Hewlett Packard
Enterprise

HPE Security ArcSight User Behavior Analytics

Software Version: 1.1.2

Release Notes

May 20, 2016

Legal Notices

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. Hewlett Packard Enterprise 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 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 Hewlett Packard Enterprise 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

Legal Notice for Open Source Code

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, on CD send a check or money order in the amount of US $10.00 (for shipping and handling) to:

Hewlett-Packard Enterprise Company

Attn: Marina

1160 Enterprise Way

Sunnyvale, CA 94089

USA

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

Support

Contact Information

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

Contents

HPE ArcSight User Behavior Analytics

This Release Notes covers the following topics:

Release Contents

The files in this release include:

File Name	Description
HPEUBA_Release_Notes_1.1.2.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
HPUBA1.1_ApplicationInsightPacks_Guide.pdf	Application Insight Packs Guide
HP_UBA_Privileged_Account_Violations_1.0.arb	Content file. **Note**: There is no change to the Content package, so this arb file retains the version 1.0.
HPUBA1.1.2.bin	Installation file
HPUBA1.1_to_1.1.2_upgrade_20160519.zip	Upgrade script from HP UBA 1.1 to HPE UBA 1.1.2
HPUBA1.1.1_to_1.1.2_upgrade_20160519.zip	Upgrade script from HP UBA 1.1.1 to HPE UBA 1.1.2

What's New

The HPE UBA 1.1.2 focuses on the security fixes using Java version 1.7_101.

Note: Due to security updates and changes to access control in HPE UBA 1.1.2, the default ROLE_siemrole may have less privilege than it had in previous versions of the applications. In order to change or configure access control for ROLE_siemrole, please go to Configure->Access Control and make changes accordingly. Please refer to pages 142 through 148 in the HPUBA1.1_Administration_Guide.pdf for more details regarding Access Control configuration.

Supported Platforms

The following platforms are supported for this release:

- RHEL 6.7
- CentOS 6.7

Supported ESM Version

The following version of ESM is supported for this release:

- ESM 6.8c

Installing the HPE UBA 1.1.2 Product

Use the HPUBA1.1.2.bin to install the HPE UBA 1.1.2 product. Please refer to the HPUBA1.1_Installation_Guide.pdf.

In order to establish a secure installation, enable MySQL connections as follows in the next section.

Enabling MySQL

To protect your system make sure you set up the password as follows:

Note: Replace terms with those specific to your configuration:

Grants a password to login to mysql server locally.

- grant all on *.* to 'root'@'localhost' identified by 'password';

  AND either
- grant all on *.* to 'root'@'192.168.1.1' identified by 'password';

  OR
- grant all on *.* to 'root'@'myhostname' identified by 'password';

Grants a password to login to mysql server remotely.

After performing the grant statements above, run "flush privileges;".

Upgrading the HPE UBA 1.1.2 Product

The following process describes how to upgrade from HP UBA 1.1 and HP UBA 1.1.1, to HPE UBA 1.1.2:

- Upgrading from HP UBA 1.1 to HPE UBA 1.1.2
- Upgrading from HP UBA 1.1.1 to HPE UBA 1.1.2

Note: The non-root user who has installed the HP UBA needs to perform the upgrade steps.

Upgrading from HP UBA 1.1 to HPE UBA 1.1.2

Perform the following steps to upgrade from HP UBA 1.1 to HPE UBA1.1.2 :

1. Stop the HP UBA application from the command line, by running:

   ```
   ./securonix.sh stop
   ```
2. Make sure there are no instances of tomcat running using [ps -ef | grep tomcat] command. If there is any instance still running we need to kill it using its pid.
3. Download the HPUBA1.1_to_1.1.2_upgrade_20160519.zip file and then unzip it.
4. Go to the HPUBA1.1_to_1.1.2_upgrade_20160519 folder and execute:

   ```
   ./upgrade.sh
   ```
5. Provide your HP UBA1.1 installation path.
6. Provide your mysql username, password, socket path and database name in that order when prompted.
7. Once the upgrade is complete, start the HP UBA application from a command line, by running:

   ```
   ./securonix.sh start
   ```
8. Launch the application on browser, for example:

   https://localhost:8443/Profiler where 8443 is the port number that you initially specify while installing the application . Port number 8080 or 8443 can be used. If the launch is successful the Version 1.1.2 is displayed at the bottom of the screen.

