



Micro Focus Security

ArcSight User Behavior Analytics

Software Version: 6.10

Release Notes

Document Release Date: July 20, 2018

Software Release Date: July 20, 2018

Legal Notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is 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

© Copyright 2018 Micro Focus or one of its affiliates.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ctp/productdocs

Contents

Overview	5
Release Contents	6
User Interface Elements	7
Geolocation	12
Op Logs	13
Debug	13
Outbox	14
Supported Browsers	15
Prerequisites	15
Supported Operating Systems	15
Supported Hadoop Deployment	15
Certification Matrix	16
What's New in this Release	17
Enhanced Ease of Use	17
Intuitive Security Dashboards	17
Lightning-fast Threat Hunting	18
Advanced Analytics	18
Customizable Threat Modeling	19
Multi-Entity Investigation Workbench	19
Simpler Data Import	19
Faster Data Processing and More Data Storage	20
Normalized Format for All Events and Enriched Data	20
Automated Response	20
Notifications	20
White lists	21
Traffic Analyzer	21
Access Outliers & Certification	21
Policy Management / Violations	21
Remote Ingester	21
New Connectors	22
Reporting	22
Granular Role-Based Access Control	22
Data Masking	22
Security, Stability, and Performance	23

Hotfix	23
Known Issues	24
Fixed Issues	26
Send Documentation Feedback	32

Overview

Micro Focus Security ArcSight User Behavior Analytics (UBA) 6.10 is a big data security analytics platform, built on Hadoop, that utilizes Micro Focus machine learning- based anomaly detection techniques and threat models to detect sophisticated cyber and insider attacks. UBA uses Hadoop both as its distributed security analytics engine and long-term data retention engine. Hadoop nodes can be added as needed, allowing the solution to scale horizontally to support over 100,000 events per second (EPS).

Features of ArcSight UBA

- Supports a rich variety of security data, including security event logs, user identity data, access privileges, threat intelligence, asset metadata, and netflow data.
- Normalizes, indexes, and correlates security event logs, network flows, and application transactions.
- Utilizes machine learning-based anomaly detection techniques, including behavior profiling, peer group analytics, pattern analysis, and event rarity to detect advanced threats.
- Provides out-of-the-box threat and risk models for detection and prioritization of insider threat, cyber threat, and fraud.
- Risk-ranks entities involved in threats to enable an entity-centric (user or devices) approach to mitigating threats.
- Provides Spotter, a blazing-fast search feature with normalized search syntax that enables investigators to investigate today's threats, and track advanced persistent threats over long periods of time, with all data available at all times.
- Includes comprehensive case management features that allow multiple teams to collaborate on investigation and response.
- Provides the Investigation Workbench to detect links across disparate datasets to enable quick investigations and hunting for cyber threats.

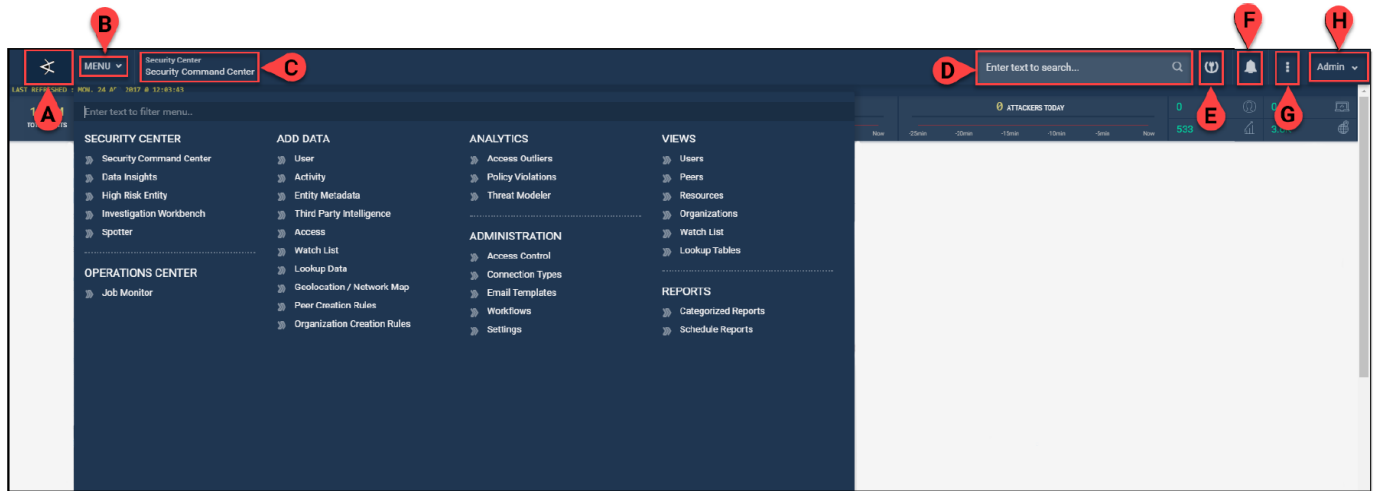
Release Contents

The files in this release include:

File Name	Description
ArcSight_UBA_6.10_Release_Notes.pdf	This document
ArcSight_UBA_6.10_Installation_Guide.pdf	Application installation guide
ArcSight_UBA_6.10_Administration_Guide.pdf	Administration guide
ArcSight_UBA_6.10_User_Guide.pdf	User's guide
ArcSight_UBA_6.10_Ingestion_Node_Installation_Guide.pdf	Ingester Node installation guide
ArcSight_UBA_6.10_Readme.txt	MySQL installation guide
ArcSight_UBA_6.10_Application_04122018.bin	Application installer file
ArcSight_UBA_6.10_Ingestion_Node_04122018.bin	Ingester Node installer file
ArcSight_UBA_6.10_package_installer.sh	MySQL 5.6.33 installer file
Customer_Letter_UBA_6.10.docx	Letter to customer

User Interface Elements

Some of the common elements found throughout the application are shown in the following image:



