



ArcSight User Behavior Analytics

Software Version: 6.10

Administration Guide

4/18/2018

Powered by  **SECURONIX**

Legal Notices

Warranty

The only warranties for Micro Focus 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. 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.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

Micro Focus 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 Micro Focus 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.

Follow this link to see a complete statement of copyrights and acknowledgments: <https://community.softwaregrp.com/t5/ArcSight-Discussions/Third-Party-Copyright-Notices-and-License-Terms/td-p/1589228>

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 Micro Focus.

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:

Micro Focus

Attn: Gordon Lee

1140 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 Micro Focus ArcSight Technical Support Page: https://softwaresupport.softwaregrp.com/documents/10180/14684/esp-support-
-------	--

Contact Information, continued

	contact-list
Support Web Site	https://softwaresupport.softwaregrp.com/
Protect 724 Community	https://community.softwaregrp.com/t5/Protect724/ct-p/Protect724

Contents

Introduction	10
Who Should Read This Guide	10
Configure Hadoop Settings for ArcSight UBA	11
Tenant-Config	12
Kafka	12
Solr	20
Impala/Hive	29
HBase	35
HDFS	41
Redis	49
Settings	52
Configuring the Application	52
Application Settings	52
Archival Settings	59
DNS Servers	64
Hadoop	65
Housekeeping Jobs	66
Avroparquet Migration Job	70
LDAP Authentication	71
Log Settings	75
Manage License	79
SAML Settings	81
SMTP Server Settings	85
UI Preferences	87
Data Masking	89
Access Control	95
Setting Up Access Control	95
Creating Roles	96
Creating Users	101
Creating Groups	106
Managing Users, Groups, and Roles	109

Granular Access Control	112
Setting up Granular Access Control	113
Password Control	117
Workflows	121
Configuring Workflows	122
Connection Types	135
Managing Connection Types	135
Adding a New Connection Type	137
Example: Configure CEF Export Connection	138
Uploading or Downloading Files	140
Registering Connectors	141
User Data	144
Importing User Data	144
Step 1: Creating a Connection	145
Importing User Data from Active Directory	145
Importing User Data from Aveksa	152
Importing User Data from Database	153
Importing User Data from File	156
Importing User Data from Google	161
Importing User Data Using LDAP	164
Importing User Data from Oracle Identity Analytics (OIA)	168
Importing User Data from Okta	171
Importing User Data from Oracle IDM	174
Importing User Data from SailPoint	177
Importing User Data from Waveset IDM	180
Step 2: Configuring User Import	183
Step 3: Scheduling Job to Run	190
Step 4: Reviewing Imported User Data	193
Peer Groups	196
Why Use Peer Groups?	196
Creating Peer Groups	196
Creating Peer Groups Using Creation Rules	197
Creating Peer Groups using Peer Assignment Rules	203

Activity Data	209
Step 1: Configuring the Datasource	212
Importing Events from Syslog Files	220
Importing Events from a JSON File (Key Value Pairs)	227
Importing Events from an XML File (Key Value Pairs)	236
Importing Events from a Delimited File	245
Importing Events from a Regex File (Capturing Groups)	252
Importing Events from a Database	261
Importing Events from Apache Subversion (SVN)	269
Importing Events from Google Reporting API	275
Importing Events from Office 365	282
Importing Events from Box	290
Importing Events from Amazon Web Services Cloudtrail	300
Importing Events from Sophos	309
Step 2: Parsing and Normalization	317
Step 3: Performing Conditional Actions	326
Step 4: Configuring Identity Attribution	347
Step 5: Reviewing Import Summary	351
Step 6: Running the Job	356
Third Party Intelligence	361
Step 1: Importing Third Party Intelligence from an Existing Connection	362
Step 1: Creating a New Connection	364
Importing TPI from a File	366
Importing TPI from the Web	373
Importing TPI from ThreatStream	380
Importing TPI from ThreatConnect	387
Step 2: Mapping Attributes	393
Step 3: Scheduling the Job	393
Watch Lists	396
Step 1: Configuring the Connection	396
Step 2: Mapping Attributes	404
Step 3: Running the Job	406
Viewing Watch Lists	409

Searching Watchlists in Spotter	411
Lookup Tables	412
Step 1: Creating a New Connection	412
Importing Lookup Data from a File	415
Importing Lookup Data from a Database	421
Step 2: Mapping Attributes	423
Step 3: Running Job	424
Geolocation/Network Map Data	429
Step 1: Importing Geolocation Data from Maxmind	429
Step 2: Importing Network Map Data from a Delimited File	434
Step 3: Running Job	437
Entity Metadata	442
Step 1: Creating a Connection	443
Importing Entity Metadata from a Database	451
Importing Entity Metadata from Qualys	453
Importing Entity Metadata from Tanium	455
Step 2: Configure Attribute Mapping	456
Step 3: Running the Job	457
Access Data	462
Step 1: Selecting the Datasource	463
Importing Access Data	463
Importing from Aveksa	469
Importing from Database	474
Importing from Files	478
Step 2: Configuring the Import	486
Step 3: Running the Job	494
Analytics	500
Behavior Profiles	506
How Behavior Profiles Work in ArcSight UBA	506
Why Monitor Behavior?	506
About Behavior Profiles	506
What are Behavior Profiles?	508
How are Behavior Baselines Established?	508

Creating Behavior Profiles	511
Viewing Behavior Profiles	514
Access Outliers	519
Running Access Outlier Analysis	522
Reviewing Access Outlier Jobs	530
Viewing Access Outlier Results	534
Access Reviews	535
Scheduling Access Review Jobs	537
Reviewing Access Review Jobs	547
Viewing Access Review Results	548
Traffic Analyzer	549
Traffic Analyzer Overview	549
Traffic Analyzer Checks	550
Rare Domain Visited	550
Rare User Agent	551
Detection of possible control avoidance	551
Multiple Protocols used on URL	552
Traffic to Algorithmically Generated Domains (DGA)	553
Detection of beaconing behavior (to possible malicious domains)	555
Detection of beaconing behavior (All proxy traffic)	556
Reference: Threshold configuration	557
Traffic Analyzer Threat Model: Persistent Malware Communication	558
Policy Violations	560
Creating Policies	561
Example Real Time Policy: Check Land Speed	614
Example Directives-Based Policy: Flight Risk User - Job Search	628
Example Behavior-Based Policy: Abnormal amount of data uploads compared to past behavior	641
Example Peer-Based Activity Outlier Policy: Only Member in Peer Group Accessing Application	653
Creating Identity /Access Policies	676
Example Identity Policy: Employees with Upcoming Terminations within 30 Days	689
Example Identity Policy: Part Time Employee	695

Example Access Policy: Accounts with Privileged Access on Active Directory	701
Viewing, Enabling, and Editing Policies	708
Searching Policies using Spotter	713
Conditions	714
Example 1: One Rule	717
Example 2: Multiple Groups with Multiple Rules	719
Operators	723
Threat Modeler	815
Creating a Threat Model for Policies	816
Creating a Threat Model for Threats	822
Importing Threat Models	827
Exporting Threat Models	829
Email Templates	832
Using Email Templates	832
Viewing and Editing Email Templates	832
Adding Email Templates	834
Job Monitor	838
Monitoring Jobs	838
Appendix A: ArcSight UBA Attribute Schema	844
Appendix B: Functions	862
Functions	862
Logical Functions	863
Math Functions	866
Other Functions	869
String Functions	873
Formula	879
Appendix C: Verbose Template Attributes	882
Appendix D: Access Privileges	900

Introduction

This guide provides detailed information about configuring and administering the ArcSight User Behavior Analytics. This guide describes how to integrate ArcSight User Behavior Analytics with other applications in a heterogeneous IT environment. Included in this guide is information about how to integrate with a rich variety of security data including security event logs, user identity data, access privileges, threat intelligence, asset metadata, and netflow data.

Who Should Read This Guide

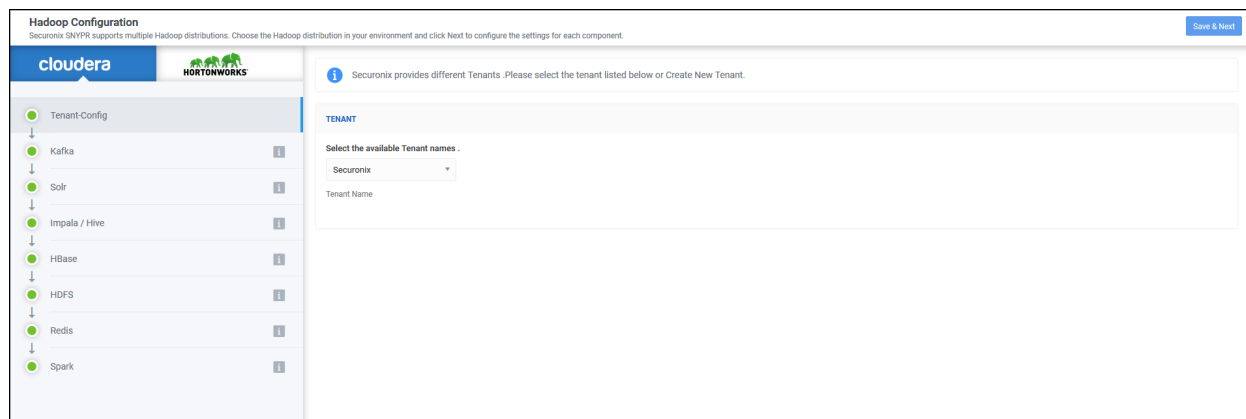
The ArcSight UBA Integration Guide is written for:

- Deployment engineers and service providers who are responsible for integrating ArcSight UBA Risk and Threat Intelligence solution with other IT systems.
- System administrators and service providers who need information about how to monitor and administer the platform at a systems level.
- Compliance officers and IT specialists who need to configure and maintain Risk Management functionality.
- Business managers and other users in a supervisory role who need information about how to use ArcSight UBA to grant employees and partners access to applications, check for policy violations, and manage cases.

Configure Hadoop Settings for ArcSight UBA

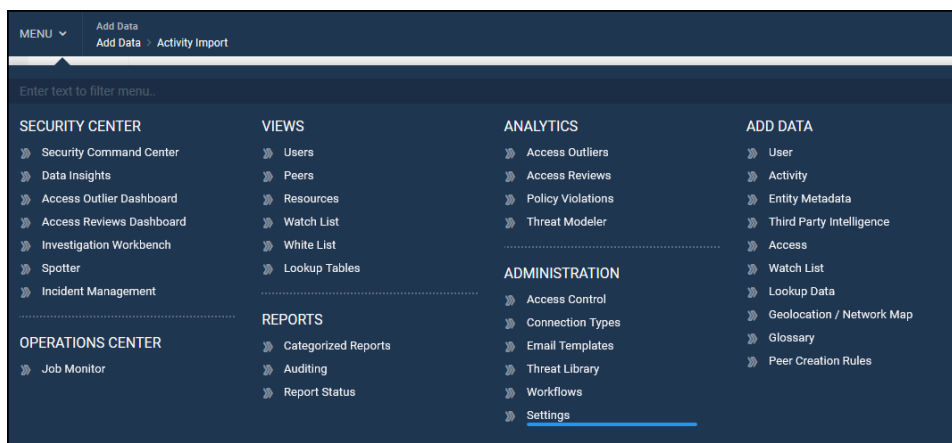
ArcSight UBA leverages Hadoop technologies including Kafka, Solr, Impala/Hive, HBase, HDFS, Redis, and Spark. After integrating Hadoop, you must configure Hadoop settings within the ArcSight UBA application.

When you log in to the ArcSight UBA application for the first time, you will be prompted to configure your Hadoop settings. You can access the Hadoop settings at any time from the Hadoop Settings menu.



To configure the Hadoop settings in ArcSight UBA, complete the following steps:

1. Log in to the application.
2. Navigate to **Menu > Administration > Settings**.



3. Click **Hadoop** from the left navigation panel.



Note: Click the green three bar icon to minimize and maximize the left navigation panel.

4. Select the Hadoop distribution in your environment:

- **Cloudera:** Cloudera, Inc. provides Apache Hadoop-based software, support and services, and training to business customers. Cloudera's open-source Apache Hadoop distribution, CDH (Cloudera Distribution including Apache Hadoop), targets enterprise-class deployments of that technology.
- **Hortonworks:** Hortonworks is a big data software company that develops and supports Apache Hadoop for the distributed processing of large data sets across computer clusters.

5. Click the name of the component you would like to configure.



Note: The circles beside the names of the components indicate the status of completion as follows:

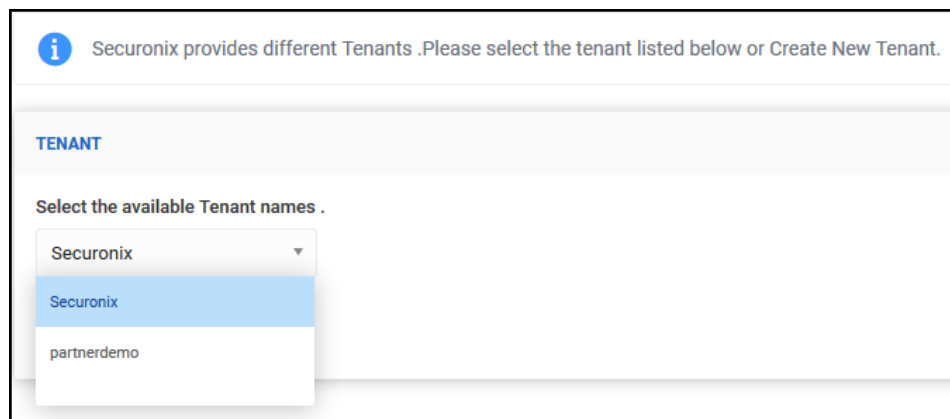
Gray: Not started

Orange: Incomplete or unsuccessfully configured

Green: Successfully configured

Tenant-Config

ArcSight UBA supports a multi-tenant environment in which multiple instances of the application can run in a shared environment within a cluster, either on different servers or on different ports on the same server. To select the tenant ID of the tenant for the current instance of the application, complete the following steps:



1. Select a tenant from the dropdown or **Create a New Tenant**.
2. Click **Save and Next**.

Kafka

Kafka is a distributed publish-subscribe messaging system that is designed to be fast, scalable, and durable. Kafka maintains feeds of messages in topics and consumers read from topics. Since Kafka is a distributed system, topics are partitioned and replicated across multiple nodes. In ArcSight UBA, Kafka plays an important role in publishing and consuming activity data and notifications.

To configure Kafka, follow these steps:

Authentication Type

AUTHENTICATION TYPE

Authentication Type

SSL ▼

The authentication mechanism used to connect.

Broker

1092,snypr-10-0-0-61:9092,snypr-10-0-0-62:9092

The URI for the Kafka Brokers. Format `host:port`, example: `snyper-10-0-3-150.securonix.com,snyper-10-0-3-151.securonix.com,snyper-10-0-3-152.securonix.com:9092`

1. Select **Authentication Type** from dropdown:
 - **NoAuth:** No further action required.
 - **SSL:** Complete the following:
 - **Client SSL Configuration for Console:** Provide the following:
 - Key Password
 - Key Store Location
 - Key Store Password
 - Trust Store Location
 - Trust Store Password
 - **Client SSL Configuration for Cluster:** Provide the following:
 - Key Password
 - Key Store Location
 - Key Store Password
 - Trust Store Location
 - Trust Store Password
 - **Broker Configuration for Console:** Provide the following:

- Key Password
 - Key Store Location
 - Key Store Password
 - Trust Store Location
 - Trust Store Password
 - **Broker SSL Configuration for Cluster:** Provide the following:
 - Key Password
 - Key Store Location
 - Key Store Password
 - Trust Store Location
 - Trust Store Password
2. Enter the URLs of the brokers including port number 9092 using commas (,) to separate entries.
Example: ArcSight-10-0-0-150:9092,ArcSight-10-0-0-151:9092,ArcSight-10-0-0-152:9092.



Note: You can find the URLs of the Kafka brokers you set up during Hadoop integration in Cloudera Manager by navigating to **Kafka > Instances**.

Topic Details

TOPIC DETAILS

Zookeeper Quorum

10.0.0.63:2181,10.0.0.64:2181,10.0.0.65:2181

Zookeeper quorum used for kafka. Example: 10.0.3.185:2181,10.0.3.186:2181,10.0.3.189:2181

Preview Topic

DeltaSNYPR6-Preview

Preview Topic used while configuring Ingestor Data Source.

Enriched Topic

DeltaSNYPR6Resource-Enriched

The topic name for the Enriched Events. Make sure that this topic is created on Kafka. example: Securonix-EnrichedEvents

Raw Topic

DeltaSNYPR6Resource-Raw

The topic name for the Raw Events. Make sure that this topic is created on Kafka. example: Securonix-RawEvents

Configuration Messages Topic

DeltaSNYPR6-Control

Configuration changes from user interface are communicated to SPARK applications using this topic. example: Securonix-UIControlFlags

Indexer Counts Topic

DeltaSNYPR6-IndexerCount

The Indexer SPARK application publishes event counts per Resource Group. example: Securonix-IndexedEventCounts

1. Enter **Zookeeper Quorum** URLs using commas (,) to separate entries. Example: ArcSight-10-0-0-150:2181,ArcSight-10-0-0-151:2181,ArcSight-10-0-0-152:2181.



Note: Default port is 2181.



Note: You can find the URLs for Zookeeper in Cloudera Manager by navigating to **Zoo-keeper > Instances**.

2. Enter the names of the Kafka topics you created when preparing the infrastructure:
 - a. **Preview Topic**
 - b. **Access Topic**
 - c. **Users Topic**
 - d. **Enriched Topic**
 - e. **Raw Topic**
 - f. **Configuration Messages Topic**
 - g. **Indexer Counts Topic**
 - h. **Job Tracker Topic**
 - i. **Log Message Topic**
 - j. **Violations Topic**
 - k. **Tier2 Topic**
 - l. **AEE Tier2 Topic**

To find the names of topics you created, use the following command from a command-line interface:

- a.

```
[root@<ipaddress> ~]# kafka-topics -list --zookeeper <ipad-  
dress>:2181
```


 Example:

```
[root@10-0-0-90 ~]# kafka-topics -list --zookeeper  
10.0.0.90:2181
```

Kafka Message Settings

1. Complete the following information:

KAFKA MESSAGE SETTINGS

Delimiter

The delimited for Raw events. example |

Publish Threshold

The number of events it publishes at one go

Max Message Size

Max Message Size for Kafka Topic

Batch Size

Batch size in bytes

Linger

If we have fewer messages than batch size accumulated for partition we will 'linger' for the specified time waiting for more records to publish.Specify Linger duration in milliseconds.

Compression Type

GZIP

Select compression type for all data generated by the producer.

Failed Events Folder

If kafka failed to publish events then these events will be moved to failed events folder.

Failed Events Folder Size in Bytes

Storage space for failed Events in Bytes.

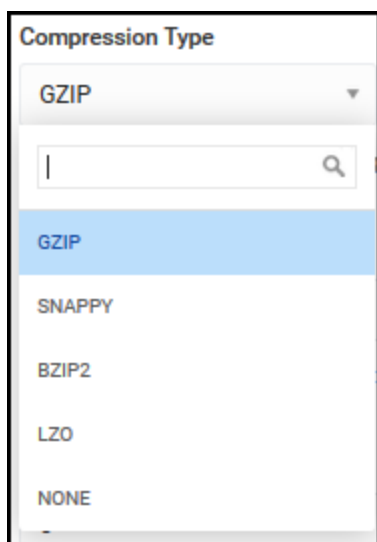
Interval to check failed events

- a. **Delimiter:** Specify the delimiter for raw events. Example |.
- b. **Publish Threshold:** Specify the number of events the application publishes at one time. Default 20000.
- c. **Max Message Size:** Specify the max message size for Kafka Topics.
- d. **Batch Size:** Specify the batch size in bytes. Default 16384.
- e. **Linger:** Specify the linger duration in milliseconds. Default 1.

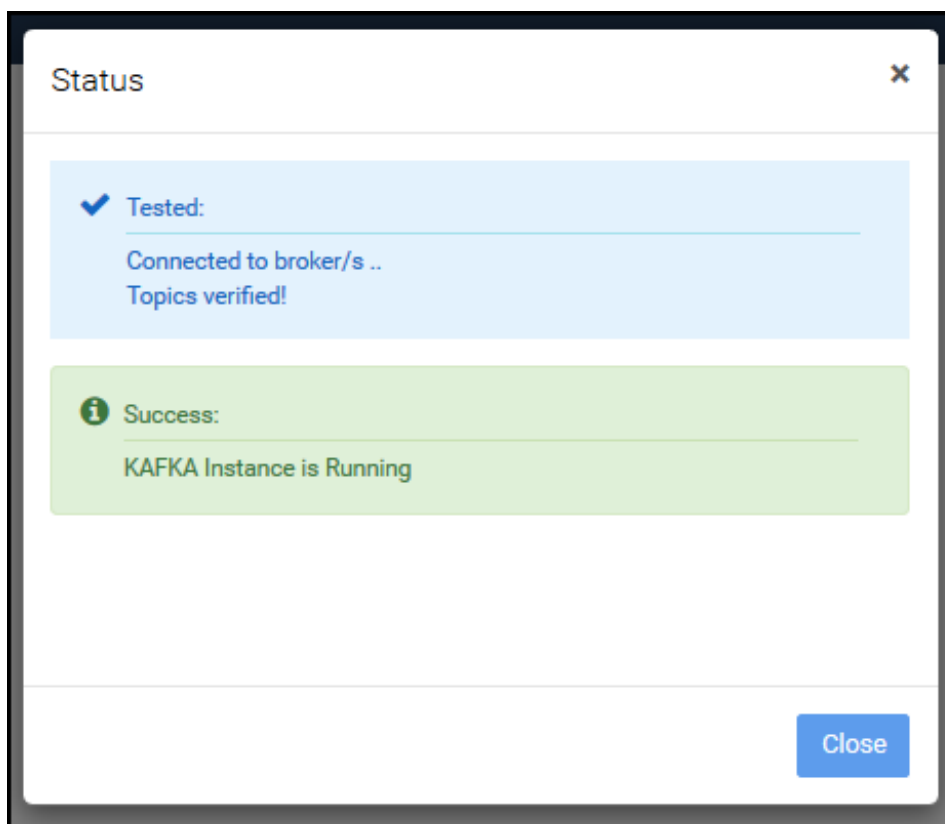


Note: If you have fewer messages than batch size accumulated for partition, the application will "linger" for the specified time waiting for more records to publish.

- f. **Compression Type:** Select the compression type for data generated by the producer from the dropdown:



- g. **Failed Events Folder:** Enter a folder name if you would like to move the events Kafka failed to publish to a specific location. Default none.
 - h. **Failed Events Folder Size in Bytes:** Enter the storage space for failed events in bytes.
 - i. **Interval to check failed events:** Specific an interval in milliseconds to check failed events. Default 0.
 - j. **Enrichment Compression Batch Size:** Specify a value. Recommended: 10000.
 - k. **Raw Compression Batch Size:** Specify a value. Recommended: 10000.
2. Click **Test** to verify connection and check status.



3. Click **Save and Next** when status is successful.

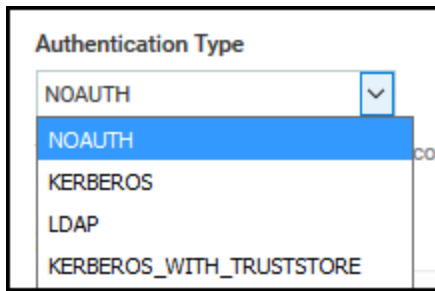
Solr

Solr is a popular search platform. It can index and search activity data and return recommendations for related content based on the search query's taxonomy. In ArcSight UBA, Solr is used in Spotter to create complex queries and interactive visualization.

To configure Solr, complete the following steps:

Authentication Type

1. Specify the **Authentication Type** from the dropdown.



The image shows a dropdown menu titled "Authentication Type". The menu is open, displaying four options: "NOAUTH", "KERBEROS", "LDAP", and "KERBEROS_WITH_TRUSTSTORE". The "NOAUTH" option is currently selected and highlighted in blue. A small downward arrow icon is visible on the right side of the dropdown box.

- a. **NoAuth:** Proceed without entering additional information.
- b. **Kerberos:** Enter the following information:

Authentication Type

KERBEROS ▼

The authentication mechanism used to connect.

Host FQDN

The fully qualified domain name of the host.

Realm

A realm is where the kerberos database is stored. The realm lives on one computer (KDC) and can have read-only slave servers (kinda' like a cluster).

Key Tab Path

A keytab is a file containing pairs of Kerberos principals and encrypted keys (which are derived from the Kerberos password).

Principal

A principal is an identity that Kerberos is able to authenticate. Principals may represent users, network hosts, or network services.

Jaas Conf File Path

Service Name

Authentication Mechanism

- **Host FQDN:** Enter the fully qualified domain name of the host.
 - **Realm:** Specify the realm where the Kerberos database is stored. The realm lives on one computer (KDC) and can have read-only slave servers (similar to a cluster).
 - **Key Tab Path:** Enter a key tab path. A key tab is a file containing pairs of Kerberos principals and encrypted keys, which are derived from the Kerberos password.
 - **Principal:** Enter a principal. A principal is an identity that Kerberos is able to authenticate. Principals may represent users, network hosts, or network services.
 - **Jaas Conf File Path:** Enter the Jaas Conf file path.
 - **Service Name:** Specify a service name.
 - **Authentication Mechanism:** Specify an authentication mechanism.
- c. **LDAP:** Enter the following information:

Authentication Type

LDAP

▼

The authentication mechanism used to connect.

Username

[help.snyper.settings.ldap.username](#)

Password

[help.snyper.settings.ldap.password](#)

- **Username:** Specify the user name. For help, see [help.snypr.settings.ldap.username](#).
 - **Password:** Specify the LDAP password. For help, see [help.snypr-settings.ldap.password](#).
- d. **Kerberos with Trust Store:** Enter the following information:

Authentication Type
 KERBEROS_WITH_TRUSTSTORE ▾
 The authentication mechanism used to connect.

Host FQDN

 The fully qualified domain name of the host.

Key Tab Path

 A keytab is a file containing pairs of Kerberos principals and encrypted keys (which are derived from the Kerberos password).

Principal

 A principal is an identity that Kerberos is able to authenticate. Principals may represent users, network hosts, or network services.

Realm

 A realm is where the kerberos database is stored. The realm lives on one computer (KDC) and can have read-only slave servers.

Service Name

 The service name of the server. For example, "impala" for Impala server.

Trust Store Path

 @Trust Store Path

Trust Store Password

 @Trust Store Password

Jaas Conf File Path

SSL Value

- **Host FQDN:** Enter the fully qualified domain name of the host.
- **Key Tab Path:** Enter a key tab path. A key tab is a file containing pairs of Kerberos principals and encrypted keys, which are derived from the Kerberos password.
- **Principal:** Enter a principal. A principal is an identity that Kerberos is able to authenticate. Principals may represent users, network hosts, or network services.
- **Realm:** Specify the realm where the Kerberos database is stored. The realm lives on one computer (KDC) and can have read-only slave servers (similar to a cluster).

- **Service Name:** Specify a service name. Example: impala.
 - **Trust Store Path:** Enter a trust store path.
 - **Trust Store Path Password:** Enter the trust store password.
 - **Jaas Conf File Path:** Enter the Jaas Conf file path.
 - **SSL Value:** Enter the SSL value.
 - **Authentication Mechanism:** Specify an authentication mechanism.
2. Enter **ZK Quorum:** URLs using commas (,) to separate entries.
Append **/solr** to the last URL after the port number.
Example: 10.0.0.62:2181,10.0.0.61:2181,10.0.0.60:2181/solr

AUTHENTICATION TYPE

Authentication Type

NOAUTH

The authentication mechanism used to connect.

ZK Quorum

search1.securonix.net:2181,search2.securonix.i

Zookeeper quorum used for Solr. e.g :[snyper-10-0-3-150.securonix.com,snyper-10-0-3-151.securonix.com,snyper-10-0-3-152.securonix.com:2181/solr]

Approximate EPS

1000

Please provide approximate EPS to get suggestion for activity and violation core. Suggested shards will be reverted to number of nodes in solrcloud if EPS given is high



Note: Default port is 2181.



Note: You can find the URL of Zookeeper in Cloudera Manager by navigating to **Zoo-keeper > Instances**.

Collection Details

In Solr, data is indexed into collections, which allow for faster results from search queries in Spotter. The collections are partitioned into individual chunks of data called shards.

For more information about how to search data collections in ArcSight UBA, refer to the ArcSight UBA User Guide.

The shards and their replication factors are configured in this section.

1. Specify a unique **Name** for each data collection:

- Lookup
- Watchlist
- Control Core
- IP Mapping
- TPI
- Entity Metadata
- Risk Score
- Activity
- Violation
- Daily Violations Summary
- Entity Relation
- Users
- Violation Control Core
- White List

COLLECTION DETAILS			
Collections			
Type	Name	No Of Shards	Replication Factor
LOOKUP	deltasnypr6-lookup	3	2
WATCHLIST	deltasnypr6-watchlist	3	2
CONTROLCORE	deltasnypr6-controlcore	3	2
IPMAPPING	deltasnypr6-ipmapping	3	2
TPI	deltasnypr6-tpi	3	2
ENTITYMETADATA	deltasnypr6-entitymetadata	3	2
RISKSCORE	deltasnypr6-riskscore	3	2
ACTIVITY	deltasnypr6-activity	6	2
VIOLATION	deltasnypr6-violation	6	2
DAILYVIOLATIONSUMMARY	deltasnypr6-dailyviolations	3	2
ENTITYRELATION	deltasnypr6-entityrelation	3	2
USERS	deltasnypr6-users	3	2
VIOLATIONCONTROLCORE	deltasnypr6-violationcontro	3	2
WHITELIST	deltasnypr6-whitelist	3	2

2. Specify the **No(number) of Shards** into which to split the data within each collection.

Note: A shard refers to an individual partition of data within Solr.

3. Enter a **Replication Factor** to specify the number of times to replicate each shard within each collection.

Solr Additional Settings

1. Enter the following information:
 - **Batch size:** Specify the number of events indexed during a single to commit to Solr during indexing. Default 1000.
 - **Inter Batch Sleep:** Specify the duration in milliseconds to wait before retrying index for a failed batch. Default 5.
 - **Percentage of Indexing Servers:** Use the dropdown to specify the percentage of indexing servers to be used for activity indexing. Default 70.
 - **Enable Multi Collection Indexing:** Select **Yes** or **No**. If enabled, multiple collections will be created by the event indexing job whenever the soft threshold is reached. Default **Yes**.
 - **Collection Soft Threshold:** Specify the size of the document each collection should have if multiple collection is enabled. This is only a soft threshold; each collection will have documents near to the configured value. Default 100,000,000.
 - **Collection Count Threshold:** Specify the collection count after which the collections gets unloaded. For example, if 100 activity collections are created and threshold is set to 50, the first 50 activity collections are unloaded from Solr.
 - **Replication Threshold:** Specify the collection count after which the replication is reduced. For example, if there are 100 activity collections and the replication threshold is set to 5, the older 95 collection replications are reduced.
 - **Solr Root Directory:** The root directory where the frozen Solr indexes are stored. For HDFS, it will be /solr. For disk-based, it should be the same as solr.frozen.bucket configured in Solr.
 - **Solr Service Username:** Specify the username of the Solr service. For HDFS, provide a username who has write access to /solr directory. For disk-based, provide the gateway node solr username.
 - **Solr Service Gateway Node Host:** Specify the SSH Hostname of the Solr Gateway node. This is only applicable for disk-based indexes.
 - **Solr Service Gateway Node Password:** Specify the SSH Password of the Solr Gateway node. This is only applicable for disk-based indexes.
 - **Solr Service Gateway Node SSH port:** Specify the SSH port of the Solr Gateway node. This is only applicable for disk-based indexes.
 - **Create Force Collection:** Select from the drop down and click **Force Create Collection**. This allows you to create a collection forcefully from the UI whenever new cores are added to

Solr.

2. Click **Test** to verify connection and test status.
3. Click **Save and Next** when status is successful.

Impala/Hive

Impala is a massively scalable parallel processing (MPP) SQL query engine for data stored in a computer cluster running Apache Hadoop. Impala brings scalable parallel database technology to Hadoop, enabling users to issue low-latency SQL queries to data stored in HDFS and Apache HBase without requiring data movement or transformation.

Apache Hive is a data warehouse software project built on top of Apache Hadoop for providing data summarization, query, and analysis. Hive gives an SQL-like interface to query data stored in various databases and file systems that integrate with Hadoop.

To configure Impala/Hive, follow these steps:

Authentication and Connection Details

Authentication Type

NOAUTH

▼

The authentication mechanism used to connect.

Connection URL

127.0.0.1:21050

Enter the Connection URL of Impala. Format- sobdin244.securonix.com:21050

Database

snypr

Enter the impala database name to use.

Table Prefix

securonixresource

Table prefix name to use for resources. Example: securonixresource

JDBC Driver

com.cloudera.impala.jdbc4.Driver

JDBC Driver name e.g :com.cloudera.impala.jdbc4.Driver

Partitions Per Page

0

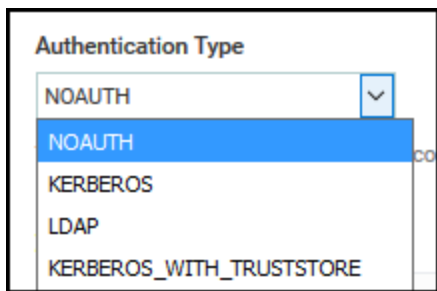
@partitionsPerPage

Hive Url

com.cloudera.impala.jdbc4.Driver

Hive Url e.g : jdbc:hive2://ipaddress:10000/database name

1. Specify the **Authentication Type** from the dropdown.



The image shows a dropdown menu titled "Authentication Type". The menu is open, displaying four options: "NOAUTH", "KERBEROS", "LDAP", and "KERBEROS_WITH_TRUSTSTORE". The "NOAUTH" option is currently selected and highlighted in blue. A small downward arrow icon is visible on the right side of the dropdown box.

- a. **NoAuth:** Proceed without entering additional information.
- b. **Kerberos:** Enter the following information:

Authentication Type

KERBEROS ▼

The authentication mechanism used to connect.

Host FQDN

The fully qualified domain name of the host.

Realm

A realm is where the kerberos database is stored. The realm lives on one computer (KDC) and can have read-only slave servers (kinda' like a cluster).

Key Tab Path

A keytab is a file containing pairs of Kerberos principals and encrypted keys (which are derived from the Kerberos password).

Principal

A principal is an identity that Kerberos is able to authenticate. Principals may represent users, network hosts, or network services.

Jaas Conf File Path

Service Name

Authentication Mechanism

- **Host FQDN:** Enter the fully qualified domain name of the host.
 - **Realm:** Specify the realm where the Kerberos database is stored. The realm lives on one computer (KDC) and can have read-only slave servers (similar to a cluster).
 - **Key Tab Path:** Enter a key tab path. A key tab is a file containing pairs of Kerberos principals and encrypted keys, which are derived from the Kerberos password.
 - **Principal:** Enter a principal. A principal is an identity that Kerberos is able to authenticate. Principals may represent users, network hosts, or network services.
 - **Jaas Conf File Path:** Enter the Jaas Conf file path.
 - **Service Name:** Specify a service name.
 - **Authentication Mechanism:** Specify an authentication mechanism.
- c. **LDAP:** Enter the following information:

Authentication Type

LDAP

▼

The authentication mechanism used to connect.

Username

[help.snyper.settings.ldap.username](#)

Password

[help.snyper.settings.ldap.password](#)

- **Username:** Specify the user name. For help, see [help.snypr.settings.ldap.username](#).
 - **Password:** Specify the LDAP password. For help, see [help.snypr-settings.ldap.password](#).
- d. **Kerberos with Trust Store:** Enter the following information:

Authentication Type
 KERBEROS_WITH_TRUSTSTORE ▾

The authentication mechanism used to connect.

Host FQDN

The fully qualified domain name of the host.

Key Tab Path

A keytab is a file containing pairs of Kerberos principals and encrypted keys (which are derived from the Kerberos password).

Principal

A principal is an identity that Kerberos is able to authenticate. Principals may represent users, network hosts, or network services.

Realm

A realm is where the kerberos database is stored. The realm lives on one computer (KDC) and can have read-only slave servers.

Service Name

The service name of the server. For example, "impala" for Impala server.

Trust Store Path

@Trust Store Path

Trust Store Password

@Trust Store Password

Jaas Conf File Path

SSL Value

- **Host FQDN:** Enter the fully qualified domain name of the host.
- **Key Tab Path:** Enter a key tab path. A key tab is a file containing pairs of Kerberos principals and encrypted keys, which are derived from the Kerberos password.
- **Principal:** Enter a principal. A principal is an identity that Kerberos is able to authenticate. Principals may represent users, network hosts, or network services.
- **Realm:** Specify the realm where the Kerberos database is stored. The realm lives on one computer (KDC) and can have read-only slave servers (similar to a cluster).

- **Service Name:** Specify a service name.
 - **Trust Store Path:** Enter a trust store path.
 - **Trust Store Path Password:** Enter the trust store password.
 - **Jaas Conf File Path:** Enter the Jaas Conf file path.
 - **SSL Value:** Enter the SSL value.
 - **Authentication Mechanism:** Specify an authentication mechanism.
2. Enter the **Connection URL** of Impala using default port 21050.
 Note: You can find the Connection URL of Impala in Cloudera Manager by navigating to **Impala > Instances**.
 3. Enter the **Database** name.

To find the Database name created during Hadoop integration, log in to the Impala shell and use the following query:

```
[<ipaddress>.securonix.com:21000] > show databases;
```

Example:

```
[10-0-0-90.securonix.com:21000]: # su - impala $ impala-shell >
show databases;
[10-0-0-90.securonix.com:21000]: # su - impala $ impala-shell>
quit;
```
 4. Specify the **Table Prefix** to use for resources. Example: securonixresource.
 5. Specify the **JDBC Driver**. Example: com.cloudera.impala.jdbc4.driver.
 6. Specify the number of **Partitions per Page**. Default 0.
 7. Specify the **Impala/Hive URL**. Example: com.cloudera.impala.jdbc4.Driver.
 8. Specify the **Impala/Hive Username** and **Impala/Hive Password**.
 9. Click **Test** to verify connection and test status.
 10. Click **Save and Next** when status is successful.

HBase

Apache HBase is an open-source non-relational (NoSQL) database that runs on top of HDFS and provides real-time read/write access to those large datasets. Hbase scales linearly to handle large datasets with billions of rows and millions of columns, and it easily combines data sources that use a wide variety of different structures and schemas.

To configure HBase, complete the following steps:

Authentication and Connection Details

Authentication Type

NOAUTH

The authentication mechanism used to connect.

Name Space

securonix

Enter namespace name for HBase, example: securonix

Split Tables

Yes

Regions

3

Resources

file:///etc/hbase/conf/hbase-site.xml

Resources required to connect to HBASE example: file:///etc/hbase/conf/hbase-site.xml and example: file:///etc/hbase/conf/core-site.xml

Resources

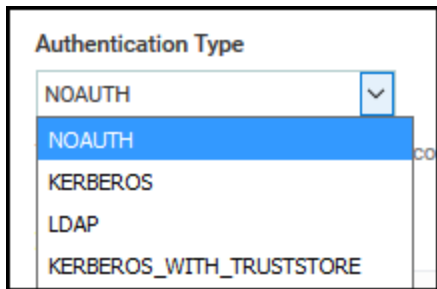
file:///etc/hbase/conf/core-site.xml

Resources required to connect to HBASE example: file:///etc/hbase/conf/hbase-site.xml and example: file:///etc/hbase/conf/core-site.xml

Test

Save

1. Specify the **Authentication Type** from the dropdown.



The image shows a dropdown menu titled "Authentication Type". The menu is open, displaying four options: "NOAUTH", "KERBEROS", "LDAP", and "KERBEROS_WITH_TRUSTSTORE". The "NOAUTH" option is currently selected and highlighted in blue. A small downward arrow icon is visible on the right side of the dropdown box.

- a. **NoAuth:** Proceed without entering additional information.
- b. **Kerberos:** Enter the following information:

Authentication Type

KERBEROS ▼

The authentication mechanism used to connect.

Host FQDN

The fully qualified domain name of the host.

Realm

A realm is where the kerberos database is stored. The realm lives on one computer (KDC) and can have read-only slave servers (kinda' like a cluster).

Key Tab Path

A keytab is a file containing pairs of Kerberos principals and encrypted keys (which are derived from the Kerberos password).

Principal

A principal is an identity that Kerberos is able to authenticate. Principals may represent users, network hosts, or network services.

Jaas Conf File Path

Service Name

Authentication Mechanism

- **Host FQDN:** Enter the fully qualified domain name of the host.
 - **Realm:** Specify the realm where the Kerberos database is stored. The realm lives on one computer (KDC) and can have read-only slave servers (similar to a cluster).
 - **Key Tab Path:** Enter a key tab path. A key tab is a file containing pairs of Kerberos principals and encrypted keys, which are derived from the Kerberos password.
 - **Principal:** Enter a principal. A principal is an identity that Kerberos is able to authenticate. Principals may represent users, network hosts, or network services.
 - **Jaas Conf File Path:** Enter the Jaas Conf file path.
 - **Service Name:** Specify a service name.
 - **Authentication Mechanism:** Specify an authentication mechanism.
- c. **LDAP:** Enter the following information:

Authentication Type

LDAP

▼

The authentication mechanism used to connect.

Username

[help.snyper.settings.ldap.username](#)

Password

[help.snyper.settings.ldap.password](#)

- **Username:** Specify the user name. For help, see [help.snypr.settings.ldap.username](#).
 - **Password:** Specify the LDAP password. For help, see [help.snypr-settings.ldap.password](#).
- d. **Kerberos with Trust Store:** Enter the following information:

Authentication Type
 KERBEROS_WITH_TRUSTSTORE ▾
 The authentication mechanism used to connect.

Host FQDN

 The fully qualified domain name of the host.

Key Tab Path

 A keytab is a file containing pairs of Kerberos principals and encrypted keys (which are derived from the Kerberos password).

Principal

 A principal is an identity that Kerberos is able to authenticate. Principals may represent users, network hosts, or network services.

Realm

 A realm is where the kerberos database is stored. The realm lives on one computer (KDC) and can have read-only slave servers.

Service Name

 The service name of the server. For example, "impala" for Impala server.

Trust Store Path

 @Trust Store Path

Trust Store Password

 @Trust Store Password

Jaas Conf File Path

SSL Value

- **Host FQDN:** Enter the fully qualified domain name of the host.
- **Key Tab Path:** Enter a key tab path. A key tab is a file containing pairs of Kerberos principals and encrypted keys, which are derived from the Kerberos password.
- **Principal:** Enter a principal. A principal is an identity that Kerberos is able to authenticate. Principals may represent users, network hosts, or network services.
- **Realm:** Specify the realm where the Kerberos database is stored. The realm lives on one computer (KDC) and can have read-only slave servers (similar to a cluster).

- **Service Name:** Specify a service name.
 - **Trust Store Path:** Enter a trust store path.
 - **Trust Store Path Password:** Enter the trust store password.
 - **Jaas Conf File Path:** Enter the Jaas Conf file path.
 - **SSL Value:** Enter the SSL value.
 - **Authentication Mechanism:** Specify an authentication mechanism.
2. Enter the **Name Space** created during Hadoop integration. Example: securonix.
To find the Name Space created during Hadoop integration, log in to the HBase shell and use the following command:


```
hbase(main):002:0: # hbase shell > list_namespace
hbase(main):002:0: # hbase shell > quit
```
 3. Use slider to select **Yes** or **No** to **Split Tables** in Hbase. Default **Yes**.
 4. Specify the number of **Regions**. Default 3.
 5. Specify the Resources required to connect to HBase. Example: file:///etc/hbase/conf/hbase-site.xml
 6. Click **Test** to verify connection and test status.
 7. Click **Save** when status is successful.

HDFS

The Hadoop Distributed File System (HDFS) is designed to store very large data sets reliably and to stream those data sets at high bandwidth to user applications. HDFS stores file system metadata and application data separately. HDFS stores metadata on a dedicated server called the NameNode. Applications data are stored on other servers called DataNodes.

To configure HDFS, complete the following steps:

Authentication and Connection Details

Authentication Type

NOAUTH ▼

The authentication mechanism used to connect.

HDFS Site

file:///etc/hadoop/conf/hdfs-site.xml

HDFS site required to connect to HDFS example: file:///etc/hadoop/conf/hdfs-site.xml

Core Site

file:///etc/hadoop/conf/core-site.xml

HDFS Core site required to connect to HDFS example: file:///etc/hadoop/conf/core-site.xml

Cluster HDFS Site

file:///etc/hadoop/conf/hdfs-site.xml

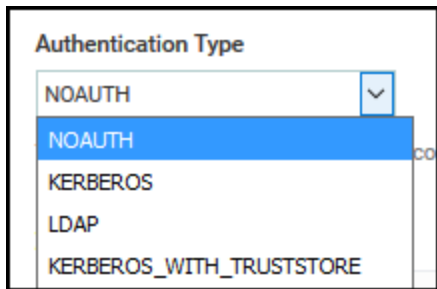
HDFS Cluster site required to connect to HDFS Cluster example: file:///etc/hadoop/conf/hdfs-site.xml

Cluster Core Site

file:///etc/hadoop/conf/core-site.xml

HDFS Cluster Core site required to connect to HDFS Cluster example: file:///etc/hadoop/conf/core-site.xml

1. Specify the **Authentication Type** from the dropdown.



The image shows a dropdown menu titled "Authentication Type". The menu is open, displaying four options: "NOAUTH", "KERBEROS", "LDAP", and "KERBEROS_WITH_TRUSTSTORE". The "NOAUTH" option is currently selected and highlighted in blue. A small downward arrow icon is visible on the right side of the dropdown box.

- a. **NoAuth:** Proceed without entering additional information.
- b. **Kerberos:** Enter the following information:

Authentication Type

KERBEROS

The authentication mechanism used to connect.

Host FQDN

The fully qualified domain name of the host.

Realm

A realm is where the kerberos database is stored. The realm lives on one computer (KDC) and can have read-only slave servers (kinda' like a cluster).

Key Tab Path

A keytab is a file containing pairs of Kerberos principals and encrypted keys (which are derived from the Kerberos password).

Principal

A principal is an identity that Kerberos is able to authenticate. Principals may represent users, network hosts, or network services.

Jaas Conf File Path

Service Name

Authentication Mechanism

- **Host FQDN:** Enter the fully qualified domain name of the host.
 - **Realm:** Specify the realm where the Kerberos database is stored. The realm lives on one computer (KDC) and can have read-only slave servers (similar to a cluster).
 - **Key Tab Path:** Enter a key tab path. A key tab is a file containing pairs of Kerberos principals and encrypted keys, which are derived from the Kerberos password.
 - **Principal:** Enter a principal. A principal is an identity that Kerberos is able to authenticate. Principals may represent users, network hosts, or network services.
 - **Jaas Conf File Path:** Enter the Jaas Conf file path.
 - **Service Name:** Specify a service name.
 - **Authentication Mechanism:** Specify an authentication mechanism.
- c. **LDAP:** Enter the following information:

Authentication Type

LDAP

▼

The authentication mechanism used to connect.

Username

[help.snyper.settings.ldap.username](#)

Password

[help.snyper.settings.ldap.password](#)

- **Username:** Specify the user name. For help, see [help.snypr.settings.ldap.username](#).
 - **Password:** Specify the LDAP password. For help, see [help.snypr-settings.ldap.password](#).
- d. **Kerberos with Trust Store:** Enter the following information:

Authentication Type
 KERBEROS_WITH_TRUSTSTORE ▾
 The authentication mechanism used to connect.

Host FQDN

 The fully qualified domain name of the host.

Key Tab Path

 A keytab is a file containing pairs of Kerberos principals and encrypted keys (which are derived from the Kerberos password).

Principal

 A principal is an identity that Kerberos is able to authenticate. Principals may represent users, network hosts, or network services.

Realm

 A realm is where the kerberos database is stored. The realm lives on one computer (KDC) and can have read-only slave servers.

Service Name

 The service name of the server. For example, "impala" for Impala server.

Trust Store Path

 @Trust Store Path

Trust Store Password

 @Trust Store Password

Jaas Conf File Path

SSL Value

- **Host FQDN:** Enter the fully qualified domain name of the host.
- **Key Tab Path:** Enter a key tab path. A key tab is a file containing pairs of Kerberos principals and encrypted keys, which are derived from the Kerberos password.
- **Principal:** Enter a principal. A principal is an identity that Kerberos is able to authenticate. Principals may represent users, network hosts, or network services.
- **Realm:** Specify the realm where the Kerberos database is stored. The realm lives on one computer (KDC) and can have read-only slave servers (similar to a cluster).

- **Service Name:** Specify a service name.
 - **Trust Store Path:** Enter a trust store path.
 - **Trust Store Path Password:** Enter the trust store password.
 - **Jaas Conf File Path:** Enter the Jaas Conf file path.
 - **SSL Value:** Enter the SSL value.
 - **Authentication Mechanism:** Specify an authentication mechanism.
2. Specify the **HDFS Site**. HDFS site is required to connect to HDFS.
Example: file:///etc/hadoop/conf/hdfs-site.xml.
 3. Specify the **Core Site**. The Core site is required to connect to HDFS.
Example: file:///etc/hadoop/conf/core-site.xml.
 4. Specify the **Cluster HDFS Site**. The Cluster HDFS Site is required to connect to HDFS Cluster.
Example: file:///etc/hadoop/conf/hdfs-site.xml.
 5. Specify the **Cluster Core Site**. The Cluster Core Site is required to connect to HDFS Cluster.
Example: file:///etc/hadoop/conf/core-site.xml.

HDFS Connection Details

Username

User name of HDFS

Working Directory

Working Directory

Product Directory

Product Directory

HDFS Directory for storing UnParsed Events

The path to the directory in HDFS where all unparsed events are stored Example: /user/securonix/unparsed

HDFS Directory for storing whitelists/temporary files for analyzing Proxy Events

The root path of directory in HDFS for all Proxy data storage

HDFS Directory for storing Violations

The path to the directory in HDFS where all violations are stored

6. Specify the **Username** of HDFS.
7. Specify the **Working Directory** created within the Service Account Folder for ArcSight UBA during Hadoop integration. Example: /user/securonix.
8. Specify the **Product Directory** created during Hadoop integration. Example: snypr.
10. Specify the **HDFS Directory for storing whitelists/temporary files for analyzing Proxy**

Events. Example: ProxyEvents.


10. Specify the **HDFS Directory for storing whitelists/temporary files for analyzing Proxy Events.** Example: ProxyEvents.
11. Specify the **HDFS Directory for storing Violations.** Example: Violations.
12. Click **Test** to verify connection and test status.
13. Click **Save and Next** when status is successful.

Redis

Redis is an open-source software project that implements data structure servers. It is networked and in-memory, and it stores keys with optional durability.

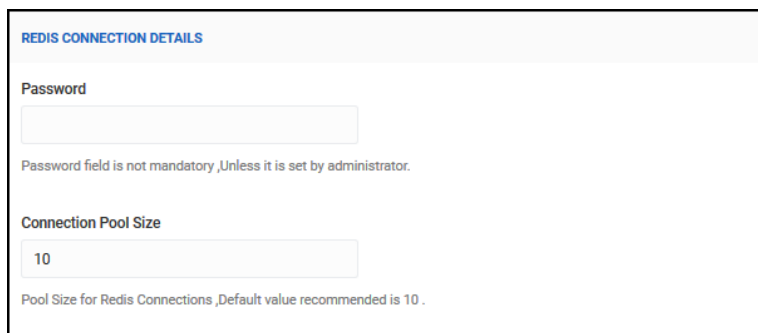
To configure Redis, complete the following steps:

Redis Nodes Details



1. Enter the IP Address or Hostname with port for Redis Inmemory-DB connection in **Node for Redis.** Example : 192.168.1.102:6379.
2. Click **Add Node** to add additional nodes.

Redis Connection Details



1. Specify a **Password** if set by the administrator.
2. Specify a **Connection Pool** size for Redis connections. Recommended default: 10.
3. Click **Test** to verify connection and test status.
4. Click **Save and Next** when status is successful.

Spark

The main feature of Spark is its in-memory cluster computing that increases the processing speed of an application. Spark is designed to cover a wide range of workloads such as batch applications, iterative algorithms, interactive queries, and streaming. In ArcSight UBA, Spark is used in ingestion, indexing, and analytics algorithms.

To configure Spark, complete the following steps:

Spark Details

SPARK DETAILS

Spark Defaults

Spark Defaults required to run Spark example: /etc/spark/conf/spark-defaults.conf

Enable Kerberos

☐ NO

Kerberos Enabled

Yarn Master IP

Yarn Master Ip e.g : 10.0.3.155

Yarn Site

Path of yarn-site.xml file. e.g. file:///etc/hadoop/conf/yarn-site.xml

1. Specify the **Spark Defaults**. The Spark Defaults are required to run Spark. Example: /etc/spark/conf/spark-defaults.conf.
2. Use the slider to **Enable Kerberos**.
 - If **Yes**: Enter **KeyTab Path** for connection to Yarn Master server. Example: /Securionix/securionix_home/security/securionix.keytab.
 - If **No**: Proceed without entering additional information.
3. Specify the **Yarn Master IP**.



Note: To find the Yarn Master IP, use Cloudera Manager to navigate to **Yarn > Instances**.
The Yarn Master IP corresponds to the ResourceManager (Active) IP.

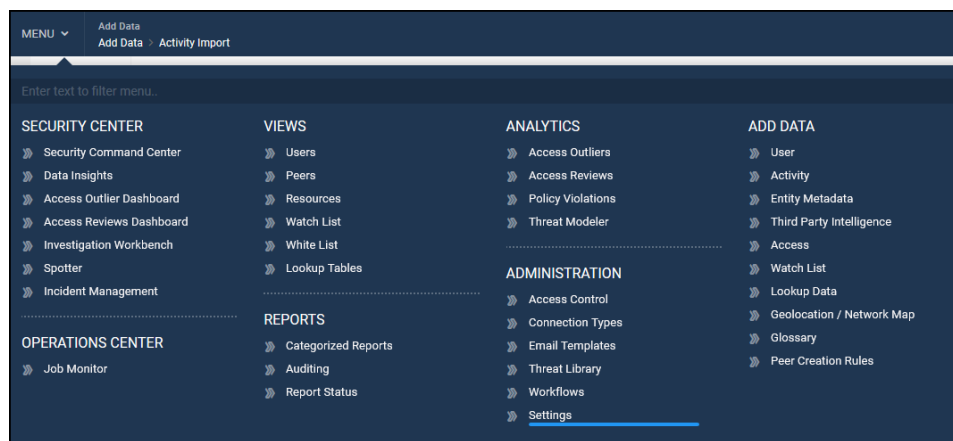
4. Specify the **SSH Port** for the Yarn Master server. Default 22.
5. Specify the **SSH UserName**. Example: securonix.
6. Specify the **SSH Password**.
7. Specify the path of the **Yarn Site** xml file. Example: /etc.hadoop/conf/yarn-site.xml.
8. Click **Save and Next**.

Settings

ArcSight UBA settings are configured from the Administration menu.

Configuring the Application

To customize ArcSight UBA settings, navigate to **Menu > Administration > Settings**.



Application Settings

On the Application Settings page, configure the following options:

General Settings

From the General Settings option, you can configure the following information:

GENERAL SETTINGS

Application Time zone

CST6CDT ▼

Select time zone of the application server.

Database Time zone

CST6CDT ▼

Select time zone of the database.

Date Format

MM/dd/yyyy ▼

Select the date format to be used through out the application.

Session Timeout

36000

Enter period in seconds after which the session expires due to inactivity.

Web Services

YES ☒

Enable the application to use web services.

Token Required For Web Services?

☐ NO

Allow web services to use token for security purposes.

IP Validation during Token authentication.

☐ NO

Allow enabled/disabled IP Validation during token authentication.

- **Application Time zone:** The time zone for the application server.
- **Database Time zone:** The time zone for the database server.
- **Date Format:** Select from multiple date/time formats from the dropdown box.
- **Session Timeout:** Enter a timeout period for sessions in seconds.
- **Web Services:** Toggle to Yes to enable the application to use web services.
- **Token Required for Web Services?:** Toggle to YES to allow web services to use token for security purposes.
- **IP Validation during Token authentication:** Toggle to YES to allow enabled/disabled IP Validation during token authentication.

Data Import Settings



Note: These settings are for advanced users only.

The application is multi-threaded to perform parallel processing. Each event file is processed by spawning multiple threads. Each thread simultaneously parses the event log file, performs correlation, and inserts the processed log into the database. You can configure the settings for various data import activities in this section.

! These settings are for Advanced Users only.

Multi threading

☒ YES

Enable the application to perform parallel processing.

For Activity Import

Maximum Threads	<input type="text" value="30"/>
Maximum Lines Per Thread	<input type="text" value="100"/>

For User Import

Maximum Threads	<input type="text" value="20"/>
Maximum Lines Per Thread	<input type="text" value="10000"/>

Preview data refresh interval

Enter time in minutes after which data will be refreshed from the data source (ArcSight, Netwitness, Splunk and WMI connector) for preview.

Do you want to set Invalid Events Threshold

☒ YES

If we set invalid threshold and invalid events count reach to threshold amount then system will skip event parsing for further events.

Save events after each file imported

☒ YES

Split input event file into smaller files

☐ NO

Lines per file

Enter the number of lines to be present in each files.

Clear correlation
☒ YES
Make the disabled access account (disabled during access import) an orphan and remove the past correlation.

Clear attributes
☐ NO
Remove all access attributes from the disabled access account (disabled during access import).

Ignore account name case
☒ YES
Import all accounts in upper case.

Multithreading: Use the Yes/No switch to enable or disable parallel processing in the application. If you select Yes, you must also configure the following settings:

For Activity Import:

- **Maximum Threads:** The number of threads that are spawned during the import of activities and events. (The default is 30.)
- **Maximum Lines per Thread:** The number of lines provided that are processed by each thread. (The default value is 20000.) Each user file is processed by spawning multiple threads. Each thread simultaneously parses the user file, checks for identity lifecycle changes, and inserts the processed data into the database.

For User Import:

- **Maximum Threads:** The number of threads that are spawned during the import of users. (The default value is 20.)
- **Maximum Lines Per Thread:** The number of lines provided that are processed by each thread. (The default value is 10000.)

Preview data refresh interval: Specify the number of minutes for which the preview data is cached. During this period, if the Preview button is clicked again, the application retrieves preview data from cache, otherwise refreshes from the data source. (The default value is 30.)

Do you want to set Invalid Events Threshold: Set to Yes/No to set invalid threshold and invalid events count threshold to skip event parsing for further events.

Save events after each file Imported (Yes/No): Enable this setting if you wish to save the events after each file is processed. If this is set to no, all of the files matching the file pattern will be processed prior to saving to the database.

Split input event file into smaller files (Yes/No): Use this setting to split the input file to smaller chunks for processing. If an extremely large file is encountered (greater than 1 GB), you can split the file to increase the processing speed.

Lines per file: Enter the number of lines to be present in each file.

Clear correlation: (Yes/No) Makes the disabled access account (disabled during access import) an orphan and removes the past correlation.

Clear attributes: (Yes/No) Removes all access attributes from the disabled access account (disabled during access import).

Ignore Account Name Case: (Yes/No) Imports all access accounts as all upper case. If the same access account name is encountered with lower case and upper case, this setting prevents duplicate account names.

