Hewlett Packard
Enterprise

HPE Security ArcSight User Behavior Analytics

Software Version: 5.0

Release Notes

July 21, 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 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 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:
https://www.protect724.hpe.com/docs/DOC-13026

Support

Contact Information

Phone	A list of phone numbers is available on the HPE Security ArcSight 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

HPE Security ArcSight User Behavior Analytics

Release Contents

The files in this release include:

File Name	Description
HPEArcSightUBA5.0_Release_Notes.pdf	This document
HPEArcSightUBA5.0_Integration_Guide.pdf	Integration and content guide
HPEArcSightUBA5.0_Installation_Guide.pdf	Installation guide
HPEArcSightUBA5.0_Administration_Guide.pdf	Administration guide
HPEArcSightUBA5.0_User_Guide.pdf	User's guide
HPEArcSightUBA5.0_Application_Insight_Packs_Guide.pdf	Application Insight Packs Guide
HPEArcSightUBA5.0_Threat_Library.pdf	Out-of-box HPE ArcSight UBA policies by data source.
HPE_ArcSight_User_Behavior_Analytics_1.1.arb	Content file, which is published on the Marketplace.
HPEArcSightUBA50_20160713.bin	Installation file

What's New

Revamped User Experience

The HPE Security ArcSight User Behavior Analytics (HPE ArcSight UBA) user interface has been redesigned and rebuilt from the ground-up using the latest technologies to provide a unified look and feel and consistent user experience across the application:

- Standardization of all user interface elements and look and feel
- Automatic user interface resizing to different screen sizes
- Cross-browser compatibility with minimum developer interference
- New top-level menu to access the most common tasks in the application
- Reduction in number of clicks the user has to go through during investigation

Security Dashboards

The security dashboards have been redesigned and enhanced with the following:

- **High-Risk Entity Dashboard:** The dashboards now show four high-risk entity types that can be used to start the investigation:
  - *Users:* users behind the activity, such as employees and contractors
  - *Uncorrelated Activity Accounts:* accounts that are not tied directly to a user, such as system accounts.
  - *Resources:* systems, devices, applications behind activities
  - *Network Addresses:* IP addresses behind activities
- **High-Risk Entity Filtering:** New filtering capabilities allow analysts to filter the list of high-risk entities by threat, policy violations, peer groups, actions taken, and top percentiles.
- **Violation Timeline View:** All violations are shown in a timeline view, with the most recent violations first. By default, the analyst will only see the newest violations (today) and can use the expand/collapse button for more details.
- **Multi-Tab Investigation:** During an investigation, the analyst can investigate a high-risk entity and open multiple violation details at the same time with the new multi-tab view.
- **Time Ranges:** When selecting a time range in a dashboard, the same time range will be applied when opening a different dashboard.

Endpoint Analytics

Major improvements and new features have been added to identify the riskiest entities in the organization, with a specific focus on Endpoint Analytics:

- Identify and investigate high-risk endpoints in the new High-Risk Entity Dashboard
- Create peer groups based on hosts and network addresses to find behavior-based anomalies between systems
- Visualize endpoints with relevant data, risk scores, and threat indicators, on a new Geolocation Map
- Over 100 behavior-based detection techniques across all entities

Advanced Analytics

New advanced analytics functions have been added for the most sophisticated use cases-to-date:

- Chained analytics with ability to create behavior profiles on top of HPE ArcSight UBA violation data
- New post-processing functions to check data against watch lists, lookup tables, threat intelligence, and geolocation

- Risk influencers to increase or decrease risk scores for entities in watch lists, when other peers are not violators, or based on any conditions on available attributes

Multi-Entity Investigation Workbench

The Investigation Workbench tool has been revamped with a highly scalable technology framework allowing analysts to:

- Investigate multiple high-risk entities at the same time
- Find commonalities and differences between entities over time
- Use workspaces to investigate multiple users, accounts, and network addresses on the same screen
- Perform data link analysis between objects with N-level drilldowns

Out-of-Box Content

HPE ArcSight UBA comes with a set of pre-defined content with over 500 behavior checks and threat indicators across 40 of the most common data sources used in HPE ArcSight UBA environments. These threat indicators are used by the threat modeling framework to identify the riskiest users and endpoints in the customer's environment.

HPE ArcSight UBA also introduces the ability to import and export content (policies, behaviors, reports, etc.) from one HPE ArcSight UBA instance to another.

Operational Dashboard

The Administrative Dashboard has been updated to provide an operational overview of the HPE ArcSight UBA application health, including a summary overview, the status of all data import and analytics jobs (created/completed/failed), and history of all policy violations.

Software Component Updates

This is the list of the main software components updated for HPE ArcSight UBA5.0:

- Apache Tomcat 8 .0.30
- Oracle Java JRE 1.8.0_92

ROLE_siemrole Privileges

Due to security updates and changes to access control in HPE ArcSight UBA, 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, go to Configure >Access Control and make changes

accordingly. Refer the HPEArcSightUBA5.0_Administration_Guide.pdf for details regarding Access Control configuration.