A. ArcSight Logo: Click from any screen to return to the Security Command Center home screen.

B. Main Menu: Click to expand navigation options.

C. Current Screen: Click to return to the home screen for the current menu item.

D. Quick Search: Enter text to search within UBA.

audit

firstname = Neerav , filename = **audit** , accountname = NJAIN@SECURONIX.COM ,
transactionstring1 = trash , usercriticality = Low , resourcename = GDriveLogs ,
employeeid = njain@securonix.com , lastname = Jain

firstname = Neerav , filename = **audit** , accountname = NJAIN@SECURONIX.COM ,
transactionstring1 = trash , usercriticality = Low , resourcename = GDriveLogs ,
employeeid = njain@securonix.com , lastname = Jain

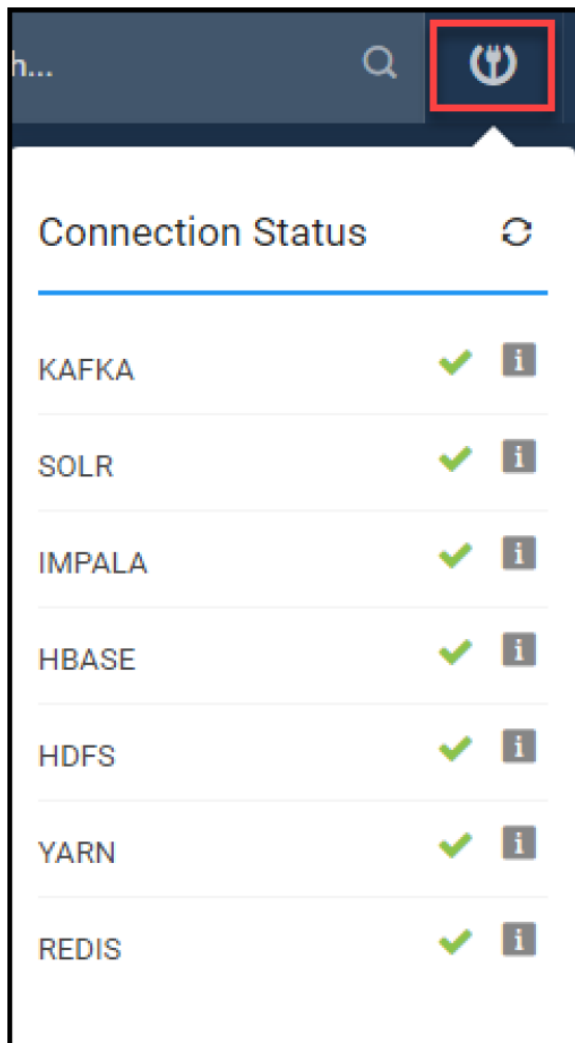
firstname = Neerav , filename = **audit** , accountname = NJAIN@SECURONIX.COM ,
transactionstring1 = trash , usercriticality = Low , resourcename = GDriveLogs ,
employeeid = njain@securonix.com , lastname = Jain

firstname = Neerav , filename = **audit** , accountname = NJAIN@SECURONIX.COM ,
transactionstring1 = trash , usercriticality = Low , resourcename = GDriveLogs ,
employeeid = njain@securonix.com , lastname = Jain


firstname = Neerav , filename = **audit** , accountname = NJAIN@SECURONIX.COM ,
transactionstring1 = trash , usercriticality = Low , resourcename = GDriveLogs ,
employeeid = njain@securonix.com , lastname = Jain

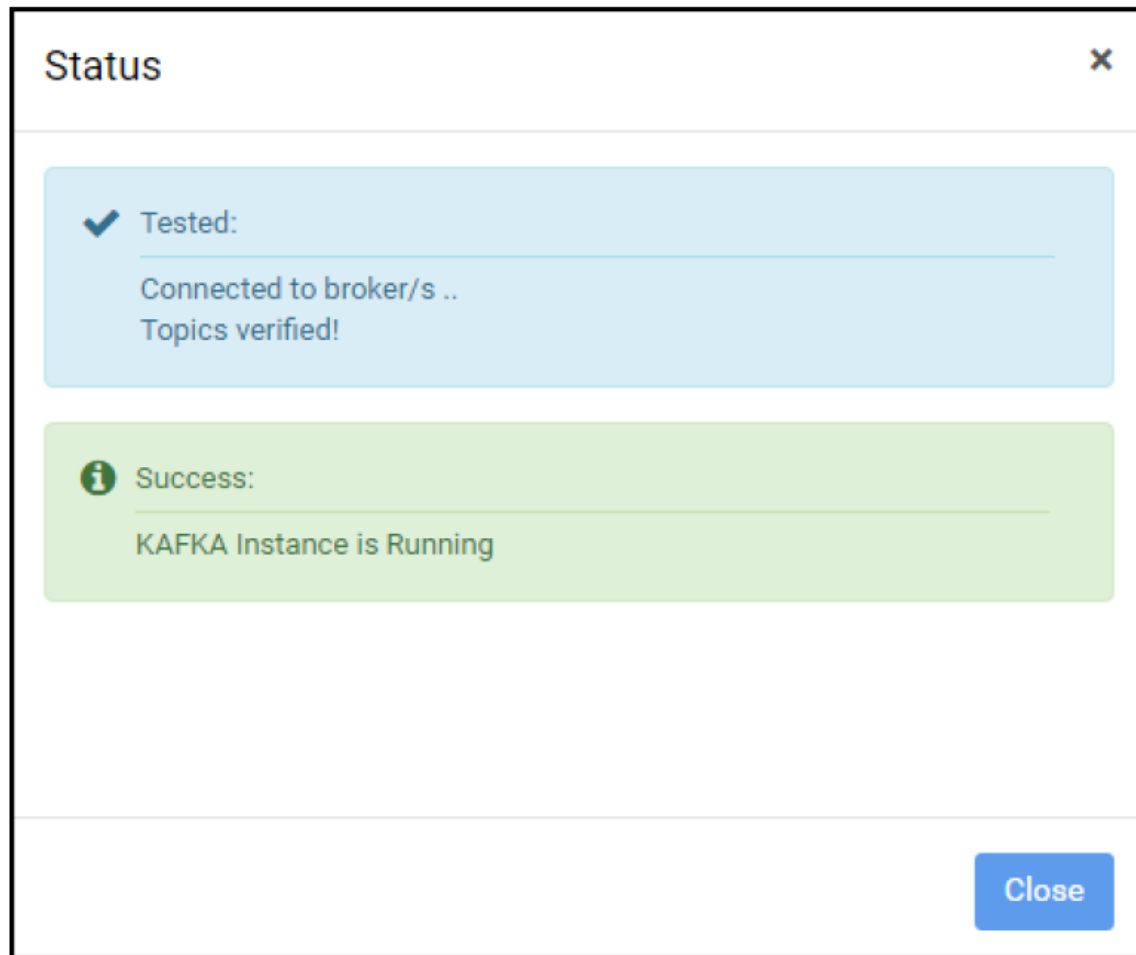
VIEW IN SPOTTER

E. Connection Status: Click the  to view the **Connection Status** for all Hadoop components running on your environment.