Single Sign-on

This screen enables the application for user authentication and Single Sign-on (SSO).

SINGLE SIGN-ON

Enable Single Sign On

☐ NO

Use CA SiteMinder, IBM TAM, OpenSSO or other SSO technology for user authentication and SSO (Single Sign-on).

Hostname

Enter name of the host registered with the policy server.

Logout URL

Enter SSO logout URL.

Hostname = Enter the URL for the host; for example, company.com.

Logout URL = Enter the logout URL, for example: <http://www.google.com>. Once you are logged out, you will be redirected to this URL.

Quick Links

This screen allows you to add items to the Menu Bar.

QUICK LINKS

Menu Title

Enter Quick Links menu title. For example "My menu".

Quick Link URLs

Name	Protocol	Url	Order	
<div></div>	http	<div></div>	<div></div>	<div>+</div> <div>-</div>

Quick Link Title

Menu Title: This field determines the label that appears on the Menu Bar.

Quick Link URLs

- **Name:** This determines the link name under the main Menu Bar name.
- **Protocol:** Select either http or https.
- **URL:** Enter the URL that you want to link to when users click the item under the Menu Bar.
- **Order:** This determines the order that in which the links appear under the Menu Bar.
- **+/-:** Click the plus sign to add another Quick Link item. Click the minus sign to remove an existing item.

Startup Jobs

This option allows you to add and control the jobs that run when the application starts. Options on this screen include the following:

STARTUP JOBS

Name: Name of the job
Enable: If 'true', job will be initialized if it does not exist. If 'false' job will be deleted if it exists.
Force Re-schedule: Use when configuration is changed. On next startup, delete existing job, create new job with new config and set flag back to 'No'.
Frequency: Frequency of the job to be scheduled. Valid values are ONCE, SECONDS, MINUTES, HOURLY, DAILY, WEEKLY, MONTHLY, YEARLY.
Time: Time at which job should be rerun, format is HH:MM:SS.
Interval: Interval after which job should be re-run.

Name	Enable	Force re-schedule	Frequency	Time*	Interval	
CertificationManagementJob <i>Sends reminder mail if access certificate is about to expire.</i>	<input type="radio"/> NO	<input type="radio"/> NO	daily	03:00:00		+ -
IMAPMailReaderJob <i>Keeps checking the mailbox for new mails and updates the case comment as per the mail contents.</i>	<input type="radio"/> NO	<input type="radio"/> NO	seconds		600	+ -
SLAJob <i>Executes functions when the SLA is missed for a case.</i>	<input type="radio"/> NO	<input type="radio"/> NO	daily	00:05:00		+ -
JiraPollJob <i>Checks if the status of the case is changed in JIRA. If yes, updates the case status in Profiler application.</i>	<input type="radio"/> NO	<input checked="" type="radio"/> YES	seconds		15	+ -
DEE Job <i>Delete expired events for AEE</i>	<input checked="" type="radio"/> YES	<input type="radio"/> NO	hourly		12	+ -
ACS Job <i>Aggregate counts</i>	<input checked="" type="radio"/> YES	<input type="radio"/> NO	daily	00:00:10	1	+ -
WatchlistUpdaterJob <i>Deletes watchlist data if the current date is greater than the expiry date.</i>	<input checked="" type="radio"/> YES	<input type="radio"/> NO	daily	00:07:00		+ -

- **Name:** Name of the job.
- **Enable:** Select **YES** to initialize a job that does not exist yet. Select **NO** to disable an existing job.
- **Force re-schedule:** Select **YES** if the configuration is changed. On the next startup, the existing job will be disabled, a new job will be created with a new configuration, and the flag will be reset to **NO**.
- **Frequency:** This determines the frequency of the job. Valid values are once, seconds, minutes, hourly, daily, weekly, monthly, or yearly.
- **Time:** Time at which job should be rerun, format is HH:MM:SS.
- **Interval:** This specifies the interval after which the job should be rerun. This field uses the value set in Frequency; for example, if you want a job to run every minute, you could set the Frequency to minutes and the Interval to 1, or Frequency to seconds and Interval to 60.

When you have finished making changes to the General Settings options, click **Save** at the bottom of the screen.

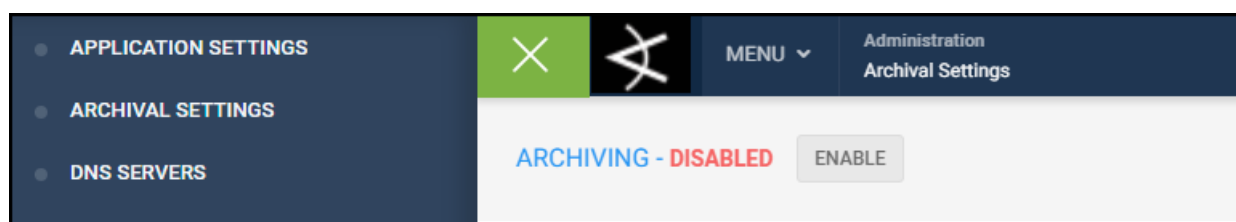
Archival Settings

The ArcSight UBA application provides a tiered archival option for storing data long term. If you want to store a large amount of data for compliance or historical analysis for a large period of time, this tiered archival option offers several benefits that optimize your storage, provide cost benefits and index data for quick search and retrieval when stored for relatively short periods of time.

The tiered storage option for archiving data is as follows:

- Hot - In this instance, the most recently indexed data is stored in Solr for the number of days specified. This indexed data is optimized for storage and quick search. It is primarily used by Spotter.
- Cold - In this instance, the event data is stored in HDFS parquet format for the number of days specified. The data is enriched, but not indexed, which translates to the search being slower. The data stored in the Cold tier is used for reports, for example.
- Frozen - In this instance, the data is archived on an Amazon Web Services (AWS) for long-term storage. The data format is not available for searching by Spotter.

Use the ArcSight UBA interface to set the archival period through the Archival Settings menu. Go to **Menu > Administration > Archival Settings**.



By default, archiving is disabled. To enable, set the archival settings to **Enable**.

Archival settings are available in two modes: Global Mode and Datasource Mode.



Note: You can set either mode, but not both at the same time. The Global Mode allows you to specify archival settings globally for all data sources. If you want to set archival settings at a data-source level only, go to the Datasource Mode.

Setting Hot and Cold Archival Settings at Global Level

To set the hot and cold storage settings on the **Global Mode** tab, follow these steps:

1. From the Archival Settings window, select **Global Mode**.
2. Set the **Index Expiry Days** for SOLR indexes to the number of days you want. At the end of the day specified, the indexed data is deleted from SOLR. This setting is set for the hot expiry of data.

The screenshot shows the 'POLICY ARCHIVAL - ENABLED' header with a 'Disable Archiving' button and a 'Save Policy' button. Below this is a blue navigation bar with 'GLOBAL MODE' and 'DATASOURCE MODE' tabs. The main content area is titled 'DEFAULT CONFIGURATION' and contains two sections. The first section, 'Connection name for archival*', features a dropdown menu with 'Create New Connection' and a description: 'Connection name configured for archival of parquet files.' The second section, 'Index Expiry Days*', has a text input field containing '90' and a description: 'Number of days after which SOLR indexes get deleted'.

POLICY ARCHIVAL - **ENABLED** [Disable Archiving](#) [Save Policy](#)

GLOBAL MODE **DATASOURCE MODE**

DEFAULT CONFIGURATION

Connection name for archival*

Create New Connection ▼

Connection name configured for archival of parquet files.

Index Expiry Days*

90

Number of days after which SOLR indexes get deleted

- Set the **Cold Expiry in Days** after which the hot data from SOLR is archived to HDFS in parquet file format for archival. This setting is set for the cold expiry of data.

Cold Expiry in Days*

365

Number of days after which the HDFS parquet files get archived to archival storage

DATASOURCE CONFIGURATION

ResourcesGroup List Included

PaloAlto

ResourcesGroup List Excluded

>
>>
<<
<

- Under **Datasource configuration**, click the > button to move a datasource to the exclusion list to the right. The **ResourcesGroup** list includes all the datasources to which you want to apply the global mode settings.
- Select **Save Policy** to save your policy settings. Any changes made to the policy take effect when the job runs next time. It deletes the activity data from SOLR and HDFS based on the rules you configured.

Setting Hot and Cold Archival Settings at Datasource Level

To set the hot and cold storage settings on the **Datasource Mode** tab, follow these steps:

1. From the Archival Settings window, select **Datasource Mode**.

The screenshot shows the 'POLICY ARCHIVAL - ENABLED' window with the 'DATASOURCE MODE' tab selected. The 'DEFAULT CONFIGURATION' section has a 'Connection name for archival*' dropdown menu with 'Create New' selected. Below it, a note states 'Connection name configured for archival of parquet files.' The 'DATASOURCE CONFIGURATION' section contains a table with the following data:

Datasource Name*	Index Expiry Days* ⓘ	Cold Expiry in Days* ⓘ	Actions
Select Resource Group ▼	60		⊕ ⊖

2. Select the datasource from the Resource Group drop-down.
3. Set the **Index Expiry Days** for SOLR indexes to the number of days you want. At the end of the day specified, the indexed data is deleted from SOLR for this datasource. This setting is set for the hot expiry of data.
4. Set the **Cold Expiry in Days** after which the hot data from SOLR is archived to HDFS in parquet file format for archival. This setting is set for the cold expiry of data.
5. Click the **+** button to add the datasource to which the news are applied when the job runs. If you want to remove the datasource, click the **-** button.
6. Select **Save Policy** to save your policy settings. Any changes made to the policy take effect when the job runs next time. It deletes the activity data from SOLR and HDFS based on the rules you configured.

Setting Frozen Archival Settings

The fields for frozen archival settings are the same at the global or datasource level. However, the only difference is that the settings at the global level apply to all datasources. If you have specified the settings at the datasource level, then the frozen archival settings only apply to the specified data sources on the Datasource Mode tab.

To set the frozen archival settings at global or datasource level, follow these steps:

1. From the Global Mode or Datasource Mode, select **Create New Connection** from the drop-down to create a connection name for the archival.
2. The Add New Connection window appears. You must provide details for the following fields to enable archiving of data for in AWS:
 - **Connection Name:** Enter a name for the archival connection.
 - **Connection Type for:** The selection defaults to Archival.
 - **Connection Type:** The selection defaults to AWS.

Under **Connection Details**, provide information for the following fields:

- **Access Key:** Enter the AWS access key. This key uniquely identifies the user who owns the AWS account.
 - **Secret Key:** Enter the secret key. The secret key is used to calculate the digital signature that you include in the request.
 - **Bucket:** Once you have provided the access and secret keys, you can test the connection to get the AWS bucket list. A bucket is a logical unit of storage in AWS.
 - Select the list from the drop-down. This bucket list is populated if the connection to AWS is successful.
 - **Source Folder:** Specify the path to the folder where the file to be uploaded is located. Default: \${SECURONIX_HOME}/import/in.
 - **Success Folder:** Specify the folder into which you would like the file to move upon successful upload. Default: \${SECURONIX_HOME}/import/success
 - **Failed Folder:** Specify the folder into which you would like the file to move upon a failed upload. Default: \${SECURONIX_HOME}/import/failed.
 - **Incremental Field:** Set this to Yes if you want incremental updates.
 - **Prefix:** Specify the path within the bucket from which logs must be extracted. You can use this to limit the response to folders that begin with the specified prefix. For example: aws/AWSLogs/853268358782/CloudTrail/us-east-1/2017 limits the search to logs from 2017.
3. Click **Save** to save your settings for the frozen, long-term storage.
 4. Select **Save Policy** to save your policy settings.



Note: The settings for datasource configuration apply to the frozen storage, too. If a datasource is excluded from the list at the global level, then activity data for that datasource is permanently deleted from the cold storage when it expires.

DNS Servers

To access the DNS Servers to add and change the IP entries for your DNS servers:

1. Navigate to **Configure > Settings**.
2. On the left navigation pane, click **DNS Servers**.
3. Change, add, or remove IP addresses as needed.

DNS SERVERS

DNS Server (Host Name/IP Address)

Perform DNS lookup to retrieve Hostnames against IP addresses or IP addresses against Hostnames. This is used during the creation of new resource groups.

<input type="text" value="208.67.220.220"/>	
<input type="text" value="208.67.222.222"/>	

Data Masking

For details about the Data Masking settings, refer to [Data Masking](#).

Hadoop

For details about the Hadoop component settings, refer to [Configure Hadoop Settings for ArcSight UBA](#).

Housekeeping Jobs

Types of Housekeeping Jobs

Job Name	Description	Recommended Schedule
User Import History	<p>Every time a user import is fired, the ArcSight UBA application stores the history of the number of new users, deleted users, updated users, etc. This job clears this table based on the input days.</p> <p>For example, query fired: DELETE FROM User-import-history WHERE importdate<Thu Sep 05 15:24:35 IST 2013</p>	90 days
Access/Activity/User Import Errors	<p>Clears the errors recorded while running Access/Activity/User imports.</p> <p>For example, query fired: DELETE FROM Resourceimporterrors WHERE last-updated<Sat Dec 14 15:30:30 IST 2013</p>	30 days
Risk Score Card History	<p>Clears the risk score card history data.</p> <p>For example, query fired: DELETE FROM Riskscorecardhistory WHERE generatedtime<Thu Nov 14 15:36:51 IST 2013</p>	180 days
Policy Violations	Clears the policy violation data.	90 days
Auditing	<p>Clears the audit history.</p> <p>For example, query Fired: DELETE FROM Sysaudit WHERE logtime<Sat Dec 14 15:57:46 IST 2013</p>	180 days
Activity User IP Mapping	<p>Clears the activity user IP mapping that is maintained for IP address attribution.</p> <p>For example, query Fired: DELETE FROM Activityuseripmapping WHERE lastupdate<Sat May 03 16:03:11 IST 2014</p>	90 days
Completed Jobs	<p>Clears the completed jobs.</p> <p>For example, query fired: DELETE FROM QuartzCustomFiredTriggers qcft WHERE qcft.startTime <= Sat May 03 16:38:43 IST 2014 and qcft.status in ('Completed','Completed with errors')</p>	90 days

Job Name	Description	Recommended Schedule
Failed Jobs	<p>Clears the failed jobs.</p> <p>For example, query fired: DELETE FROM QuartzCustomFiredTriggers qcft WHERE qcft.startTime < Sat May 03 16:41:10 IST 2014and qcft.status in ('Failed')</p>	90 days
Clean Files	<p>Clear the files in success folder and failed folder on the system.</p> <p>Inputs: folder path(s): List of comma separated folder path (updated to support securonix_home).</p> <p>File name: File name or regex pattern of the files to be deleted from above paths.</p> <p>No. of days: File modified before this number of days.</p> <p>Include sub folders: Scans the sub folders for previously listed jobs.</p> <p>Remove non empty files: Deletes files with data. (This should be set to true by default.)</p>	Varies on file volume per day (30 days)

Running Housekeeping Jobs

1. Click **Schedule Housekeeping job**.
2. Choose the job that you want to run.
3. Provide a value for **Remove all data from X days prior to today's date**.
4. Click **Save & Next**.

Job type	Job info
<input type="radio"/> User Import History	User Import History
<input checked="" type="radio"/> Access/Activity/User Import Errors	Clears the errors record data maintained while running Access/Activity/User imports
<input type="radio"/> Risk Score Card History	Clears the risk score card history data
<input type="radio"/> Policy Violations	Clears the policy violation data
<input type="radio"/> Auditing	Clears the audit history
<input type="radio"/> Activity User IP Mapping	Clears the activity user ip mapping
<input type="radio"/> Completed Jobs	Clears the completed jobs
<input type="radio"/> Failed Jobs	Clears the failed jobs
<input type="radio"/> Clean Files	Clear the unwanted files from system

Remove all data from X days prior to today's date

[Prev](#) [Save & Next](#)

6. On the Schedule Housekeeping Job screen, you can enter a **Job Description** in the text box (optional).
7. To configure email notifications, set **Enable Job Related Notifications** to **YES**.
8. You can configure the application to send notification emails upon success, failure, or misfired. Complete the email notifications as needed.
9. From the **Run Job** options, select the frequency for which you want to run the housekeeping job.
10. To save the housekeeping job, click **Save**. To run the housekeeping job now, click **Run**.

Avroparquet Migration Job

A nightly job consolidates events from Avro and migrates it to compressed Parquet format in HDFS. This functionality enables you to migrate events from Avro to Parquet format manually.

1. To run the migration job manually, navigate to **Menu > Settings > Administration > AvroParquet Migration Job**.

AvroParquet Migration Job Can be Triggered Manually. Functionality Allows to select ResourceGroup and Run Migration Job .

ResourcesGroup List Excluded

- file_import
- test-syslog
- thess
- WMI_import
- Databluecoat
- bloue
- File-import_jobs
- console_import
- Test_file_import
- Test_policy
- Test-policy-with_users

ResourcesGroup List Included

AvroParquet Migration allows users to select ResourceGroups from the List and allows to run manual migration. If We Navigate From Page Then We Need To Reselect ResourceGroups.

Run Migration

2. Use **>** or **>>** to select the resource groups from the left and move them to the right.
3. Click **Run Migration** to trigger the migration job. The job is triggered immediately to migrate the events from Avro to Parquet.

LDAP Authentication

Prerequisites for setting up LDAP Authentication

1. The LDAP account should have read permissions for the organizational unit against which the application authenticates.
2. Identify the DN (Distinguished Name) for the account. For example: cn=svc_[DN];OU=ServiceAccounts;DC=[DN];DC=com
3. Identify the following additional parameters that are required for AD authentication:
 - The IP address/hostname of the domain controller.
 - The OU (organizational units) containing the different users that should be authenticated.

Understanding the Configuration

By default, the application authenticates against the local MySQL data store. However, this can be changed to authenticate the users against Active Directory.



Note: The authorization for the users is performed based on locally assigned roles.

- managerDn = <the username used for authenticating against AD>
- managerPassword = <the password used for authenticating against AD>
- grails.plugins.springsecurity.ldap.context.server = <ldap url="">(ex:ldap://xx.xx.xx.xx:389 or ldaps://xx.xx.xx.xx:636)
- grails.plugins.springsecurity.ldap.authorities.groupSearchBase = <group search base>
- grails.plugins.springsecurity.ldap.search.base = <user search base>

To change the default LDAP authentication:

1. Add the following line to the ldap-config.properties file in the “/securonix/securonix_home/conf/”:

```
grails.plugins.springsecurity.ldap.authorities.groupSearchFilter=member={0}
```

2. Add the userid (same as AD login) for the application, and provide the appropriate access controls. By default, the system uses the sAMAccountName for authentication. This can be changed by changing the following value:

```
grails.plugins.springsecurity.ldap.search.filter=sAMAccountName={0}
```

3. Change ‘sAMAccountName’ to cn, dn, or other distinguishable value as required.
4. If local user authentication must be enabled, comment the following line; otherwise, authentication will be only against AD. Uncomment it to authenticate only against AD.

```
grails.plugins.springsecurity.providerNames = ldapAuthProvider
```

5. To debug the errors faced, make the following changes to the log4j.properties files:

```
log4j.logger.org.springframework.security=DEBUG
```

Note: If there are multiple domains to be configured, create a virtual directory that has the entire list of users. Use the credentials of the virtual directory in the ldap-config.properties files.

Configure LDAP

1. Navigate to “/securonix/securonix_home/conf/”.
2. Open the file: ldap-config.properties.
3. Make following changes:

```

grails.plugins.springsecurity.providerNames = ldapAuthProvider
grails.plugins.springsecurity.ldap.context.managerDn = The path
of LDAP
grails.plugins.springsecurity.ldap.context.managerPassword =
Password
grails.plugins.springsecurity.ldap.context.server =
ldap://master server ip
grails.plugins.springsecurity.ldap.authorities.ignorePartialRes
ultException = true
grails.plugins.springsecurity.ldap.search.searchSubtree = true
grails.plugins.springsecurity.ldap.search.base =
dc=oracledemo,dc=com
grails.plugins.springsecurity.ldap.authorities.groupSearchFilte
r=member(0)

```

4. In the application, navigate to **Menu > Administration > Settings**, and then select **LDAP Authentication**.
5. For the **Enable LDAP Authentication** setting, select **YES**.
6. Complete the following settings:
 - **Server:** Enter the IP address for Active Directory (ldap://[ip]:[port]/).
 - **Base:** Enter the base directory to start the search. For example, dc=mycompany,dc=com].
 - Enter the appropriate **Manager DN**.
 - Enter the appropriate **Manager Password**.
 - **Retrieve Database Roles:** Select whether to retrieve additional roles from the database using the User/Role many-to-many.
 - **Retrieve Group Roles:** Select, whether to infer roles based on group membership.
 - **Ignore Partial Result Exception:** Select whether to ignore partial result exceptions.
 - **Search Subtree:** Select whether you want to search in subtrees.
 - **Search Filter:** This is the pattern to be used for the user search. For Example, {0} is the user's DN.

LDAP AUTHENTICATION

Authentication Properties

The Securonix application can authenticate and authorize users on the specified LDAP directory. Enable this setting if you want to use Active Directory or another LDAP compliant directory for authenticating and/or authorizing users

Enable LDAP Authentication

☒ YES

Server & Base

Server	Base	Actions
ldap://11.111.111.111:10389	dc=securonix,dc=com	

Server: Address of the LDAP server Example: ldap://71.252.211.110:10389

Base: Context name in which to search, relative to the base of the configured ContextSource, e.g. 'dc=example,dc=com', 'ou=users,dc=example,dc=com'

Manager DN

cn=Administrator,cn=Users,dc=securonix,dc=com

DN to authenticate with

Manager Password

.....

Username to authenticate with

Retrieve Database Roles

☒ NO

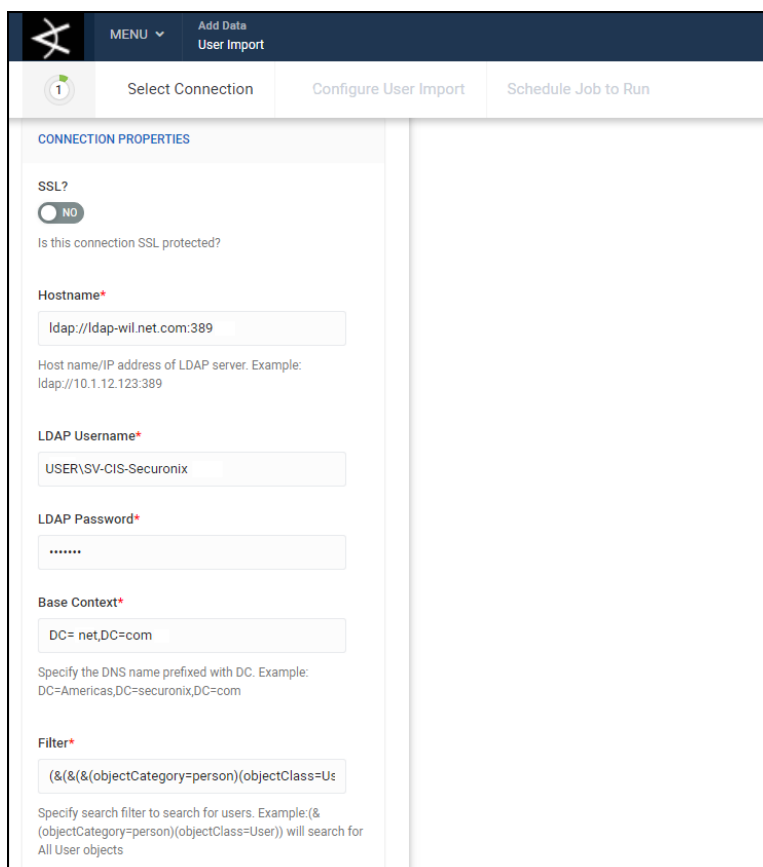
Check to retrieve additional roles from the database using the User/Role many-to-many.

Retrieve Group Roles

☒ NO

Check to infer roles based on group membership.

- **Group Search Base:** Enter the base DN from which the search for group membership should be performed.
- **Group Search Filter:** Enter the pattern to be used for the user search. For example, {0} is the user's DN.
- **Group Role Attribute:** Enter the ID of the attribute which contains the role name for a group.



1 Select Connection | Configure User Import | Schedule Job to Run

CONNECTION PROPERTIES

SSL?
☒ NO
Is this connection SSL protected?

Hostname*
ldap://ldap-wil.net.com:389
Host name/IP address of LDAP server. Example:
ldap://10.1.12.123:389

LDAP Username*
USER\SV-CIS-Securonix

LDAP Password*

Base Context*
DC=net,DC=com
Specify the DNS name prefixed with DC. Example:
DC=Americas,DC=securonix,DC=com

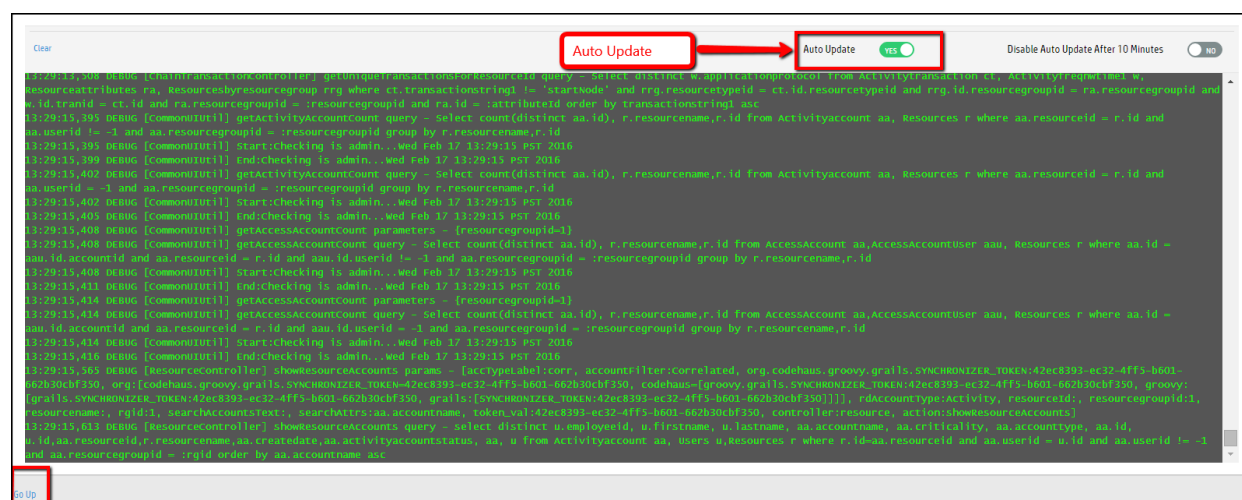
Filter*
(&(&(objectCategory=person)(objectClass=User))
Specify search filter to search for users. Example: (&(objectCategory=person)(objectClass=User)) will search for All User objects

7. When you have finished, click **Save**.

Log Settings

Application Logs

This option displays the application logs and provides an option to set the application logs to auto update. If you select **YES**, an additional option to **Disable Auto Update After** a specified period is available.



Logging

Setting up Logging to securonix.log File

The ArcSight User Behavior Analytics application logs both errors and debug statements to a log file. Conveniently named securonix.log, the log file is located in the "<TOMCAT_HOME>/logs" directory.

You can change the location of the securonix.log file to any desired folder.

To specify the location of the log file:

1. Navigate to <TOMCAT_HOME>/WEB-INF/classes.
2. Search for a file named log4j.properties.
3. Open the file with a text editor.
4. To specify the location of the logs file, search for the following line under the # File Appender heading:

```
log4j.appender.file.file=.../securonix.log
```

Note: To begin logging to the new location, you must restart the application.

Changing the log format

By default, the log file does not include the date on which the log was written. This is because of the following directive in log4j.properties:

```
log4j.appender.file.layout.ConversionPattern=%d{ABSOLUTE} %-5p [%c{1}] %m%n
```

For example, from securonix.log:

```
09:37:26,744 DEBUG [LoginController] auth. Getting license information...
```

If you want to change this setting to include the date, use the following format:


```
log4j.appender.file.layout.ConversionPattern==%d{dd MMM yyyy HH:mm:ss,SSS} %-4r [%t] %-5p %c{1} %x - %m%n
```

Log Levels

ERROR: The ERROR level designates error events that might still allow the application to continue running.

FATAL: The FATAL level designates very severe error events that will presumably lead the application to abort.

OFF: Turn off logging.

WARN: The WARN level designates potentially harmful situations.

INFO: The INFO level designates informational messages that highlight the progress of the application at coarse-grained level.

ALL: The ALL level has the lowest possible rank and is intended to turn on all logging.

DEBUG: The DEBUG level designates fine-grained informational events that are most useful to debug an application.

TRACE: The TRACE level designates finer-grained informational events than the DEBUG level.

Changing Logging Levels

Logging can be changed for each module within the application. To change the logging levels, perform the following steps:

1. Navigate to **Menu > Administration > Settings**.
2. On the left navigation pane, click **Log Settings > Logging**.
3. Change the log level for the desired module.
4. To save your changes, click **Update**.

Change Log Levels for Modules

The following modules are available for logging:

- **Imports:** Logging for User Import and Glossary Import actions.
- **Activity Imports:** Logging for Activity Import for various connections.
- **Policy Engine:** Detect Behavioral Analytics, Anomaly Detection
- **Web Services:** Web application components.
- **Work Flow:** SOC Team Review, Activity Outlier Workflow, Access Certification Workflow.
- **Licensing:** Logging for Managing, updating license.

- **Views:** Users, Resources, Peers, Organizations, Application.
- **Run:** Access, Activity, Policy violations, Behavior Profiles.
- **Reports:** Running and rendering reports.
- **Configure:** All actions available under the configure menu.
- **UI Utilities:** Analytical Activities, Applications, Dashboard, Incidents, Organizations, Peer, Resource, Detect, Transaction, User, Utility Impl, Token, Common UI Utilities, Workbench Util.

Log Level Choices

All modules have the same log level choices. The default setting for each, however, is different. Choices are:

- **All:** All has the lowest possible rank and is intended to turn on all logging.
- **Debug:** Designates fine-grained informational events that are most useful to debug an application.
- **Error:** Designates error events that might still allow the application to continue running.
- **Fatal:** Designates very severe error events that will presumably lead the application to abort.
- **Info:** Designates informational messages that highlight the progress of the application at a coarse-grained level.
- **Off:** Off has the highest possible rank and is intended to turn off logging.
- **Trace:** Designates finer-grained informational events than debug.
- **Warn:** Designates potentially harmful situations.

Set Log Levels

To set the log levels:

1. From the **Select a resource to view logs** dropdown list, select a module to view its current Log Level.
2. To change the current log level for a specific module, select an option from the **Log Level** dropdown.
3. To save your changes, click **Update**.

SET LOG LEVELS

Select Module to View the current Logging Level. You can also change the logging level. We recommend that all logging be set to ERROR in production

Select a resource to view logs

Activity Imports

Module	Log Level <i></i>
Activity File Import	ERROR
Activity Arcsight Import	ERROR
Activity ResourceDB Import	ERROR
Activity NetWitness Import	ERROR
Activity Nitro Import	ERROR
Activity Splunk Import	ERROR

Manage License

This section allows you to review your licenses installed with the application. View details about the current licenses including number of users and resources licensed, license issue and expiration date and issuer details. To manage licenses, navigate to **Menu > Administration > Settings**. Select **Manage License** from the left pane.

Current License

CURRENT LICENSE INFORMATION			
Licensed To	Anjan	License Type	
License Usage	666 / 100000000	Licensed Resources	100000000
Events Per Day	-1	Allocated Disk Space In GB	-1
Issued Date	Wed Apr 12 01:00:00 CDT 2017		
Expires On	Mon Jun 10 01:00:00 CDT 2030	Additional Information	
Not Valid Before	Wed Apr 12 01:00:00 CDT 2017		
Available Products			
Product	Expires On	Packs	
SNYPR Platform	Mon Jun 10 01:00:00 CDT 2030		

Installed Licenses

This section displays the installed licenses, which you can uninstall by clicking the **Uninstall** button.

INSTALLED LICENSES			
Filename	Installed On		Actions
/Securonix/tenants/four/snypr6/securonix_home/conf/lic/securonix.lic	2017-03-23 19:47:18.0	View License Details	<button>Uninstall</button>

Install/Upgrade License

In the **Install/Upgrade License** options you can upload a new license and enter a new activation key.

INSTALL/UPGRADE LICENSE			
Install/Upgrade License			
License File	<div>securonix.lic</div> <div>Upload new license file</div>	Enter Activation Key	<div></div> <div><button>Install</button></div>
Issuer Details			
Name	Securonix Solutions	Location	Los Angeles
State/Province	CA	Organization	Securonix Corp.
Organization Unit	Software Asset Management	Country Abbreviation	United States
Street	5777 W. Century Blvd	Identification	Securonix License Management

SAML Settings

Security Assertion Markup Language (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. SAML settings are related to configuration of single-sign on (SSO), which help reduce the administrative overhead of distributing multiple authentication tokens to the user.

SAML SETTINGS

Metadata Management for SAML

As an end user you can generate Service provider metadata and send it to the Identity Provider(IDP) which is usually a third party application. Ideally, on the deployment of the Securonix application you will need to generate the Service provider metadata once and share this with the IDP. Metadata is what makes SAML authentication work. Use the link below to change any metadata settings or regenerate the service provider metadata. Please be sure to resend this information to the IDP.

Click here to generate new service provider metadata

This is the currently used and stored metadata for Securonix. Please click on the link to know the properties that were set during its generation.

List of Service providers:

The Identity provider is the entity that authenticates the user and passes its authentication token to Securonix. By default we provide SSOCircle metadata. This has to be replaced in file with which ever identity provider you want to support. Use the box below to add a new IDP.

List of registered Identity providers:
http://idp.ssocircle.com

Add a new IDP by pasting the metadata information in the box below

Submit

To configure the SAML settings:

1. Navigate to **Menu > Administration > Settings**, and then from the left navigation pane, select **SAML Settings**. On the **SAML Settings** page, you can:
 - Generate metadata for the new Service Provider
 - Share the metadata for the Service Provider
 - Obtain a list of registered Identity Providers

- Create users with ArcSight UBA
2. Click the **Click here to generate new service provider metadata** link.
 3. The **SAML Current Settings** screen appears.

SAML CURRENT SETTINGS

New Metadata for the Service Provider

Store for the current session?

Yes

The Service Provider updates will be applied to the current session as well.

Entity ID:

10.0.0.21

Entity ID is a unique identifier for an identity or service provider. Value is included in the generated metadata.

Entity Base URL

https://10.0.0.21:8443/Snyl

Base to generate URLs for this server. For example: https://myServer:443/saml-app. The public address your server will be accessed from should be used here.

Entity Alias:

10.0.0.21

Alias is an internal mechanism allowing collocating multiple service providers on one server. Alias must be unique.

Include IDP Discovery

☒

If set IDP Discovery will be included in the meta data.

SSO Bindings

Which bindings to use for SSO?

☒

Post

☒

PAOS

☒

Artifact

- **Entity ID:** The Entity ID is a unique identifier for an identity or service provider. This value is included in the generated metadata.
- **Entity Base URL:** Base to generate URLs for this server. For example: https://myServer:443/saml-app. Enter the public address from which your server will be accessed.
- **Entity Alias:** The Alias is an internal mechanism that allows the application to collocate multiple service providers on one server. The alias entity must be unique.
- **Include IDP Discovery:** Select this option to include identity provider discovery in the metadata.
- **SSO Bindings:** Select the bindings to use for SSO, which include Post, PAOS, and Artifact. The binding, in general, determine how an SAML request and response map to protocols for messaging and communication.

Security Profile

Meta/OP

Security profile determines how is trust of signature, encryption and SSL/TLS credentials handled. In Meta/OP mode credential is deemed valid when it's declared in the metadata document of the peer entity. No validation of the credentials is made. The value is recommended as a default. PKIX profile verifies credentials against a set of trust anchors. By default certificates present in the metadata are treated as trust anchors together with the additional selected trusted keys.

Signing Key

ping (ping)

Key used for digital signatures of SAML messages.

Encryption Key

ping (ping)

Key used for digital encryption of SAML messages.

SSL/TLS key

ping (ping)

Key used to authenticate this instance for SSL/TLS connections.

- **Security Profile:** From the dropdown list, select the option you want to use for trust of signature, encryption, and SSL/TLS credentials.
- **Signing Key:** The key used for digital signatures of SAML messages
- **Encryption Key:** The key used for digital encryption of SAML messages
- **SSL/TLS Key:** The key used to authenticate an instance for SSL/TLS connections

Sign metadata
☐
 If set the generated metadata will be digitally signed using the specified signature key.

Sign sent AuthNRequests
☐
 If set the generated metadata will be digitally signed using the specified signature key.

Require signed authentication Assertion
☐
 If set the generated metadata will be digitally signed using the specified signature key.

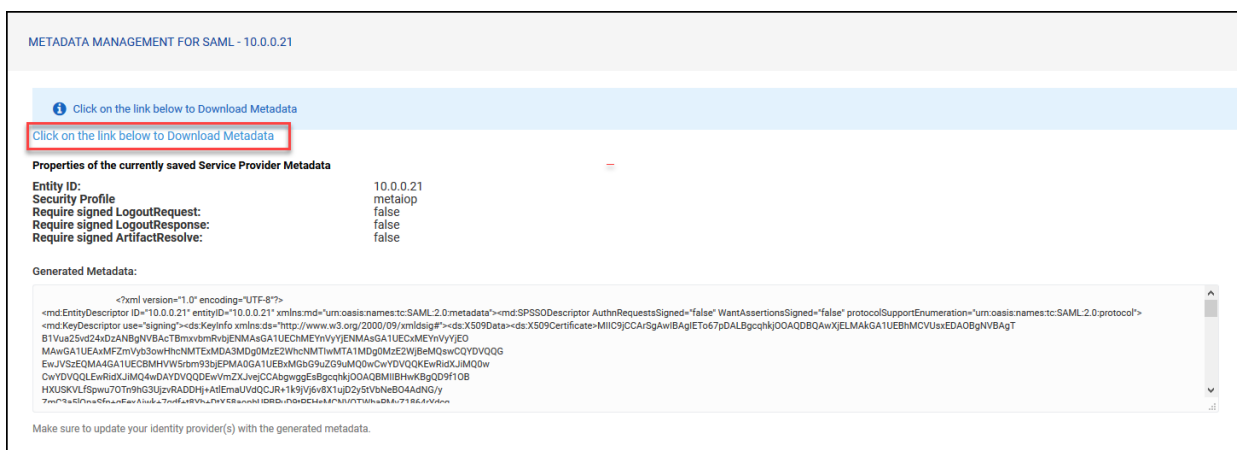
Require signed LogoutRequest
☐
 If set the generated metadata will be digitally signed using the specified signature key.

Require signed LogoutResponse
☐
 If set the generated metadata will be digitally signed using the specified signature key.

Require signed ArtifactResolve
☐
 If set the generated metadata will be digitally signed using the specified signature key.

[Generate Metadata](#)

- **Sign metadata:** Select this option to digitally sign the generated metadata with the specified signature key.
 - **Sign sent AuthNRequests:** If selected, the generated metadata is digitally signed using the specified signature key.
 - **Require signed authentication Assertion:** If selected, the generated metadata is digitally signed using the specified signature key.
 - **Require signed LogoutRequest:** If selected, the generated metadata request is digitally signed for logout requests using the specified signature key.
 - **Require signed LogoutResponse:** If selected, the generated metadata request is digitally signed for logout responses using the specified signature key.
 - **Require signed ArtifactResolve:** If selected, the generated metadata request is digitally signed for artifact resolution using the specified signature key.
4. To continue, click **Generate Metadata**. The new Service Provider metadata is generated.
 5. The **Metadata Management for SAML** screen appears with the newly-generated Service Provider metadata. Share the metadata with the Service Provider to allow for redirection of request to the application.



6. Click the link to obtain a list of registered identity providers. The Metadata Management for SAML screen appears to download the metadata for the Identity Provider.
7. Copy the metadata provided by the SAML provider in the text box to register the new Identity Provider.
8. Click **Submit** to save the identity provider (IDP) metadata.

SMTP Server Settings

The application uses the mail server for the following purposes:

- To send email notifications on a violation.
- To send job success/failure notifications.
- To send email notifications on user lifecycle changes (new, updated, and terminated users).
- To send notification emails for case-related issues.
- To receive emails when comments are added to existing cases.

Adding an SMTP Server

Add New Mail Server

DEFAULT

General Settings

Mail Box Name*
default

Outgoing mail server's host name

Host*
imap.gmail.com

Outgoing mail server's host name

Port*
465

Outgoing mail server's port number

From Email
test@securonix.com

Sender's name

SSL Enabled?
☒ NO

SSL is a secure protocol developed for sending information securely over the Internet.

Authentication Required
☒ YES

UserName*
test@securonix.com

To set up a new SMTP server:

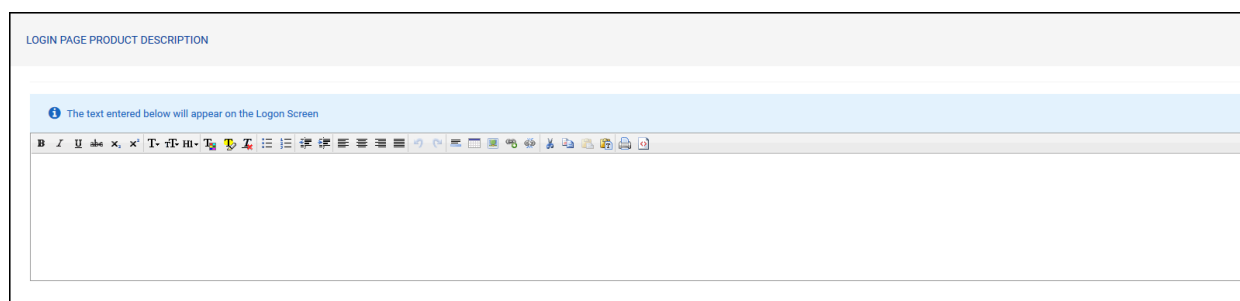
1. Navigate to **Menu > Administration > Settings**.
2. On the left navigation pane, click **SMTP Server Settings**.
3. To add a new server, click **Add New Mail Server**.
4. Use the following steps to configure the General Settings section:
 - a. **Mail Box Name:** You can keep the default setting or provide a name of your choice.

- b. **Host:** Enter a host name for the mail server.
 - c. **Port:** Enter an outgoing port.
 - d. **From email:** Type the name of the email account used for sending email.
 - e. **SSL enabled?:** Toggle the **YES/NO** switch to enable or disable SSL communication.
 - f. **Authentication required:** If the mail server requires authentication, select **YES**.
 - g. **UserName** and **Password:** If authentication is set to YES, enter the username and password.
6. Use the following steps to configure the **More Settings** section:
 - a. **Font name:** Select a font type from the dropdown list. The default font is Arial.
 - b. **Font size:** Enter the size of the font you want to use in your email notifications. The default font size is 2.
 - c. **Batch size:** Enter the number of email notifications that are sent in a batch. The default setting is 25.
 - d. **Interval:** Enter the number of seconds for retrial. The default is 10.
 - e. **Process In Batch:** Choose whether you want to send email notifications in batches. The default is Yes.
 - f. **Stop When Done:** Choose whether you want to stop sending email notifications when all of the messages in queue are completed. The default is Yes.
7. When you have finished, click **Save**. You can also save settings and send a test email, or test the SMTP server using choices at the bottom of the Mail Server Settings screen:



UI Preferences

From this screen, you can enter text to appear on the ArcSight UBA Logon screen. For example, display the company privacy policy.



Data Masking

Data masking allows you to mask users and entities such as activity account, access account, resource name, IP address and datasource attributes displayed to users.

To mask data, follow these steps:

Go to **Menu > Administration > Settings**. By default, data masking is disabled. To enable data masking, click the **Enable** button.

The screenshot shows a web interface for configuring data masking. At the top, a status bar indicates "MASKING - ENABLED" in green text next to a blue button labeled "Disable Masking". Below this is a navigation bar with three steps: "Select Entities" (active, with a person icon), "Select Event Attributes" (with a double arrow icon), and "Select Access Attributes" (with a key icon). A blue "Next" button is on the right. The main content area has three sections, each with a toggle switch set to "NO":
1. "Mask Users Attributes": Includes a note "Select User Attributes to mask. NOTE: This is a global setting applicable to all user datasources".
2. "Mask Activity Account": Includes a note "Mask all the Activity Account Name globally".
3. "Mask IP Address": Includes a note "Enabling this will mask IP Addresses across all datasources".

Select Entities

- On the **Select Entities** tab, move the toggle to **Yes** to mask the attributes. Enabling an attribute masks that information in the user interface:
 - Mask Users Attributes:** Masks user attributes for all the user datasources. This is a global setting. If you set the toggle to **Yes**, the following screen appears for you to select the attributes:

Mask Users Attributes

YES

Select User Attributes to mask. NOTE: This is a global setting applicable to all user datasources

USER ATTRIBUTES TO MASK EVENT DATA

customfield23
customfield24
customfield25
customfield26
customfield27
customfield28
customfield29
customfield30
department

employeeid
lastname

Do you want to enable conditional masking?

NO

Mask all users data with conditional masking. For Eg: Mask all users whose Department = "Engineering"

- Select the user attributes from the left panel and move them to the right panel. The selected user attributes in the right panel are masked when you save the configuration and run the job successfully. For example, the employeeid and the lastname is masked as shown in the following figure when you view users.

Enter your search criteria						
				employeeid		
	Employee ID	First Name	Last Name	Manager Employee ID	Email	
	EAFO2F10BBAC26C0D2937ECAEAE29C17	HARRY	1E54FD1C1AF47B2209EA5C37862DE365	1012	HARRY.OGWA@scnx.com	
	747875EF7C7E8EBFA810E8C2E064C592	HOMER	85128E4B90B36CAA5D0E3F68750976F4	1001	HOMER.OGWAL@scnx.com	
	6936CD89E579E09DE4CD34A633A4A290	HILLARY	1E54FD1C1AF47B2209EA5C37862DE365	1001	HILLARY.OGWA@scnx.com	

3. Once you have selected the attributes, you can apply conditional masking to the user attributes. For example: Mask all users whose Department = "Engineering".

Do you want to enable conditional masking?

☒ YES

Mask all users data with conditional masking. For Eg: Mask all users whose Department = "Engineering"

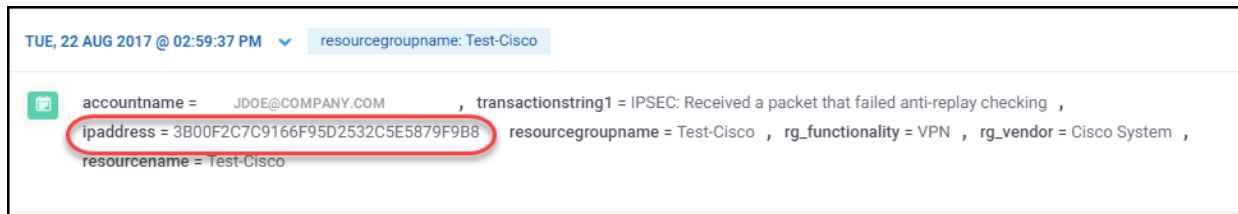
Attribute	Condition	Value		
department	Equal To	engineering	AND	<input type="button" value="+"/> <input type="button" value="-"/>

4. When you run the job after enabling conditional masking on department= "engineering", all users who belong to the engineering department are masked as shown:

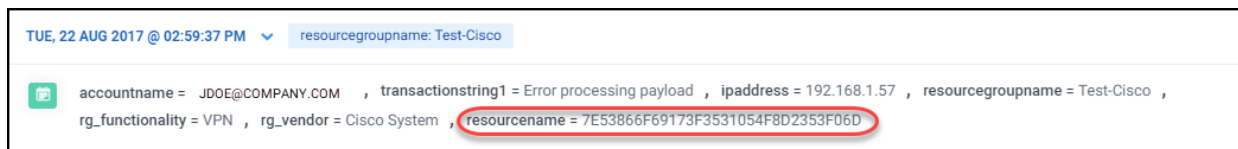
Enter your search criteria						
				employeeid		
	Employee ID	First Name	Last Name	Manager Employee ID	Email	Department
	73A7320F40621D5CAB8453D550CD8809	SEAN	706EC732AA71ABC56B43C3A7EB6E7026	1013	SEAN.connelly@scnx.com	673885E37626A8C1D8954633AA0D1028

5. Similarly, you can enable masking for fields such as activity account, IP address, resource name and access account as follows:
- **Mask Activity Account:** Masks all the activity account names globally. If you enable this option, all activity accounts are masked globally.

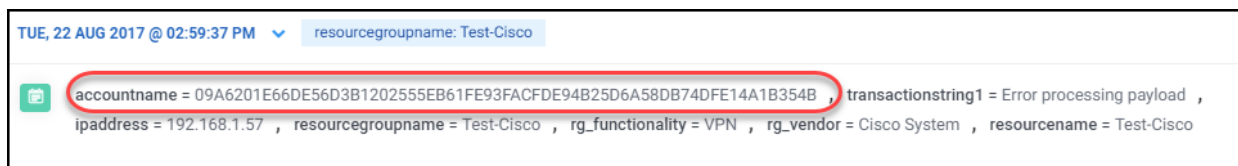
- **Mask IP Address:** Masks the IP address for all the datasources.



- **Mask Resource Name:** Masks all the resource names globally. The following figures shows an example a masked resourcename.



- **Mask Access Account:** Masks all the access account names globally. If access accounts are enabled for masking, the access account names are masked for all datasources globally as shown:



6. Click **Next**.

Select Event Attributes

- On the **Select Event Attributes** tab, select the datasource and the attributes that you want to mask. This screen allows you to select the specific datasources for which you want to mask event attributes.



Note: The global settings for masking event attributes override the datasource settings.

The screenshot shows the 'Select Event Attributes' tab. At the top, it says 'MASKING - ENABLED' with a 'Disable Masking' button. Below this is a navigation bar with three tabs: 'Select Entities', 'Select Event Attributes' (which is active and highlighted with a blue circle), and 'Select Access Attributes'. To the right of the tabs are 'Prev' and 'Next' buttons. Below the navigation bar is a button labeled 'Add Datasource Attributes'.

- Click the **Add Datasource Attributes** button to add the datasource attributes. Select the data-source from the **Select Datasource** dropdown.
- Select the attributes and move them to the right panel, and click **Add**. The datasource attributes you selected appear to the right of the screen.

The screenshot shows the 'Add Datasource Attributes' dialog box. It has a title bar with a close button (X). Inside, there is a 'Select Datasource' dropdown menu currently showing 'Bluecoat Proxy'. Below this is a section titled 'Datasource attributes to mask event data'. It contains two lists of attributes. The left list includes: eventlatitude, eventlongitude, eventregion, Filetype, Method, msg, objectname, Object_Type, and postalcode. The right list includes: username, Filename, and hostname. Between the two lists are four arrow buttons: a single right arrow (>), a double right arrow (>>), a double left arrow (<<), and a single left arrow (<). At the bottom right of the dialog is an 'Add' button.

- Click **Next**.

Select Access Attributes

- On the **Select Access Attributes** tab, select the datasource and the attributes that you want to mask. This screen allows you to select the specific datasources for which you want to mask access attributes.



Note: The global settings for masking event attributes override the datasource settings.

- Click the **Add Datasource Attributes** button to add the datasource attributes. Select the attributes and move them to the right panel, and click **Add**. The datasource attributes you selected appear to the right of the screen.

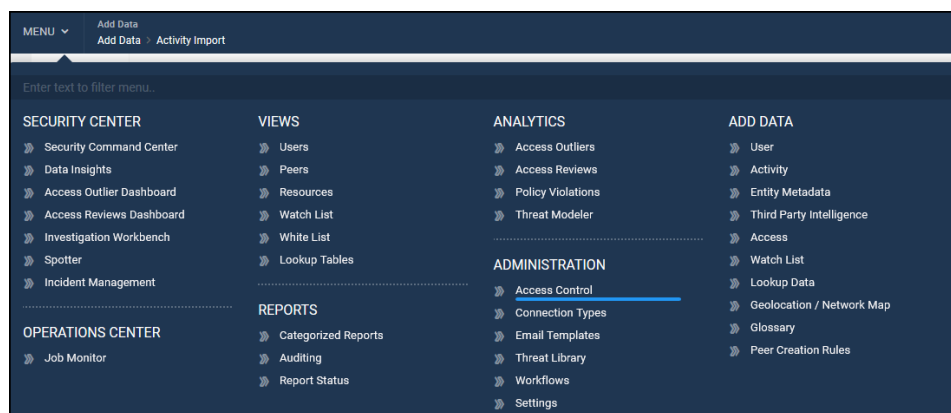
- Save and run the job to enable masking in the user interface.

You can view the job summary under **Data Masking > Masking Job Details**.

Access Control

ArcSight UBA allows Administrators to restrict access to selected screens in the user interface. Access is restricted to authorized users based on their roles. Roles are created based on job functions.

To configure role based access control, navigate to **Menu > Administration > Access Control**.



Setting Up Access Control

The screenshot shows the 'ACCESS CONTROL' interface. On the left is a sidebar with options: Manage Users, Manage Roles, Manage Groups, Granular Access Control, and Password Control. The main area displays a table of users with columns for User Name, Enabled status, First Name, Last Name, Email, and Actions. The table contains 10 rows of user data. At the bottom, there is a pagination bar showing 'First', '1', '2', '3', '4', '5', 'Last', 'Show', and '10'. The total results are 59, and the total pages are 6.

User Name	Enabled	First Name	Last Name	Email	Actions
1001	YES	HARRY	OWWA	HARRY.OWWA@scnx.com	[Edit] [Delete]
1005	YES	TERRY	MERRITT	TERRY.MERRITT@scnx.com	[Edit] [Delete]
1012	YES	JOE	KELLINGTON	JOE.KELLINGTON@scnx.com	[Edit] [Delete]
1013	YES	ROBERT	WELLINGTON	ROBERT.WELLINGTON@scnx.com	[Edit] [Delete]
1025	YES	Ted	Thomson	ted.thomson@scnx.com	[Edit] [Delete]
1044	YES	NORA	LEWIS	NORA.LEWIS@scnx.com	[Edit] [Delete]
1045	YES	FAHAD	WALKER	FAHAD.WALKER@scnx.com	[Edit] [Delete]
1063	YES	Meredith	COLEMAN	Meredith.COLEMAN@scnx.com	[Edit] [Delete]
1064	YES	Cedric	Castaneda	Cedric.Castaneda@scnx.com	[Edit] [Delete]
1065	YES	Ainsley	Moses	Ainsley.Moses@scnx.com	[Edit] [Delete]

Before setting up access control, determine the roles and capabilities to assign to each role. Additionally, decide which users should be assigned to each role.

Setting up access control requires two steps:

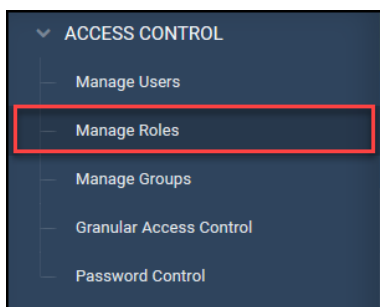
1. Create roles and assign capabilities to roles.
2. Create users and assign them to roles.
3. Create groups and assign users to groups.
4. (optional) Configure Granular Access Control for groups.

Creating Roles

Roles with meaningful names (for example: Auditors, security operations, forensics, investigator, etc.) make it easier to perform access control. You can assign multiple capabilities to Roles. These capabilities allow users to access specific modules of the application.

To create a role, complete the following steps:

1. Navigate to **Menu > Administration > Access Control**.
2. Click **Manage Roles** from the Access Control navigation panel.



1. Click +.
2. Provided the following information when form opens:

Create Role

Role Name*

Description

Privileges* ⓘ

Dashboard ▾

Dashboard-Security Dashboard
Dashboard-Security Dashboard-High Risk Users [shows high risk users graph]
Dashboard-Security Dashboard-High Risk Users[shows list of high risk users]
Dashboard-Security Dashboard-High Risk Access [shows high risk access users graph]
Dashboard-Security Dashboard-High Risk Access[shows list of high risk access users]
Dashboard-Security Dashboard-High Risk Activities [shows high risk activities graph]
Dashboard-Security Dashboard-High Risk Activities[shows list of high risk activities]
Dashboard-Security Dashboard-DLP Alerts [shows DLP alerts graph]
Dashboard-Security Dashboard-DLP Alerts[shows list of DLP alerts]
Dashboard-Security Dashboard-High Risk Accounts[shows list of high risk accounts]
Dashboard-Security Dashboard-Incidents [shows incidents graph]
Dashboard-Security Dashboard-Incidents[shows list of incidents]
Dashboard-Security Dashboard-Incidents [shows incident progress]

>
>>
<<
<

- **Role Name:** Enter a unique name for the role.
- **Description:** Enter a brief description about the purpose and privileges granted to the role.
- **Privileges:** Grant privileges to the role.
 - a. Select the areas of the UI to which the role is granted access. These areas include
 - **Dashboard**
 - **Views**
 - **Add Data**
 - **Analytics**
 - **Reports**
 - **Administration**
 - **Third Party Intelligence**

- Other
- Geolocation
- Investigation Workbench
- Spotter
- Security Command Center
- Operations Center

- b. Select individual privileges within the areas (for example, Configure-System) using > or >> to select all.



Note: Privileges are grouped based on the module (i.e. dashboard, manage, detect, respond, reports, and configure). For a complete list of privileges, see [Appendix D: Access Privileges](#).

Example: Grant all dashboard privileges to role

Create Role

Role Name*

Auditor

Description

IT-Auditor

Privileges* ⓘ

Dashboard

>

>>

<<

<

Dashboard-Security Dashboard

Dashboard-Security Dashboard-High Risk Users [shows high risk users graph]

Dashboard-Security Dashboard-High Risk Users[shows list of high risk users]

Dashboard-Security Dashboard-High Risk Access [shows high risk access users graph]

Dashboard-Security Dashboard-High Risk Access[shows list of high risk access users]

Dashboard-Security Dashboard-High Risk Activities [shows high risk activities graph]

Dashboard-Security Dashboard-High Risk Activities[shows list of high risk activities]

Dashboard-Security Dashboard-DLP Alerts [shows DLP alerts graph]

Dashboard-Security Dashboard-DLP Alerts[shows list of DLP alerts]

Dashboard-Security Dashboard-High Risk Accounts[shows list of high risk accounts]

Dashboard-Security Dashboard-Incidents [shows incidents graph]

Dashboard-Security Dashboard-Incidents[shows list of incidents]

Dashboard-Security Dashboard-Incidents [shows incident progress]

3. Click **Save**.

The following table shows typical Roles included in the application:

Role	Description
Access Certifier	<p>Main task: Certify user access privileges</p> <ul style="list-style-type: none"> • Can log in and view the risky entitlements for the users who report to the manager/certifier • Has access to specific Security Dashboards (Access Review Category only)
Access Scanner	<p>Main Task: Detect user access privilege outliers</p> <ul style="list-style-type: none"> • Is a role typically assigned to users running access outliers and on-boarding access entitlements into the application and limits access within the application to only access-related screens and access-related resource groups • Has screen access configured by the admin
Admin	<p>Main Task: Configure the application</p> <p>Has highest level of access available</p> <ul style="list-style-type: none"> • Has ability to add/ delete data in the application • Has ability to create/ modify/ delete jobs • Has ability to create / modify / delete users, roles, and groups • Has ability to control access to the application • Has ability to encrypt / mask data
Auditor	<p>Main Task: Monitor the ArcSight UBA application health</p> <ul style="list-style-type: none"> • Has ability to access the administrative dashboard to review all operational/ IT metrics about events and data sources in the systems
Business Unit Manager	<p>Main Task: Monitor risk profile for business units</p> <ul style="list-style-type: none"> • Allows business unit managers to log in to the application and review the risk profile associated to the users within their business units. • Is not typically given admin privileges and is unable to add or remove data within the application.