Upgrading from HP UBA 1.1.1 to HPE UBA 1.1.2

Perform the following steps to upgrade from HP UBA 1.1.1 to HPE UBA1.1.2 :

1. Stop the HP UBA application from the command line, by running:

   ```
   ./securonix.sh stop
   ```

2. Make sure there are no instances of tomcat running using [ps -ef | grep tomcat] command. If there is any instance still running we need to kill it using its pid.
3. Download the HPUBA1.1.1_to_1.1.2_upgrade_20160519.zip file and then unzip it.
4. Go to the HPUBA1.1.1_to_1.1.2_upgrade_20160519 folder and execute:

   ```
   ./upgrade.sh
   ```
5. Provide your HP UBA1.1 installation path.
6. Provide your mysql username, password, socket path and database name in that order when prompted.
7. Once the upgrade is complete, start the HP UBA application from a command line, by running:

   ```
   ./securonix.sh start
   ```
8. Launch the application on browser, for example:

   https://localhost:8443/Profiler where 8443 is the port number that you initially specify while installing the application . Port number 8080 or 8443 can be used. If the launch is successful the Version 1.1.2 is displayed at the bottom of the screen.

Usage Notes

Login to HPE UBA Through the Integration Command

If the user is unable to login to HPE UBA through the Integration Command, then clearing the browser cache will enable login to HPE UBA.

Open Ports Not Listed in the Installation Guide

- Open port 8009 for use with AJP connectors where Tomcat clusters are being run behind an Apache web server.
- Block port 111 as the manager folder of Tomcat uses this port, and since the manger folder is removed from tomcat the port is not used by the HPE UBA application.

Editing the URL of the Integration Command for HPE UBA Without Using the SSL Protocol

The URL link of the Integration Command is set for SSL using https and port 8443 as default. Therefore, in order to use for UBA without SSL, update the URL to use http and port 8080 instead.

Perform the following steps:

1. Go to ESM console > Resources > Integration Commands > /All Integration Commands/ArcSight Solutions/HP User Behavior Analytics > HP UBA Dashboard.
2. Click the button at the end of URL link to edit URL by replacing https and 8443 with http and the port that was set during HP UBA installation.
3. Click Apply.

Perform the same steps for HP UBA User Information - Destination and HP UBA User Information - Source.

Unable to Login to the Browser

If a siemuser does not logout from the browser while using the Integration Command then the user may not be able to login again. An error "You are not authorized to view this page" is displayed. To resolve this issue the siemuser needs to logout first and then login again.

Fresh Install of HPE UBA1.1.2 on an Existing HPE UBA 1.1.2 Build

Although the system currently allows users to install a new HPE UBA1.1.2 build along with an existing HPE UBA 1.1.2 build using the same database, this is not recommended and should not be done.

HP UBA 1.1 and HPE UBA 1.1.2 on the Same Machine

Although the system allows users to have both HP UBA 1.1 and HPE UBA 1.1.2 installed on the same machine, this is not recommended and should not be done.

Use of Context Menus on the Investigation Workbench

When using the Investigation Workbench, it is recommended to use the context sensitive menus on the nodes for navigation instead of the drag and drop objects available in the left panel specially when navigating to the second and third level objects. Using the drag and drop objects from the left panel may lead to “Internal Server Error” messages when viewing activities from the lower level nodes.

.

Open Issues in this Release

Note: Please refer to the existing open issues from the HP UBA 1.1.1 Release Notes.

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

Number	Description and Workaround Instructions
AT-391	Administrative Dashboard > Schedule Job Calendar shows incorrect dates for different job activities as in, a day after the actual date.
AT-405	Security Dashboard -> Threats - Unable to export "Rule Base Violations" table on IE. Workaround: Use either Firefox or Chrome.
AT-407	Administrative Dashboard - Activity Import History shows only the first job. Workaround: Review the data in the table for more details as the graph is having issues.
AT-408	User Import History shows the wrong time in the graph.
AT-414	Unable to export High Risk Users report on the Security Dashboard as the user gets an error message "Error processing request. Please contact Administrator" Workaround: Restarting the application will enable the report to be exported.
AT-417	Third Party Intelligence: The import of Threat Intelligence data for Spyeye Tracker is not currently working.
AT-418	Import Watch List Data: The validation is missing for mandatory mapping of an entity name.
AT-419	User Import History graph is not displayed when the custom date range is selected.
AT-420 and AT-424	When using the Advance Search, if the user either hits the Enter key or if both the condition fields are empty, then an error message is displayed on the UI, "Error processing request".

Number	Description and Workaround Instructions
AT-423	The Run Policy from the View Policies Violated on the Investigation Workbench is not functioning.

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 (HPE Security ArcSight User Behavior Analytics 1.1.2)

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@hpe.com.

We appreciate your feedback!