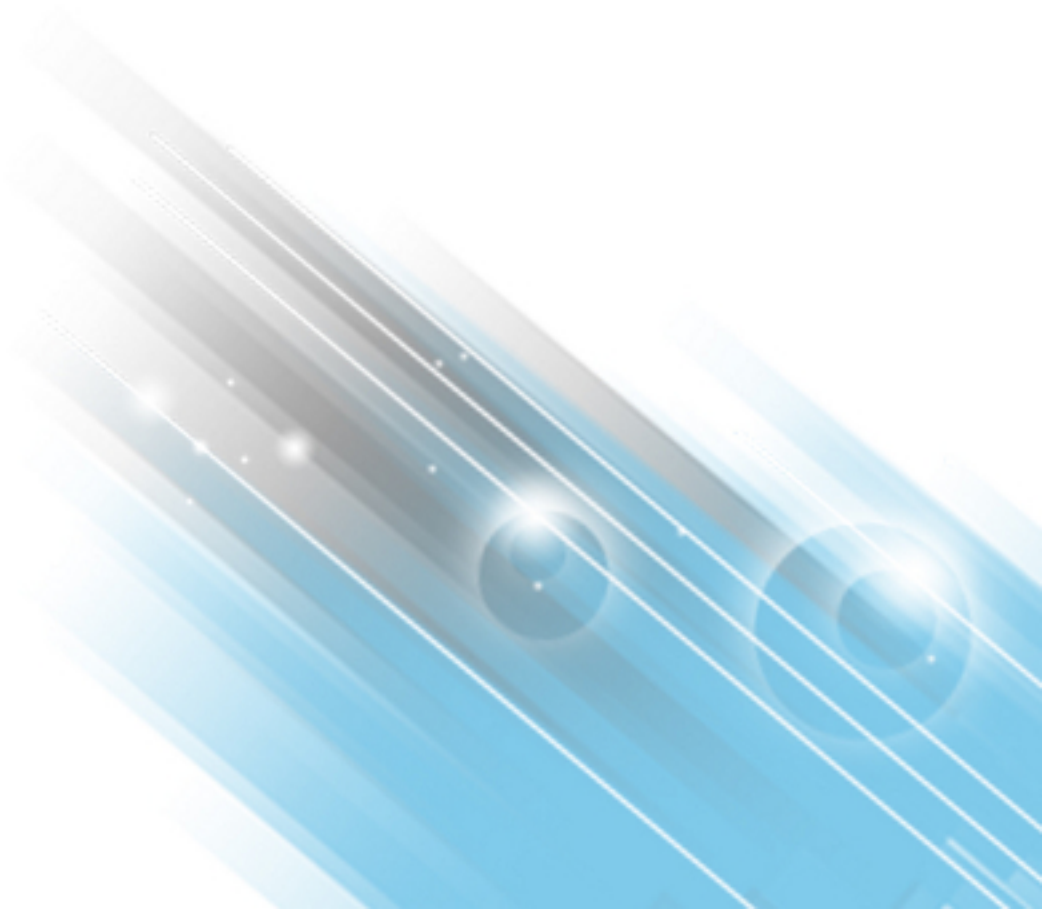
HP ArcSight User Behavior Analytics

Software Version: 1.1

Release Notes



August 31, 2015

Legal Notices

Warranty

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.

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.

HP 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 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.

Copyright Notice

Follow this link to see a complete statement of copyrights and acknowledgements:
http://www.hpenterprisesecurity.com/copyright

Support

Contact Information

Phone	A list of phone numbers is available on the HP ArcSight Technical Support Page: https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hp.com
Protect 724 Community	https://protect724.hp.com

Contents

HP User Behavior Analytics 1.1

These release notes cover the following topics:

Release Contents

The files in this release include:

File Name	Description
HPUBA1.1_Release_Notes.pdf	This document
HPUBA1.1_Integration_Guide.pdf	Integration and content guide
HPUBA1.1_Installation_Guide.pdf	Installation guide
HPUBA1.1_Administration_Guide.pdf	Administration guide
HPUBA1.1_User_Guide.pdf	User's guide
HP_UBA_Privileged_Account_Violations_1.0.arb	Content file. **There is no change to the Content package, so this arb file retains the version 1.0.**
HPUBA11_8_17_1.bin	Installation file

What's New

HP UBA 1.1 introduces the following capabilities to be licensed with HP UBA Premium:

- HP UBA Premium connects into IAM systems mine access entitlements and perform peer analytics and other application specific techniques to automatically identify and risk rank rogue and

high risk access on applications, servers, databases, and mainframe systems for certification and cleanup.