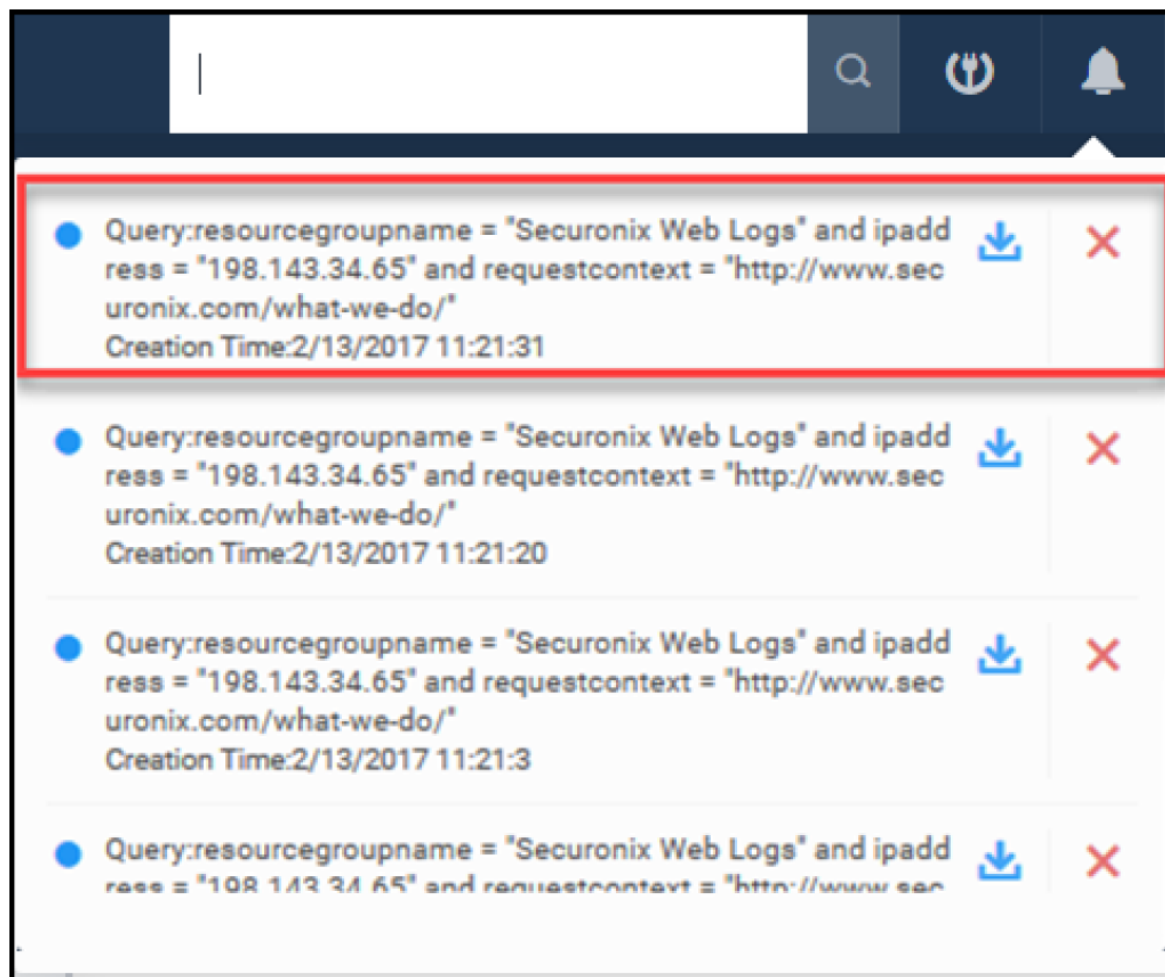
The green check mark indicates the component is running; a red X indicates the component is not running.

Click  to view details of each component.



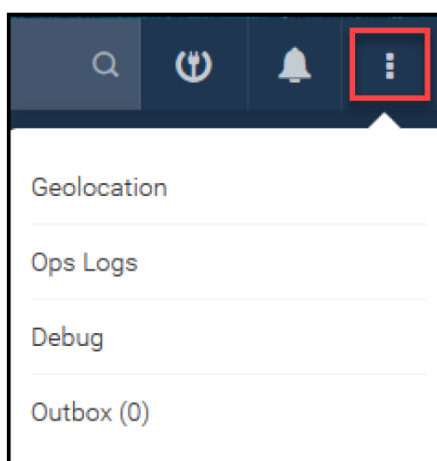
To configure settings for Hadoop components, navigate to **Menu > Administration > Settings > Hadoop** and following the instructions in Configuring Hadoop Settings.

F. Notifications: View job failure notifications and download exports including Spotter reports and query results. To delete notifications, click the red X.



