Hewlett Packard Enterprise

# HPE Security ArcSight User Behavior Analytics

Software Version: 5.0c Patch 2

## Release Notes

June 16, 2017

*Powered by* SECURONIX

# 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

## 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 Enterprise 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 the source code.

## 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 |

**Contact Information, continued**

| | |
|---|---|
| **Support Web Site** | https://softwaresupport.hpe.com |
| **Protect 724 Community** | https://www.protect724.hpe.com |

# Contents

# What is HPE UBA 5.0c Patch 2?

HPE UBA 5.0c Patch 2 is the latest cumulative set of fixes for the HPE ArcSight UBA release. HPE UBA 5.0c Patch 2 packages additional product fixes to HPE ArcSight UBA customers into a single bundle that can be easily applied on an existing installation of HPE ArcSight UBA.

A significant number of HPE UBA 5.0c Patch 2 fixes are under the following areas of the product:

- Security Dashboard
- Case Management and Workflow
- Violation Data
- Encryption and Masking
- Threat Modeler

### Important Updates

- If you are using threat models in your environment, *please read carefully* and go through all the steps described in the **Prerequisites** section of How to Apply HPE UBA 5.0c Patch 2.

For the full list of fixes available in HPE UBA 5.0c Patch 2, please refer to Issues Addressed in HPE UBA 5.0c Patch 2.

# How to Apply HPE UBA 5.0c Patch 2

**Important**: Prior to applying HPE UBA 5.0c Patch 2, you must first upgrade to version 5.0c Patch 1 if you are using a different version.

**Note**: If the application is running in a Master/Child environment, follow the steps below for every node.

## Prerequisites

**Note**: User performing the installation must have read/write/execute permissions on the HPE ArcSight UBA installation folder.

If you are using threat models in your HPE ArcSight UBA application, follow Steps 1 through 5 below to apply this Cumulative Update. If you do not feel comfortable with these steps, contact HPE ArcSight UBA support for help.

**Note**: Take database backup of all master and child nodes connected to the master node before the upgrade.

### Step 1: Disable Threat Models

From the HPE ArcSight UBA user interface, complete the following steps:

1. Navigate to Analytics > Threat Modeler.
2. Disable all threat models by setting **Online** toggle to **No** for all threat models.

### Step 2: Stop the Application

Stop the HPE ArcSight UBA application from your installation folder: `./securonix.sh stop`.

### Step 3: Clean Up Threat Models

1. Connect to your HPE ArcSight UBA master node database.
2. Run the following query: `select * from risk_scorecard where modelid != -1;`
   - If the query returns 0 rows, proceed to *Step 4: Proceed with Patch*.
   - If the query returns 1 or more rows, you have entries in risk_scorecard for modelid = 0. Complete the following steps to correct this:
     1. Delete any entries for modelid -2 or modelid > 0 by running this query: `delete from risk_scorecard where modelid = -2 or modelid > 0;`
     2. Run this query: `select * from risk_scorecard where typeid in (select id from risk_type where source like 'PolicyCategory%' and modelid ! =-1;`

        **Note**: If the above query returns any results, delete those entries.

3. If you still have entries in risk_scorecard for modelid = 0 after the above steps, reset modelids to -1 for these policy entries by running this query: `update risk_scorecard set modelid = -1 where modelid = 0;`
4. If the above is giving a duplicate entry error (for example, `Error Code: 1062. Duplicate entry '8-1036-Users-1--1' for key 'PRIMARY'`), delete the duplicate records. For each of the duplicate entry error:
   - Identify the entityid, typeid, entity, riskthreatid, and modelid from the error (for example, `'8-1036-Users-1--1' –> 'entityid-typeid-entity-riskthreaid-modelid'`)
   - Run the following query (substitute the values from the example with the ones you found): `delete from risk_scorecard where entity='Users' and entityid = 8 and typeid = 1036 and riskthreatid = 1 and modelid = -1;`
5. Run the query from Step 3 again and delete the duplicate records as described in Step 4 until the query does not return any error.

### Step 4: Proceed with Patch

Upgrade the HPE ArcSight UBA application to HPE UBA 5.0c Patch 2 by proceeding to *Download and Unzip the Patch*.

### Step 5: Enable Threat Models

When the upgrade is completed successfully, log in to your HPE ArcSight UBA application to complete the following steps:

1. Navigate to Analytics > Threat Modeler.
2. Enable the threat models you would like to use.

## Download and Unzip the Patch

1. Download the Patch from the HPE support portal.
2. Open a new terminal and navigate to your HPE ArcSight UBA installation folder (you should see a 'Tomcat' and 'securonix_home' within that folder).
3. Copy the zip file to your HPE ArcSight UBA installation folder and unzip the file: unzip **HPEArcSightUBA50cP2_20170427.zip**.

