結果の詳細な分析に役立つフィルタリング機能と併せて、結果の要約が 2 つの円で表示されます。

左側の円は、全体的なリスク レベルを示します。右側の円は、測定タイプ別のリスクを示します。

画面の中心部分には、Cisco IV アプリケーションがモニタリングするすべての Cisco デバイスがリストされ、各デバイスの全体的なリスク レベルと測定固有のリスク レベルが表示されます。

図 5-1. IV アプリケーション（ベータ版）– [DEVICES] タブ



デバイス ステータスの概要

IV アプリケーションのモニタリング対象デバイスごとに、全体的および個別の測定タイプごとのリスク・レベルが示されます。デバイスのホスト名またはリスク アイコンのいずれかをクリックすると、その測定結果に関する詳細情報が表示されます。詳細については、「詳細なデバイス整合性測定結果の表示」（5-5 ページ）を参照してください。

デバイス リストのエントリは、列見出しをクリックして並べ替えることができます。さらに、以降のセクションで説明するフィルタ機能を使用して調査の対象を絞り込むこともできます。

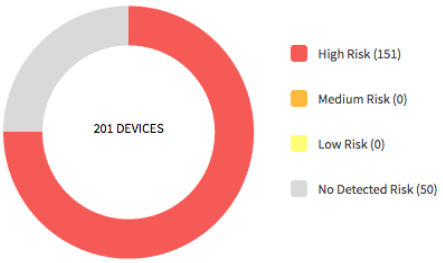
表 5-1. IV リスク レベル

リスク レベル	説明
高リスク	通常、このリスク レベルは正誤条件に対応し、チェック対象のファイルのハッシュは既知の適正な値（すなわち、適正なソフトウェア ファイルのハッシュ）ではありません。詳細については、表 5-2 の「ソフトウェア リスク」と「プラットフォーム リスク」の説明を参照してください。 エラー ステータスを詳しく調べて、エラーの原因が以下のいずれかであるかどうかを判断する必要があります。 • デバイス上で実行されているソフトウェアの既知の適正な値が IV アプリケーションにインストールされていない。（「既知の適正な値（Known Good Values）」（3-1 ページ）を参照） • デバイス上で実行されているソフトウェアの既知の適正な値を Cisco がまだ公開していない。（「サポートされるプラットフォーム」（6-2 ページ）を参照） • デバイス上で実行されているソフトウェアが改ざんされている。 注：デバイスの全体的なリスク レベルなどの要約リスク レベルは、累積的なものです。何らかの問題がある場合、整合性チェックのエラーの数が多ければ、それだけ確実な証拠になります。

中リスク	通常、このリスク レベルは、デバイスでは一般にまれなイベント（リモート シェル アクセス、ハードウェア インベントリの変更など）に対応します。詳細な結果と組織の運用ドキュメンテーションを詳しく調べて、変更がデバイスでの最近のメンテナンス アクティビティ（追加モジュールのインストールなど）の結果であるか、それともさらに調査が必要な不正なアクティビティであるどうかを判断してください。 詳細については、表 5-2 に記載されている「ハードウェア リスク」の説明を参照してください。
低リスク	システム構成で予期しない変更が検出されたことを示します。変更を調べて、その変更が本当に予期されないものであるのか、あるいは IV アプリケーションに統合されていないシステムによる変更であるのかどうかを判断してください。詳細については、表 5-2 に記載されている「構成リスク」の説明を参照してください。
検出されたリスクなし	整合性テストは不合格ではありません。また、予期しない変更も示されませんでした。ただし、必ずしもデバイスが侵害されていないことを意味するわけではありません。詳細については、「測定値の整合性と「No Detected Risk」」（1-2 ページ）を参照してください。

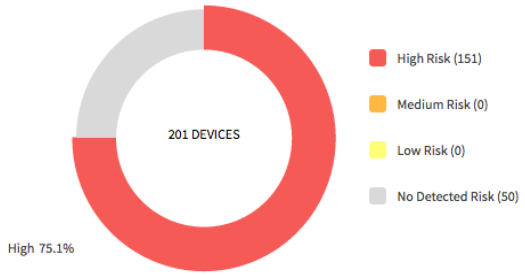
リスク レベル フィルタの使用

選択した全体リスク レベルを持つデバイスのみを表示するには、目的のリスク レベルに対応する円のセグメントをクリックします。



円の中心に示されている数字は、IV アプリケーションでモニタリングしているデバイスの合計数です。

円のスライスの上にカーソルを置くかマウスのポインターを合わせると、選択したリスク レベルを持つデバイスのパーセンテージが表示されます。



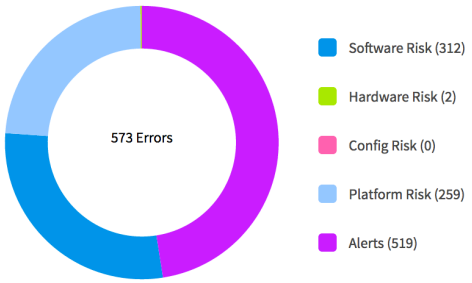
リスク タイプ フィルタの使用

IV アプリケーションで使用されているリスク タイプを表 5-2. IV 測定タイプ別リスクに記載します。

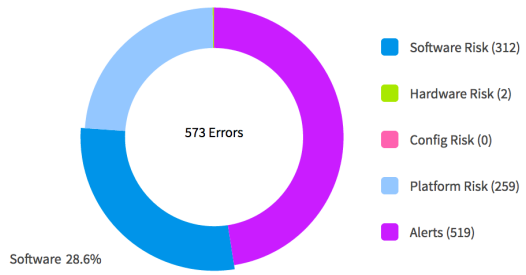
表 5-2. IV 測定タイプ別リスク

リスク タイプ	説明
ソフトウェア	1 つ以上の「ソフトウェア」整合性測定テストに不合格だったデバイスのみをフィルタリングして表示します。詳細については、「ソフトウェアの整合性」（5-12 ページ）を参照してください。
ハードウェア	1 つ以上の「ハードウェア」整合性測定テストに不合格だったデバイスのみをフィルタリングして表示します。詳細については、「ハードウェアの整合性」（5-18 ページ）を参照してください。
構成	1 つ以上の「構成」整合性測定テストに不合格だったデバイスのみをフィルタリングして表示します。詳細については、「構成の整合性測定」（5-20 ページ）を参照してください。
プラットフォーム	1 つ以上の「プラットフォーム」整合性測定テストに不合格だったデバイスのみをフィルタリングして表示します。詳細については、「プラットフォームの整合性」（5-8 ページ）を参照してください。
アラート	整合性検証機能に対するデバイスのサポートに関する主要な側面を強調する通知アラート。このリリースの IV アプリでは、「プラットフォーム」リスク タイプの主要なコンポーネントである「ブート整合性の可視性」（BIV）機能をサポートしていないデバイスを明らかにするために、アラートが使用されます。BIV 機能とこの機能を実装するために使用されている基礎的なデバイス保護技術（イメージ署名、セキュア ブート、セキュア アイデンティティ（SUDI））は信頼できるシステムの要となりつつあります。そのため、Cisco では、ネットワーク内に存在する高リスクのプロファイルを持つデバイスを、お客様が識別できるよう支援することが重要だと考えています。お客様は、そのようなデバイスがネットワーク内でサービスを提供している場所を評価して、このリスク増大を受け入れるかどうかに対する組織の姿勢、およびとるべきアクションを判断する必要があります。

