

Release Notes

Compliance Insight Package
for IT Governance 4.01

ArcSight Logger™

November 15, 2012



Release Notes Compliance Insight Package for IT Governance 4.01

ArcSight Logger™

Copyright © 2012 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Follow this link to see a complete statement of copyrights and acknowledgements:

<http://www.hpenterprisesecurity.com/copyright>

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

This document is confidential.

Revision History

Date	Product Version	Description
11/15/2012	Logger CIP for IT Governance 4.01	The software installer component has been updated to enable installation on ArcSight Logger 5.3.

Contact Information

Phone	1-866-535-3285 (North America) +44 203-564-1189 (EMEA) +49 69380789455 (Germany)
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.arcsight.com

Contents

Logger CIP for IT Governance 4.01 5

 Release Contents 6

 Minimum Requirements 6

 Installing Logger CIP for IT Governance 6

 Open Issues in this Release 6

 Issues Fixed in this Release 7

 Alerts 7

 Reports 7

Logger CIP for IT Governance 4.01



Version 4.01 of ArcSight Logger Compliance Insight Package for IT Governance (Logger CIP for IT Governance) provides an updated software installer component, which enables you to install the package on ArcSight Logger 5.3 or later. For information about other supported versions of ArcSight Logger, see ["Minimum Requirements" on page 6](#).

Version 4.01 is for new installations. If you have an earlier, supported version of the package installed and are upgrading to Logger 5.3 or later, you do not need to upgrade to version 4.01.

Logger CIP for IT Governance is a package of reports and alerts designed to support compliance with the following IT Governance standards:

- ISO 27002:2005
- NIST 800-53

Logger CIP for IT Governance is a stand-alone package that is installed on ArcSight Logger. Logger CIP for IT Governance leverages ArcSight Logger's litigation-quality, long-term repository of log and event data to facilitate IT Governance compliance using ArcSight Logger's reporting and alerting capability.

These release notes contain the following sections:

- ["Release Contents" on page 6](#)
- ["Minimum Requirements" on page 6](#)
- ["Installing Logger CIP for IT Governance" on page 6](#)
- ["Open Issues in this Release" on page 6](#)
- ["Issues Fixed in this Release" on page 7](#)
- ["Alerts" on page 7](#)
- ["Reports" on page 7](#)

Release Contents

The files included in this release are:

File name	Description
Logger_ITGov_CIP_ReleaseNotes_4.01.pdf	Product description and open issues (this document).
Logger_ITGov_CIPGuide_4.0.pdf	Product architecture, installation, configuration, and operation instructions, and product contents description.
ArcSight-ComplianceInsightPackage-Logger-ITGov.4.01.1238.0.enc	Content package to install on ArcSight Logger appliances.
ArcSight-ComplianceInsightPackage-Logger-ITGov.4.01.1238.0.bin	Content package to install on the software version of Logger.

Minimum Requirements

Logger CIP for IT Governance 4.01 is supported on version 5.1 or later of both the Logger appliance and the software Logger. To determine your Logger version, click the **About** option in the upper-right corner of the Logger interface.

Logger CIP for IT Governance is self-contained and does not rely on any other ArcSight CIP packages or solutions.

Installing Logger CIP for IT Governance

For detailed information about installing Logger CIP for IT Governance, see the *ArcSight Solution Guide Compliance Insight Package IT Governance 4.0*.

Open Issues in this Release

This release contains the following open issues.

Number	Description
SOL-1453	<p>Logger CIP for SOX and Logger CIP for IT Governance share the following set of parameters:</p> <ul style="list-style-type: none">• internalNetwork• productionNetwork• thirdPartyNetwork• testingNetwork• wirelessNetwork• developmentNetwork <p>If both the Logger CIP for IT Governance and Logger CIP for SOX are installed on the same Logger, the original values for shared parameters of the first CIP installation are overwritten when the second CIP is installed. Any customizations to the original values are lost.</p> <p>Workaround: Record the customized values before installing the second CIP.</p>

Number	Description
SOL-1452	In the drill-down reports, do not drill down from charts. Instead, drill down from the fields in the tables. Drilling down from a chart might result in incorrect data.

Issues Fixed in this Release

The following issues are fixed in this release:

Number	Description
LOG-9797 SOL-3211	If the software Logger 5.1 or later was installed as root, and then a Compliance Insight Package was also installed as root, and no forwarder was configured, attempting to edit and save an alert from the installed package failed with the following message: <code>There was a problem saving your changes: FileNotFoundException - <install_dir>/current/arc sight/logger/user/logger/logger_ processor.properties (Permission denied)</code>
LOG-3464	ArcSight Logger did not strip the trailing spaces from events fields. For example, trailing spaces from usernames in the <code>sourceUserName</code> and <code>destinationUserName</code> fields were not stripped. This meant that user names without a space and a user name with a space were reported as two separate users. For example, <code>root<space></code> and <code>root</code> were reported separately. This could affect the outcome of drill-down reports.

Alerts

A maximum of five alerts can be enabled at one time. If five alerts are enabled on the Logger, you need to disable an alert before enabling another alert.

If you configure an email notification destination for an alert and the alert is triggered, it might take a few minutes after the email message is sent and received for the alert notification to be available for searching on the **Analyze | Alerts** page.

Reports

Logger reports render differently on different browsers. For best results, use the Microsoft Internet Explorer browser.