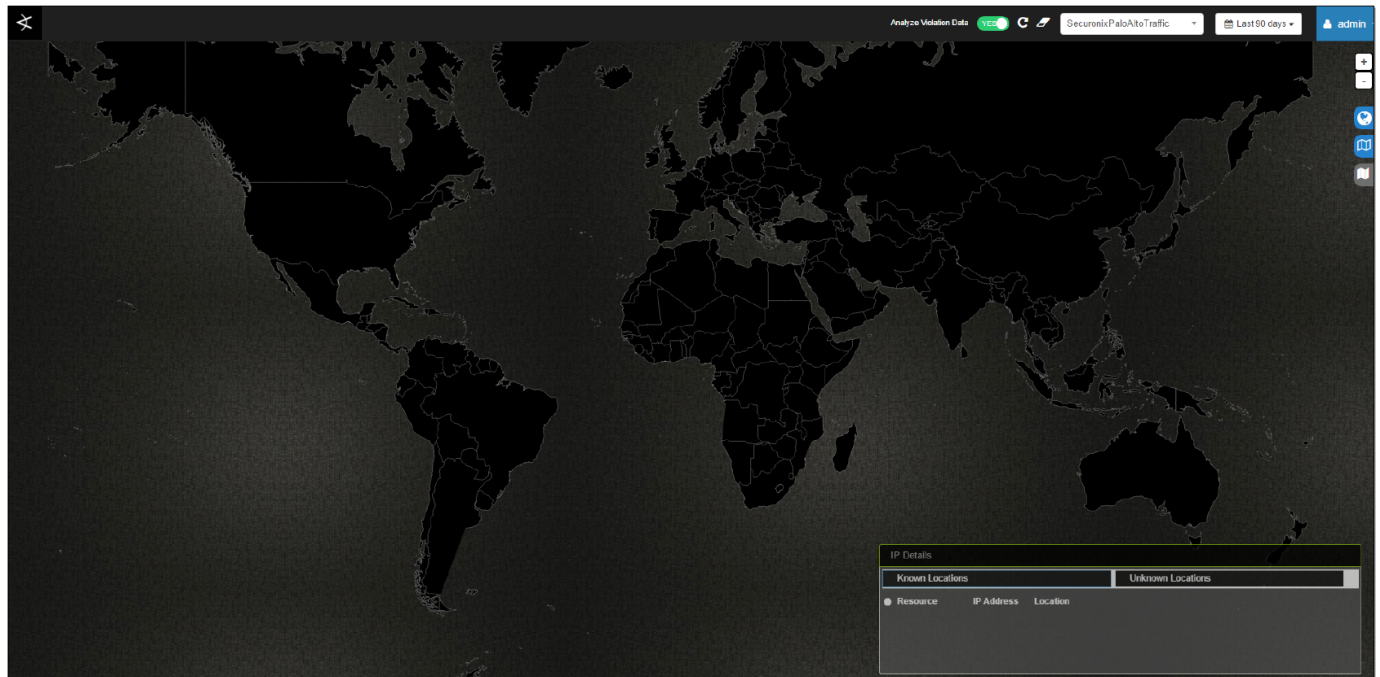
To download reports, click the download icon. For information on how to export Spotter reports, see Spotter.

G. Three Dot Menu: Access the following screens:



Geolocation

From this screen, view the geolocation of the network source of specific resources



You can perform the following actions:

- Toggle Analyze Violation Data to Yes to analyze data.
- Click refresh icon to refresh results.
- Click erase icon to clear results
- Select a resource from the dropdown.
- Select a time range from the dropdown.
- Use +/- to zoom in/out from the map.
- Click and drag mouse around to pan and tilt map view.
- Click icons on the right side to switch map view:



Op Logs

From this screen, you can view messages generated while executing Spark jobs.

Operational Messages are generated while executing spark jobs and we can view these messages by starting consumer with appropriate filters.

Consumer 1 +

Datasource	Job	Policy	Source	Max Number Of Messages
GoogleDriveLogs	All	Activity to a Non-Corporate Dom...	All	1000

Stop

Source	Server Time	Current Time	Message
10-0-00.securonix.com	Thu, 13 Apr 2017 18:33:19 GMT	Thu Apr 13 2017 16:29:34 GMT-0500 (Central Daylight Time)	msg+Hadoop configuration obtained!

To view messages, complete the following:

1. Click + to start a **Consumer**.
2. Select **Datasource**, **Job**, **Policy**, and **Policy** from dropdowns.
3. Specify the max number of messages. Default 1000.
4. Click Stop to stop retrieving messages.

Debug

From this screen, view error messages and associated data to debug the UBA application.

MENU

Security Center
Debug

Enter text to search...

Lpherson@securonix.com

Available Tables

snyp6tanalyticsjobstatus

snyp6tpeer19_department

snyp6tpeer19_division

snyp6tpeer3_department

snyp6tpeer5_division

snyp6tpeer0


Click an option to see associated data.

Outbox

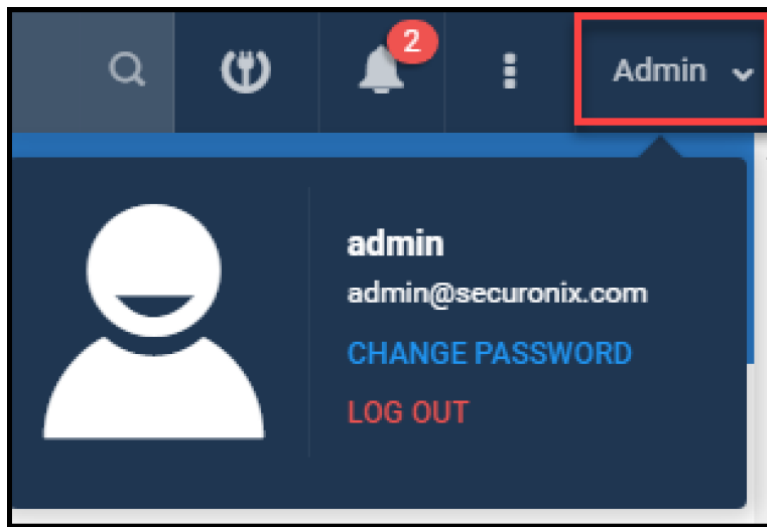
From this screen, view the UBA email queue and send or delete messages in the outbox.

Send selected mail(s)

Delete selected mail(s)

	Sender name	From	To	CC	BCC	Subject	Last updated	High Priority
<div>First < > Last</div>								

H. Admin: View the user name of the current user, change current user password, and log out.



To change the current user's password, click **Change Password**, enter the old and new password, confirm the new password, and click **Update**. To log out, click **Log Out**.

Supported Browsers

The application can be launched using any of the following browsers:

- Firefox 33 and above
- Internet Explorer 11
- Chrome (latest)

Prerequisites

- Oracle Java 8 (on all nodes, including YARN containers for Spark)
- MySQL 5.6.33 or above (on the ArcSight UBA Console Servers)

Note: Follow the instructions in *ArcSight_UBA_6.10_Installation_Guide.pdf* to install MySQL Community version or follow the instructions in *ArcSight_UBA_6.10_Readme.txt* to install MySQL 5.6.33 Standard Edition.