Role	Description
Case Analyst	<p>Main Task: View and Manage Cases</p> <ul style="list-style-type: none"> • Has access to the Incident Dashboard • Has ability to review and work on cases • Is unable to configure any jobs or import data into the application
Hunters	<p>Main Task: Hunt team</p> <ul style="list-style-type: none"> • Has access to Security Dashboards • Has ability to drill-down and investigate incidents using tools such as the Investigation Workbench for data link analysis
License Manager	<p>Main Task: Manage application licensing</p> <ul style="list-style-type: none"> • Has access only to the license screen to re-register license details and validate licenses • Is unable to access any other screen or view data for the user
Operations Team	<p>Main Task: End-to-end monitoring of the application</p> <ul style="list-style-type: none"> • Has ability to view the health and operation of the application from end-to-end • Has ability to ensure data imports were scheduled correctly, activity imports and scheduled jobs ran properly • Has ability to modify the settings to ensure the end-to-end flow is working
Privacy Manager	<p>Main Task: Decrypt PII (Personally identifiable information) data</p> <ul style="list-style-type: none"> • Has the ability to decrypt users' PII data within the application when data encryption is enabled • Has access only to certain screens controlled by the admin (typical screens are 'Manage Users' and 'High-Risk Users') • Is not typically given access to view the underlying data that caused violations

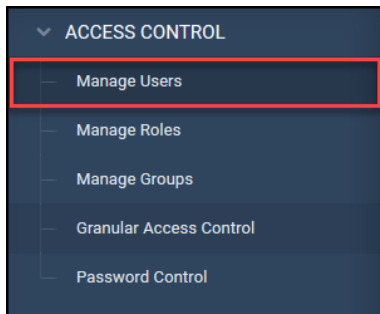
Role	Description
System Owner	<p>Main Task: Manage risk posture by application</p> <ul style="list-style-type: none"> • Allows application owners to view the risk profile for all users of the application • Is typically given admin privileges to the application for which they are the owners • Has screen access configurable from the UI
User Admin	<p>Main Task: Manage applications</p> <ul style="list-style-type: none"> • Is a role assigned to application admins. • Can be configured if users need <i>some</i> super user privileges but not <i>all</i> admin privileges. • Has screen access configurable from the UI

Creating Users

You can grant analysts access to the application and assign them specific privileges. To create a new analyst and grant privileges, complete the following steps:

Enter User Information

1. Navigate to **Menu > Administration > Access Control**.
2. Click **Manage Users** from the Access Control navigation panel.



3. Click **+**.
4. Provide the following details when form opens:

Create User

1

Enter User Information

Assign roles to the user

Assign groups to the user

User Name*

Enter Username

Password*

Enter Password

Re-enter Password*

Re-Enter Password

First Name*

Enter Firstname

Last Name*

Enter Lastname

Email*

5.

- **User Name:** Enter the name user will use to log in to the application.
- **Password:** Enter the password user will use to log in to the application.
- **Re-Enter Password:** Re-enter the password user will use to log in to the application.
- **First Name:** Enter the user's first name.
- **Last Name:** Enter the user's last name.
- **Email:** Enter the user's email.
- **Badge Background Color:** Select a color from color picker.
- **Enabled?:** Toggle to **Yes** to enable user.

6. Click **Save & Next**.

Assign Roles to the user

1. Toggle the slider to **Yes** for the roles you would like to assign to this user.



Note: Users will only be able to access certain screens in the UI based on the roles you select.

User Details

1

Enter User Information

Assign roles to the user

Assign groups to the user

Prev

Save & Next

Assign Roles to users to grant access to functionalities within the Securonix application.

Role Name		Description
ROLE_ADMIN	<input type="checkbox"/>	System Administrator
ROLE_AUDITOR	<input type="checkbox"/>	IT Auditor
ROLE_USERADMIN	<input type="checkbox"/>	Administers Users within the Securonix application
ROLE_BUSMANAGER	<input type="checkbox"/>	Business Unit Manager
ROLE_PRIVACYMASTER	<input type="checkbox"/>	Grives permission to decrypt data
ROLE_ACCESSCERTIFIER	<input type="checkbox"/>	Access certification Owner
ROLE_SYSTEMOWNER	<input type="checkbox"/>	System Owner
ROLE_ACCESS_SCANNER	<input type="checkbox"/>	Access Scanner Role
ROLE_LICENSEMANAGER	<input type="checkbox"/>	License Manager Role
ROLE_PRIVACYMASTERMASKING	<input type="checkbox"/>	Search user based on masked key
ROLE_SECURITY_ANALYST	<input checked="" type="checkbox"/>	Security Analyst
ROLE_HUNTERS	<input type="checkbox"/>	Hunters
ROLE_OPERATIONS_TEAM	<input type="checkbox"/>	Operations Team
ROLE_CASE_ANALYST	<input type="checkbox"/>	Case Analyst

2. Click **Save & Next**.

Assign Groups to the users

Based on the groups you select for this analyst, they will only be able to view or take actions on cases assigned to this group. Admin users can view all cases, regardless of the group to which the case is assigned. To assign groups to this analyst, complete the following steps:

1. Toggle to **Yes** to assign the user to a group.

The 'User Details' form has three tabs: 'Enter User Information' (active), 'Assign roles to the user', and 'Assign groups to the user'. A blue banner below the tabs reads: 'Manage multiple users by assigning them to the same group. Groups may also be used for case assignment and response.' Below this is an 'Add New Group' button. The main table has columns for 'Name', a toggle switch, and 'Type'.

Name		Type
Administrators	<input type="radio"/> NO	admin
SECURITYOPERATIONS	<input checked="" type="radio"/> YES	

To add a new group, Click **Add New Group** and enter the following information:

- **Name:** Enter the group name.
- **Type:** Select a group type from the dropdown.
- **Email:** Specify the group email address.

The 'Create Group' modal form contains the following fields: 'Name' (text input), 'Enter Group Name' (placeholder text), 'Type' (dropdown menu with 'None' selected), 'Choose Group Type' (placeholder text), and 'Email' (text input). A 'Save' button is located at the bottom right.

2. Click **Save & Next**.
3. Ensure the user was created successfully from the **Access Control** main screen.

Creating Groups

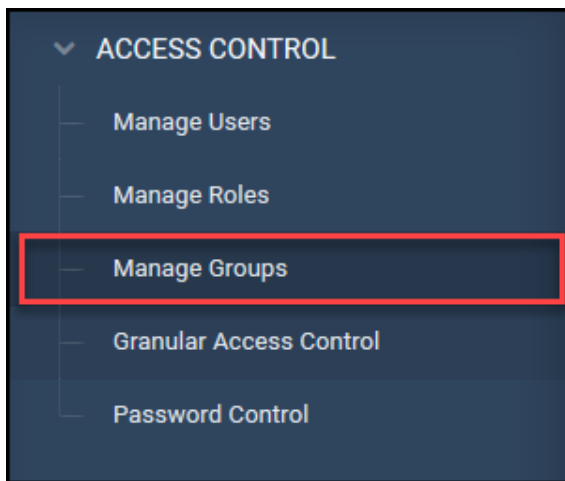
By creating groups and assigning users to them, you have more control over user permissions. You can directly assign roles to groups and assign organizations to groups. All users belonging to the group will inherit the roles and organizations assigned to the group.



Note: Groups are required to configure Granular Access Control. Granular Access Control is used to grant Groups such as Security Operations access to users, policies, and threat models on selected resources.

To create a group, complete the following steps:

1. Navigate to **Menu > Administration > Access Control**.
2. Click **Manage Groups** from the Access Control navigation panel.



1. Navigate to +.
2. Provide the following details:

Create Group

1

Enter Group Details

Add user(s) to group

Assign roles to group

Name

SECURITYOPERATIONS

Enter Group Name

Type

None

Choose Group Type

Email

admin@mycompany.com

Enter Group Email Address

Mail Box

default

Choose Mail Box

Parent Group

🔍

✕

Choose Parent Group

- **Name:** Enter a descriptive name for the group.
 - **Type:** Select a group type from the dropdown.
 - **Email:** Specify the group email address.
 - **Mail Box:** Select mail box from dropdown. Default: default.
 - **Parent group:** Search to select a Parent Group from existing groups (for example, Administrators).
3. Click **Next**.
 4. Click **Add User(s)** to add users to group or click **Next**.

Search for specific users to add

	User Name	Last Name	Email
<input type="checkbox"/>	1001	HARRY OGWA	HARRY.OGWA@scnx.com
<input type="checkbox"/>	1005	TERRY MERRITT	TERRY.MERRITT@scnx.com
<input type="checkbox"/>	1012	JOE KELLINGTON	JOE.KELLINGTON@scnx.com
<input type="checkbox"/>	1013	ROBERT WELLINGTON	ROBERT.WELLINGTON@scnx.com
<input type="checkbox"/>	1025	Ted Thomson	ted.thomson@scnx.com
<input type="checkbox"/>	1044	NORA LEWIS	NORA.LEWIS@scnx.com
<input type="checkbox"/>	1045	FAHAD WALKER	FAHAD.WALKER@scnx.com
<input type="checkbox"/>	1063	Meredith COLEMAN	Meredith.COLEMAN@scnx.com
<input type="checkbox"/>	1064	Cedric Castaneda	Cedric.Castaneda@scnx.com

Add Selected User(s)































- a. **Add User(s)**: Search for specific users or type * to search all, check the boxes of the users you would like to add, and click **Add Selected User(s)**.
 - b. **Next**: Proceed to **Assign roles to group**.
5. Toggle to **Yes** for each of the roles you would like to assign to the group.

Role Name		Description
ROLE_ADMIN	Yes	System Administrator
ROLE_AUDITOR	No	IT Auditor
ROLE_USERADMIN	No	Administrators Users within the Securonix application
ROLE_BUSMANAGER	No	Business Unit Manager
ROLE_PRIVACYMASTER	No	Grives permission to decript data
ROLE_ACCESSCERTIFIER	No	Access certification Owner
ROLE_SYSTEMOWNER	No	System Owner
ROLE_ACCESS_SCANNER	No	Access Scanner Role
ROLE_LICENSEMANAGER	No	License Manager Role
ROLE_PRIVACYMASTERMASKING	No	Search user based on masked key
ROLE_SECURITY_ANALYST	No	Security Analyst
ROLE_HUNTERS	No	Hunters
ROLE_OPERATIONS_TEAM	No	Operations Team
ROLE_CASE_ANALYST	No	Case Analyst

6. Click **Save**.




Managing Users, Groups, and Roles

From the left sidebar menu on the Access Control main screen, you can edit settings for users, roles, and groups, set Granular Access Control, and set password control options.

ACCESS CONTROL						
<div> <div> <div>×</div> <div>✈</div> <div>MENU</div> <div>Administration</div> <div>Access Control</div> </div> <div>Enter text to search...</div> <div> <div>🔍</div> <div>🔔</div> <div>👤</div> <div>Lpherson</div> </div> </div>						
<div> <div>+</div> <div>Enter your search criteria</div> <div>username</div> <div>🔍</div> </div>						
User Name	Enabled	First Name	Last Name	Email	Actions	
1001	<input checked="" type="checkbox"/>	HARRY	OGWA	HARRY.OGWA@scnx.com	  	
1005	<input checked="" type="checkbox"/>	TERRY	MERRITT	TERRY.MERRITT@scnx.com	  	
1012	<input checked="" type="checkbox"/>	JOE	KELLINGTON	JOE.KELLINGTON@scnx.com	  	
1013	<input checked="" type="checkbox"/>	ROBERT	WELLINGTON	ROBERT.WELLINGTON@scnx.com	  	
1025	<input checked="" type="checkbox"/>	Ted	Thomson	ted.thomson@scnx.com	  	
1044	<input checked="" type="checkbox"/>	NORA	LEWIS	NORA.LEWIS@scnx.com	  	
1045	<input checked="" type="checkbox"/>	FAHAD	WALKER	FAHAD.WALKER@scnx.com	  	
1063	<input checked="" type="checkbox"/>	Meredith	COLEMAN	Meredith.COLEMAN@scnx.com	  	
1064	<input checked="" type="checkbox"/>	Cedric	Castaneda	Cedric.Castaneda@scnx.com	  	
1065	<input checked="" type="checkbox"/>	Ainsley	Moses	Ainsley.Moses@scnx.com	  	
<div> <div>First</div> <div><</div> <div>1</div> <div>2</div> <div>3</div> <div>4</div> <div>5</div> <div>></div> <div>Last</div> <div>Show</div> <div>10</div> <div>▼</div> </div>						Total results : 59 Total pages : 6

Manage Users

You can take the following actions from the icons on the right side of each user listing:

	Change Password
	Edit User
	Delete User



Note: You cannot delete or disable the Admin user.

Manage Roles

ACCESS CONTROL		
Manage Users		
Manage Roles		
Manage Groups		
Granular Access Control		
Password Control		

Role Name	Description	Actions
ROLE_ACCESSCERTIFIER	Access certification Owner	
ROLE_ACCESS_SCANNER	Access Scanner Role	
ROLE_ADMIN	System Administrator	
ROLE_AUDITOR	IT Auditor	
ROLE_BUMANAGER	Business Unit Manager	
ROLE_CASE_ANALYST	Case Analyst	
ROLE_HUNTERS	Hunters	
ROLE_LICENSEMANAGER	License Manager Role	
ROLE_OPERATIONS_TEAM	Operations Team	
ROLE_PRIVACYMASTER	Gives permission to decrypt data	

First < 1 2 > Last Show 10

Total results: 14 | Total pages: 2

You can take the following actions on the right side of each role listing:

	Edit Role
	Delete Role



Note: A special role in ArcSight UBA gives users with the role ROLE_PRIVACYMANAGERMASKING the ability to unmask (not unencrypt) masked data with a few steps. When creating users and groups, enable the role ROLE_PRIVACYMANAGERMASKING to use this feature.

Manage Groups


ACCESS CONTROL		
Manage Users		
Manage Roles		
Manage Groups		
Granular Access Control		
Password Control		

Name	Type	Email	Actions
Administrators	admin		
SECURITYOPERATIONS		admin@mycompany.com	

First < 1 > Last Show 10

Total results: 2 | Total pages: 1

You can take the following actions on the right side of each group listing:

	Edit Group
	Delete Group

Granular Access Control

You can further restrict access at the following levels:

- User
- Resource
- Resource Group
- Policy Category
- Threat Model

Configure Granular Access Control for the Groups you created in previous steps. Granular, data-level access control grants Groups such as Analysts access to users, policies, and threat models on selected resources. When data level access is enabled for a group, logged-in users can only view the accounts (access/activity), and policy and threat violations on the resources for which you have provisioned access. All other resources are restricted.

At the resource level, you can restrict access to the following:

Admin-level access: Complete access to accounts (access/activity) on the resource, even for accounts owned by users who do not belong to the user and resource groups to which the group has been granted access. Admin-level access is granted when creating Roles.

Non-admin level access: Access only to those accounts (access/activity) on resources that are owned by users belonging to the user and resource groups for which the group has been granted access.

Resource-group level access: You can control access at the resource (data source) level. If a resource (data source) is part of multiple resource groups, you can restrict access to accounts (access/activity) belonging to specific resource groups. For instance, if a resource (data source) is part of Windows Events and DLP, access can be restricted to only the DLP stream.

How Granular Access Control Works

The application looks at the roles and the data level access associated with a user to make only other associated users and resources visible to that user.

When the user logs into the application, ArcSight UBA performs the following actions:

1. Checks for roles associated with logged in user.
2. Checks for resources and resource groups associated with the logged in user.

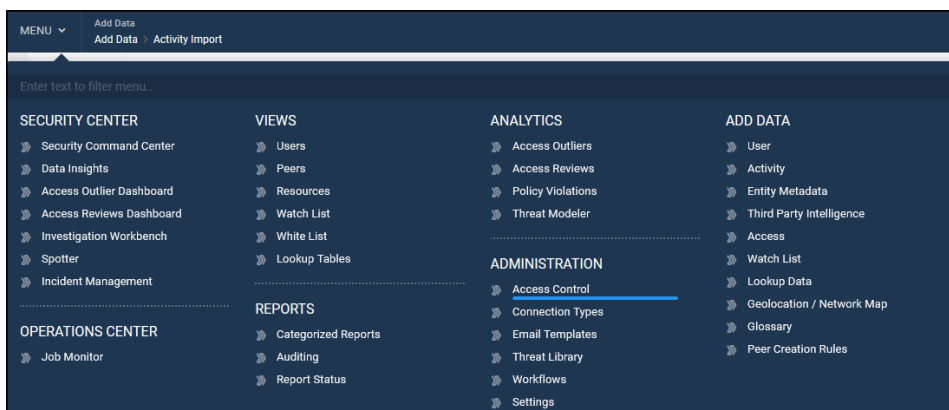
Notes:

- The capabilities of the logged in user are based on the role assigned to the user.
- The list of users the logged in user can see is limited based on their role and the user and resource groups to which they have access.
- The list of resources the logged in user can access is limited based on their role and the resource groups to which they have been granted access.
- The list of violations for policies and threat models the user can view and access is limited based on the resources to which they have been granted access.

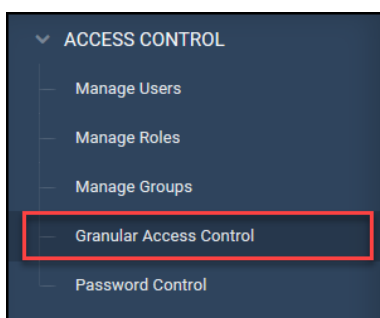
Setting up Granular Access Control

To enable Granular Access Control, complete the following steps:

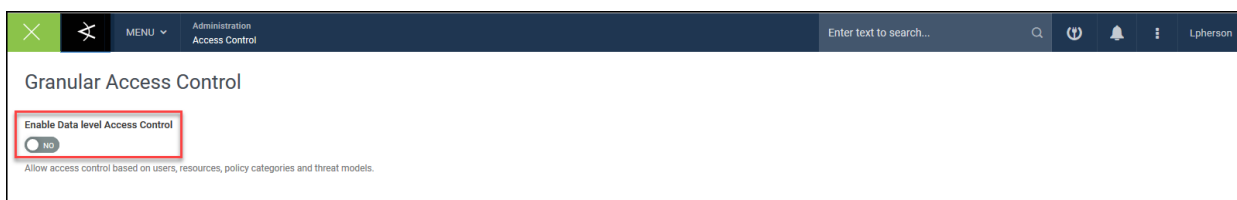
1. Navigate to **Menu > Administration > Access Control**.



2. Click **Granular Access Control** from the Access Control navigation panel.



3. Set **Enable Data level Access Control** to **Yes**.



4. Select a Group from the **Sec Group** to view Access Configurations for the group.

5. Click **Add** to edit Access Configurations for the selected group.

Granular Access Control

Enable Data level Access Control

YES

Allow access control based on users, resources, policy categories and threat models.

Select Sec Group

Analysts

Select Sec group to view tenant configuration

TENANT	ACCESS CONFIGURATIONS				ACTIONS
	USER	RESOURCE GROUP	POLICY CATEGORY	THREAT	
Securonix	No user based access control configured. Click on edit button to add configuration.	undefined	undefined	undefined	Add

First < 1 > Last TOTAL 1

6. Enable **What users do you want to grant access to?** slider to **YES** to select users the group will be able to view.

What users you want to grant access to?

YES

SEARCH BY	SEARCH CONDITION	PROVIDE VALUE	SELECT OPERATOR	
location	Equal To	Dallas	AND	+ -
employeetype	Equal To	Full Time	AND	+ -
manageremployeeid	Equal To	6782	AND	+ -

1. Specify the following:

- **Search By:** Select a user attribute from the dropdown. Example: Location.
- **Search Condition:** Select a condition from the dropdown. Example: Equal To.
- **Provide Value:** Provide a value for the selected user attribute. Example: Dallas.
- **+/-:** Click to add/remove users.



Note: The group will only be able to see the users selected.

7. Enable **What resources you want to grant access to?** to **YES** to select resources the group will be able to view.

What resources you want to grant access to?

YES

Type To Filter

☐ AD

☒ ADAccess

☐ Bluecoat

☒ CiscoACS_10102017_XON

1. Select the resources the group will be able to view.

2. Type text to Filter list.



Note: The group will only be able to see the resources selected.

8. Enable **What policy categories you want to grant access to?** to **YES** to select the categories of policies the group will be able to view.

What policy categories you want to grant access to?

YES

Type To Filter

☒ INSIDER THREAT

☐ CONFIGURATION ERROR

☒ TRAFFIC ANOMALY

☒ IDENTITY ISSUE

1. Select the policy categories the group will be able to view.
2. Type text to Filter list.



Note: The group will only be able to see violations for the policy categories selected.

9. Enable **What threat models you want to grant access to?** to **YES** to select the threat models the group will be able to view.

What threat models you want to grant access to?

☒ YES

Type To Filter

☒ Insider Threat

1. Select the threat models the group will be able to view.
2. Type text to Filter list.



Note: The group will only be able to see violations for the threat models selected.

10. Click Save Configuration.
11. View the configuration on the Granular Access Control screen.

Granular Access Control

Enable Data level Access Control ☒

Allow access control based on users, resources, policy categories and threat models.

Select Sec Group

Analysts

Select Sec group to view tenant configuration

TENANT	ACCESS CONFIGURATIONS				ACTIONS
	USER	RESOURCE GROUP	POLICY CATEGORY	THREAT	
Securonix	1 Rules are configured → location EQUALS Dallas → employeetype EQUALS Full Time → manageremployeid EQUALS 6782	2 Select Operator → ADAccess → CiscoACS_10102017_XON	3 Policy categories are configured → INSIDER THREAT → TRAFFIC ANOMALY → IDENTITY ISSUE	4 Threat models are configured → Insider Threat	undefined

First < 1 > Last TOTAL 1

12. Set **Enable Data level Access Control** slider to **NO** to turn off Granular Access Control.

Password Control

Toggle slider to **Yes** to manage password settings.

ACCESS CONTROL

Manage Users

Manage Roles

Manage Groups

Granular Access Control

Password Control

Enable Password Control?

YES

Minimum Length

8

Set minimum length of password

Maximum Length

16

Set maximum length of password

Minimum Upper Case Letters

2

Set minimum upper case letters required in password.

Minimum Lower Case Letters

2

Set minimum lower case letters required in password.

Numbers Allowed?

YES

Minimum Numbers

2

Set minimum numbers required in password.

Special Characters Allowed?

YES

Lock after 'n' login failures

20

Set the number of login failures after which the account is locked.

20

Set the number of login failures after which the account is locked.

Password never expires?

☐ NO

Password expiration period

20

Set the number of days after which the password will expire.

Remainder Interval

Set the number of days for password expiry notification.

Password Settings

Parameter	Description
Minimum Length	The minimum number of characters used in a password.
Maximum Length	The maximum number of characters used in a password.
Minimum Upper Case Letters	The minimum number of upper case letters required in a password.
Minimum Lower Case Letters	The minimum number of lower case letters required in a password.
Numbers Allowed?	By default, numbers are allowed in passwords. Toggle to No to disallow numbers in passwords.
Minimum Numbers	The minimum count of numbers required in a password.
Special Characters Allowed	This option only appears if Numbers Allowed? is set to Yes . By default, special characters are allowed in a password. Toggle to No to disallow special characters in a password.
Lock after 'n' login failures	The number of login attempts that will result in account lockout.
Password never expires?	Set to Yes to have passwords be non-expiring. If set to YES , the password expiration period and Remainder Interval settings disappear.
Password expiration period	If Password never expires? is set to No , enter the number of days before a password change is required.
Remainder Interval	Set the number of days for password expiry notification.



Note: From a security standpoint, best practice recommends the Lock **after 'n' failures** setting.

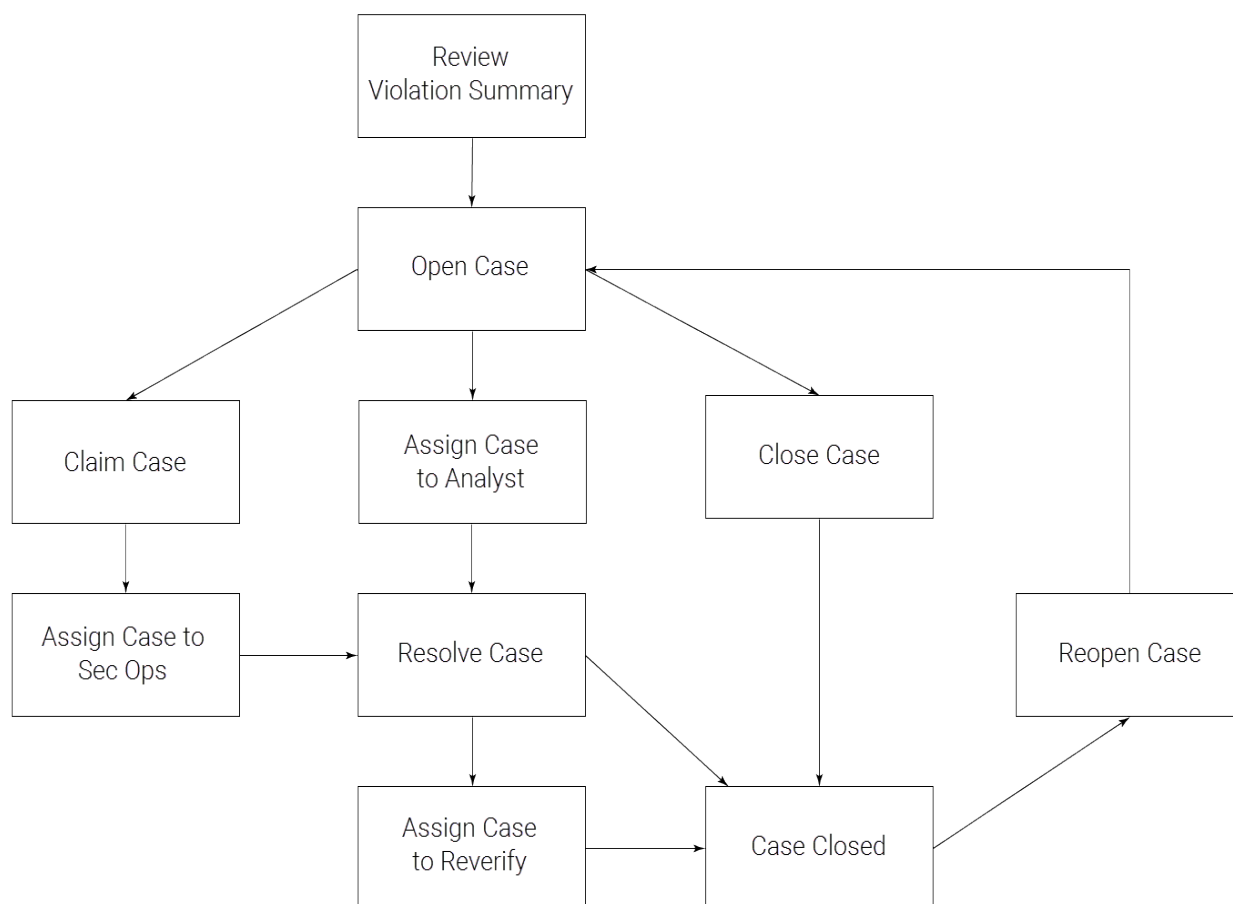
Workflows

ArcSight UBA provides several default workflows to handle incidents and case management. You can create custom workflows to take specific actions on cases, or you can make changes to the existing workflows. Workflows are invoked in the following screens within the application:

- Security Command Center
- Policy Violations
- Investigation Workbench

The diagram displays the following sample workflow:

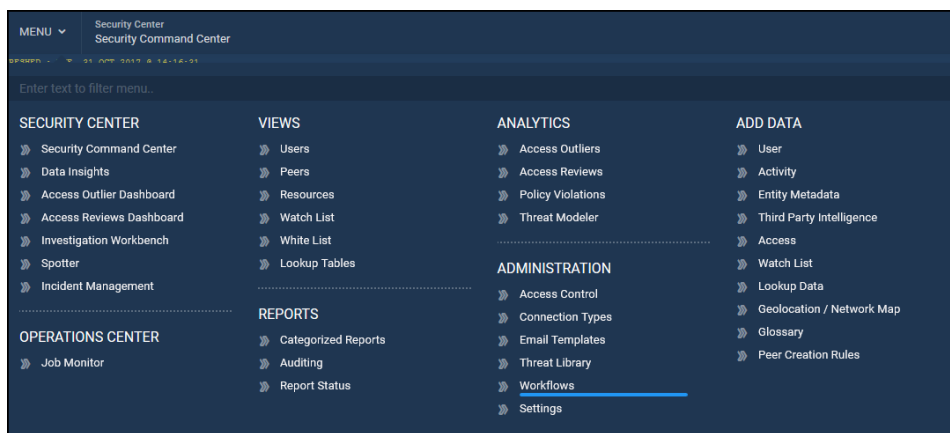
1. The user begins the case workflow by creating a case from the [Security Command Center](#).
2. The user takes action to claim the case, assign the case to another analyst, or close the case.
3. The analyst to whom the case is assigned takes appropriate action to resolve the case.
4. The case is closed or assigned to another analyst to re-verify the resolution, or the user can reopen the closed case for further investigation. See [Incident Management](#) in the ArcSight UBA User Guide for more information about cases.



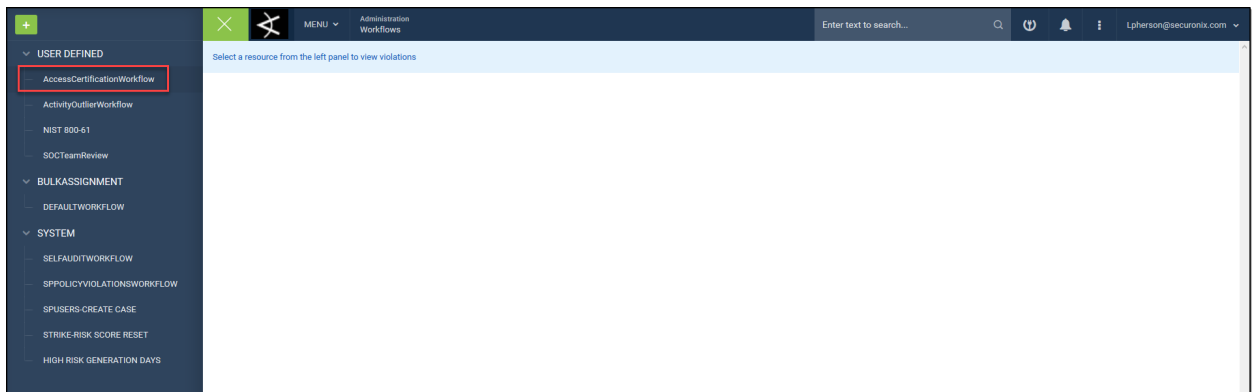
Configuring Workflows

To configure workflows, complete the following steps:

1. Navigate to **Menu > Administration > Workflows**.



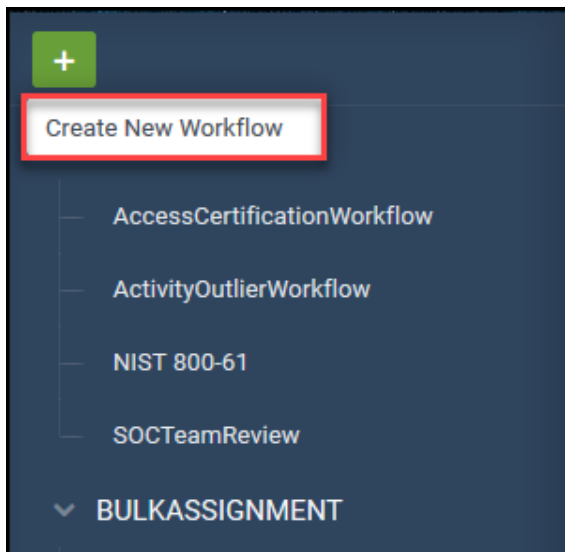
2. View existing **User Defined**, **Bulk Assignment**, and **System** workflows from the left navigation panel.



3. Click the name of a workflow to configure.

OR

4. Click **+ > Create New Workflow**.



General Details

1. Complete the following information:

- a. **Workflow Name:** Enter a unique name for the workflow.
- b. **Default Assign To:** Select one or all of the **Assign To** options (Groups, Users, and Other).
To change the order of the **Assign To** options, use your mouse to click and drag the options into the correct order.



Note: The order in which the options are selected will be the order in which the application will assign the case. For example, if the order is Group followed by User, ArcSight UBA will try to assign the case to the group. If the group is unavailable, the case is assigned to the individual user selected.

- a. **Assign Case to selected Group:** Select from dropdown to assign cases in this workflow to a particular group.

The screenshot shows the 'Default Assign To' configuration. The checkbox 'Assign Case to selected Group' is checked. Below it is a dropdown menu currently showing 'Administrators'. A search bar with a magnifying glass icon is visible. The dropdown list is open, showing options: '-Select-', 'Administrators' (highlighted in blue), and 'SECURITYOPERATIONS'.

- b. **Assign Case to select User:** Select from dropdown to assign cases in this workflow to a particular user.

The screenshot shows the 'Default Assign To' configuration. The checkbox 'Assign case to selected User' is checked, while 'Assign Case to selected Group' is unchecked. Below it is a dropdown menu currently showing '-Select-'. A search bar with a magnifying glass icon is visible. The dropdown list is open, showing options: '-Select-' (highlighted in blue), 'admin [Admin Admin]', 'auditor [IT Auditor]', 'useradmin [User Administrator]', and 'accessscanner [Access'.

- c. **Assign case to Other:** Use > or >> to assign case in this workflow to other.
Example: Organization Owner.

Default Assign To

☐ Assign Case to selected Group

☐ Assign case to selected User

☒ Assign case to Other

Account Owner

Organization Owner

Peer Owner

Policy Owner

Policy Remediator

Policy Violator

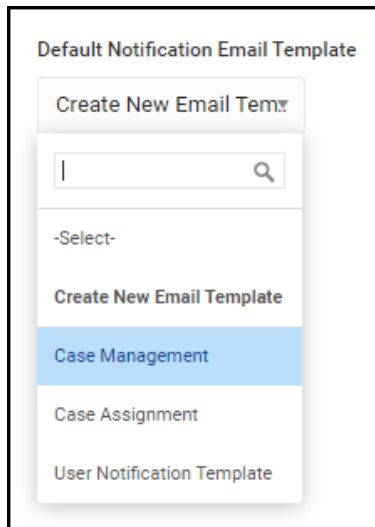
>

>>

<<

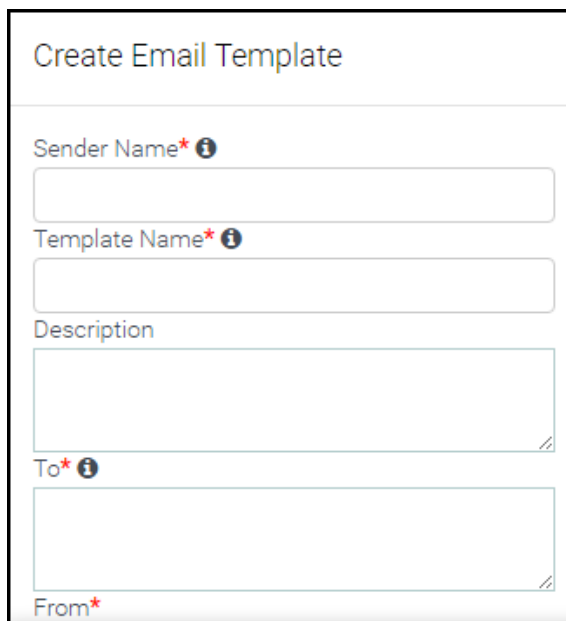
<

- a. **Default Notification Email Template:** Select from dropdown or **Create New Email Template:**



The screenshot shows a dropdown menu titled "Default Notification Email Template". At the top of the dropdown is a button labeled "Create New Email Template". Below the button is a search bar with a magnifying glass icon. Under the search bar is a list of options: "-Select-", "Create New Email Template", "Case Management" (which is highlighted in blue), "Case Assignment", and "User Notification Template".

Create New Email Template: Complete the pop up form to create a new template:



The screenshot shows a form titled "Create Email Template". The form contains the following fields:

- Sender Name*** (required, with an information icon): A text input field.
- Template Name*** (required, with an information icon): A text input field.
- Description**: A text area.
- To*** (required, with an information icon): A text input field.
- From*** (required): A text input field.

From*
test@securonix.com
CC ⓘ

BCC ⓘ

Subject ⓘ

HTML Enabled
☒ YES

Store in Outbox prior to sending?

☒ YES ☐ NO

Use this template for *

-Select-

Owner 

Administrators
SECURITYOPERATIONS

>

>>

<<

<

Email Body ⓘ
[Add Email Template Variables](#)

B

I

U


abc


x₁


x²


T₁


HI

















































































































- Sender Name:** Enter the name of the sender.
- Template Name:** Enter a unique template name.
- Description:** Enter a brief description of the template.
- To:** Enter the email address of the recipient in the form of recipient@domain.com.
- CC:** Enter the email address of the carbon copied recipient in the form of recipient@domain.com.

- f. **BCC:** Enter the email address of the blind carbon copied recipient in the form of recipient@domain.com.
- g. **Subject:** Enter a one-line description of the contents of the email.
- h. **HTML Enabled:** Select **Yes** or **No**. Default: **Yes**.
- i. **Store in Outbox prior to sending?:** Select **Yes** or **No**. Default: **Yes**.
- j. **Use this template for:** Select from dropdown. Example: Access Outlier.
- k. **Owner:** Use > or >> to select the user that will own the organization. Use < or << to remove users.
- l. **Email body:** Enter the contents of the email.
- m. **Add Email Template Variables:** Select variables to add to the email and click **Add**. Example: \${access_value}.

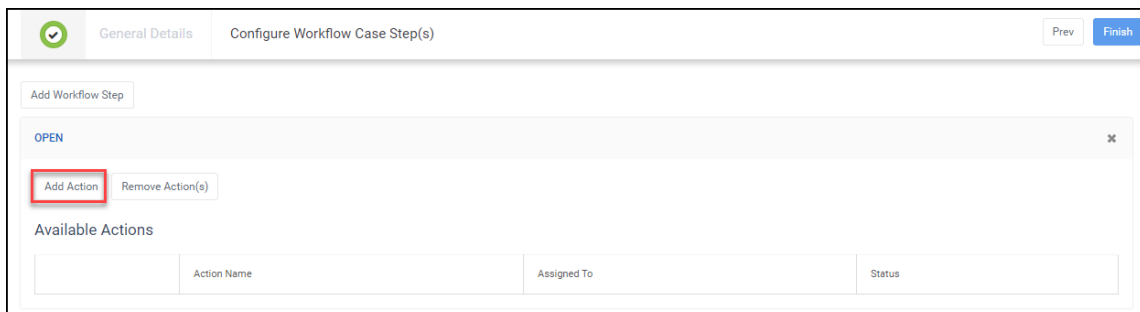
Email			
<input type="checkbox"/>	Variable Name <small>⌵</small>	Description	Module
<input type="checkbox"/>	\${access_history}	Access history	Access Review
<input type="checkbox"/>	\${access_value}	Access value	Access Outlier
<input type="checkbox"/>	\${account_name}	Account name	Event Import Quick Alerts
<input type="checkbox"/>	\${approver_email}	Approver Email	User Import
<input type="checkbox"/>	\${approver_firstname}	Approver Firstname	User Import
<input type="checkbox"/>	\${approver_lastname}	Approver Lastname	User Import
<input type="checkbox"/>	\${assignee_first_name}	Assignee first name	Case Management
<input type="checkbox"/>	\${assignee_last_name}	Assignee last name	Case Management
<input type="checkbox"/>	\${assignee_manager}	Assignee's manager	Case Management
<input type="checkbox"/>	\${attributes}	Attributes	Event Import Quick Alerts
<input type="checkbox"/>	\${attribute_value}	Attribute value	Access Outlier

2. Click **Save & Next** to proceed to [Configure Workflow Case Step\(s\)](#).

Configure Workflow Case Step(s)

Add steps in the workflow to configure actions for assigning the case, executing pre-defined functions, changing case status, sending notifications, opening user input form, and updating SLAs.

1. Click **Add Action** to add an action for this step in the workflow.



General Details | Configure Workflow Case Step(s) | Prev | Finish

Add Workflow Step

OPEN

Add Action Remove Action(s)

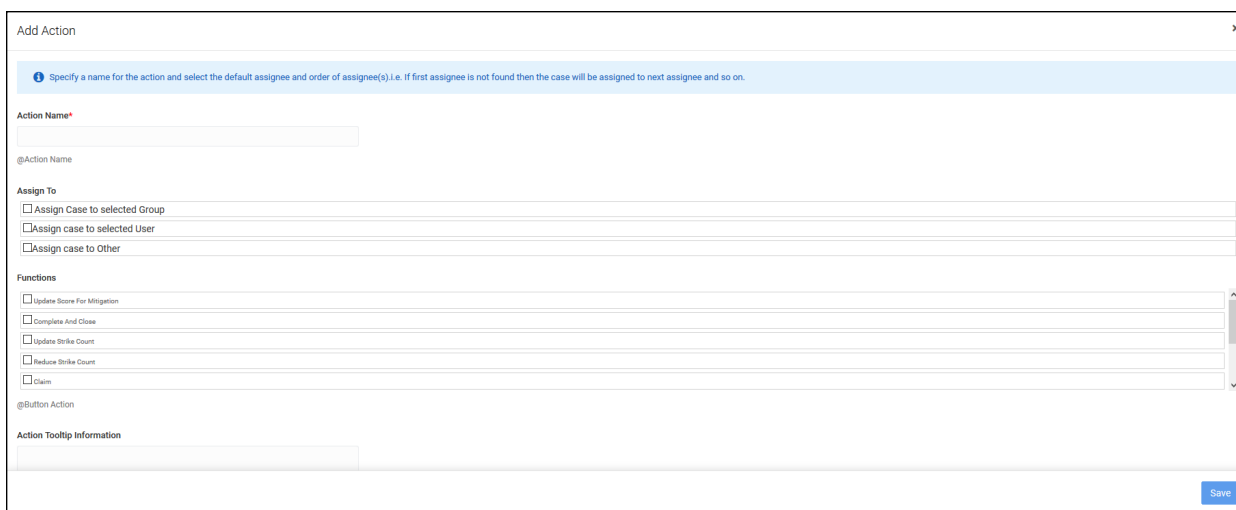
Available Actions

Action Name	Assigned To	Status
-------------	-------------	--------



Note: The Open case step for this workflow is already in place.

2. Configure actions:



Add Action

Specify a name for the action and select the default assignee and order of assignee(s). i.e. If first assignee is not found then the case will be assigned to next assignee and so on.

Action Name*

@Action Name

Assign To

☐ Assign Case to selected Group

☐ Assign case to selected User

☐ Assign case to Other

Functions

☐ Update Score For Mitigation

☐ Complete And Close

☐ Update Strike Count

☐ Reduce Strike Count

☐ Claim

@Button Action

Action Tooltip Information

Save

@Button Action

Action Tooltip Information

@This is to show Action Information in tooltip

Change Case Status to

Do Not Change ▾

Notification Email Template

-Select- ▾

Show User Input Form? ⓘ

☐ NO

SLA Configuration

☐ NO

Save

- a. **Action Name:** Enter a unique name for the action.
- b. **Assign to:** Select assignees and use mouse to drag options into the order in which the application will assign the case.
- c. **Functions:** Select functions and use mouse to drag into the order in which the application will process them.
- d. **Action Tooltip Information:** Enter information to show in tool tip.
- e. **Change Case Status to:** Select from dropdown. Example: Open.
- f. **Show User Input Form?:**
 1. Select **Yes** to create an input screen that will be displayed to the user when this action is taken during the case work flow.



Note: You can add fields to an input screen including text, dropdown menu choices, rich text, assignment option, date, and file upload. You can add fields in one section or create separate screen sections. You can require input by setting the toggle to **Yes**.

2. Click **Design New Screen** to create new input screen and **Save**:

Design New Screen

Screen Name
Screen1

@Screen Name

Create New Section

Field Label	Field Type	Field Value	Dimension	Required?	
Comments	textarea		Width Height	NO	+ -

Save

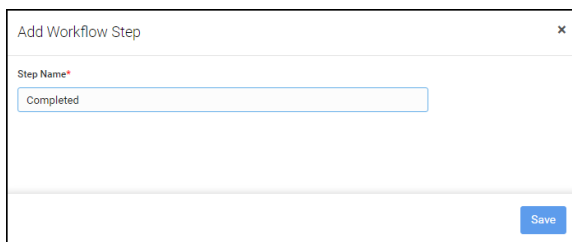
- a. **Screen Name:** Enter a unique screen name. Example: User Comment.
- b. **Create New Section:** Click to create a new Section.
- c. **Field Label:** Enter a label name for the field.
- d. **Field Type:** Select from dropdown. Example: text area.
- e. **Field Value:** Select if available for Field Type.
- f. **Dimension:** Enter a Width and Height.
- g. **Required?:** Toggle to **Yes** to require the user complete input screen.
- h. **+/-:** Use to add/remove comments.
- g. **SLA Configuration:** Toggle to **Yes** to enable SLA configuration.

SLA Configuration

YES

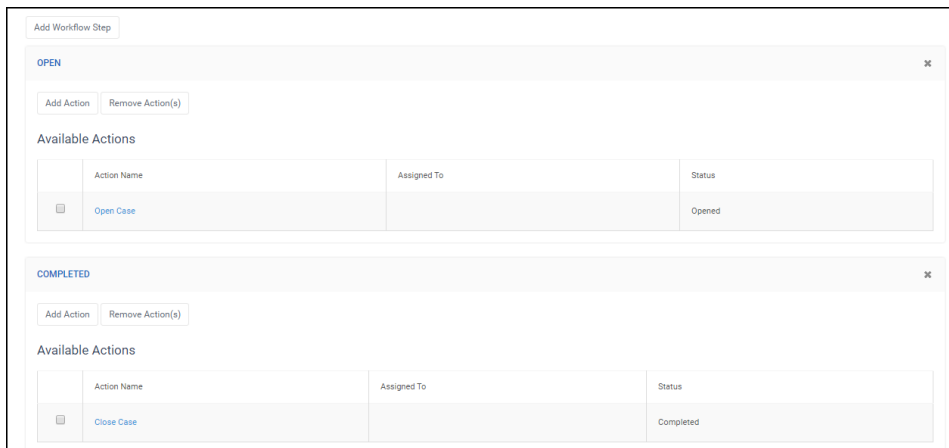
Level	Duration Days	Notification Email Template	Functions	Add/Remove
		-Select-	<input type="checkbox"/> Assign <input type="checkbox"/> Create JIRA Issue <input type="checkbox"/> Update Workflow	+ -

- a. **Level:** Enter a value for SLA level.
 - b. **Duration Days:** Enter a numeric value for duration in days.
 - c. **Notification Email Template:** Select from dropdown or **Create New Email Template**.
 - d. **Functions:** Select from list.
 - e. **+/-:** Use to add/remove entries.
3. Click **Add Workflow Step** to add a new step to the workflow.



A dialog box titled "Add Workflow Step" with a close button (X) in the top right corner. It contains a text input field labeled "Step Name*" with the word "Completed" entered. Below the input field is a blue "Save" button.

1. Enter a **Step Name**. Example: Completed.
2. Click **Save**.
3. **Add Actions** for this step in the workflow using the steps described previously.
4. View available actions for each step in the workflow.
Click **Remove Action(s)** to remove actions from steps.



The workflow editor interface shows two steps: "OPEN" and "COMPLETED". Each step has a header bar with its name and a close button (X). Below each header are "Add Action" and "Remove Action(s)" buttons. Under the "OPEN" step, the "Available Actions" table shows one action: "Open Case" with a status of "Opened". Under the "COMPLETED" step, the "Available Actions" table shows one action: "Close Case" with a status of "Completed".

	Action Name	Assigned To	Status
<input type="checkbox"/>	Open Case		Opened

	Action Name	Assigned To	Status
<input type="checkbox"/>	Close Case		Completed

5. Click **Finish**.
6. View or edit Workflow from the left navigation panel on the **Menu > Administration > Workflows** main screen.

The screenshot displays the 'Administration Workflows' interface. On the left, a sidebar lists various workflow categories: USER DEFINED, BULK ASSIGNMENT, and SYSTEM. Under 'USER DEFINED', 'NIST 800-61' is highlighted with a red box. The main panel is titled 'Configure Workflow Case Step(s)' and features a 'Add Workflow Step' button. Below this, there are two sections: 'OPEN' and 'CLAIMED', each with an 'Add Action' and 'Remove Action(s)' button. The 'OPEN' section contains a table with two rows of available actions: 'ASSIGN TO USER' (status: OPEN) and 'CLAIM' (status: CLAIMED). The 'CLAIMED' section contains a table with three rows of available actions: 'ASSIGN TO USER' (status: OPEN), 'ACCEPT RISK' (status: COMPLETED), and 'CLOSE AS FIXED' (status: COMPLETED).

Available Actions (OPEN)

	Action Name	Assigned To	Status
<input type="checkbox"/>	ASSIGN TO USER		OPEN
<input type="checkbox"/>	CLAIM		CLAIMED

Available Actions (CLAIMED)

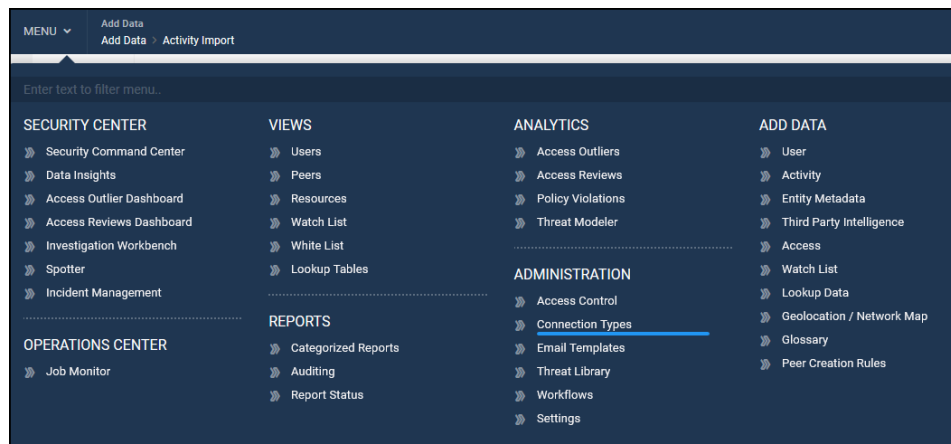
	Action Name	Assigned To	Status
<input type="checkbox"/>	ASSIGN TO USER		OPEN
<input type="checkbox"/>	ACCEPT RISK		COMPLETED
<input type="checkbox"/>	CLOSE AS FIXED		COMPLETED

Connection Types

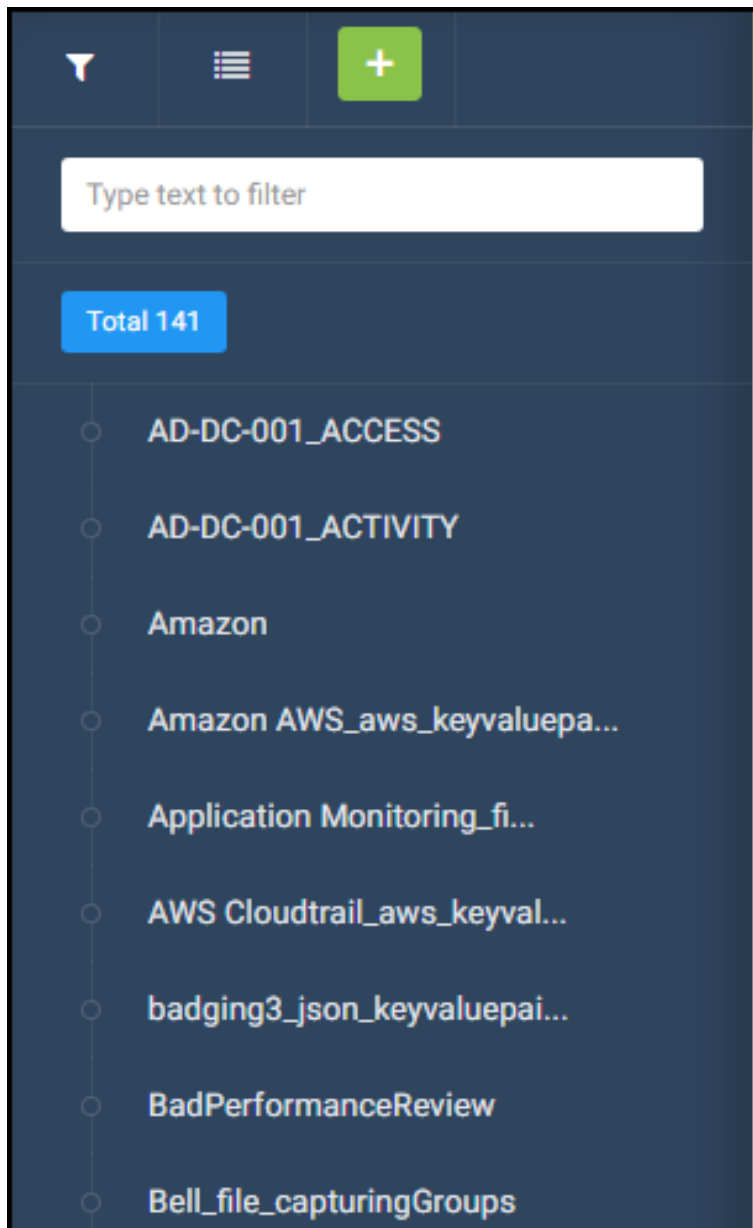
When you ingest data into ArcSight UBA, you must set up connections with the source system. These connections can all be viewed collectively in Connection Types.

Managing Connection Types


To manage Connection Types, navigate to **Menu > Administration > Connection Types**.

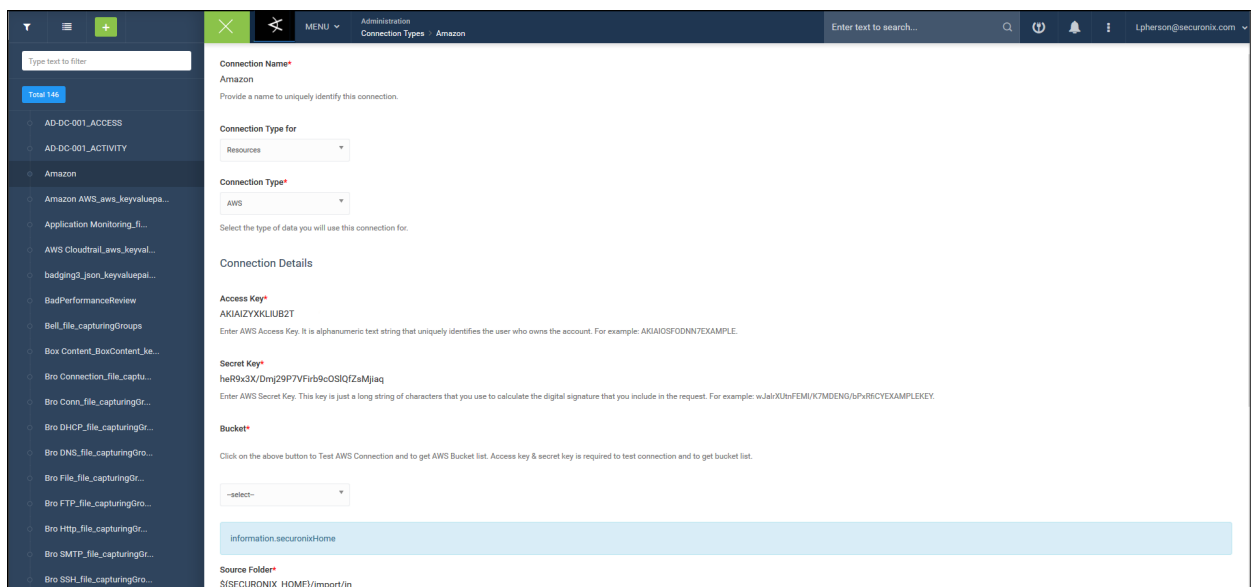


From the left navigation panel, take the following actions:



- Filter the connection types using the Filter Icon .

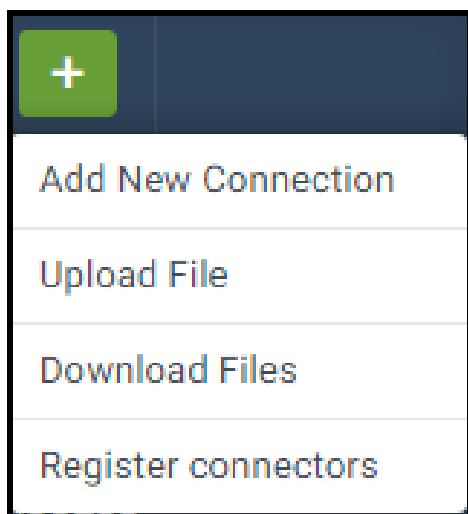
- Use the Advanced Options icon  for advanced filtering of the connection types.
- Click the + button to add a new connection, upload or download a file for connection types, and register connectors.
- Click any pre-configured connection type from the left panel to view, edit, or delete.



The screenshot shows the 'Add New Connection' form in the Securonix Administration console. The left sidebar lists various connection types, including 'Amazon'. The main form area is titled 'Connection Name' and 'Amazon'. It includes fields for 'Connection Type for' (Resources), 'Connection Type' (AWS), 'Access Key' (AKIAIZYXXLIUBZT), 'Secret Key' (heR9x3X/Dmg29P7VFib9cOSIQZ4Mjiaq), and 'Bucket' (a dropdown menu). A 'Test' button is visible at the bottom of the form. The top navigation bar shows 'Administration', 'Connection Types', and 'Amazon'.

Adding a New Connection Type

To add a new connection type, click the + button, and select **Add New Connection** from the drop-down.



Add the new connection in the screen that appears to the right.

Connection Name*

Provide a name to uniquely identify this connection.

Connection Type for

-Select- ▼

Connection Type*

-Select- ▼

Select the type of data you will use this connection for.

Connection Details

Enter details into the respective fields, select the relevant options from the dropdown, and click **Save**.

This new connection type becomes available in the left panel, which you can edit or delete later.

Example: Configure CEF Export Connection

To configure a connection for CEF export, complete the following steps:

1. Navigate to **Menu > Administration > Connection Types**.
2. Click **+** to add a new connection.
3. Complete the following information:

The screenshot shows the ArcSight Administration console. On the left is a sidebar with a search bar and a list of connection types. The main area displays the 'Add Connection' form for 'CEExport'. The form includes fields for 'Connection Name' (CEExport), 'Connection Type for' (Export Policy Violations), and 'Connection Type' (CEF Export). Below these are 'Connection Details' including 'Protocol' (udp), 'Host' (192.168.1.35), and 'Port' (514). There is a 'Generate Token?' toggle set to 'NO' and a detailed note about token generation and the URL to use for access.

- **Connection Name:** Provide a unique name for the connection. Example: CEFExport.
- **Connection Type for:** Select **Export Policy Violations** from dropdown.
- **Connection Type:** Select **CEF Export** from dropdown.



Note: You may also select RSA Archer or RSA Netwitness to export CEF from ArcSight UBA.