選択したリスク タイプを持つデバイスのみを表示するには、目的のリスク タイプに対応する円のセグメントをクリックします



円のスライスの上にカーソルを置くかマウスのポインターを合わせると、選択したリスク タイプを持つデバイスのパーセンテージが表示されます。

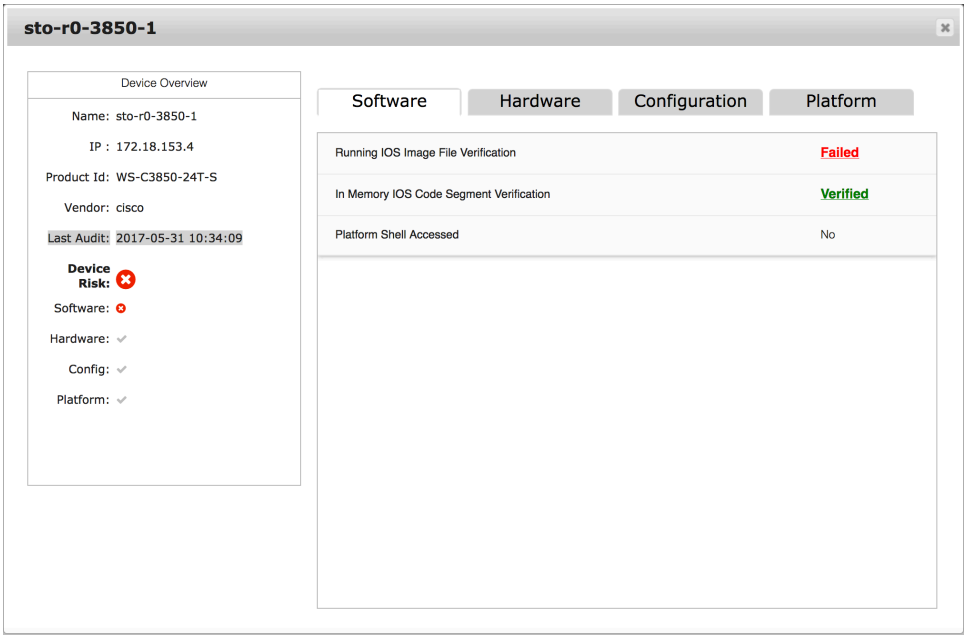


フィルタの削除

フィルタを削除してすべてのデバイスを表示するには、ウィンドウの左上にある Clear Filters ボタンをクリックします。

詳細なデバイス整合性測定結果の表示

デバイスの名前またはそのリスク アイコンのいずれかをクリックすると、詳細な測定検証情報を表示するウィンドウが開きます。



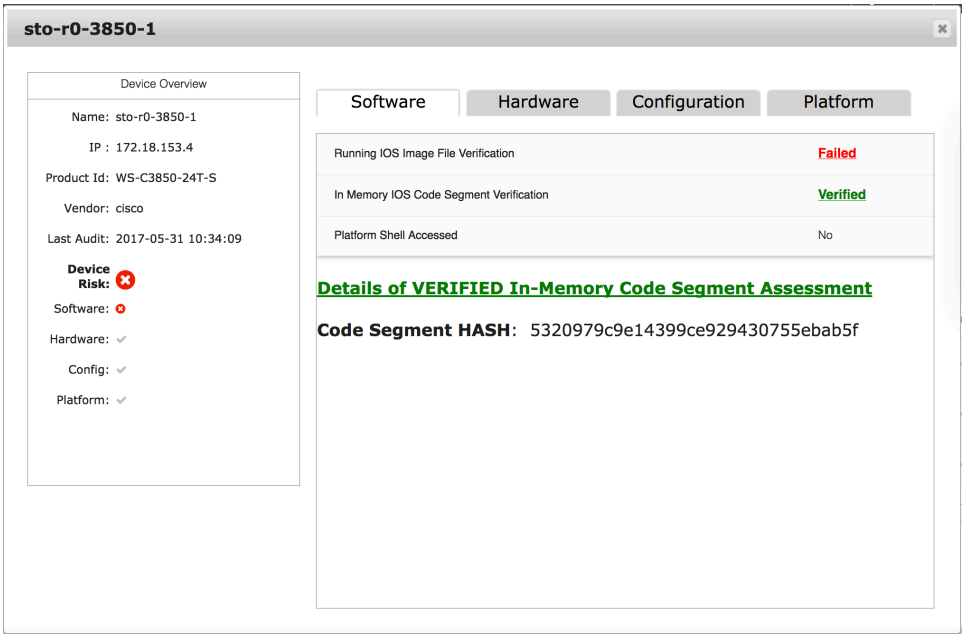
ウィンドウの左側には、結果の概要が表示されます。このうち重要な情報は、「Last Audit」です。ここには、このデバイスで最後に実行された整合性検証チェックのタイムスタンプが示されます。

ウィンドウの右側には、整合性測定タイプ別のタブがあります。これらのタブの内容は一貫しています。最上部のセクションには、実行されたテストとその結果が表示されます。結果は次のいずれかになります。

表 5-3. 検証結果

結果	説明
Verified	テストが実行されて、合格しました。
Failed	テストが実行されましたが、不合格でした。
Yes / No	モニタリング対象のイベントが観測されたかどうかを示します。
Unverified	「Verified」または「Failed」以外の結果です。以下の原因が考えられます。 • 該当するアセスメントに対し、IV サービス全体のアセスメントが非アクティブになっている（[No] に設定されている）。 • アセスメント（すなわち CLI）がそのデバイスでサポートされていない。 • デバイスがコマンドを認識しなかった。 • デバイスとの接続がダウンしている。 • イメージ ファイル アセスメントの「ファイルが不明」であった（つまり、ファイルが認識されなかったかデバイス上に存在していなかった（CLI が送信された場合）、ファイル パスがオフボックスであった（tftp）、コマンドが送信されていないなど）。

結果に下線が付いている場合、その結果をクリックすると、該当するテストの詳細が表示されます。以下のスクリーン ショットに、「**Verified**」をクリックした場合の例を示します。



現在、検証チェックには 3 つの主要なタイプがあります。

表 5-4. IV 検証チェックのタイプ

検証チェック	説明
既知の適正な値（Known Good Values、KGV）	KGV のアセスメントでは、デバイスからさまざまな整合性データを収集し、そのデータを Cisco 提供の既知の適正な値データベースと比較して、有効なデータであるかどうかを判別します。 一般的な検証エラーの原因と、エラーをクリアするための方法は、以下のとおりです。 1. チェック対象のアイテムが侵害されている - このエラーをクリアする唯一の方法は、侵害されたアイテムを適正な Cisco ソフトウェアのバージョンで置き換えることです。 2. チェック対象のアイテムの KGV がない - このエラーをクリアするには、該当するアイテムの KGV をインストールします。 上記のいずれの場合も、次回の APIC-EM ポーリング間隔で関連する整合性検証チェックがデバイスに対して行われると、エラーがクリアされます。
刻印値	刻印値のアセスメントでは、デバイスからさまざま整合性データのスナップショットを収集し、そのデータのスナップショットを「刻印値」として使用します。一定の期間にわたってデータが収集され、そのデータが「刻印値」と比較されて、データが期待される値から変更されているかどうかが評価されます。これらのチェックは単純な比較によるチェックですが、侵害の兆候（IoC）を検出する上での貴重なツールとなります。 これらのエラーをクリアするには、新しい値を有効な値として受け入れ、以降の整合性検証チェックではそれらの値を新しい刻印値として使用します。 注意：**誤った変更やデバイスまたはネットワークの運用に有害な変更が隠れていないことを確認するために新しい情報を調べる際は、特に注意してください。新しい情報が正確であると 100 パーセント確信できる場合にのみ、Accept Changes をクリックしてください。**
イベントの発生	これらのアセスメントでは、通常の運用中には発生しないイベントを探します。たとえば、通常の運用中に「シェル アクセス」イベントが観測された場合、それは IoC である可能性があります。 これらのエラーをクリアするには、イベントを有効なイベントとして受け入れます。 注意：**このイベントをクリアする前に、プラットフォーム シェルに誰が、なぜアクセスしたのかを必ず把握してください。シェル アクセス中にデバイスが不正に改ざんされていないと 100 パーセント確信できる場合にのみ、Accept Changes をクリックしてください。**

整合性測定のタイプ

表 5-5. 整合性測定のタイプ に、IV アプリケーションが実行する検証チェックのカテゴリを記載します。

表 5-5. 整合性測定のタイプ

測定のタイプ	機能	参照先
プラットフォーム	適正なデバイスであるかどうかを調べる機能。セキュア ブート プロセスおよびデバイスのアイデンティティを検証します。	「プラットフォームの整合性」（5-8 ページ）
ソフトウェア	適正なデバイスで使用されるソフトウェアであるかどうかを調べる機能。ソフトウェア ファイルおよびメモリ内の内容をチェックします。	「ソフトウェアの整合性」（5-12 ページ）
ハードウェア	デバイスに含まれるハードウェア コンポーネントが期待されるものであるかどうかを調べる機能。ハードウェア インベントリをチェックします。	「ハードウェアの整合性」（5-18 ページ）
構成	デバイス構成に予期しない変更が加えられているかどうかを調べる機能。実行コンフィギュレーションをチェックします。	「構成の整合性測定」（5-20 ページ）

