



## Cisco Integrity Verification Application (Beta) on APIC-EM User Guide, Release 1.5.0.266

August 1, 2017

### **Cisco Systems, Inc.**

[www.cisco.com](http://www.cisco.com)

Cisco has more than 200 offices worldwide.  
Addresses, phone numbers, and fax numbers  
are listed on the Cisco website at  
[www.cisco.com/go/offices](http://www.cisco.com/go/offices).

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). 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)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2017 Cisco Systems, Inc. All rights reserved.



<b>Preface .....</b>	<b>v</b>
About .....	v
Organization .....	v
Conventions .....	vi
<b>Related Documentation .....</b>	<b>vii</b>
Obtaining Documentation and Submitting a Service Request .....	vii
<b>Overview .....</b>	<b>1-1</b>
About the Cisco IV Application .....	1-1
Integrity of Measurements and No Detected Risk .....	1-2
Cisco IV Application Workflow Overview .....	1-2
<b>Deployment .....</b>	<b>2-1</b>
Cisco IV Application on APIC-EM .....	2-1
Deploying Cisco APIC-EM .....	2-1
Installing or Upgrading the Cisco IV Application .....	2-1
Accessing the Cisco IV Application .....	2-6
Cisco IV Application Home Page .....	2-7
<b>Known Good Values .....</b>	<b>3-1</b>
Installing New KGV Data .....	3-2
<b>Cisco IV Application Settings .....</b>	<b>4-1</b>
Resetting Configuration Imprint Values .....	4-3
<b>Integrity Monitoring .....</b>	<b>5-1</b>
Summary Device Status .....	5-2
Using the risk level filter .....	5-3
Using the risk type filter .....	5-3
Removing Filters .....	5-4
Viewing Detailed Device Integrity Measurement Results .....	5-5

Integrity measurement types .....	5-7
Platform Integrity Measurements .....	5-8
Software Integrity Measurements .....	5-11
Hardware Integrity Measurements .....	5-16
Configuration Integrity Measurements .....	5-18
<b>Support .....</b>	<b>6-1</b>
System Requirements .....	6-1
Hardware and Software Requirements .....	6-1
Technical Support .....	6-1
Feature Requests .....	6-1
Supported Platforms .....	6-2





## Preface

---

### About

The Cisco Integrity Verification (IV) application provides automated and continuous monitoring of network device integrity measurements, noting any unexpected or invalid results that may indicate compromise. The objective of the IV application is early detection of a compromise, so as to reduce its impact. The IV application operates within Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM).

### Organization

This guide includes the following chapters:

Chapter	Title	Description
1	Overview	Provides information on the IV application, the associated work flows and how to access the application.
2	Deployment	Provides instructions on how to deploy the IV application within an APIC-EM environment.
3	Known Good Values	Provides instructions on maintaining known good values (golden hashes) used within the IV application to verify integrity measurements obtained from the device.
4	Application Settings	Provides instructions on how to configure the IV application to enable/disable the service and monitoring functions.
5	Integrity Monitoring	Provides detailed information on how to use the IV application after its deployment and configuration.
6	Support	Identifies how to obtain support, the supported platforms, and how to request new features for the IV application.

## Conventions

This document uses the following conventions.

Convention	Indication
<b>bold font</b>	Commands and keywords and user-entered text appear in <b>bold font</b> .
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
[ ]	Elements in square brackets are optional.
{x   y   z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[ x   y   z ]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in <code>courier font</code> .
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

**Note:** Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

**Caution:** Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

### **Warning: IMPORTANT SAFETY INSTRUCTIONS**

Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

### **SAVE THESE INSTRUCTIONS**

**Regulatory:** Provided for additional information and to comply with regulatory and customer requirements.

## Related Documentation

Documentation	Description
Cisco APIC-EM Documentation Roadmap	Provides a list of all Cisco APIC-EM product documentation. This document is designed to help you get the most out of the controller and its applications. You can find links to all of the documentation, including Cisco IWAN at: <a href="http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/tsd-products-support-series-home.html">http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/tsd-products-support-series-home.html</a>

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>.

Subscribe to What's New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.





# Overview

## About the Cisco IV Application

Integrity Verification (IV) monitors key product data for unexpected changes or invalid values that represent indicators of compromise (IOC). The objective is to minimize the impact of a compromise by substantially reducing the time to detect unauthorized changes to a product. Key components of integrity verification include:

- Technology and integrity measurement capabilities embedded within platforms that enable the detection of unexpected conditions
- Run-time monitoring and visibility into these integrity measurements to enable rapid response to indicators of compromise
- Deeper on-line and off-line forensics capabilities to confirm an attack and help determine its source, objectives and means to counter future attacks

The IV application leverages the capabilities provided by APIC-EM to obtain integrity measurements from monitored devices, evaluates these measurements for correctness and unexpected changes, and provides visibility into the results. The integrity measurement types supported by the IV application are described in Table 1-1. Details can be found using the associated reference.

**Table 1-1. Integrity Measurement Types**

Measurement Type	Function	Reference
Platform	Is the device authentic? Includes verification of the boot process measurements and the identity of the device.	Platform Integrity , Page 5-8
Software	Is the software used by the device authentic? Includes checks of the software files and in-memory contents.	Software Integrity , Page 5-11
Hardware	Does the device contain the hardware components that are expected? Includes checks of the hardware inventory.	Hardware Integrity , Page5-16

Configuration	Are there any unexpected changes in the device configuration? Includes checks of the running configuration.	Configuration Integrity Measurements, Page5-18
---------------	---	--

**Note:** The Cisco IV application is currently available as a beta for proof-of-concept use and trials. While the software has undergone rigorous development and testing in its current form, additional features beyond the core capabilities in this release will be added. The IV application (beta version) has the following objectives:

- Assist in protecting our customer's networks by accelerating the availability of Cisco core integrity verification capabilities.
- Obtain feedback from our customers to help identify and drive future feature development required to improve the effectiveness of this new security tool.

## Integrity of Measurements and No Detected Risk

The IV application obtains integrity measurements from a device and compares them to expected or known good values. While Cisco's newer products contain technologies to protect the integrity of the measurement collection and retrieval process, not all products contain these technologies. There is always the risk that a device has been compromised and is providing the expected instead of the actual measurements.

**Note:** The integrity verification status "No Detected Risk" indicates one of the following scenarios:

- Integrity measurements obtained from the device were as expected.
- Device does not support the integrity measurement.
- Integrity assessment is not enabled using the "IV Settings" options in the application.

A "No Detected Risk" status does not indicate that the device has not been compromised. To reduce the risk that a compromised device is providing misleading measurements, legacy systems should be refreshed with Cisco's newer and more secure products.

## Cisco IV Application Workflow Overview

**Table 1-2. Basic Workflow for Accessing Cisco IV**

No.	Action	Reference
1	Deploy Cisco APIC-EM.	Deploying Cisco APIC-EM, page 2-1
2	Install the latest version of the IV application.	Installing or Upgrading the Cisco IV Application, page 2-1  <b>Note:</b> You need to deploy the Cisco APIC-EM controller prior to downloading, installing, and enabling the Cisco IV application.
3	Log into Cisco APIC-EM to access the Cisco IV application.	Accessing the Cisco IV Application, page 2-6
4	Configure and enable the IV application	<ul style="list-style-type: none"> <li>• Install known good values, page 3-1</li> <li>• IV application settings, page 4-1</li> </ul>
5	Monitor device integrity	<ul style="list-style-type: none"> <li>• Integrity monitoring, page 5-1</li> </ul>



## Deployment

---

### Cisco IV Application on APIC-EM

As described in the Overview, the Cisco IV application (IV app) operates through Cisco APIC-EM, as a tool within the APIC-EM browser-based interface. You should note the following considerations when deploying and configuring either the APIC-EM controller or the IV application.

#### **Separate Cisco IV App Release Schedule and Numbering**

The Cisco IV application is:

- Decoupled from the APIC-EM release schedule, and from the APIC-EM installation and upgrade processes.
- IV app release numbering is independent of APIC-EM release numbering.
- Download the IV app separately from APIC-EM, then install or upgrade the app using the APIC-EM “App Management” page. See *Installing or Upgrading the Cisco IV Application*, page 2-1.

#### **System Requirements**

The IV application requires Cisco APIC-EM release 1.5.0.x. System requirements for the APIC-EM apply to the IV app. The release notes describe the software compatible with IV app releases, including APIC-EM.

### Deploying Cisco APIC-EM

Access the Cisco IV application from the Cisco APIC-EM graphical user interface (GUI). To use the IV app, you must first deploy Cisco APIC-EM.

You can deploy Cisco APIC-EM either on a server (bare-metal hardware) or in a virtual machine in a VMware vSphere environment. You can deploy Cisco APIC-EM either as a single host or in a multi-host environment.

Deploy Cisco APIC-EM according to the instructions in the APIC-EM installation guide, available on the APIC-EM [Install and Upgrade Guides](#) page.

### Installing or Upgrading the Cisco IV Application

#### **Before Installing or Upgrading the IV Application**

Do the following before installing the IV app:



- If APIC-EM is not already installed, then install it according to the instructions in the APIC-EM installation guide, available on the APIC-EM [Install and Upgrade Guides](#) page. If necessary, install any necessary patches to upgrade APIC-EM to the desired release.
- Verify that your Cisco APIC-EM release (release 1.5.0.x or higher is required) and the software versions of other elements in the network are compatible with the IV app version you are installing. See the release notes for details.

**Note:** When upgrading from an earlier release of the IV app, the log of operations done by the earlier release will not be preserved after the upgrade.

### Recommendations

- Create a backup of the current APIC-EM configuration. See APIC-EM documentation for details about backup and restore. The basic steps are:
  1. In APIC-EM, select: Settings (gear button) > App Management.
  2. Select the Backup & Restore tab.
  3. Click the Create New Backup button.
- If upgrading from a previous IV app release, perform a backup of the IV configuration before upgrading. See Backup and Restore, Recovery, and Delete.

### Cisco IV Application Deployment Procedure

Perform the steps in the following procedure to download, install, and enable the IV application.

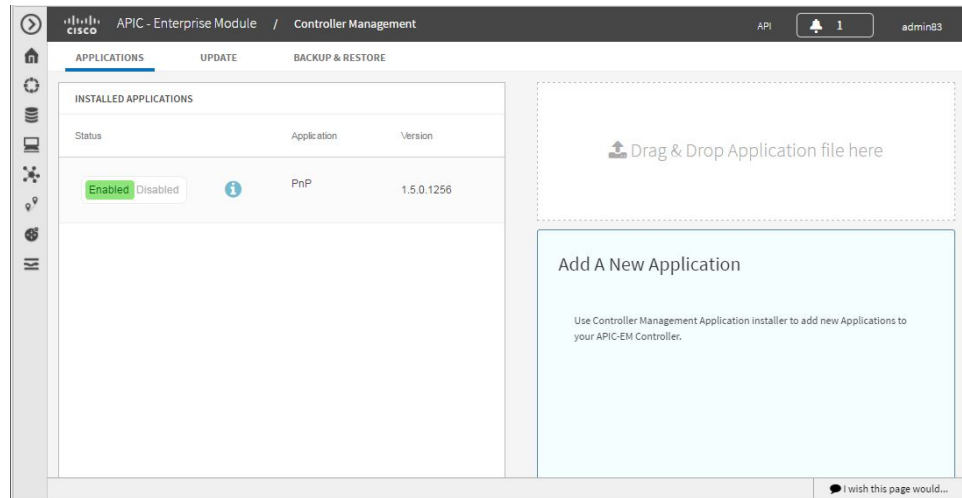
Procedure	
<b>Step 1</b>	Using the Cisco Download Software tool, navigate to Policy and Automation Controllers, and select APIC-EM, or use this direct link: <a href="https://software.cisco.com/download/type.html?mdfid=286208072&amp;flowid=77162">https://software.cisco.com/download/type.html?mdfid=286208072&amp;flowid=77162</a>
<b>Step 2</b>	Locate the Cisco Integrity Verification Application (Beta) software option. Download the IV application. Note the location of the downloaded file.

### Step 3

Start APIC-EM and open the APIC-EM Applications page.