Connection Details

- **Protocol:** Enter connection protocol. Example: UDP.
- **Host:** Enter the IP address to which you will export CEF data.
- **Port:** Enter the port for the IP address to which you will export CEF data.
- **Generate token:** Enable slider to YES to generate a token.

This will create a user called "siemuser" and a role called "ROLE_siemrole" under **Configure > Access Control**. This will also create a token that can be used to access the Securonix application from ArcSight ESM. You can create a device URL in ArcSight ESM using following URL: `https://<hostname>:<port>/Snypr/manageData/showUserSearch?token=${generated-token}&accountid=${destinationUserName}`



Note: Replace <hostname> with appropriate network address/domain name and <port> with port number.

4. Click **Save**.

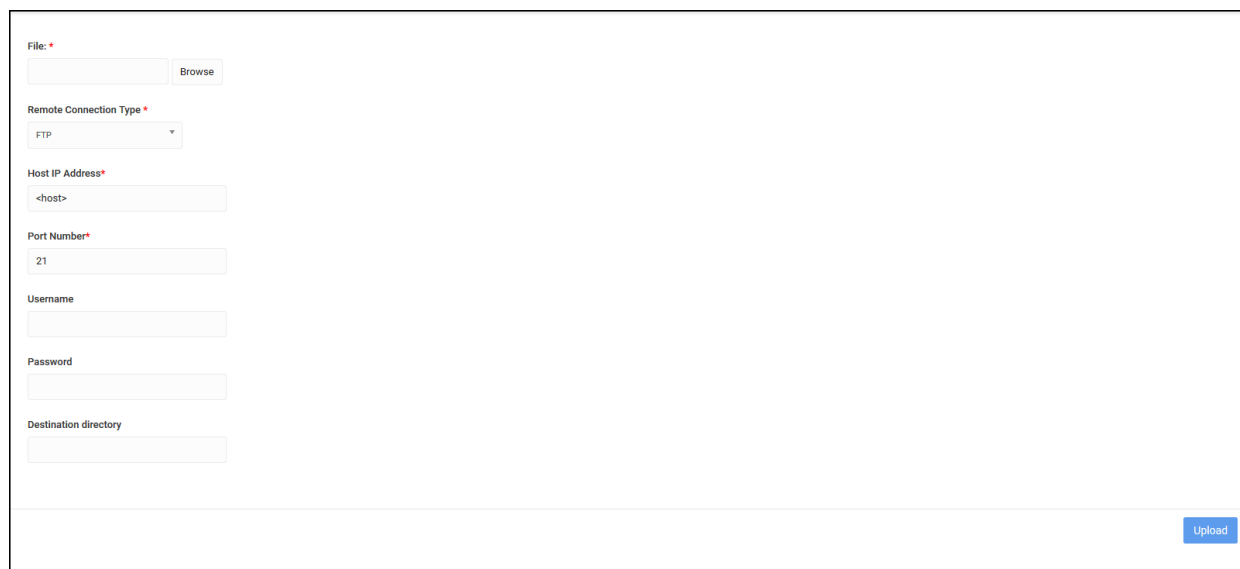
Uploading or Downloading Files

Click the + button to upload or download files for the connection types. This functionality allows you to FTP, SFTP, or SCP any file to a source or destination of your choice.

Upload Files

Use this function to upload files to ArcSight UBA directories. Example: Add a file to **securonix/tenants/<tenantname>/securonix_home/import/in** to import activity data.

To upload files to a ArcSight UBA directory, complete the following information:



The screenshot shows a web form for uploading files. It includes the following fields and controls:

- File:** A text input field with a red asterisk, followed by a "Browse" button.
- Remote Connection Type:** A dropdown menu with "FTP" selected.
- Host IP Address:** A text input field with a red asterisk, containing the placeholder text "<host>".
- Port Number:** A text input field with a red asterisk, containing the value "21".
- Username:** A text input field.
- Password:** A text input field.
- Destination directory:** A text input field.
- Upload:** A blue button located at the bottom right of the form.

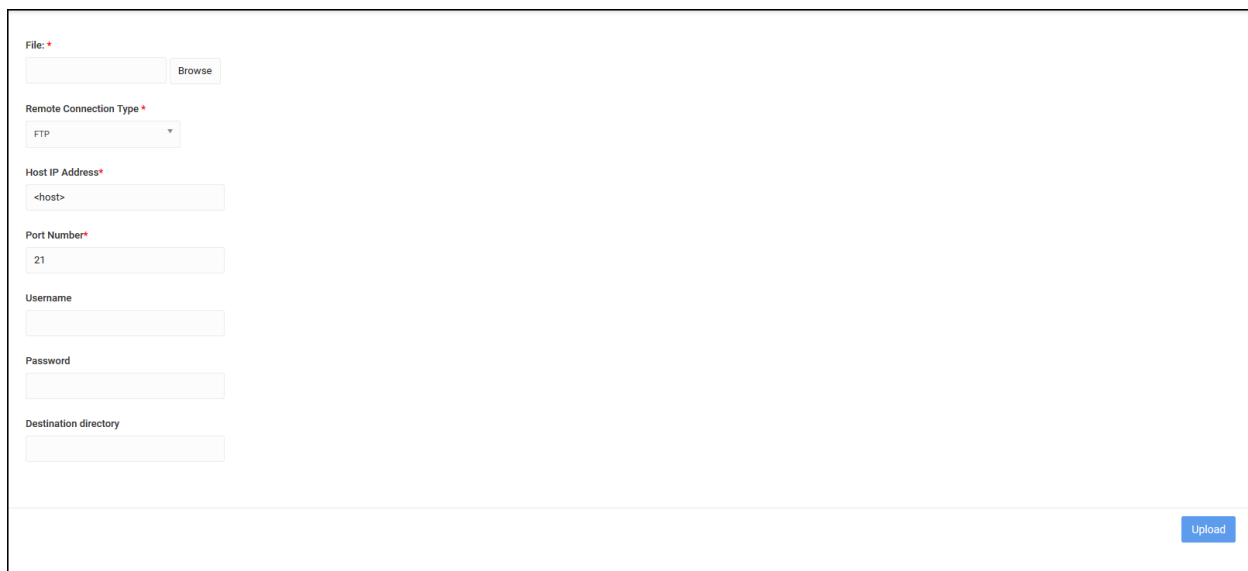
- **File:** Specify the file name and path or click Browse to select from local machine.
- **Remote Connection Type:** Select from the dropdown.
- **Host IP Address:** Select the Host IP address from which to upload the file.
- **Port Number:** Provide the port number. Default: 21 of the host IP address.
- **Username:** Provide the username for the server.
- **Password:** Provide the password for the server.
- **Destination directory:** Provide the destination directory into which to upload the file.
Example: **securonix/tenants/<tenantname>/securonix_home/import/in**.

Click **Upload**.

Download Files

Use this function to download files from ArcSight UBA directories. Example: Download a properties file from **securonix/tenants/<tenantname>/securonix_home/response/activedirectory** to edit connection details.

To download files from a ArcSight UBA directory, complete the following information:



The screenshot shows a web form for configuring a remote connection. It includes the following fields and controls:

- File:** A text input field with a red asterisk, followed by a "Browse" button.
- Remote Connection Type:** A dropdown menu with "FTP" selected and a red asterisk.
- Host IP Address:** A text input field with a red asterisk and a placeholder value "<host>".
- Port Number:** A text input field with a red asterisk and a placeholder value "21".
- Username:** A text input field.
- Password:** A text input field.
- Destination directory:** A text input field.
- Upload:** A blue button located at the bottom right of the form.

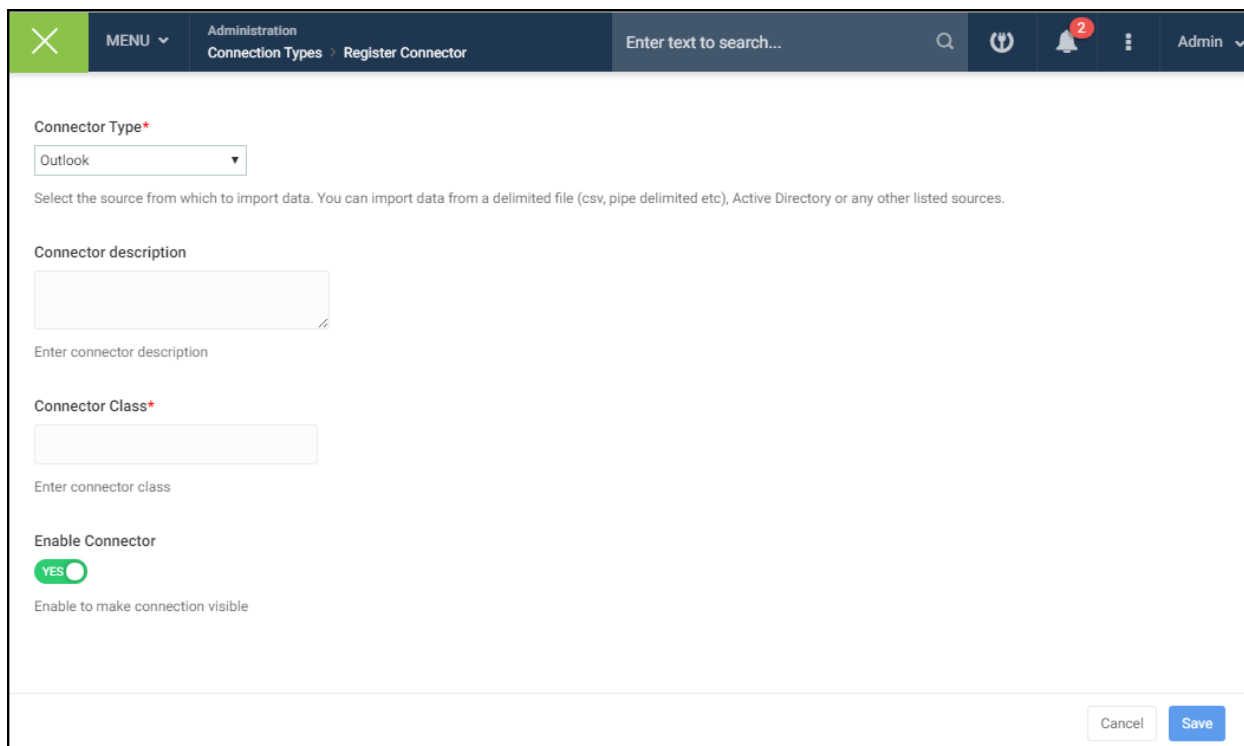
- **Remote Connection Type:** Select from the dropdown.
- **Host IP Address:** Select the Host IP address to which to download the file.
- **Port Number:** Provide the port number. Default: 21 of the host IP address.
- **Username:** Provide the username for the server.
- **Password:** Provide the password for the server.
- **Source directory:** Provide the source directory from which to download the file. Example: securonix/tenants/<tenantname>/securonix_home/response/activedirectory.
- **File Name:** Provide the file name to download.

Click **Download**.

Registering Connectors

If a new connector is added to ArcSight UBA, you need to register it first so that it is available for configuring data import.

Click the **+** button and select **Register Connectors** from the dropdown to register a connector.



Connector Type*

Outlook

Select the source from which to import data. You can import data from a delimited file (csv, pipe delimited etc), Active Directory or any other listed sources.

Connector description

Enter connector description

Connector Class*

Enter connector class

Enable Connector

YES

Enable to make connection visible

Cancel Save

Enter all the relevant fields, such as the source you want to connect to and the connector class. By default, the class files for connectors are present in the folder **[Custom Location]/webapps/Snypr/WEB-INF/classes**.











Enable the connector to make the connection visible, and click **Save**. If you disable the connector, it is hidden from the list of connections for importing data.

Available Connectors

View the list of connectors available in ArcSight UBA To edit default connectors, click the edit icon



and complete the steps described above.

Available Connectors				
Connector type	Connector description	Connector class	Enabled	Actions
activedirectory	UserAD Connector	com.securonix.connector.user.ad.UserADConnector	true	
aws	AWS cloudtrail connector	com.securonix.connector.awscloudtrail.AWSCloudTrailConnector	true	
boxcontent	Box Content connector	com.securonix.connector.boxcontent.BoxConnector	true	
clouderaaudit	Cloudera Audit Connector	com.securonix.connector.cloudera.ClouderaAuditConnector	true	
database	Database connector	com.securonix.connector.database.DatabaseConnector	true	
file	File connector	com.securonix.snypr.connector.FileConnector	true	
googlereport	Reporting API from Google	com.securonix.connector.google.GoogleReportConnector	true	
json	JSON Connector	com.securonix.connector.json.JSONConnector	true	
ldap	UserAD Connector	com.securonix.connector.user.ad.UserADConnector	true	
nitrows	Nitro WS	com.securonix.connector.nitrows.NitroWSCConnector	true	

User Data

ArcSight User Behavior Analytics ingests user identity data, correlates it, and detects anomalies indicative of different types of threats. Data ingested by the application is normalized and correlated to enable context-aware monitoring and analysis using advanced algorithms to identify threats.

User identity data is information about the user such as first name, last name, department, division, title, manager, etc. ArcSight UBA uses the user identity data to add context to events and activities. Additionally, this information is used during analytics to identify suspicious activities. User details from one or more identity data sources can be fed to the application. ArcSight User Behavior Analytics provides connections to several different identity stores including directories, databases, delimited files, identity management systems, and identity governance technologies.

Importing User Data

Generally, to import data, you must follow these steps:

1. Configure the connection method from an existing connection method or create a custom connection.
2. Configure user import:
 - a. Map event data attributes with corresponding ArcSight UBA attributes.
 - b. Set conditional actions for user life cycle changes, white listing, and pre and post actions on identity data.
3. Schedule and run the job.



ArcSight UBA imports user data using traditional collection methods and out-of-the-box premium connectors.

Collection Using Traditional Methods

Traditional collection methods include structured and unstructured datasources. You can select from existing connection methods or create a custom connection. ArcSight UBA can ingest data using the following traditional collection methods:

- Structured File Formats:
 - JSON
 - Key Value
 - XML
 - LEEF
- [Importing User Data from File](#)
 - Delimited
 - Capturing Groups
- [Importing User Data from Database](#)

To start importing data, navigate to [Step 1: Creating a Connection](#).

Collection Using Premium Connectors

ArcSight UBA provides out-of-the-box premium connectors for datasources that provide default attribute mapping and conditional actions, which you can customize to suit your environment. Data can be ingested using the following premium connectors:

- [Importing User Data from Active Directory](#)
- [Importing User Data from Aveksa](#)
- [Importing User Data from Google](#)
- [Importing User Data from Oracle Identity Analytics \(OIA\)](#)
- [Importing User Data from Okta](#)
- [Importing User Data from Oracle IDM](#)
- [Importing User Data from SailPoint](#)
- [Importing User Data from Waveset IDM](#)

To start importing data, follow these steps:

Step 1: Creating a Connection

Importing User Data from Active Directory

This section covers how to import data into the ArcSight UBA application from Active Directory. ArcSight UBA can connect to Active Directory using an LDAP or LDAP over SSL connection. The application uses an LDAP search to query the directory for the appropriate data. It requires an account with read permissions to perform the search on the Active Directory. Follow the steps below to establish a connection, query Active Directory and import user identity data.

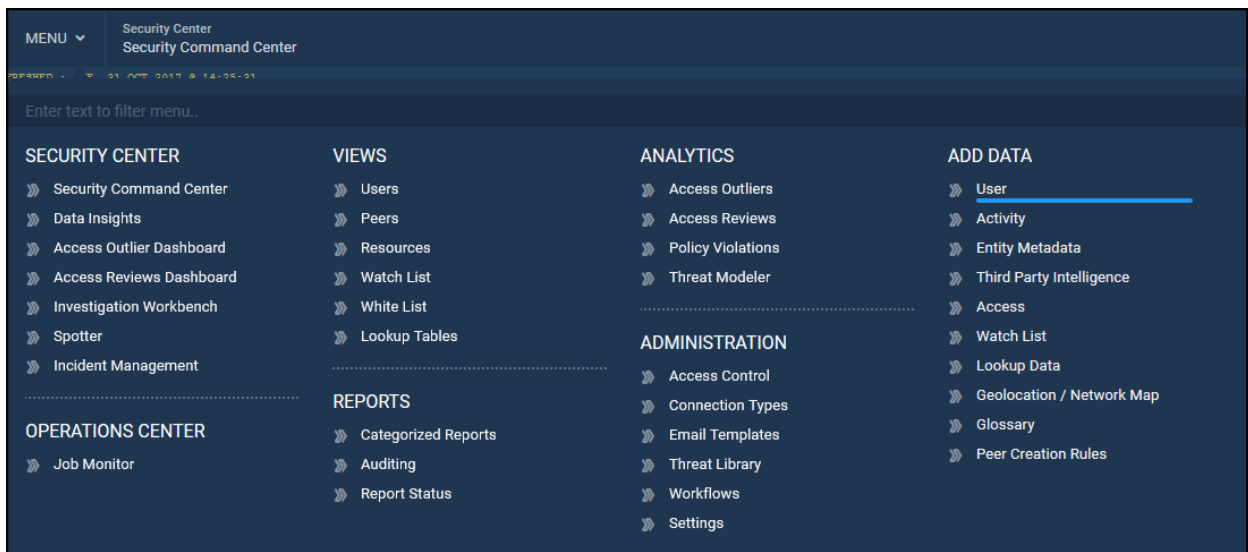
Prerequisites for importing users from Active Directory

Prior to importing data from Active Directory, make sure to have the following information:

- Host name of the LDAP server
- Credentials to establish LDAP connection (username and password)

To Import Data from Active Directory

1. Navigate to **Menu > Add Data > User**.




2. Select **New Connection** to create a new connection or **Existing Connection** to edit an existing connection.
3. Complete the following information for **Connection Method**:


1

Select Connection

Configure User Import

Select Connection to use to import users. You can create a new connection by selecting Create New from the Connection drop down.

 EXISTING CONNECTION

 NEW CONNECTION

CONNECTION METHOD *

Active Directory

Select the source from which to import data. You can import data from a delimited file (csv, pipe delimited etc), Active Directory or any other listed sources.

Connection Name*

ActiveDirectory

Provide a name to uniquely identify this connection.

Import Using

Console

- a. **Connection Method:** Select **Active Directory** from the dropdown.
 - b. **Connection Name:** Provide a name to uniquely identify this connection.
 - c. **Import Using:** Select **Console** or remote ingester name from the dropdown.
4. Complete the following for **Connection Properties**:

CONNECTION PROPERTIES

SSL?
☒ YES

Hostname*

Host name/IP address of LDAP server. Example:
ldap://10.1.12.123:389

LDAP Username*

LDAP Password*

Base Context *

Specify the DNS name prefixed with DC. Example:
DC=Americas,DC=securonix,DC=com

Filter*

Specify search filter to search for users. Example:
(&(objectCategory=person)(objectClass=User)) will search for All User
objects

- a. **SSL?** Select **YES** if LDAP connection requires SSL.

To enable SSL connections, add Certificates to Java Keystore by completing the following steps:

- From the terminal, get the location of JAVA_HOME using the command `echo $JAVA_HOME`. Invoke the key tool utility (found in the `$JAVA_HOME/bin/` folder) to import the new certificate to the existing keystore.

- To import the new CA certificate, run the following command:

```
sudo $JAVA_HOME/bin/keytool -import -alias [alias] -file
[file location of the new certificate] -keystore $JAVA_
HOME/jre/lib/security/cacerts
```

- The default password for the keystore is `changeit`. Type **Yes** to the question **Trust this certificate?**
- The Certificate was added to keystore message indicates the successful import of the new certificate. Restart Tomcat to reflect the changes.

- b. **Hostname:** Enter the IP address of the machine that holds the LDAP accounts.

- c. **LDAP Username:** Enter LDAP username with privileges to search the OU structure where the user records are present. The default format is the domain\username.

- d. **LDAP Password:** Specify the password for the Active Directory account.

- e. **Base Context:** Enter the Base Context for Active Directory. This is usually the location in the AD tree structure where the search starts. The search is always down the tree structure rather than upwards. For example, Base context can be `DC=securonix,DC=com`).

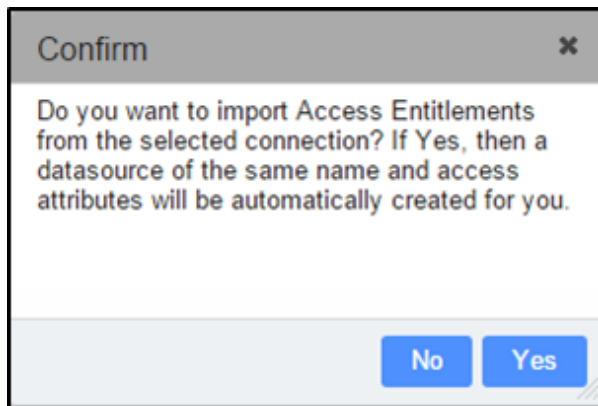
- f. **Filter:** Active Directory contains service accounts, user accounts, computer accounts and other accounts. Not all accounts are required. The application restricts the search by specifying filters to extract user identity details, for example, `(&(objectCategory=person)(objectClass=User))`. This could vary depending on the client configuration of the Active Directory.

5. Click **Test Connection** to check the credentials provided are correct and you are able to connect to Active Directory without any issues.

If you are unable to establish a connection, verify that the hostname/IP address of the LDAP context server is configured correctly in the **ldap.config.properties** file in the **/Securonix/tenants/Snypr/securonix_home/conf** (example) folder: `//grails.plugins.springsecurity.ldap.context.server = ldap://71.252.225.132:20389 Ex. 'ldaps://<server>:<port>/'`

6. Click **Save And Next** and go to [Step 2: Configuring User Import](#).

Before moving to the next screen, the solution provides an option to use Active Directory as the source for Access Entitlements. If you want to evaluate Active Directory group memberships, click **YES**. If you do not want to import group memberships, click **NO**.



Importing User Data from Aveksa

Aveksa is an access governance product provided by RSA to perform tasks like access certification, role management, and access auditing. Customers have deployed Oracle Identity Analytics to aggregate identity data and correlate access entitlements in order to get a single view to who has access to what across their environment.

ArcSight UBA integrates directly with the Aveksa product to collect identity and access privileges and analyze the access privileges to detect abnormal privileges assigned to users. Additionally, customers can use the Aveksa product to perform access certifications only on the suspicious access detected by the application.

Prerequisites for importing users from Aveksa

Prior to importing data from Aveksa, ensure you have the following information:

- JDBC URL to connect to the Aveksa application (IP Address or host name, port number, Database name and type).
- Credentials to establish the connection.

To Import Data from Aveksa

1. Navigate to **Menu > Add Data > User**.
2. Select **New Connection** to create a new connection or **Existing Connection** to edit an existing connection.
3. Select the **Connection Method** Aveksa.
4. Select the **Database Type** (Oracle).
5. Enter the **JDBC URL** and provide the user name and password.
6. Enter the query to get all users from the Aveksa database. Example: `select first_name, user_id, department, last_name, location, title, case when (is_ter-`

```
minated=1) then 'Yes' else 'No' End as Terminated from avuser-  
.tmaster_enterprise_users tmeu
```



Note: Choose the fields that you have populated in Aveksa by viewing all available fields in the T_Master_Enterprise_Users table.

7. Click **Save And Next** and go to [Step 2: Configuring User Import](#).

Importing User Data from Database

This section shows how to import data from a database, such as MySQL, MSSQL Server, and Oracle.

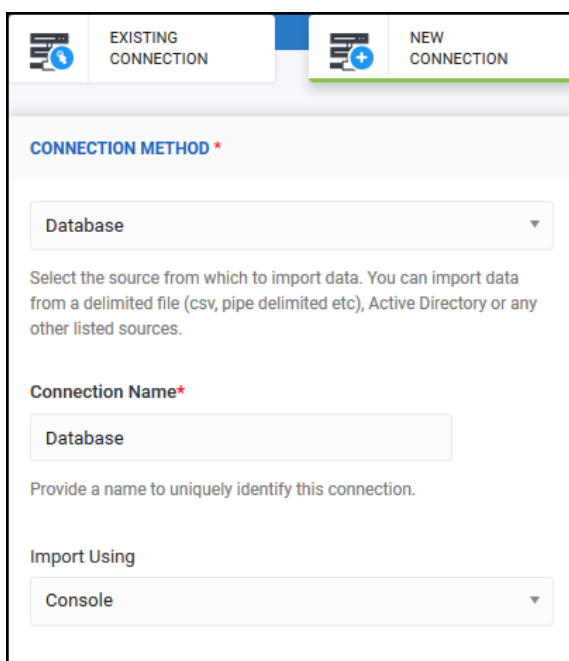
Prerequisites for importing users from Database

Prior to importing data from Database ensure you have the following information:

- JDBC URL to connect to the Database (IP Address or host name, port number, Database name and type).
- Credentials to establish the connection.

To Import Data from a Database

1. Navigate to **Menu > Add Data > User**.
2. Select **New Connection** to create a new connection or **Existing Connection** to edit an existing connection.
3. Complete the following information for **Connection Method**:



The screenshot shows the 'NEW CONNECTION' form. At the top, there are two tabs: 'EXISTING CONNECTION' and 'NEW CONNECTION'. The 'NEW CONNECTION' tab is active. Below the tabs, the form is titled 'CONNECTION METHOD *'. There are three main sections: 1. 'Database' dropdown menu. 2. 'Connection Name*' text input field. 3. 'Import Using' dropdown menu.

Database

Select the source from which to import data. You can import data from a delimited file (csv, pipe delimited etc), Active Directory or any other listed sources.

Connection Name*

Database

Provide a name to uniquely identify this connection.

Import Using

Console

- a. **Connection Method:** Select **Database** from the dropdown.
 - b. **Connection Name:** Provide a name to uniquely identify this connection.
 - c. **Import Using:** Select **Console** or remote ingester name from the dropdown.
4. Complete the following information for **Connection Properties**:

CONNECTION PROPERTIES

Database Type *

MySQL ▼

JDBC URL *

jdbc:mysql://<host>:<3306>/<database>

Connection string to connect to particular database. Example:
jdbc:mysql://hostname:port/database_name

Driver Class *


com.mysql.jdbc.Driver

Database specific class

Database Username *

Database Password *

SQL Query *

- a. **Database type:** Select from dropdown. Example: MySQL.
 - b. **JDBC URL:** Enter the JDBC URL. Example: jdbc:mysql://<host>:<3306>/<database>.
 - c. **Driver Class:** Enter the database specific class. Example: com.mysql.jdbc.Driver.
 - d. **Database Username:** Enter the username for the database.
 - e. **Database Password:** Enter the password for the database.
 - f. **SQL Query:** Enter the SQL query for the data import. Example: select employeeid, first-name, lastname, department, workemail from users.
5. Click the Refresh  button in the top-right corner of the screen to preview the input.
6. Click **Save And Next** to proceed to [Step 2: Configuring User Import](#).

Importing User Data from File

This section describes how to import data to ArcSight User Behavior Analytics from a delimited (comma or pipe separated) file.

Prerequisites for Importing Users from File

Prior to importing data from a file, ensure you have the following information:

- File Name, location, type (fixed length), file delimiter.
- The connection method, host IP address, port number, credentials, and source directory if the file is located on a remote server.
- The URL and credentials for the proxy server if the remote server is a proxy server.

To Import Data from Files

1. Navigate to **Menu > Add Data > User**.
2. Select **New Connection** to create a new connection or **Existing Connection** to edit an existing connection.
3. Complete the following information for **Connection Method**:

CONNECTION METHOD *

File ▼

Select the source from which to import data. You can import data from a delimited file (csv, pipe delimited etc), Active Directory or any other listed sources.

Connection Name*

File

Provide a name to uniquely identify this connection.

Import Using

Console ▼

- a. **Connection Method:** Select **Database** from the dropdown.
 - b. **Connection Name:** Provide a name to uniquely identify this connection.
 - c. **Import Using:** Select **Console** or remote ingester name from the dropdown.
4. Complete the following information for **Connection Properties**:

CONNECTION PROPERTIES

Upload a file?
☐ NO

File Name*

Name of the file containing data to import. Example: hrdata.csv, hrdata.log, hrdata.txt.
This file must be located in `/Securonix/tenants/partnerdemo/securonix_home\import\in`. You can change this location by clicking on **More Settings** below.

Fixed Length
☐ NO

Is it a fixed length file?

Column Delimiter

Specify the delimiter between the fields in the input file. Example: , (comma) | (pipe)

Column Identifier

Specify the symbol if any, used to enclose each column in the input file. Leave blank if no symbol is used. Example: " (double quotes)

Import from Remote Server?
☐ NO

Use FTP/SFTP/SCP to ingest file located in a remote location?

- a. **Upload a file?:** Select YES to browse for a file on the local machine or NO to specify the complete path to the folder in which the file to be imported is located. Default: \$securonix_home/import/in.
 - b. **Fixed Length:** Enable if the file is a fixed length file.
 - **NO:** Specify the **Column Delimiter** and **Column Identifier**.
 - **YES:** Proceed to next step.
 - c. **Import from Remote Server?:** Enable to use FTP/SFTP/SCP to ingest the file located in a remote location.
 - **NO:** Proceed to **More Settings**.
 - **YES:** Complete the following information:
 - a. Select a **Remote Connection Type** from the dropdown.
 - b. Enter the **Host IP Address** (for FTP, SFTP, etc.) or **URL** (for HTTP, HTTPS).
 - c. Enter the **Port Number** (for FTP, SFTP, etc.). Default 22.
 - d. Enter the **Username**.
 - e. Enter the **Password**.
 - f. Enter the **Source Directory**.
 - g. Select **Yes** or **No** for **Proxy Server?**
 - a. If **No:** Proceed to next step.
 - b. If **Yes:** Enter **Proxy Server URL**, **Username**, and **Password**.
 - h. **Test** the remote connection.
5. Complete the following information for **More Settings**:

MORE SETTINGS

`${SECURONIX_HOME}` is set to `/Securonix/tenants/partnerdemo/securonix_home`.
You can also replace `${SECURONIX_HOME}` below with the direct path to the folder where the file exists.
Example: `/Users/dev/files/`

Source Folder*

`${SECURONIX_HOME}/import/in`

Enter the complete path to the directory where this file is located.

Success Folder*


`${SECURONIX_HOME}/import/success`

Enter the complete path to the directory where this file must be moved once the import is completed successfully.

Failed Folder*

`${SECURONIX_HOME}/import/failed`

Enter the complete path to the directory where this file must be moved if the import job fails to complete.

- a. **Source Folder:** By default, ArcSight User Behavior Analytics expects the file to be in the `${SECURONIX_HOME}/import/in` folder. If the input data file is located in another location, provide the location of the folder by editing the **Source Folder** text box.
 - b. **Success Folder:** After the import is completed, ArcSight UBA compresses the imported data file and moves it to the Success folder (`${SECURONIX_HOME}/import/success`). Change the location of the folder by editing the **Success Folder** text box.
 - c. **Failed Folder:** If the file fails to import, ArcSight UBA compresses the file and moves it to the Failed folder (`${SECURONIX_HOME}/import/failed`). Change the location of the folder by editing the **Failed Folder** text box.
6. Complete the following for Additional Settings:
- a. **Exclude Header:** To exclude header lines from being imported, select **YES** and enter a value (example: 1) in Number of Lines to Ignore.
 - b. **Exclude Footer:** To exclude header lines from being imported, select **YES** and enter a value (example: 1) in Number of Lines to Ignore.
7. Click the Refresh  button in the top-right corner of the screen to preview the user data.
8. Click **Save And Next**, and then go to [Step 2: Configuring User Import](#).

Importing User Data from Google

This section describes how to import data from a Google data source.



Note: Prior to configuring the Google data source, you must configure the Google API to register the ArcSight UBA product.

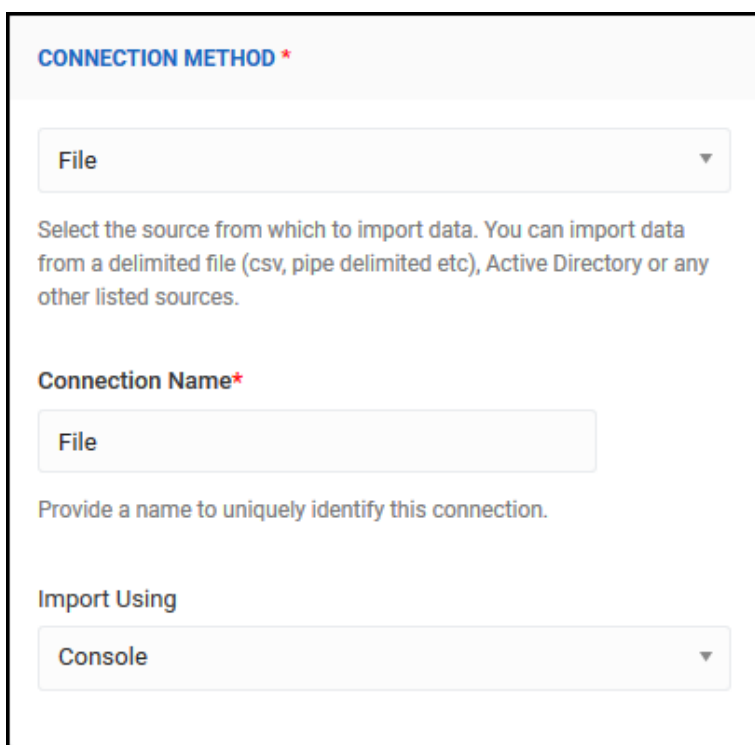
Prerequisites for Importing Users from Google

ArcSight UBA uses open authentication (OAuth) to connect to Google to import data. Ensure you have the following information prior to setting up the connection:

- Name of the project that holds ArcSight UBA related information to connect to Google.
- The service account email used to provision the project.
- The admin user email used to create the service account.
- The domain from where the data is to be imported.
- The private key file for OAuth connection to the Google API.

To Import Data from Google

1. Navigate to **Menu > Add Data > User**.
2. Select **New Connection** to create a new connection or **Existing Connection** to edit an existing connection.
3. Complete the following information for **Connection Method**:



The screenshot shows a form titled "CONNECTION METHOD" with a red asterisk. It contains three main sections: a dropdown menu for "File", a text input field for "Connection Name" with a red asterisk, and a dropdown menu for "Import Using" set to "Console".

CONNECTION METHOD *

File ▼

Select the source from which to import data. You can import data from a delimited file (csv, pipe delimited etc), Active Directory or any other listed sources.

Connection Name*

File

Provide a name to uniquely identify this connection.

Import Using

Console ▼

- a. **Connection Method:** Select **Google Directory** from the dropdown.
 - b. **Connection Name:** Provide a name to uniquely identify this connection.
 - c. **Import Using:** Select **Console** or remote ingester name from the dropdown.
4. Complete the following information for **Connection Properties**:

CONNECTION PROPERTIES

Project *

Use Google API Console to project

Service Account Email *

Use Google API Console to create service account

Admin User Email *

Admin User Email Address which is used to generate service email account

Domain *

Enter domain name to pull from Google API

Private Key File (.p12 file)


Browse...

No files selected.

You can generate this file from Google API Console using your credentials. Please make sure that file is present at /Securonix /tenants/partnerdemo/securonix_home "/conf/google/"

OR

Specify File Name

- a. **Project:** Provide the Project created in Google for ArcSight UBA.
 - b. **Service Account Email:** Provide the service account email used to provision the project.
 - c. **Admin User Email:** Provide the admin email to connect to the domain.
 - d. **Domain:** Provide the domain from which to import the data.
 - e. **Private Key File:** Provide the Private Key File used for Google API authentication.
 - a. Upload the file to **[Custom Folder]\snypr6/securonix_home/conf/google** or specify the file name after it is copied to this location.
5. Click the Refresh  icon to preview the input.
6. Click **Save And Next** to proceed to [Step 2: Configuring User Import](#).

Importing User Data Using LDAP

This section covers how to import data into the ArcSight UBA application using LDAP (Lightweight Directory Access Protocol). ArcSight UBA can connect using an LDAP or LDAP over SSL connection. The application uses an LDAP search to query the directory for the appropriate data. It requires an account with read permissions to perform the search. Follow the steps below to establish a connection, and import user identity data.

Prerequisites for importing users using LDAP

Prior to importing data using LDAP, make sure to have the following information:

- Host name
- Credentials to establish LDAP connection (username and password)
- Domain

To Import Data Using LDAP

1. Navigate to **Menu > Add Data > User**.
2. Select **New Connection** to create a new connection or **Existing Connection** to edit an existing connection.
3. Complete the following information for **Connection Method**:

The screenshot shows a web interface for creating a new connection. At the top, there are two tabs: 'EXISTING CONNECTION' and 'NEW CONNECTION'. The 'NEW CONNECTION' tab is active. Below the tabs, the section is titled 'CONNECTION METHOD *'. There is a dropdown menu with 'LDAP' selected. Below this, a text box explains: 'Select the source from which to import data. You can import data from a delimited file (csv, pipe delimited etc), Active Directory or any other listed sources.' Below this, there is a 'Connection Name*' field with 'LDAP' entered. A note below this field says: 'Provide a name to uniquely identify this connection.' Below this, there is an 'Import Using' section with a dropdown menu showing 'Console'.

- a. **Connection Method:** Select **LDAP** from the dropdown.
 - b. **Connection Name:** Provide a name to uniquely identify this connection.
 - c. **Import Using:** Select **Console** or remote ingester name from the dropdown.
4. Complete the following for **Connection Properties**:

CONNECTION PROPERTIES

SSL?
☐ NO
Is this connection SSL protected?

Hostname*

Host name/IP address of LDAP server. Example:
ldap://10.1.12.123:389

LDAP Username*

LDAP Password*

Base Context*

Specify the DNS name prefixed with DC. Example:
DC=Americas,DC=securonix,DC=com

Filter*

Specify search filter to search for users. Example:
(&(objectCategory=person)(objectClass=User)) will search for All User objects

Referrals


- a. **SSL?** Select **YES** if LDAP connection requires SSL.

To enable SSL connections, add Certificates to Java Keystore by completing the following steps:

- From the terminal, get the location of JAVA_HOME using the command `echo $JAVA_HOME`. Invoke the key tool utility (found in the `$JAVA_HOME/bin/` folder) to import the new certificate to the existing keystore.
- To import the new CA certificate, run the following command:

```
sudo $JAVA_HOME/bin/keytool -import -alias [alias] -file
[file location of the new certificate] -keystore $JAVA_
HOME/jre/lib/security/cacerts
```

- The default password for the keystore is `changeit`. Type **Yes** to the question **Trust this certificate?**
 - The Certificate was added to keystore message indicates the successful import of the new certificate. Restart Tomcat to reflect the changes.
- b. **Hostname:** Enter the IP address of the machine that holds the LDAP accounts.
Example: `ldap://ipaddress:389`.
- c. **LDAP Username:** Enter LDAP username with privileges to search the OU structure where the user records are present. The default format is the `domain\username`.
- d. **LDAP Password:** Specify the password for the LDAP account.
- e. **Base Context:** Specify the DNS name prefixed with DC. Example: `DC=Americas, DC=securonix, DC=com`.
- f. **Filter:** Specify the search filter to search for users. Example: `(&(objectCategory=person)(objectClass=User))`.
- g. **Referrals:** Select an option from the dropdown to indicate to the service provider how to handle referrals. If this property is not set, the default is to **Ignore** referrals.
- **Ignore:** Ignore referrals.
 - **Follow:** Automatically follow any referrals.
 - **Throw:** Throw a Referral Exception for each referral.
- h. **Source Folder:** By default, ArcSight User Behavior Analytics expects the file to be in the `${SECURONIX_HOME}/import/in` folder. If the input data file is located in another location, provide the location of the folder by editing the **Source Folder** text box.
- i. **Success Folder:** After the import is completed, ArcSight UBA compresses the imported data file and moves it to the Success folder (`${SECURONIX_HOME}/import/success`). Change the location of the folder by editing the **Success Folder** text box.

- j. **Failed Folder:** If the file fails to import, ArcSight UBA compresses the file and moves it to the Failed folder(`${SECURONIX_HOME}/import/failed`). Change the location of the folder by editing the **Failed Folder** text box.
5. Click **Test Connection** to check the credentials provided are correct and you are able to connect to Active Directory without any issues.
If you are unable to establish a connection, verify that the hostname/IP address of the LDAP context server is configured correctly in the **ldap.config.properties** file in the **/Securonix/tenants/Snypr/securonix_home/conf** (example) folder: `//grails.plugins.springsecurity.ldap.context.server = ldap://71.252.225.132:20389` Ex. 'ldaps://<server>:<port>/'
6. Click the Refresh  button in the top-right corner of the screen to preview the input.
7. Click **Save And Next** to proceed to [Step 2: Configuring User Import](#).

Importing User Data from Oracle Identity Analytics (OIA)

This section describes how to import from OIA. Oracle Identity Analytics provides enterprises with the ability to define and manage roles and automate critical identity-based controls. ArcSight UBA integrates directly with OIA to collect identity and access privileges, and analyze the access privileges to detect abnormal privileges assigned to users. Additionally, customers can use OIA to perform access certifications only on the suspicious access detected by the ArcSight UBA application.

Prerequisites for importing Users from OIA

Prior to importing data from OIA, make sure to have the following information:

- JDBC URL to connect to the Database application (IP Address or host name, port number, Database name and type).
- Credentials to establish the connection.

To Import Data from OIA

1. Navigate to **Menu > Add Data > User**.
2. Select **New Connection** to create a new connection or **Existing Connection** to edit an existing connection.
3. Complete the following information for **Connection Method**:

CONNECTION METHOD *

Oracle Identity Analytics ▼

Select the source from which to import data. You can import data from a delimited file (csv, pipe delimited etc), Active Directory or any other listed sources.

Connection Name*

OracleIdentity Analytics

Provide a name to uniquely identify this connection.

- a. **Connection Method:** Select **Oracle Identity Analytics** from the dropdown.
 - b. **Connection Name:** Provide a name to uniquely identify this connection.
4. Complete the following information for **Connection Properties**:

CONNECTION PROPERTIES

Database Type *

MySQL ▼

JDBC URL *

jdbc:mysql://<host>:<3306>/<database>

Connection string to connect to particular database. Example:
jdbc:mysql://hostname:port/database_name

Driver Class*


com.mysql.jdbc.Driver

Database specific class

Database Username*

Database Password*

SQL Query*

- a. **Database type:** Select from dropdown. Example: MySQL.
 - b. **JDBC URL:** Enter the JDBC URL. Example: jdbc:mysql://<host>:<3306>/<database>.
 - c. **Driver Class:** Enter the database specific class. Example: com.mysql.jdbc.Driver.
 - d. **Database Username:** Enter the username for the database.
 - e. **Database Password:** Enter the password for the database.
 - f. **SQL Query:** Enter the SQL query for the data import. Example: `select employeeid, firstname, lastname, department, workemail from users`
5. Click the Refresh  button in the top-right corner of the screen to preview the input.
 6. Click **Save And Next** and go to [Step 2: Configuring User Import](#).

Importing User Data from Okta

This section describes how to import from Okta.

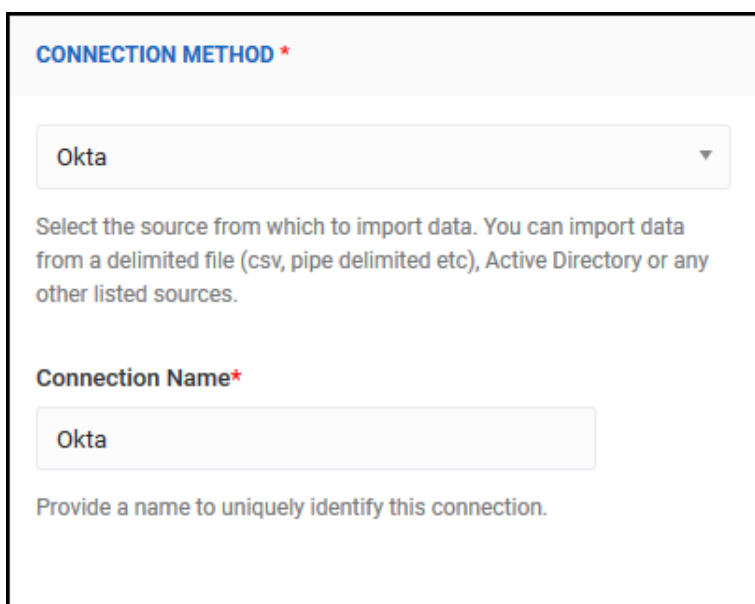
Prerequisites for importing users from Okta

Prior to importing data from Okta, make sure to have the following information:

- Okta URL and Token

To Import Data from Okta

1. Navigate to **Menu > Add Data > User**.
2. Select **New Connection** to create a new connection or **Existing Connection** to edit an existing connection.
3. Complete the following information for **Connection Method**:



The screenshot shows a form titled "CONNECTION METHOD" with a red asterisk. It contains a dropdown menu with "Okta" selected. Below the dropdown is a text instruction: "Select the source from which to import data. You can import data from a delimited file (csv, pipe delimited etc), Active Directory or any other listed sources." Below this is a label "Connection Name" with a red asterisk, followed by a text input field containing "Okta". At the bottom is a text instruction: "Provide a name to uniquely identify this connection."

- a. **Connection Method**: Select **Okta** from the dropdown.
 - b. **Connection Name**: Provide a name to uniquely identify this connection.
4. Complete the following for **Connection Properties**:

CONNECTION PROPERTIES

URL*

Token*

`${SECURONIX_HOME}` is set to `/Securonix/tenants/partnerdemo/securonix_home`.
You can also replace `${SECURONIX_HOME}` below with the direct path to the folder where the file exists.
Example: `/Users/dev/files/`

Source Folder*


Enter the complete path to the directory where this file is located.

Success Folder*

Enter the complete path to the directory where this file must be moved once the import is completed successfully.

Failed Folder*

Enter the complete path to the directory where this file must be moved if the import job fails to complete.

- a. **URL:** Provide the Okta URL.
 - b. **Token:** Provide the Okta Token.
 - c. **Source Folder:** By default, ArcSight User Behavior Analytics expects the file to be in the `${SECURONIX_HOME}/import/in` folder. If the input data file is located in another location, provide the location of the folder by editing the **Source Folder** text box.
 - d. **Success Folder:** After the import is completed, ArcSight UBA compresses the imported data file and moves it to the Success folder (`${SECURONIX_HOME}/import/success`). Change the location of the folder by editing the **Success Folder** text box.
 - e. **Failed Folder:** If the file fails to import, ArcSight UBA compresses the file and moves it to the Failed folder(`${SECURONIX_HOME}/import/failed`). Change the location of the folder by editing the **Failed Folder** text box.
5. Click the Refresh  button in the top-right corner of the screen to preview the input.
 6. Click **Save And Next** to proceed to [Step 2: Configuring User Import](#).

Importing User Data from Oracle IDM

The following section describes how to import from Oracle IDM.

Prerequisites for importing users from Oracle IDM

Prior to importing data from OIM, make sure to have the following information:

- OIM Host Name and Port.
- Credentials to establish the connection.

To Import Data from OIM

1. Navigate to **Menu > Add Data > User**.
2. Select **New Connection** to create a new connection or **Existing Connection** to edit an existing connection.
3. Complete the following information for **Connection Method**:

The screenshot shows the 'NEW CONNECTION' form. At the top, there are two tabs: 'EXISTING CONNECTION' and 'NEW CONNECTION'. The 'NEW CONNECTION' tab is selected. Below the tabs, the 'CONNECTION METHOD' is set to 'Oracle IDM' in a dropdown menu. A text input field for 'Connection Name' contains the value 'OracleIDM'. A note at the bottom states: 'Provide a name to uniquely identify this connection.'

- a. **Connection Method:** Select **Oracle IDM** from the dropdown.
 - b. **Connection Name:** Provide a name to uniquely identify this connection.
4. Complete the following for **Connection Properties**:

CONNECTION PROPERTIES

Host Name*

Port*

Username*


Password*

Naming Context Factory ⓘ

Provider ⓘ

Login Config

OIM Home

- a. **Host Name:** Provide the OIM host name.
 - b. **Port:** Provide the OIM port.
 - c. **Username:** Provide the OIM username.
 - d. **Password:** Provide the OIM password.
 - e. **Naming Context Factory:** Provide the initial context for lookup. This field is preloaded with the connector. If different from default value, provide information.
 - f. **Provider:** Provide the location of the registry for initial context. This field is preloaded with the connector. If different from default value, provide information.
 - g. **Login Config:** Provide the login config.
 - h. **OIM Home:** Provide the OIM home.
5. Click the Refresh  button in the top-right corner of the screen to preview the input.
 6. Click **Save And Next** to proceed to [Step 2: Configuring User Import](#).

Importing User Data from SailPoint

SailPoint provides streamlined access reviews, improves audit performance, and reduces the cost of compliance. It also provides access certification, centralized IAM certification across all systems and acts as an access provisioning engine.

ArcSight UBA has the ability to detect and score rogue access privileges using advanced peer group-analysis techniques. It also reduces the burden and rubber stamping during access certifications by providing only high risk access privileges for review. ArcSight UBA improves the access request process by ensuring appropriate approvals for high risk access.

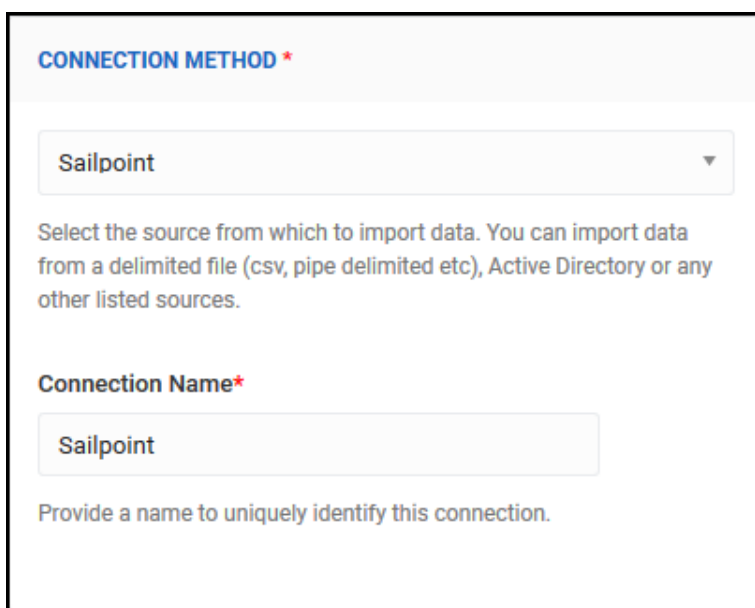
Prerequisites for importing users from SailPoint

Prior to importing data from SailPoint, make sure to have the following information:

- JDBC URL to connect to the Database application (IP Address or host name, port number, Database name and type).
- Credentials to establish the connection.

To Import Data from SailPoint

1. Navigate to **Menu > Add Data > User**.
2. Select **New Connection** to create a new connection or **Existing Connection** to edit an existing connection.
3. Complete the following information for **Connection Method**:



The screenshot shows a form titled "CONNECTION METHOD" with a red asterisk. It contains a dropdown menu with "Sailpoint" selected. Below the dropdown is a text box with the instruction: "Select the source from which to import data. You can import data from a delimited file (csv, pipe delimited etc), Active Directory or any other listed sources." Below this is a label "Connection Name" with a red asterisk, followed by a text input field containing "Sailpoint". At the bottom is a text box with the instruction: "Provide a name to uniquely identify this connection."

- a. **Connection Method:** Select **Sailpoint** from the dropdown.
 - b. **Connection Name:** Provide a name to uniquely identify this connection.
4. Complete the following information for **Connection Properties**:

CONNECTION PROPERTIES

Database Type *

-Select-

JDBC URL *

Connection string to connect to particular database. Example:
jdbc:mysql://hostname:port/database_name

Driver Class*

Database specific class

Database Username*


Database Password*

File Source

-Select-

Connection defining file information

SQL Query*

- a. **Database type:** Select from dropdown. Example: MySQL.
 - b. **JDBC URL:** Enter the JDBC URL. Example: jdbc:mysql://<host>:<3306>/<database>.
 - c. **Driver Class:** Enter the database specific class. Example: com.mysql.jdbc.Driver.
 - d. **Database Username:** Enter the username for the database.
 - e. **Database Password:** Enter the password for the database.
 - f. **File Source:** Select from dropdown. Example: HRFile.
 - g. **SQL Query:** Enter the SQL query for the data import. Example: `select employeeid, firstname, lastname, department, workemail from users`
5. Click the Refresh  button in the top-right corner of the screen to preview the input.
6. Click **Save And Next** and go to [Step 2: Configuring User Import](#).

Importing User Data from Waveset IDM

This section describes how to import from Waveset IDM.

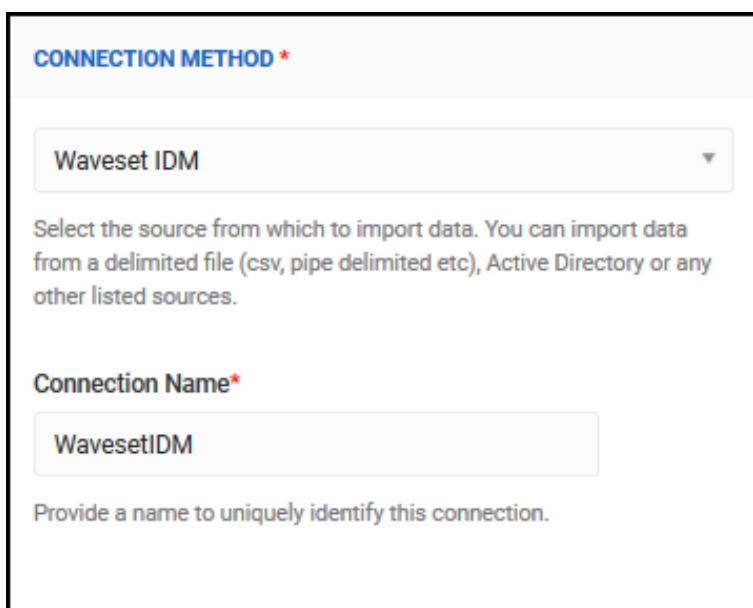
Prerequisites for importing users from Waveset IDM

Prior to importing data from Waveset IDM, make sure to have the following information:

- URL
- Credentials to establish the connection

To Import Data from Waveset IDM

1. Navigate to **Menu > Add Data > User**.
2. Select **New Connection** to create a new connection or **Existing Connection** to edit an existing connection.
3. Complete the following information for **Connection Method**:



The screenshot shows a form titled "CONNECTION METHOD" with a red asterisk. It contains a dropdown menu with "Waveset IDM" selected. Below the dropdown is a text box with the instruction: "Select the source from which to import data. You can import data from a delimited file (csv, pipe delimited etc), Active Directory or any other listed sources." Below this is a section titled "Connection Name" with a red asterisk, followed by a text input field containing "WavesetIDM". At the bottom, there is a text box with the instruction: "Provide a name to uniquely identify this connection."

- a. **Connection Method:** Select **Waveset IDM** from the dropdown.
 - b. **Connection Name:** Provide a name to uniquely identify this connection.
4. Complete the following information for **Connection Properties**:

CONNECTION PROPERTIES

URL*


Username*

Password*

User Request Filter

SQL Query*

```
SELECT
name,description,manager,firstname,lastna
me,email,manager_status,inactive,last_login,
created,modified,owner,extended1,extended
2,extended3,extended4,attributes from
CIQ_identity
```

- a. **URL:** Provide the URL for Waveset IDM.
 - b. **Username:** Provide the username for Waveset IDM. Example: configurator.
 - c. **Password:** Provide the password associated with the username.
 - d. **User Request Filter:** Provide the User Request Filter for Waveset IDM.
 - e. **SQL Query:** Enter the SQL query for the data import. Example: `select employeeid, firstname, lastname, department, workemail from users`
5. Click the Refresh  button in the top-right corner of the screen to preview the input.
6. Click **Save And Next** and go to [Step 2: Configuring User Import](#).

Step 2: Configuring User Import

This step consists of two sections: Attribute Mapping and Additional Settings.

Attribute Mapping

The Attribute Mapping section describes the mapping of the fields in the data file to the corresponding attributes in ArcSight UBA.



Note: For a complete list of attributes in ArcSight UBA, see [Appendix A: ArcSight UBA Attribute Schema](#).

1

Select Connection

Configure User Import

Schedule Job to Run

Prev

Save And Next

Specify column positions in file that map to Securonix Fields

ATTRIBUTE MAPPING

Input File Column Position	Mapped To Securonix Field	Maintain Change History ⓘ	Date Format ⓘ	Add/Remove
1	employeeid	<input checked="" type="checkbox"/> NO		+ -
2	lanid	<input checked="" type="checkbox"/> NO		+ -
3	networkid	<input checked="" type="checkbox"/> NO		+ -
4	firstname	<input checked="" type="checkbox"/> NO		+ -
5	middlename	<input checked="" type="checkbox"/> NO		+ -
6	lastname	<input checked="" type="checkbox"/> NO		+ -
7	nameprefix	<input checked="" type="checkbox"/> NO		+ -

PREVIEW

First 10 lines from input file are shown below. Headers in the table correspond to column positions. Enter the position number above and select corresponding field to map to. You can choose not to map columns you do not wish to import.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Employeeid	UniqueCode	Networkid	firstname	middlename	lastname	nameprefix	namesuffix	preferredname	department	division	orgunitnumber	companycode	companynumber	hierarchy	location	location
1644	TG1644	TGULAT1	Tanuj		Gulati				SAP Administrator	Global Technology	12	TECH	TECH12	3	ALABAMA	
1631	LC1631	LClarke	Lauren		Clarke				Legal Department	Legal	13	LEG	LEG13	4	ALABAMA	
1642	EF1642	EFennell	Erica		Fennell				Legal Department	Legal	13	LEG	LEG13	4	ALABAMA	
1025	TT1025	TThomson	Ted		Thomson				Executive Management	Executive Management	1	CEO	CEO	1	NEWYORK	
1068	AW1068	AWolfe	Amal		Wolfe				Executive Management	Business Banking	1	BBM	BBM1	2	NEW JERSEY	
1097	KB1097	KBlake	Katell		Blake		Katie		Client Development Group	Business Banking	1	BBM	BBM1	3	NEW JERSEY	
1104	OW1104	OWilliams	Olivia		Williams				Client Development Group	Business Banking	1	BBM	BBM1	4	NEW JERSEY	
1129	RH1129	RHutchinson	Ray		Hutchinson				Client Development Group	Business Banking	1	BBM	BBM1	4	NEW JERSEY	
1142	AM1142	AMorgan	Anastasia		Morgan		Ana		Client Development Group	Business Banking	1	BBM	BBM1	4	NEW JERSEY	

1. **Input File Column Position:** Map to the correct columns of the input file to the positions in ArcSight UBA. You can map fields such as employeeid, firstname, department, division, manageremployeeid, and hiredate. Example: Column 1 Employeeid to Input File Column Position 1.
2. **Mapped to Securonix Field:** Select the corresponding ArcSight UBA attribute from the drop-down to match to the input file field. Example: Map Position 1: Employeeid to Securonix Field: employeeid.



Note: To skip a field, exclude the corresponding column number and the column name.

3. **Maintain Change History:** Enable the slide to **YES** for the fields to maintain previously stored values for existing users.



Note: Date formatted fields (hiredate, sunrise, sunset, terminationdate) expect a date format. Select the date format from the dropdown. (Example: MM/dd/YY = 10/25/13, MM/dd/yyyy = 10/25/2013, MMM dd, yyyy for Oct 25, 2013), or type the date format you prefer to use.