整合性測定の各タイプについての詳細は、実行される検証チェック、エラーが特定された場合に提供されるデータの例を含め、以降のセクションで説明します。

プラットフォームの整合性測定

Cisco IV アプリケーションが取得する測定値によって、プラットフォームの整合性について、以下の質問に対する答えを見つけることができます。

- デバイスが適正な Cisco ハードウェアであるかどうか。
- デバイスは適正な Cisco ソフトウェアを使用してブートしたかどうか。
- デバイスは本当に期待されるデバイスであるかどうか。

表 5-6. プラットフォームの検証チェック に、これらの質問の答えを見つけるために実行される検証チェックを記載します。

表 5-6. プラットフォームの検証チェック

検証チェック	機能	説明
セキュア アイデンティティ	デバイスの真のアイデンティティを調べる機能	高リスク セキュア アイデンティティの検証チェックでは、デバイスのアイデンティティまたは関連する証明書チェーンを認証できない場合、「**Failure**」が宣言されます。 ブート整合性の検証チェックでは、デバイスのブートに使用されたソフトウェアの整合性測定値を Cisco で公開している KGV と比較します。ブート ソフトウェアに対応する KGV が見つからない場合、「**Failure**」が宣言されます。 デバイスからの応答を認証できない場合も「**Failure**」が宣言されます。 これらの検証チェックの両方で、Cisco のブート整合性の可視性（BIV）機能が提供する機能が使用されます。 BIV 機能については、次のリンク先のドキュメントで説明しています。 http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3650/software/release/16-3/configuration_guide/b_163_consolidated_3650_cg/b_163_consolidated_3650_cg_chapter_01110010.pdf BIV をサポートしているプラットフォームは、表 6-3.ブート整合性の可視性に対するサポートに記載されています。 これらの検証チェックは、IV アプリが新しいデバイスおよびデバイスのリブートを検出した時点で実行されます。
ブート整合性	デバイスのブートに使用されたソフトウェアのバージョンと、そのソフトウェアが適正な Cisco ソフトウェアであるかどうかを調べる機能	

セキュア アイデンティティの検証チェックでは、デバイスのアイデンティティおよび関連する証明書チェーンの両方が検証されます。検証には、デバイスのトラスト アンカーに格納されているデバイスのセキュア アイデンティティ証明書、証明書に関連付けられている秘密キー、リプレイ アタックを防ぐためのナンス、信頼性を確保するための暗号化が使用されます。以下の例に、証明書チェーンのいずれかのアイテムが無効な場合に表示されるエラーを示します。図 5-2. セキュア アイデンティティ チェック - 詳細なエラー情報に、この画面で提供されるすべての情報が表示されています。

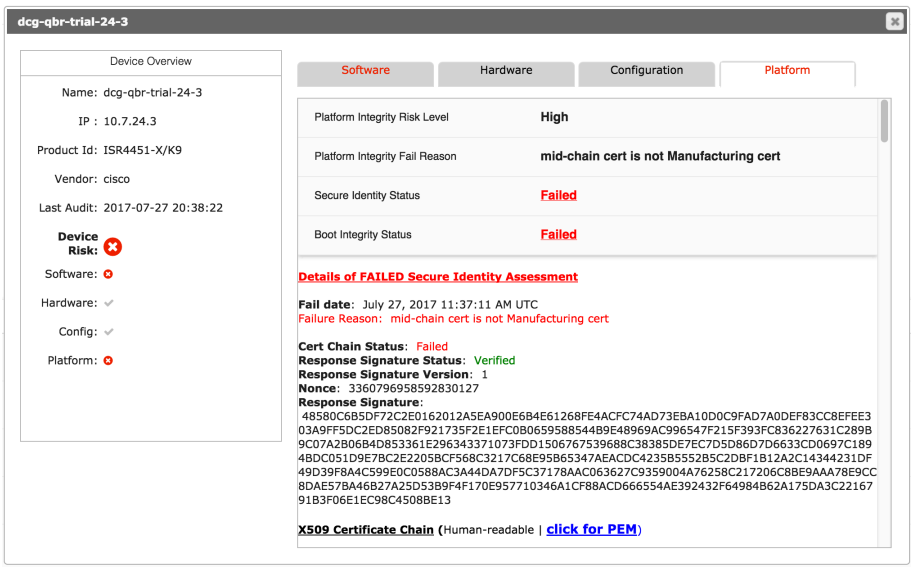


図 5-2. セキュア アイデンティティ チェック - 詳細なエラー情報

Details of FAILED Secure Identity Assessment

Fail date: July 27, 2017 11:37:11 AM UTC
Failure Reason: mid-chain cert is not Manufacturing cert

Cert Chain Status: Failed
Response Signature Status: Verified
Response Signature Version: 1
Nonce: 3360796958592830127
Response Signature:
48580C6B5DF72C2E0162012A5EA900E6B4E61268FE4ACFC74AD73EBA10D0C9FAD7A0DEF83CC8EFEE303A
9FF5DC2ED85082F921735F2E1EFC0B0659588544B9E48969AC996547F215F393FC836227631C289B9C07A2
B06B4D853361E296343371073FDD1506767539688C38385DE7EC7D5D86D7D6633CD0697C1894BDC051D9
E7BC2E2205BCF568C3217C68E95B65347AEACDC4235B5552B5C2DBF1B12A2C14344231DF49D39F8A4C59
9E0C0588AC3A44DA7DF5C37178AAC063627C9359004A76258C217206C8BE9AAA78E9CC8DAE57BA46B27
A25D53B9F4F170E957710346A1CF88ACD666554AE392432F64984B62A175DA3C2216791B3F06E1EC98C45
08BE13

X509 Certificate Chain (Human-readable | **click for PEM**)

-----BEGIN CERTIFICATE-----
<省略>
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
<省略>
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
<省略>
-----END CERTIFICATE-----

ブート整合性のチェックでは、デバイスのブートに使用されたソフトウェアを検証するために、セキュア ブート プロセス中にトラスト アンカーに格納された関連するファイルの整合性測定値を抽出し、リプレイ アタックを防ぐためのナンスと暗号化を使用して信頼性を確保します。図 5-3. ブート整合性チェック - 詳細なエラー情報 下のに、ソフトウェアが侵害されている場合に表示されるエラーを示します。「**Boot Integrity Signature Status: Verified**」ステータスは、デバイスから情報が正常に取得され、その情報が認証されたことを意味します。ただし、デバイスのブートに使用されたイメージは、IV アプリケーションで適正なイメージとして既知になっていないものです。