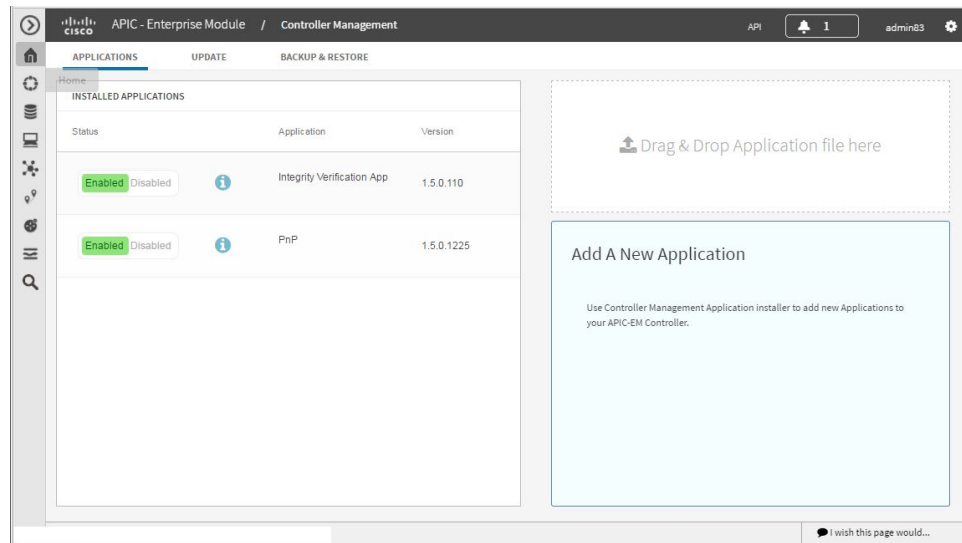
- a. Select: Settings (gear button) > App Management
- b. Ensure that the Applications tab is displayed.

(The example below shows a PnP Application already installed on the APIC-EM.)



If a version of the IV app has been installed previously, it appears in the Installed Applications list.

(The example below shows an earlier release of the IV app.)

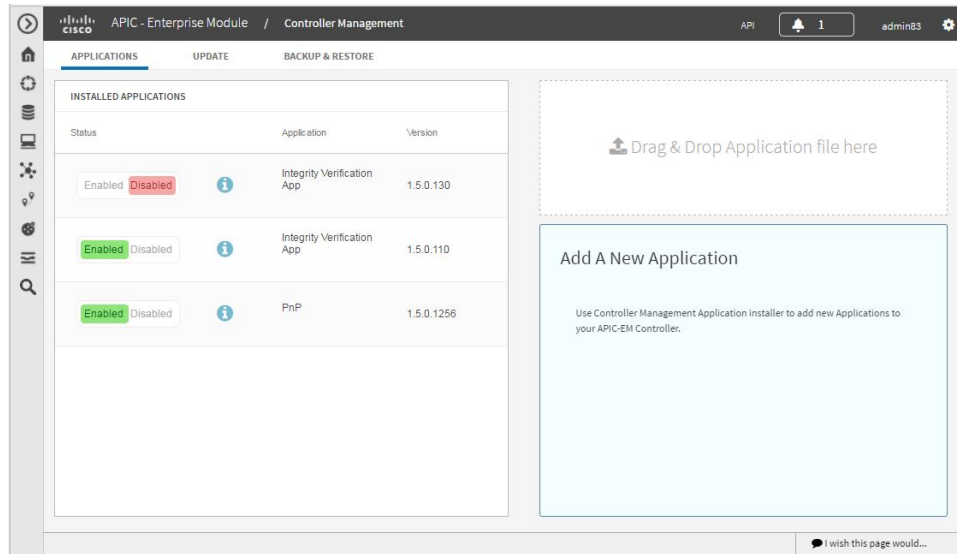


- c. Note the **Drag&Drop Application file here** box at the right side of the APIC-EM Applications page.

**Step 4**

Drag-and-drop the downloaded IV app installation file onto the **Drag&Drop Application file here** box. The new IV app appears in the list of applications, and is shown as Disabled.

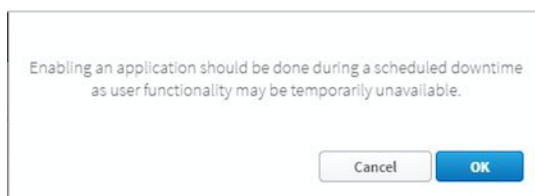
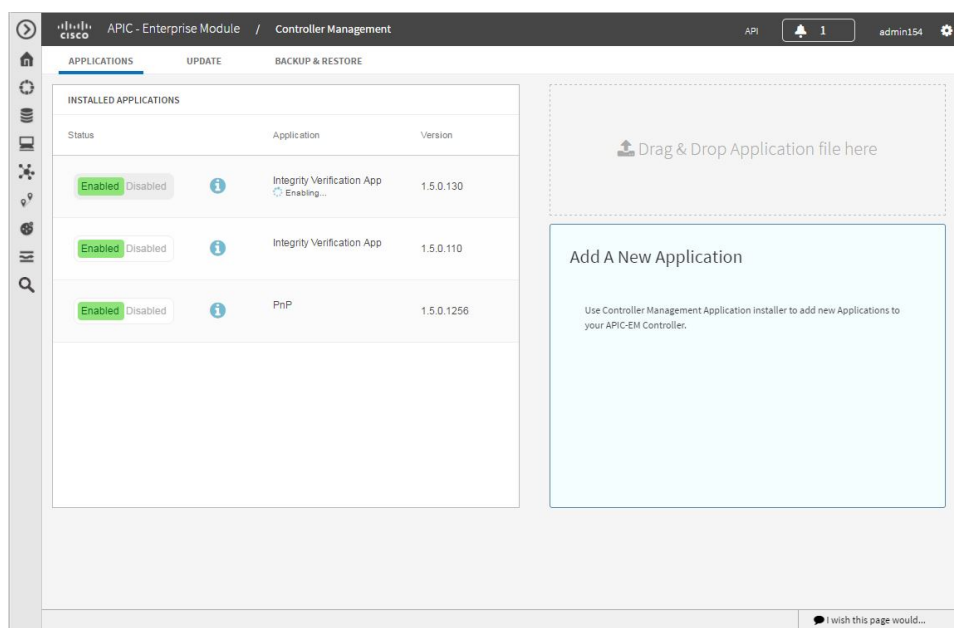
(The example below shows an earlier release of the IV app.)



When upgrading from a previous version of the IV app, the earlier version of IV continues to appear in the list at this point in the installation.

**Step 5**

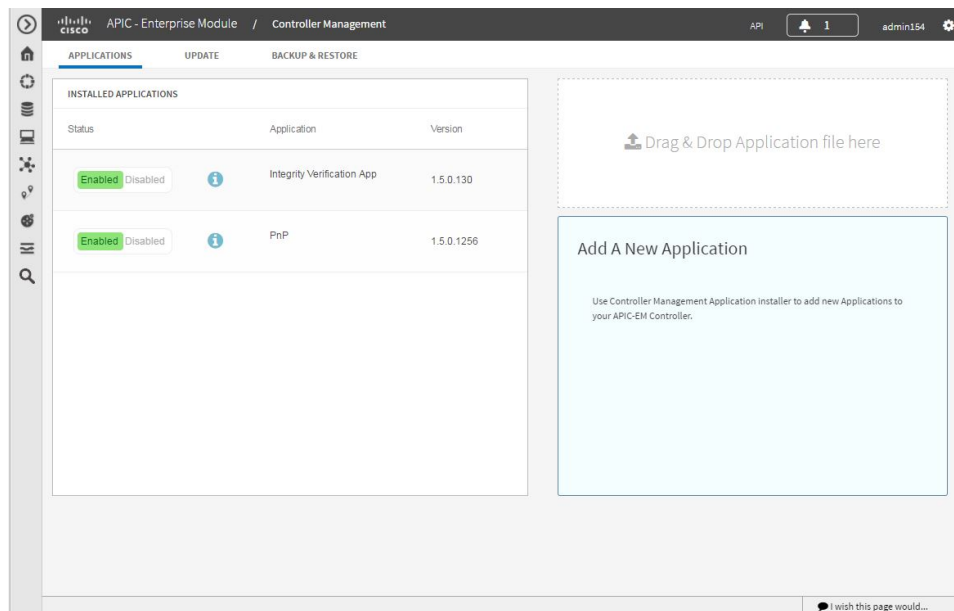
Click Enabled for the new IV application. APIC-EM enables the new version. When upgrading from a previous version of the IV app, APIC-EM preserves the existing IV configuration. The page indicates that the enable process is in progress. Wait for the process to complete. Installation time depends on the cluster size and other factors. (The example below shows an earlier release of the IV app.)



**Note:** Pay special attention to the pop-up warning when enabling the IV application. The process can be time consuming and may temporarily impact APIC-EM user functionality. The IV application installation and enablement process should be performed during scheduled downtime.

**Step 6**


When the installation and enabling are complete, clear the browser cache and refresh the APIC-EM Applications page. The Status column shows that the new IV app is enabled, and the Version column shows the new IV app version. Any previous version of the IV app is removed from the list.

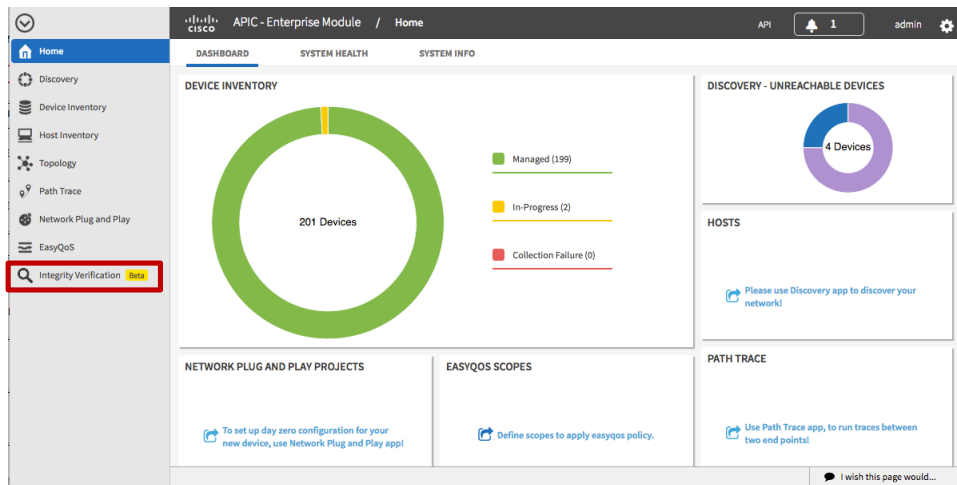


## Accessing the Cisco IV Application

Access the Cisco IV application from the Cisco APIC-EM GUI.

**Procedure**

- Step 1** Using Google Chrome or Mozilla Firefox, enter the IP address or the fully qualified domain name (FQDN) for Cisco APIC-EM.
- Step 2** Enter a username and password, and then click Log In.
- Step 3** When logging in for the first time, review and confirm the Telemetry Disclosure, and then click **Confirm**. The Cisco APIC-EM GUI appears.
- Step 4** From the Cisco APIC-EM GUI left navigation pane, click on the “Integrity Verification Beta” icon, . The Cisco IV application home page opens. See Cisco IV Application Home Page below.