Additional Settings

Additional Settings has a series of pull out configuration areas, click the down arrow by each area to access, and change settings. Configuration areas under Additional Settings:

- User Lifecycle Changes
- White List
- Pre and Post Actions
- Merge data with existing user identity
- Notifications/Alerts

User Lifecycle Changes

Additional Settings

User Lifecycle Changes

Select conditions to indicate user Termination ⓘ

User not present in input source

Select an option for detecting terminated users. If user identities are removed from the source, choose "user not present in input source". If a flag is set to specify terminated users, choose the field to status description and then choose "User status description rule".

Select condition to indicate User Transfer ⓘ

costcentercode
sunsetdate
technicalapproverid
terminationdate
timezoneoffset
transferreddate
usergroup
userid
userstate
vacationend
vacationstart
workemail

>
>>
<<
<

manageremployeeid
department
division
jobcode
title

You can select multiple attributes that indicate user transfer.
Example: Costcentercode and jobcode
If Costcentercode and jobcode changes then user is indicated as transferred.
You also select condition as "OR" which indicates a user transfer if costcentercode OR job code changes

Condition OR

Is Duplicate Employee ID Allowed?

NO

White List

Select conditions to indicate user termination

When a user is terminated from the organization, the user record may be deleted from the source identity system or it may be flagged. ArcSight UBA identifies user identities that have been terminated, based on the value provided under Select conditions to indicate user Termination. The choices are:

- Do nothing.
- **User not present in input source:** Choose this option if the user is not present in the data file during the user import, and hence is considered terminated.
- **User status flag set to terminate:** Upon selecting this value, the **Status Field** dropdown and text box are displayed where you can enter the value that indicates a terminated user in the data source.

- **User-status description rule:** Different HR systems use different nomenclature for capturing the status of employees within the organization. You can specify rules to make sure that ArcSight UBA marks these users as Active or Inactive, by mapping the status field from the user identity file to the status description field within the application. (For example: the HR file has a field with values Term, Furlough, Departed, and Fulltime. Map the column position where these values appear to the status description field and set up User Status values as Term = 0, Furlough = 0, Departed = 0, Fulltime = -1.)

Select condition to indicate User Transfer

When a user is transferred, their HR record changes. In most cases there is a change to the user's department, division, manageremployeeid, jobcode, costcentercode, etc.

Select the fields that will indicate User Transfer. For example, choose title, department, and division fields to indicate user transfer. Use the **Condition** switch (“**AND**” or “**OR**”) to set whether any or all of the selected fields must change to indicate a transfer.

Is Duplicate Employee ID Allowed?

If a User has more than one Employee ID, select **YES**. This will allow a user to be represented by various IDs used to identify them. (For example, the Employee ID in the HR system is 0012. The Employee ID in the Access Management system is AB112. Select **YES** to identify the employee by both IDs.)

White List

You can specify user from the import file to add to global or targeted White lists in ArcSight UBA. See [Views](#) in the User Guide for more information about creating and managing global or targeted White Lists.

Specify which Users will get added in White List on which condition.

Whitelist Name: VIP Employees Add New Whitelist

New Whitelist Name:

Whitelist Forever: ☒

Do you want to reduce the risk score for selected user to zero? ☒

Selecting Yes will reduce the risk score of the user to zero. The selected user will be stripped next time he violates a policy.

Add Group

Attribute	Condition	Value		
title	Contains	Executive	AND	✔ ✖

Remove Group

Attribute	Condition	Value		
department	Equal To	Finance	AND	✔ ✖

Select Risk Type

Access Manager Certification
Access Owner Certification

User Certification
User Aggregate Risk

1. **Add Users in White List?** Enable slider to **YES** to add imported users to a White List automatically.
2. **Whitelist Name:** Select a white list from the dropdown or **Add New Whitelist** to provide a **New Whitelist Name**.
3. **Whitelist Forever:** Select **YES** if users should remain on the Whitelist forever. If **NO**, select an expiry date for **Whitelist Until**.
4. **Do you want to reduce the risk score for selected user to zero?:** Toggle to **YES** to reduce the risk score of the selected users to zero. The users will be ignored if they violate a policy.
5. **White List Conditions:** Use dropdowns to select the conditions to filter users in the White List. Example: **Attribute:** title | **Condition:** Contains | **Value:** Executive.
Use **+/-** to add or remove rules in a group. Click **Add Group** to add a new group of rules. Click **Remove Group** to remove groups of rules.
6. **Select Risk Type:** Use **>** or **>>** to add Risk Types that apply to the white list. Example: User Aggregate Risk and User Certification.

Pre and Post Actions

The pre and post processor actions allow modifications to the data feed before or after user import. Pre-processor actions modify the data before it is imported, and the modified data is placed in the Users table of your database. With post-processor actions, the data is modified after it is imported into the database. You can create a class or a SQL query to run before or after the user import.

Example :

Input Location Field: newyork1

Modified Email Field : New York

Pre and Post Actions

Run custom pre-processors or post-processors that execute before or after user import. It can be custom class or SQL query.

Name	Type	Enabled?	Processor Class	SQL	Actions
<input type="text"/>	Preprocessor	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>	<div><div></div><div></div><div></div></div>

Merge data with existing user identity

You can merge data from two sources to avoid duplicate users when user data is ingested from two different sources such as Sailpoint and LDAP. To merge the data from the different data sources, use **Merge data with existing user identity**.

For example, data from Sailpoint is missing fields like manageremployeeid and the last log on date. These fields are available from Active Directory. You can merge the user data on any attribute, such as employeeid from Sailpoint and Active Directory to include fields from both datasources.

Merge data with existing user identity defaults to **NO**. If enabled, complete the following steps:

1. Select an existing connection from the dropdown to **Merge Imported Data With** the data you are importing.
2. Select **YES** to import new users.
3. Select data fields on which user data can merge. For example, merge if employeeid matches.

The screenshot shows a configuration window titled "Merge data with existing user identity". It includes an information icon and the text "Configuration for merging data from multiple data sources." Below this, there are three main sections:

- Merge data with existing user identity:** A toggle switch is set to "YES".
- Merge Imported Data With*:** A dropdown menu is set to "HRFile".
- Import new users?:** A toggle switch is set to "NO".

Below these sections is a label "Import new users while merging data with existing user identity".

The bottom section is titled "Select the field(s) on which user data will merge*". It features two lists of fields with arrows between them to move items:


- Left List:** approveremployeeid, city, comments, companycode, companynumber, contractenddate.
- Right List:** employeeid.


The "employeeid" field is currently selected in the right list.

Notifications and Alerts

You can set up email notifications for selected life cycle changes by using an existing email template or creating a new email template:

Specify the email address of users to be notified in the **Email** field for each **Email Template** you select from the dropdown

 Notifications/Alerts

 Send email notifications for certain conditions

Send Email for All User Lifecycle Changes

admin@sec.com

Email Template

User Import- new hired user...▼

Send Email for New Users detected

analysts@sec.com

Email Template

User Import- terminated use...▼

Send Email for Terminated Users detected

Email

Email Template

-Select- ▼

OR

Select **Create New Email Template** from the **Email Template Select** dropdown menu. See [Email Templates](#) for more information about creating email templates.

Create Email Template

ENTER EMAIL TEMPLATE INFORMATION

Sender Name*

Template Name*

Description

Save

Click **Save And Next** to proceed to [Step 3: Scheduling Job to Run](#).

Step 3: Scheduling Job to Run

To schedule the job to run, complete the following steps:

Select Connection

Configure User Import

Schedule Job to Run

Prev

Save

Run

Provide job details and schedule job. Job can be saved and run later by clicking Save. To run job, click on Run.

JOB DETAILS

Job Name*

User_HRFile_FILE_2017_10_30_16_23_45

Job Description

User Import Job

Enable Job Related Notifications

☒ Yes
 ☐ No

JOB SCHEDULING INFORMATION

Run Job*

☒ Do you want to run job Once ?
 ☐ Do you want to schedule this job for future ?

Job will be scheduled according to the server time. Current server time is - 10/30/2017 16:25:06

Job Details

1. Specify a **Job Name** or use auto-generated name.
2. Enter a **Job Description**.

3. **Enable Job Related Notifications** if you would like to receive email notifications when the job is run.
 - a. If **No**: Proceed without entering additional information.
 - b. If **Yes**:
 - **On Success**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template:
 - **On Failure**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template.
 - **On Misfired**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template.
 - **On Completed with Errors**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template:

Create New Email Template

Sender Name* ⓘ

Template Name* ⓘ

Description

To* ⓘ

From*
test@securonix.com
CC ⓘ

BCC ⓘ

Subject ⓘ

HTML Enabled
YES ☒

Store in Outbox prior to sending?
YES ☒

Use this template for *

Owner ⓘ
Administrators
SECURITYOPERATIONS

Email Body ⓘ
Add Email Template Variables

Rich text editor toolbar: Bold, Italic, Underline, Link, Unlink, Bulleted List, Numbered List, Decrease Indent, Increase Indent, Undo, Redo, Font Color, Background Color, Insert Image, Insert Video, Insert Document, Insert Table, Insert Quote, Insert Code Block, Insert Horizontal Line, Insert Separator.

Job Scheduling Information

1. Select when you would like the job to run.

JOB SCHEDULING INFORMATION

Run Job

☒ Do you want to run job Once ?

☐ Do you want to schedule this job for future ?

 Job will be scheduled according to the server time. Current server time is - 5/1/2017 14:40:57

- Select **Do you want to run job Once?** to run now.
- Select **Do you want to schedule this job for future?** to run the job later and complete the relevant fields.

☒ Do you want to schedule this job for future ?

☒ Seconds

Minutes

Hourly

Daily

Weekly

Monthly

Specify Date

Select how often you want the job to run

Start Job At *

02:38:00 PM

NOTE: This is the server time

Run Every *

Seconds

Stop after

Times

1. **Save** job.
2. Click **Run**.
3. Review the job status to ensure data was loaded successfully.

The Job Monitor screen for this job will appear automatically. To find specific jobs, navigate to **Menu > Operations Center > Job Monitor** and select **User Import** from left navigation panel.

The screenshot shows the 'Job Monitor' interface for 'User Import' jobs. The left sidebar lists various import types, with 'User Import' selected. The main area displays a table of jobs. Two jobs are shown, both with a status of 'COMPLETED'.

Job Name	Creation Date	Start Date	Next Trigger Date	Job Status
USER_IMPORT_FILE_2017_09_05_17_14_47 <small>CREATED BY: ADMIN / JOB TYPE: USER IMPORT</small> <small>EDIT JOB RE-RUN JOB DELETE JOB</small>	TUE, 5 SEP 2017 @ 05:15:19.000 PM	<small>START DATE:</small> TUE, 5 SEP 2017 @ 05:15:18.000 PM <small>END DATE:</small> TUE, 5 SEP 2017 @ 05:15:23.000 PM	NOT SCHEDULED	COMPLETED
USER_IMPORT_FILE_2017_09_05_15_54_05 <small>CREATED BY: ADMIN / JOB TYPE: USER IMPORT</small> <small>EDIT JOB RE-RUN JOB DELETE JOB</small>	TUE, 5 SEP 2017 @ 03:56:59.000 PM	<small>START DATE:</small> TUE, 5 SEP 2017 @ 03:56:59.000 PM <small>END DATE:</small> TUE, 5 SEP 2017 @ 03:57:00.000 PM	NOT SCHEDULED	COMPLETED

At the bottom, there is a pagination bar showing 'First', 'Last', and 'Show 10' options, and a status 'Total results : 2 | Total pages : 1'.

Step 4: Reviewing Imported User Data

To review and manage imported user data, complete the following steps:

1. Navigate to **Menu > Views > User.**

Employee ID	First Name	Last Name	Manager Employee ID	Email	Department	Division	Title	Employee Type
1001	HARRY	OGWA	1012	HARRY.OGWA@scnx.com	Mainframe and Midrange Administration	Global Technology	Vice President Mainframe and Midrange	FT
1002	HOMER	OGWAL	1001	HOMER.OGWAL@scnx.com	Mainframe and Midrange Administration	Global Technology	Associate Mainframe Administrator	FT
1003	HILLARY	OGWA	1001	HILLARY.OGWA@scnx.com	Mainframe and Midrange Administration	Global Technology	Associate Mainframe Administrator	FT
1004	TERRY	MERRITT	1005	TERRY.MERRITT@scnx.com	Consumer Risk	Corporate Risk	Managing Dir. Consumer Risk	FT
1005	TERRY	MERRITT	1025	TERRY.MERRITT@scnx.com	Executive Management	Corporate Risk	Managing Dir. Compliance Risk	FT
1006	MEL	GIBSON	1001	MEL.GIBSON@scnx.com	Mainframe and Midrange Administration	Global Technology	Associate Mainframe Administrator	PT
1007	RAJESH	RAO	1001	RAJESH.RAO@scnx.com	Mainframe and Midrange Administration	Global Technology	Associate Mainframe Administrator	PT
1008	AKON	SHATSU	1001	AKON.SHATSU@scnx.com	Mainframe and Midrange Administration	Global Technology	Associate Mainframe Administrator	PT
1009	HENRY	PATSUN	1001	HENRY.PATSUN@scnx.com	Mainframe and Midrange Administration	Global Technology	Associate Mainframe Administrator	PT
1010	TONY	KULDIP	1001	TONY.KULDIP@scnx.com	Mainframe and Midrange Administration	Global Technology	Associate Mainframe Administrator	FT
1012	JOE	KELLINGTON	1025	JOE.KELLINGTON@scnx.com	Executive Management	Executive Management	Managing Dir. Global Technology	FT
1013	ROBERT	WELLINGTON	1012	ROBERT.WELLINGTON@scnx.com	Data Services	Global Technology	Vice President Data Services	FT
1014	JOHN	KELLER	1013	JOHN.KELLER@scnx.com	Data Services	Global Technology	Associate Data Services	FT
1015	KEVIN	milton	1013	KEVIN.milton@scnx.com	Data Services	Global Technology	Associate Data Services	FT
1016	LARRY	elison	1013	LARRY.elison@scnx.com	Data Services	Global Technology	Associate Data Services	FT

2. Click an Employee ID to view and manage details about users. See [Views](#) in the ArcSight UBA User Guide for more information about what you can do from the Users view screen.

GENERAL DETAILS			
USER ID	EMPLOYEE ID	FIRST NAME	MIDDLE NAME
-	1080	Demetria	N
LAST NAME	JOB CODE	DOMESTIC/INTERNATIONAL	ORGANIZATION UNIT NUMBER
Bridges	M1	-	9
EMPLOYEE TYPE	PROMOTED	EMPLOYEE TYPE DESCRIPTION	LAST PERFORMANCE REVIEW DATE
FT	-	FullTime	-
FULL TIME/PART TIME	COST CENTER NAME	COST CENTER CODE	SHIFT CODE
FullTime	IPROCC09	IPROCC09	-
ORGANIZATION UNIT NUMBER	MAIL CODE	NAME PREFIX	USER GROUP
9	-	-	-
STANDARD HOURS	DEPARTMENT	LAST PERFORMANCE REVIEW RESULT	REGULAR/TEMPORARY
-	Advertising	-	Regular
CRITICALITY	NETWORK ID	COMPANY CODE	NAME SUFFIX
Low	DBridges	MKTG	-
COMPANY NUMBER	PREFERRED NAME	HIERARCHY	TITLE
MKTG9	-	3	Vice President Advertising
STATUS	DIVISION	STATUS DESCRIPTION	COMMENTS
1	Global Marketing, Branding and Corporate Affairs	Active	-
LAN ID	DATASOURCE		
DB1080	HRFile		

Search using Spotter

Upon successful import, the user data will be available for searching in Spotter. To search users in Spotter, complete the following steps:

1. Navigate to **Menu > Security Center > Spotter**.
2. Type `index=users` in search bar and click search icon.

The screenshot displays the ArcSight Spotter search results for the query `index=users`. The interface includes a search bar at the top with the query entered, and a status bar indicating 1,332 events fetched out of 1,332 matched events. The results are presented in a table format with a left-hand sidebar for field selection and a main area for the data rows.

Selected Fields:

- country: 2
- firstname: 100+
- preferredname: 33
- title: 100+
- employeeid: 100+
- hiredate: 27
- division: 14
- companycode: 20
- workphone: 100+
- department: 42
- employeetype: 2
- u_workemail1504649718...: 100+
- statusdescription: 1
- manageremployeeid: 55
- middlename: 14
- lanid: 100+
- employeetypedescription: 2
- lastname: 100+
- jobcode: 23
- workemail: 100+
- location: 22
- costcentername: 19

Search Results:

The results show three user records, each with a blue icon and a list of attributes:

- Record 1:** `companycode = DEP , costcentername = IMFGCCC10 , country = USA , department = Deposit and Debit Card Fulfillment , division = Deposit and Card Products , employeeid = 2843 , employeetype = FT , employeetypedescription = FullTime , firstname = Lars , hiredate = 08/08/2009 00:00:00.000 , jobcode = R1 , lanid = L52843 , lastname = Shah , location = Indianapolis , manageremployeeid = 2835 , status = 1 , statusdescription = Active , title = Associate Deposits and Debit Cards , workemail = Lars.Shah@scnx.com`
- Record 2:** `companycode = DEP , costcentername = IMFGCCC10 , country = USA , department = Deposit and Debit Card Fulfillment , division = Deposit and Card Products , employeeid = 2842 , employeetype = FT , employeetypedescription = FullTime , firstname = Monika , hiredate = 08/08/2009 00:00:00.000 , jobcode = R1 , lanid = Md2842 , lastname = de Chalendar , location = Indianapolis , manageremployeeid = 2835 , status = 1 , statusdescription = Active , title = Associate Deposits and Debit Cards , workemail = Monika.de.Chalendar@scnx.com`
- Record 3:** `companycode = DEP , costcentername = IMFGCCC10 , country = USA , department = Deposit and Debit Card Fulfillment , division = Deposit and Card Products , employeeid = 2841 , employeetype = FT , employeetypedescription = FullTime , firstname = Paul , hiredate = 08/08/2009 00:00:00.000 , jobcode = R1 , lanid = PM2841 , lastname = McLoughlin , location = Indianapolis , manageremployeeid = 2835 , status = 1 , statusdescription = Active , title = Associate Deposits and Debit Cards , workemail = Paul.McLoughlin@scnx.com`



Note: Click for more information about searching [Spotter](#) or see the ArcSight UBA User Guide.

Peer Groups

A Peer Group in ArcSight UBA is defined as a grouping of users that perform similar job functions. Users may be grouped based on department, job code, location, and reporting manager. HR user attributes are typically used for this purpose. You can also derive peer groups based on resources to which users have access. Any number of peer groups can be defined based on business requirements. There is no limit to the number of peer groups that can be created or the number of users assigned to peer groups.

Examples of Peer Groups:

- Employees in the Finance department who perform similar functions
- Employees with the same job code or title who may perform similar functions

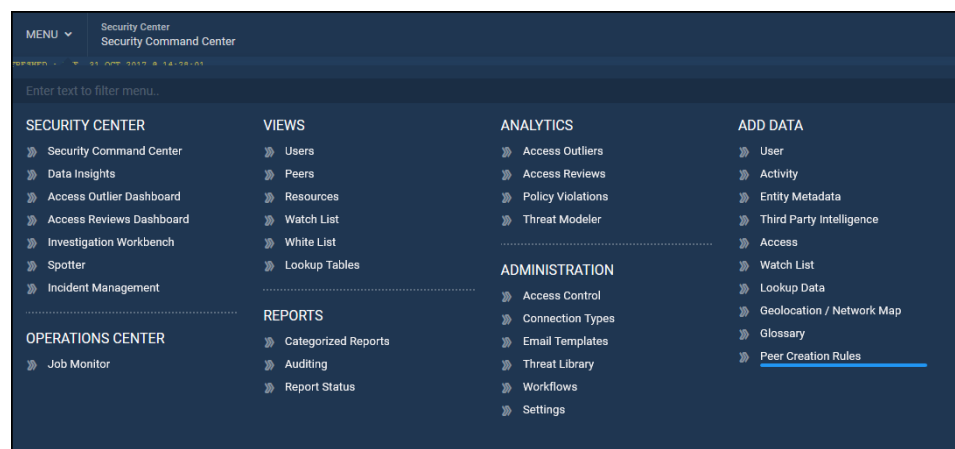
Why Use Peer Groups?

Peer Groups are created to manage Access Outliers, access, and activity logs of the users that belong to a particular Peer Group. A User may belong to one or multiple Peer Groups based on their identity attributes. Each peer group that a user is assigned to may contain other users with different access privileges. Peer Groups are dynamic. The membership and structure change over time.

Some Peer Groups are more “cohesive” than others. Peer Cohesiveness depends on the number of shared properties within the Peer Group. Each access privilege held by a user is compared across the members of each Peer group to determine the number of users that hold the same access privilege. The greater the number of users that hold the same privilege, the less the probability of the access privilege being an outlier. The privilege is determined to be an outlier if it crosses a threshold. Each user within the Peer Group may have one or multiple access privileges that are outliers. The more the number of access privileges that are outliers the higher the overall Access Risk for the user.

Creating Peer Groups

To create a new Peer Group, navigate to **Menu > Add Data > Peer Creation Rules**.



There are three ways to create peer groups and assign users to them:

1. **Peer Creation Rules:** Create Peer Groups using HR attributes and assigns users based on selection criteria automatically.
2. **Peer Assignment Rules:** Assign users to the appropriate Peer Groups based on the criteria specified.
This feature can help maintain user to peer group assignments periodically and when new users are on-boarded into the organization.

Example :

Create a peer group called Financial Analyst and assign all users with title "Associate Financial Accountant" to the Financial Analyst Peer Group.

Example :

Create Peer Groups based on JobCode, Department and the combination of JobCode and Department. Assign users to these Peer groups depending on their jobcode and department.

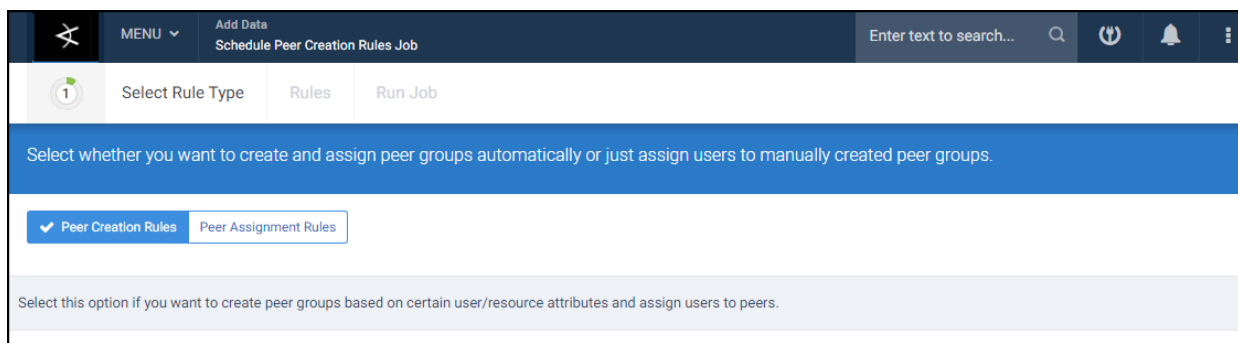
Creating Peer Groups Using Creation Rules

You can create Peer Groups automatically using any user identity attribute. All unique values of the user identity attribute may be used to generate the peer groups. The users will be assigned automatically to these peer groups if they match the criteria.

To add peer groups using **Peer Creation Rules**, complete the following steps:

Select Rule Type

1. Navigate to **Menu > Add Data > Peer Creation Rules**.
2. Select **Peer Creation Rules**.



The screenshot shows a web application interface for configuring Peer Creation Rules. At the top, there is a dark blue header bar with a 'MENU' dropdown, a 'Schedule Peer Creation Rules Job' button, and a search bar. Below the header, there is a white bar with three tabs: 'Select Rule Type', 'Rules', and 'Run Job'. The 'Select Rule Type' tab is active. Below the tabs, there is a blue banner with the text: 'Select whether you want to create and assign peer groups automatically or just assign users to manually created peer groups.' Below the banner, there are two buttons: 'Peer Creation Rules' (which is selected with a checkmark) and 'Peer Assignment Rules'. At the bottom, there is a light blue box with the text: 'Select this option if you want to create peer groups based on certain user/resource attributes and assign users to peers.'

3. Click **Save and Next**.

Rules

1. Select one of the following options from the **Create Peers using attributes for** dropdown:
Users: Creates peer group based on attributes mapped during User Import. Example: department, jobcode, jobtitle, location.

- a. **Rules:** Click **Add Rule** for each rule to add to the Peer Group.



Note: Each rule corresponds to one peer group type. For example, to create peer groups based on user's title attribute, create a new Peer Group Type called Title and select title from Attribute dropdown

- b. **Peer Group Type:** Select a peer group type from the dropdown (Example: Division) OR **Create New Peer Type** to name a new **Peer Group Type**.
- c. **Attribute:** Select user attributes from the dropdown. Example: Department.
- d. **+/-:** Add or remove attributes from rule.

Resources Access: Creates peer group based on attributes mapped during Access Import. Example: memberOf, manager, employeeid.

2 Select Rule Type Rules Run Job

Create Peer Groups based on User or Resource attributes.

Create Peers using attributes for

Resources Access ▼

Select Users to create peer group based on user attributes like title, department, division etc.
Typically, peer groups can be created based on attributes like title, department, jobcode, costcentercode, division, manager etc.
Select Resource to create peer groups based on resource attributes like memberOf, role etc.

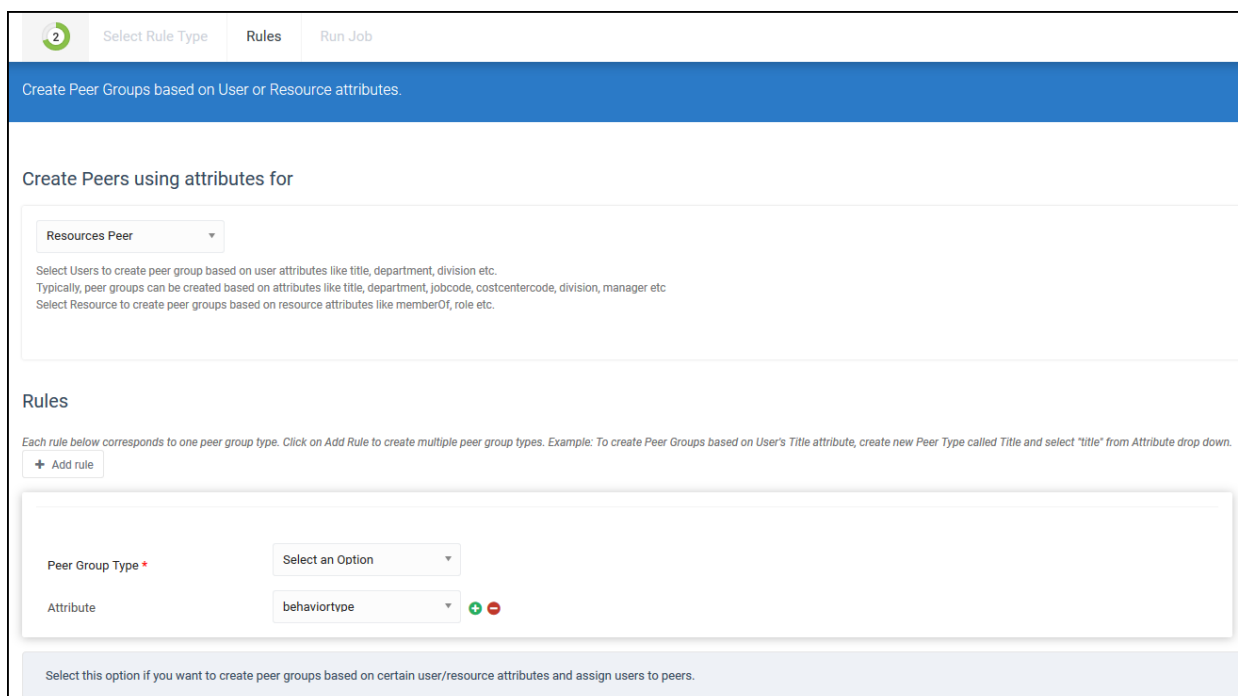
Rules

Object	Attribute	Peer Groups
Access Data ▼	sAMAccountName ▼ <div> <input type="text"/> <input type="button" value="Q"/> </div> <ul style="list-style-type: none"> sAMAccountName homeMTA memberOf manager employeeID 	Peer Group Type * -Select- ▼

Select this option if you want to create peer groups based on certain user/resource attributes

- Object:** Select an object from the dropdown. Example: Access Data.
- Attribute:** Select an attribute from the drop down on which to base the peer group.
Example: memberOf.
- Peer Group Type:** Select a peer group type from the dropdown (Example: Division) OR **Create New Peer Type** to name a new **Peer Group Type**.

Resources Peer: Creates peer group based on certain user/resource attributes.
Example: hierarchy, behavior type, classification.



2 Select Rule Type Rules Run Job

Create Peer Groups based on User or Resource attributes.

Create Peers using attributes for

Resources Peer

Select Users to create peer group based on user attributes like title, department, division etc.
Typically, peer groups can be created based on attributes like title, department, jobcode, costcentercode, division, manager etc.
Select Resource to create peer groups based on resource attributes like memberOf, role etc.

Rules

Each rule below corresponds to one peer group type. Click on Add Rule to create multiple peer group types. Example: To create Peer Groups based on User's Title attribute, create new Peer Type called Title and select "title" from Attribute drop down.

+ Add rule

Peer Group Type *	Select an Option
Attribute	behaviortype + -

Select this option if you want to create peer groups based on certain user/resource attributes and assign users to peers.

- a. **Rules:** Click **Add Rule** for each rule to add to the Peer Group.




Note: Each rule corresponds to one peer group type. For example, to create peer groups based on user's title attribute, create a new Peer Group Type called Title and select title from Attribute dropdown.

- b. **Peer Group Type:** Select a peer group type from the dropdown (Example: Division) OR **Create New Peer Type** to name a new **Peer Group Type**.
- c. **Attribute:** Select user attributes from the dropdown. Example: behavior type..
- d. **+/-:** Add or remove attributes from rule.

2. Click **Save and Next**.

Run Job



Select Rule Type

Rules

Run Job

Provide job details and schedule job. Job can be saved and run later by clicking Save. To run job, click on Run.

Rule Name*

PeerCreationRule_Department_2017_10_23_16_48_47


Rule Description

Create Peer Groups and assign users to peer groups

Run Job

☒ Do you want to run job Once ?

☐ Do you want to schedule this job for future ?



Job will be scheduled according to the server time. Current server time is - 10/23/2017 16:50:26

1. Specify a **Rule Name** or use auto-generated name.
2. Enter a **Rule Description** (optional).

3. Select when you would like the job to run.

JOB SCHEDULING INFORMATION

Run Job

☒ Do you want to run job Once ?

☐ Do you want to schedule this job for future ?

Job will be scheduled according to the server time. Current server time is - 5/1/2017 14:40:57

- Select **Do you want to run job Once?** to run now.
- Select **Do you want to schedule this job for future?** to run the job later and complete the relevant fields.

☒ Do you want to schedule this job for future ?

Select how often you want the job to run

Start Job At *

02:38:00 PM

NOTE: This is the server time

Run Every *

Seconds

Stop after

Times

1. Select when you would like the job to run.
2. **Save** job.
3. Click **Run**.
4. Review the job status to ensure data was loaded successfully.
The Job Monitor screen for this job will appear automatically. To find specific jobs, navigate to **Menu > Operations Center > Job Monitor** and select **Peer Creation Import** from left nav-

igation panel.

Job Name	Creation Date	Start Date	Next Trigger Date	Job Status
PEERCREATIONRULE_DIVISION_2017_9_11_11_58_9 CREATED BY: ADMIN / JOB TYPE: PEER CREATION EDIT JOB RE-RUN JOB DELETE JOB	MON, 11 SEP 2017 @ 01:58:15.000 PM	START DATE: MON, 11 SEP 2017 @ 01:58:15.000 PM END DATE: MON, 11 SEP 2017 @ 01:58:16.000 PM	NOT SCHEDULED	COMPLETED
PEERCREATIONRULE_DEPARTMENT_2017_9_11_11_57_30 CREATED BY: ADMIN / JOB TYPE: PEER CREATION EDIT JOB RE-RUN JOB DELETE JOB	MON, 11 SEP 2017 @ 01:57:36.000 PM	START DATE: MON, 11 SEP 2017 @ 01:57:36.000 PM END DATE: MON, 11 SEP 2017 @ 01:57:36.000 PM	NOT SCHEDULED	COMPLETED

First 1 Last Show 10 Total results: 2 | Total pages: 1

5. Navigate to **Menu > Views > Peers** to view and manage the Peer Groups.

See [Views](#) in the ArcSight UBA User Guide for information about what you can do from this screen.

Peer Name	Member Count	Location	Peer Group Type
A1	1		Job Code
Advertising	12		Department
Ainsley_Moses_1065	13		Manager
Aisling_Culkin_2681	4		Manager
ALABAMA	12		Location
Amal_Wolfe_1068	2		Manager
ANNA_Muldowney_2588	39		Manager
Antoinette_Denvir_1810	3		Manager
Associate Advertising	10		Title

Creating Peer Groups using Peer Assignment Rules

Peer Assignment Rules allow you to specify the rules by which users will be assigned to Peer Groups. To specify Peer Assignment Rules to create Peer Groups, complete the following steps:

Select Rule Type

1. Navigate to **Menu > Add Data > Peer Creation Rules**.
2. Click **Peer Assignment Rules**.
3. Click **Save and Next**.

Rules





Specify the rule by which the users or resources will be added to the selected Peer Groups.

2
Select Rule Type
Rules
Run Job
Prev
Save & Next

Create Peer Groups based on User or Resource attributes.

Specify rules to filter users based on a certain criteria and select peers you want to assign the users to.

Rules

Object	Attribute	Condition	Value*	Operator	
User	employeetype	Equal To	Part Time	AND	 
Resources	locationcode	Equal To	02	AND	 

Add peer groups

+ Add Peer Group(s)
- Remove Peer Group(s)

	Criticality	Peer Name	Member Count	Owner Id	Location	Peer Group Type

- Object:** Select from dropdown:
Users: Specify the user attributes to add users to Peer Groups. Example: Employee Type.
Resources: Specify Resource attributes to add users to Peer Groups. Example: memberOf.
- Attribute:** Select User or Resource attribute from dropdown.
- Condition:** Select from dropdown. Example: Equal To.
- Value:** Specify the value of the attribute. Example: Part Time.
- +/-:** Add or remove rules.

Add Peer Groups

1. Click **Add Peer Group(s)**.

Add Peer Groups

*


activitycohesivness

<input type="checkbox"/>	Criticality	Peer Name	Member Count	Location	Peer Group Type	Risk Score
<input type="checkbox"/>		A1	1		Job Code	0.01
<input checked="" type="checkbox"/>		Advertising	12		Department	0.01
<input checked="" type="checkbox"/>		Ainsley_Moses_1065	13		Manager	0.01
<input type="checkbox"/>		Aisling_Culkin_2681	4		Manager	0.01
<input type="checkbox"/>		A1 ADAMS	10		Location	0.01

Add Selected Peer Groups

- a. Search for specific Peer Groups by attribute and value (optional).
 - b. Select the Peer Groups to which users or resources will be added when above rules are met.
Example: Advertising.
 - c. Click **Add Selected Peer Groups**.
 - d. Click **Remove Peer Groups** to remove the selected Peer Groups.
2. Click **Save and Next**.

Run Job



Select Rule Type

Rules

Run Job

Provide job details and schedule job. Job can be saved and run later by clicking Save. To run job, click on Run.

Rule Name*

PeerCreationRule_Department_2017_10_23_16_48_47


Rule Description

Create Peer Groups and assign users to peer groups

Run Job

☒ Do you want to run job Once ?

☐ Do you want to schedule this job for future ?




Job will be scheduled according to the server time. Current server time is - 10/23/2017 16:50:26

1. Specify a **Rule Name** or use auto-generated name.
2. Enter a **Rule Description** (optional).

3. Select when you would like the job to run.

JOB SCHEDULING INFORMATION

Run Job 

☒ Do you want to run job Once ?

☐ Do you want to schedule this job for future ?

 Job will be scheduled according to the server time. Current server time is - 5/1/2017 14:40:57

- Select **Do you want to run job Once?** to run now.
- Select **Do you want to schedule this job for future?** to run the job later and complete the relevant fields.

☒ Do you want to schedule this job for future ?

✓ Seconds Minutes Hourly Daily Weekly Monthly Specify Date

Select how often you want the job to run

Start Job At *

02:38:00 PM

NOTE: This is the server time

Run Every *

Seconds

Stop after

Times

1. Select when you would like the job to run.
2. **Save** job.
4. Review the job status to ensure data was loaded successfully.
The Job Monitor screen for this job will appear automatically. To find specific jobs, navigate to **Menu > Operations Center > Job Monitor** and select **Peer Creation Import** from left nav-

igation panel.

Job Name	Creation Date	Start Date	Next Trigger Date	Job Status
PEERCREATIONRULE_DIVISION_2017_9_11_11_58_9 CREATED BY: ADMIN / JOB TYPE: PEER CREATION EDIT JOB RE-RUN JOB DELETE JOB	MON, 11 SEP 2017 @ 01:58:15.000 PM	START DATE: MON, 11 SEP 2017 @ 01:58:15.000 PM END DATE: MON, 11 SEP 2017 @ 01:58:16.000 PM	NOT SCHEDULED	COMPLETED
PEERCREATIONRULE_DEPARTMENT_2017_9_11_11_57_30 CREATED BY: ADMIN / JOB TYPE: PEER CREATION EDIT JOB RE-RUN JOB DELETE JOB	MON, 11 SEP 2017 @ 01:57:36.000 PM	START DATE: MON, 11 SEP 2017 @ 01:57:36.000 PM END DATE: MON, 11 SEP 2017 @ 01:57:36.000 PM	NOT SCHEDULED	COMPLETED

First 1 Last Show 10 Total results : 2 | Total pages : 1

- Review the job status to ensure data was loaded successfully.

The Job Monitor screen for this job will appear automatically. To find specific jobs, navigate to **Menu > Operations Center > Job Monitor** and select **Peer Creation Import** from left navigation panel.

Job Name	Creation Date	Start Date	Next Trigger Date	Job Status
PEERCREATIONRULE_DIVISION_2017_9_11_11_58_9 CREATED BY: ADMIN / JOB TYPE: PEER CREATION EDIT JOB RE-RUN JOB DELETE JOB	MON, 11 SEP 2017 @ 01:58:15.000 PM	START DATE: MON, 11 SEP 2017 @ 01:58:15.000 PM END DATE: MON, 11 SEP 2017 @ 01:58:16.000 PM	NOT SCHEDULED	COMPLETED
PEERCREATIONRULE_DEPARTMENT_2017_9_11_11_57_30 CREATED BY: ADMIN / JOB TYPE: PEER CREATION EDIT JOB RE-RUN JOB DELETE JOB	MON, 11 SEP 2017 @ 01:57:36.000 PM	START DATE: MON, 11 SEP 2017 @ 01:57:36.000 PM END DATE: MON, 11 SEP 2017 @ 01:57:36.000 PM	NOT SCHEDULED	COMPLETED

First 1 Last Show 10 Total results : 2 | Total pages : 1

- Navigate to **Menu > Views > Peers** to view and manage the Peer Groups.

See [Views](#) in the ArcSight UBAUser Guide for information about what you can do from this screen.

Activity Data

ArcSight UBA uses out-of-the-box and custom connectors to ingest security log events data from a variety of structured and unstructured data sources including enterprise applications, endpoint monitoring, perimeter security, identity systems, SIEM, and non-technical data sources such as badge readers and social media that are not supported by typical log management solutions.

During ingestion, ArcSight UBA super enriches event data with meaningful context including entity metadata, threat intelligence, geolocation, lookup data, and user identity information such as job function, access privileges, location, peer groups, and activity. This makes raw event data easy to understand, search, and investigate, as in the following illustration:

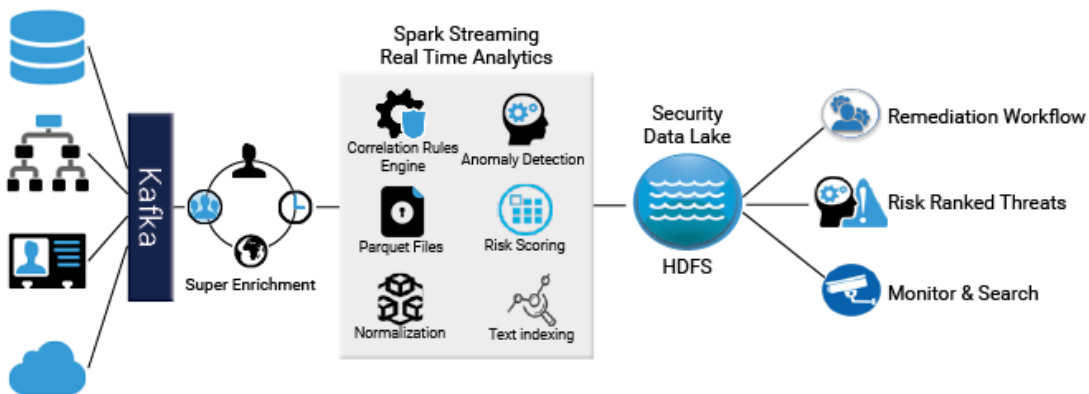
Event Data in SNYPR



The super enriched data is normalized, run through the correlation rules engine, analyzed using policy evaluators and anomaly detection, risk scored, indexed for quick searching, and converted to Parquet. The enriched data is then stored in ArcSight UBA Security Data Lake for long-term compliance. You can view risk ranked results on the Security Dashboard, take action on threats for remediation, and hunt threats using Spotter natural language search engine.

ArcSight UBA can ingest data from both on-premise and remote ingester nodes.

Data Ingestion within SNYPR



ArcSight UBA imports event data using traditional collection methods and out-of-the-box premium connectors. This section describes how to import activity data using the following methods:

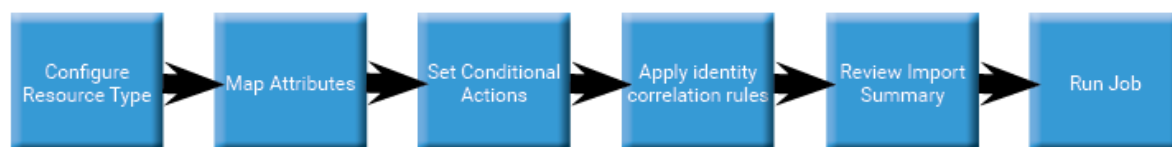
Traditional Collection Methods

Traditional collection methods include structured and unstructured datasources including syslog, JSON, XML, delimited and capturing groups files, and database connection. You can select from existing resource types or create a custom connection.

Steps to configure import from a traditional collection method:

1. Configure the resource type from an existing resource type or create a custom connection.
2. Map event data attributes with corresponding ArcSight UBA attributes.
3. Set conditional actions using enrichment data such as user identity data, entity metadata, geo-location, and third party intelligence.
4. Apply identity correlation rules to attribute user identity to events.
5. Review the import summary, save configuration template, and create behavior profiles to apply to the datasource.
6. Schedule and run the job.

Ingesting Activity Data using traditional Collection Methods



ArcSight UBA can ingest data using the following examples of traditional collection methods:

- [Importing Events from Syslog Files](#)
- Structured log formats
 - [Importing Events from Syslog Files](#)
 - [Importing Events from Syslog Files](#)
- Files
 - [Importing Events from a Delimited File](#)
 - [Importing Events from a Delimited File](#)
- [Importing Events from a Database](#)

To create a new resource type using traditional collection methods, see [Step 1: Configuring the Data-source](#).

Premium Connectors

ArcSight UBA includes premium connectors out-of-the-box, including datasources such as Google, Office 365, Box, Splunk, and Windows WMI. Premium Connectors include out-of-the-box attribute mapping, conditional actions, and identity correlation rules, which you can customize to suit your environment.

Steps to configure import from a premium connector:

1. Configure the resource type from an existing resource type.
2. Review the import summary, save configuration template, and create behavior profiles to apply to the datasource.
3. Schedule and run the job.

Ingesting Activity Data using Premium Connectors



ArcSight UBA can ingest data using the following examples of premium connectors:

- [Importing Events from Apache Subversion \(SVN\)](#)
- [Importing Events from Apache Subversion \(SVN\)](#)
- [Importing Events from Apache Subversion \(SVN\)](#)
- [Importing Events from Apache Subversion \(SVN\)](#)
- [Importing Events from Amazon Web Services Cloudtrail](#)
- [Importing Events from Apache Subversion \(SVN\)](#)

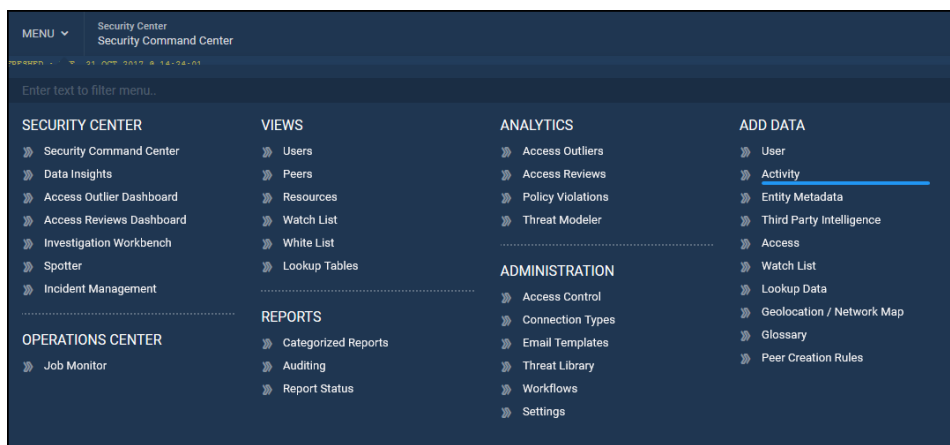
To import activity data into ArcSight UBA, complete the following steps.

Step 1: Configuring the Datasource

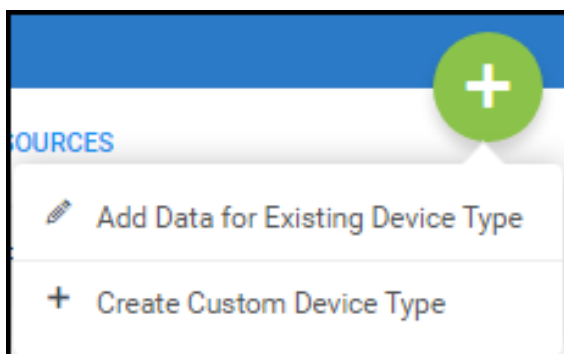
Use traditional collection methods to import activity data from files, applications, databases, security products, network devices, and other sources.

To use traditional collection methods to import activity data, complete the following steps:

1. Navigate to **Menu > Add Data > Activity**.



2. Click **+** to add a datasource.



3. Select **Add Data for Existing Device Type** or **Create Custom Device Type**.
 - a. **Existing Device Type:** Select a **Vendor** or **Functionality**, **Device Type**, and **Collection Method**.

DEVICE TYPE INFORMATION

Vendor

 OR

Functionality

Vendors	Device Types	Collection Method
<div></div>	<div></div>	<div></div>
<div>Securonix</div>	<div>Axway</div>	<div>Syslog [file]</div>
<div>Axway</div>		
<div>Beyond Trust</div>		
<div>Blackberry Limited</div>		
<div>Box</div>		
<div>Branch Office Solutions</div>		

- b. **Custom Device Type:** Select **Duplicate Parser From** from **Device Type Information** drop downs OR create a custom device to indicate how ArcSight UBA should parse the incoming data.

- **Duplicate Parser:** Select **Vendor** OR **Functionality**, **Resource Type**, and **Collection Method** from drop downs to select the collection method from which to duplicate the parsing technique.

- **Custom:** Complete the following steps to create a custom device:
 1. Select **Create New Vendor** and enter Vendor name in the pop up window.

2. Select **Functionality**.
Enter **Resource Type**.
Select **Collection Method** from dropdown.
Select **Import Using** Console or ID of Ingestion Node for environments using remote

ingester.

DEVICE TYPE INFORMATION

Duplicate Parser From ▾

Vendor ▾ OR Functionality ▾

Vendor *

Create New Vendor ▾

Functionality *

Create New Functionality ▾

Resource Type *

Collection Method *

-Select- ▾

Import Using

Console ▾



Note: The information you select will populate the **Device Type Information** section.

4. Complete the following steps to configure the connection:

Device Type Information

Complete the following information:

DEVICE TYPE INFORMATION

Duplicate Parser From ▾

Vendor ▾ OR Functionality ▾

Vendor *

Create New Vendor ▾

Functionality *

Create New Functionality ▾

Resource Type *

Collection Method *

-Select- ▾

Import Using

Console ▾

- Vendor:** Specify new Vendor name.
- Functionality:** Specify a Vendor or Functionality from the dropdown.
- Resource Type:** Specify the resource type based on the vendor or functionality.
- Collection Method:** Specify a collection method based on the available methods for the
- Import Using:** Select from dropdown to specify **Console** or ID of a Ingestion Node.



Note: This option exists only if Ingestion Node is configured for this environment.

Datasources imported from the remote ingester will appear with a cloud icon.

Import activities from files, applications, databases, security products, network devices & other sources.

Enter text to filter datasource

PaloAlto-Monitoring
Palo Alto

Proopoint Protection
ProofPoint Email Gateway

Bluecoat
Bluecoat Proxy

Device Information

Complete the following information:

DEVICE INFORMATION

Datasource Name
Bluecoat Proxy

IP Address

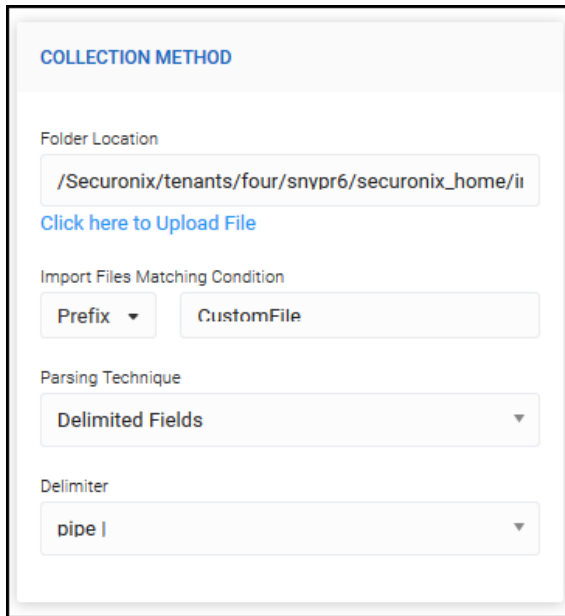
Specify timezone for activity logs
CST6CDT

- Datasource Name:** Specify a unique datasource name.
- IP Address:** Enter an IP address or hostname for the datasource, if required.
- Specify timezone for activity logs:** Specify the time zone for logs using dropdown.

Collection Method

This section is unique to each **Collection Method**. Complete the fields as appropriate for the **Collection Method** you selected in the previous steps.

Example: Delimited File



The screenshot shows a web form titled "COLLECTION METHOD". It contains the following fields:

- Folder Location:** A text input field containing the path `/Securonix/tenants/four/snypr6/securonix_home/ii`. Below it is a blue link that says "Click here to Upload File".
- Import Files Matching Condition:** Two buttons: "Prefix" (with a dropdown arrow) and "CustomFile".
- Parsing Technique:** A dropdown menu currently showing "Delimited Fields".
- Delimiter:** A dropdown menu currently showing "pipe |".

- a. **Folder Location:** Click to upload a file from the local machine or specify the complete path to the folder in which the file to be imported is located. Default: \$securonix_home/import/in.
- b. **Import Files Matching Conditions:** Specify a condition to upload multiple files with the same prefix or postfix. Example: CustomFile_ to select all files between CustomFile_1 and CustomFile_50.
- c. **Parsing Technique:** Select from dropdown. Some options generate a second field.
 - a. **Delimited Fields:** Select to parse delimited fields. Specify a **Delimiter**.
 - b. **Capturing Groups:** Select to parse capturing groups.
 - c. **Key Value Pair:** Select to parse key value pairs.
 - d. **CEF Parser:** Select to parse using CEF.
 - e. **LEEF Parser:** Select to parse using LEEF.
 - f. **Snare Parser:** Select to parse using Snare.
 - g. **Psloglist Parser:** Select to parse using Psloglist.
 - h. **Do Not Parse:** Select to skip **Parsing and Normalization**.

More Settings

Complete the following information:

MORE SETTINGS

Action Taken On Unparsed Events

SAVE IN UNPROCESSED FOLDER ON HDFS

Success Folder

/Securonix/tenants/partnerdemo
/securonix_home/import/success/

Failed Folder

/Securonix/tenants/partnerdemo
/securonix_home/import/failed/

Specify staging folder (Only required for data requiring preprocessing)

/Securonix/tenants/partnerdemo
/securonix_home/import/in/

Enable Preprocessor

YES

Preprocessor Class

- a. **Action Taken on Unparsed Events:** Select from dropdown. The following options are available:
 - Save in unprocessed folder on HDFS
 - Drop Events
 - Ingest as unparsed events
 - a. **Success Folder:** Specify the folder into which you would like the file to move upon successful upload. Default:/Securonix/ArcSight/uba6/securonix_home/import/success/
 - b. **Failed Folder:** Specify the folder into which you would like the file to move upon a failed upload. Default:/Securonix/ArcSight/uba6/securonix_home/import/failed/
 - c. **Staging Folder:** Specify the staging folder (required for data requiring pre-processing). Default:/Securonix/ArcSight/uba6/securonix_home/import/in/
 - d. **Enable Preprocessor:** Set slider to **YES** to enable.
 - a. Provide **Preprocessor Class** value.
5. **Preview Input** to ensure the data has uploaded successfully.

Import activities from files, applications, databases, security products, network devices & other sources.