Supported Operating Systems

The application supports the following operating systems:

- CentOS 6.8 and above, 7.1 and above
- RHEL 6.8 and above, 7.1 and above

Supported Hadoop Deployment

ArcSight UBA provides the following deployment option:

- An ArcSight UBA deployment on an existing Hadoop cluster (Cloudera 5.x or Hortonworks 2.4, or 2.5).

The Hadoop distributions and the version of the services required are listed in the following table.

Certification Matrix

Service	CDH 5.10	CDH 5.11	CDH 5.12	CDH 5.13	Hortonworks 2.5	Hortonworks 2.6.x
Hadoop	2.6.x	2.6.x	2.6.x	2.6.x	2.7.x	2.7.x
HBase	1.2.x	1.2.x	1.2.x	1.2.x	1.1.x	1.1.x
Hive	1.1.x	1.1.x	1.1.x	1.1.x	1.2.x	1.2.x
Impala	2.9.x	2.9.x	2.9.x	2.9.x	N/A	N/A
ZooKeeper	3.4.x	3.4.x	3.4.x	3.4.x	3.4.x	3.4.x
Kafka	0.10.x	0.10.x	0.10.x	0.10.x	0.10.x	0.10.x
Spark	1.6.x	1.6.x	1.6.x	1.6.x	1.6.x	1.6.x
	2.1x	2.2	2.1x	2.1x	2.1x	2.1x
Solr	4.10.x	4.10.x	4.10.x	4.10.x	5.5.x	5.5.x

What's New in this Release

Enhanced Ease of Use

The UBA user interface has been redesigned and rebuilt from the ground up using the latest technologies to provide a unified look and feel, and an enhanced user experience across the application:

- Easier to navigate through the application from the Security Command Center, which combines all types of threats and violations, and offers incident management from a single dashboard
- Meaningful use of colors and animations to help you quickly find the information you need
- Bite-sized pieces of information in modular cards to help you focus on the information that's important to you
- Redesigned main menu to help you find functionality more easily
- Global search to quickly find exactly the information you need
- Use Case-driven view with summarized data to give you an overview of threats to make it easier to investigate and take action

Intuitive Security Dashboards

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

- **Security Command Center:** New Security Command Center feature provides a real-time view of threats as they happen and allows you to drill down into each user or violation and take action.
 - Offers a 360° view into the security and risk posture of the organization
 - Allows analysts to detect, investigate, and respond to incidents in real-time
- **Data Insights:** New customizable dashboards allow you to create, modify, save, and share custom dashboards to gain data insights for your organizations with the My Dashboards feature
 - Dashboards are now more interactive. Clicking on a value in a dashboard widget provides an option to
 - Add Filter to all widgets by the selected value.
 - Get Details by providing a drill-down view of user details, watchlist, threat intel, or geolocation information.
 - Dashboards can be shared with other users or groups.
 - Dashboards for PCI and HIPAA Compliance and popular devices are provided.

- **Case Management:** New case management interface allows you to more easily track the life cycle of a case.
 - The improved Incident and Case Management features a bold new look and workflow improvements to make it easier for analysts to manage an incident through its life cycle. It provides quick filters for analysts to see incidents in their queue, see incidents assigned to members of their groups, and easily claim or assign incidents.
 - Activity Stream features a chronological view of case-related activity with the ability to attach documents and evidence to a case. It includes a real-time chat window to facilitate collaboration among analysts.

Lightning-fast Threat Hunting

UBA 6.10 features Spotter, a lightning fast natural-language search engine with a Lucene core. Spotter now includes:

- Search and hunt capabilities across incidents, and enriched and raw events
- Ad-hoc visualization and reports of search results
- New commands and operators were added to support different use cases. These include DISTVALUE, PCR, SPAN. Enhancements were made to the FILTER, WHERE, ORDERBY commands, and new aggregation and evaluation operators were added: AVG, DEC, HEX, BASE64, UNBASE64.
- Spotter interface displays friendly names for generic fields. For example, if the field 'CustomString1' contains the patient name, then the user defined/friendly name 'Patient Name' will be displayed.
- Results from a Spotter query can be saved to a columnar Report template in addition to various other formats such as PDF, Excel, CSV, etc.

Note: ArcSight UBA 6.10 has a maximum retention for raw logs of 30 days. These logs are kept in SOLR and do not get archived to HDFS. You may find areas in the documentation that reference retention and archiving capabilities not available due to these limitations.

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 UBA violation data
- New analytical checks to check data against watch lists, lookup tables, threat intelligence, and geolocation
- Added 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
- Conditional Behavior Profiles
- Enhanced Peer Group Analysis to detects outliers by analyzing peer behavior for the following entities:

- Users
- Devices
- IP Addresses
- Over 100 behavior-based detection techniques across all entities

Customizable Threat Modeling

UBA 6.10 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 UBA environments. These threat indicators are used by the threat modeling framework to identify the riskiest users and endpoints in the customer's environment.

Enhancements to Threat Modeling include:

- Kill-chain based threat visualization
- Ability to customize threat models from the dashboard

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 drill downs

Simpler Data Import

UBA 6.10 new includes premium connectors to connect to new data sources for simpler and faster data import. New premium connectors include:

- Google Apps
- Google Users
- Sales Force
- ThreatStream

Faster Data Processing and More Data Storage

UBA 6.10 includes new data processing and compression features that allow for faster processing and data storage.

- 40+ additional attributes added to Event schema
- Tenant information for multi-tenant environments
- 90% compression of event data into structured JSON format for access by third party tools

Normalized Format for All Events and Enriched Data

All event data in UBA is stored in a super-enriched, normalized, self-describing format called the Open Event Format (OEF, see openeventformat.com for details). The OEF:

- Enables events to be used later with all the relevant data enrichment without joining or merging with other information
- Ensures historical changes to the enriched data are captured with the event at the time it occurred
- Maintains the original source event in the OEF event

Automated Response

- In addition to being able to access violations and events for an incident, analysts can now launch playbooks that take automated response actions to facilitate rapid incident triage. Examples of an automated response include gathering the reputation of artifacts from threat intel sources such as an IP address, domain, file, process, device; taking actions to disable an AD account, kill a process, or disable USB device; and creating tickets or incidents in 3rd-party systems.
- The automated response framework provides out-of-the-box integrations with Active Directory, VirusTotal, PassiveTotal, Spamhaus, Tanium, Nessus, Qualys, Phantom, Demisto, RSA Archer, RSA NetWitness, with many more integrations on the way.
- Source code templates are provided to facilitate development of custom integrations.