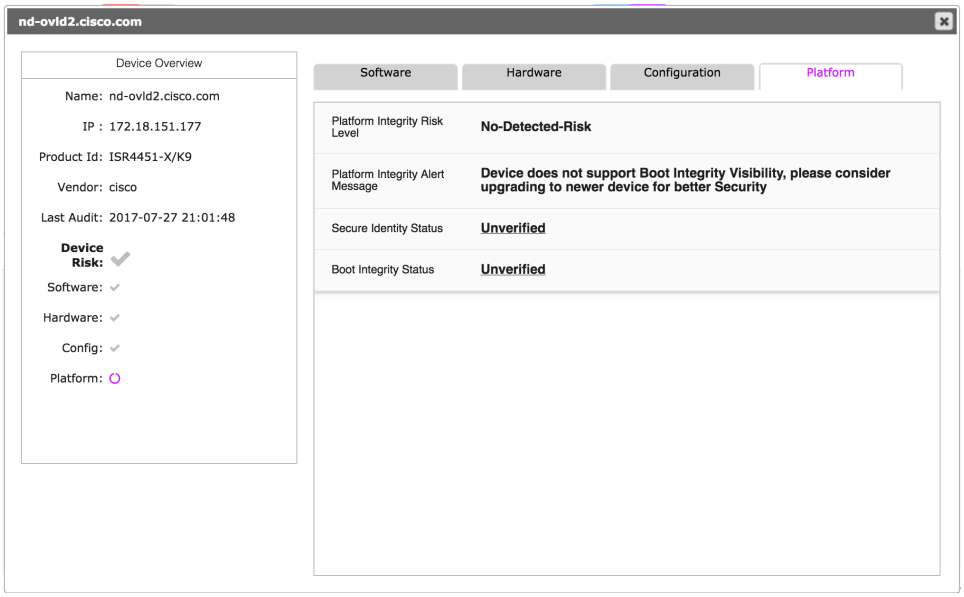
図 5-3. ブート整合性チェック - 詳細なエラー情報

Details of FAILED Boot Integrity Assessment

Fail date: June 14, 2017 5:57:53 PM UTC
Failure Reason: unknown boot0 Measurement
Boot Integrity Signature Status: Verified
Boot Integrity Signature Version: 1
Boot Integrity Signature:
9727755BAFE52F252CADCB9AF3B088738175A149DB0CD01B172F40F50ABC63B3F85571
73F401DD771CF15DCFFE8F8AC819E60AA0FB643B2EF250ECCB1CDF85DFBF2C7187B01F
A1B8AE3DD8CE4DF593177B3192E202210C46565D9E487F7B162CF01C96BDE88C91823A
BB973FA530A7E6D24F6194FB662B42FD0891022031B3426DE2D025D71772A27D60C0DD2
D2FBED3F21D9DA76AF0A5E57B5904CC4C2E5FF4CEEA4B3D6C89DBBEC71A4107B0B97F
A46897DF06EC7EF8614318F09DF8BA92B6C4ED4F62CB5BE6033DAEB265F3D485DE5524B
685DEBD8E0136F9F744EC115A33234015A0B08A42E89CC9DE706AF6831F3119D48A29B2
69DA4FD37CB42D471669
Boot Integrity Signature Nonce: 13852234143476132704
Boot 0 Status: Failed
Boot 0 Version: F01001R06.03c1d3d202013-01-18
Boot 0 Hash:
60FE9BB990E9ED6931D4CBB3BB9DD2703195B6710FE878C1C65CAE2A1FF84F11
Boot Loader Status: Verified
Boot Loader Version: 16.2(1r)
Boot Loader Hash:
515A951D7C54395AA0FCD15DCBBE69BDAA1FD1DD2DBD8D1D94436718E1903BD67D5A9
D08AA426C1A8EFE5797A5EDF532E371220DCC8F757BA6A9AEA962B20F70
OS Image Status: Verified
OS Image Version: 16.04.01
OS Image Hash:
40601905E08A02593D500C0A4C3B156AEB807389BEC2F1DB49900E8981190CADBE8EE0E
558BF8C6EBB94B81A4DB96669AB2CB281A9518555101C797B263A5877
PCR0: 81891910E20EDAD7144CE18AABD2246C0FC8E7E4F4FDE4B814B6D5375058168D
PCR8: 6C209FDC95C25D303578F4AC229773849AD052B9AF1D343F3DBE6BD7C6307D25

注：図 5-4. ブート整合性チェック - 未検証には、強調すべき特殊なケースが示されています。このプラットフォーム整合性チェックは、整合性検証トラスト チェーンにおける初期アンカーを提供します。これらのチェックは、デバイスのアイデンティティおよび初期ブート ステータスを証明するのに非常に確実な方法となります。以降のすべての整合性チェックは、このアンカーに基づいて行われます。「**Unverified**」の結果となる原因は多数ありますが、最も可能性が高いのは、プラットフォーム整合性チェックに必要な機能を、デバイスがサポートしていないことです。そのようなデバイスが侵害されるリスクとその影響を評価して、Cisco の新しいセキュアなデバイスのいずれかで更新することを検討することを強く推奨します。

図 5-4. ブート整合性チェック - 未検証



ソフトウェアの整合性測定

Cisco IV アプリケーションが取得する測定値によって、ソフトウェアの整合性について、以下の質問に対する答えを見つけることができます。

- 適正なデバイスで使用されているソフトウェアであるかどうか。
- 正しいファイルであるかどうか。実行中に変更が加えられたかどうか。
- 悪意のあるアクティビティを示す可能性がある、不正アクセスが行われたかどうか。

表 5-7. ソフトウェアの検証チェック に、これらの質問の答えを見つけるために実行される検証チェックを記載します。

表 5-7. ソフトウェアの検証チェック

検証チェック	機能	説明
実行中イメージ ファイルの検証	適正なデバイスで使用されるソフトウェア ファイルであるかどうかを調べる機能	高リスク このチェックでは、ソフトウェア ファイルの整合性測定値を Cisco で公開している KGV と比較します。一致する KGV が見つからない場合、「**Failure**」が宣言されます。 この検証チェックは、ブート整合性チェックをサポートしていないデバイスでも限定的な機能を提供します。実行中イメージ ファイル検証機能は、主に次の点でブート整合性検証機能と異なります。 • Boot0 やブートローダ ソフトウェアは対象としません。 • 測定値がトラスト アンカーで保護されません。 • 測定値の認証は行われません。 検証チェックは、IV アプリが新しいデバイスおよびデバイスのリブートを検出した時点で実行されます。

検証チェック	機能	説明
メモリ内 IOS コードセグメントの検証	デバイス上で実行されているソフトウェアが現在も適正なものであるかどうかを調べる機能。つまり、予期しない変更が行われていないかを調べる機能	高リスク このチェックでは、デバイスの初期検出時またはデバイスのリブート検出時に IV のアプリケーションが取得する初期刻印値に対して、メモリ内のソフトウェアの整合性測定値を照合します。取得した測定値が初期刻印値と一致しない場合、「**Failure**」が宣言されます。 注：メモリ内チェックは、現在 IOS デバイスでのみサポートされています。 デバイスへの不正アクセス（クレデンシャルのフィッシングまたは内部攻撃）や、既知あるいは不明な脆弱性を利用してシステムが侵害される可能性があります。 注：新しい脆弱性に対処するために、脆弱性が見つかったら、パッチを適用するか、新しいソフトウェアを導入してソフトウェアを最新の状態に保つことを強く推奨します。 この検証チェックは、デバイスの APIC-EM ポーリング間隔ごとに実行されます。
プラットフォームのシェル アクセス	プラットフォームのシェルへのアクセスがあったかどうかを調べる機能。通常の運用中は、シェル アクセスが発生することはありません。プラットフォームのシェルへのアクセスがあった場合は、誰がどのような理由でアクセスしたのかを調べる必要があります。	中リスク このチェックでは、デバイスの Syslog をモニタリングしてシェル アクセス イベントの有無を確認します。シェル アクセス イベントが見つかった場合、「**Failure**」が宣言されます。 デバイスの通常操作中にシェル アクセスが行われることは通常ありません。シェル アクセスが行われたことが検出された場合、それはデバイスに対する悪意のあるアクティビティを意味する可能性があります。 この検証チェックは、デバイスの APIC-EM ポーリング間隔ごとに実行されます。

図 5-5 には、実行中イメージ ファイル検証チェックが不合格だった場合に表示されるエラーの例を示します。表 5-8.イメージ ファイル検証の実行 - 主要な結果で、主要なエラー結果項目を説明します。