## Apply the Patch

To apply this instance for every HPE ArcSight UBA instance (unless specified for master or child node).

1. Take a backup of the master node and all child nodes connected to the master before applying the Patch.
2. Stop your HPE ArcSight UBA application (if running) from your HPE ArcSight UBA installation folder: `bin/securonix.sh stop`
3. Navigate to the **HPEArcSightUBA50cP2_20170427** folder.
4. Update the database by running the following script: `./apply_sql_updates.sh`

   **Note**: If this step results in any MySQL errors, contact your DB admin or run the `HPEArcSightUBA50cP2_20170427.sql` manually.
5. Apply the Patch by running the following script: `./apply_application_updates.sh`.
6. Navigate back to HPE ArcSight UBA installation folder.
7. Start your HPE ArcSight UBA application: `bin/securonix.sh start.`
8. Navigate to your web browser and clear the browser's cache.
9. Log in to the HPE ArcSight UBA application.

   **Note**: The backup of the existing Profiler and securonix_home files will be present in **/HPEArcSightUBA50cP2_20170427_logs** location.

## Revert the Patch

**Note**: This procedure is not recommended. Please contact support if help is required.

**Note**: Perform the steps to revert the Patch on all the master and child nodes, unless specified otherwise.

**Note**: Take database backups of all master and child nodes for the steps to work as expected.

1. Open a terminal and unzip the Profiler backup zip file that was created when you applied the Patch (located within the **HPEArcSightUBA50cP1_20170427_logs** folder) in a temporary location: unzip **HPEArcSightUBA50cP1_Profiler_backup_<timestamp>.zip**.
2. Navigate to the HPE ArcSight UBA installation folder and stop the HPE ArcSight UBA application: `bin/securonix.sh stop`.
3. Copy all the **HPEArcSightUBA50cP1** backup files, unzipped in step 1, in the **Tomcat/webapps/Profiler/** and **securonix_home** folders.
4. Revert the database to the HPEArcSightUBA50cP1 database by using your database backup.
5. Start the HPE ArcSight UBA application: `bin/securonix.sh start`
6. Go to your web browser and clean its cache.
7. Log in to the HPE ArcSight UBA application.

# Additional Settings

## Ticket #202526: Cases not showing up in threat model

In the Category view, the case count in a threat model will be shown only at entity level, but not at policy level.

## Ticket #202140: Enhancement – Need Case Assigned Date in Report Generated Under Incident Dashboard Screen

To enable this enhancement, add the following SQLs:

```
INSERT INTO `configxml` (`xmlkey`, `xmlvalue`) VALUES ('LAST_
ASSIGNED_CASE_QUERY', 'select MAX(jch.lastupdate) from Jbp-
mCustomHistory jch where jch.caseid = jbpm.caseId and jch.action
like \'%CLAIM%\'');
```

**Note**: If the above query is already present and the results are not as per expectations, please modify the Hibernate query accordingly based on the different workflows you might have.

## Miscellaneous

### Category View

When you navigate to the Category view with threat models enabled, only the entities will be shown when the page first loads. The details of the threat models and policies will be loaded as you click on each entity.

### Threat Models

When using threat models, follow these guidelines:

- Threat model names and policy names must be unique across the application: Threat models and policies used by threat models with the same name are not supported.
- A policy used in a threat model can only be part of one category: Policies with multiple categories are not supported for threat models.
- A threat indicator (and associated policy) used in a threat model can only be part of one category: Threat indicators that are mapped to policies used by multiple categories are not supported for threat models.
- Threat Models using Weight Multiplier as Weight Type: If you are using one or more zero-risk score policies in a threat model, add those policies as the last rule(s) in the threat model. If you don't (e.g., the first rule is a zero-risk policy), the weight multiplier will not be applied.