Notifications

- Notifications on policy violations can be sent via email or forwarded as Syslog/CEF formatted messages to a 3rd-party system.

White lists

- The new white list feature supports creation of Global and Targeted white lists to allow analysts to exclude Entities (users, accounts, IPs, resources) from ongoing monitoring, globally or for specific Policies triggered by an Entity.

Traffic Analyzer

- Traffic Analyzer provides purpose-built analytics to detect behaviors exhibited by malware. It performs checks against web proxy traffic to detect algorithmically generated domains, patterns of malicious or robotic behavior, access to rare domains, use of user agents, and other checks to detect compromised endpoints.

Access Outliers & Certification

- The popular Access Outliers Detection, Access Review and Certification features have been introduced on the UBA platform. These features allow organizations to rapidly detect access privileges of individuals that differ from their peers using a variety of sophisticated analytical techniques such as “peer group cohesiveness factor”. A certification workflow allows managers to review, certify or revoke outlier privileges.

Policy Management / Violations

- A policy can now be created for a Functionality (i.e. Device Category) rather than a specific Resource (i.e. Device Type). This allows Threat Content developers to create one policy for multiple resources, rather than having to create and maintain duplicate policies for each resource.
- A simplified policy creation screen limits available options based on selections in earlier steps to make policy creation more intuitive.

Remote Ingester

- Remote Ingester was redesigned for ease of deployment, ease of use, and secure data transfer over the public internet. Remote Ingesters can now be fully configured from the UBA console.
- ArcSight Event Broker/Event Broker DoK can be used to configure from Remote Ingester to point to UBA Kafka
- WMI service was added to support collection from a large number of Windows endpoints across multiple domain controllers.

- Besides Syslog and WMI, activity collection from Remote Ingesters is now possible using a wide range of API based connectors such as File, Database, JSON, Splunk, Elastic, etc. User import is required for event enrichment. Attribution is supported for Active Directory.
- Event preview capability was added to verify events being collected and support rapid creation of new regex line filters to parse new event types.
- A Syslog-ng style event filtering framework was added for Syslog and WMI collectors to limit event collection and for matching events to a specified datasource.
- Event metering was introduced to enforce licensed limits such as events per day (EPD) and disk usage (DU).

New Connectors

- Dozens of REGEX parsers and API based connectors were added to the list of supported datasources as such as Azure, SaleForce, Netskope, etc.

Reporting

- Dynamic .jrxml report templates were introduced to make report creation easy, fast, and fully managed within the UBA console.
- Reports preview option allows the report query to be verified.
- Merge Reports allows several reports to be merged into a single report.
- The reporting framework now allows access to all UBA data repositories: Data in Solr (activity, violations, user, threat intel, etc.) using Spotter queries, HDFS data in Parquet files using Apache Hive SQL Syntax, and Case Management data saved in MySQL repository.

Granular Role-Based Access Control

Role based access control (RBAC) was enhanced to limit a user's access to specified Resources and content.

Data Masking

- Data Masking allows an organization to implement granular Privacy controls. It is now possible to mask any attribute of a user.
- Granular rules can also be setup to mask information of users, e.g. users belonging to a specific department or having certain access privileges.

Security, Stability, and Performance

- UBA utilizes recent Hadoop libraries to take advantage of security features, and stability and performance improvements.
- Spark 2.0 libraries support secure communications across Hadoop nodes, and services and authentication using Kerberos.
- Solr 6.6 libraries include a number of stability and performance improvements for handling large numbers of index collections, supporting disk based indexes for faster indexing and searching, and supporting multiple Solr servers on a host.

Hotfix

There is a Hotfix available to enable LDAP Authentication feature, please contact Micro Focus support to get the Hotfix.

Note: After the hotfix is unzipped, navigate to the folder Hotfix_AT-829_2018-04-25 and ignore the extra folder __MACOSX.

Known Issues

The following known issues exist in UBA 6.10:

SNYP-1892	Installer- Syslog-Ng server cannot be installed using latest installer
SNYP-1898	Installer- Redis installation selection does not show up and it asks for sudo password for redis during syslog-ng server installation step
SNYP-1899	Installer - security issue- Redis server password is maintained in plain text in installvariables.properties file
SNYP-1901	Installer/packaging- "Error deploying securonixwebsocket" error can be seen in log while application startup
SNYP-1905	Installer - cannot uninstall database- it says database connection failed, though can connect to database
SNYP-1907	Installer(Console mode):-Uninstaller does not remove all the components.
SNYP-1915	Installer- Two roboticbehavior job is packaged in sparkjobs folder, remove unwanted one
SNYP-1916	Installer- Security - Passwords are mentioned in plain text in license.properties file
SNYP-1919	Installer(GUI/Console)- Incorrect Minimum system requirement shows up in install wizard
SNYP-1920	left pane menu options (Pre-Installation summary) and right pane headers (Install Complete) are not in sync
SNYP-1921	Installer(GUI/Console)- Incorrect message shows up when install only Ingestor at install complete stage
SNYP-1922	Installer(Console):-Validation missing on "Choose Product Features" step
SNYP-1928	Installer(GUI/Console):- Should allow user to connect an existing Redis server
SNYP-1929	Installer(Console):-Issues on Step "Choose Product Features"
AT-697	Exit Installation option hangs while installing. Workaround: Manually kill the installation process to exit.
AT-724	Getting NonfatalInstallException Database schema creation failed error in installation log
AT-755	The field in "Select Event Field" is not saved in the correlation rule. Workaround: When editing an activity import job and editing a correlation rule, re-select the attributes that were selected before.
AT-804	Preview of Data Coming to UBA via Syslog is not working. Workaround: Manually add lines instead of using the preview function.