図 5-5. 実行中イメージ ファイル検証 – エラーの例

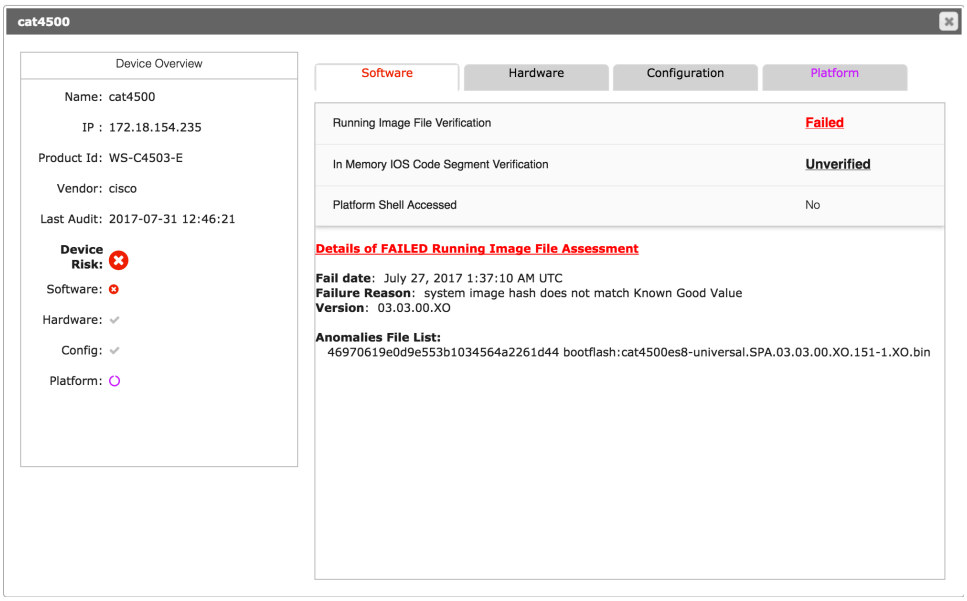


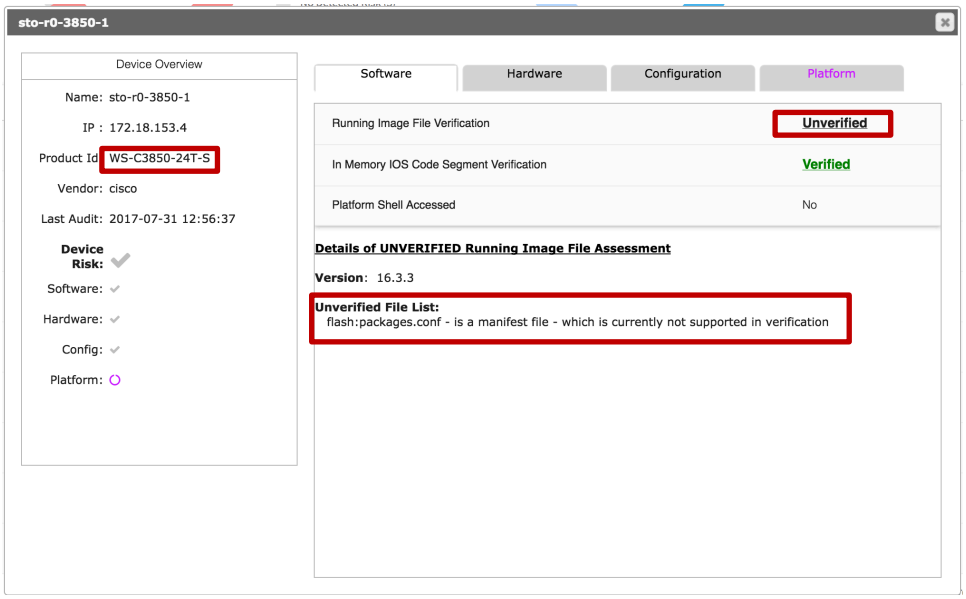
表 5-8. イメージ ファイル検証の実行 - 主要な結果

内容	機能
Fail date:	IV アプリケーションがこのエラーを検出した日時。表示される日時は、おそらく実際の発生日時とは異なります。IV アプリケーションは、APIC EM 用に定義されたポーリング間隔に基づいて整合性測定値をチェックします。したがって、APIC EM ポーリング間隔が 25 分に設定されているとしたら、実際に失敗した時間は、表示されている日時より最大 25 分前であることになります。 注：注意すべき例外として、IV アプリケーションが起動したばかりであるか、新しいデバイスが IV アプリケーションによって検出されたばかりである場合、実際の失敗日時と表示される日時の差は大幅に長くなる場合があります。このような場合、実際の失敗日時は確定できません。
Anomalies File List:	実行中イメージ ファイルの測定されたハッシュ（`17e0c15d12eb5c86220f3d325750d2f4`）とパスおよびファイル名（`bootflash:isr4400-universalk9.16.04.01.SPA.bin`）を表示します。 注：デバイスが侵害されているかどうかを判断するために最初に調査しなければならないことは、当該イメージの KGV データがロードされているかどうかです。ロードされていない場合、失敗の原因は、単に KGV データが欠落していることにあります。

図 5-6. 実行中イメージ ファイルの検証 - バンドルに、別の特殊なケースを示します。「サポートされるプラットフォーム」に関するセクションで注記したように（注 1：）、現在のバージョンの IV アプリケーションではまだ、インストール時にイメージ ファイルをバンドル解除する特定の少数のデバイスに対応していません。これらのデバイスについては、デバイスからイメージ ファイルの名前として `packages.conf` が返され、この名前が「Unverified File List」に示されます。このファイルに関連付けられている KGV は、KGV データには含まれません。また、IV アプリケーションでは現在のところ、インストール時にバ

ンドル解除された個々のイメージ ファイルをチェックしません。誤検出になることを防ぐために、IV アプリケーションは、これらのデバイスの実行中イメージ ファイルの検証チェックは行いません。これは「**Unverified**」として表示されます。

図 5-6. 実行中イメージ ファイルの検証 - バンドル

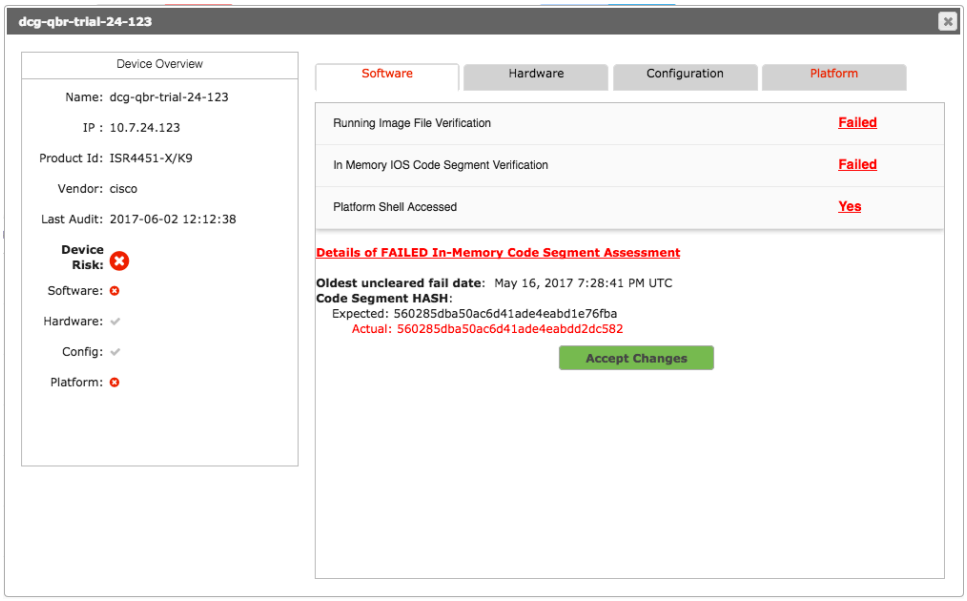


システム イメージ ファイルが「**Unverified**」として特定される理由には、他にも以下があります。

- デバイス上で実行中イメージ ファイルが見つからないか、他のエラーが発生した。IV ログを確認してください。
- 実行中イメージ ファイルがオフ デバイス イメージ ファイルである。現時点では、このファイルは検証でサポートされていません。
- 実行中イメージ ファイルがマニフェスト ファイルである。現時点では、このファイルは検証でサポートされていません。
- イメージ ファイル アセスメント機能がデバイスでサポートされていない。
- デバイスが到達不能であるか、他のエラーが発生した。IV ログを確認してください。
- イメージ ファイル アセスメントが非アクティブとして設定されている。
- 最後の監査時に、検証に有効なイメージ ファイル名がなかった。

図 5-7. メモリ内 IOS コード セグメントの検証 - 失敗 に、メモリ内プログラムの初期刻印値が変更されている場合の例を示します。許可されていないユーザ（不正アクター）がメモリ内のプログラムを変更し、不正なアクションを行ってからデバイスをリブートして変更の証拠を消したことが考えられます。元の検証チェックでのエラー検出結果が失われないように、IV アプリケーションは手動でクリアされるまでエラー条件を保持します。

図 5-7. メモリ内 IOS コード セグメントの検証 - 失敗



注意：理想的には、デバイスでフォレンジックを行ってから先に進める必要があります。ただし、直ちにアクションをとるべき状態である場合は、以下の手順を実行することを検討してください。