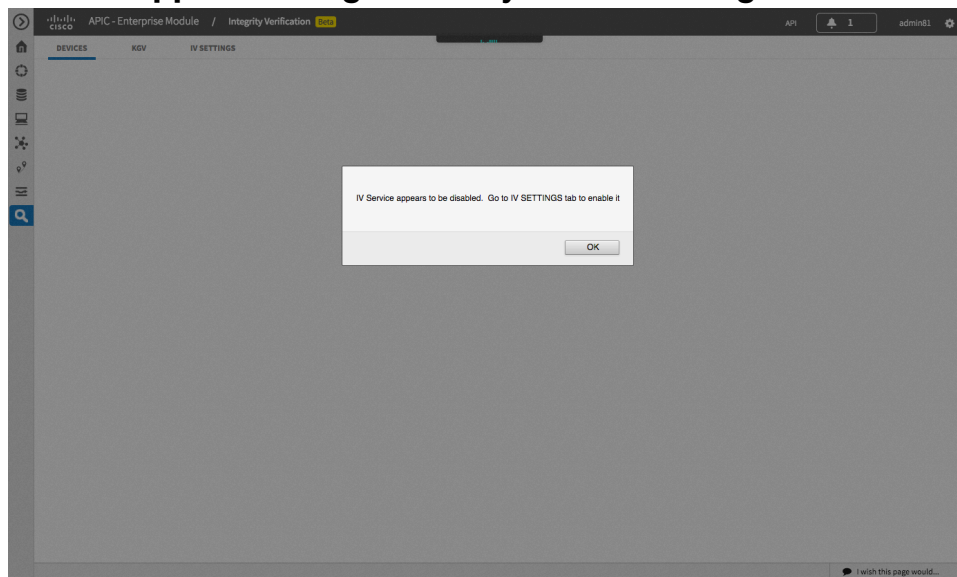


## Cisco IV Application Home Page

For an initial setup, the Cisco IV application home page indicates that the IV service has not yet been enabled. The steps to configure and enable the IV application are as follows:

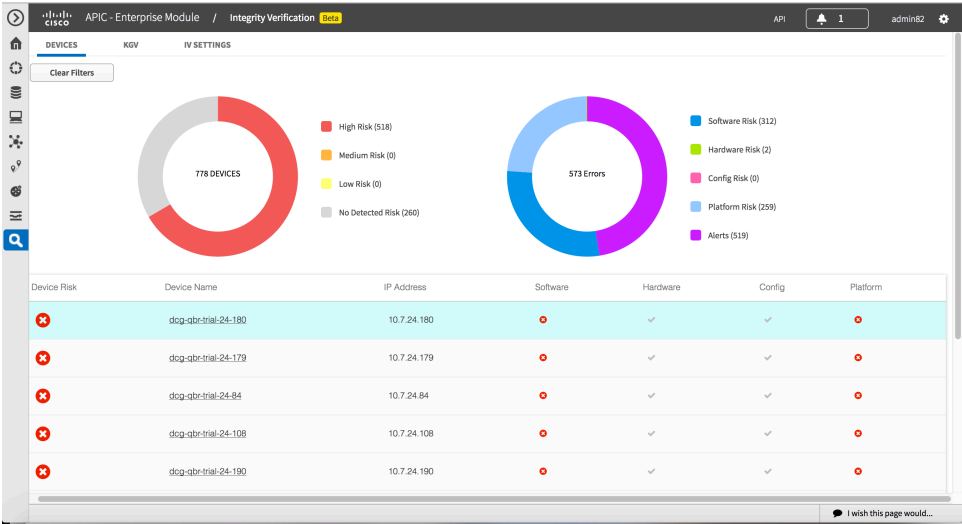
1. Load the latest known good values (KGV) into the IV application. See Known Good Values, page 3-1.
2. Select the Integrity measurement types that are to be monitored and enable the IV service. See Cisco IV Application Settings, page 4-1.

**Figure 2-1. Cisco IV App Home Page—New System Initial Login**



After you have configured and provisioned Cisco IV, the home page provides more information. For example, it displays devices, their overall device risk, risk by integrity measurement type as shown in the following figure.

Figure 2-2. Cisco IV App Home Page—After Provisioning



Task Area	Function	Reference
DEVICES	Display and manage indicators of compromise	Integrity Monitoring, page 5-1
KGV	Install and manage known good values (KGV)	Known Good Values, page 3-1
IV SETTINGS	Enable and select options for the integrity verification application	IV Application Settings, page 4-1



# CHAPTER 3

## Known Good Values

In order to provide a level of security integrity, Cisco devices must be verified as running authentic and valid software. Currently, Cisco devices in the field have no point of reference to determine they are running authentic Cisco software. The Cisco IV application uses a system to compare collected image integrity data to Known Good Values (KGV) for Cisco software.

Cisco produces and publishes a Known Good Value Data file that contains KGV's for many of its products. This KGV file is in standard JSON format, is signed by Cisco, and is bundled with other files into a KGV Combo Bundle that can be retrieved from Cisco.

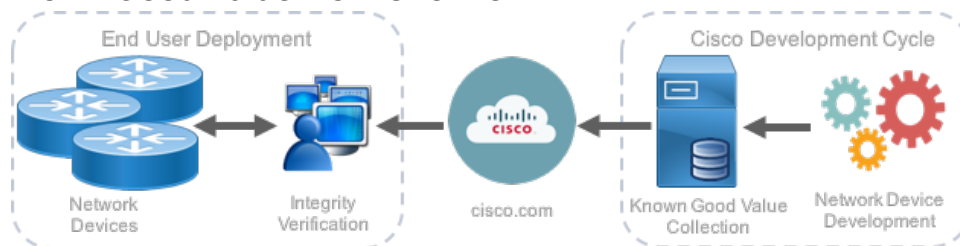
**Note:** KGV data is posted at: [https://tools.cisco.com/cscrd/security/center/files/trust/Cisco\\_KnownGoodValues.tar](https://tools.cisco.com/cscrd/security/center/files/trust/Cisco_KnownGoodValues.tar)

The KGV file is loaded into the IV application and used to verify integrity measurements obtained from the network devices. **Note:** Device integrity measurements are made available to and used entirely within the IV application. Connectivity between the IV application and cisco.com is not required. The KGV file can be air-gap transferred into a protected environment and loaded into the IV application. See Installing New KGV Data below for more information.

Figure 3-1. Known Good Value Flow Overview depicts the KGV flow from its initial harvesting during the development process, its posting on cisco.com and ultimately to its use by the IV application.

**Note:** Device integrity measurements are made available to and used entirely within the IV application. Connectivity between the IV application and cisco.com is not required. The KGV file can be air-gap transferred into a protected environment and loaded into the IV application. See Installing New KGV Data below for more information.

**Figure 3-1. Known Good Value Flow Overview**



The current Cisco produced KGV Data File includes measurements for the following component categories:

- Boot Integrity Visibility hashes
  - Boot 0
  - Bootloader / ROMMON
  - OS Image

- Running Image File hashes

**Note:** KGV data must be loaded into the IV application prior to activating the service.

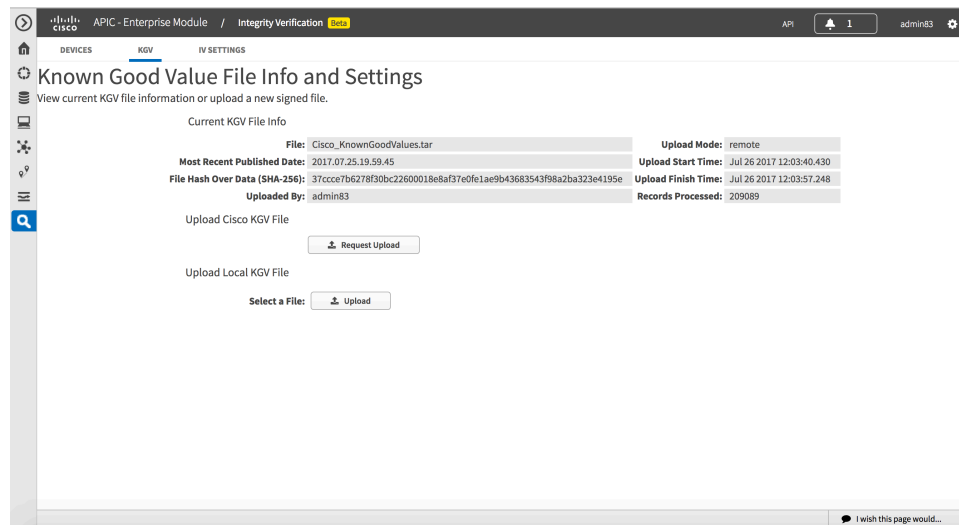
Click on “**KGV**” at the top of the IV application screen to access the KGV system. The KGV screen, see Figure 3-2, displays information on the currently loaded KGV and provides a button to upload new KGV data into the IV application.

The key information from this screen is:

- **Most Recent Published Date:** 2017.06.14.18.54.51

This identifies the date and time that a snapshot of the KGV data was taken and published. It is important that this date be more recent than the publish dates of any software used on the devices being monitored by the IV application. Having software that is more recent than the KGV published date will result in a “**Failure**” condition as the KGV for the software is not known by the IV application.

**Figure 3-2. KGV Screen Information**



Users should update KGV periodically and at least whenever a newer version of software is deployed in their system.

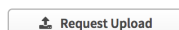
**Note:** Failure to maintain current KGV data could result in false positive failure indications caused when KGV for installed software is not available to the IV application.

## Installing New KGV Data

There are two methods for installing new KGV data into the IV application:

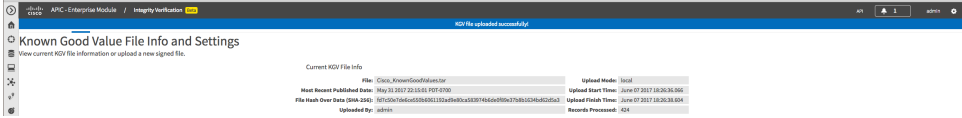
1. If the APIC-EM controller has internet connectivity, you can download and install the latest KGV file from Cisco by clicking the “Request Upload” button:

Upload Cisco KGV File



2. Alternatively, you can download the latest KGV data onto your system, then install it into the IV application. This method does not require the APIC-EM controller to have internet connectivity. To use this method, follow the instructions provided in Table 3-1. KGV Upload Procedure.

Table 3-1. KGV Upload Procedure

Procedure	
Step 1	<p>Download the current KGV data onto your local system using this link:</p> <p><a href="https://tools.cisco.com/cscrdtr/security/center/files/trust/Cisco_KnownGoodValues.tar">https://tools.cisco.com/cscrdtr/security/center/files/trust/Cisco_KnownGoodValues.tar</a></p> <p>Remember the location where you save the file for Step 3 below.</p>
Step 2	<p>Click the “Upload” button:</p> <p>Upload Local KGV File</p> <p>Select a File: <input type="button" value="Upload"/></p>
Step 3	<p>When the file browser window for your system appears, navigate to the directory where you saved the KGV data in Step 1.</p> <p>Select the Cisco_KnownGoodValues.tar and click “Open”</p>
Step 4	<p><b>KGV file successfully uploaded</b> will be displayed at the top of the window if the KGV data is successfully uploaded into the IV application.</p>
	

For an initial setup, once KGV data has been installed proceed to Cisco IV Application Settings to configure and enable the IV service.



# CHAPTER 4

## Cisco IV Application Settings

The IV service is disabled by default. To enable the IV service, click “Yes” for “IV Service” then click “Save”. A description of the available settings is provided in Table 4-1. For all settings, clicking "Yes" enables the feature or functionality and clicking "No" disables the feature or functionality.

**Note:** KGV values should be installed prior to enabling the IV service. See Known Good Values, page 3-1, for further instructions.

**Figure 4-1. IV Settings—Initial Selections**

The screenshot shows the Cisco APIC - Enterprise Module / Integrity Verification settings page. The page title is "Integrity Verification Service-Wide Settings". Below the title, it says "Select options below to enable or disable or reset data of Integrity Verification assessments." The settings are listed as follows:

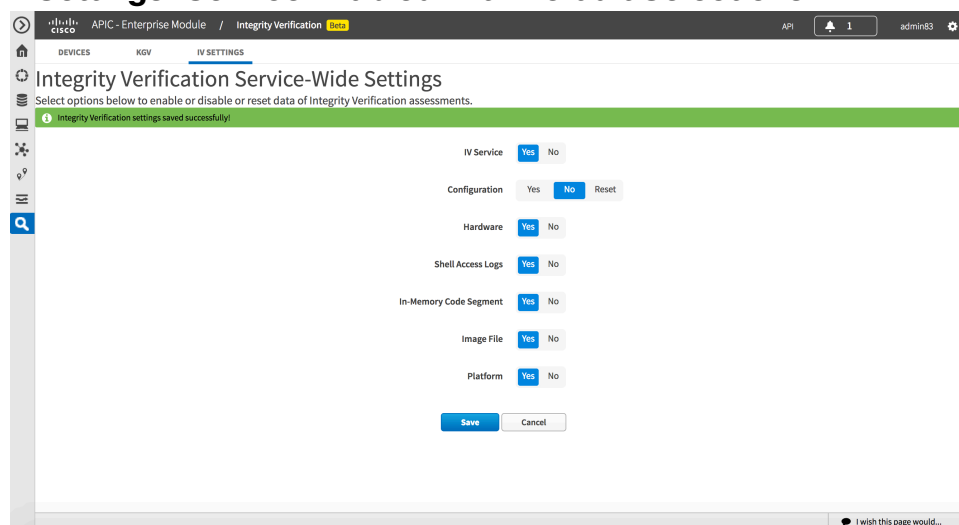
Setting	Yes	No	Reset
IV Service	<input checked="" type="button" value="Yes"/>	<input type="button" value="No"/>	
Configuration	<input checked="" type="button" value="Yes"/>	<input type="button" value="No"/>	<input type="button" value="Reset"/>
Hardware	<input checked="" type="button" value="Yes"/>	<input type="button" value="No"/>	
Shell Access Logs	<input checked="" type="button" value="Yes"/>	<input type="button" value="No"/>	
In-Memory Code Segment	<input checked="" type="button" value="Yes"/>	<input type="button" value="No"/>	
Image File	<input checked="" type="button" value="Yes"/>	<input type="button" value="No"/>	
Platform	<input checked="" type="button" value="Yes"/>	<input type="button" value="No"/>	

At the bottom of the settings list are two buttons: "Save" and "Cancel".

