Cisco Integrity Verification Application (Beta) on APIC-EM Release Notes, Release 1.5.0.266

First Publish: August 01, 2017

Cisco Systems, Inc.
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.

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. 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.

CONTENTS

Introduction **1**

What's New in Release 1.5.0.266 ..... **1**

System Requirements **2**

Supported Platforms **3**

Limitations **8**

Related Documentation **9**

Obtaining Documentation and Submitting a Service Request **9**

Introduction

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).

Note: Cisco IV App, currently in its Beta phase, is available for proof-of-concept use and trials. The application is supported with Cisco APIC-EM release 1.5.0.x.

What's New in Release 1.5.0.266

This software release provides the following new features and functions:

- The ability to instruct the IV Application, via a "Request Upload" button on the KGV tab of the IV UI page, to retrieve the latest published Cisco_KnownGoodValues.tar file from https://tools.cisco.com, verify the file's signature and add the latest KGV values to the IV KGV database.
- A "Clear Filters" button has been added to the DEVICES tab of the IV UI page, which clears any existing filters that were in effect, and displays all available devices.
- The "Hostname" column of the Device table under the DEVICES tab of the IV UI page has been renamed to the "Device Name" column.
- The 'ntp clock-period' line of a device's running-config display has been excluded from IV Configuration Analytics verification, due to its dynamic nature. This prevents false positives from IV Configuration Analytics due to 'ntp clock-period' changes.
- A "Reset" option has been added to the Configuration setting on the IV SETTINGS tab of the IV UI. This Reset setting can only be transitioned to from the "No" setting. The "Reset" setting causes the IV configuration integrity data for all devices to be reset to "default" values, effectively clearing all previous configuration integrity data for all devices. This option is useful for scenarios where a "maintenance activity" may cause significant "false positives" in the IV Configuration Analytics verification.
- A new field, "Unverified File List", has been added under the Software tab of the Device Details pop-up window, as part of the "Running Image File Verification" details. This field will list any image file names that could not be verified, along with the reason why they could not be verified. If there are no unverified image files, this field will not be present in the display.
- The ability to toggle between a PEM Certificate Chain display and a 'human readable' Certificate Chain display has been added under the Platform tab of the Device Details pop-up window, as part of the "Secure Identity Status" details display.
- A new field "Details" has been added under the Platform tab of the Device Details pop-up window, as part of the "Secure Identity Status" details display. This field will typically only be present when the "Secure Identity Status" is "Unverified". The field will give an indication of why the Secure Identity Status of the device is Unverified.
- A new field "Details" has been added under the Platform tab of the Device Details pop-up window, as part of the "Boot Integrity Status" details display. This field will typically only be present when the "Boot Integrity

Status" is "Unverified". The field will give an indication of why the Boot Integrity Status of the device is Unverified.

- A new field "Platform Integrity Alert Message" has been added under the Platform tab of the Device Details pop-up window. This field is used to alert the customer of a possible security condition with the device's platform, but which is not necessarily an Indication of Compromise. The field will only be present when an alert has been identified for a particular device. As part of this new feature, a new icon has been created to indicate when a device has an Alert message identified by IV. The new icon is a purple open circle with a notch at the top, and will be displayed under the Platform column on the DEVICES tab of the IV UI for any device whose platform is in an Unverified condition by IV, and it also has an Alert message identified by IV. The User can hover the mouse over this icon, and a pop-up will be displayed with the Alert message identified for the device. Also, as part of this new feature, a new category is added to the existing "result summary circle" on the right side of the DEVICES tab of the IV UI. This new category, "Alerts", will indicate the number of devices that have an Alert message identified. The "result summary circle" itself will also indicate a segment of the circle in 'purple', which represents the devices that have an Alert message identified. The User can click on this segment of the circle to filter the display of Devices to only those Devices with an Alert message identified.

System Requirements

Hardware and Software Requirements

The Cisco IV application has the same system requirements as the Cisco APIC-EM controller. For more information, see the Cisco Application Policy Infrastructure Controller - Enterprise Module Data Sheet.