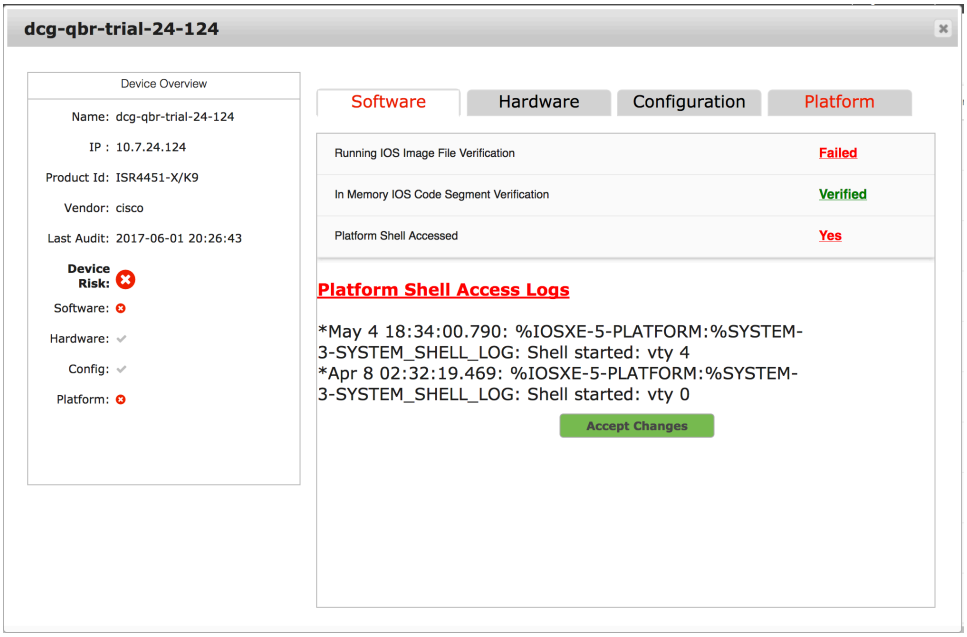
1. ブート イメージ ファイルが適正なものであることを確認します。
2. 直ちにデバイスをリブートします。
3. デバイスのリブート時に、Accept Changes をクリックします。

これにより、認証済みソフトウェアからデバイスがブートされて既知の適正な状態に戻ります。また、IV がメモリ内プログラムの新しい刻印値を取得し、以降の変更の有無に関するテストを開始します。

プラットフォーム シェルへのアクセスは、通常は行われないことです。デバイスの通常の操作中には、シェル アクセスは行われません。通常の操作中に「シェル アクセス」イベントが観測された場合、それは IoC である可能性があります。図 5-8. プラットフォーム シェル アクセス - 失敗 に、シェル アクセスが検出された場合に表示される結果を示します。このエラーの表示は、イベントを有効として受け入れることによってクリアできます。

注意：イベントをクリアする前に、誰が、どのような理由でプラットフォーム シェルにアクセスしたのかを把握する必要があります。シェル アクセス中にデバイスが不正に改ざんされていないと 100 パーセント確信できる場合にのみ、Accept Changes をクリックしてください。

図 5-8. プラットフォーム シェル アクセス - 失敗



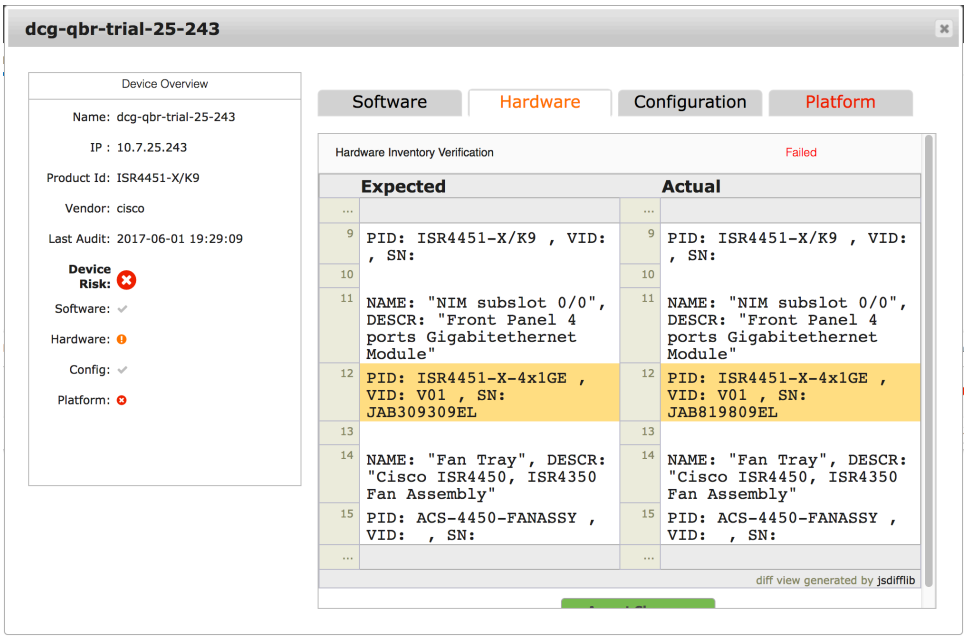
ハードウェアの整合性測定

デバイスが不明な理由でオフラインになった後、オンラインに戻りました。デバイスのハードウェアに不正な変更が加えられた可能性はあるでしょうか。この質問に対する答えを見つけるための検証チェックについて、表 5-9. ハードウェアの検証チェックで説明します。

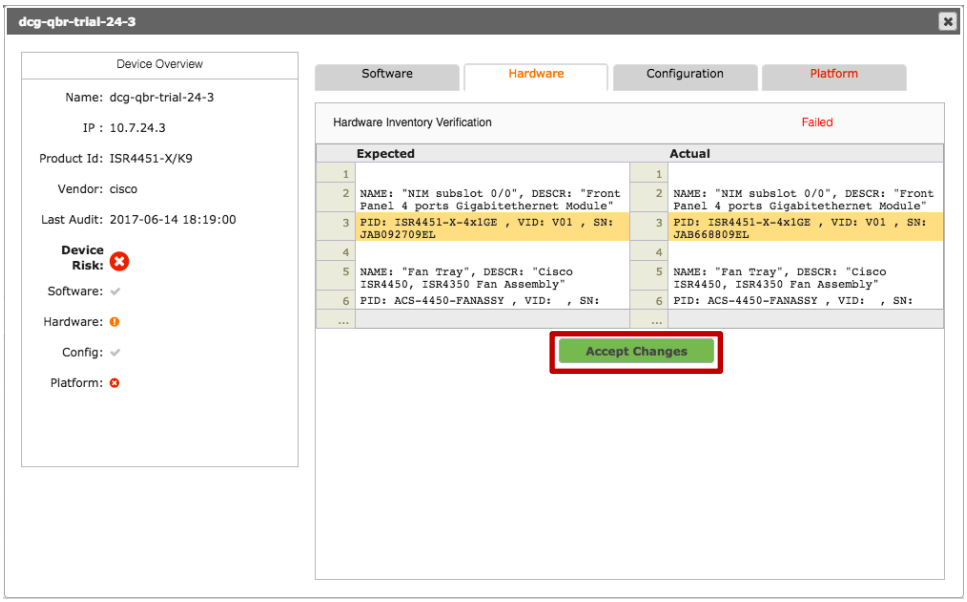
表 5-9. ハードウェアの検証チェック

検証チェック	機能	参照先
ハードウェア インベントリ	デバイスのハードウェアに不正な変更が加えられているかどうかを調べる機能	中リスク この検証チェックでは、IV アプリケーションによるデバイスの初期ディスカバリで取得された初期刻印値に対して、ハードウェア インベントリを照合します。取得した測定値が初期刻印値と一致しない場合、「**Failure**」が宣言されます。 この検証チェックは、デバイスの APIC-EM ポーリング間隔ごとに実行されます。

ハードウェア インベントリで変更が検出された場合、表示される詳細な結果の部分に、相違点が強調表示された状態で、期待されるインベントリと実際のインベントリが示されます。以下に示す例では、ISR4451-X-4x1GE カードのシリアル番号が SN: JAB309309EL から SN: JAB819809EL に変わっています。



この変更は意図的なものである場合も（不良パーツを交換した場合など）、他の予期しないアクティビティの結果である場合もあります。変更が有効かつ期待されるものである場合、インベントリ リストの最後にある [Accept Changes] ボタンをクリックすることで、その変更を「受け入れ」て、新しいハードウェア インベントリを今後の整合性チェックで使用する刻印値にすることができます。



注意： Accept Changes **をクリックする前に、十分に注意してインベントリ変更リストを詳しく調べてください。最初の差分だけを確認して性急に新しいインベントリを受け入れると、検出されていない有害な変更を見落とす可能性があります。**