**Note:** When the IV application is first activated, it will run IV assessments on each device as the APIC polls that device, so it will take a full polling interval for all devices to show up in the IV Device Table (polling interval as defined by the "Polling Time" value in the APIC-EM Settings page, under the 'Polling Interval' in the DISCOVERY CREDENTIALS section).

This first interval is where most of the additional processing power is needed by both the IV application and the devices, as many of the highest CPU usage IV assessments are only run the initial time the IV application becomes aware of the device, and when a device reboot is detected. Subsequent polling intervals will see a significant reduction in processing power used by the IV Service.

**Figure 4-2. IV Settings—Service Enabled with Default Selections**



**Table 4-1. Integrity Verification Service-Wide Settings**

Setting	Function	Reference
IV Service	The master on/off switch for the IV service. For all settings, clicking "Yes" enables the feature or functionality and clicking "No" disables the feature or functionality.	N/A
Configuration	Monitors for unexpected changes in the running configuration. As APIC-EM has similar capabilities, this service is disabled by default.	Configuration Integrity Measurements, Page 5-18
Hardware	Monitors for unexpected changes in the hardware inventory.	Hardware Integrity , Page 5-16
Shell Access Logs	Shell access on devices that support it should not occur during normal operation. The presence of a log entry indicating that the shell has been accessed is an indicator of compromise.	Software Integrity , Page 5-11
In-Memory Code Segment	Monitors for unexpected changes in program content in memory.	Software Integrity , Page 5-11
Image File	Verify program content in files with KGV.	Software Integrity , Page 5-11
Platform	Verify boot results with KGV and validate platform identity.	Platform Integrity , Page 5-8

# Resetting Configuration Imprint Values

The configuration verification check compares the running configuration against an initial imprint value obtained on initial discovery of the device by the IV application. There may be cases where you need to recapture the imprint values based on the current configurations. Two potential scenarios include:

- 1. The IV application is not currently integrated with APIC-EM configuration functions. If APIC-EM were to push changes into a large number of devices, these changes would be flagged as unexpected changes by the IV application, requiring the IV application user to individually review and accept the changes for each device. The reset function could be used to re-imprint all devices.
- 2. In response to customer feedback, the IV application has been modified to mask out changes in the configuration that are normal and expected. (e.g., ntp clock-period). The reset function can be used to clear items that were previously flagged as unexpected changes.

Table 4-2. Configuration Reset Procedure provides the instructions required to utilize the reset function. While this reset function provides a time saving capability, it should be used with caution to reduce the possibility of its use hiding a pre-existing unexpected change.

**Table 4-2. Configuration Reset Procedure**

Procedure	
Step 1	
	Configuration <input checked="" type="button" value="Yes"/> <input type="button" value="No"/> <input type="button" value="Reset"/>
	If the current Configuration setting is "Yes":
	Configuration <input type="button" value="Yes"/> <input checked="" type="button" value="No"/> <input type="button" value="Reset"/>
	Then change the setting to "No":
	<input checked="" type="button" value="Save"/> <input type="button" value="Cancel"/>
	And click "Save":
	After the operation completes, proceed with Step 2

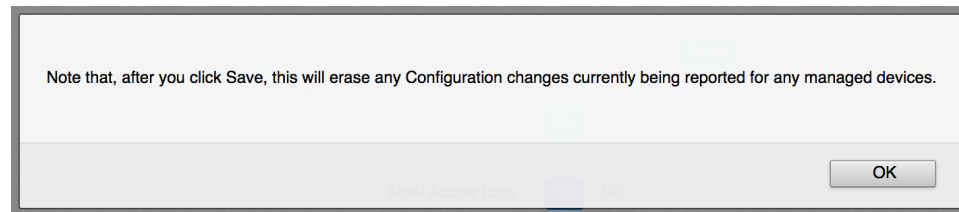


## Step 2

Configuration Yes No **Reset**

Click “Reset”:

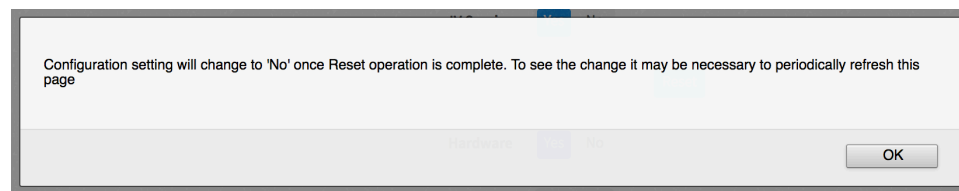
The following popup message will appear, click “OK” to confirm you understand that this operation will erase the current imprint value for device configuration checks – resulting in the configuration from the next scan of the device becoming the new imprint value to be used for future configuration checks.



**Save** Cancel

And click “Save”:

The following popup message will appear, click “OK” to confirm you understand that once the “Reset” operation completes, the Configuration setting will change to “No”



After the operation completes, as indicated by Configuration set to “No”, proceed with Step 3

Configuration Yes **No** Reset

## Step 3

If you wish to re-enable configuration checking, change the setting to “Yes”:

Configuration **Yes** No Reset

**Save** Cancel

And click “Save”:



## Integrity Monitoring

---

The IV application performs a series of verification tests using information obtained from a device. This information is compared with known good or expected values and results recorded (see Table 5-3. Verification Results). The results for a device are summarized into a risk level (see Table 5-1. IV Risk Levels) for each integrity measurement type (see Table 5-5. Integrity Measurement Types). An overall risk level is also assigned to the device.

“Risk Level” represents the strength of the possibility that the verification test failures for a device are indicators of compromise. The IV application provides a view into the integrity of a device, but cannot and does not claim with absolute certainty that the device is or is not compromised.

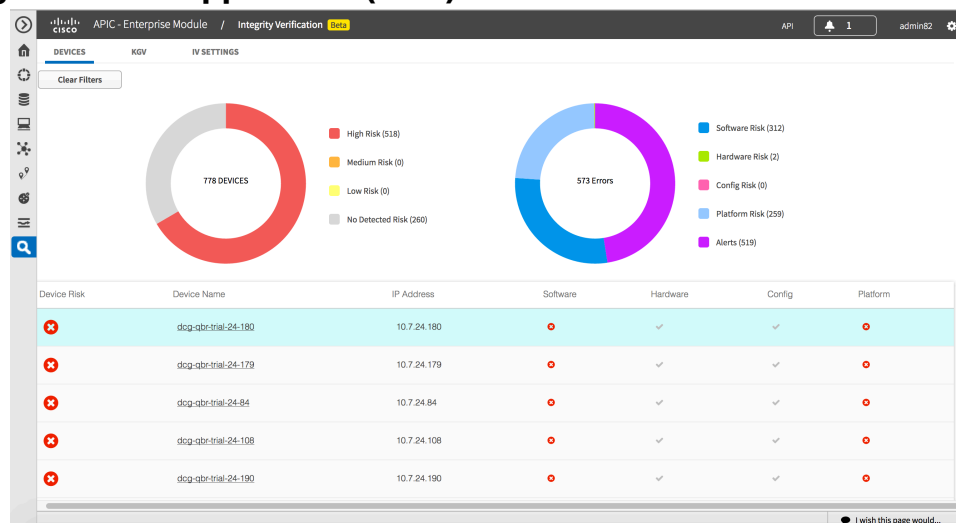
An analogy is the fuel gauge in an automobile. We look at the gauge to determine how much fuel remains in the tank. While we tend to believe the information from the gauge, failures in the gauge can occur. You can run out of fuel when the gauge shows the tank as being full. Some drivers use additional inputs to help determine if the fuel gauge is reporting correct information. For example, the number of miles driven since their last fill up. If approaching the number of miles where the tank normally needs to be refilled, the driver would hopefully take action. Likewise, the results provided by the IV application should be used as one of many indicators of a device’s integrity. More people likely run out of fuel by not paying attention to the fuel gauge than from a faulty gauge. Similarly, the IV application provides valuable, but not infallible, insight into the integrity of a device.

The Cisco IV application’s “DEVICES” tab displays the results of the integrity verification tests. The top portion of the “DEVICES” window has two circles that display a summary of the results, as well as providing filtering capabilities to further aid in analysis of the results.

The left circle is for overall risk level. The right circle is for measurement type risks.

The main body of the screen contains a list of all Cisco devices monitored by the Cisco IV application, with overall risk level and measurement-specific risk levels displayed for each device.

**Figure 5-1. IV Application (Beta) – Devices Tab**





## Summary Device Status

Each device monitored by the IV application has an overall and individual measurement type risk levels. Click on a device’s hostname or any of its risk icons to view detailed information about the measurement results. Refer to Viewing Detailed Device Integrity Measurement Results, page 5-5, for more information.

Entries in this list can be sorted by clicking the column headings. You can further focus the investigations by using the filter capabilities described in the following sections.

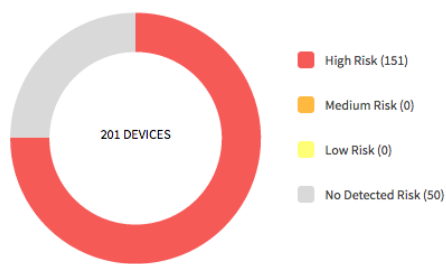
**Table 5-1. IV Risk Levels**

Risk Level	Description
<div style="display: inline-block; width: 15px; height: 15px; background-color: red; margin-right: 5px;"></div> <b>High Risk</b>	<p>This risk level typically corresponds to true-false conditions; the hash of the file being checked is not a known good value (i.e., the hash of an authentic software file). For more information, refer to the descriptions of “Software Risk” and “Platform Risk” in Table 5-2.</p> <p>The failure status should be examined closely to determine if the cause of the failure is one of the following:</p> <ul style="list-style-type: none"> <li>The known good values for the software running on the device have not been installed into the IV application. (see Known Good Values, page 3-1)</li> <li>The known good values for the software running on the device have not been published by Cisco. (see Supported Platforms, page 6-2)</li> <li>The software running on the device has been altered.</li> </ul> <p><b>Note:</b> For summary risk levels, such as the device overall risk level, risks are cumulative. More failures of integrity checks becomes a preponderance of evidence that something may be wrong.</p>
<div style="display: inline-block; width: 15px; height: 15px; background-color: orange; margin-right: 5px;"></div> <b>Medium Risk</b>	<p>This risk level typically corresponds events that are normally rare for a device, such as remote shell access or changes in the hardware inventory. The detailed results and your organization’s operations documentation should be examined closely to determine if the change is the result of a recent maintenance activity on the device, such as installing an additional module, or appears to be unauthorized activity that warrants further investigation. For more information, refer to the description of “Hardware Risk” in Table 5-2.</p>

 Low Risk	An unexpected change in the system configuration has been detected. The change should be examined to determine if it was truly unexpected or simply made by a system that has not been integrated with this IV application. For more information, refer to the description of “Config Risk” in Table 5-2.
 No Detected Risk	The integrity tests did not fail or indicate unexpected changes. This DOES NOT mean that the device has not been compromised. For more information, refer to “Integrity of Measurements and No Detected Risk”, Page 1-2

## Using the risk level filter

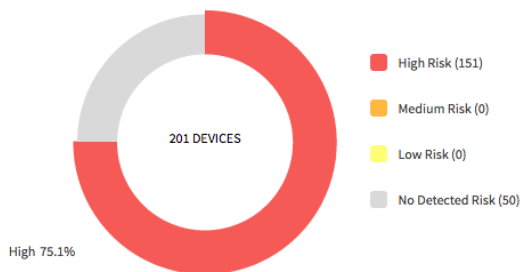
To display only devices with a selected overall risk level, click on the segment of the circle that corresponds to the desired risk level.



