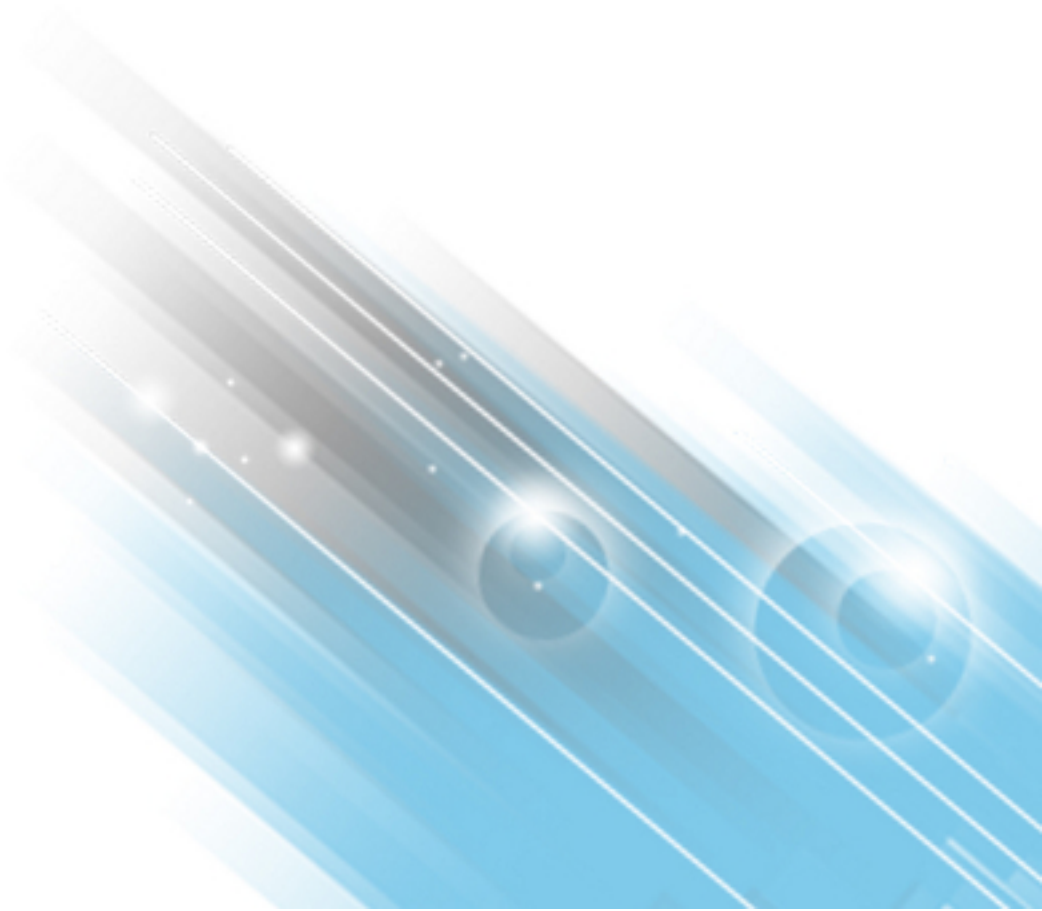
HP ArcSight User Behavior Analytics

Software Version: 1.1.1

Release Notes



April 13, 2016

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

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, send a check or money order in the amount of US $10.00 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 HPArcSight 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

Contents

HP ArcSight User Behavior Analytics 1.1.1

This Release Notes covers the following topics:

Release Contents

The files in this release include:

File Name	Description
HPUBA_Release_Notes_1.1.1.pdf	This document
HPUBA111.zip	Upgrade file

What's New

HP UBA 1.1.1 introduces the following capabilities to be licensed with HP UBA Premium:

HP UBA 1.1.1 is a patch to the HP UBA 1.1 release. HP UBA 1.1.1 introduces Threat Management, improves Case Management, and addresses bugs found in previous releases of the product.

Threat Management offers a new way to look at high-risk users and policy violations, and review potential threats. Analysts can use multiple ways to filter the views in the high-risk user dashboard (for example: users that have violated policies or have been marked as confirmed violators) and take actions on potential violations such as “Confirmed Violation”, “Potential Violation”, “Exception”, “Approved Activity”, and so on.

New Features and Enhancements

The new features and enhancements for this release are listed in the following table:

Key	Summary
SASS-2695	Provide capability to manage Threats and Violations by marking as Concern, Not a concern, Possible Threat, Still Investigating.
SASS-2265	Eliminate zero risk user from high risk dashboard.
SASS-2106	Export Utility for violations from the view violations screen.
SASS-2393	Assign case to specific analyst.
SASS-2638	Ability to search based on child case number.
SASS-2642	Sticky feature - When client filters out cases by a specific group - after taking action on a specific case and when he returns to the incident screen - the filter should be enabled.
SASS-2546	Enhancement for Securonix user auditing.
SASS-2565	Never Lock Admin Account.

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

Upgrading from HP UBA 1.1 to HP UBA 1.1.1

The following process describes how to upgrade from HP UBA 1.1 to HP UBA 1.1.1, and, if necessary how to revert to HP UBA 1.1:

Note: The non-root user who has installed/backed up the HP UBA files needs to revert this changes.

Back up

Perform the following steps to backup the HP UBA 1.1:

1. Stop the HP UBA application from a 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 , kill it using its pid.

3. Back up hpuba11 database:

   ```
   mysqldump -uroot -p --socket=/path/to/mysql.sock hpuba11 > /tmp/hpuba11.sql
   ```

4. Back up the `securonix_home` folder and `/Tomcat/webapps/Profiler.war file`.

Upgrade

Before upgrading, back up the HP UBA 1.1 database and files.

1. Stop the HP UBA application from a 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 `HPUBA111.zip` file and then unzip it.

4. Go to the HPUBA111 folder located in your system through command line and execute

   ```
   ./upgrade.sh
   ```

5. Provide your HP UBA11 installation path, mysql username, password, socket path and database name in that order when prompted.

6. Once the upgrade is complete, start the HP UBA application from a command line, by running:

   ```
   ./securonix.sh start
   ```

7. 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 1.1.1 is displayed at the bottom of the screen.

Revert to HP UBA 1.1

Perform the following steps to revert to HP UBA 1.1:

1. Stop the HP UBA application from a 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. Connect to mysql server and then drop schema database:

   ```
   drop schema hpuba11;
   ```

4. Create schema database:

   ```
   create schema hpuba11;
   ```

5. Put back the hpuba11 to database:

   ```
   mysql -uroot -p --socket=/path/to/mysql.sock hpuba11 < /tmp/hpuba11.sql
   ```

6. Put back `/securonix_home` folder `and /Tomcat/webapps/Profiler.war`

7. Remove `/Tomcat/webapps/Profiler` folder

8. Start the HP UBA application from a command line, by running:

   ```
   ./securonix.sh start
   ```

Open Issues in this Release

Note: Please refer to the existing Open issues from HP UBA 1.1 Release Notes.

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

Number	Description and Workaround Instructions
AT-328	Detected date is not sorted when reports of High-Risk users are exported.
AT-317	On Securonix Dashboar > High-Risk users, when the policy violations of an user is expanded, the Search filter automatically sets to the user that was expanded. Workaround: Clear the filter and all the users are visible again.
AT-305	In the Securonix Dashboard there is an inconsistency between the View by Filter and the Add Filter. Workaround: The result displayed on the dashboard is from the View by Filer and not from the Add Filter.

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 1.1.1)

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@hpe.com.

We appreciate your feedback!