Supported Platforms and Versions

Supported Platforms

The following platforms are supported for this release:

- RHEL 6.7
- CentOS 6.7

Supported ESM Version

The version of ESM supported for this release is ESM 6.9.1c.

Supported MySQL Version

The version of MySQL supported for this release is MySQL 5.6.30.

Downloading and Installing HPE ArcSight UBA Content Package

To download the HPE ArcSight UBA content package from the Marketplace to the machine on which you run the ArcSight Console:

1. Log into the Marketplace (https://saas.hpe.com/marketplace/arcsight).
2. Navigate to **User Behavior Analytics** to find the HPE ArcSight UBApackage, `HPE_ArcSight_User_Behavior_Analytics_1.1.arb` and download.

See the HPEArcSightUBA5.0_Integration_Guide.pdf for details on installing the HPE ArcSight UBA content package.

Usage Notes

Start syslog-ng Manually

After reboot, be sure to restart `syslog-ng` manually. It will not restart automatically.

Log into HPE ArcSight UBA Through the Integration Command

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

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.

Syslog Active Channel Not Loading in ArcSight Command Center

If Syslog active channel is not loading in the ArcSight Command Center, then delete the Syslog active channel from ESM console and create new Syslog active channel. After this you would see Syslog active channel loading in the ArcSight Command Center with events.

Open Issues in this Release

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

Number	Description and Workaround Instructions
AT-489	In the Policy Violation Trends of the Administrative Dashboards, some of the policy counts are not accurate and not showing properly on the graphs.
AT-488	In the ACCOUNT MISUSE dashboard, the user is not able to edit an entity to create a case (pencil icon missing). Workaround: Use the Security Dashboard > Entities to perform that action.

Number	Description and Workaround Instructions
AT-481	In some cases, after selecting different time range selections in the High Risk Entities dashboard, the section for to export, edit, collapse and search is missing. Workaround: Re-load the page.
AT-476	Not able to add multiple conditions as part of the Advanced Search of the Investigation Workbench feature. Workaround: Limit the Advanced Search to one condition.
AT-475	Not able to create a lookup table with a dash (-) in the name. Workaround: Create a lookup table without a dash (-) in the name.
AT-474	When using the MaxMind geolocation connection, from time to time the user might see a connection timed out error. Workaround: Make sure you have access to the internet and try again.
AT-470	On the Threats dashboard, the total number of results might be different from other counts seen on the page.
AT-469	Not able to re-run a real-time policy job the first time of the day. Workaround: Restart the application and re-run the job.
AT-466	When enabling and disabling password control settings multiple times, the password control settings are not being enforced. Workaround: Enable password control once only when the deployment is ready for use.
AT-457	Console mode uninstallation does not ask to uninstall syslog-ng. Workaround: Leave syslog-ng as-is or manually uninstall syslog-ng.
AT-443	Hibernate Exception when running a peer-based outlier job using the resourceType field in the outlier analysis. Workaround: Do not schedule or run a job with resourceType field in outlier analysis.
AT-424	When using the Advanced Search, if the user presses Enter or if both the condition fields are empty, then the error message "Error processing request" displays.
AT-418	The validation is missing for mandatory mapping of an entity name for imported Watch List data.
AT-414	Unable to export High Risk Users report on the Security Dashboard and get the error message "Error processing request. Please contact Administrator". Workaround: Restart the application to enable report export.

Number	Description and Workaround Instructions
AT-362	Sometimes, when the user tries to edit the Privileged Activities by a Non Privileged User policy, the page becomes unresponsive. Workaround: Try again after some time, or in a different browser.
AT-328	Detected date is not sorted when reports of High-Risk users are exported.
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-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-191	During behavior profile creation, select at least one attribute in the Configuration step.
AT-134	User Risk Score is not sent to ESM.
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.
SASS-5025	In the High Risk Entities dashboard, clicking on a watchlisted entity opens a blank page. Workaround: View watchlisted users from Views > Watch List.
SASS-4958	Sometimes the archival job status will show Green even if the job has failed. Workaround: Check the job details message to make sure the archival job ran properly.
SASS-4951	In some cases, the total number of uncorrelated accounts in the High Risk Entities dashboard is not accurate.
SASS-4900	In the 'Behavior Policy' screen under the Policy View dashboard, the details of the behavior based policies are not available. Workaround: Use another dashboard such as the Security Dashboard > Entities to see the details of policy violations.
SASS-4741	There are duplicate entries in the Threat Indicator list when defining a policy. Workaround : Select one of the two threat indicators, this will not cause an issue.
SASS-2471	No installation log generated when installer is running in Console mode.
SASS-2456	Uninstaller in Console mode does not uninstall the database. Workaround: Remove the database manually post uninstallation ; refer to the HPEArcSightUBA5.0_Installation_Guide.pdf for details.

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 5.0)

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!