The Cisco IV App will use additional memory, disk storage and processing power to perform the following tasks:

- Collect Integrity data for the supported devices
- Analyze that integrity data
- Store the per device integrity data and analytic results

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.

Supported Platforms

The platforms supported by the IV application 1.5, along with the integrity measurement types supported by each platform, are identified in Table 1.

Table 1. Platform Support

Device	Integrity Measurement Type Support						
	Platform	Software				Hardware	Configuration
		Image	In-Memory	IMA	Shell Access		
Switches							
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
Industrial Ethernet Switches							
Cisco Industrial Ethernet 2000 Series Switches	N	Y[1]	Y	N	Y	Y	Y
Cisco Industrial Ethernet 3000 Series Switches	N	Y[1]	Y	N	Y	Y	Y
Cisco Industrial Ethernet 4000 Series Switches	N	Y[1]	Y	N	Y	Y	Y
Routers							
Cisco Integrated Service Router (ISR) 800 Series	N	Y	N	N	Y	Y	Y
Cisco Integrated Services Router (ISR) 2900 Series	N	Y	Y[2]	N	Y	Y	Y
Cisco Integrated Services Router (ISR) 3900 Series	N	Y	Y[2]	N	Y	Y	Y

Device	Integrity Measurement Type Support						
	Platform	Software				Hardware	Configuration
		Image	In-Memory	IMA	Shell Access		
Cisco Integrated Service Router (ISR) 4000 Series	Y[3]	Y	Y	N	Y	Y	Y
Cisco ASR 1000 Series Aggregation Services Router	Y[3]	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.

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

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 3.

Table 2. In-Memory check exceptions

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

Table 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[4] WS-C3850-24XS[4] WS-C3850-48XS[4] 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 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 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:
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

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

Limitations

The Cisco Integrity Verification Application 1.5.0.x is only compatible with the APIC-EM 1.5.0 Releases.

The Cisco IV application uses the APIC-EM controller's discovery service to discover network devices and the controller's inventory service to continuously poll these network devices. You can configure the polling interval using the controller's GUI. Refer to the Cisco APIC-EM documentation for information about the procedure to configure the polling interval.

Additional known functionality limitations contained in this release are described in the following table:

Limitation	Description
An outbound connection is required for the remote KGV File retrieval function (see first bullet in section "What's New in Release 1.5.0.265" on page 1)	In order to allow the customer to use the new remote KGV File retrieval function, an outbound connection to the internet and a DNS configuration that enables your APIC-EM controller to reach the following site is required: ➢ https://tools.cisco.com Refer to the following link for an example of how to test your controller internet connectivity (using the above url as part of the described procedure): ➢ https://help.ciscoactiveadvisor.com/solution/articles/13000030655-how-do-i-check-to-see-if-my-apic-em-controller-has-access-to-the-necessary-web-services-to-function-p The "Upload Local KGV File" option is also available on the KGV tab of the IV UI page.
Risk Level result summary circle – unable to select low percentage items Refer to the IV Application (Beta) User Guide – User Guide Figure 5 1. IV Application (Beta) – Devices Tab	A risk level slice representing an extremely low percentage of devices might be too narrow to display or to click on. To navigate to the display of those devices in the lower table, you can: • Increase the max devices display setting in the lower left corner of the table • Toggle the sort order of devices by clicking on the "Device Risk" column header
Risk Type result summary circle – unable to select low percentage items Refer to the IV Application (Beta) User Guide – User Guide Figure 5 1. IV Application (Beta) – Devices Tab	A risk type slice representing an extremely low percentage of device errors might be too narrow to display or to click on. To navigate to the display of those devices in the lower table, you can: • Increase the max devices display setting in the lower left corner of the table • Toggle the sort order of that particular risk type by clicking on the corresponding column header
Some versions of the Cisco Catalyst 3850 contain a defect, CSCve69298, in their Boot Integrity Visibility feature.	This defect results in a "Failed" integrity verification test result. See "**Note 4:** " above for more details.

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 at: http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/tsd-products-support-series-home.html

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.