# Issues Addressed in HPE UBA 5.0c Patch 2

## Customer Issues

| Component/s | Customer Ticket Number | Summary |
|---|---|---|
| Behavior Based Anomaly Detection | 201772 | CEF MAPPING is not getting saved |
| Case Management | 202524 | Case count is incorrect at user level |
| | 202140 | Need Case Assigned Date In Report Generated Under Incident Dashboard Screen |
| | 202250 | Email not sent when a case with email template is opened |
| | 202294 | Case count not shown correct when we creating case at user level |
| | 201841 | Count of cases in Incidents screen incorrect |
| | 202259 | Create case window does not dis-appear after creating a policy level case. |
| | 201597 | Workflow custom Screen not sav-ing, cannot change from opened to claimed. |
| Dashboard | 202607 | Policies Appearing Twice on the Dashboard |
| | 202306 | Feature Fix: Data should persist on changing the Date filter under the Monitor Activities tab |
| | 202391 | Summarized attribute not showing up properly on the UI |

| Component/s | Customer Ticket Number | Summary |
|---|---|---|
| Encryption and Masking | 202525 | Unable to search encrypted users |
| | 202527 | User name not showing for encrypted users under Incidents screen |
| Import Watchlist & Lookup Data | 202289 | Bug: lookup tables not synching, missing entry in CTUC |
| Investigation Workbench | 201561 | Geolocation Map Not Populating |
| Manage User, Resource, Peer | 202299 | User search showing only one page of results |
| | 202248 | View User Search Issues - Advanced search |
| Master Child Configuration | 201939 | Possible Bug: Changes to database connection string are not replicated to hibernate files |
| | 201938 | Bug: clustering password resets when editing cluster information |
| Peer Based Activity Outlier | 201975 | Peer based outliers issues |
| Policy Engine | 202537 | Not able to view violations |
| | 202323 | Violations not getting deleted properly using Delete Policy Violations Feature |
| Reporting | 201370 | Ability to export more than 500 violations at a time. |
| Third Party Integration | 201200 | JIRA integration |
| Threat Management | 202522 | Analyst unable to see action on a past user |

| Component/s | Customer Ticket Number | Summary |
|---|---|---|
| Threat Modeler | 202475 | Threat model performance issues |
| | 202442 | Changing actions on use cases with Threat model causing UI to hang. |
| | 202432 | Threat model name and Risk score not updating properly |
| | 201694 | Unable to create threat model on resources and ip based use cases |
| User Interface | 201748 | Dashboard not showing all violations for currentdate |
| | 201854 | Filters Non Functional under Category View |
| Violation Data | 201904 | Apply Filter Error |
| | 202441 | Violations Not Visible for Ipaddresses at the Category Level |

# Additional Issues

| Component/s | Internal Ticket Number | Summary |
|---|---|---|
| Access Outlier | SASS-6292 | Access outlier is not getting finalized when we select Top 100% in job configuration. |
| Access Review | SASS-6063 | Option for Add Resources and Remove Resources not required for All Resources while selecting Resources on Access Review page. |
| | SASS-5646 | Access Review : Page freezes on rejecting during Access Review |

| Component/s | Internal Ticket Number | Summary |
|---|---|---|
| Activity Import | SASS-6307 | Exception in catalina logs while importing summarized data. |
| | SASS-6156 | Child resource-groups are appearing at Add Data--Activity for Arcsight. |
| | SASS-5901 | Clustering: Hibernate exception on securonix logs while running ArcSight import job |
| Behavior Based Anomaly Detection | SASS-6380 | Hibernate exception while running tier2 behavior based outlier |

| Component/s | Internal Ticket Number | Summary |
|---|---|---|
| Case Management | SASS-6467 | NPE in catalina log while taking action as completed on the case at incident screen |
| | SASS-6466 | Comments are not available when we create case for peer group based outlier. |
| | SASS-6412 | ASCII value of special characters getting displayed on UI |
| | SASS-6379 | Landing page is not getting retained after removing filter at Incident screen |
| | SASS-6375 | NPE while clicking on the case number of High Risk Users. |
| | SASS-6362 | Exception in catalina logs while creating case at policy level at category dashboard for policies with violation entity as users. |
| | SASS-6256 | Inconsistent risk score is seen on Incident screen. |
| | SASS-6133 | Case is getting generated at Policy level but not at User level |
| | SASS-6093 | NumberFormatException when case is created at policy level for rule based policy with Violation entity as Users. |
| | SASS-6015 | Exception on clicking the case number created for High Risk Resources. |
| | SASS-5952 | Violations are not shown for User based policy |

| Component/s | Internal Ticket Number | Summary |
|---|---|---|
| | SASS-5939 | Incorrect case count when case is generated as User level at High Risk Entities dashboard |
| | SASS-5864 | Case count not seen at Header in Category View |
| | SASS-5831 | Color mismatch at incident screen |
| | SASS-5708 | Date Wild Card Search For Case Management. |