構成の整合性測定

Cisco IV アプリケーションが取得する測定値によって、構成の整合性について、以下の質問に対する答えを見つけることができます。

- デバイスが期待されるとおりに動作しているかどうか。
- デバイスの構成に不正な変更または予期しない変更が加えられているか。

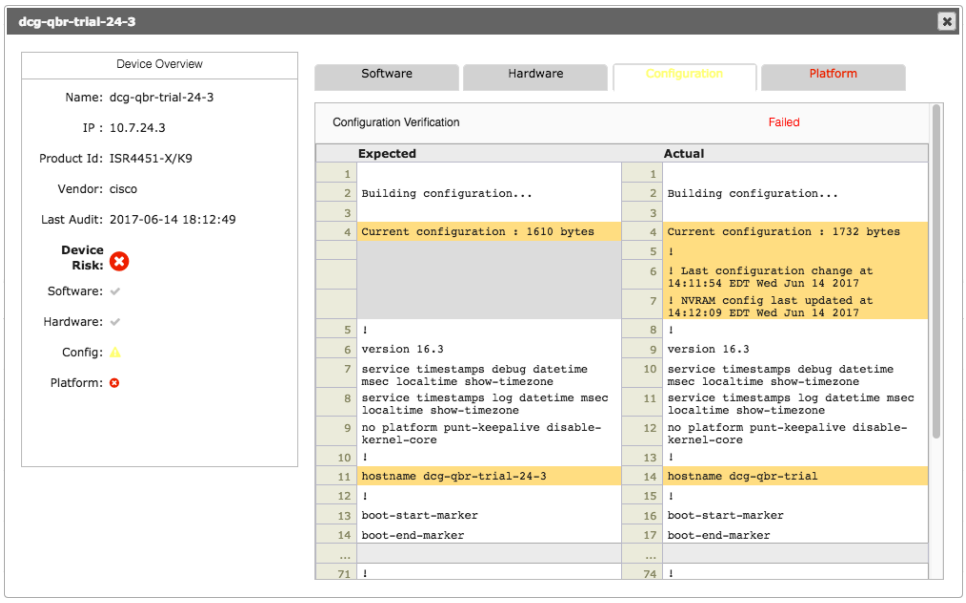
表 5-10. 構成の検証チェック に、これらの質問の答えを見つけるために実行される検証チェックを記載します。

注：IV アプリケーションのこの初期リリースは APIC EM コントローラ構成管理と統合されていないため、コントローラ駆動による変更も予期しない変更として見なされて、「**Failure**」が宣言されます。このことから、デフォルトでは構成のチェックは無効にされています。

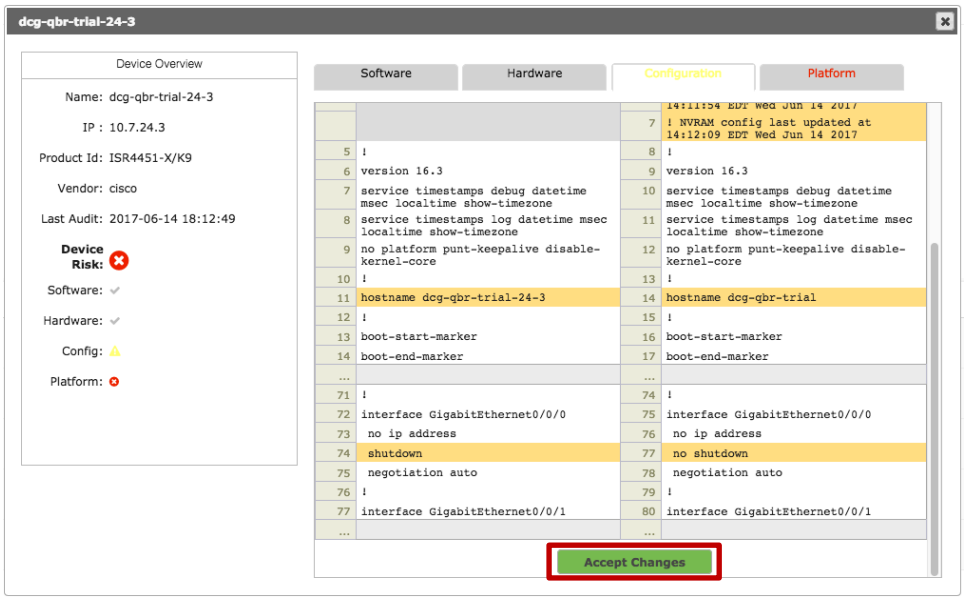
表 5-10. 構成の検証チェック

検証チェック	機能	参照先
実行コンフィギュレーション	デバイスの構成に不正な変更または予期しない変更が加えられているかどうかを調べる機能	低リスク 構成検証チェックでは、IV アプリケーションによるデバイスの初期ディスカバリで取得された初期刻印値に対して、実行コンフィギュレーションを照合します。取得した測定値が初期刻印値と一致しない場合、「**Failure**」が宣言されます。 **注：**IV アプリケーションでは、この検証チェックがデフォルトで無効にされています。 この検証チェックは、デバイスの APIC-EM ポーリング間隔ごとに実行されます。

実行コンフィギュレーションで変更が検出された場合、表示される詳細結果には、相違点が強調表示された状態で、期待される実行コンフィギュレーションと実際の実行コンフィギュレーションが示されます。以下の例では、多数の変更が示されています。構成全体をスクロールして、変更を評価および把握するようにしてください。



変更は意図的なものである場合もあれば（新しい隣接ノードの追加、QoS ポリシーの変更など）、予期しないアクティビティの結果である場合もあります。変更が有効かつ期待されるものである場合、インベントリ リストの最後にある [Accept Changes] ボタンをクリックすることで、その変更を受け入れて、新しい構成を今後の整合性チェックで使用する刻印値にすることができます。



注意：**[Accept Changes]** をクリックする前に、十分に注意して構成変更リストを詳しく調べてください。最初の差分だけを確認して性急に新しい構成を受け入れると、検出されていない有害な変更を見落とす可能性があります。

サポート

システム要件

ハードウェアおよびソフトウェアの要件

APIC-EM のシステム要件は、IV アプリにも適用されます。詳細については、Cisco Application Policy Infrastructure Controller - Enterprise Module Data Sheet を参照してください。

注：IV アプリケーションを初めてアクティブ化すると、APIC がポーリングするデバイスのそれぞれに対して IV アセスメントが行われます。したがって、IV デバイス テーブルにすべてのデバイスが表示されるまでには、ポーリング期間の分だけ時間がかかります（ポーリング期間は、[APIC-EM Settings] ページの [DISCOVERY CREDENTIALS] セクションにある [Polling Interval] で [Polling Time] 値として定義されます）。

最も CPU 使用率が高いのは、IV アプリケーションがデバイスを初めて認識した時点、およびデバイスのリブートが検出された時点でのみ実行される IV アセスメントであるため、この最初のポーリング期間では IV アプリケーションでもデバイスでも追加処理能力が最も多く必要になります。以降のポーリング期間では、IV サービスが使用する処理能力は大幅に減ります。

テクニカル サポート

APIC-EM 1.5 上の IV アプリケーションは、「ベータ版」オファリングとして提供されます。そのため、サポートはベスト エフォート ベースで提供されます。IV アプリケーションに関するご質問や、IV アプリケーションで発生した問題に関する情報は、IV アプリケーション サポート チームの電子メール アドレス iv-app-support-external@cisco.com 宛にお送りください。

注：IV アプリケーション サポート チームはそれぞれの質問や問題を確認して対処するよう努めますが、それらの電子メールに対して個別に、あるいは即時に返信できない場合もあります。

機能リクエスト

IV アプリケーションに求める新しい機能はありますか。各ウィンドウの右下隅にある I wish this page would... をクリックして、IV アプリケーションの改善方法をご提案ください。

注：詳細結果を表示している場合、I wish this page would... をアクティブにするにはポップアップ ウィンドウを閉じる必要があります。

サポートされるプラットフォーム

表 6-1 に、IV アプリケーションでサポートされているプラットフォームならびに各プラットフォームでサポートされる整合性測定のタイプ を記載します。

注：この一覧は、このドキュメントが公開された時点で正確なものです。このリストの更新内容については、ご使用のバージョンの IV アプリケーションのリリース ノートを参照してください。

注：IV アプリケーションは「サポート対象デバイス」とサポート対象外デバイスを区別しません。あらゆるデバイスに対してアクティブ アセスメントを試みます。サポート対象外のデバイスについては異なる結果が示される場合があり、デバイスが整合性測定をサポートしていない場合は「**Unverified**」が、デバイスの KGV が利用できない場合は「**Failed**」が示されることがあります。