L

The number in the center of the circle represents total number of devices being monitored by the IV application.



Placing your cursor on or hovering over a slice of the circle causes the percentage of devices with the selected risk level to be displayed.






## Using the risk type filter

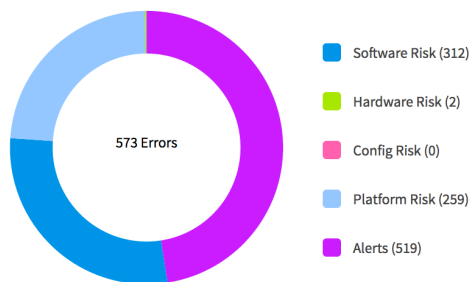
The risk types used in the IV application are described in Table 5-2. IV Measurement Type Risks

**Table 5-2. IV Measurement Type Risks**

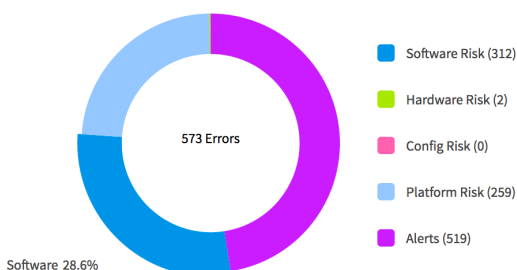
Risk Type	Description
 Software	Filter and only show devices that failed at least one “Software” integrity measurement test. For more information, see “Software Integrity”, Page 5-11
 Hardware	Filter and only show devices that failed at least one “Hardware” integrity measurement test. For more information, see “Hardware Integrity”, Page 5-16

 Configuration	Filter and only show devices that failed at least one “Configuration” integrity measurement test. For more information, see “Configuration Integrity Measurements”, Page 5-18
 Platform	Filter and only show devices that failed at least one “Platform” integrity measurement test. For more information, see “Platform Integrity”, Page 5-8
 Alerts	Informational alerts to highlight key aspects of a device’s support for integrity verification capabilities. For this release of the IV app, alerts are used to highlight devices that do not support the “Boot Integrity Visibility (BIV)” capability which is the key component of the “Platform” risk type. Since the BIV capability and the underlying device protection technologies used to implement this capability (Image Signing, Secure Boot, Trust Anchors and Secure Identities (SUDI)) are becoming table stakes for trustworthy systems, we believe it important to help customers identify devices in their network that have a higher risk profile. Customers should evaluate the place these devices serve in their networks to determine their organization’s position on the acceptance of this increased risk and any actions that may be warranted.

To display only devices with a selected risk type, click on the segment of the circle that corresponds to the desired risk type



Placing your cursor on or hovering over a slice of the circle causes the percentage of devices with the selected risk type to be displayed.



## Removing Filters

To remove filters and show all devices, click on the

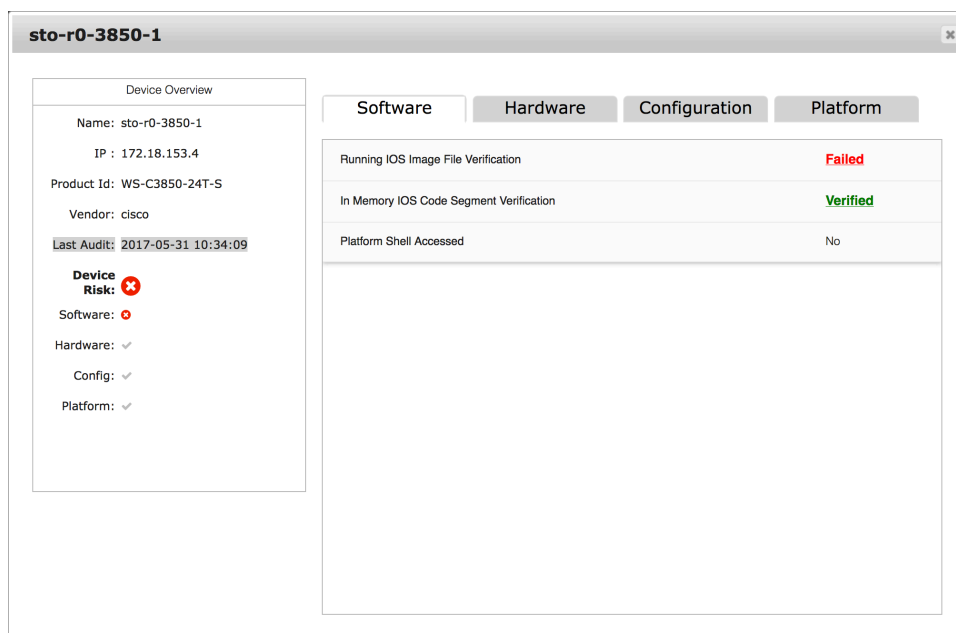
Clear Filters

button located on the top left portion of the window.



## Viewing Detailed Device Integrity Measurement Results

Clicking on a device's name or any of its risk icons will bring up a window that displays detailed measurement verification information.



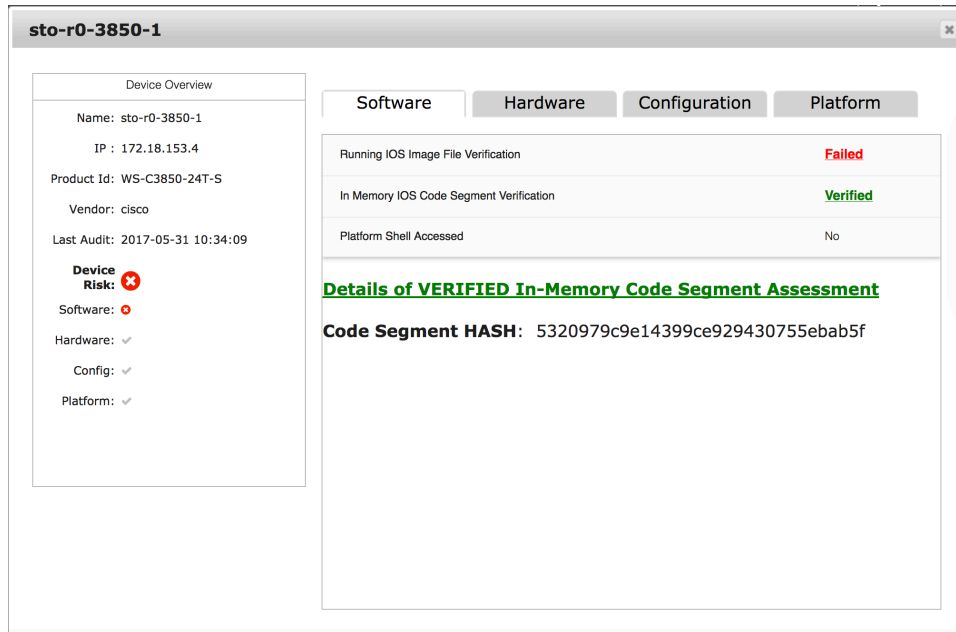
The left side of the display contains the summary results. A key piece of information is “Last Audit” which is the timestamp of the last integrity verification check performed on this device.

The right side of the display has tabs for each of the integrity measurement types. The content is consistent in each tab. The top section contains the tests performed with their corresponding results. The results are one of the following:

**Table 5-3. Verification Results**

Result	Description
<u>Verified</u>	Test has been performed and passed
<u>Failed</u>	Test has been performed but failed
<u>Yes</u> / No	The monitored event was or was not observed
<u>Unverified</u>	Any result other than Verified or Failed. Possible reasons may include: <ul style="list-style-type: none"> <li>• IV Service Wide Assessment inactive (set to NO) for the assessment in question.</li> <li>• Assessment (i.e. CLI) not supported on the device</li> <li>• Device did not recognize the command</li> <li>• Device Connection down</li> <li>• “Unknown File” for Image File Assessment (i.e. file not recognized or not on the box, if CLI was sent) (file path is off-box (tftp), command will not be sent, etc..)</li> </ul>

If a result is underlined, you can click on the result to see the corresponding test details. For example, Verified was clicked in the following screen shot.



There are currently three main types of validation checks:

**Table 5-4. IV Validation Check Types**

Validation Check	Description
Known Good Value (KGV)	<p>These assessments involve collecting a distinct piece of Integrity data from the device, and comparing it to a Known Good Value database provided by Cisco to determine if it is valid data.</p> <p>The typical verification failure causes and associated methods to clear the failure include the following:</p> <ol style="list-style-type: none"> <li>1. The item being checked has been compromised – the only way to clear this failure is to replace the compromised item with a version that is authentic Cisco software.</li> <li>2. Missing KGV for the item being checked – install the KGV for the associated item to clear this failure.</li> </ol> <p>In both cases above, the failure would be cleared after the next APIC-EM polling interval and associated integrity verification checks for the device.</p>



Validation Check	Description
Imprint Value	<p>These assessments involve collecting a snapshot of a distinct piece of Integrity data from a device, and using that snapshot of that data as the “imprint value”. As data is collected over time, the collected data is then compared to the “imprint value” to assess if the data has changed from the expected value. Although these are simple comparison checks, they are a valuable tool in detecting indicators of compromise (IoC).</p> <p>These failures can be cleared by accepting the new values as valid, making them the new imprint value to be used for future integrity verification checks.</p> <p><b>Caution:</b> Be extra careful when reviewing the new information to ensure there are no hidden changes that are incorrect and/or detrimental to the operation of the device or network. Only click <span>Accept Changes</span> when you are absolutely certain the new information is correct.</p>
Event occurrence	<p>These assessments look for events that should not occur during normal operation. For example, observing a “shell access” event during normal operation may be an IoC.</p> <p>These failures can be cleared by accepting the event as valid.</p> <p><b>Caution:</b> Be certain you understand WHY and WHO accessed the platform shell before clearing this event. Only click <span>Accept Changes</span> when you are absolutely certain no one has adversely tampered with the device while in shell access.</p>

## Integrity measurement types

The categories of verification checks performed by the IV application are described in Table 5-5. Integrity Measurement Types.

**Table 5-5. Integrity Measurement Types**

Measurement Type	Function	Reference
Platform	Is the device authentic? Includes verification of the boot process and the identity of the device.	Platform Integrity , Page 5-8
Software	Is the software used by the device authentic? Includes checks of the software files and in-memory contents.	Software Integrity , Page 5-11
Hardware	Does the device contain the hardware components that are expected? Includes checks of the hardware inventory.	Hardware Integrity , Page 5-16
Configuration	Are there any unexpected changes in the device configuration? Includes checks of the running configuration.	Configuration Integrity Measurements, Page 5-18

Detailed information for each integrity measurement type, including descriptions of the verification checks performed and example data provided when a failure is identified, is provided in the following sections.