AT-807	<p>The restart command for scnx-arcsight_eb_to_securonix service does not start the service again.</p> <p>Workaround: Instead of using the restart command, the user can use the stop command, make sure processes are not running, then use the start command.</p>
AT-813	<p>File Import from Remote Ingestor is not working when we use duplicate parser to create activity import</p> <p>Workaround: Create a new activity import instead of duplicating parser when ingesting data through remote ingestor.</p>
AT-814	<p>Not able to import activity from Syslog using Remote Ingestor when we use duplicate parser or Add Data for Existing Device Type for the first time.</p> <p>Workaround: When using the duplicate parser or add data for existing device type with a remote ingestor, the user would need to save a first time, then edit a second time, then restart the ingestor service for the changes to take effect.</p>
AT-815	<p>Import Using' option always goes back to console when edit the existing Activity Import job with import from Remote Ingestor.</p> <p>Workaround: When editing an activity import job, re-select the "Import Using" dropdown.</p>
AT-820	<p>In IE 11 Save & Next Icon doesn't work while creating Identity Policy.</p> <p>Workaround: Use different browser such as Chrome.</p>
AT-821	<p>Mapping of Event Fields is not available in IE 11 while importing Activity Import .</p> <p>Workaround: Use different browser such as Chrome.</p>
AT-822	<p>Edit button beside 'import using' while importing activity for existing device type is not working in Firefox.</p> <p>Workaround: Use different browser such as Chrome.</p>
AT-825	<p>Unable to get the users correlated even though updated the correlation rule for the existing job.</p> <p>Workaround: Try to create new activity import job.</p>
AT-827	<p>Application Logs in Log Settings is empty . It displays ' Logfile not present please check the log4j.properties file'</p> <p>Workaround: Go to the command line to use commands like grep to find errors, exceptions, etc.</p>

Fixed Issues

This release contains the following fixed issues.

Key	Components	Summary
SNYP- 3860	3rd Party Integration	Office 365 Optimization and Improvements
SNYP- 2896		Netskope connector Events Endpoint
SNYP- 2435		Improvements for Netskope Connector
SNYP- 3823	Access Control	SSOlogin with ADFSIntegration.
SNYP- 3617	Access Import	UI Issues: Access Module [Access Import, Access Reviews Job, Access Outliers Job, Access Reviews Dashboard, Access Outliers Dashboard]
SNYP- 3242	Access Outliers	Access Outliers Job Screen: Added"View Details" option
SNYP- 3234		Show jobconfiguration details for access outlier jobs
SNYP- 3358	Activity Import	Delete Jobs When Resource groupis deleted
SNYP- 2936		Checkpoint parser
SNYP- 3895		Accountname is mappedas UNKNOWN inspite of IFTHENELSE condition - Windows WINEVENT Collector
SNYP- 3436		Capability to mapmultiple resource attributes having same mapped attribute to different keys
SNYP- 3186		Activity import: show functionality basedpolicy in summary screen
SNYP- 3277		Update policies cardin Activity Import Summary screen
SNYP- 1856	Analytics	Analyst can whitelist any entity
SNYP- 4027	Case Management	MM: Provide a link to the case at save time
SNYP- 3606	Encryption and Masking	View -> Users: "Advance Search" option removed when masking is enabled.
SNYP- 3533		IWBMasking - plain text employeeidin spotter query when click on "View Violations"
SNYP- 3351	Hadoop Configuration	UI change required to accept "access" topic in Kafka configuration
SNYP- 3159		Timezone For Tenant
SNYP- 3473		Solr Replication Factor value shouldbe greater than equal to one (validation)
SNYP- 2869	Ingester	Delete Ingester Jobs From Job Screen
SNYP- 2828		Ingester Jobs Pause Play Options From Job Monitor Screen
SNYP- 2294		Ingester Linux Service
SNYP- 2721	Job Monitor	Job Screen Changes

Key	Components	Summary
SNYP- 3408	Job Monitoring UI	jobs play pause not showing under view jobs label
SNYP- 4040	Notification framework	Show policy name in place of policy Id in notification.
SNYP- 3254	Policy Engine	Create New Risk Booster For Checking Against Watchlist
SNYP- 2915	Reporting	New Ui Steps Wizard Changes for Report Screen
SNYP- 3024		Reporting Not able map attribute with special characters
SNYP- 2816		Show Report Format on spotter reports
SNYP- 2707		Merge Multiple Spotter Reports
SNYP- 3400		Validation message not present for stats query in create Report
SNYP- 2249	Security Command Center	Level 2 drill down in violation info
SNYP- 3735	Settings	Special Characters Not Allowed in Username position, which prevents SSOenabling
SNYP- 3079	Spotter	Show user defined attributes in events table on left panel gear toggle
SNYP- 2988		If query contains index then it should be present in new search
SNYP- 2695		Hide raw events if masking is enabled and no privacy role
SNYP- 2457		job paused after 1 min timeout
SNYP- 4010	UI	Unable to view full comment for "Action Taken"
SNYP- 3397	Workflows	Workflow :- Removed "Assign Incident to Other" option from "Default Assign To"
SNYP- 3424	3rd Party Integration	Connector for CrowdStrike using Falcon API
SNYP- 2648		Connector for Workday
SNYP- 2323		Integration with Active Directory
SNYP- 2322		Integration with Phantom
SNYP- 2073		Integration with ServiceNow
SNYP- 2030		Integration with Passive Total
SNYP- 2029		Integration with VirusTotal
SNYP- 1652		Send CEF formatted violations to RSA NetWitness
SNYP- 1651		Send CEF formatted violations to RSA Archer
SNYP- 2836		Connector for Azure Reporting API
SNYP- 1845		Integration with Tanium
SNYP- 1628		Get asset inventory from Tanium
SNYP- 3272	Access Import	Glossary Import: Not getting datasources list in "Datasource Name" dropdown