PREVIEW INPUT

DBAudit.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<Audit xmlns="http://xmlns.oracle.com/oraclees/schema/observer_auditmail-10.2.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://xmlns.oracle.com/oraclees/schema/observer_auditmail-10.2.xsd">
  <Version>10.2</Version>
  <AuditRecord>
    <Audit_Type>1</Audit_Type>
    <Session_Id>900001</Session_Id>
    <StatementId>1</StatementId>
    <EntryId>1</EntryId>
    <Extended_Timestamp>2017-03-24T23:14:49.399000</Extended_Timestamp>
    <DB_User>R01001</DB_User>
    <Client_Id>1001</Client_Id>
  </AuditRecord>
</Audit>
```

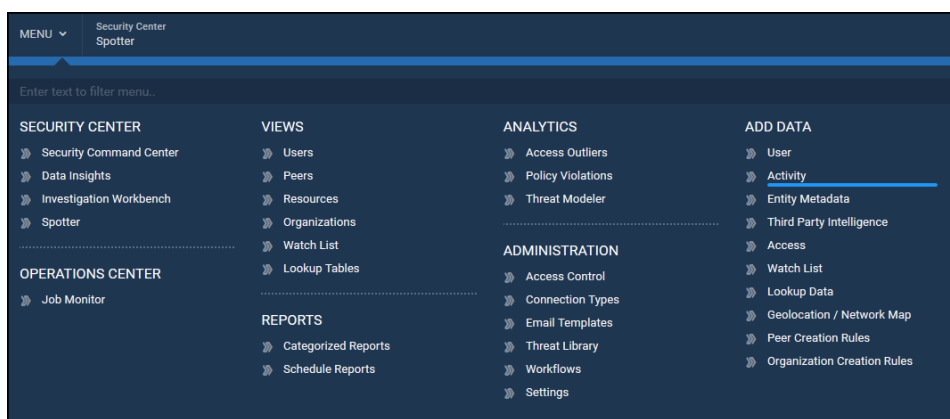
- Click **Save & Next** to proceed to [Step 2: Parsing and Normalization](#).

Importing Events from Syslog Files

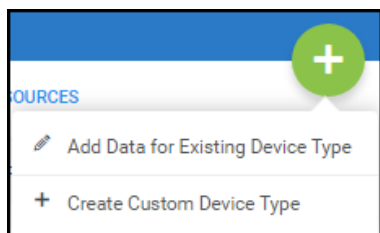
This section describes how to import data from Syslog Files.

To import activity data from a Syslog file, complete the following steps:

- Navigate to **Menu > Add Data > Activity**.



- Click **+** to add a datasource.



3. Select **Add Data for Existing Device Type** or **Create Custom Device Type** from the drop-down.
 - a. **Existing Device Type:** Select a **Vendor** or **Functionality**, **Device Type**, and **Collection Method**.

DEVICE TYPE INFORMATION

Vendor ▾ OR Functionality ▾

Vendors	Device Types	Collection Method
<input type="text"/>	<input type="text"/>	<input type="text"/>
Securonix >	Axway >	Syslog [file] >
Axway >		
Beyond Trust >		
Blackberry Limited >		
Box >		
Branch Office Solutions >		

- b. **Custom Device Type:** Select **Duplicate Parser From** from Device Type Information drop-downs OR create a custom device to indicate how ArcSight UBA should parse the incoming data.

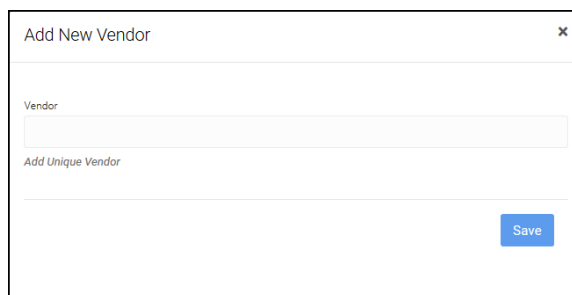
- **Duplicate Parser:** Select **Vendor** OR **Functionality**, **Resource Type**, and **Collection Method** from dropdowns to select the collection method from which to duplicate the parsing technique.

The screenshot shows the 'DEVICE TYPE INFORMATION' form. At the top, there are two dropdown menus: 'Vendor' and 'Functionality', separated by 'OR'. Below these, there are three columns: 'Vendors', 'Device Types', and 'Collection Method'. The 'Vendors' column has a search bar and a list of vendors: '-1', 'Axway', 'Beyond Trust', 'Blackberry Limited', 'Box', 'Branch Office Solutions', and 'Cisco Systems'. The 'Device Types' column has a search bar and one item: 'Watchdax'. The 'Collection Method' column has a search bar and one item: 'Syslog (LEEF) [qradar]'.

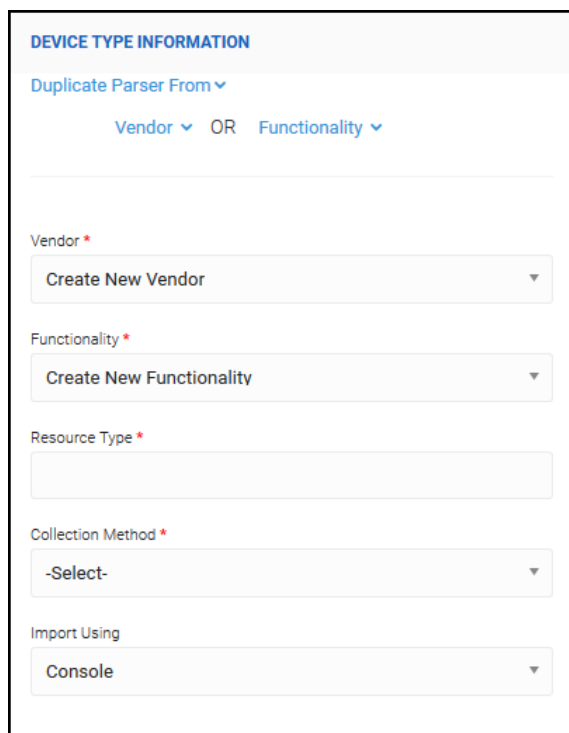
Vendors	Device Types	Collection Method
-1	Watchdax	Syslog (LEEF) [qradar]
Axway		
Beyond Trust		
Blackberry Limited		
Box		
Branch Office Solutions		
Cisco Systems		

- **Custom:** Complete the following steps to create a custom device:

1. Select **Create New Vendor** and enter Vendor name in the pop up window.

A pop-up window titled "Add New Vendor" with a close button (X) in the top right corner. It contains a text input field labeled "Vendor" with the placeholder text "Add Unique Vendor". At the bottom right, there is a blue "Save" button.

2. Select **Functionality**.
Enter **Resource Type**.
Select **Collection Method** from dropdown.
Select **Import Using Console** or ID of Ingestion Node.

A form titled "DEVICE TYPE INFORMATION" with a blue header. Below the title is a section "Duplicate Parser From" with two dropdown menus: "Vendor" and "Functionality", separated by "OR". Below this are four required fields, each with a red asterisk: "Vendor" (dropdown menu showing "Create New Vendor"), "Functionality" (dropdown menu showing "Create New Functionality"), "Resource Type" (text input field), and "Collection Method" (dropdown menu showing "-Select-"). At the bottom is the "Import Using" dropdown menu showing "Console".

Note: The information you select will populate the **Device Type Information** section.

4. Complete the following steps to configure the connection:

Device Type Information

Complete the following information:

DEVICE TYPE INFORMATION

Vendor ▾ OR Functionality ▾

Vendor

Palo Alto Networks

Resource Type

Palo Alto Threat

Collection Method

Syslog [file]

- Functionality:** Specify the Vendor name selected or created in the last step. Example: Palo Alto Networks.
- Resource Type:** Specify the resource type based on the vendor or functionality. Example: Palo Alto Threat.
- Collection Method:** syslog [file].
- Import Using:** Select **Console** or ID of Ingestion Node if using remote ingester in the environment.

Device Information

Complete the following information:

DATASOURCE INFORMATION

Datasource Name

Palo Alto Threat

IP Address

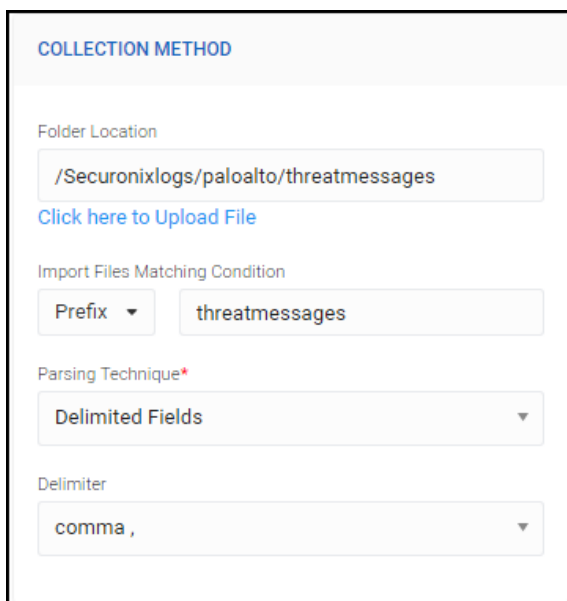
Specify timezone for activity logs

CDT ▾

- a. **Datasource Name:** Specify a unique datasource name. Example: Palo Alto Threat.
- b. **IP Address:** Not required.
- c. **Specify timezone for activity logs:** Specify the time zone for logs using dropdown.

Collection Method

Complete the following information:



The screenshot shows a web form titled 'COLLECTION METHOD' in blue text. Below the title, there are four sections: 1. 'Folder Location' with a text input field containing '/Securonixlogs/paloalto/threatmessages' and a blue link 'Click here to Upload File' below it. 2. 'Import Files Matching Condition' with a 'Prefix' dropdown menu and a text input field containing 'threatmessages'. 3. 'Parsing Technique*' with a dropdown menu showing 'Delimited Fields'. 4. 'Delimiter' with a dropdown menu showing 'comma ,'. The form has a light gray background and a thin black border.

- a. **Folder Location:** Click to upload a file from the local machine or specify the complete path to the folder in which the file to be imported is located. Example: /securonix-logs/paloalto/threatmessages.
- b. **Import Files Matching Conditions:** Specify a condition to upload multiple files with the same prefix or postfix. Example: DBAudit.xml.
- c. **Parsing Technique:** Delimited Fields.
- d. **Delimiter:** Select from dropdown. Example: comma ,.

More Settings

Complete the following information:

MORE SETTINGS

Action Taken On Unparsed Events
 SAVE IN UNPROCESSED FOLDER ON HDFS

Success Folder
 /Securonix/tenants/partnerdemo
 /securonix_home/import/success/

Failed Folder
 /Securonix/tenants/partnerdemo
 /securonix_home/import/failed/

Specify staging folder (Only required for data requiring preprocessing)
 /Securonix/tenants/partnerdemo
 /securonix_home/import/in/

Enable Preprocessor
 YES

Preprocessor Class

- a. **Action Taken on Unparsed Events:** Select from dropdown. The following options are available:
 - Save in unprocessed folder on HDFS
 - Drop Events
 - Ingest as unparsed events
 - a. **Success Folder:** Specify the folder into which you would like the file to move upon successful upload. Default:/Securonix/ArcSight/uba6/securonix_home/import/success/
 - b. **Failed Folder:** Specify the folder into which you would like the file to move upon a failed upload. Default:/Securonix/ArcSight/uba6/securonix_home/import/failed/
 - c. **Staging Folder:** Specify the staging folder (required for data requiring preprocessing). Default:/Securonix/ArcSight/uba6/securonix_home/import/in/
 - d. **Enable Preprocessor:** Set slider to **YES** to enable.
 - a. Provide **Preprocessor Class** value.
5. **Preview Input** to ensure the data has uploaded successfully.

Datasource

Parsing & Normalization

Conditional Actions

Identity Attribution

Summary

Save & Next

Import activities from files, applications, databases, security products, network devices & other sources

BACK TO DATASOURCES

RESOURCE INFORMATION

Vendor

OR

Functionality

Vendor

Palo Alto Networks

Resource Type

Palo Alto Threat

Collection Method

Syslog [file]

DATASOURCE INFORMATION

Datasource Name

Palo Alto Threat

IP Address

Specify timezone for activity logs

CDT

PREVIEW INPUT

threatmessages-2017042605+

OR

Add Sample Lines

Apr 26 05:00:26 10.0.1.2.1	2017/04/26 05:00:25	009401020639	THREAT	url	1	2017/04/26 05:00:25	10.1.51.5	52.71.100.66	209.116.216.129	52.71.100.66	Internet Outgoing	ssl
Apr 26 05:00:34 10.0.1.2.1	2017/04/26 05:00:33	009401020639	THREAT	url	1	2017/04/26 05:00:33	10.1.51.5	13.107.3.128	209.116.216.129	13.107.3.128	Internet Outgoing	skype
Apr 26 05:00:51 10.0.1.2.1	2017/04/26 05:00:51	009401020639	THREAT	url	1	2017/04/26 05:00:51	10.0.1.10	23.1.53.34	209.116.216.129	23.1.53.34	Internet Outgoing	web-brow
Apr 26 05:00:54 10.0.1.2.1	2017/04/26 05:00:54	009401020639	THREAT	url	1	2017/04/26 05:00:54	10.0.0.90	151.101.32.167	209.116.216.129	151.101.32.167	Internet Outgoing	web-brow
Apr 26 05:01:12 10.0.1.2.1	2017/04/26 05:01:12	009401020639	THREAT	url	1	2017/04/26 05:01:12	10.1.51.5	52.71.100.66	209.116.216.129	52.71.100.66	Internet Outgoing	ssl
Apr 26 05:01:29 10.0.1.2.1	2017/04/26 05:01:28	009401020639	THREAT	url	1	2017/04/26 05:01:28	10.1.51.5	107.20.157.74	209.116.216.129	107.20.157.74	Internet Outgoing	web-brow
Apr 26 05:01:33 10.0.1.2.1	2017/04/26 05:01:33	009401020639	THREAT	url	1	2017/04/26 05:01:33	10.1.51.5	172.217.8.174	209.116.216.129	172.217.8.174	Internet Outgoing	google-p
Apr 26 05:01:54 10.0.1.2.1	2017/04/26 05:01:53	009401020639	THREAT	url	1	2017/04/26 05:01:53	10.0.0.90	151.101.32.167	209.116.216.129	151.101.32.167	Internet Outgoing	web-brow
Apr 26 05:01:57 10.0.1.2.1	2017/04/26 05:01:56	009401020639	THREAT	url	1	2017/04/26 05:01:56	10.1.51.5	52.71.100.66	209.116.216.129	52.71.100.66	Internet Outgoing	ssl
Apr 26 05:02:21 10.0.1.2.1	2017/04/26 05:02:21	009401020639	THREAT	url	1	2017/04/26 05:02:21	10.1.51.5	13.107.3.128	209.116.216.129	13.107.3.128	Internet Outgoing	skype
Apr 26 05:02:23 10.0.1.2.1	2017/04/26 05:02:23	009401020639	THREAT	url	1	2017/04/26 05:02:23	10.0.201.1	151.101.48.167	209.116.216.129	151.101.48.167	Internet Outgoing	ssl
Apr 26 05:02:40 10.0.1.2.1	2017/04/26 05:02:40	009401020639	THREAT	url	1	2017/04/26 05:02:40	10.0.51.235	216.58.192.142	209.116.216.129	216.58.192.142	Internet Outgoing	google-s
Apr 26 05:02:40 10.0.1.2.1	2017/04/26 05:02:40	009401020639	THREAT	url	1	2017/04/26 05:02:40	10.0.51.235	172.217.9.78	209.116.216.129	172.217.9.78	Internet Outgoing	google-s
Apr 26 05:02:42 10.0.1.2.1	2017/04/26 05:02:42	009401020639	THREAT	url	1	2017/04/26 05:02:42	10.1.51.5	52.71.100.66	209.116.216.129	52.71.100.66	Internet Outgoing	ssl
Apr 26 05:02:51 10.0.1.2.1	2017/04/26 05:02:51	009401020639	THREAT	url	1	2017/04/26 05:02:51	10.0.1.10	23.1.53.34	209.116.216.129	23.1.53.34	Internet Outgoing	web-brow
Apr 26 05:02:54 10.0.1.2.1	2017/04/26 05:02:53	009401020639	THREAT	url	1	2017/04/26 05:02:53	10.0.0.90	151.101.32.167	209.116.216.129	151.101.32.167	Internet Outgoing	web-brow

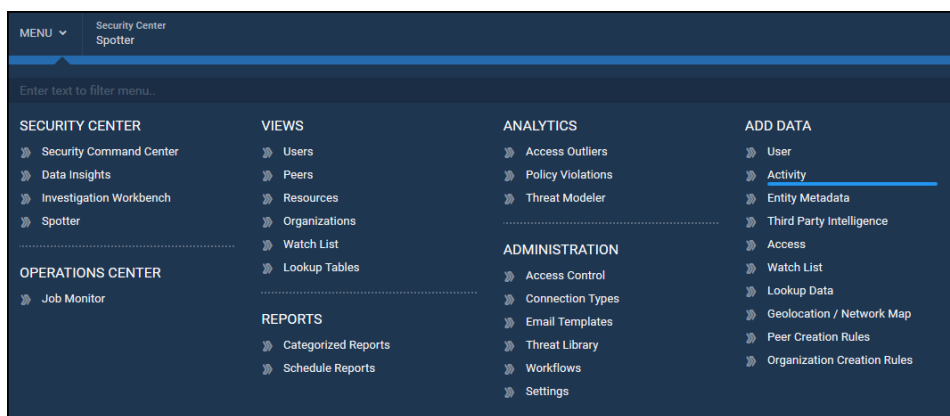
- Click **Save & Next** to proceed to [Step 2: Parsing and Normalization](#).

Importing Events from a JSON File (Key Value Pairs)

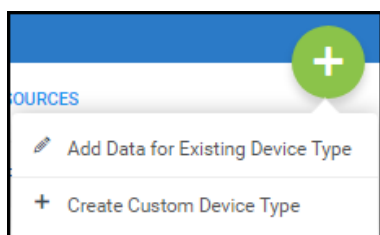
This section describes how to import data in JSON format.

To import activity data from an JSON file, complete the following steps:

- Navigate to **Menu > Add Data > Activity**.



- Click **+** to add a datasource.



3. Select **Add Data for Existing Device Type** or **Create Custom Device Type** from the drop-down.
 - a. **Existing Device Type:** Select a **Vendor** or **Functionality**, **Device Type**, and **Collection Method**.

The screenshot shows a web interface titled "DEVICE TYPE INFORMATION". Below the title, there are two tabs: "Vendor" (selected) and "Functionality". The "Vendor" tab is active, displaying a list of vendors in a table. The table has three columns: "Vendors", "Device Types", and "Collection Method". Each column has a search bar at the top. The "Vendors" column lists several vendors, with "Axway" highlighted. The "Device Types" column shows "Axway" selected. The "Collection Method" column shows "Syslog [file]" selected.

Vendors	Device Types	Collection Method
Securonix		
Axway	Axway	Syslog [file]
Beyond Trust		
Blackberry Limited		
Box		
Branch Office Solutions		

- b. **Custom Device Type:** Select **Duplicate Parser From** from Device Type Information drop downs OR create a custom device to indicate how ArcSight UBA should parse the incoming data.

- **Duplicate Parser:** Select **Vendor** OR **Functionality**, **Resource Type**, and **Collection Method** from drop downs to select the collection method from which to duplicate the parsing technique.

DEVICE TYPE INFORMATION

Duplicate Parser From ▾

Vendor ▾ OR Functionality ▾

	Vendors	Device Types	Collection Method
Vendor *	<input type="text" value="-Select-"/>	<input type="text" value="-Select-"/>	<input type="text" value="-Select-"/>
Functionality	SiteMinder >	bluecoatProxy >	JSON [file] >
-Select-	Sophos >	Bluecoat >	
	Symantec / Blue Coat Systems >	Bluecoat Proxy >	
Resource Ty	Tap2Print >	Bluecoat Proxy ELFF >	
	Unix >	Bluecoat Proxy JSON >	
	Varonis Systems >	Bluecoat Proxy RSync >	
Collection M	Xceedium Inc. / Irdeto >	bluecoatip >	

- **Custom:** Complete the following steps to create a custom device:

DEVICE TYPE INFORMATION

Duplicate Parser From ▾

Vendor ▾ OR Functionality ▾

Vendor *

-Select- ▾

Functionality *

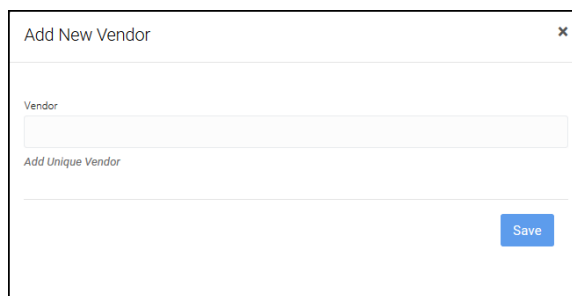
-Select- ▾

Resource Type *

Collection Method *

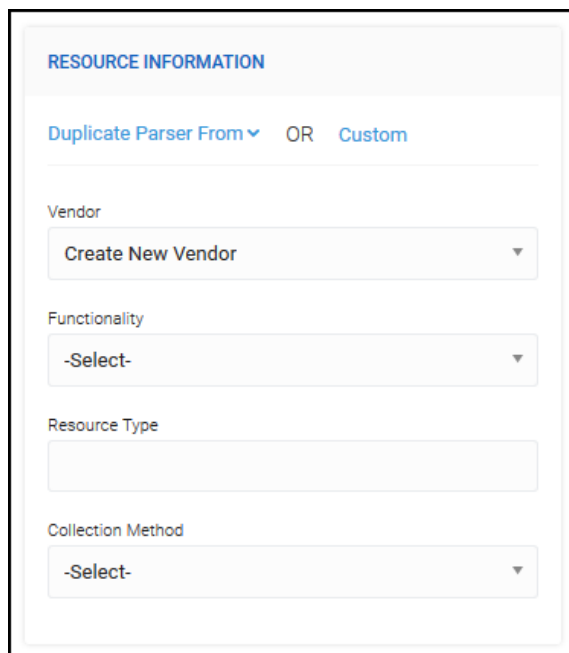
-Select- ▾

1. Select **Create New Vendor** and enter Vendor name in the pop up window.
Example: Securonix.



The screenshot shows a modal window titled "Add New Vendor" with a close button (X) in the top right corner. Inside the window, there is a text input field labeled "Vendor". Below the input field, the text "Add Unique Vendor" is displayed. At the bottom right of the window, there is a blue button labeled "Save".

2. Select **Functionality** or create new Functionality. Example: Web Gateway /Filtering /Proxy.



The screenshot shows a configuration form titled "RESOURCE INFORMATION". At the top, there are two options: "Duplicate Parser From" with a dropdown arrow, followed by "OR" and "Custom". Below this, there are four fields: "Vendor" with a dropdown menu showing "Create New Vendor"; "Functionality" with a dropdown menu showing "-Select-"; "Resource Type" with a text input field; and "Collection Method" with a dropdown menu showing "-Select-".

3. Enter a value for Resource Type. Example: JSON Security Logs.
4. Select **JSON** for the **Collection Method** from the dropdown.
5. Select **Import Using Console** or ID of Ingestion Node if using remote ingester in the environment.

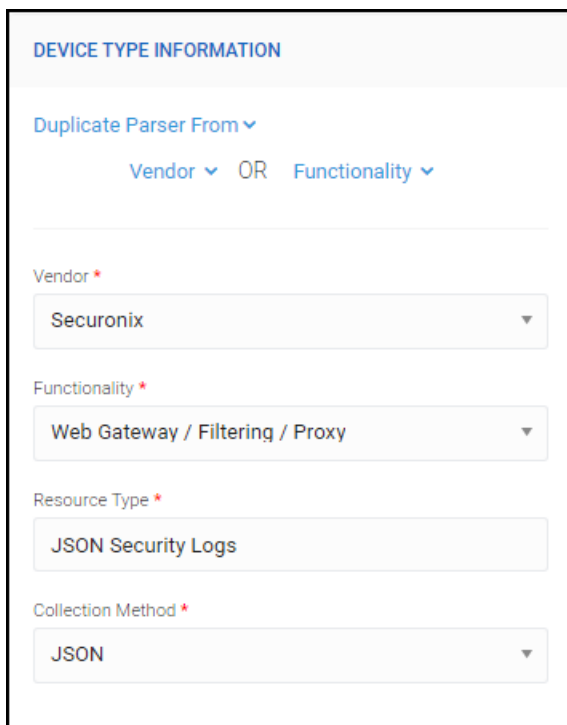


Note: The information you select will populate the **Device Type Information** section.

4. Complete the following steps to configure the connection:

Device Type Information

Complete the following information:



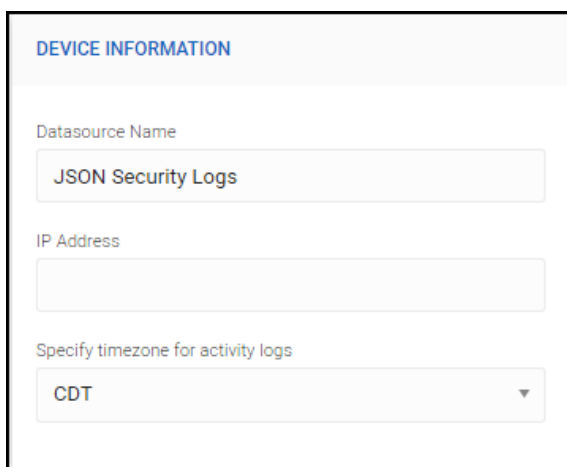
The screenshot shows a configuration form titled "DEVICE TYPE INFORMATION". At the top, there is a section "Duplicate Parser From" with two dropdown menus: "Vendor" and "Functionality", separated by "OR". Below this, there are four required fields, each with a red asterisk:

- Vendor ***: A dropdown menu with "Securonix" selected.
- Functionality ***: A dropdown menu with "Web Gateway / Filtering / Proxy" selected.
- Resource Type ***: A text input field containing "JSON Security Logs".
- Collection Method ***: A dropdown menu with "JSON" selected.

- Vendor**: Specify the Vendor name selected or created in the last step. Example: Securonix.
- Functionality**: Specify the Functionality selected or created in the last step. Example: Web Gateway /Filtering / Proxy.
- Resource Type**: Specify the resource type based on the vendor or functionality. Example: JSON Security Logs.
- Collection Method**: JSON
- Import Using**: Select **Console** or ID of Ingestion Node if using remote ingester in the environment.

Device Information

Complete the following information:



DEVICE INFORMATION

Datasource Name
JSON Security Logs

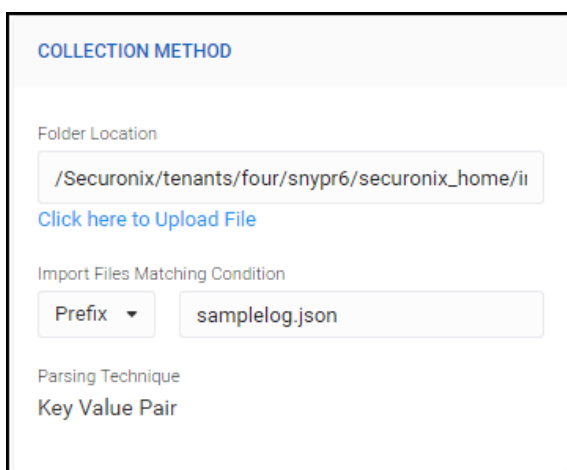
IP Address

Specify timezone for activity logs
CDT

- Datasource Name:** Specify a unique datasource name. Example: JSON Security Logs.
- IP Address:** Not required.
- Specify timezone for activity logs:** Specify the time zone for logs using dropdown.

Collection Method

Complete the following information:



COLLECTION METHOD

Folder Location
/Securonix/tenants/four/snypr6/securonix_home/i
[Click here to Upload File](#)

Import Files Matching Condition
Prefix samplelog.json

Parsing Technique
Key Value Pair

- Folder Location:** Click to upload a file from the local machine or specify the complete path to the folder in which the file to be imported is located. Default: \$securonix_home/import/in.
- Import Files Matching Conditions:** Specify a condition to upload multiple files with the same prefix or postfix. Example: samplelog.json.
- Parsing Technique:** Key Value Pair.

More Settings

Complete the following information:

MORE SETTINGS

Action Taken On Unparsed Events

SAVE IN UNPROCESSED FOLDER ON HDFS

Batch Size

50000

Include Header

NO

Success Folder

/Securonix/tenants/four/snypr6/securonix_home/import/success/

Failed Folder

/Securonix/tenants/four/snypr6/securonix_home/import/failed/

Specify staging folder (Only required for data requiring preprocessing)

/Securonix/tenants/four/snypr6/securonix_home/import/in/

- Action Taken on Unparsed Events:** Select from dropdown. The following options are available:
 - Save in unprocessed folder on HDFS
 - Drop Events
 - Ingest as unparsed events
- Batch Size:** Specify a batch size. Default: 50000.
- Include Header:** Enable to include the header during import.
- Success Folder:** Specify the folder into which you would like the file to move upon suc-

- Successful upload. Default: /Securonix/ArcSight/uba6/securonix_home/import/success/
- e. **Failed Folder:** Specify the folder into which you would like the file to move upon a failed upload. Default: /Securonix/ArcSight/uba6/securonix_home/import/failed/
 - f. **Staging Folder:** Specify the staging folder (required for data requiring preprocessing). Default: /Securonix/ArcSight/uba6/securonix_home/import/in/
5. **Preview Input** to ensure the data has uploaded successfully.

Import activities from files, applications, databases, security products, network devices & other sources.

+ BACK TO DATASOURCES

DEVICE TYPE INFORMATION

Duplicate Parser From

Vendor

Securonix

Functionality

Web Gateway / Filtering / Proxy

Resource Type

JSON Security Logs

Collection Method

JSON

PREVIEW INPUT

samplelog.json

```
[{"event": {"sourceip": "10.0.3.205", "destinationip": "127.0.0.1", "eventcount": "1", "sourceport": "0", "protocolid": "255", "username": "NULL", "logsourceid": "63", "starttime": "1462769861739", "category": "4015", "destinationport": "0", "uid": "38750003", "magnitude": "9", "identityip": "0.0.0.0", "audittype": "LogonEvent"}, {"sourceip": "10.0.3.205", "destinationip": "127.0.0.1", "eventcount": "1", "sourceport": "0", "protocolid": "255", "username": "NULL", "logsourceid": "63", "starttime": "1462770000021", "category": "8052", "destinationport": "0", "uid": "38750003", "magnitude": "9", "identityip": "0.0.0.0"}, {"sourceip": "10.0.3.205", "destinationip": "127.0.0.1", "eventcount": "1", "sourceport": "0", "protocolid": "255", "username": "NULL", "logsourceid": "63", "starttime": "1462770000027", "category": "8052", "destinationport": "0", "uid": "38750003", "magnitude": "9", "identityip": "0.0.0.0"}, {"sourceip": "10.0.3.205", "destinationip": "127.0.0.1", "eventcount": "1", "sourceport": "0", "protocolid": "255", "username": "NULL", "logsourceid": "63", "starttime": "1462770000035", "category": "8052", "destinationport": "0", "uid": "38750003", "magnitude": "9", "identityip": "0.0.0.0"}, {"sourceip": "10.0.3.205", "destinationip": "127.0.0.1", "eventcount": "1", "sourceport": "0", "protocolid": "255", "username": "NULL", "logsourceid": "63", "starttime": "1462770000039", "category": "8052", "destinationport": "0", "uid": "38750003", "magnitude": "9", "identityip": "0.0.0.0"}, {"sourceip": "10.0.3.205", "destinationip": "127.0.0.1", "eventcount": "1", "sourceport": "0", "protocolid": "255", "username": "NULL", "logsourceid": "63", "starttime": "1462770000039", "category": "8052", "destinationport": "0", "uid": "38750003", "magnitude": "9", "identityip": "0.0.0.0"}, {"sourceip": "10.0.3.205", "destinationip": "127.0.0.1", "eventcount": "1", "sourceport": "0", "protocolid": "255", "username": "NULL", "logsourceid": "63", "starttime": "1462770000039", "category": "8052", "destinationport": "0", "uid": "38750003", "magnitude": "9", "identityip": "0.0.0.0"}, {"sourceip": "10.0.3.205", "destinationip": "127.0.0.1", "eventcount": "1", "sourceport": "0", "protocolid": "255", "username": "NULL", "logsourceid": "63", "starttime": "1462770000039", "category": "8052", "destinationport": "0", "uid": "38750003", "magnitude": "9", "identityip": "0.0.0.0"}, {"sourceip": "10.0.3.205", "destinationip": "127.0.0.1", "eventcount": "1", "sourceport": "0", "protocolid": "255", "username": "NULL", "logsourceid": "63", "starttime": "1462770000039", "category": "8052", "destinationport": "0", "uid": "38750003", "magnitude": "9", "identityip": "0.0.0.0"}, {"sourceip": "10.0.3.205", "destinationip": "127.0.0.1", "eventcount": "1", "sourceport": "0", "protocolid": "255", "username": "NULL", "logsourceid": "63", "starttime": "1462770000042", "category": "8052", "destinationport": "0", "uid": "38750003", "magnitude": "9", "identityip": "0.0.0.0"}, {"sourceip": "10.0.3.205", "destinationip": "127.0.0.1", "eventcount": "1", "sourceport": "0", "protocolid": "255", "username": "NULL", "logsourceid": "63", "starttime": "1462770000044", "category": "8052", "destinationport": "0", "uid": "38750003", "magnitude": "9", "identityip": "0.0.0.0", "testcustom": "TEST EVENT"}]
```

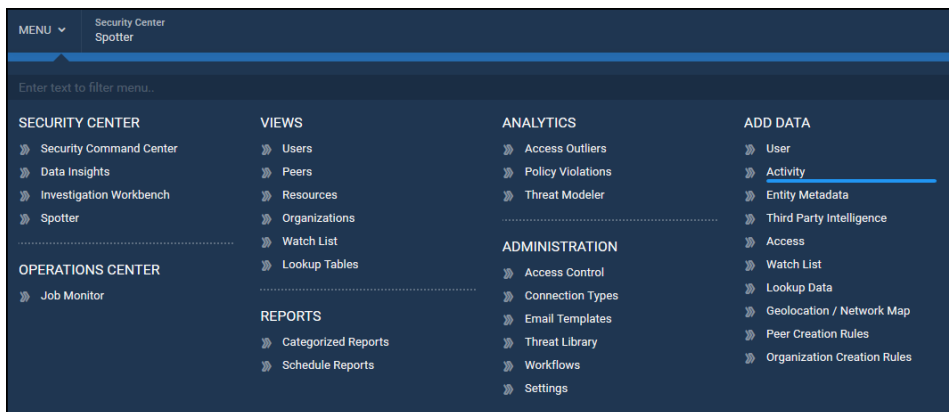
6. Click **Save & Next** to proceed to [Step 2: Parsing and Normalization](#).

Importing Events from an XML File (Key Value Pairs)

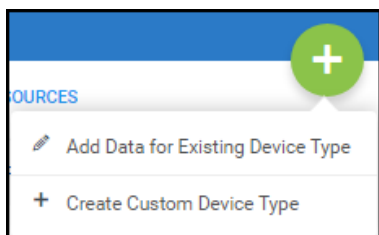
This section describes how to import data in XML format.

To import activity data from an XML file, complete the following steps:

1. Navigate to **Menu > Add Data > Activity**.



2. Click **+** to add a datasource.



3. Select **Add Data for Existing Device Type** or **Create Custom Device Type** from the drop-down.
 - a. **Existing Device Type:** Select a **Vendor** or **Functionality**, **Device Type**, and **Collection Method**.

DEVICE TYPE INFORMATION

Vendor ▼ OR Functionality ▼

Vendors	Device Types	Collection Method
<input type="text"/>	<input type="text"/>	<input type="text"/>
Securonix >	Axway >	Syslog [file] >
Axway >		
Beyond Trust >		
Blackberry Limited >		
Box >		
Branch Office Solutions >		

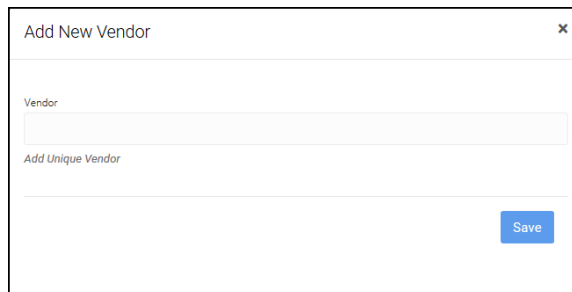
- b. **Custom Device Type:** Select **Duplicate Parser From** from Device Type Information drop downs OR create a custom device to indicate how ArcSight UBA should parse the incoming data.

- **Duplicate Parser:** Select **Vendor** OR **Functionality**, **Resource Type**, and **Collection Method** from drop downs to select the collection method from which to duplicate the parsing technique.

The screenshot shows the 'DEVICE TYPE INFORMATION' form with the 'Duplicate Parser From' dropdown menu open. The menu has two tabs: 'Vendor' and 'Functionality'. The 'Vendor' tab is selected, showing a list of vendors. The 'Functionality' tab is also visible, showing a list of functionalities. The 'Collection Method' dropdown is also visible, showing a list of collection methods.

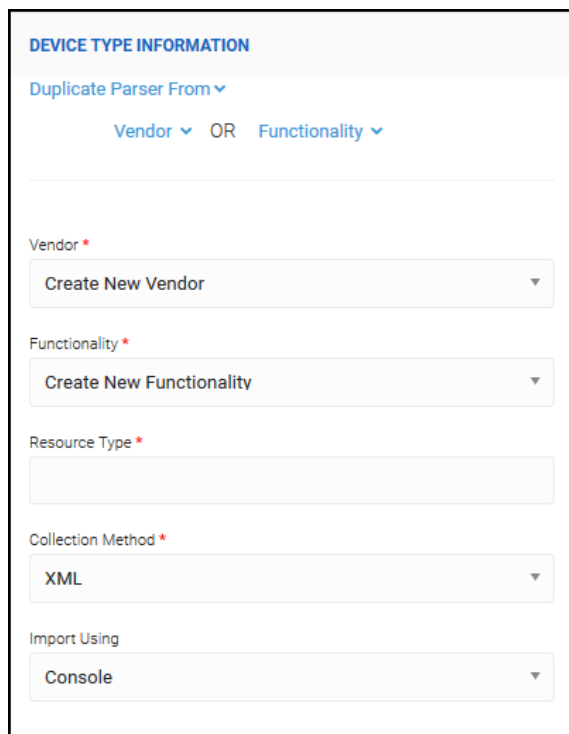
Vendors	Device Types	Collection Method
-1	Powerbroker	Database [database]
Axway		Splunk [splunk]
Beyond Trust		
Blackberry Limited		
Box		
Branch Office Solutions		
Cisco Systems		

- **Custom:** Complete the following steps to create a custom device:
 1. Select **Create New Vendor** and enter Vendor name in the pop up window.
Example: Securonix.



The screenshot shows a modal window titled "Add New Vendor" with a close button (X) in the top right corner. Inside the window, there is a text input field labeled "Vendor". Below the input field, the text "Add Unique Vendor" is displayed. At the bottom right of the window, there is a blue button labeled "Save".

2. Select **Functionality** from dropdown or **Create New Functionality**. Example: Data loss prevention.



The screenshot shows a form titled "DEVICE TYPE INFORMATION". At the top, there is a section "Duplicate Parser From" with a dropdown arrow. Below this, there are two options: "Vendor" and "Functionality", separated by "OR". The "Vendor" option is selected. Below the "Vendor" option, there is a dropdown menu with "Create New Vendor" selected. Below the "Functionality" option, there is a dropdown menu with "Create New Functionality" selected. Below these, there is a text input field labeled "Resource Type". Below that, there is a dropdown menu labeled "Collection Method" with "XML" selected. At the bottom, there is a dropdown menu labeled "Import Using" with "Console" selected.

3. Enter **Resource Type** based on vendor and functionality.
4. Select **XML** from **Collection Method** dropdown.
5. Select **Import Using Console** or ID of Ingestion Node if using remote ingester in the environment.



Note: The information you select will populate the Device Type Information section.

4. Complete the following steps to configure the connection:

Device Type Information

Complete the following information:

DEVICE TYPE INFORMATION

Vendor ▼ OR Functionality ▼

Functionality

Securonix

Resource Type

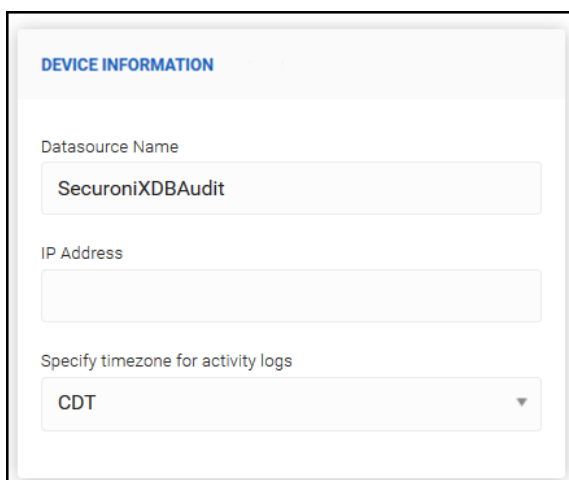
Collection Method

xml [xml]

- a. **Vendor:** Specify the Vendor name selected or created in the last step. Example: Securonix.
- b. **Functionality:** Specify the Functionality selected or created in the last step. Example: Data Loss Prevention
- c. **Resource Type:** Specify the resource type based on the vendor or functionality. Example: Security Logs.
- d. **Collection Method:** XML.
- e. **Import Using:** Select **Console** or ID of Ingestion Node if using remote ingester in the environment.

Device Information

Complete the following information:

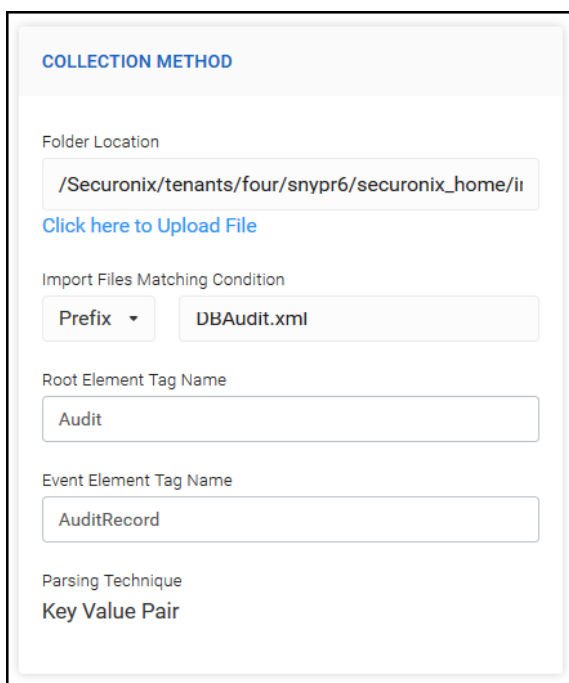


The screenshot shows a web form titled "DEVICE INFORMATION". It contains three fields: "Datasource Name" with the value "SecuroniXDBAudit", "IP Address" which is empty, and "Specify timezone for activity logs" with a dropdown menu showing "CDT".

- a. **Datasource Name:** Specify a unique datasource name. Example: SecuroniXDBAudit.
- b. **IP Address:** Not required.
- c. **Specify timezone for activity logs:** Specify the time zone for logs using dropdown.

Collection Method

Complete the following information:



The screenshot shows a web form titled "COLLECTION METHOD". It contains several fields: "Folder Location" with the value "/SecuroniX/tenants/four/snypr6/securonix_home/it", a link "Click here to Upload File", "Import Files Matching Condition" with a "Prefix" dropdown and the value "DBAudit.xml", "Root Element Tag Name" with the value "Audit", "Event Element Tag Name" with the value "AuditRecord", and "Parsing Technique" with the value "Key Value Pair".

- a. **Folder Location:** Click to upload a file from the local machine or specify the complete path to the folder in which the file to be imported is located. Default: \$securonix_home/import/in.
- b. **Import Files Matching Conditions:** Specify a condition to upload multiple files with the same prefix or postfix. Example: DBAudit.xml.
- c. **Root Element Tag Name:** Specify the root element tag name from the XML file. Example: Audit
- d. **Event Element Tag Name:** Specify the event element tag name from the XML file. Example: AuditRecord
- e. **Parsing Technique:** Key Value Pair.

More Settings

Complete the following information:

MORE SETTINGS

Action Taken On Unparsed Events

SAVE IN UNPROCESSED FOLDER ON HDFS

Batch Size

50000

Include Header

NO

Record Element

Record Attribute

Success Folder

/Securonix/tenants/zohra/securonix_home/import/success/

Failed Folder

/Securonix/tenants/zohra/securonix_home/import/failed/

Specify staging folder (Only required for data requiring preprocessing)

/Securonix/tenants/zohra/securonix_home/import/in/

- a. **Action Taken on Unparsed Events:** Select from dropdown. The following options are available:
 - Save in unprocessed folder on HDFS
 - Drop Events
 - Ingest as unparsed events
 - a. **Batch Size:** Specify a batch size. Default: 50000.
 - b. **Include Header:** Enable to include the header during import.
 - c. **Record Element:** Enter the XML record element.
 - d. **Record Attribute:** Enter the XML record attribute.
 - a. **Success Folder:** Specify the folder into which you would like the file to move upon successful upload. Default: /Securonix/ArcSight/uba6/securonix_home/import/success/
 - b. **Failed Folder:** Specify the folder into which you would like the file to move upon a failed upload. Default: /Securonix/ArcSight/uba6/securonix_home/import/failed/
 - c. **Staging Folder:** Specify the staging folder (required for data requiring preprocessing). Default: /Securonix/ArcSight/uba6/securonix_home/import/in/
5. **Preview Input** to ensure the data has uploaded successfully.

The screenshot shows the 'Preview Input' step in the ArcSight User Behavior Analytics 6.10 Administration Guide. The interface is divided into a sidebar and a main content area. The sidebar contains a 'Resource Type Information' section with a 'Vendor' dropdown set to 'Securonix' and a 'Resource Type' field. Below this is a 'Datasource Information' section with a 'Datasource Name' field set to 'SecuronixDBAudit'. The main content area displays a preview of XML data for 'DBAudit.xml'. The XML data is shown in a table format with various fields and their values, including 'Audit_Type', 'Session_Id', 'StatementId', 'EntryId', 'Extended_Timestamp', 'DB_User', 'Client_Id', and 'DB_User'.

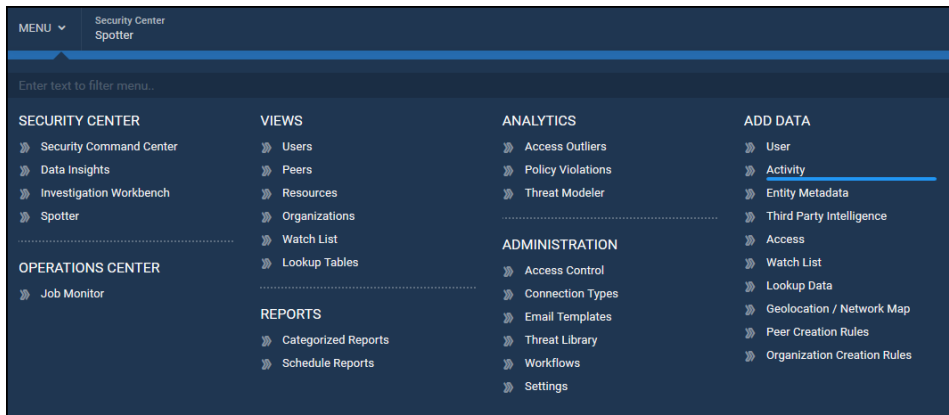
6. Click **Save & Next** to proceed to [Step 2: Parsing and Normalization](#).

Importing Events from a Delimited File

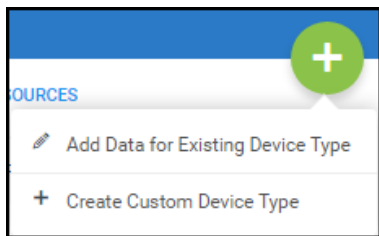
This section describes how to import data from a delimited .csv file.

To import activity data from a delimited file, complete the following steps:

1. Navigate to **Menu > Add Data > Activity**.



2. Click **+** to add a new datasource.



3. Select **Add Data for Existing Device Type** or **Create Custom Device Type** from the drop-down.



Note: You can search for **Existing Device Types** to find the specific vendor or functionality you are looking for. If you do not find the specific resource, select **Create Custom Device Type**.

- a. **Existing Device Type:** Select a **Vendor** or **Functionality, Device Type**, and **Collection Method**.

DEVICE TYPE INFORMATION

Vendor

 OR

Functionality

Vendors	Device Types	Collection Method
<div></div>	<div></div>	<div></div>
<div>Securonix</div>	<div>Axway</div>	<div>Syslog [file]</div>
<div>Axway</div>		
<div>Beyond Trust</div>		
<div>Blackberry Limited</div>		
<div>Box</div>		
<div>Branch Office Solutions</div>		

- b. **Custom Device Type:** Select **Duplicate Parser From** from Device Type Information drop downs OR create a custom device to indicate how ArcSight UBA should parse the incoming data.

- **Duplicate Parser:** Select **Vendor** OR **Functionality**, **Resource Type**, and **Collection Method** from drop downs to select the collection method from which to duplicate the parsing technique.

- **Custom:** Complete the following steps to create a custom device:
 1. Select **Create New Vendor** and enter Vendor name in the pop up window.

2. Select **Functionality**, enter **Resource Type**, and select **Collection Method** from dropdown.
3. Select **Import Using** Console or ID of Ingestion Node if using remote ingester in the environment.




Note: The information you select will populate the **Device Type Information** section.

4. Complete the following steps to configure the connection:

Device Type Information

The following information is populated by the previous step:

DEVICE TYPE INFORMATION	
Vendor	Palo Alto Networks
Resource Type	Palo Alto
Collection Method	Delimited-pipe [file]
Import Using	Console 

- Functionality:** Vendor name. Example: Palo Alto Networks.
- Resource Type:** The **Resource Type** you specified. Example: Palo Alto.
- Collection Method:** Delimited-pipe [file]
- Import Using:** Select **Console** or ID of Ingestion Node if using remote ingester in the environment.

Device Information

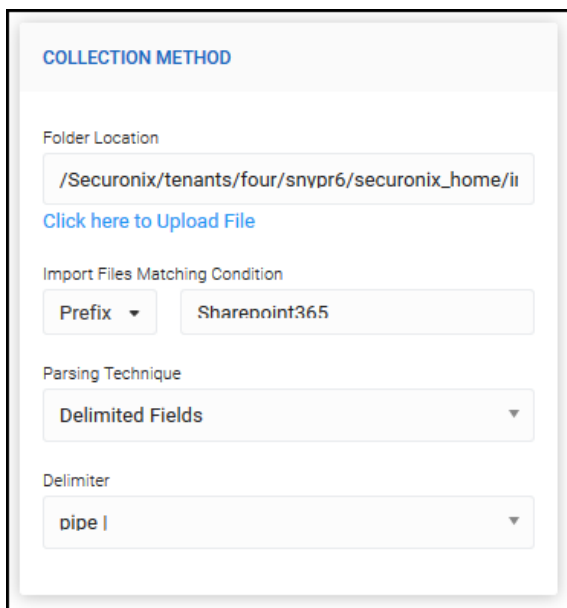
1. Complete the following information:

DEVICE INFORMATION
Datasource Name
<input type="text" value="PaloAlto-Monitoring"/>
IP Address
<input type="text"/>
Specify timezone for activity logs
<input type="text" value="CST"/>

- Datasource Name:** Specify a unique Datasource name.
- IP Address:** Not required.
- Specify timezone for activity logs:** Specify your time zone using dropdown.

Collection Method

2. Complete the following information:



The screenshot shows a web form titled "COLLECTION METHOD". It contains the following fields and options:

- Folder Location:** A text input field containing the path `/Securonix/tenants/four/snypr6/securonix_home/ii`. Below the field is a blue link that says "Click here to Upload File".
- Import Files Matching Condition:** A section with a dropdown menu set to "Prefix" and a text input field containing "Sharepoint365".
- Parsing Technique:** A dropdown menu set to "Delimited Fields".
- Delimiter:** A dropdown menu set to "pipe |".

- a. **Folder Location:**
 - a. Specify the folder location of the file(s) you want to import. Default: `/Securonix/ArcSight/uba6/securonix_home/import/in`
OR
 - b. Click to upload file and browse for file on your local machine.
- b. **Import Files Matching Condition:** Specify the prefix or postfix and supply a condition to upload multiple files. Example: Prefix `Sharepoint365)_` will upload `Sharepoint365_1` through `Sharepoint365_50`.
- c. **Parsing Technique:** Delimited Fields.
- d. **Delimiter:** | (pipe).

More Settings

3. Complete the following information:

MORE SETTINGS

Action Taken On Unparsed Events
SAVE IN UNPROCESSED FOLDER ON HDFS

Success Folder
/Securonix/tenants/partnerdemo
/securonix_home/import/success/

Failed Folder
/Securonix/tenants/partnerdemo
/securonix_home/import/failed/

Specify staging folder (Only required for data requiring preprocessing)
/Securonix/tenants/partnerdemo
/securonix_home/import/in/

Enable Preprocessor
YES

Preprocessor Class

- a. **Action Taken on Unparsed Events:** Select from dropdown. The following options are available:
 - Save in unprocessed folder on HDFS
 - Drop Events
 - Ingest as unparsed events
- a. **Success Folder:** Specify the folder into which you would like the file to move upon successful upload. Default:/Securonix/ArcSight/uba6/securonix_home/import/success/
- b. **Failed Folder:** Specify the folder into which you would like the file to move upon a failed upload. Default:/Securonix/ArcSight/uba6/securonix_home/import/failed/
- c. **Staging Folder:** Specify the staging folder (required for data requiring preprocessing). Default:/Securonix/ArcSight/uba6/securonix_home/import/in/
- d. **Enable Preprocessor:** Set slider to **YES** to enable.
 - a. Provide **Preprocessor Class** value.

4. **Preview Input** to ensure the data has uploaded successfully.

Resource Type Information Parsing & Normalization Conditional Actions Identity Attribution Summary Save & Next											
<div> <div> Import activities from files, applications, databases, security products, network devices & other sources. </div> <div> + BACK TO DATASOURCES </div> <div> <div>RESOURCE INFORMATION</div> <div> Vendor ▼ OR Functionality ▼ </div> <div> Functionality Securonix </div> <div> Resource Type </div> <div> Collection Method Delimited pipe file </div> </div> <div> <div>DATASOURCE INFORMATION</div> <div> Datasource Name SharepointCsrTest </div> <div> IP Address </div> <div> Specify timezone for activity logs CDT </div> </div> </div>											
PREVIEW INPUT											
174	SharePointOnline0365	Catherine.Ryan@acme.com	10.251.58.202	FileDownloaded	2016-11-8 21:11:12	174-174-174	membership	Patrick.Walsh@sec.com	SharePoint	https://acme.sharepoint.com/teftoc	
76	SharePointOnline0365	Robert.Meadows@acme.com	10.75.162.41	FileDownloaded	2016-11-12 8:9:46	76-76-76	membership	Arya.Majid@sec.com	SharePoint	https://acme.sharepoint.com/teftoc	
228	SharePointOnline0365	Joseph.Farnet@acme.com	10.225.119.127	FileDownloaded	2016-11-26 17:59:0	228-228-228	membership	Alexia.Quail@sec.com	SharePoint	https://acme.sharepoint.com/teftoc	
59	SharePointOnline0365	Ann.McCormack@acme.com	10.0.0.10	FileDownloaded	2016-11-6 18:21:32	59-59-59	membership	Caren.Foley@sec.com	SharePoint	https://acme.sharepoint.com/teftoc	
141	SharePointOnline0365	Paula.Finlay@acme.com	10.0.0.10	FileDownloaded	2016-11-25 12:39:35	141-141-141	membership	Harvey.Lock@sec.com	SharePoint	https://acme.sharepoint.com/teftoc	
234	SharePointOnline0365	Joanna.Kelly@acme.com	10.192.16.124	FileDownloaded	2016-11-11 12:35:20	234-234-234	membership	Conor.Edmonds@sec.com	SharePoint	https://acme.sharepoint.com/teftoc	
61	SharePointOnline0365	Hedley.Carmel@acme.com	10.22.124.16	FileDownloaded	2016-11-14 14:9:32	61-61-61	membership	Stuart.Gleeson@sec.com	SharePoint	https://acme.sharepoint.com/teftoc	
3	SharePointOnline0365	Ursula.Angelo@acme.com	10.52.160.128	FileDownloaded	2016-11-25 14:21:18	3-3-3	membership	Chaim.Villanet@sec.com	SharePoint	https://acme.sharepoint.com/teftoc	
211	SharePointOnline0365	NORA.LEWIS@acme.com	10.203.109.172	FileDownloaded	2016-11-15 16:11:12	211-211-211	membership	Assumpta.Mooney@sec.com	SharePoint	https://acme.sharepoint.com/teftoc	
98	SharePointOnline0365	Laura.Craigh@acme.com	10.69.64.223	FileDownloaded	2016-11-12 3:4:37	98-98-98	membership	Megan.Scandenberg@sec.com	SharePoint	https://acme.sharepoint.com/teftoc	
216	SharePointOnline0365	David.Rukowski@acme.com	10.0.0.10	FileDownloaded	2016-11-1 22:52:56	216-216-216	membership	Seamus.O'Malley@sec.com	SharePoint	https://acme.sharepoint.com/teftoc	
61	SharePointOnline0365	Alice.Knight@acme.com	10.57.31.166	FileDownloaded	2016-11-20 10:35:59	61-61-61	membership	Aon-Marie.Barry@sec.com	SharePoint	https://acme.sharepoint.com/teftoc	
216	SharePointOnline0365	Judith.McMahon@acme.com	10.166.22.234	FileDownloaded	2016-11-16 18:5:18	216-216-216	membership	Virginia.Kavanagh@sec.com	SharePoint	https://acme.sharepoint.com/teftoc	
218	SharePointOnline0365	Carolina.Buckley@acme.com	10.255.38.31	FileDownloaded	2016-11-30 20:31:48	218-218-218	membership	Rajni.Hendrix@sec.com	SharePoint	https://acme.sharepoint.com/teftoc	
56	SharePointOnline0365	Jan.Gyork@acme.com	10.0.0.10	FileDownloaded	2016-11-16 22:40:4	56-56-56	membership	Michael.Cassidy@sec.com	SharePoint	https://acme.sharepoint.com/teftoc	

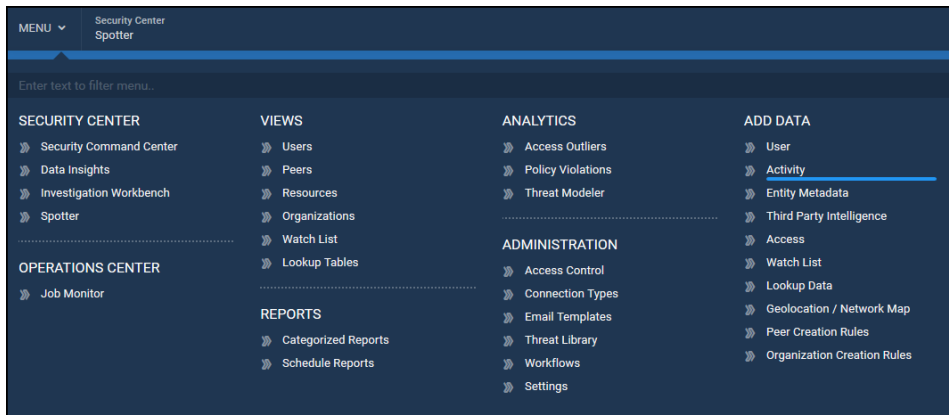
5. Click **Save & Next** to proceed to [Step 2: Parsing and Normalization](#).

Importing Events from a Regex File (Capturing Groups)

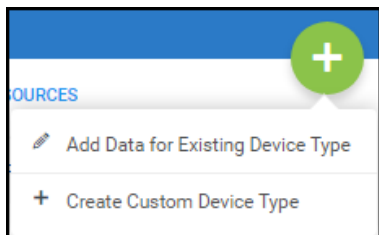
This section describes how to import data from a Regex (regular expression) file.

To import activity data from a regex (capturing groups) file, complete the following steps:

1. Navigate to **Menu > Add Data > Activity**.



2. Click **+** to add a new datasource.



3. Select **Add Data for Existing Device Type** or **Create Custom Device Type** from the drop-down.



Note: You can search for **Existing Device Types** to find the specific vendor or functionality you are looking for. If you do not find the specific resource, select **Create Custom Device Type**.

- a. **Existing Device Type:** Select a **Vendor** or **Functionality**, **Device Type**, and **Collection Method**.

DEVICE TYPE INFORMATION		
Vendor ▼ OR Functionality ▼		
Vendors	Device Types	Collection Method
<input type="text"/>	<input type="text"/>	<input type="text"/>
Securonix >	Axway >	Syslog [file] >
Axway >		
Beyond Trust >		
Blackberry Limited >		
Box >		
Branch Office Solutions >		

- b. **Custom Device Type:** Select **Duplicate Parser From** from Device Type Information drop downs OR create a custom device to indicate how ArcSight UBA should parse the incoming data.

- **Duplicate Parser:** Select **Vendor** OR **Functionality**, **Resource Type**, and **Collection Method** from drop downs to select the collection method from which to duplicate the parsing technique.

DEVICE TYPE INFORMATION

Duplicate Parser From ▾

Vendor ▾ OR Functionality ▾

Vendors	Device Types	Collection Method
<input type="text"/>	<input type="text"/>	<input type="text"/>
-Select-		
Box >	Citrix_VPN >	Regex [file]
Cerner >		Delimited-pipe [file]
Cisco Systems >		
Citrix_VPN_SK >		
Digital Guardian >		
Google >		
Infoblox >		

Vendor *
-Select-

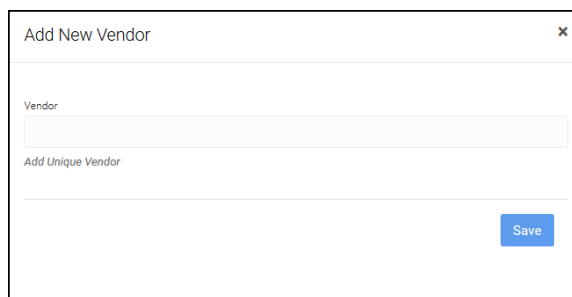
Functionality
-Select-

Resource Ty
-

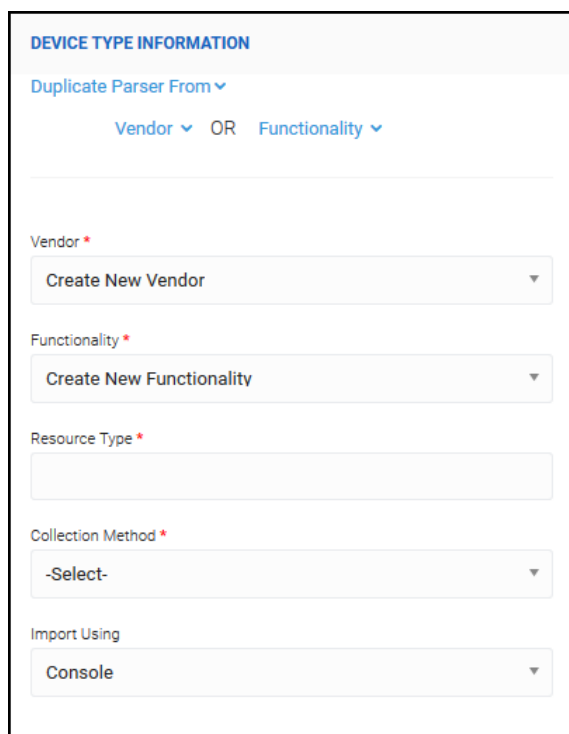
Collection M
-Select-

- **Custom:** Complete the following steps to create a custom device:

1. Select **Create New Vendor** and enter Vendor name in the pop up window.



2. Select **Functionality**, enter **Resource Type**, and select **Collection Method** from dropdown.



3. Select **Import Using** Console or ID of Ingestion Node if using remote ingester in the environment.




Note: The information you select will populate the **Device Type Information** section.

4. Complete the following steps to configure the connection:

Device Type Information

The following information is populated by the previous step:

DEVICE TYPE INFORMATION	
Vendor	F5 Networks
Resource Type	F5 ASM Audit
Collection Method	Regex [file]
Import Using	Console 

- Functionality:** Vendor name.
- Resource Type:** The **Resource Type** you specified.
- Collection Method:** Regex [file].
- Import Using:** Select **Console** or ID of Ingestion Node if using remote ingester in the environment.

Device Information

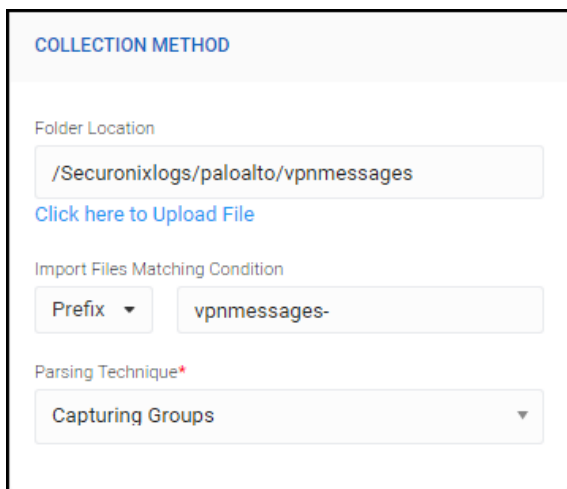
- Complete the following information:

DEVICE INFORMATION	
Datasource Name	
<input type="text" value="F5Audit_XON"/>	
IP Address	
<input type="text"/>	
Specify timezone for activity logs	
<input type="text" value="CST"/>	

- Datasource Name:** Specify a unique Datasource name.
- IP Address:** Not required.
- Specify timezone for activity logs:** Specify your time zone using dropdown.

Collection Method

2. Complete the following information:



The screenshot shows a web form titled "COLLECTION METHOD" with a light blue header. Below the header, there are three sections: "Folder Location" with a text input field containing "/Securionixlogs/paloalto/vpnmessages" and a blue link "Click here to Upload File"; "Import Files Matching Condition" with a "Prefix" dropdown menu and a text input field containing "vpnmessages-"; and "Parsing Technique*" with a dropdown menu showing "Capturing Groups".

a. **Folder Location:**

a. Specify the folder location of the file(s) you want to import.

OR

b. Click to upload file and browse for file on your local machine.

b. **Import Files Matching Condition:** Specify the prefix or postfix and supply a condition to upload multiple files. Example: Prefix vpnmessages_ will upload vpnmessages_1 through vpnmessages_50.

c. **Parsing Technique:** Capturing Groups.

More Settings

3. Complete the following information:

MORE SETTINGS

Action Taken On Unparsed Events

SAVE IN UNPROCESSED FOLDER ON HDFS

Success Folder

/Securonix/tenants/praful/snypr6/securonix_home/import/success/

Failed Folder

/Securonix/tenants/praful/snypr6/securonix_home/import/failed/

Specify staging folder (Only required for data requiring preprocessing)

/Securonix/tenants/praful/snypr6/securonix_home/import/in/

Enable Preprocessor

YES

Preprocessor Class

- a. **Action Taken on Unparsed Events:** Select from dropdown. The following options are available:
 - Save in unprocessed folder on HDFS
 - Drop Events
 - Ingest as unparsed events
- a. **Success Folder:** Specify the folder into which you would like the file to move upon successful upload. Default:/Securonix/ArcSight/uba6/securonix_home/import/success/
- b. **Failed Folder:** Specify the folder into which you would like the file to move upon a failed upload. Default:/Securonix/ArcSight/uba6/securonix_home/import/failed/
- c. **Staging Folder:** Specify the staging folder (required for data requiring preprocessing). Default:/Securonix/ArcSight/uba6/securonix_home/import/in/
- d. **Enable Preprocessor:** Toggle to **Yes** if you want to enable.
 - a. **Preprocessor Class** (optional): Enter a preprocessor class if Preprocessor is enabled.

4. **Preview Input** to ensure the data has uploaded successfully.

The screenshot shows the ArcSight 'PREVIEW INPUT' interface. On the left, there are two sections: 'RESOURCE INFORMATION' and 'DATASOURCE INFORMATION'. The 'RESOURCE INFORMATION' section includes fields for Vendor (Palo Alto Networks), Resource Type (Palo Alto VPN), and Collection Method (Regex [file]). The 'DATASOURCE INFORMATION' section includes fields for Datasource Name (Palo Alto VPN), IP Address, and a dropdown for Specify timezone for activity logs (set to CDT). The main area displays a list of log entries with timestamps and details. The entries are filtered by the date range Mar 23 10:12:17 to Mar 23 10:47:17. The log entries include details such as User name, Client OS version, and Client version.

5. Click **Save & Next** to proceed to [Step 2: Parsing and Normalization](#).

Importing Events from a Database

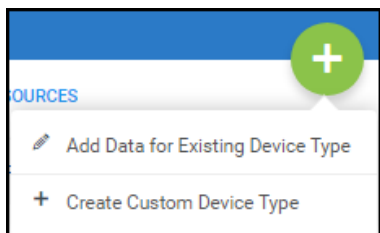
This section describes how to import data from a database such as MySQL, MSSQL, Oracle, Hive, or Impala.

To import activity data from a database, complete the following steps:

1. Navigate to **Menu > Add Data > Activity**.

The screenshot shows the ArcSight 'MENU' interface. The 'MENU' dropdown is open, showing a list of categories and sub-items. The 'ADD DATA' category is highlighted, and the 'Activity' sub-item is selected. The 'Activity' sub-item is highlighted with a blue bar. The 'Activity' sub-item is highlighted with a blue bar.

2. Click **+** to add a new datasource.

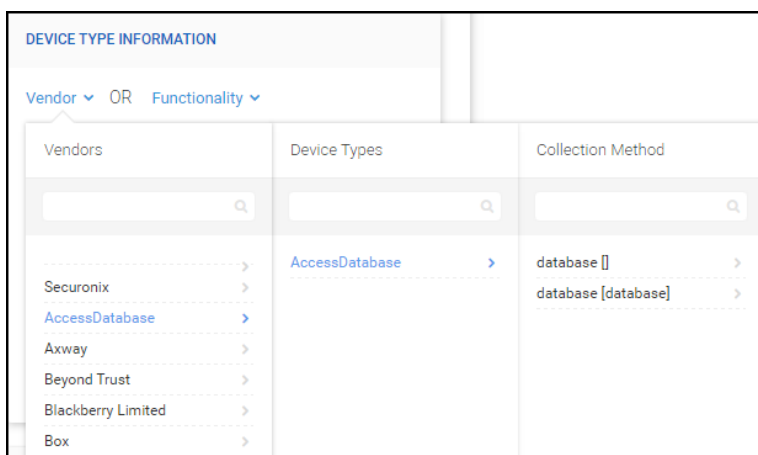


3. Select **Add Data for Existing Device Type** or **Create Custom Device Type** from the drop-down.



Note: You can search for **Existing Device Types** to find the specific vendor or functionality you are looking for. If you do not find the specific resource, select **Create Custom Device Type**.

- a. **Existing Device Type:** Select a **Vendor** or **Functionality**, **Device Type**, and **Collection Method**.



- b. **Custom Device Type:** Select **Duplicate Parser From** from Device Type Information drop-downs OR create a custom device to indicate how ArcSight UBA should parse the incoming data.

- **Duplicate Parser:** Select **Vendor** OR **Functionality**, **Resource Type**, and **Collection Method** from dropdowns to select the collection method from which to duplicate the parsing technique.
- **Custom:** Complete the following steps to create a custom device:
 1. Select **Create New Vendor** and enter Vendor name in the pop up window.
 2. Select **Functionality**, enter **Resource Type**, and select **Collection Method** from dropdown.
 3. Select **Import Using** Console or ID of Ingestion Node if using remote ingester in the environment.



Note: The information you select will populate the **Device Type Information** section.

4. Complete the following steps to configure the connection:

Device Type Information

The following information is populated by the previous step:

DEVICE TYPE INFORMATION

Vendor ▼ OR Functionality ▼

Functionality

Securonix

Resource Type

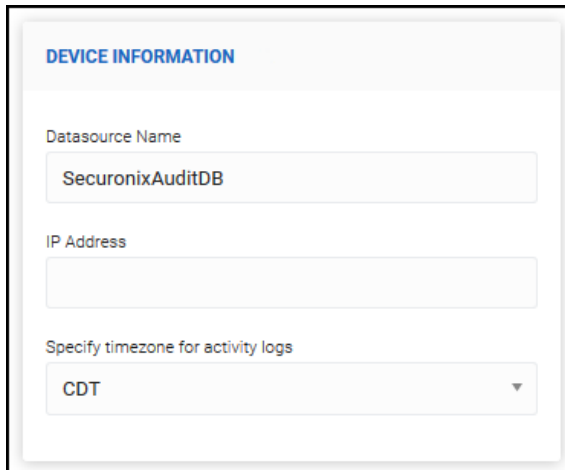
Collection Method

database [database]

- Functionality:** Vendor name. Example: Securonix.
- Resource Type:** The Resource Type you specified or left blank.
- Collection Method:** database [database]
- Select **Import Using** Console or ID of Ingestion Node if using remote ingester in the environment.

Device Information

1. Complete the following information:



The screenshot shows a form titled "DEVICE INFORMATION" with a light blue header. Below the header, there are three input fields. The first field is labeled "Datasource Name" and contains the text "SecuronixAuditDB". The second field is labeled "IP Address" and is empty. The third field is labeled "Specify timezone for activity logs" and is a dropdown menu with "CDT" selected. The form is enclosed in a black border.

- a. **Datasource Name:** Specify a unique Datasource name. Example: SecuronixAuditDB.
- b. **IP Address:** Not required.
- c. **Specify timezone for activity logs:** Specify your time zone using dropdown.

Collection Method

2. Complete the following information:

COLLECTION METHOD

Database Type

MySQL

JDBC URL

jdbc:mysql://10.0.0.60:3306/deltasnypr6

Driver Class

com.mysql.jdbc.Driver

Database Username

root

Database Password

••••••••

Query