表 6-1. プラットフォームのサポート

デバイス	整合性測定タイプのサポート						
	プラットフォーム	ソフトウェア				ハードウェア	構成
		イメージ	インメモリ	IMA	シェル アクセス		
スイッチ							
Cisco Catalyst 2960-S	N	Y[1]	Y	N	Y	Y	Y
Cisco Catalyst 2960-X/XR	N	Y[1]	Y	N	Y	Y	Y
Cisco Catalyst 3560CG	N	Y[1]	Y	N	Y	Y	Y
Cisco Catalyst 3560CX	N	Y[1]	Y	N	Y	Y	Y
Cisco Catalyst 3560-X	N	Y[1]	Y	N	Y	Y	Y
Cisco Catalyst 3650	Y[3]	Y[1]	Y	N	Y	Y	Y
Cisco Catalyst 3750-X	N	Y[1]	Y	N	Y	Y	Y
Cisco Catalyst 3850	Y[3 & 4]	Y[1]	Y	N	Y	Y	Y
Cisco Catalyst 4500（Sup7E）	N	Y[1]	N	N	Y	Y	Y
Cisco Catalyst 4500（Sup8E）	N	Y[1]	N	N	Y	Y	Y
Cisco Catalyst 4500-X	N	Y[1]	N	N	Y	Y	Y

デバイス	整合性測定タイプのサポート						
	プラットフォーム	ソフトウェア				ハードウェア	構成
		イメージ	インメモリ	IMA	シェル アクセス		
産業用イーサネット スイッチ							
Cisco Industrial Ethernet 2000 シリーズ スイッチ	N	Y[1]	Y	N	Y	Y	Y
Cisco Industrial Ethernet 3000 シリーズ スイッチ	N	Y[1]	Y	N	Y	Y	Y
Cisco Industrial Ethernet 4000 シリーズ スイッチ	N	Y[1]	Y	N	Y	Y	Y
ルータ							
Cisco Integrated Service Router（ISR）800 シリーズ	N	Y	N	N	Y	Y	Y
Cisco Integrated Services Router（ISR）2900 シリーズ	N	Y	Y[2]	N	Y	Y	Y
Cisco Integrated Services Router（ISR）3900 シリーズ	N	Y	Y[2]	N	Y	Y	Y
Cisco Integrated Service Router（ISR）4000 シリーズ	Y[3]	Y	Y	N	Y	Y	Y
Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ	Y[3]	Y	Y	N	Y	Y	Y

注 1：APIC-EM 上の IV アプリケーションの初期リリースでは、「BUNDLE」インストール モードを使用してソフトウェアがインストールされているスイッチのみをサポートしています。「INSTALL」インストール モードを使用してソフトウェアがインストールされているデバイスは、現時点ではサポートされません。そのようなデバイスの実行中イメージ ファイルの検証は多くの場合、失敗します。詳細については、「図 5-6. 実行中イメージ ファイルの検証 - バンドル」を参照してください。

注 2：表 6-2. メモリ内チェックの例外に記載されているデバイスは、示されているソフトウェア バージョンではメモリ内検証チェックをサポートしていません。

表 6-2. メモリ内チェックの例外

デバイス	ソフトウェア バージョン	警告 ID 番号
Cisco Integrated Service Router（ISR）3900 シリーズ	15.6 より前のバージョン	CSCus44043
Cisco Catalyst 4500 シリーズ	すべてのバージョン	なし
Cisco Integrated Service Router（ISR）1800 シリーズ	すべてのバージョン	CSCuv19944
Cisco Integrated Service Router（ISR）800 シリーズ	すべてのバージョン	CSCvc58273

注 3：プラットフォームの整合性測定を行う「ブート整合性の可視性」機能をサポートしているプラットフォームとそのプラットフォームに関連付けられている最小ソフトウェア リリースは、表 6-3 に記載されているとおりです。

表 6-3. ブート整合性の可視性に対するサポート

プラットフォーム	最小ソフトウェア リリース バージョン	最小 Rommon/ブートローダ バージョン
ISR4221	16.4.2	16.4(3r)
ISR4321 ISR4331 ISR4351 ISR4431 ISR4451-X	16.3.1a	16.2(1r)
ASR1000-RP3 ASR1001-X ASR1001-HX ASR1002-HX	16.3.2	16.3(2r)

プラットフォーム	最小ソフトウェア リリース バージョン	最小 Rommon/ブートローダ バージョン
WS-C3650-24TS WS-C3650-48TS WS-C3650-24PS WS-C3650-48PS WS-C3650-24TD WS-C3650-48TD WS-C3650-24PD WS-C3650-48PD WS-C3650-48TQ WS-C3650-48PQ WS-C3650-24PDM WS-C3650-48FQM WS-C3650-8X24PD WS-C3650-8X24UQ WS-C3650-12X48UQ WS-C3650-12X48UZ WS-C3650-12X48UR	16.3.2	4.26
WS-C3850-12XS[4] WS-C3850-24XS[4] WS-C3850-48XS[4] WS-C3850-24XU WS-C3850-12X48U	16.3.2	4.28

注 4：上記の表 3 に記載されている Cisco Catalyst 3850 のバージョンはブート整合性の可視性機能をサポートしていますが、既知の問題 CSCve69298 により、整合性検証テストは「Failed」の結果になります。図 6-1 問題 CSCve69298 - Cisco Catalyst 3850 プラットフォームの整合性チェックの結果 に、詳細なテスト結果を示します。この問題が既知となっているのは、Cisco Catalyst 3850 の以下のバージョンのみです。

- WS-C3850-12XS
- WS-C3850-24XS
- WS-C3850-48XS

図 6-1 問題 CSCve69298 - Cisco Catalyst 3850 プラットフォームの整合性チェックの結果

Platform Integrity Risk Level	**High**
Platform Integrity Fail Reason	**pcr8 integrity failure**
Secure Identity Status	**Verified**
Boot Integrity Status	**Failed**

Details of FAILED Boot Integrity Assessment

Fail date: June 23, 2017 2:36:59 AM UTC
Failure Reason: pcr8 integrity failure
Boot Integrity Signature Status: Verified
Boot Integrity Signature Version: 1
Boot Integrity Signature:
D0FB0FC82CFAEAFF51E26FF068F647EFB9605182D50CEBDF3CCB659E7A5FE2303B0A4BE6E0DE5697F7
621E1D1F4EFC33FDC46411EB80194CF0580762B39B1F35B6ABA22D87CA972D076AF5B2B2A8755761ED
874A499C9E5A822D563D10881E566F40E1FBAA6A1E48E02A6A0FEA4FC6381A18A8EF223D0D15238451
C01925A9680819582271FC1AAF44CFCB9D89D20C498023E2117234CF9C4D13819410FDFF7CDD086307
DEAC03273C63EA445BC8AD64D7D334282F67D77D40BF08F4508DBA4208E3B20DB6374EFFF6EF791518
B32E3CA6E63A1F860D476BF7CDCBB8D7D62D2F0A079FBEF0F3DF564343D9447A2EAC28B045418887EA
1BD63EFC2FFD00761409
Boot Integrity Signature Nonce: 4395002834110399586
Boot 0 Status: Verified
Boot 0 Version: F01032R12.18e8d1c732014-06-16
Boot 0 Hash: 66C9A649D3D2B0F3E0C2DC25482DEF691FD9FC0394987AE21638530DF4E32102
Boot Loader Status: Verified
Boot Loader Version: CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 4.318, RELEASE SOFTWARE (P)
Boot Loader Hash:
ED19739F28FA2ECC61CBB0F65E4898C146E69244BDEA7327C81BEE8F47678FEE9AF0AEC74F4AAFC72E
3487BE8DC70C6F689D267670149E27EAFC755F2EDCC4A1
OS Image Status: Failed
OS Image Version: 16.05.01a
OS Image Hash:
2A032EC6C5EBF60607FC9CE246AE2F7B4E1F69E7024CCDDC1238D42DDA9A08504EFE45F513DE442D1
7EC72DB6ECD796733F2730A081822B73823EFB8DEFAF91C
PCR0: E134BBD05A21B43DC147DDBD9CC35AF56E87FC8FAE78240D25A7C799B47C66A1
PCR8: A15A2E774B47D186B5ED618AEF1331943A21AB63CD21E0C2D17D3BC680A6BBA8

注意：**Cisco Catalyst 3850** でのプラットフォームの整合性テスト結果が「**Failed**」となる原因は CSCve69298 にあり、他の不明な理由や予期しない理由ではないことを確認するには、ご使用のデバイスの結果が以下の結果と同じであることを確認してください。

Platform Integrity Fail Reason **pcr8 integrity failure**

Secure Identity Status Verified

Boot Integrity Status Failed

Failure Reason: pcr8 integrity failure

Boot Integrity Signature Status: Verified

Boot 0 Status: Verified

Boot Loader Status: Verified

OS Image Status: Failed