Key	Components	Summary
SNYP- 3271	Access Outliers	Access Outlier Dashboard: Multiple Export option added.
SNYP- 3241		Access Outlier: Exclude Attribute from Outlier Analysis
SNYP- 3105	Analytics	Normalizing The Risk Scores of Policies/Behavior Based Outliers
SNYP- 1841	Case Management	Create Case For Policy or Threat Model
SNYP- 1575		Update Case Management Layout and Workflow
SNYP- 3106		Case Management on Threat Models
SNYP- 2748	Connection Types	Windows: File Beats Connector from LogStash [ELK]
SNYP- 1854	Documentation	UBA Troubleshooting Guide
SNYP- 2653	HDFS Data	Addcollection freeze unfreeze process to Data LifyCycle process
SNYP- 1859	Ingester	WMI Collector
SNYP- 2039	Installer	Build Remote Ingester Installer for SaaSdeployments
SNYP- 142	Kafka Producer	Remote Ingester Updates
SNYP- 1706	Notification framework	Risk Scoring job initiate the email notification
SNYP- 2094	Response framework	Mapriskthreat indicator to response actions
SNYP- 3130	Risk score	Add capability to skip risk scoring andsaving for NONE criticality policy
SNYP- 2025	SaaS	SaaS Tenant Monitoring Tool
SNYP- 2504		SaaS: new collection methods for WMI & Syslog-ng
SNYP- 3465	Settings	Develop UI for CAC
SNYP- 2758		Common Access Card(CAC) support for UBA
SNYP- 2253	Spark Streaming	Update all jobs to use SPARK 2.0 libs
SNYP- 3476	Spotter	SPAN operator, calculate average number of emails per day
SNYP- 3419		Limit simple query results to save resources
SNYP- 2250		Pagination For Stats Command
SNYP- 2190		DistValue function to display groupby count
SNYP- 1946		Impala Queries Optimization
SNYP- 3007	Watchlist	Cannot addmember to watchlist froma violation
SNYP- 3616	3rd Party Integration	Exchange Reporting - MessageTrace Connector

Key	Components	Summary
SNYP- 3666	Access Control	Increase in account identifier length
SNYP- 3664		Remove the isOldPasswordCorrect service
SNYP- 3405	Access Outliers	Access Outlier - View Config option not selecting peer criteria/user criteria
SNYP- 4158	Activity Import	Winparser not able to parse data
SNYP- 3943		Resource Name have trailing white space causes issue when displaying Violation Summary and Graph
SNYP- 3864		Wineventparser not parsing data
SNYP- 3785		Incremental DBImport does not work
SNYP- 3691		Data duplication upon restart of application
SNYP- 3636		LEEF Parser is parsing data incorrectly
SNYP- 2894		Fix Label for Salesforce collection method
SNYP- 4019	Case Management	Violation events query is missing double quotes after account name
SNYP- 3940		Populated Spotter Search within Incident is not Correct
SNYP- 3938		Stored XSSVulnerability within Conversation/Chat Window in Incidents
SNYP- 3805		Case Management: Violation Events - Account name attribute holds employee id value
SNYP- 2717		Play Book appears in 2 different places in UI
SNYP- 1207		Unable to set default assign to groups/users in Case Management
SNYP- 3319	Encryption and Masking	Activity attributes not getting masked
SNYP- 3633	Event Enrichment	Enrichment Job Failing
SNYP- 3692	Event Parsing	UBA - Remote Ingester unable to parse specific JSON events
SNYP- 2281		Duplicate category fields
SNYP- 4022	Geolocation / Network Map	Geolocation job counts do not get updated
SNYP- 3627	Hadoop Configuration	Soft Threshold - Value is set as 250 million..set it as 100 million
SNYP- 3553		Double Slashes on Hadoop screen
SNYP- 2835	Installer	Misc UBA installer issues affecting auto tenant setup
SNYP- 3684	Job Monitoring UI	User Import from Ingester using LDAP was showing negative counts on Job Monitor
SNYP- 1914	Licensing	Manage Encryption Enabled
SNYP- 3835	Maintenance Jobs	DEE job is not deleting the expired events

Key	Components	Summary
SNYP- 3322	Notification framework	Email templates are not getting triggered
SNYP- 4065	Policy Engine	Policy Screen - Addwarning message on step 1 if entity selected under violator is not mapped for selected data source
SNYP- 3739		ERROR While Running 5th Job when multivalued is enabled for fields in analysis
SNYP- 3663		Concurrent Modification Exception In IEE jobs while checking against Lookup tables
SNYP- 3662		Policy configuration needs to be validated for policy id-440
SNYP- 3041	Policy Violations	Violation Count is not matching with number of violations on the UI
SNYP- 2712		Traffic Analyzer policy screen should only display applicable attributes
SNYP- 2091		Missing and duplicate features in policy screen
SNYP- 1824		Threat Indicator issues in Policies
SNYP- 2716		Policy filters By Analytical Type return no results
SNYP- 3511	Reporting	Spotter report on index=violation returns an empty pdf
SNYP- 3043		Schedule Report is missing Save button
SNYP- 2948		Reports UI is missing a way to schedule a report
SNYP- 2719		Save Reports downloads a corrupt file
SNYP- 2262	Risk Score	Reporting for Spotter requires admin privileges
SNYP- 2261		Risk score reverts back to non-zero
SNYP- 3160	Security Command Center	Violator Count Discrepancy
SNYP- 3688	Solr	Solr connection timed out when searched for employee id.
SNYP- 3760	Spotter	Cannot save spotter queries
SNYP- 3759		Cannot export reports from Spotter
SNYP- 3667		Spotter is not displaying all the results (restricts to 15 / page - navigation to the second page not available)
SNYP- 3625		STAT function doesn't give the full results on the Spotter
SNYP- 3550		Spotter - Error when unpacking Solr Collection
SNYP- 2715		Reports option in Spotter Search Results is not visible
SNYP- 2714		Spotter results summary on LHS is missing category outcome field
SNYP- 3863	Third Party Intelligence	Issues with TPI Import
SNYP- 3714		TPI condition does a reverse contains match
SNYP- 3682		TPI Import Job Failure

Key	Components	Summary
SNYP- 3928	UI	Wrong Entity Profile under Top Threats/Top Violations/Top Violations
SNYP- 3862		Zero Risk policy name is missed in Reason Section of threat Model
SNYP- 3833		Wrong Threat Verbose Displayed under Top Violators
SNYP- 3391		Display Issue
SNYP- 2711		Colors in the Cluster visualization should be consistent
SNYP- 2690		Forgot Password Not Working
SNYP- 2634	User Import	Can't import Sailpoint data from Oracle database into UBA 6.0
SNYP- 3927		User Import - Throwing an error : ConcurrentModificationException
SNYP- 1310	Views-Peers	View Peers: When we click on Behavior Profile from Left panel getting Missing Method Exception
SNYP- 3006	Watchlist	Cannot add members to a watchlist

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 computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Release Notes (User Behavior Analytics 6.10)

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 arcsight_doc@microfocus.com.

We appreciate your feedback!