```
select id,module, objectclass, objecttype,
objectkey,methodname, action, description, identifier,
logtime, remoteip,localip, status,message, updatedbyuser
from sysaudit
```

Incremental

☒ YES

Incremental

YES

Incremental Field

logtime

Select attribute to retrieve incremental events. The query sent to the database is appended with this field (Example: and logtime > \${logtime})

Type

Time

Select the data type for this field. Example: If the Incremental field is Date

Format

yyyy-MM-dd HH:mm:ss

Provide format for the field

Incremental Condition Created

where logtime > '\${logtime}'

Force Ascending Order

NO

Parsing Technique

Delimited Fields

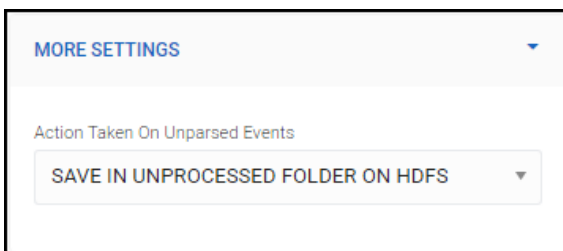
Delimiter

|

- a. **Database Type:** Select the database type from the dropdown. Example: MySQL.
- b. **JDBC URL:** Specify the JDBC URL. Example: jdbc:mysql://10.0.0.60:3306/deltasnypr6.
- c. **Driver Class:** Specify the driver class. Example: com.mysql.jdbc.Driver.
- d. **Database Username:** Specify the username. Example: root.
- e. **Database Password:** Specify the password.
- f. **Query:** Enter a query to extract information from the database. Example: `select id, -module, objectclass, objecttype, objectkey, methodname, action, description, identifier, logtime, remoteip, localip, status, message, updatedbyuser from sysaudit`
- g. **Incremental:** Toggle to **Yes** if you would like to retrieve incremental events.
 - a. **No:** Proceed to **Parsing Technique**.
 - b. **Yes:** Specify the following:
 - a. **Incremental Field:** Select an attribute to retrieve incremental events from dropdown. The query sent to the database is appended with this field. Example: logtime.
 - b. **Type:** Select the data type for the Incremental Field from the dropdown. Example: Time.
 - c. **Format:** Specify the date/time format, if required.
 - d. **Incremental Condition Created:** This field will auto-populate based on the information entered in the previous steps. Example: where logtime > '\${logtime}'
 - e. **Force Ascending Order:** Toggle to **Yes** if you would like to force ascending order.
 - f. **Parsing Technique:** Delimited Fields.
 - g. **Delimiter:** | (pipe).

More Settings

3. Complete the following information:



MORE SETTINGS ▼

Action Taken On Unparsed Events

SAVE IN UNPROCESSED FOLDER ON HDFS ▼

a. **Action Taken on Unparsed Events:** Select from dropdown. The following options are available:

- Save in unprocessed folder on HDFS
- Drop Events
- Ingest as unparsed events

4. **Preview Input** to ensure the data has uploaded successfully.

Import activities from files, applications, databases, security products, network devices & other sources.

+

BACK TO DATASOURCES

DEVICE TYPE INFORMATION

Vendor ▼ OR Functionality ▼

Functionality

Securix

Resource Type

Collection Method

database [database]

DEVICE INFORMATION

Data source Name

SecurixAudrDB

IP Address

Specify timezone for activity logs

CDT

PREVIEW INPUT

GET PREVIEW

OR

Add Sample Lines

1	SCHEDULER	GROUP_SYSTEM	QuartzJob	-1	DeleteExpiredEventsJob	TRIGGERED	Job Invoked - DEE Job	System	201
2	LOGIN_CONTROLLER	LOGINCONTROLLER	N/A	-1	N/A	LOGIN	Successful Login	admin	201
3	LOGOUT_CONTROLLER	LOGOUTCONTROLLER	N/A	-1	N/A	LOGOUT	Successful Logout	admin	201
4	LOGIN_CONTROLLER	LOGINCONTROLLER	N/A	-1	N/A	LOGIN	Successful Login	admin	201
5	SCHEDULER	GROUP_SYSTEM	QuartzJob	-1	GraphTrendDetailsJob	TRIGGERED	Job Invoked - GraphTrendDetailsJob	System	201
6	SCHEDULER	GROUP_SYSTEM	QuartzJob	-1	DeleteExpiredEventsJob	TRIGGERED	Job Invoked - DEE Job	System	201
7	LOGIN_CONTROLLER	LOGINCONTROLLER	N/A	-1	N/A	LOGIN	Successful Login	admin	201
8	SCHEDULER	GR_USER_IMPORT	QuartzJob	-1	UserImportJob	TRIGGERED	Job Invoked - User_Database_DATABASE_2017_03_23_20_40_42	admin	201
9	SCHEDULER	GR_USER_IMPORT	QuartzJob	-1	UserImportJob	TRIGGERED	Job Invoked - User_Database_DATABASE_2017_03_23_20_43_09	admin	201
10	SCHEDULER	GR_USER_IMPORT	QuartzJob	-1	UserImportJob	TRIGGERED	Job Invoked - User_HRFile_FILE_2017_03_23_20_54_04	admin	201
11	SCHEDULER	GROUP_SYSTEM	QuartzJob	-1	GraphTrendDetailsJob	TRIGGERED	Job Invoked - GraphTrendDetailsJob	System	201
12	SCHEDULER	GR_USER_IMPORT	QuartzJob	-1	UserImportJob	TRIGGERED	Job Invoked - User_TerminationData_FILE_2017_03_23_21_00_20	admin	201
13	PEER_CONTROLLER	PEERCONTROLLER	N/A	-1	N/A	IMPORTED	Peer Creation/Assignment Rules Job	admin	201
14	SCHEDULER	GROUP_PEER_GENERATION	QuartzJob	-1	PeerGenerationJob	TRIGGERED	Job Invoked - PeerCreationRule_1490320039654	admin	201
15	PEER_CONTROLLER	PEERCONTROLLER	N/A	-1	N/A	IMPORTED	Peer Creation/Assignment Rules Job	admin	201

5. Click **Save & Next** to proceed to [Step 2: Parsing and Normalization](#).

Importing Events from Apache Subversion (SVN)

This section describes how to import data from Apache Subversion (SVN) using a premium connector.

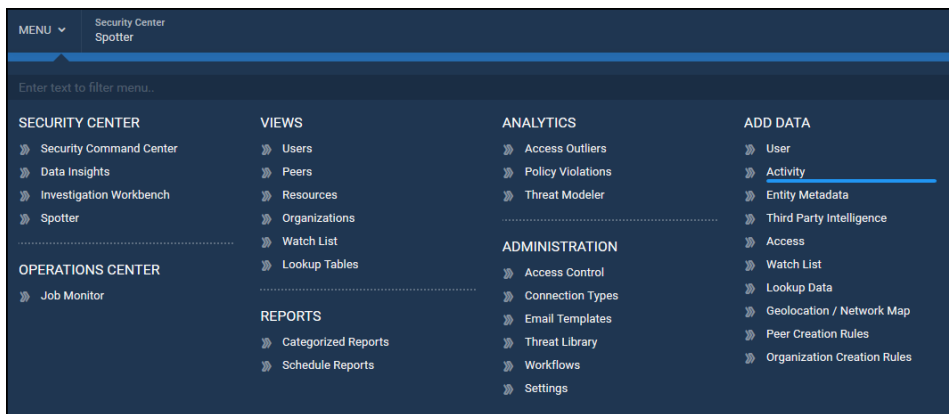
Prerequisites for Importing Events from SVN

Ensure you have the following information prior to setting up the connection:

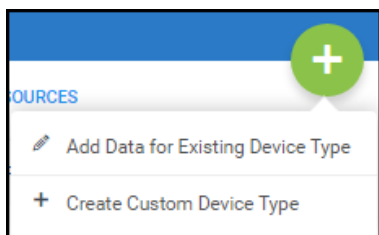
- **SVN URL:** The URL of the server to which you want to connect.
- **SVN Username:** The username for a user authorized to connect to SVN.
- **SVN Password:** The password for the authorized user account.
- **Start Revision:** The revision number from which you want to begin importing events.

To import events from SVN, complete the following steps:

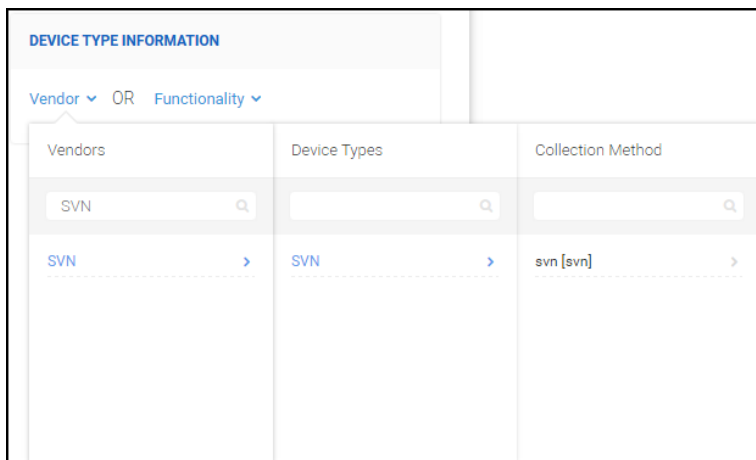
1. Navigate to **Menu > Add Data > Activity**.



2. Click **+** to add a new datasource.



3. Select **Add Data for Existing Device Type**.
4. **Click Vendor** and select the following:



- **Vendors:** SVN.
- **Device Types:** SVN.
- **Collection Method:** svn [svn].



Note: The information you select will populate the Device Type Information section.

5. Complete the following steps to configure the connection:

Device Type Information

The following information is populated by the previous step:

DEVICE TYPE INFORMATION

Vendor ▾ OR Functionality ▾

Vendor

SVN

Resource Type

SVN

Collection Method

svn [svn]

- a. **Vendor:** SVN.
- b. **Resource Type:** SVN.
- c. **Collection Method:** svn [svn].
- d. **Import Using:** **Console** or ID of Ingestion Node.

Device Information

1. Complete the following information:

DEVICE INFORMATION

Datasource Name

Securonix SVN

IP Address

Specify timezone for activity logs

CDT ▼

- a. **Datasource Name:** Provide a unique name. Example: Securonix SVN.
- b. **IP Address:** Not required.
- c. **Specify timezone for activity logs:** Specify your time zone using dropdown.

Collection Method

2. Complete the following information:

COLLECTION METHOD

SVN Url

svn://profiler.servebbs.com/profilerSVN

SVN Username

pilam

SVN Password

.....

Start Revision

0

Parsing Technique

Delimited Fields

Delimiter

|

- SVN URL:** Specify the URL for the server to which you want to connect. Example: svn://-profiler.servebbs.com/profilerSVN.
- SVN Username:** Specify the authorized user name.
- SVN Password:** Specify the authorized user's password.
- Start Revision:** Specify the revision number at which you want to begin importing events. Default 0.
- Parsing Technique:** Delimited Fields.
- Delimiter:** Specify a delimiter. Example | (pipe).

More Settings

2. Complete the following information:

MORE SETTINGS

Action Taken On Unparsed Events

SAVE IN UNPROCESSED FOLDER ON HDFS

a. **Action Taken on Unparsed Events:** Select from dropdown. The following options are available:

- Save in unprocessed folder on HDFS
- Drop Events
- Ingest as unparsed events

4. **Preview Input** to ensure the file has uploaded successfully.

PREVIEW INPUT

GET PREVIEW OR Add Sample Lines

Revision	Author	Time	Message	Type	Path	CopyPath	CopyRevision
1	lgu	Sun Mar 07 21:37:01 CST 2010	"Tuhits code"	A	/testsrc/hbproject		
1	lgu	Sun Mar 07 21:37:01 CST 2010	"Tuhits code"	A	/testsrc/src/testsrc/Main.java		
1	lgu	Sun Mar 07 21:37:01 CST 2010	"Tuhits code"	A	/testsrc/build.xml		
1	lgu	Sun Mar 07 21:37:01 CST 2010	"Tuhits code"	A	/testsrc/manifest.mf		
1	lgu	Sun Mar 07 21:37:01 CST 2010	"Tuhits code"	A	/testsrc/hbproject/project.xml		
1	lgu	Sun Mar 07 21:37:01 CST 2010	"Tuhits code"	A	/testsrc/test		
1	lgu	Sun Mar 07 21:37:01 CST 2010	"Tuhits code"	A	/testsrc/hbproject/build-impl.xml		
1	lgu	Sun Mar 07 21:37:01 CST 2010	"Tuhits code"	A	/testsrc/hbproject/project.properties		
1	lgu	Sun Mar 07 21:37:01 CST 2010	"Tuhits code"	A	/testsrc/src/testsrc		
1	lgu	Sun Mar 07 21:37:01 CST 2010	"Tuhits code"	A	/testsrc		
1	lgu	Sun Mar 07 21:37:01 CST 2010	"Tuhits code"	A	/testsrc/hbproject/genfiles.properties		
1	lgu	Sun Mar 07 21:37:01 CST 2010	"Tuhits code"	A	/testsrc/src		
2	arjan	Sun Mar 07 21:41:10 CST 2010	"initial import"	A	/trunk		
2	arjan	Sun Mar 07 21:41:10 CST 2010	"initial import"	A	/tags		
2	arjan	Sun Mar 07 21:41:10 CST 2010	"initial import"	A	/branches		

RESOURCE INFORMATION

Vendor OR Functionality

Vendor

SVN

Resource Type

SVN

Collection Method

svn [svn]

DATASOURCE INFORMATION

Datasource Name

Securix SVN

IP Address

Specify timezone for activity logs

CDT

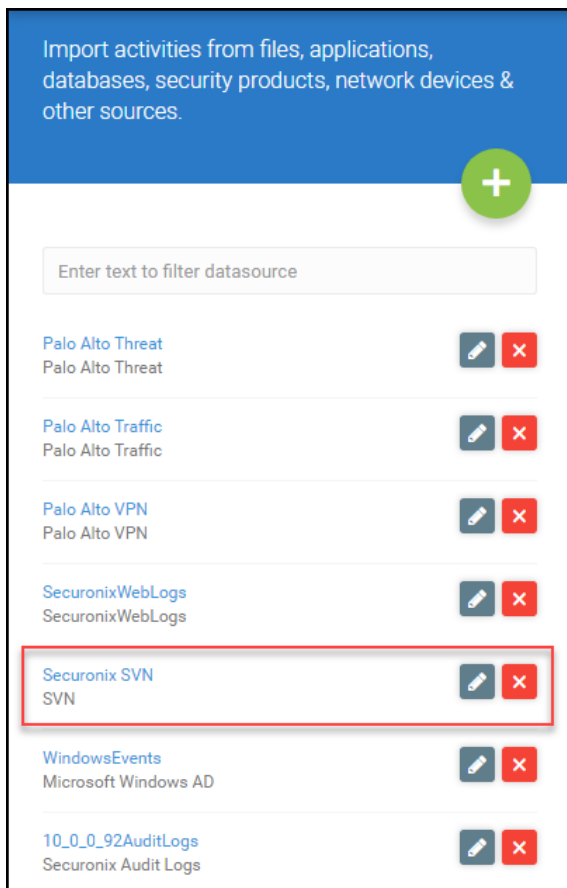
ADD A NEW ACTION METHOD

4. Click **Save & Next** to proceed to [Step 5: Reviewing Import Summary](#).

Editing the Connection

To edit the existing Google connection, navigate to **Menu > Add Data > Activity** and complete the following steps:

1. Locate the datasource.



2. Click and proceed to any of the following steps to edit the information:

- [Step 2: Parsing and Normalization](#)
- [Step 3: Performing Conditional Actions](#)
- [Step 4: Configuring Identity Attribution](#)

OR



3. Click to delete the datasource.

Importing Events from Google Reporting API

This section describes how to import data from a Google data source using a premium connector.

Prerequisites for Importing Events from Google

ArcSight UBA uses open authentication (OAuth) to connect to Google to import data. Ensure you have the following information prior to setting up the connection:

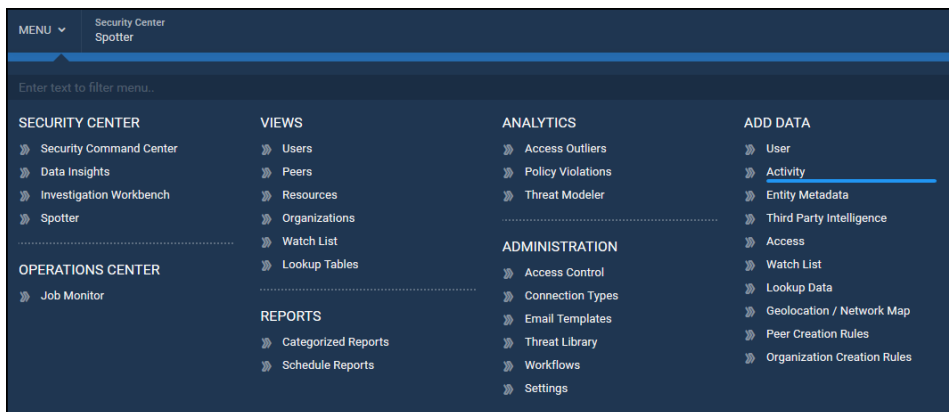
- **Project:** The project that holds ArcSight UBA related information to connect to Google.
- **Service account email:** The service account email that is used to provision the project.
- **Admin user email:** The email account of the administrative user for the service account.
- **Domain:** The domain from where the data is to be imported.
- **Private Key File:** The private key file required for OAuth connection to the Google API



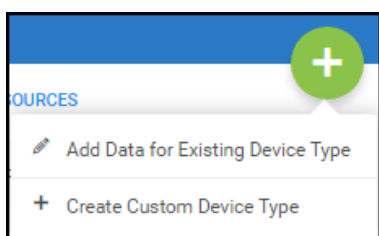
Note: For information about Google Service accounts, see Securonix Google API Configuration.

To import events from Google, complete the following steps:

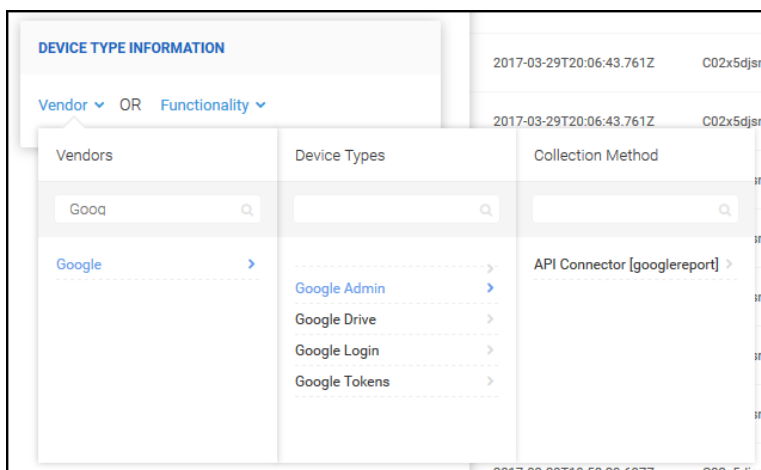
1. Navigate to **Menu > Add Data > Activity**.



2. Click **+** to add a new datasource.



3. Select **Add Data for Existing Device Type**.
4. **Click Vendor** and select the following:



- **Vendors:** Google
- **Device Types:** Google Admin
- **Collection Method:** API Connector [googlereport]
- **Import Using:** **Console** or ID of Ingestion Node.



Note: The information you select will populate the Device Type Information section.

5. Complete the following steps to configure the connection:

Device Type Information

The following information is populated by the previous step:

DEVICE TYPE INFORMATION	
Vendor	Google
Resource Type	Google Admin
Collection Method	Delimited-pipe [file]

- Functionality:** Google.
- Resource Type:** Google Admin.
- Collection Method:** [googlereport]
- Import Using:** Select **Console** or ID of Ingestion Node if using remote ingester in the environment.

Device Information

1. Complete the following information:

DEVICE INFORMATION	
Datasource Name	<input type="text" value="Google Admin"/>
IP Address	<input type="text"/>
Specify timezone for activity logs	<input type="text" value="CDT"/>

- a. **Datasource Name:** GoogleAdmin
- b. **IP Address:** Not required.
- c. **Specify timezone for activity logs:** Specify your time zone using dropdown.

Collection Method

2. Complete the following information:

COLLECTION METHOD

Project

GoogleApps

Service Account Email

777450131@developer.qserviceaccount.com

Admin User Email

smal@secu.com

Private Key File (.p12 file)

`${SECURONIX_HOME}/conf/google/GoogleApps-0f`

Please make sure that file is present at /Securonix/tenants/your/snypr6/securonix_home/conf/google/

Application Name

drive

Parsing Technique

Delimited Fields

Delimiter

|

- a. **Project:** Specify the project name. Example: GoogleApps.
- b. **Service Account Email:** Specify the Service Account Email.
- c. **Admin User Email:** Specify the admin user's email address.
- d. **Private Key File (.p12 file):** Specify the private key file in .p12 format.



Note: Ensure the file is present in /Securonix/tenants/four/snypr6/securonix_home/-conf/google.

- e. **Application Name:** Specify the application name. Example: drive.
- f. **Parsing Technique:** Delimited Fields.
- g. **Delimiter:** Specify a delimiter. Example | (pipe).

More Settings

3. Complete the following information:

MORE SETTINGS

Action Taken On Unparsed Events

SAVE IN UNPROCESSED FOLDER ON HDFS

Success Folder

/Securonix/tenants/partnerdemo
/securonix_home/import/success/

Failed Folder

/Securonix/tenants/partnerdemo
/securonix_home/import/failed/

Specify staging folder (Only required for data requiring preprocessing)

/Securonix/tenants/partnerdemo
/securonix_home/import/in/

Enable Preprocessor

YES

Preprocessor Class

- a. **Action Taken on Unparsed Events:** Select from dropdown. The following options are available:
 - Save in unprocessed folder on HDFS
 - Drop Events
 - Ingest as unparsed events

- b. **Success Folder:** Specify the folder into which you would like the file to move upon successful upload. Default: /Securonix/ArcSight/uba6/securonix_home/import/success/
 - c. **Failed Folder:** Specify the folder into which you would like the file to move upon a failed upload. Default: /Securonix/ArcSight/uba6/securonix_home/import/failed/
 - d. **Staging Folder:** Specify the staging folder (required for data requiring preprocessing). Default: /Securonix/ArcSight/uba6/securonix_home/import/in/
 - e. **Enable Preprocessor:** Toggle to **Yes** if you want to enable.
 - a. **Preprocessor Class** (optional): Enter a preprocessor class if Preprocessor is enabled.
3. **Preview Input** to ensure the file has uploaded successfully.

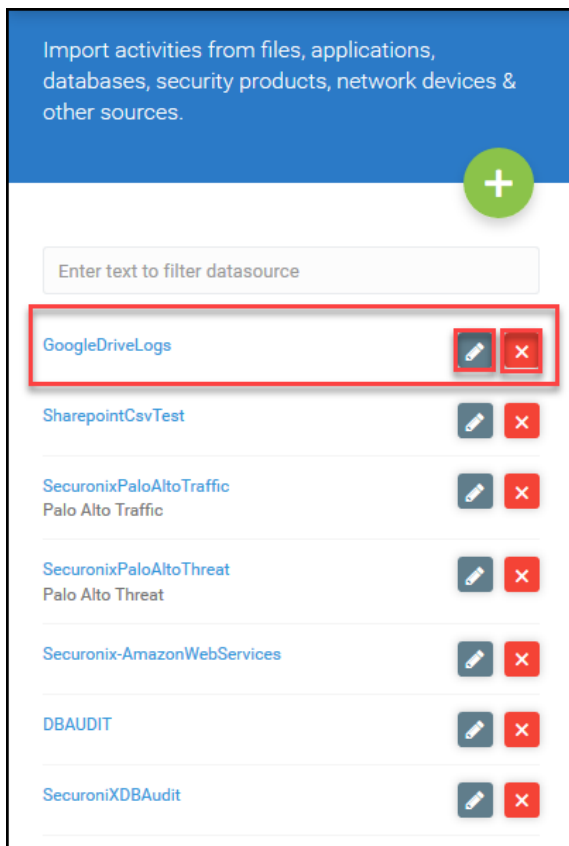
Resource Type Information									
PREVIEW INPUT									
time	customerid	applicationName	uniqueQualifier	kind	etag	ownerDomain	ipAddress	email	
2017-03-28T19:52:26.015Z	C02x5dgm	drive	129777065963668692	admin#reports#activity	"DbspNbnLzQPWbSpGf2-ZaFu0-KbxV3EK-3EaIQpOZ3hVjmk"			pchatu	
2017-03-28T19:52:26.015Z	C02x5dgm	drive	129777065963668692	admin#reports#activity	"DbspNbnLzQPWbSpGf2-ZaFu0-KbxV3EK-3EaIQpOZ3hVjmk"			pchatu	
2017-03-28T19:52:26.015Z	C02x5dgm	drive	129777065963668692	admin#reports#activity	"DbspNbnLzQPWbSpGf2-ZaFu0-KbxV3EK-3EaIQpOZ3hVjmk"			pchatu	
2017-03-28T19:52:26.015Z	C02x5dgm	drive	129777065963668692	admin#reports#activity	"DbspNbnLzQPWbSpGf2-ZaFu0-KbxV3EK-3EaIQpOZ3hVjmk"			pchatu	
2017-03-28T19:52:26.015Z	C02x5dgm	drive	129777065963668692	admin#reports#activity	"DbspNbnLzQPWbSpGf2-ZaFu0-KbxV3EK-3EaIQpOZ3hVjmk"			pchatu	
2017-03-28T19:52:06.919Z	C02x5dgm	drive	-708044380847930236	admin#reports#activity	"DbspNbnLzQPWbSpGf2-ZaFu0-7AD1pWzgrfGkSpLmdqWYUQ6v"		2601.86.101.3e1d71ca.eebb.9218.d66	pchatu	
2017-03-28T19:51:56.621Z	C02x5dgm	drive	-4664204866847494189	admin#reports#activity	"DbspNbnLzQPWbSpGf2-ZaFu0-UJbJ231aaefwPFd5vB7-7Dv0"			pchatu	
2017-03-28T19:51:53.768Z	C02x5dgm	drive	-3022506215576853418	admin#reports#activity	"DbspNbnLzQPWbSpGf2-ZaFu0-1-y2uPdp11CDFFcsOH6vV99dM"			pchatu	
2017-03-28T19:51:53.768Z	C02x5dgm	drive	-3022506215576853418	admin#reports#activity	"DbspNbnLzQPWbSpGf2-ZaFu0-1-y2uPdp11CDFFcsOH6vV99dM"			pchatu	
2017-03-28T19:51:53.768Z	C02x5dgm	drive	-3022506215576853418	admin#reports#activity	"DbspNbnLzQPWbSpGf2-ZaFu0-1-y2uPdp11CDFFcsOH6vV99dM"			pchatu	
2017-03-28T19:51:53.768Z	C02x5dgm	drive	-3022506215576853418	admin#reports#activity	"DbspNbnLzQPWbSpGf2-ZaFu0-1-y2uPdp11CDFFcsOH6vV99dM"			pchatu	
2017-03-28T19:51:53.768Z	C02x5dgm	drive	-3022506215576853418	admin#reports#activity	"DbspNbnLzQPWbSpGf2-ZaFu0-1-y2uPdp11CDFFcsOH6vV99dM"			pchatu	
2017-03-28T19:51:53.768Z	C02x5dgm	drive	-3022506215576853418	admin#reports#activity	"DbspNbnLzQPWbSpGf2-ZaFu0-1-y2uPdp11CDFFcsOH6vV99dM"			pchatu	
2017-03-28T19:51:53.768Z	C02x5dgm	drive	-3022506215576853418	admin#reports#activity	"DbspNbnLzQPWbSpGf2-ZaFu0-1-y2uPdp11CDFFcsOH6vV99dM"			pchatu	

4. Click **Save & Next** to proceed to [Step 5: Reviewing Import Summary](#).

Editing the Connection

To edit the existing Google connection, navigate to **Menu > Add Data > Activity** and complete the following steps:

1. Locate the datasource.



2. Click  and proceed to any of the following steps to edit the information:

- [Step 2: Parsing and Normalization](#)
- [Step 3: Performing Conditional Actions](#)
- [Step 4: Configuring Identity Attribution](#)

OR



3. Click  to delete the datasource.

Importing Events from Office 365

This section describes how to import data from Office365 using a premium connector.

Prerequisites for Importing Events from Office 365

ArcSight UBA uses authentication from Azure AD to connect to the Office 365 Management API to import data from Office 365. Ensure you have the following information prior to setting up the connection:

- **Tenant ID:** The unique global identifier for the Office 365 account.



Note: This is different than your tenant name or domain.

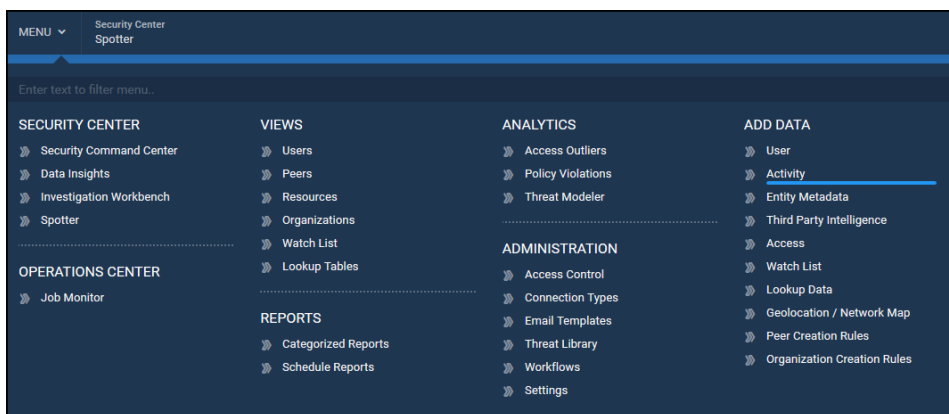
- **Key (Client Secret):** The access token generated by Azure AD.
- **Code:** The authorization code used to request the client secret key.
- **Client ID:** A value automatically generated by Azure AD when requesting consent from tenant admins to use Office 365 Management API to connect.



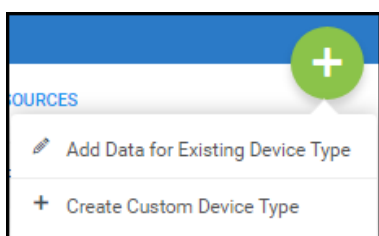
Note: For information about Office 365 accounts, visit your Office 365 Azure Management portal.

To import events from Office365, complete the following steps:

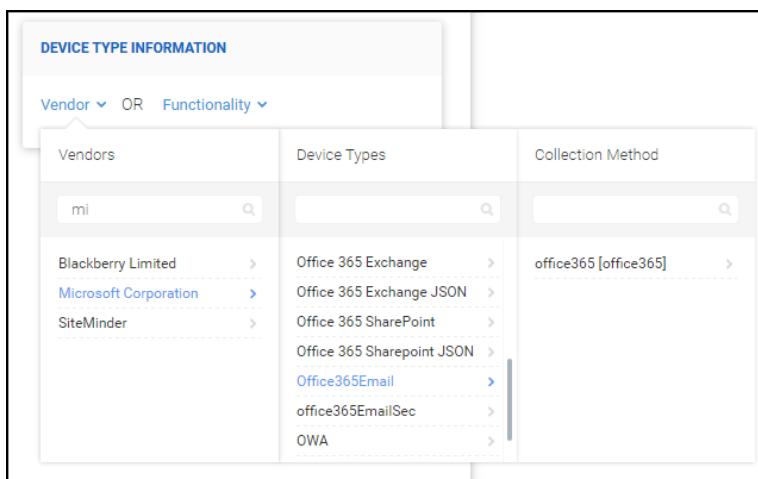
1. Navigate to **Menu > Add Data > Activity**.



2. Click **+** to add a new datasource.



3. Select **Add Data for Existing Device Type**.
4. **Click Vendor** and select the following:



- **Vendors:** Microsoft Corporation.
- **Device Types:** Select an available device type. Example: Office365Email.
- **Collection Method:** Select from the options generated by the device type. Example: office365 [office365].
- **Import Using:** Select **Console** or ID of Ingestion Node if using remote ingester in the environment.



Note: The information you select will populate the Device Type Information section.

5. Complete the following steps to configure the connection:

Device Type Information

The following information is populated by the previous step:

DEVICE TYPE INFORMATION

Vendor ▼ OR Functionality ▼

Vendor

Microsoft Corporation

Resource Type

office365EmailSec

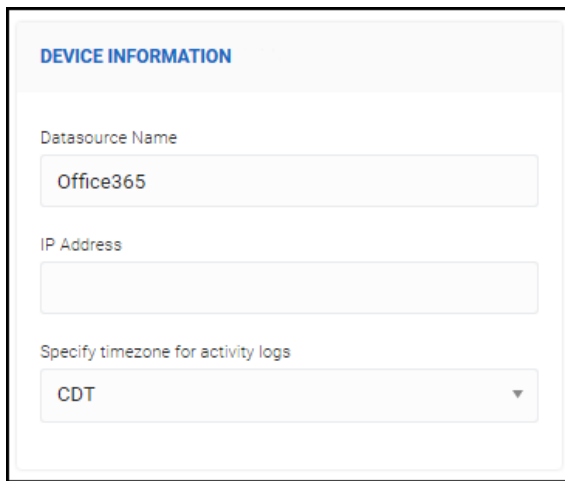
Collection Method

office365 [office365]

- Functionality:** Microsoft Corporation.
- Resource Type:** Office365EmailSec.
- Collection Method:** office365 [office365].
- Import Using:** Select **Console** or ID of Ingestion Node if using remote ingester in the environment.

Device Information

- Complete the following information:

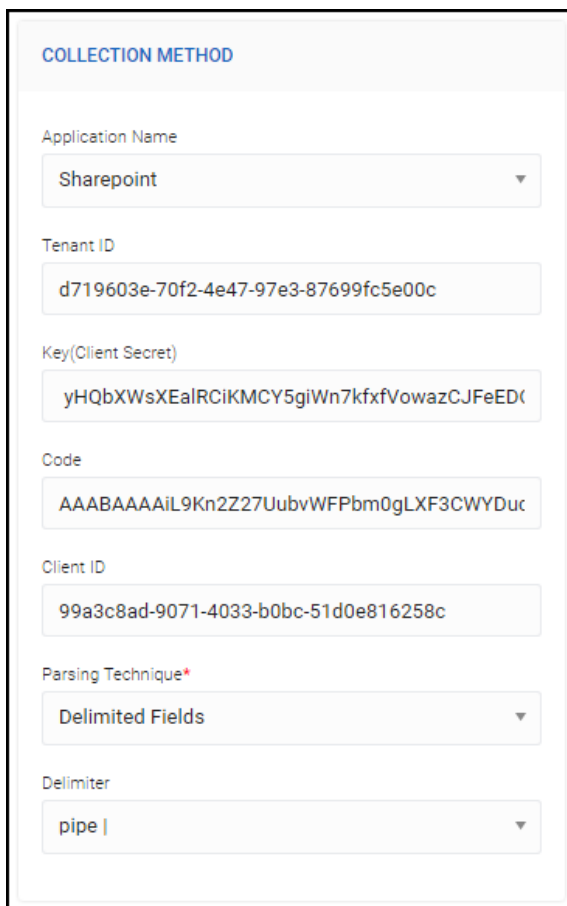


The screenshot shows a configuration form titled "DEVICE INFORMATION" in a light blue header. Below the header, there are three input fields. The first field, labeled "Datasource Name", contains the text "Office365". The second field, labeled "IP Address", is empty. The third field, labeled "Specify timezone for activity logs", is a dropdown menu with "CDT" selected and a downward arrow on the right.

- a. **Datasource Name:** Office365.
- b. **IP Address:** Not required.
- c. **Specify timezone for activity logs:** Specify your time zone using dropdown.

Collection Method

2. Complete the following information:



COLLECTION METHOD

Application Name
Sharepoint ▼

Tenant ID
d719603e-70f2-4e47-97e3-87699fc5e00c

Key (Client Secret)
yHQbXWsXEalRCiKMCY5giWn7kxfVowazCJFeEDC

Code
AAABAAAiL9Kn2Z27UubvWFPbm0gLXF3CWYDuc

Client ID
99a3c8ad-9071-4033-b0bc-51d0e816258c

Parsing Technique*
Delimited Fields ▼

Delimiter
pipe | ▼

- Application Name:** Select the Office 365 application from the dropdown. Example: Sharepoint.
- Tenant ID:** Specify the tenant ID.
- Key (Client Secret):** Specify the access token generated by Azure AD.
- Code:** Specify the authorization code generated by Azure AD.
- Client ID:** Specify the client ID value generated by Azure AD.
- Parsing Technique:** Delimited Fields.
- Delimiter:** Specify a delimiter. Example | (pipe).

More Settings

3. Complete the following information:

MORE SETTINGS

Action Taken On Unparsed Events
SAVE IN UNPROCESSED FOLDER ON HDFS

Success Folder
/Securonix/tenants/partnerdemo
/securonix_home/import/success/

Failed Folder
/Securonix/tenants/partnerdemo
/securonix_home/import/failed/

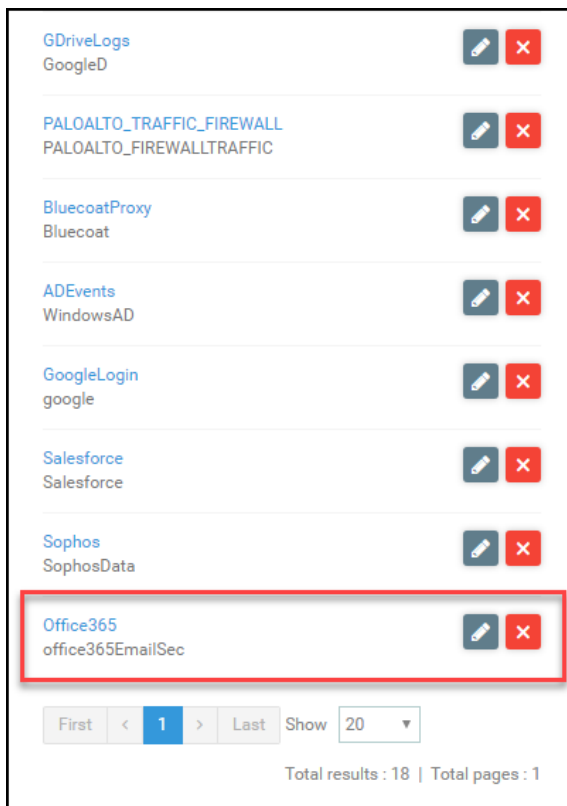
Specify staging folder (Only required for data requiring preprocessing)
/Securonix/tenants/partnerdemo
/securonix_home/import/in/

Enable Preprocessor
YES

Preprocessor Class

- a. **Action Taken on Unparsed Events:** Select from dropdown. The following options are available:
 - Save in unprocessed folder on HDFS
 - Drop Events
 - Ingest as unparsed events
 - a. **Success Folder:** Specify the folder into which you would like the file to move upon successful upload. Default: /Securonix/ArcSight/uba6/securonix_home/import/success/
 - b. **Failed Folder:** Specify the folder into which you would like the file to move upon a failed upload. Default: /Securonix/ArcSight/uba6/securonix_home/import/failed/
 - c. **Staging Folder:** Specify the staging folder (required for data requiring preprocessing). Default: /Securonix/ArcSight/uba6/securonix_home/import/in/
 - d. **Enable Preprocessor:** Toggle to **Yes** if you want to enable.
 - a. **Preprocessor Class** (optional): Enter a preprocessor class if Preprocessor is enabled.
4. **Preview Input** to ensure the file has uploaded successfully.

1. Locate the data source.



2. Click  and proceed to any of the following steps to edit the information:

- [Step 2: Parsing and Normalization](#)
- [Step 3: Performing Conditional Actions](#)
- [Step 4: Configuring Identity Attribution](#)

OR



3. Click  to delete the datasource.

Importing Events from Box

This section describes how to import data from a Google data source using a premium connector.

Prerequisites for Importing Events from Box

ArcSight UBA uses open authentication (OAuth) to connect to Box to import data. Ensure you have the following information prior to setting up the connection:

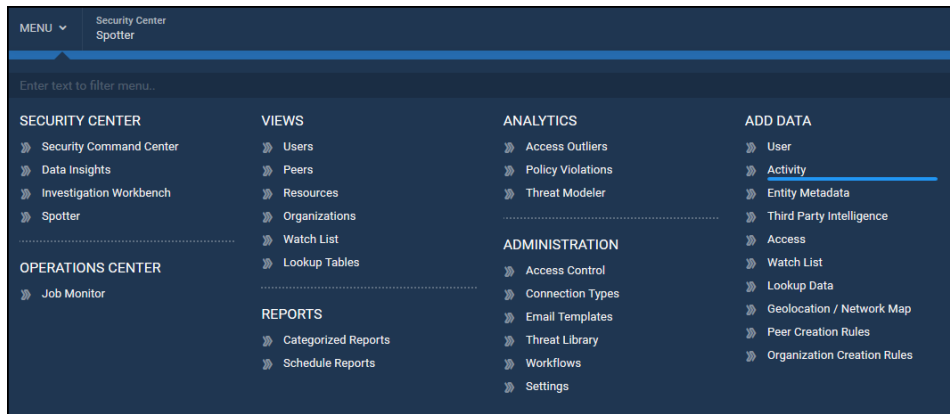
- **Client Key:** The Client ID OAuth 2.0 credential from your Box App.
- **Secret Key:** The Client Secret OAuth 2.0 credential from your Box App.



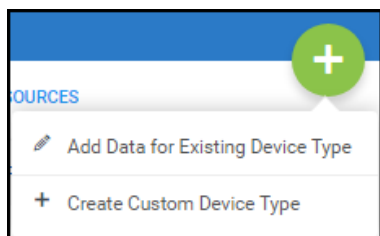
Note: For information about Box Apps, see Box API Configuration.

To import events from Box, complete the following steps:

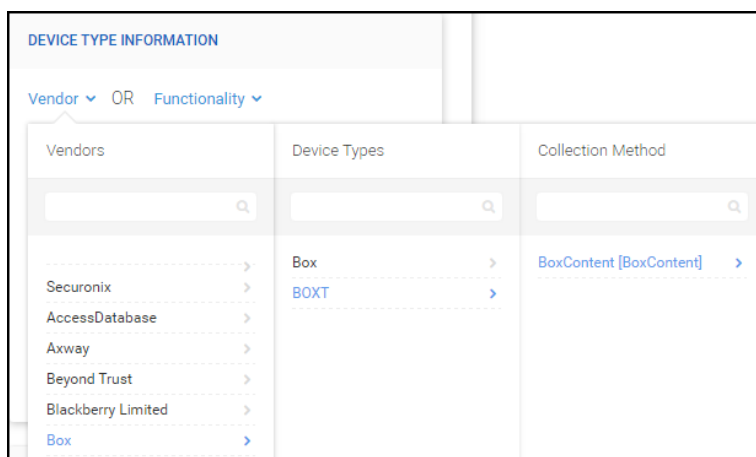
1. Navigate to **Menu > Add Data > Activity**.



2. Click **+** to add a new datasource.



3. Select **Add Data for Existing Device Type**.
4. **Click Vendor** and select the following:



- **Vendors:** Box.
- **Device Types:** BoxT.
- **Collection Method:** BoxContent [BoxContent].
- **Import Using:** Select **Console** or ID of Ingestion Node if using remote ingester in the environment.



Note: The information you select will populate the Device Type Information section.

5. Complete the following steps to configure the connection:

Device Type Information

The following information is populated by the previous step:

DEVICE TYPE INFORMATION

Vendor ▼ OR Functionality ▼

Vendor

Box

Resource Type

BOXT

Collection Method

BoxContent [BoxContent]

- Vendor:** Box.
- Resource Type:** BOXT.
- Collection Method:** BoxContent[BoxContent]
- Import Using:** Select **Console** or ID of Ingestion Node if using remote ingester in the environment.

Device Information

1. Complete the following information:

DEVICE INFORMATION

Datasource Name

BOX

IP Address

Specify timezone for activity logs

CDT ▼

- a. **Datasource Name:** Box.
- b. **IP Address:** Not required.
- c. **Specify timezone for activity logs:** Specify your time zone using dropdown.

Collection Method

2. Complete the following information:

COLLECTION METHOD

Key

87ozlr7x2wt5aii09gjdnhh3ogc55us5

The Key you got from Box Initial Step(Create account at Box)

Secret

tPuFx5MdP6H89TQK9ZLLGFz1TF8yS0TP

The Secret you got from Box Initial Step(Create account at Box)

GENERATE TOKENS

POPULATE TOKENS

Access Token

t6zHOelMqBKN2Hrv4WzCC6AlHgQfYIrV

Refresh Token

YPPGost5xJmvNWYPVn54QNLVzuf7AfE2x8

Parsing Technique

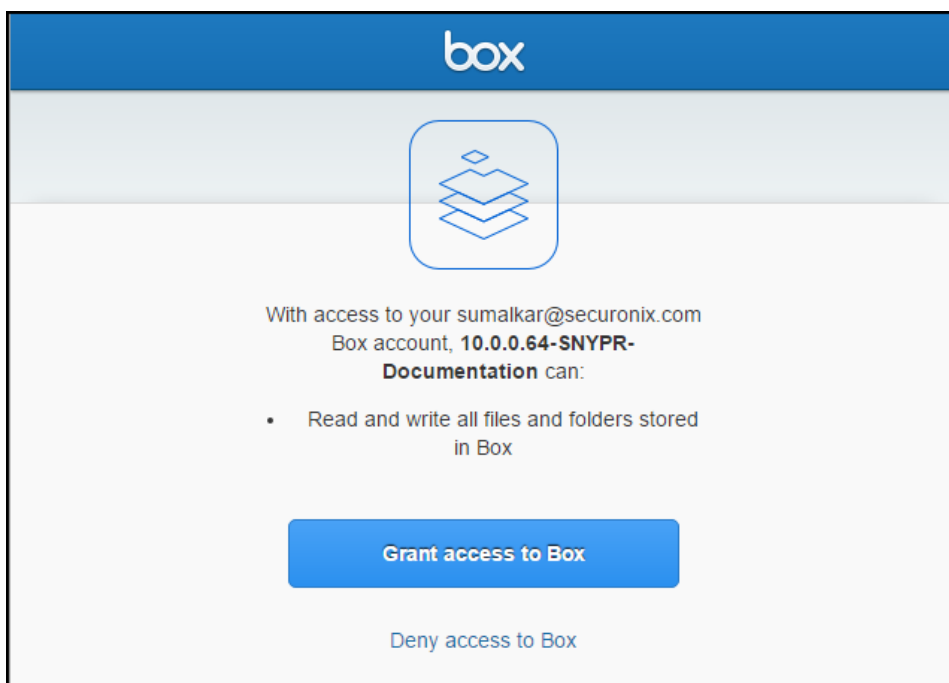
Key Value Pair

- a. **Key:** Enter Client ID from Box App.
 - b. **Secret:** Enter Client Secret from Box App.
3. Click **Generate Tokens**.
The Box log in screen will appear as a pop up window.



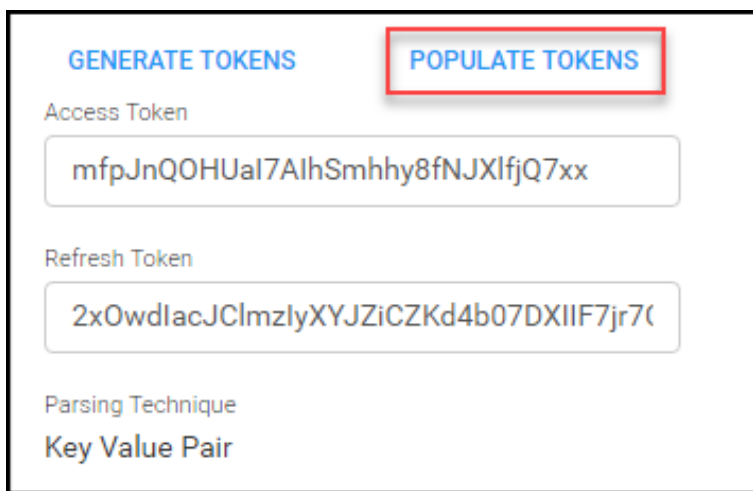
Note: If the window does not appear, check your browser for blocked pop ups.

4. Enter credentials to **Log in to grant access to Box**.
5. Click **Authorize**.
6. Click **Grant access to Box**.



Box will generate Access and Refresh tokens.

7. Click **Populate Tokens** in the ArcSight UBA Activity Import window.



8. Click **Close this window** in the Box window.


Access and refresh tokens have been generated. Click on the "Populate Tokens" button in parent window. [Close this window.](#)




Note: The **Parsing Technique** will auto-populate for Key Value Pair.

More Settings


9. Complete the following information:

MORE SETTINGS 


Action Taken On Unparsed Events

SAVE IN UNPROCESSED FOLDER ON HDFS 


Success Folder

/Securonix/tenants/partnerdemo
/securonix_home/import/success/ 

Failed Folder

/Securonix/tenants/partnerdemo
/securonix_home/import/failed/ 

Specify staging folder (Only required for data requiring preprocessing)

/Securonix/tenants/partnerdemo
/securonix_home/import/in/ 

Enable Preprocessor

YES ☒

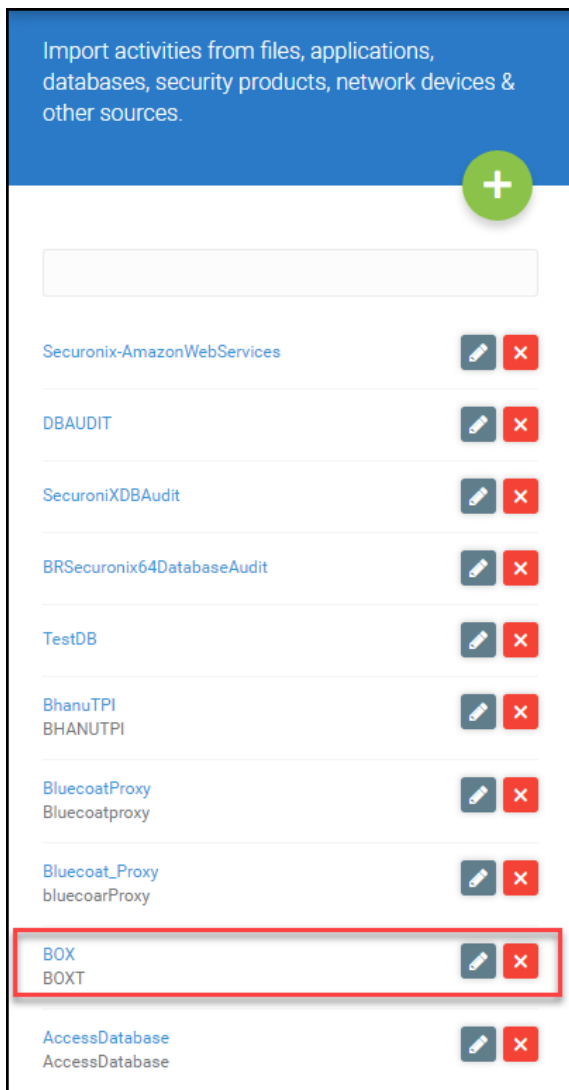
Preprocessor Class

- a. **Action Taken on Unparsed Events:** Select from dropdown. The following options are available:
 - Save in unprocessed folder on HDFS
 - Drop Events
 - Ingest as unparsed events
 - a. **Success Folder:** Specify the folder into which you would like the file to move upon successful upload. Default: /Securonix/ArcSight/uba6/securonix_home/import/success/
 - b. **Failed Folder:** Specify the folder into which you would like the file to move upon a failed upload. Default: /Securonix/ArcSight/uba6/securonix_home/import/failed/
 - c. **Staging Folder:** Specify the staging folder (required for data requiring preprocessing). Default: /Securonix/ArcSight/uba6/securonix_home/import/in/
 - d. **Enable Preprocessor:** Toggle to **Yes** if you want to enable.
 - a. **Preprocessor Class** (optional): Enter a preprocessor class if Preprocessor is enabled.
10. **Preview Input** to ensure the file has uploaded successfully.
11. Click **Save & Next** to proceed to [Step 5: Reviewing Import Summary](#).

Editing the Connection

To edit the existing Google connection, navigate to **Menu > Add Data > Activity** and complete the following steps:

1. Locate the datasource.



2. Click  and proceed to any of the following steps to edit the information:

- [Step 2: Parsing and Normalization](#)
- [Step 3: Performing Conditional Actions](#)
- [Step 4: Configuring Identity Attribution](#)

OR



3. Click  to delete the datasource.

Importing Events from Amazon Web Services Cloudtrail

This section describes how to import events from AWS Cloudtrail through a premium connector.

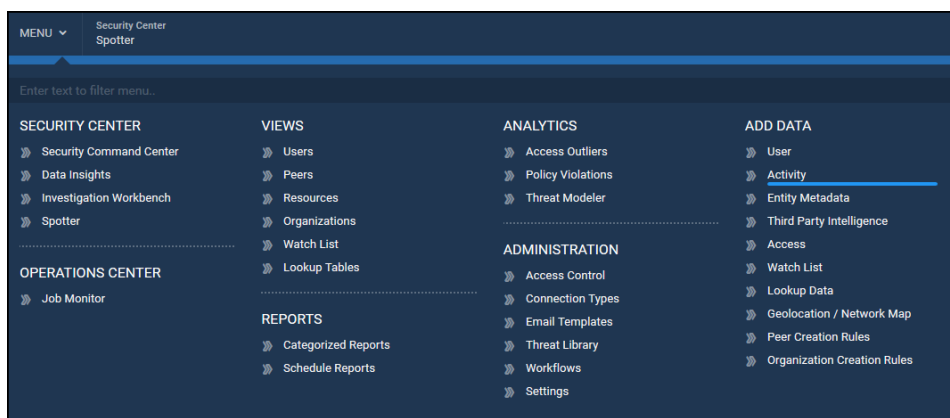
ArcSight UBA uses account-specific key pairs to connect to AWS Cloudtrail. Ensure you have the following information before configuring the connection:

Prerequisites

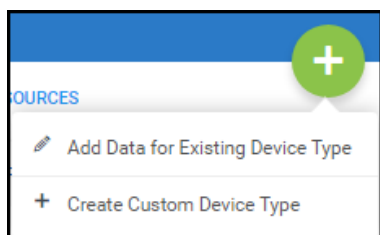
- **AWS Access Key:** The key that uniquely identifies the user who owns the account. Example: KIAIOSFODNN7EXAMPLE.
- **Secret Key:** The key used to calculate the digital signature included in the request. Example: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY.

To import events from AWS Cloudtrail, complete the following steps:

1. Navigate to **Menu > Add Data > Activity**.

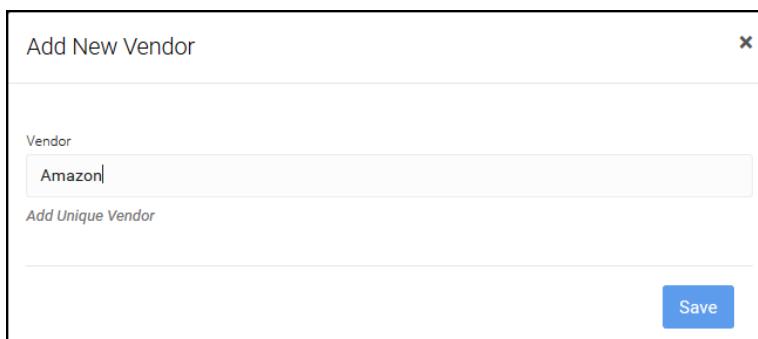


2. Click **+** to add a new datasource.

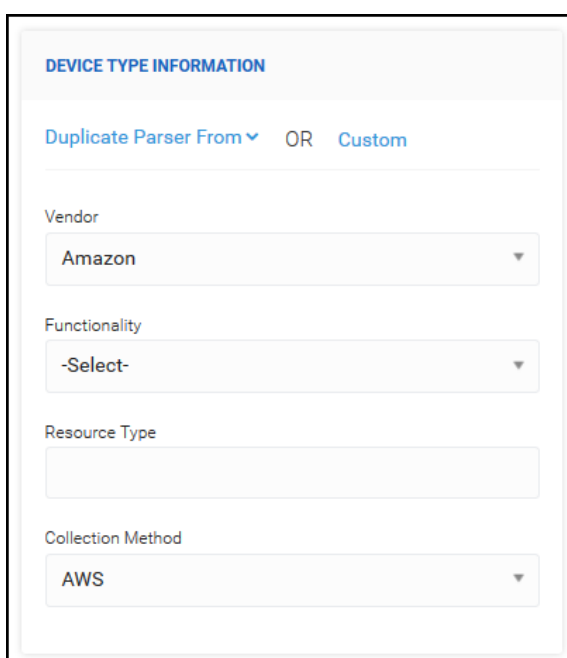


3. Click Select **Add Data for Existing Device Type** or **Create Custom Device Type** from the dropdown.

4. Click **Create New Vendor** and enter the Vendor name:



5. Complete the following information:



- **Vendors:** Amazon
- **Functionality:** Select from dropdown.
- **Resource Types:** Enter a value.
- **Collection Method:** AWS
- **Import Using:** Select **Console** or ID of Ingestion Node if using remote ingester in the environment.

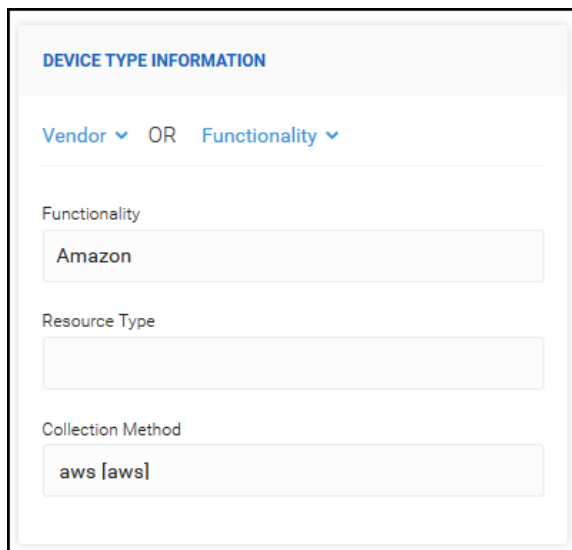


Note: The information you select will populate the Device Type Information section.

6. Complete the following steps to configure the connection:

Device Type Information

The following information is populated by the previous step:



DEVICE TYPE INFORMATION

Vendor ▼ OR Functionality ▼

Functionality

Amazon

Resource Type

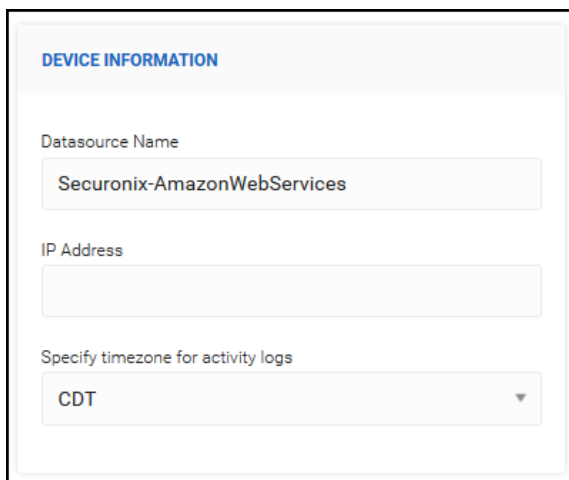
Collection Method

aws [aws]

- Functionality:** Amazon.
- Resource Type:** Left blank.
- Collection Method:** aws [aws]
- Import Using:** Select **Console** or ID of Ingestion Node if using remote ingester in the environment.

Device Information

- Complete the following information:



DEVICE INFORMATION

Datasource Name

Securonix-AmazonWebServices

IP Address

Specify timezone for activity logs

CDT ▼

- a. **Datasource Name:** Enter your unique datasource name. Example: Securonix-AmazonWebServices
- b. **IP Address:** Not required.
- c. **Specify timezone for activity logs:** Specify your time zone using dropdown.

Collection Method

2. Complete the following information:

COLLECTION METHOD

Access Key

AKIAIZYXKLIUB2TEADDA

Enter AWS Access Key. It is alphanumeric text string that uniquely identifies the user who owns the account. For example: AKIAIOSFODNN7EXAMPLE.

Secret Key

heR9x3X/Dmj29P7VFirb9cOSIQfZsMjiaqvNl

Enter AWS Secret Key. This key is just a long string of characters that you use to calculate the digital signature that you include in the request. For example: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY.

Bucket

[TEST CONNECTION & GET BUCKETS](#)

Click on the above button to Test AWS Connection and to get AWS Bucket list. Access key & secret key is required to test connection and to get bucket list.

sudbucket

Incremental Field

☐ NO

Enable it to allow incremental update.

Incremental Field

☐ NO

Enable it to allow incremental update.

Prefix*

aws/AWSLogs/853268358782/CloudTrail/u

Specify the path within the bucket from which logs must be extracted. You can use this to limit the response to folders that begin with the specified prefix. Example: aws/AWSLogs/853268358782/CloudTrail/us-east-1/2017 limits the search to logs from 2017.

Parsing Technique

Key Value Pair

- a. **Access Key:** Enter your unique AWS Access Key. Example: AKIAIOSFODNN7EXAMPLE.
- b. **Secret Key:** Enter your unique AWS Secret Key. Example: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY.
- c. **Bucket:** Click **Test Connection and Get Buckets** and select a bucket from the dropdown. Example: sudbucket.
- d. **Incremental:** Toggle to **Yes** if you would like to retrieve incremental events.
 - a. **No:** Proceed to **Parsing Technique**.
 - b. **Yes:** Specify the following:
 - a. **Incremental Field:** Select an attribute to retrieve incremental events from dropdown. The query sent to the database is appended with this field. Example: logtime.
 - b. **Type:** Select the data type for the Incremental Field from the dropdown. Example: Time.
 - c. **Format:** Specify the date/time format, if required.
 - d. **Incremental Condition Created:** This field will auto-populate based on the information entered in the previous steps. Example: where logtime > '\${logtime}'
 - e. **Force Ascending Order:** Toggle to **Yes** if you would like to force ascending order.
 - c. **Parsing Technique:** Key Value Pair.

More Settings

3. Complete the following information:

MORE SETTINGS

Action Taken On Unparsed Events

SAVE IN UNPROCESSED FOLDER ON HDFS

Success Folder

/Securonix/tenants/partnerdemo
/securonix_home/import/success/

Failed Folder

/Securonix/tenants/partnerdemo
/securonix_home/import/failed/

Specify staging folder (Only required for data requiring preprocessing)

/Securonix/tenants/partnerdemo
/securonix_home/import/in/

Enable Preprocessor

YES

Preprocessor Class

- a. **Action Taken on Unparsed Events:** Select from dropdown. The following options are available:
 - Save in unprocessed folder on HDFS
 - Drop Events
 - Ingest as unparsed events
- a. **Success Folder:** Specify the folder into which you would like the file to move upon successful upload. Default:/Securonix/ArcSight/uba6/securonix_home/import/success/
- b. **Failed Folder:** Specify the folder into which you would like the file to move upon a failed upload. Default:/Securonix/ArcSight/uba6/securonix_home/import/failed/
- c. **Staging Folder:** Specify the staging folder (required for data requiring preprocessing). Default:/Securonix/ArcSight/uba6/securonix_home/import/in/
- d. **Enable Preprocessor:** Toggle to **Yes** if you want to enable.
 - a. **Preprocessor Class** (optional): Enter a preprocessor class if Preprocessor is enabled.

3. **Preview Input** to ensure the file has uploaded successfully.

Import activities from files, applications, databases, security products, network devices & other sources.

[+ BACK TO DATASOURCES](#)

RESOURCE INFORMATION

Vendor **OR** Functionality

Functionality
Securonix

Resource Type

Collection Method
aws [aws]

DATASOURCE INFORMATION

Datasource Name
Securonix-AmazonWebServices

IP Address

Specify timezone for activity logs

PREVIEW INPUT

[GET PREVIEW](#) **OR** [Add Sample Lines](#)

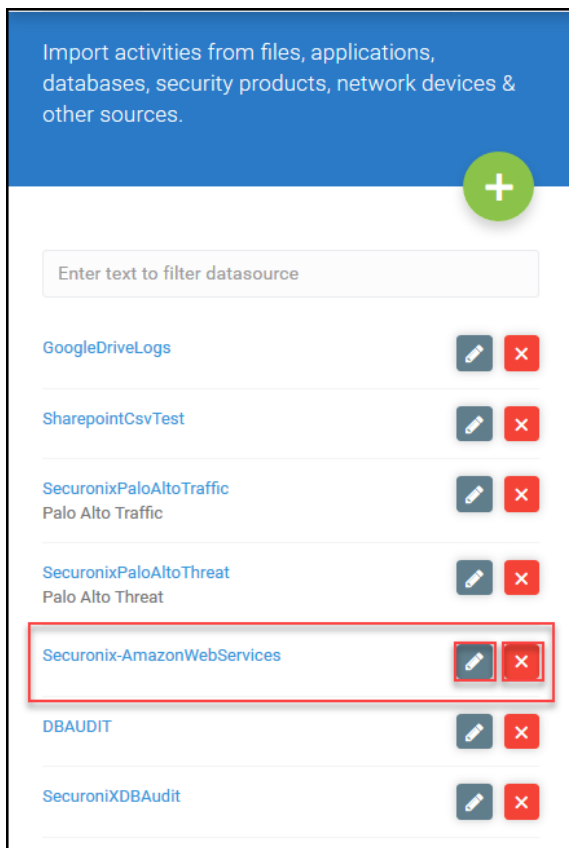
eventVersion="1.01"	userIdentity.type="Root"	userIdentity.principalId="853268359782"	userIdentity.userName="aws:iam:853268359782:root"	userIdentity.accountId="853268359782"	userIdentity.invokedBy="signin.amazonaws.com"
eventVersion="1.01"	userIdentity.type="Root"	userIdentity.principalId="853268359782"	userIdentity.userName="aws:iam:853268359782:root"	userIdentity.accountId="853268359782"	userIdentity.accessKeyId="ASIAJG4XISQUBBVKE"
eventVersion="1.01"	userIdentity.type="Root"	userIdentity.principalId="853268359782"	userIdentity.userName="aws:iam:853268359782:root"	userIdentity.accountId="853268359782"	userIdentity.accessKeyId="ASIAJG4XISQUBBVKE"
eventVersion="1.01"	userIdentity.type="Root"	userIdentity.principalId="853268359782"	userIdentity.userName="aws:iam:853268359782:root"	userIdentity.accountId="853268359782"	userIdentity.accessKeyId="ASIAJG4XISQUBBVKE"
eventVersion="1.01"	userIdentity.type="Root"	userIdentity.principalId="853268359782"	userIdentity.userName="aws:iam:853268359782:root"	userIdentity.accountId="853268359782"	userIdentity.accessKeyId="ASIAJG4XISQUBBVKE"
eventVersion="1.01"	userIdentity.type="Root"	userIdentity.principalId="853268359782"	userIdentity.userName="aws:iam:853268359782:root"	userIdentity.accountId="853268359782"	userIdentity.accessKeyId="ASIAJG4XISQUBBVKE"
eventVersion="1.01"	userIdentity.type="Root"	userIdentity.principalId="853268359782"	userIdentity.userName="aws:iam:853268359782:root"	userIdentity.accountId="853268359782"	userIdentity.accessKeyId="ASIAJG4XISQUBBVKE"
eventVersion="1.01"	userIdentity.type="Root"	userIdentity.principalId="853268359782"	userIdentity.userName="aws:iam:853268359782:root"	userIdentity.accountId="853268359782"	userIdentity.accessKeyId="ASIAJG4XISQUBBVKE"
