



**Hewlett Packard**  
Enterprise

# **HPE ArcSight Security Release Notes**

Compliance Insight Package for Sarbanes-Oxley 4.0

ArcSight Logger

June 13, 2011

## Warranty

The only warranties for Hewlett Packard Enterprise 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. HPE shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

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

HPE Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

## Restricted Rights Legend

Confidential computer software. Valid license from HPE 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.

## Copyright Notice

© Copyright 2012 Hewlett Packard Enterprise Development LP

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

<https://www.protect724.hpe.com/docs/DOC-13026>

## Contact Information

---

<b>Phone</b>	A list of phone numbers for HPE ArcSight Technical Support is available on the HPE Enterprise Security contacts page: <a href="http://www.hpe.com/software/support/contact_list">www.hpe.com/software/support/contact_list</a>
<b>Support Web Site</b>	<a href="http://www.hpe.com/software/support">www.hpe.com/software/support</a>
<b>Protect 724 Community</b>	<a href="https://www.protect724.hpe.com">https://www.protect724.hpe.com</a>

---

# Contents

---

**Logger CIP for SOX v4.0 ..... 1**

    Release Contents ..... 1

    Installing Logger CIP for SOX ..... 2

    Open Issues in this Release ..... 2

---

# Logger CIP for SOX v4.0

---

ArcSight Logger™ is a storage solution optimized for extremely high event throughput. An event is a time-stamped log entry, either sent by protocols such as syslog, or appended to a log file. Logger receives and stores events, and can optionally forward selected events.

ArcSight Logger™ Compliance Insight Package for Sarbanes-Oxley (Logger CIP for SOX) is a package of coordinated reports that support Sarbanes-Oxley security monitoring requirements. Logger CIP for SOX is a stand-alone package that is installed on ArcSight Logger™.

- [“Release Contents” on page 1](#)
- [“Installing Logger CIP for SOX” on page 2](#)
- [“Open Issues in this Release” on page 2](#)

## Release Contents

The files included in this release are:

File name	Description
<a href="#">Logger_SOX_CIP_ReleaseNotes_v40.pdf</a>	Product description and open issues.
<a href="#">Logger_SOX_CIPGuide_v40.pdf</a>	Product architecture, installation, configuration, and operation instructions, and product contents description.
<a href="#">ArcSight-ComplianceInsightPackage-Logger-SOX.4.0.2132.cab</a>	Content package to install on ArcSight Logger appliances.
<a href="#">ArcSight-ComplianceInsightPackage-Logger-SOX.4.0.1112.bin</a>	Content package to install on the software version of Logger.

# Installing Logger CIP for SOX

Logger CIP for SOX v4.0 is supported on the following versions:

- **Software Logger**—For the software version of Logger running on your hardware, ArcSight Logger v5.0 Patch 2 (5.0.0.nnnn.2) or greater is supported, where [nnnn](#) is the four digit build number.
- **Logger Appliance**—For the version of Logger running on preconfigured hardware, ArcSight Logger v2.0 Patch 1 (2.0.0.2127) or greater is supported.



Logger CIP for SOX v4.0 is a new package that utilizes the new features of the ArcSight Logger v2.0 release. The Logger CIP for SOX v4.0 package and the ArcSight Logger CIP For Sarbanes-Oxley v1.0 package are completely independent and can coexist on the same ArcSight Logger. Logger CIP for SOX v4.0 is *not* an upgrade of ArcSight Logger CIP For Sarbanes-Oxley v1.0.

For detailed instructions on determining the installed version of Logger, see the *ArcSight™ Compliance Insight Package Guide-Sarbanes-Oxley v4.0* ([Logger\\_SOX\\_CIPGuide\\_v40.pdf](#)). In addition, the *ArcSight™ Compliance Insight Package Guide-Sarbanes-Oxley v4.0* contains complete installation and upgrade instructions.

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

## Open Issues in this Release

This release contains the following open issues.

Number	Description and work-around instructions
SOL-1191 TTP#47357	<p><b>Issue:</b> When running a report that generates a large result set, the report can take a long time to display the resulting data. For example, with a large result set, the following reports may take a long time to display:</p> <ul style="list-style-type: none"><li>• <i>ISO 6 - Attacks from Third-Party Systems</i></li><li>• <i>ISO 6 - Attacks on Third-Party Systems</i></li><li>• <i>ISO 4 - High Risk Events</i></li></ul> <p><b>Work-around:</b> To shorten the amount of time to display the report, try running the report with the <b>Multipage</b> option selected:</p> <ol style="list-style-type: none"><li>1 From the Logger navigation bar, select <b>Reports</b>.</li><li>2 From the left panel menu, select <b>Solution Reports/Sarbanes Oxley</b>.</li><li>3 For the desired report, select <b>Edit</b>. The Report Designer displays.</li><li>4 Select the <b>Multipage</b> option and click <b>Run</b>.</li></ol>

Number	Description and work-around instructions
SOL-1453 TTP#54425	<p><b>Issue:</b> Logger CIP for SOX and Logger CIP for IT Governance share the following set of parameters:</p> <ul style="list-style-type: none"> <li>• internalNetwork</li> <li>• productionNetwork</li> <li>• thirdPartyNetwork</li> <li>• testingNetwork</li> <li>• wirelessNetwork</li> <li>• developmentNetwork</li> </ul> <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><b>Work-around:</b> Record the customized values before installing the second CIP.</p>