| Component/s | Internal Ticket Number | Summary |
|---|---|---|
| Dashboard | SASS-6457 | Export not working at High Risk Policy View for Rule based policy with violation entity as Network address. |
| | SASS-6456 | Error on securonix log while navigating to High Risk Policy View for Activity and HQL policy. |
| | SASS-6450 | Policies are not seen for which user is a violator at category dashboard. |
| | SASS-6438 | Case_ID is missing in Security Dashboard |
| | SASS-6437 | No events are shown when we click on occurred number of times. |
| | SASS-6373 | Violations are not seen for High Risk Network Addresses at High Risk Policy View. |
| | SASS-6316 | Incorrect count and pagination issue on summarized events |
| | SASS-6314 | Page keeps on loading for Access Review on Rejection |
| | SASS-6245 | Mismatch in count for summarized data at threat dashboard |
| | SASS-6168 | On Dashboard, search for Incidents is not working accordingly |
| | SASS-6147 | No information details after exporting data. |
| | SASS-6130 | Number format exception on catalina log for Monitoring activities of High Risk Users |

| Component/s | Internal Ticket Number | Summary |
|---|---|---|
| | SASS-6126 | Incorrect Risk score count for High risk users and for High Risk Uncor-related account |
| | SASS-6051 | Number format exception in catalina log while navigating to next page at threat dashboard for sum-marized data. |
| | SASS-6050 | Incorrect count of results shown for summarized data on threat dash-board |
| | SASS-6010 | Report query is getting printed on securonix logs while exporting high risk users. |
| | SASS-5984 | Organization screen appears blank on Dashboard |
| | SASS-5966 | Threat Dashboard appears blank for rule based policy |

| Component/s | Internal Ticket Number | Summary |
|---|---|---|
| Encryption and Masking | SASS-6428 | User name not showing for encrypted users under Incidents screen |
| | SASS-6326 | Account name not masked in user details on Dashboard |
| | SASS-5910 | Encryption key is not working for decrypting the data. |
| | SASS-5881 | Unable to Decrypt in Encypt/Decrypt text options in Encryption masking |
| | SASS-5879 | Encryption Masking--List of options under Conditions are not available and scroll issues |
| | SASS-5661 | Encryption failing for Access Account |
| Housekeeping Jobs | SASS-6446 | Hose keeping jobs are not working as expected |
| Import Users | SASS-6186 | Incorrect query shown for OIA User Import |
| | SASS-6086 | Matcher Reader exception seen for User LifecycleChanges |
| | SASS-5726 | Whitelisted User caught in Violation |
| Import Watchlist & Lookup Data | SASS-5533 | Cannot create a new connection for watchlist on first attempt |
| Investigation Workbench | SASS-6321 | IWB - Not all options are working on Transactions , Console shows multiple error |
| | SASS-5665 | Workbench - Exception on View Activities for Summarization Events not shown |

| Component/s | Internal Ticket Number | Summary |
|---|---|---|
| Other | SASS-5682 | Application Statistics: Landing page does not display the graphs for Application Statistics |
| Outlier Analysis | SASS-6131 | Save job functionality for behavior profile job is not working properly |
| Reporting | SASS-6306 | Ad-hoc Report - Unable to select options from Table Column |
| Threat Management | SASS-5492 | Threat Management Auditing Error |
| Threat Modeler | SASS-6377 | Threat Modeler-Getting exception in securonix log when we click on Show Results from Job Status Page. |
| User Interface | SASS-6459 | Different name is present for export in Compact view and tabular view |

| Component/s | Internal Ticket Number | Summary |
|---|---|---|
| Violation Data | SASS-6333 | No Violations are seen for High Risk Uncorrelated activity accounts at entity/category dashboard - Issue with "by Percentile" only |
| | SASS-6285 | Peer Group based Activity IP Outlier generating duplicate violations on Dashboard |
| | SASS-6284 | Violations are not seen at High Risk Policy View for Tier 2/ Tier 2 HQL Policy. |
| | SASS-6283 | No Violations are displayed when we select same date at threat dash-board |
| | SASS-6258 | Exception in Catalina log when we sort violations by transaction |
| | SASS-6163 | No violations are seen for High Risk Network Addresses |
| | SASS-6153 | No Violations are detected for Access policies |
| | SASS-6148 | No violation details for the access based policy |
| | SASS-6017 | No violations are seen for access policies at Access dashboard. |
| | SASS-5913 | No Violations are shown for High Risk Uncorrelated Activity Accounts |

# 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 Documentation (HPE Security ArcSight User Behavior Analytics 5.0c Patch 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!