## Platform Integrity Measurements

The following are possible platform integrity questions that can be answered by the measurements taken by the Cisco IV application:

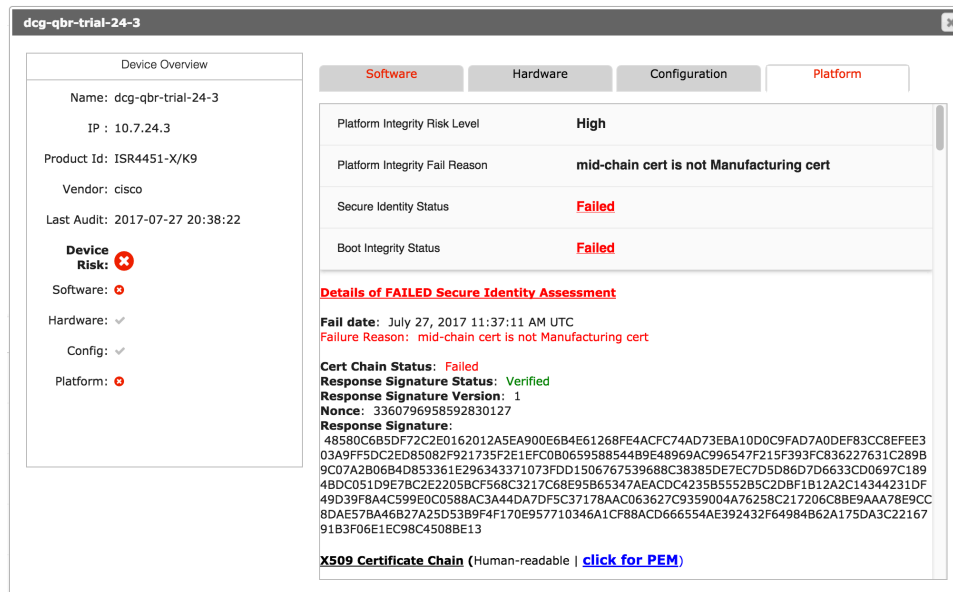
- Is the device authentic Cisco hardware?
- Did the device boot properly using only authentic Cisco software?
- Is it truly the expected device?

The verification checks performed to help answer these questions are described in Table 5-6. Platform Verification Checks.

**Table 5-6. Platform Verification Checks**

Verification Check	Function	Description
Secure Identity	What is the true identity of the device?	 High Risk  For Secure Identity, a “ <b>Failure</b> ” is declared if the device’s identity or the associated certificate chain cannot be authenticated.
Boot Integrity	What versions of software were used to boot the device and are they authentic Cisco software?	  Boot Integrity verifies the integrity measurement of the software used to boot the device against Cisco’s published KGVs. A “ <b>Failure</b> ” is declared if a matching KGV is not found for any of the boot software.  A “ <b>Failure</b> ” is also declared if the response from the device cannot be authenticated.  Both of these verification checks utilize the capabilities provided by Cisco’s Boot Integrity Visibility (BIV) feature.  The BIV feature is described in this document: <a href="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">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</a>  The list of platforms that support BIV is provided in Table 6-3. Boot Integrity Visibility support.  These verification checks are performed when the IV app discovers a new device and when it detects a reboot of the device.

The Secure Identity check verifies both the identity of the device and the associated certificate chain. It does this using the device’s secure identity certificate stored in the device’s trust anchor, its associated private key, a nonce to prevent re-play attacks, and cryptography to ensure authenticity. The example below depicts an error where one of the items in the certificate chain is invalid. The complete set of information provided in this screen is shown in Figure 5-2. Secure Identity Check – Detailed Failure Information.



**Figure 5-2. Secure Identity Check – Detailed Failure Information**

#### 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:**

48580C6B5DF72C2E0162012A5EA900E6B4E61268FE4ACFC74AD73EBA10D0C9FAD7A0DEF83CC8EFEE303A9FF5DC2ED85082F921735F2E1EFC0B0659588544B9E48969AC996547F215F393FC836227631C289B9C07A2B06B4D853361E296343371073FDD1506767539688C38385DE7EC7D5D86D7D6633CD0697C1894BDC051D9E7BC2E2205BCF568C3217C68E95B65347AEACDC4235B5552B5C2DBF1B12A2C14344231DF49D39F8A4C599E0C0588AC3A44DA7DF5C37178AAC063627C9359004A76258C217206C8BE9AAA78E9CC8DAE57BA46B27A25D53B9F4F170E957710346A1CF88ACD666554AE392432F64984B62A175DA3C2216791B3F06E1EC98C4508BE13

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

-----BEGIN CERTIFICATE-----

<snip>

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

<snip>

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

<snip>

-----END CERTIFICATE-----

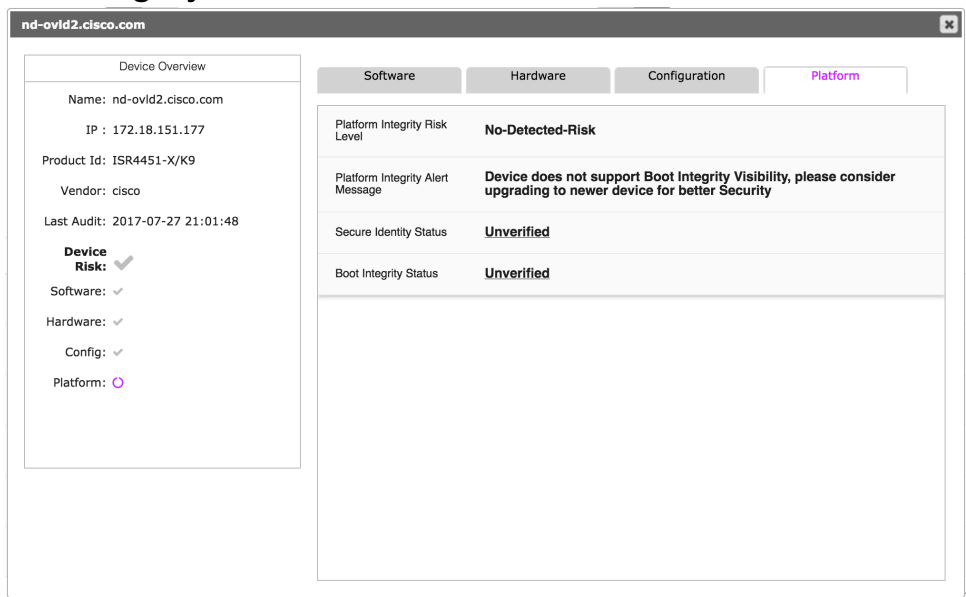
The Boot Integrity check verifies the software used to boot the device by extracting the associated file integrity measurements, stored in the device's trust anchor during the boot process, using a nonce to prevent re-play attacks, and cryptography to ensure authenticity. The Figure 5-3. Boot Integrity Check – Detailed Failure Information below depicts an error where the software has been compromised. The “**Boot Integrity Signature Status: Verified**” status indicates that the information was obtained from the device correctly and has been authenticated. However, the images used to boot the device are not known to be good by the IV application.

**Figure 5-3. Boot Integrity Check – Detailed Failure Information**

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

**Note:** Figure 5-4. Boot Integrity check – Unverified depicts a special case that warrants highlighting. The platform integrity checks provide the initial anchor in the integrity verification trust chain. They provide an extremely strong method to attest to the identity and initial boot status of the device. All future integrity checks build on this anchor. While there are numerous reasons for an “**Unverified**” result, the most likely reason is the device does not support the features required for platform integrity checks. Customers are strongly urged to evaluate the risk and impact of a compromise to these devices and consider refreshing with one of Cisco’s more current and secure devices.

Figure 5-4. Boot Integrity check – Unverified





Software Integrity Measurements


The following are possible software integrity questions that can be answered by the measurements taken by the Cisco IV application.

- Is the software used on the device authentic?
- Are the files correct? Have there been any changes to them during execution?
- Has anyone gained unauthorized access which may indicate nefarious activities?

The verification checks performed to help answer these questions are described in Table 5-7. Software Verification Checks

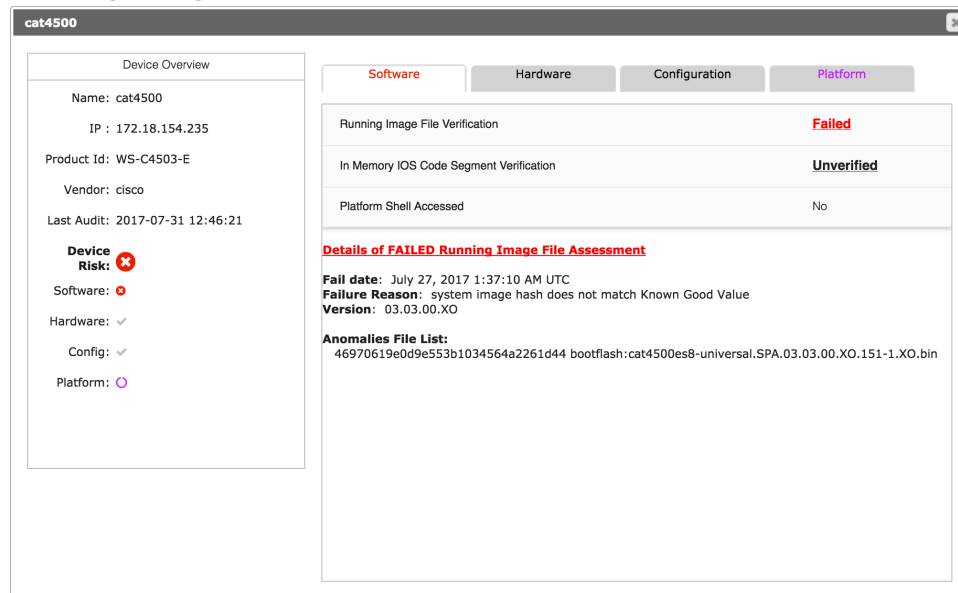
**Table 5-7. Software Verification Checks**

Verification Check	Function	Description
Running Image File Verification	Are the software files used by the device authentic?	<p> High Risk</p> <p>This check verifies the integrity measurement of a software file against Cisco's published KGVs. A <b>"Failure"</b> is declared if a matching KGV is not found.</p> <p>This verification check offers limited coverage for devices that do not support the Boot Integrity check. Key differences between the Running Image File Verification capability and the Boot Integrity Verification capability include the following:</p> <ul style="list-style-type: none"> <li>• Does not cover boot0 or bootloader software</li> <li>• Measurements not protected in the trust anchor</li> <li>• Measurements not authenticated</li> </ul> <p>This verification check is performed when the IV app discovers a new device and when it detects a reboot of the device.</p>
In-Memory IOS Code Segment Verification	Is the software that is running on the device still authentic? i.e., have there been any unexpected changes?	<p> High Risk</p> <p>This check verifies the integrity measurement of software in memory against an initial imprint value obtained on initial discovery or reboot detection of the device by the IV application. A <b>"Failure"</b> is declared if future measurements do not match the imprint value.</p> <p><b>Note:</b> The in-memory check is currently only supported for IOS devices.</p> <p>A system could potentially be compromised via unauthorized access to the device (phishing for credentials or insider attacks) or by leveraging a known or unknown vulnerability.</p> <p><b>Note:</b> Customers are urged to keep their software current and deploy patches or new software to address new vulnerabilities as they are discovered.</p> <p>This verification check is performed at each APIC-EM polling interval of the device.</p>

Verification Check	Function	Description
Platform Shell Accessed	Has the platform shell been accessed? This should not normally occur. If the platform shell has been accessed, then by whom and why?	<p> Medium Risk</p> <p>This check monitors the device syslog looking for a shell access event. A <b>“Failure”</b> is declared if the event is found.</p> <p>Shell access is abnormal during normal operation of a device. Detection that shell access has occurred could indicate nefarious activity on the device.</p> <p>This verification check is performed at each APIC-EM polling interval of the device.</p>

An example where the Running Image File Verification check has failed is depicted in Figure 5-5. Key failure results items are discussed in Table 5-8. Running Image File Verification - Key Results.