- HP UBA Premium automatically identifies Data Exfiltration risk using identity, behavior, and peer analysis associated with users and accounts that are demonstrating multiple indicators of exfiltration risk in advance, during, and after an attack, proactively monitoring data exfiltration risk coming from inside and outside the organization.
- Application Insight Packages introduce the following capabilities for the following enterprise applications (Cerner, EPIC, CyberArc, Lieberman, AWS, Google Apps, and Box). Application Insight Packages require a separate license and can only be used with concurrent license for HP UBA and HP UBA Premium.

Note: Upgrade and migration from version 1.0 to version 1.1 are not supported in this release.

Supported Platforms

The following platforms are supported for this release:

- RHEL 6.5
- CentOS 6.5

Supported ESM Version

The following version of ESM is supported for this release:

- ESM 6.8c

Open Issues in this Release

The open issues for this release are listed in the following table:

Number	Description and Workaround Instructions
AT-46	There is no pre-flight check in the installer to check for minimum recommended space for MySQL database installation. Workaround: Follow the steps in Change MySQL Data Directory in the HP User Behavior Analytics Installation Guide.
AT-109	Sometimes, the selected user information may not display when running an integration command from ESM for Source or Destination. Workaround: Use the Search box on the top right to display the selected user.
AT-134	User Risk Score is not sent to ESM.
AT-138	The uninstaller does not stop MySQL processes during uninstall. Workaround: Before running uninstall, manually stop all MySQL processes.
AT-148	CEFExport Connection to the system, where the syslog connector is installed, always fails with Connection Unsuccessful.
AT-155	During an Activity import, if the job fails due to Logfile missing. This is because the arcsight.properties file that is added to the datasource is missing. Workaround: Go to Configure > Jobs > Import > Activities > Select activity data source > Step 2 > More Settings > Set Use CEF Parser = Yes. Then Add CEF Properties File Name = arcsight.properties Click Save and Next.
AT-162	Unable to import Access Entitlement from 2 Active Directories at the same time. Workaround: Perform the import Access Entitlements one at a time.

Number	Description and Workaround Instructions
AT-189	Running Reports > Ad-hoc reports results in exception message on the user interface and in Securonix log. Workaround: This is a sample ad-hoc report that will not work by default. The user will have to make changes to the report before running it.
AT-194	Running any report using Reports > By Categories results in error messages. Workaround: An error is shown when running this report because of the space in the name of the report.
AT-195	Behavior Profile is not working with 'Selected Resource Types'. Workaround: Outlier techniques must be setup by data sources. Outlier techniques are not designed to be used at the resource type level.
AT-239	The only valid installation mode is through the GUI. The console and silent installation modes are not supported.
AT-245	If a job has just been scheduled, you can cancel it from the user interface. But if the job is in progress state, you cannot cancel the job from the user interface.
AT-247	Unable to import a user from an Active Directory; issue occurs only when using Chrome. Workaround: Clear the browser cache.
AT-254	After the machine is rebooted, syslog-ng should start automatically. Workaround: Start syslog-ng manually.
AT-257	Unable to save modification of policy condition from Import > Activities. Workaround: Navigate to Run > Policy Violations > By Datasource > <select datasource> to edit the policy condition.

Number	Description and Workaround Instructions
AT-273	When modifying user from Run > Behavior Profiles > Actions > Schedule Behavior Profile > Job, the Watchlist and Whitelist list no users, and then enabling Decrypted > selected users results in the error "Please select users". Workaround: Navigate to Manage > Users and edit users from that location rather than when scheduling a Behavior Profile.
AT-277	The integration command between HP ArcSight ESM and HP UBA was modified in HP UBA 1.1 to reduce the privileges associated with the user of the ESM integration command within HP UBA. The default privileges are to enable the ‘siemrole’ to only view the destination and/or source user profile. The default privileges do not enable the user to view the HP UBA Security Dashboard. Workaround: To enable the ‘siemrole’ user to view the HP UBA Dashboard, the user must change the access settings for ‘siemrole’ within HP UBA and the user must use the ESM integration command initially with the destination user or source user integration command.
VEN-72	When drilling down on a field with the 'null' value in the dashboard with a chart view, the drilldown results are empty. Workaround: Switch the dashboard to the table view and run the drilldown after that, that will display the correct data.

Fixed Issues in this Release

The fixed issues for this release are listed in the following table:

Number	Description and Workaround Instructions
AT-6	The HP UBA software should be installed by a non-root user, however the installer does not provide a warning. This issue has been fixed.

Legal Notice

vLGPLv3, LGPLv2, EPL 1.0, CCDL

This product includes code licensed under the LGPLv3 licensed-code, LGPLv2 licensed-code, Eclipse Public License 1.0, CCDL-licensed code, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett-Packard Company.

To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett-Packard Company

Attn: HP Enterprise Security Products ArcSight R&D

1160 Enterprise Way

Sunnyvale, CA 94089

USA

Please specify the product and version for which you are requesting source code.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Release Notes (User Behavior Analytics 1.1)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arc-doc@hp.com.

We appreciate your feedback!