**Figure 5-5. Running Image File Verification - Failed Example**



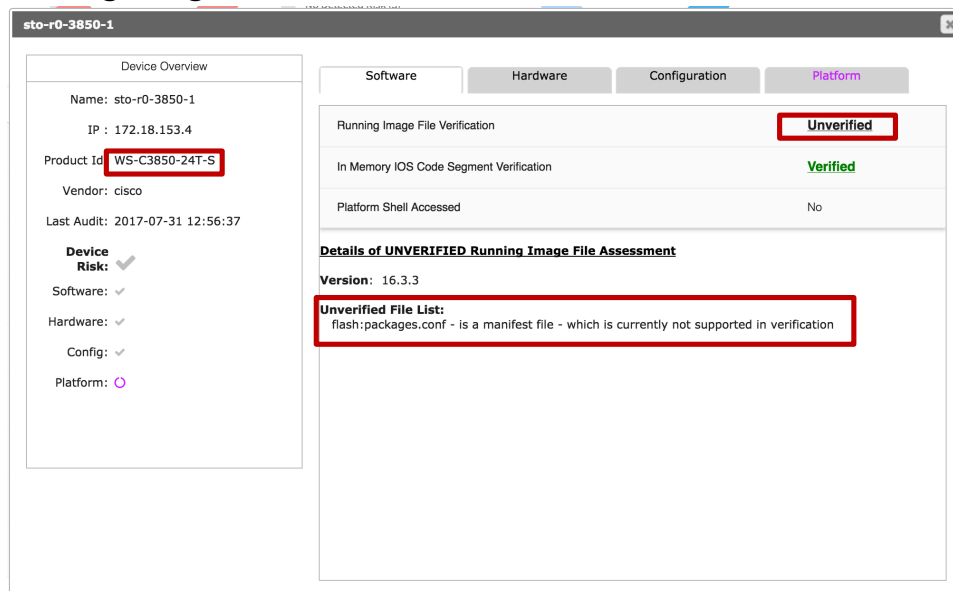
**Table 5-8. Running Image File Verification - Key Results**

Content	Function
Fail date:	<p>When the IV application detected this failure. The displayed date and time are likely NOT the actual occurrence of the failure. The IV application checks integrity measurements based on the polling interval setting cycle defined for APIC-EM. Therefore, If the APIC-EM polling interval setting were set to 25 minutes, then the time of the actual failure is between the date/time displayed and 25 minutes or so prior to this date/time.</p> <p><b>Note:</b> One notable exception - the actual failure time could be significantly longer in cases where the IV application has just started or a new device has just been discovered by the IV application. In these cases, the actual failure date/time is indeterminate.</p>

Content	Function
Anomalies File List:	<p>Provides the measured hash (17e0c15d12eb5c86220f3d325750d2f4) and path and file name (bootflash:isr4400-universalk9.16.04.01.SPA.bin) for the running image file.</p> <p><b>Note:</b> The first item to investigate is to ensure you have KGV data loaded for this image to determine if the device has been compromised; or, the error is simply the result of missing KGV data.</p>

Figure 5-6. Running Image File Verification – Bundles, depicts another special case. As noted (**Note 1:**) in the section on Supported Platforms, the current version of the IV application does not yet handle a few select devices that unbundle the image file during installation. For these devices, the image file name returned by the device is `packages.conf` which is listed in the “Unverified File List”. The KGV associated with this file is not available in the KGV data. Nor does the IV application currently check the individual image files that were unbundled during installation. To prevent false positive results, the IV application does not perform the running image file verification check for these devices. This is indicated in the display as “**Unverified**”.

**Figure 5-6. Running Image File Verification – Bundles**



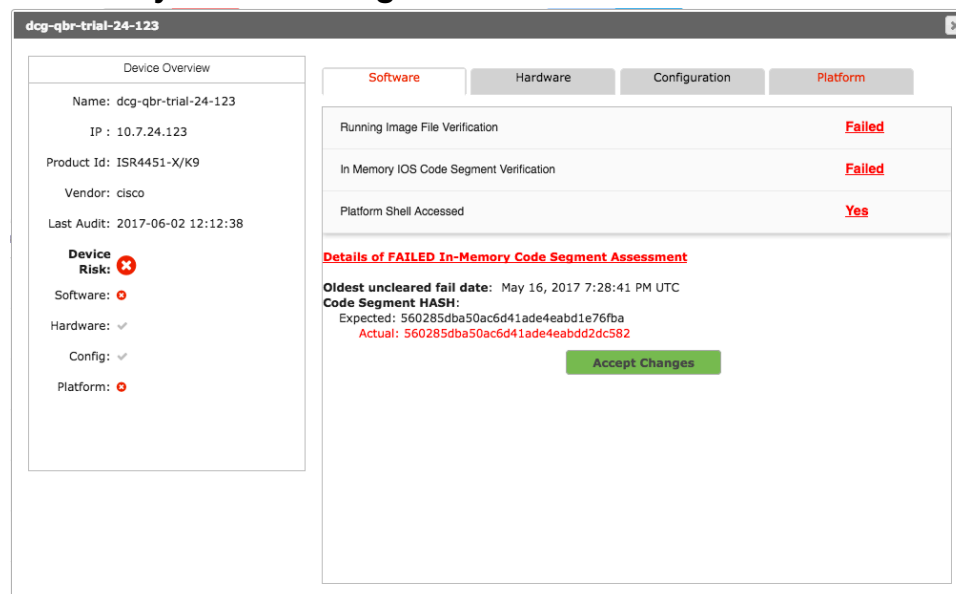
Additional reasons where the System Image File(s) is/are identified as being “**Unverified**” include:

- file not found on device – or other error – check IV logs
- is an off device image file – which is currently not supported in verification
- is a manifest file – which is currently not supported in verification
- Image File Assessment capability not supported on device
- device unreachable – or other error – check IV logs
- Image File Assessment Setting is INACTIVE
- No Image File names available for verification at Last Audit Time



Figure 5-7. In-Memory IOS Code Segment Verification – Failed, depicts an example where the initial imprint value of the program in memory has changed. It is conceivable that an unauthorized individual (bad actor) could change the program in memory, perform unauthorized actions, and then reboot the device to erase any evidence of the change. To prevent the loss of the original verification check failure detection, the IV application retains the failure condition until manually cleared.

**Figure 5-7. In-Memory IOS Code Segment Verification – Failed**



**Caution:** Ideally, one should perform forensics on the device before proceeding. However, if conditions warrant taking immediate action one should consider these steps:

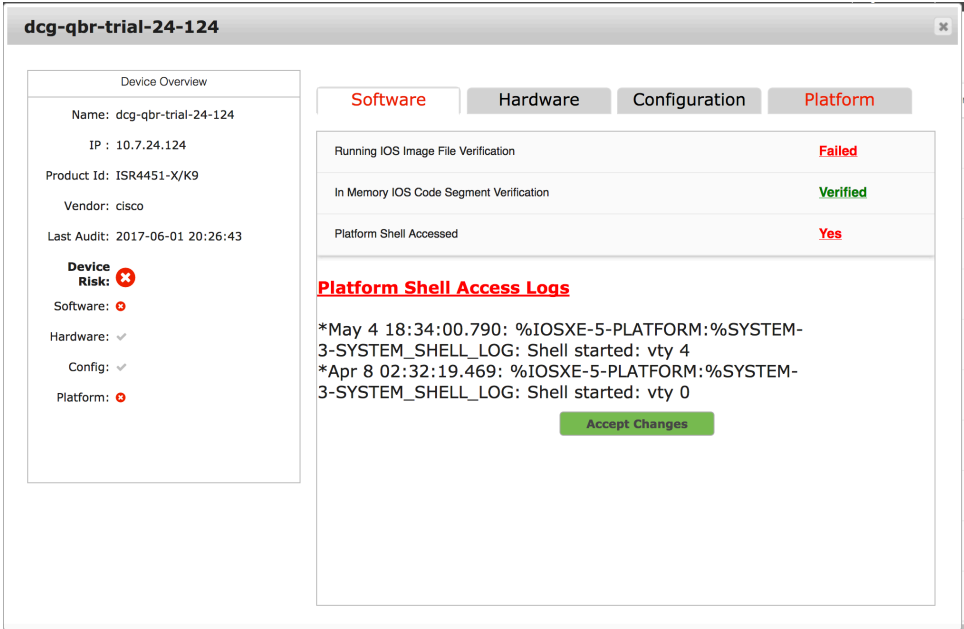
1. Verify that the boot image files are authentic
2. Immediately reboot the device
3. While the device is rebooting, click Accept Changes

This will return the device to a known good state by booting from authenticated software, cause IV to take a new imprint value of the program in memory, and begin testing for any changes in the future.

Accessing the platform shell is an atypical event. It should not happen during normal operation of the device. Observing a “shell access” event during normal operation may be an IoC. Figure 5-8. Platform Shell Accessed – Failed depicts the results provided when shell access has been discovered. This failure indication can be cleared by accepting the event as valid.

**Caution:** You must know who and understand why they accessed the platform shell before clearing the event. Only click Accept Changes, when you are absolutely certain that no one has adversely tampered with the device while in shell access.

Figure 5-8. Platform Shell Accessed - Failed



Hardware Integrity Measurements

My device went off-line for an unknown reason then came back online later. Were any unauthorized changes made to the device hardware? The verification check performed to help answer this question is described in Table 5-9. Hardware Verification Checks

Table 5-9. Hardware Verification Checks

Verification Check	Function	Reference
Hardware Inventory	Have any unauthorized hardware changes been made to my device?	<div><div></div>Medium Risk</div> <p>This compares the hardware inventory against an initial imprint value obtained on initial discovery of the device by the IV application. A <b>Failure</b> is declared if future measurements do not match the imprint value.</p> <p>This verification check is performed at each APIC-EM polling interval of the device.</p>

If a change is detected in the hardware inventory, the detailed results portion of the display will show the expected and actual inventories, highlighting the differences. In the example provided below, the serial number of ISR4451-X-4x1GE card has changed from SN: JAB309309EL to SN: JAB819809EL.

dcg-qbr-trial-25-243

Device Overview

Name: dcg-qbr-trial-25-243  
IP : 10.7.25.243  
Product Id: ISR4451-X/K9  
Vendor: cisco  
Last Audit: 2017-06-01 19:29:09  

Device Risk: ✖  
Software: ✔  
Hardware: !  
Config: ✔  
Platform: ✖

Software

Hardware

Configuration

Platform

Hardware Inventory Verification

Failed

Expected	Actual
...	...
9 PID: ISR4451-X/K9 , VID: , SN:	9 PID: ISR4451-X/K9 , VID: , SN:
10	10
11 NAME: "NIM subslot 0/0", DESCR: "Front Panel 4 ports Gigabitethernet Module"	11 NAME: "NIM subslot 0/0", DESCR: "Front Panel 4 ports Gigabitethernet Module"
12 PID: ISR4451-X-4x1GE , VID: V01 , SN: JAB309309EL	12 PID: ISR4451-X-4x1GE , VID: V01 , SN: JAB819809EL
13	13
14 NAME: "Fan Tray", DESCR: "Cisco ISR4450, ISR4350 Fan Assembly"	14 NAME: "Fan Tray", DESCR: "Cisco ISR4450, ISR4350 Fan Assembly"
15 PID: ACS-4450-FANASSY , VID: , SN:	15 PID: ACS-4450-FANASSY , VID: , SN:
...	...

diff view generated by jsdifflib

This change could be intentional; for example, due to the replacement of a bad part or as the result of some other unexpected activity. If the change is valid and expected, you can “accept” the change and make the new hardware inventory the imprint value to be used for future integrity checks by clicking on the “Accept Changes” button found at the end of the inventory list.

dcg-qbr-trial-24-3

Device Overview

Name: dcg-qbr-trial-24-3  
IP : 10.7.24.3  
Product Id: ISR4451-X/K9  
Vendor: cisco  
Last Audit: 2017-06-14 18:19:00  

Device Risk: ✖  
Software: ✔  
Hardware: !  
Config: ✔  
Platform: ✖

Software

Hardware

Configuration

Platform

Hardware Inventory Verification

Failed

Expected	Actual
1	1
2 NAME: "NIM subslot 0/0", DESCR: "Front Panel 4 ports Gigabitethernet Module"	2 NAME: "NIM subslot 0/0", DESCR: "Front Panel 4 ports Gigabitethernet Module"
3 PID: ISR4451-X-4x1GE , VID: V01 , SN: JAB092709EL	3 PID: ISR4451-X-4x1GE , VID: V01 , SN: JAB668809EL
4	4
5 NAME: "Fan Tray", DESCR: "Cisco ISR4450, ISR4350 Fan Assembly"	5 NAME: "Fan Tray", DESCR: "Cisco ISR4450, ISR4350 Fan Assembly"
6 PID: ACS-4450-FANASSY , VID: , SN:	6 PID: ACS-4450-FANASSY , VID: , SN:
...	...

Accept Changes

**Caution:** Before clicking on Accept Changes, take extra care and look closely at the inventory change list. Hastily accepting the new inventory after reviewing only the first deltas could result in missing an adverse change that will remain undetected.

## Configuration Integrity Measurements


The following are possible configuration integrity questions which can be answered by the measurements taken by the Cisco IV application:

- Is the device operating as expected?
- Has anyone made unauthorized or unexpected changes to its configuration?

The verification check performed to help answer these questions are described in Table 5-10. Configuration Verification Checks

**Note:** This initial release of the IV application has not been integrated with the APIC-EM controller configuration management, so any controller driven changes will also show up as an unexpected change and result in a “**Failure**” being declared. For this reason, configuration checking has been disabled by default.

**Table 5-10. Configuration Verification Checks**

Verification Check	Function	Reference
Running Configuration	Have any unauthorized or unexpected changes been made to my device's configuration?	 Low Risk  This verification check compares the running configuration against an initial imprint value obtained on initial discovery of the device by the IV application. A “ <b>Failure</b> ” is declared if future measurements do not match the imprint value.  <b>Note:</b> This check is disabled by default for the IV application.  This verification check is performed at each APIC-EM polling interval of the device.

If a change is detected in the running configuration, the detailed results portion of the display will show the expected and actual configurations, highlighting the differences. In the example provided below, there are numerous changes. Make sure you scroll through the entire configuration to evaluate and understand the changes.

dcg-qbr-trial-24-3

Device Overview

Name: dcg-qbr-trial-24-3  
IP : 10.7.24.3  
Product Id: ISR4451-X/K9  
Vendor: cisco  
Last Audit: 2017-06-14 18:12:49  
**Device Risk:** ✖  
Software: ✔  
Hardware: ✔  
Config: ⚠  
Platform: ✖

Software

Hardware

Configuration

Platform

Configuration Verification

Failed

Expected	Actual
1	1
2 Building configuration...	2 Building configuration...
3	3
4 Current configuration : 1610 bytes	4 Current configuration : 1732 bytes
5 !	5 !
6	6 ! Last configuration change at 14:11:54 EDT Wed Jun 14 2017
7	7 ! NVRAM config last updated at 14:12:09 EDT Wed Jun 14 2017
8	8 !
9 version 16.3	9 version 16.3
10 service timestamps debug datetime msec localtime show-timezone	10 service timestamps debug datetime msec localtime show-timezone
11 service timestamps log datetime msec localtime show-timezone	11 service timestamps log datetime msec localtime show-timezone
12 no platform punt-keepalive disable-kernel-core	12 no platform punt-keepalive disable-kernel-core
13 !	13 !
14 hostname dcg-qbr-trial-24-3	14 hostname dcg-qbr-trial
15 !	15 !
16 boot-start-marker	16 boot-start-marker
17 boot-end-marker	17 boot-end-marker
...	...
71 !	74 !

This change could be intentional; for example, the addition of a new adjacent node or a change in QOS policy or the result of some other unexpected activity. If the change is valid and expected, you can “accept” the change and make the new configuration the imprint value to be used for future integrity checks by clicking on the “Accept Changes” button found at the end of the inventory list.

dcg-qbr-trial-24-3

Device Overview

Name: dcg-qbr-trial-24-3  
IP : 10.7.24.3  
Product Id: ISR4451-X/K9  
Vendor: cisco  
Last Audit: 2017-06-14 18:12:49  
**Device Risk:** ✖  
Software: ✔  
Hardware: ✔  
Config: ⚠  
Platform: ✖

Software

Hardware

Configuration

Platform

5 !	7 ! NVRAM config last updated at 14:12:09 EDT Wed Jun 14 2017
6 version 16.3	8 !
7 service timestamps debug datetime msec localtime show-timezone	9 version 16.3
8 service timestamps log datetime msec localtime show-timezone	10 service timestamps debug datetime msec localtime show-timezone
9 no platform punt-keepalive disable-kernel-core	11 service timestamps log datetime msec localtime show-timezone
10 !	12 no platform punt-keepalive disable-kernel-core
11 hostname dcg-qbr-trial-24-3	13 !
12 !	14 hostname dcg-qbr-trial
13 boot-start-marker	15 !
14 boot-end-marker	16 boot-start-marker
...	17 boot-end-marker
71 !	...
72 interface GigabitEthernet0/0/0	74 !
73 no ip address	75 interface GigabitEthernet0/0/0
74 shutdown	76 no ip address
75 negotiation auto	77 no shutdown
76 !	78 negotiation auto
77 interface GigabitEthernet0/0/1	79 !
...	80 interface GigabitEthernet0/0/1
	...

Accept Changes

**Caution:** Before clicking on “Accept Changes”, take extra care and look closely at the configuration change list. Hastily accepting the new configuration after reviewing only the first deltas could result in missing an adverse change that will remain undetected.





## Support

---

### System Requirements

#### Hardware and Software Requirements

System requirements for the APIC-EM also apply to the IV App. For more information, see the [Cisco Application Policy Infrastructure Controller - Enterprise Module Data Sheet](#).

**Note:** When the IV application is first activated, it will run IV assessments on each device as the APIC polls that device, so it will take a full polling interval for all devices to show up in the IV Device Table (polling interval as defined by the "Polling Time" value in the APIC-EM Settings page, under the 'Polling Interval' in the DISCOVERY CREDENTIALS section).

This first interval is where most of the additional processing power is needed by both the IV application and the devices, as many of the highest CPU usage IV assessments are only run the initial time the IV application becomes aware of the device, and when a device reboot is detected. Subsequent polling intervals will see a significant reduction in processing power used by the IV Service.

### Technical Support


The IV application on APIC-EM 1.5 is provided as a "Beta" offering. As such, support will be provided on a best-effort basis. Customers may send questions or information about issues they are encountering with the IV application to the IV application support e-mail address: [iv-app-support-external@cisco.com](mailto:iv-app-support-external@cisco.com)

**Note:** While the IV application support team will review and attempt to address each question or issue, we may not be able to provide individual or immediate responses to everyone.

### Feature Requests

Want something new for the IV application? Simply click  I wish this page would... located at the bottom right corner of each window and tell us how we can make the IV application better.

**Note:** If you are viewing detail results, you will need to close the popup window to make active.

 I wish this page would...

## Supported Platforms

The platforms supported by the IV application, along with the Integrity measurement types supported by each platform, are identified in Table 6-1.

**Note:** This list is accurate at the time this document was published. Refer to the release notes for the version of the IV application that you are using for any updates to this list.

**Note:** The IV application does not differentiate between "supported devices" and unsupported devices. It will attempt the active assessments on any device. The results for any unsupported devices may vary and include **"Unverified"** if the device does not support the integrity measurement or **"Failed"** if the KGV for the device is not available.

**Table 6-1. Platform Support**

Device	Integrity Measurement Type Support						
	Platform	Software				Hardware	Configuration
		Image	In-Memory	IMA	Shell Access		
<b>Switches</b>							
Cisco Catalyst 2960-S	N	Y <sup>1</sup>	Y	N	Y	Y	Y
Cisco Catalyst 2960-X/XR	N	Y <sup>1</sup>	Y	N	Y	Y	Y
Cisco Catalyst 3560CG	N	Y <sup>1</sup>	Y	N	Y	Y	Y
Cisco Catalyst 3560CX	N	Y <sup>1</sup>	Y	N	Y	Y	Y
Cisco Catalyst 3560-X	N	Y <sup>1</sup>	Y	N	Y	Y	Y
Cisco Catalyst 3650	Y <sup>3</sup>	Y <sup>1</sup>	Y	N	Y	Y	Y
Cisco Catalyst 3750-X	N	Y <sup>1</sup>	Y	N	Y	Y	Y
Cisco Catalyst 3850	Y <sup>3 &amp; 4</sup>	Y <sup>1</sup>	Y	N	Y	Y	Y
Cisco Catalyst 4500 (Sup7E)	N	Y <sup>1</sup>	N	N	Y	Y	Y
Cisco Catalyst 4500 (Sup8E)	N	Y <sup>1</sup>	N	N	Y	Y	Y
Cisco Catalyst 4500-X	N	Y <sup>1</sup>	N	N	Y	Y	Y
<b>Industrial Ethernet Switches</b>							
Cisco Industrial Ethernet 2000 Series Switches	N	Y <sup>1</sup>	Y	N	Y	Y	Y
Cisco Industrial Ethernet 3000 Series Switches	N	Y <sup>1</sup>	Y	N	Y	Y	Y
Cisco Industrial Ethernet 4000 Series Switches	N	Y <sup>1</sup>	Y	N	Y	Y	Y
<b>Routers</b>							
Cisco Integrated Service Router (ISR) 800 Series	N	Y	N	N	Y	Y	Y



Device	Integrity Measurement Type Support						
	Platform	Software				Hardware	Configuration
		Image	In-Memory	IMA	Shell Access		
Cisco Integrated Services Router (ISR) 2900 Series	N	Y	Y <sup>2</sup>	N	Y	Y	Y
Cisco Integrated Services Router (ISR) 3900 Series	N	Y	Y <sup>2</sup>	N	Y	Y	Y
Cisco Integrated Service Router (ISR) 4000 Series	Y <sup>3</sup>	Y	Y	N	Y	Y	Y
Cisco ASR 1000 Series Aggregation Services Router	Y <sup>3</sup>	Y	Y	N	Y	Y	Y

**Note 1:** The initial release of the IV application on APIC-EM only supports switches where the software was installed using the “BUNDLE” installation mode. Devices where the software was installed using the “INSTALL” installation mode are not currently supported. The Running Image File Verification for these devices will likely fail. See Figure 5-6. Running Image File Verification – Bundles for more information.

**Note 2:** The devices listed in Table 6-2. In-Memory check exceptions do not support in-memory verification checks for the identified software versions.

**Table 6-2. In-Memory check exceptions**

Device	Software Version	Caveat ID Number
Cisco Integrated Service Router (ISR) 3900 Series	version <15.6	<a href="#">CSCus44043</a>
Cisco Catalyst 4500 Series	all versions	none
Cisco Integrated Service Router (ISR) 1800 Series	all versions	<a href="#">CSCuv19944</a>
Cisco Integrated Service Router (ISR) 800 Series	all versions	<a href="#">CSCvc58273</a>

**Note 3:** The specific platforms and associated minimum software releases that support the “Boot Integrity Visibility” feature which provides the platform integrity measurements are identified in Table 6-3.

**Table 6-3. Boot Integrity Visibility support**

Platform	Minimum Software Release Version	Minimum Rommon / Bootloader Version
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)
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 <sup>4</sup> WS-C3850-24XS <sup>4</sup> WS-C3850-48XS <sup>4</sup> WS-C3850-24XU WS-C3850-12X48U	16.3.2	4.28

**Note 4:** While the versions of Cisco Catalyst 3850 listed in Table 3 above do support the Boot Integrity Visibility feature, there is an existing defect, [CSCve69298](#), that results in a “Failed” integrity verification test result. The detailed test results are provided in Figure 6-1 Defect CSCve69298 - Cisco Catalyst 3850 Platform Integrity Check Results. This defect is only known to exist in these versions of the Cisco Catalyst 3850:

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

**Figure 6-1 Defect CSCve69298 - Cisco Catalyst 3850 Platform Integrity Check Results**

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:**  
D0FB0FC82CFAEAF51E26FF068F647EFB9605182D50CEBDF3CCB659E7A5FE2303B0A4BE6E0DE5697F7  
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  
3487BE8DC70C6F689D267670149E27EAF755F2EDCC4A1  
**OS Image Status:** Failed  
**OS Image Version:** 16.05.01a  
**OS Image Hash:**  
2A032EC6C5EBF60607FC9CE246AE2F7B4E1F69E7024CCDDC1238D42DDA9A08504EFE45F513DE442D1  
7EC72DB6ECD796733F2730A081822B73823EFB8DEFAF91C  
**PCR0:** E134BBD05A21B43DC147DDBD9CC35AF56E87FC8FAE78240D25A7C799B47C66A1  
**PCR8:** A15A2E774B47D186B5ED618AEF1331943A21AB63CD21E0C2D17D3BC680A6BBA8

**Caution:** To ensure a Platform Integrity “Failed” test result for a Cisco Catalyst 3850 is the result of [CSCve69298](#) and not due to other unknown or unexpected reasons, verify that the results for your device match the following:

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**