eventVersion="1.01"	userIdentity.type="Root"	userIdentity.principalId="853268359782"	userIdentity.userName="aws:iam:853268359782:root"	userIdentity.accountId="853268359782"	userIdentity.accessKeyId="ASIAJG4XISQUBBVKE"
eventVersion="1.01"	userIdentity.type="Root"	userIdentity.principalId="853268359782"	userIdentity.userName="aws:iam:853268359782:root"	userIdentity.accountId="853268359782"	userIdentity.accessKeyId="ASIAJG4XISQUBBVKE"
eventVersion="1.01"	userIdentity.type="Root"	userIdentity.principalId="853268359782"	userIdentity.userName="aws:iam:853268359782:root"	userIdentity.accountId="853268359782"	userIdentity.accessKeyId="ASIAJG4XISQUBBVKE"
eventVersion="1.01"	userIdentity.type="Root"	userIdentity.principalId="853268359782"	userIdentity.userName="aws:iam:853268359782:root"	userIdentity.accountId="853268359782"	userIdentity.accessKeyId="ASIAJG4XISQUBBVKE"
eventVersion="1.01"	userIdentity.type="Root"	userIdentity.principalId="853268359782"	userIdentity.userName="aws:iam:853268359782:root"	userIdentity.accountId="853268359782"	userIdentity.accessKeyId="ASIAJG4XISQUBBVKE"
eventVersion="1.01"	userIdentity.type="Root"	userIdentity.principalId="853268359782"	userIdentity.userName="aws:iam:853268359782:root"	userIdentity.accountId="853268359782"	userIdentity.accessKeyId="ASIAJG4XISQUBBVKE"
eventVersion="1.01"	userIdentity.type="Root"	userIdentity.principalId="853268359782"	userIdentity.userName="aws:iam:853268359782:root"	userIdentity.accountId="853268359782"	userIdentity.accessKeyId="ASIAJG4XISQUBBVKE"
eventVersion="1.01"	userIdentity.type="Root"	userIdentity.principalId="853268359782"	userIdentity.userName="aws:iam:853268359782:root"	userIdentity.accountId="853268359782"	userIdentity.accessKeyId="ASIAJG4XISQUBBVKE"


4. Click **Save & Next** to proceed to [Step 5: Reviewing Import Summary](#).

Editing the Connection


To edit the existing AWS Cloudtrail connection, navigate to **Menu > Add Data > Activity** and complete the following steps:

1. Locate the datasource.



2. Click  and proceed to any of the following steps to edit the information:
 - [Step 2: Parsing and Normalization](#)
 - [Step 3: Performing Conditional Actions](#)
 - [Step 4: Configuring Identity Attribution](#)

OR

3. Click  to delete the datasource.

Importing Events from Sophos

This section describes how to import data from Sophos source using a premium connector.

Prerequisites for Importing Events from Sophos

ArcSight UBA uses Sophos UTM Restful API to connect to Sophos to import data. Ensure you have the following information prior to setting up the connection:

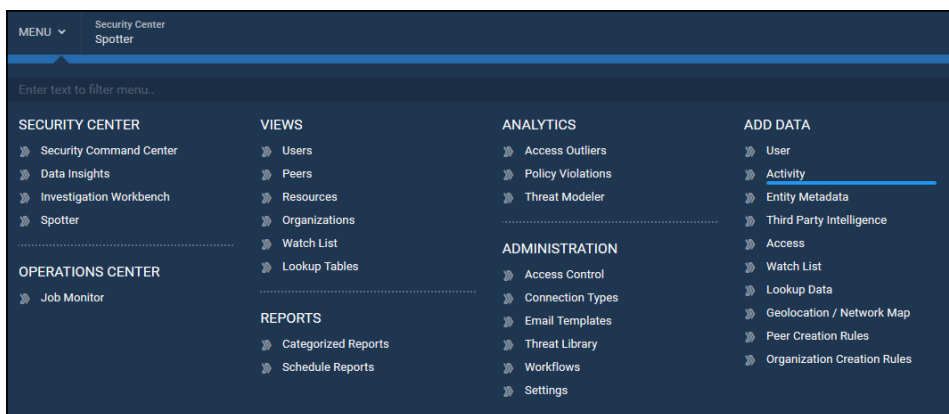
- **URL:** The URL of the API that ArcSight UBA uses to connect.
- **API Key:** The token used to authenticate the API connection.
- **Authorization:** The authorization code to verify access to the UTM.



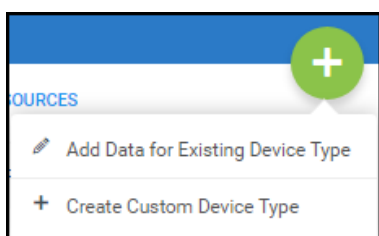
Note: For information about enabling and configuring the Sophos UTM RESTful API, see Sophos UTM documentation.

To import events from Google, complete the following steps:

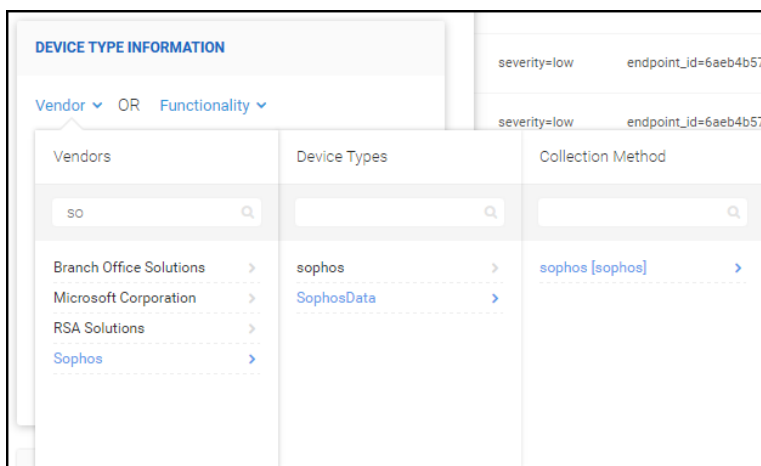
1. Navigate to **Menu > Add Data > Activity**.



2. Click **+** to add a new datasource.



3. Select **Add Data for Existing Device Type**.
4. **Click Vendor** and select the following:



- **Vendors:** Sophos.
- **Device Types:** SophosData.
- **Collection Method:** sophos [sophos].
- **Import Using:** Select **Console** or ID of Ingestion Node if using remote ingester in the environment.



Note: The information you select will populate the Device Type section.

5. Complete the following steps to configure the connection:

Device Type Information

The following information is populated by the previous step:

DEVICE TYPE INFORMATION

Vendor OR Functionality

Resource Type

Collection Method

Import Using

- a. **Functionality:** Sophos.
- b. **Resource Type:** SophosData.
- c. **Collection Method:** sophos [sophos].
- d. **Import Using:** Select **Console** or ID of Ingestion Node if using remote ingester in the environment.

Device Information

1. Complete the following information:

DEVICE INFORMATION

Datasource Name
Sophos

IP Address

Specify timezone for activity logs
CDT ▼

- a. **Datasource Name:** Sophos.
- b. **IP Address:** Not required.
- c. **Specify timezone for activity logs:** Specify your time zone using dropdown.

Collection Method

2. Complete the following information:

COLLECTION METHOD

URL

https://api1.central.sophos.com/gateway

API Key

v6BoxMLeW05peMKY6TbAQ8lpXN9gXTMN58tOLc

Authorization

ZTYyNzVkNjctNDE5Yi00MjJhLWJhODktYjRmNWE1

Type of Data

Events ▼

Parsing Technique

Key Value Pair

- URL:** Specify the URL of the API. Example: https://api1.central.sophos.com/gateway.
- API Key:** Specify the token generated by Sophos UTM to authenticate the connection to the API.
- Authorization:** Specify the authorization to access to Sophos UTM.
- Type of Data:** Select from the dropdown. Example: Events.
- Parsing Technique:** Key Value Pair.

More Settings

3. Complete the following information:

MORE SETTINGS

Action Taken On Unparsed Events

SAVE IN UNPROCESSED FOLDER ON HDFS

Success Folder

/Securonix/tenants/partnerdemo
/securonix_home/import/success/

Failed Folder

/Securonix/tenants/partnerdemo
/securonix_home/import/failed/

Specify staging folder (Only required for data requiring preprocessing)

/Securonix/tenants/partnerdemo
/securonix_home/import/in/

Enable Preprocessor

YES

Preprocessor Class

- a. **Action Taken on Unparsed Events:** Select from dropdown. The following options are available:
 - Save in unprocessed folder on HDFS
 - Drop Events
 - Ingest as unparsed events
 - b. **Success Folder:** Specify the folder into which you would like the file to move upon successful upload. Default:/Securonix/ArcSight/uba6/securonix_home/import/success/
 - c. **Failed Folder:** Specify the folder into which you would like the file to move upon a failed upload. Default:/Securonix/ArcSight/uba6/securonix_home/import/failed/
 - d. **Staging Folder:** Specify the staging folder (required for data requiring preprocessing). Default:/Securonix/ArcSight/uba6/securonix_home/import/in/
 - e. **Enable Preprocessor:** Toggle to **Yes** if you want to enable.
 - a. **Preprocessor Class** (optional): Enter a preprocessor class if Preprocessor is enabled.
4. **Preview Input** to ensure the file has uploaded successfully.

Import activities from files, applications, databases, security products, network devices & other sources.

+

BACK TO DATASOURCES

DEVICE TYPE INFORMATION

Vendor OR Functionality

Vendor

Sophos

Resource Type

SophosData

Collection Method

sophos [sophos]

DEVICE INFORMATION

Datasource Name

Sophos

IP Address

Specify timezone for activity logs

CDT

PREVIEW INPUT

GET PREVIEW OR Add Sample Lines

















severity=low	endpoint_id=37e9602f-2c12-3495-8a35-602c7206f660	created_at=2017-04-24T20:04:00.354Z	source=Wendy Gianacker	type=Event:Endpoint:Device:AlertedOnly	when=2017-04-24T20:04:00.354Z	endpoint_type
severity=low	endpoint_id=4be4c67c-f6d6-64bd-983e-1d120170b4d0	created_at=2017-04-24T20:12:47.404Z	source=Shubhangee Charan	type=Event:Endpoint:Device:AlertedOnly	when=2017-04-24T20:12:47.404Z	endpoint_type
severity=low	endpoint_id=6eeb4b57-deee-7474-081e-181256426a26	created_at=2017-04-24T20:16:48.449Z	source=Mika Test1	type=Event:Endpoint:Device:AlertedOnly	when=2017-04-24T20:16:48.449Z	endpoint_type
severity=low	endpoint_id=6eeb4b57-deee-7474-081e-181256426a26	created_at=2017-04-24T20:17:06.209Z	source=Mika Test1	type=Event:Endpoint:Device:AlertedOnly	when=2017-04-24T20:17:06.209Z	endpoint_type
severity=low	endpoint_id=95e99015-6bda-e46b-9805-4ab3933a6d4	created_at=2017-04-24T20:17:51.304Z	source=Esqel Muraadadeh	type=Event:Endpoint:Device:AlertedOnly	when=2017-04-24T20:17:51.304Z	endpoint_type
severity=low	endpoint_id=292da57a-5a35-7408-1892-d7214e81094c	created_at=2017-04-24T20:20:58.290Z	source=Sandra Perin	type=Event:Endpoint:Device:AlertedOnly	when=2017-04-24T20:20:58.290Z	endpoint_type
severity=low	endpoint_id=4ed140db-630d-4d23-6949-c219a5065d10	created_at=2017-04-24T20:26:46.908Z	source=James McNary	type=Event:Endpoint:Device:AlertedOnly	when=2017-04-24T20:26:46.908Z	endpoint_type
severity=low	endpoint_id=99a2842b-7dbf-046b-8c29-4e92e662b2c2	created_at=2017-04-24T20:27:39.971Z	source=Jessica Steele	type=Event:Endpoint:Device:AlertedOnly	when=2017-04-24T20:27:39.971Z	endpoint_type
severity=low	endpoint_id=27357019-976b-3426-9a83-1b1967125eca	created_at=2017-04-24T20:30:45.018Z	source=Gusana Dea	type=Event:Endpoint:Device:AlertedOnly	when=2017-04-24T20:30:45.018Z	endpoint_type
severity=low	endpoint_id=27357019-976b-3426-9a83-1b1967125eca	created_at=2017-04-24T20:30:45.249Z	source=Gusana Dea	type=Event:Endpoint:Device:AlertedOnly	when=2017-04-24T20:30:45.249Z	endpoint_type
severity=low	endpoint_id=27357019-976b-3426-9a83-1b1967125eca	created_at=2017-04-24T20:30:45.351Z	source=Gusana Dea	type=Event:Endpoint:Device:AlertedOnly	when=2017-04-24T20:30:45.351Z	endpoint_type
severity=low	endpoint_id=38792342-0f14-4e4b-2a4f-6cdee7d3a7	created_at=2017-04-24T20:31:44.396Z	source=Jim Perizo	type=Event:Endpoint:Device:AlertedOnly	when=2017-04-24T20:31:44.396Z	endpoint_type
severity=low	endpoint_id=414069c3-8201-1409-6902-4c5941b4a49	created_at=2017-04-24T20:35:16.392Z	source=Zhenkargovda Matelgova	type=Event:Endpoint:Update:Success	when=2017-04-24T20:35:16.391Z	endpoint_type
severity=low	endpoint_id=961931a5-4e5b-040f-aade-f909746d0203	created_at=2017-04-24T20:35:30.771Z	source=Chris Bell	type=Event:Endpoint:Update:Success	when=2017-04-24T20:35:30.738Z	endpoint_type
severity=low	endpoint_id=47c6390d-6645-7411-aef8-1dfe51c74cde	created_at=2017-04-24T20:35:57.186Z	source=Gudashan Bakirshman	type=Event:Endpoint:Device:AlertedOnly	when=2017-04-24T20:35:57.186Z	endpoint_type

4. Click **Save & Next** to proceed to [Step 5: Reviewing Import Summary](#).

Editing the Connection

To edit the existing Google connection, navigate to **Menu > Add Data > Activity** and complete the following steps:

1. Locate the datasource.

GDriveLogs GoogleD	 
PALOALTO_TRAFFIC_FIREWALL PALOALTO_FIREWALLTRAFFIC	 
BluecoatProxy Bluecoat	 
ADEvents WindowsAD	 
GoogleLogin google	 
Salesforce Salesforce	 
Sophos SophosData	 
Office365 office365EmailSec	 



2. Click and proceed to any of the following steps to edit the information:

- [Step 2: Parsing and Normalization](#)
- [Step 3: Performing Conditional Actions](#)
- [Step 4: Configuring Identity Attribution](#)

OR



3. Click to delete the datasource.

Step 2: Parsing and Normalization

ArcSight UBA extracts fields based on the parsing technique selected in the previous screen. In this section, you will parse events into individual attributes and map them to corresponding attributes in the Securonix event schema.



Note: For a complete list of attributes in ArcSight UBA, see [Appendix A: ArcSight UBA Attribute Schema](#).

The screenshot shows the 'Parsing & Normalization' tab in the ArcSight UBA interface. The 'PREVIEW RAW DATA' section displays a table of event data. The table has columns for 'EventTime', 'CustomerID', 'ApplicationName', 'UniqueIdentifier', 'Kind', 'Etag', 'OwnerDomain', and 'IPAddress'. The 'ApplicationName' column is highlighted with a red box, and a callout points to it with the text 'Attribute extracted from datasource.' Another callout points to the 'ApplicationName' column in the table with the text 'Corresponding attribute in Securonix event schema.'

EventTime	CustomerID	ApplicationName	UniqueIdentifier	Kind	Etag	OwnerDomain	IPAddress
2017-09-28T20:22:27.232Z	C02x5dgm	drive	40635	admin:reports:activity	"DdtpNbnLzQPlwBpSjF2-ZoF0/208wvE1DXlpHh_Qombas2HE"	70.119.137.183	
2017-09-28T20:22:11.213Z	C02x5dgm	drive	-18700173410081506	admin:reports:activity	"DdtpNbnLzQPlwBpSjF2-ZoF0/O_jpwHqKfme4KkKewuBEOQv7K"	70.119.137.183	
2017-09-28T20:21:55.277Z	C02x5dgm	drive	89335061644946396	admin:reports:activity	"DdtpNbnLzQPlwBpSjF2-ZoF0/hu_a68yyNwktBqTnQ_GWmGSc"	104.249.224.18	
2017-09-28T20:19:04.457Z	C02x5dgm	drive	-7889349304352342967	admin:reports:activity	"DdtpNbnLzQPlwBpSjF2-ZoF0/CU2LTgO7v7A_2tpOUktn1nmU"	67.21.178.236	
2017-09-28T20:18:56.514Z	C02x5dgm	drive	-823708145729627031	admin:reports:activity	"DdtpNbnLzQPlwBpSjF2-ZoF0/N7DWQLSINvNjAha7DPVv4D30"	2601.40c-4302-d8db-84F9-5145-146d39	
2017-09-28T20:18:54.945Z	C02x5dgm	drive	-353727224541544344	admin:reports:activity	"DdtpNbnLzQPlwBpSjF2-ZoF0/Bhu_TP4pH3uakGdX9Dec4QJad"	104.249.224.18	
2017-09-28T20:18:39.453Z	C02x5dgm	drive	-821232837235257929	admin:reports:activity	"DdtpNbnLzQPlwBpSjF2-ZoF0/Bhu_TP4pH3uakGdX9Dec4QJad"	208.116.216.129	
2017-09-28T20:16:04.390Z	C02x5dgm	drive	-4985157402370058448	admin:reports:activity	"DdtpNbnLzQPlwBpSjF2-ZoF0/7QMTOk7jDmmLzJkXUJM3bm0"	67.21.178.236	
2017-09-28T20:15:54.994Z	C02x5dgm	drive	193529462314656808	admin:reports:activity	"DdtpNbnLzQPlwBpSjF2-ZoF0/vz0aADPigaBkXvVeePULZ4JvU"	104.249.224.18	
2017-09-28T20:13:04.312Z	C02x5dgm	drive	-454313802962626614	admin:reports:activity	"DdtpNbnLzQPlwBpSjF2-ZoF0/vRXX774_gMclbVamp1BE5rmeFE"	67.21.178.236	
2017-09-28T20:10:04.252Z	C02x5dgm	drive	-8901827406158707672	admin:reports:activity	"DdtpNbnLzQPlwBpSjF2-ZoF0/BXZ3suXKwZu5dQes_R6U_pM"	67.21.178.236	

To parse and normalize data in ArcSight UBA, complete the following steps:

Line Filters

1. Click **+** to create a new line filter.
2. Enter the **Line Filter Name**. Example: AllLines.
3. Click **Extract Fields**.

This will parse the fields and allow you to map them to corresponding ArcSight UBA attributes.

4. Click **+** to Extract additional fields.

Map Attributes

time	customerid	applicationName	uniqueQualifier	kind	etag	ownerDomain	ipAddress	email	profileId	eventName	eventType	docId	docType	docTitle	owner	oldValue	newValue	sourceFolderId	sourceFolderTitle	destinationFolderId	destinationFolderTitle	targetUser	targetDomain
EventTime (DATETIME)	CustomerID (destinationuserid)	ApplicationName (deviceprocessname)	UniqueQualifier (additionaldetails1)	Kind (customstring1)	ETag (additionaldetails2)	OwnerDomain (sourcendomain)	IPAddress (address)																
time	customerid	applicationName	uniqueQualifier	kind	etag	ownerDomain	ipAddress																
2017-05-28T20:22:27.252Z	C02x5dqm	drive	4063540791372268594	admin#reports#activity	"DdtxpNbnLz2QPlwBpScf2-ZoF0/Z08wvE10X9jctvL_Gumtba52HE"		70.119.137.183																
2017-05-28T20:22:11.213Z	C02x5dqm	drive	-1870017534100881506	admin#reports#activity	"DdtxpNbnLz2QPlwBpScf2-ZoF0/O_gywtKpXfme40KzKewuBED0a7k"		70.119.137.183																
2017-05-28T20:21:55.277Z	C02x5dqm	drive	893350616644946396	admin#reports#activity	"DdtxpNbnLz2QPlwBpScf2-ZoF0/ha_s68IyyNfsekRqT3o_GWGGc"		104.249.224.18																
2017-05-28T20:19:04.457Z	C02x5dqm	drive	-7889349304352342967	admin#reports#activity	"DdtxpNbnLz2QPlwBpScf2-ZoF0/CU2LTgQ7yp7A_2f6dUJXm1emU"		67.21.178.236																
2017-05-28T20:18:56.514Z	C02x5dqm	drive	-8237081457729627031	admin#reports#activity	"DdtxpNbnLz2QPlwBpScf2-ZoF0/N7DQWQLSNVgAha7J6PVH4D30"		2601.40c:4302:adeb:849f:5145:146d:39																
2017-05-28T20:18:54.943Z	C02x5dqm	drive	-353372724541544344	admin#reports#activity	"DdtxpNbnLz2QPlwBpScf2-ZoF0/HPUQmhd36fWauGfX11zzPBY"		104.249.224.18																
2017-05-28T20:18:39.453Z	C02x5dqm	drive	-8212328372352537929	admin#reports#activity	"DdtxpNbnLz2QPlwBpScf2-ZoF0/Bhu_LTP4dR3cdhGdX9Dec4QJua"		209.116.216.129																
2017-05-28T20:16:04.390Z	C02x5dqm	drive	-695515740237005848	admin#reports#activity	"DdtxpNbnLz2QPlwBpScf2-ZoF0/7QMTOK7y0vnmJnJ3UJMJ38m0"		67.21.178.236																
2017-05-28T20:15:54.994Z	C02x5dqm	drive	193529462314656808	admin#reports#activity	"DdtxpNbnLz2QPlwBpScf2-ZoF0/vsDaAGPpIaXteYvdesPUZAJyw"		104.249.224.18																
2017-05-28T20:13:04.312Z	C02x5dqm	drive	-45431380290262614	admin#reports#activity	"DdtxpNbnLz2QPlwBpScf2-ZoF0/ufRX774_gM5d5bVamp18E3rtimefE"		67.21.178.236																
2017-05-28T20:10:54.353Z	C02x5dqm	drive	-89018374041540207475	admin#reports#activity	"DdtxpNbnLz2QPlwBpScf2-ZoF0/BB87BwvYATDv7u55CwvB6f1u6E"		67.21.178.236																

1. Click each datasource attribute highlighted in blue to map to a corresponding ArcSight UBA field.

2017-08-03T16:45:08.000Z	C02x5djsm	login
EventTime (DATETIME)	CustomerID (destinationuserid)	ApplicationName (de

Attribute Name

Map With

DATETIME ▼

Format

[Validate Format](#)

Description

Populate Using Function

Select Function X

Indexed?

YES ☒

Display on UI?

YES ☒

Is Multivalued?

NO ☐

Remove Mapping

Save

- Attribute Name:** Specify the name of the attribute in the datasource.
- Map With:** Select a corresponding ArcSight UBA attribute from the dropdown.
- Format:** Specify a DATETIME format if required or proceed to next field.
- Description:** Enter a brief a description of the attribute.
- Indexed?:** Toggle to **Yes** to index the attribute in Solr to be available in Spotter search results. Toggle to **No** to exclude the field from Spotter search results.
- Display on UI?:** Toggle to **Yes** to display the attribute in results on the UI. Select **No** to exclude the field from results on the UI.

- g. **Is Multivalued?:** Toggle to **Yes** if the attribute has multiple values separated by a delimiter and specify **Delimiter**.
- h. **Populate Using Function:** Click **Select Function** to view and select available functions/formulas to perform operations on attribute values.

Functions include:

- **Logical Functions**
- **Math Functions**
- **Other Functions**
- **String Functions**
- **Formula**



Note: For a complete list of functions, see [Appendix B: Functions](#).

Populate Using Function

Function/Formula are used to perform operations on attribute value. You can create Formula or select Function from below.

field

Logical Functions
Math Functions
Other Functions
String Functions
Formula
Add Field

IF_GREATER_OR_EQUAL	This implements the condition if(A>=B) then C else D . 4 pipe separated attributes/constants which are in order of A,B,C,D from the above description. E.g. : IF_GREATER_OR_EQUAL(attr1 100 OK NOT OK)
IF_THEN_ELSE	This implements the condition if(A.equals(B)) then C else D.(A and B are matched as string). 4 pipe separated attributes/constants which are in order of A,B,C,D from the above description. E.g. : IF_THEN_ELSE(attr1 100 OK NOT OK)
SIMPLE_MAP	This function replaces the value found on the basis of preconfigured values found from map. List of pipe separated parameters, first parameter is attribute name whose value needs to be checked an updated. Others '=' separated key value pairs. E.g. : SIMPLE_MAP(attr1 foo=100 bar=200)
SEVERITY_NUMERIC_RANGE	Severity is set according to the numeric range. Two parameters first being the attribute name, second is a coma separated 4 specifying the range of severity. (order is LOW,MEDIUM,HIGH,VERY HIGH,CRITICAL) E.g. : SEVERITY_NUMERIC_RANGE(attr1 100,200,300,400)
SEVERITY_STRING_MATCHER	Severity is set according to the string encountered. List of pipe separated parameters, first parameter is attribute name whose value needs to be checked an updated. Others '=' separated key value pairs(value can be multivalue separated by coma) E.g. : SEVERITY_STRING_MATCHER(attr1 HIGH=foo1,foo2 LOW=foo3)

Add

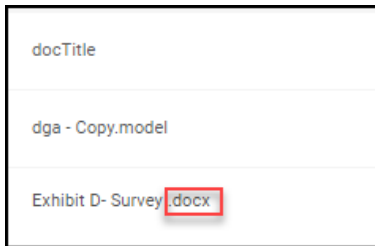
- a. Click the name of the function to select the function.

OR

- b. Click **Add Field** to create a formula.
- c. Click **Add** to return to the previous screen.

Use functions to extract certain information from a field as in the following example:

Extract file extension from DocTitle field



Use this string function to extract only the specified string within a field to appear in search and dashboard results.

1. Click the field from which to extract file extension.

implementation@securonix.com

DocOwner (emailsender) DocTitle (oldfilename) OldValue (customstring1)

Attribute Name

DocOwner

Map With

emailsender

Description

Populate Using Function

Select Function X

Indexed?

YES

Display on UI?

YES

Is Multivalued?

NO

Remove Mapping Save

2. Click **Select Function**.
3. Click **String Functions**.
4. Click **FILE_EXTENSION_EXTRACTOR**.

i Function/Formula are used to perform operations on attribute value. You can create Formula or select Function from below.

Logical Functions	Math Functions	Other Functions	String Functions	Formula
<p>TO_UPPER Converts the string read to upper case. Only one parameter which is the attribute name of the parameter to convert. E.g. : TO_UPPER(attr1)</p> <p>TO_LOWER Converts the string read to lower case. Only one parameter which is the attribute name of the parameter to convert. E.g. : TO_LOWER(attr1)</p> <p>CONCATENATE Concatenate the list attributes or constant. Pipe separated list of attributes and/or constants. E.g. : CONCATENATE(attr1 'abc' attr3)</p> <p>CONSTANT Replaces the destination attribute to a given constant. E.g. : CONSTANT('abc')</p> <p>TRIM Trims the given attribute. Only one parameter which is the attribute name of the parameter to convert. E.g. : TRIM(attr1)</p> <p>REGEX_TOKEN Returns the first token match for the given string. Two parameter first being the attribute name and second being the regex token. E.g. : REGEX_TOKEN(attr1 'fo+(o.*)'(r)')</p> <p>TOP_LEVEL_DOMAIN Extracts the top level domain of any url. Only one parameter which contains the hostname. E.g. TOP_LEVEL_DOMAIN</p> <p>FILE_EXTENSION_EXTRACTOR Get file extension.(c:/temp/test.txt returns txt) Only one parameter which is the attribute name of the parameter to convert. E.g. : FILE_EXTENSION_EXTRACTOR(attr1)</p>				

Add

5. Click **field**.

Populate Using Function

i Function/Formula are used to perform operations on attribute value. You can create Formula or select Function from below.

FILE_EXTENSION_EXTRACTOR(**field**)

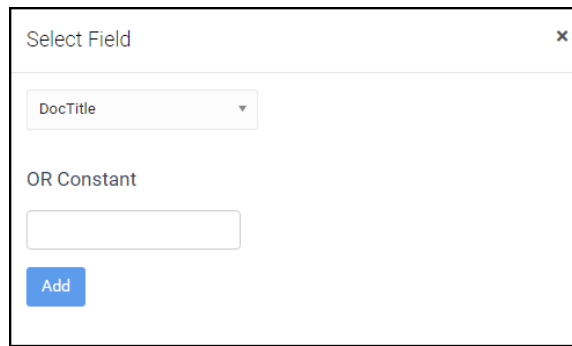
Logical Functions	Math Functions	Other Functions	String Functions	Formula
-------------------	----------------	-----------------	------------------	---------

6. Select a **Field** from the dropdown. Example: DocTitle.

OR

7. Enter a **Constant** value.

8. Click **Add**.



The image shows a 'Select Field' dialog box with a close button (X) in the top right corner. Inside the dialog, there is a dropdown menu currently showing 'DocTitle'. Below the dropdown, the text 'OR Constant' is displayed above an empty text input field. At the bottom left of the dialog is a blue button labeled 'Add'.

9. Click **Add** from the Populate Using Functions window.
10. Click **Save** in the attribute mapping window.

The screenshot shows a configuration window for mapping an attribute. At the top, there are three tabs: 'implementation@securonix.com', 'DocOwner (emailsender)', and 'DocTitle (oldfilename)'. The 'DocOwner (emailsender)' tab is selected. Below the tabs, the form contains the following fields and controls:

- Attribute Name:** A text input field containing 'DocOwner'.
- Map With:** A dropdown menu showing 'emailsender'.
- Description:** A large text area for additional information.
- Populate Using Function:** A button labeled 'Select Function' and a button labeled 'X'.
- Indexed?:** A toggle switch set to 'YES'.
- Display on UI?:** A toggle switch set to 'YES'.
- Is Multivalued?:** A toggle switch set to 'NO'.

At the bottom right of the form, there are two buttons: 'Remove Mapping' (red) and 'Save' (blue).

ArcSight UBA will extract only the file extension from this field in the indexed results (if enabled) and on the UI (if enabled).



Note: The file name will not appear in the results.

2. Click **Save**.



Note: To clear mapping from the attribute and start over, click **Remove Mapping**.

3. Preview results on the Preview Raw Data screen to ensure the attributes are mapped correctly.

PREVIEW RAW DATA
Click on sample events highlighted in blue in below section to map them with Snyptr fields

time	customerid	applicationName	uniqueQualifier	kind	etag	ownerDomain	ipAddress	email	profileId	eventName	eventType	docId	docType	docTitle	owner	oldValue	newValue	sourceFolderId
sourceFolderTitle	destinationFolderId	destinationFolderTitle	targetUser	targetDomain														

EventTime (DATETIME)	CustomerID (destinationuserid)	ApplicationName (deviceprocessname)	UniqueQualifier (additionaldetails1)	Kind (customating1)	ETag (additionaldetails2)	OwnerDomain (sourcendomain)	IPAddress (ipaddress)
time	customerid	applicationName	uniqueQualifier	kind	etag	ownerDomain	ipAddress
2017-03-28T20:22:27.252Z	C02x5djam	drive	4063540791372268594	admin#reports#activity	"DdtrpNbnLzQPilw8pScjF2-ZoF0/Z08wvE10X9jzrlV_Oxmhsa52HE"		70.119.137.183
2017-03-28T20:22:11.213Z	C02x5djam	drive	-1870017534100881506	admin#reports#activity	"DdtrpNbnLzQPilw8pScjF2-ZoF0/Q_yprwKpXfme4KKzKewuBED0s7k"		70.119.137.183
2017-03-28T20:21:55.277Z	C02x5djam	drive	893350616644946396	admin#reports#activity	"DdtrpNbnLzQPilw8pScjF2-ZoF0/hs_a68IyyN9sef8qTbG_GWVG0c"		104.249.224.18

4. Click **Save & Next** to proceed to [Step 3: Performing Conditional Actions](#).

Step 3: Performing Conditional Actions

In this section, you can specify the actions to perform when events meet conditions specified in filters. Multiple actions can be specified on the same condition.

Action Filters

Action filters allow you to perform actions when events meet the conditions specified in the filters.

Perform actions when events meet conditions specified in filters. Multiple actions can be specified on the same condition.

ACTION FILTERS

Set_Event_Category YES

IP ADDRESS TO ACCOUNT NAME RELATIONSHIP

Enable Storage of IP Address to Account Name Information

☐ NO

Record the account name using an IP Address and use it for associating the events that do not have account name information.

SAVE

DERIVED FIELDS (AVAILABLE:2)

+ Add New

EmailDirectionvalue
transactionstring1

SenderValue
emailsender

Add Conditions

1. Click **+** to add a condition.

2. Specify the following to create the **Condition** action:
 - a. **Attribute:** Select the attribute to which to apply the condition from the dropdown of the attributes mapped in the previous step. Example: EventName.
 - b. **Operator:** Specify the Operator. Examples: Equal To, Contains, Ends With, Starts With.
 - c. **Value:** Specify the value of the attribute. Example: Delete.
 - d. **Add/Remove:** Use **+/-** to add/remove conditions.
 - e. **Do you want to drop Events that do not get correlated?:** Enable slider to **YES** to evaluate the specified conditions after correlation of event data.

Select Actions for Conditions

You can configure ArcSight UBA to take specific actions when the conditions configured in the previous step are met. You can add multiple actions for the conditions.



To Select Actions for Above Conditions, click **+** to add as many actions as you wish to perform for the condition. Click **Remove action** to remove the action.

Actions to take for conditions include the following:

Set Device Severity

When configured conditions are met, set a criticality for the events to prioritize events on the security dashboard as in the following example:

ADD CONDITIONS


Attribute	Operator	Value	Condition	Add/Remove
Event Name	Equal To	delete	AND	 

Do you want to drop Events that do not get correlated?

☐ NO

If yes then above conditions will be evaluated after correlation of event data.

SELECT ACTIONS FOR ABOVE CONDITIONS

 Click on + icon to add actions

SET_DEVICE_SEVERITY REMOVE ACTION

Set Device Severity

Medium

CANCEL SAVE

For **Condition**:

- Attribute**: EventName | **Operator**: Equal To | **Value**: delete.



Set Device Severity:

- Set Device Severity**: Select from the dropdown. Example: Critical.

Set Event Category

When configured conditions are met, set an event category to group event types with similar event types across multiple datasources:

ADD CONDITIONS


Attribute	Operator	Value	Condition	Add/Remove
Event Name	Equal To	LOGIN_FAILURE	AND	 

Do you want to drop Events that do not get correlated?

☒ NO

If yes then above conditions will be evaluated after correlation of event data.

SELECT ACTIONS FOR ABOVE CONDITIONS

 Click on + icon to add actions

SET_EVENT_CATEGORY REMOVE ACTION

Category Object (OBJECT ACTED UPON)
Application

Category Behavior (ACTION TAKEN)
Authentication

Category Outcome (OUTCOME OF ACTION)
Failure

CANCEL SAVE

For **Condition**:

- a. **Attribute**: Event Name | **Operator**: Equal to | **Value**: LOGIN_FAILURE

Set Event Category:

- Category Object**: Specify the object acted upon. Example: Application.
- Category Behavior**: Specify the action to be taken. Example: Authentication.
- Category Outcome**: Specify the outcome of the action. Example: Failure.

Enrich from TPI

When configured conditions are met, enrich the event data with Third Party Intelligence data. In this example, when transactions are blocked by a firewall, check the IP address against TPI.

ADD CONDITIONS

Attribute	Operator	Value	Condition	Add/
<div> <div>EventName</div> </div>	<div> <div>Equal To</div> </div>	<div> <div>Blocked</div> </div>	<div> <div>AND</div> </div>	<div> <div>+</div> </div>

Do you want to drop Events that do not get correlated?
☐ NO
If yes then above conditions will be evaluated after correlation of event data.

SELECT ACTIONS FOR ABOVE CONDITIONS

+

Click on + icon to add actions

ENRICH_FROM_TPI REMOVE ACTION

Select attribute that gets Enriched with TPI information

Destination IP

CANCEL SAVE

For **Condition**:

- a. **Attribute:** EventName | **Operator:** Equal To | **Value:** Blocked

Enrich from TPI

- a. **Enrich From TPI:** Select the attribute to be enriched with TPI information from the dropdown.
Example: Destination IP.

Populate ActiveList

When configured conditions are met, populate an active list. Active lists are used in ArcSight UBA to maintain a history of activity on specified attributes for each event for a specified duration of time for faster processing and analytical checks. Active lists are stored in Redis in-memory database. In this example, populate an active list for accountname + filename when a user checks out a file to quickly view violations such as uploading the file to a person email or file sharing/storage site.

Click on + icon to add actions

POPULATE_ACTIVELIST REMOVE ACTION

+ CREATE NEW ACTIVE LIST

Activelist Name	Active List Rule	Duration (in Seconds)	Enable
accountname+Filename	accountname+filename	3600	<input type="checkbox"/> NO
Failed Login+Accountname	transactionstring2+sessionid	10	<input type="checkbox"/> NO
emailsender+filename	emailsender+filename	3600	<input type="checkbox"/> NO

Enabled Active List will be populated during enrichment with specified rule.

For **Condition**:

- a. **Attribute**: Transactionstring1 | **Operator**: Equal To | **Value**: File Checked Out

Populate Activelist:

a. Enable an existing Active List. Example: accountname+Filename.

OR

b. **Create New Active List:**

Create New Active List

Activelist Name
Account Name+Filename

Duration (In Seconds)
600

Active List Rule
accountname+filename

Please specify mapped attributes.e.g. accountname+ipaddress
transactionstring1(50)+accountname(1,3)
emailsender()+filename

Cancel Save

- **Active List Name:** Specify a list name. Example: Account Name+Filename. The Account Name and File Name will be retained in-memory for the following specified duration.
- **Duration:** Specify the duration in seconds for list to remain active in in-memory database. Example: 600 (10 minutes).
- **Active List Rule:** Specify the mapped attributes to include in the active list. Example: accountname+filename.

Geolocate Attributes

When configured conditions are met, enrich with geolocation attributes. ArcSight UBA can use geolocation attributes to detect land speed violations and other threats for which a geolocation is required. In this example, enrich events with geolocation when a user successfully logs in.

For Condition:

- a. **Attribute:** Transactionstring1 | **Operator:** Equal To | **Value:** Authentication: Successful

Enrich with Geolocation Attributes:

- a. **Specify fields to get Geolocated:** Use > or >> to add fields from the available attributes.
Example: IP Address.

Enrich from Watchlist

When configured conditions are met, enrich attributes with Watchlist data. In this example, check account name against a watchlist for bad performance reviews when a user performs activity on a document that contains the word "confidential" to detect possible data exfiltration.

For Condition:

- a. **Attribute:** DocTitle | **Operator:** Contains | **Value:** confidential

Enrich from Watchlist:

- a. **Match Condition:** Check the selected watchlist against the specified attribute in the event data.
 - a. **Select Watchlist:** Select Watchlist from dropdown. Example: Bad Performance Review.
 - b. **Matches:** Specify mapped attributes to match. Example: accountname.
- b. **Perform Enrichment:** Add an additional attribute to event data when the previous condition is met.
 - a. **Extract value from:** Select an existing value to extract from using dropdown. Bad Performance Review_entityname.
 - b. **Store In:** Create a new enrichment attribute to add to the event data when conditions match:



Note: The attribute you select cannot already be mapped to an attribute for this data-source.

- a. **Attribute Name:** Provide a unique name to identity the new attribute in the event data.
- b. **Map With:** Select an unmapped attribute from the dropdown.
- c. **Description:** Enter a brief description of the attribute.
- d. **Populate Using Function:** Click to populate attribute using a function. For more information about Functions, see [Derived Fields](#).
- e. Enable **Indexed?** to index the attribute in Solr to be available in Spotter search results. Disable to exclude the field from Spotter search results.
- f. Enable **Display on UI?** to display the attribute in results on the UI. Disable to exclude the field from results on the UI.

Enrich from Lookup Table

When configured conditions are met, Enrich from Lookup Table. In the following example, enrich

with data from non-business domain lookup table if a user changes permissions in Google to check if the permissions have been changed to a non-business domain such as a personal file sharing account or competitor domain.

SELECT ACTIONS FOR ABOVE CONDITIONS

Click on + icon to add actions

ENRICH_FROM_LOOKUP_TABLE REMOVE ACTION

MATCH CONDITION: Select Lookup: Non_business_domains Matches: Email Recipient Domain

Please specify mapped attributes e.g. accountname+ipaddress
transactionstring1(50)+accountname(1,3)
emailsender+(.)+filename

PERFORM ENRICHMENT: Extract value from: Non_business_domains_header Store In: Create Enrichment Attribute

For Condition:

- a. **Attribute:** EventName | **Operator:** Contains | **Value:** Permissions Changed

Enrich from Lookup Table:

- a. **Match Condition:** Check the selected lookup table against the specified attribute in the event data.
 - a. **Select Lookup:** Select Lookup Table from dropdown. Example: Non_Business_Domains.
 - b. **Matches:** Specify mapped attributes to match. Example: Email Recipient Domain.
- b. **Perform Enrichment:** Add an additional attribute to event data when the previous condition is met.
 - a. **Extract value from:** Select an existing value to extract from using dropdown. Example: Non_business_domains_header.
 - b. **Store In:** Select an enrichment attribute or **Create Enrichment Attribute**.

Add New Attribute

Attribute Name: Non Business Domain

Map With: customstring3

Description:

Populate Using Function: Select Function X

Indexed? YES

Display on UI? YES

Save

Enrich From Asset Metadata

When conditions are met, enrich attributes with Asset Metadata. In this example, use asset metadata for laptop owner to identify a user when an account name is null.

The screenshot shows a configuration window titled "SELECT ACTIONS FOR ABOVE CONDITIONS". Inside, there is a section for "ENRICH_FROM_ASSET_METADATA" with a "REMOVE ACTION" link. The configuration is divided into two main parts: "MATCH CONDITION" and "PERFORM ENRICHMENT".

MATCH CONDITION:

- Select Asset Metadata:** A dropdown menu with "DallasAssetMetadata" selected.
- Matches:** A text input field containing "Source hostname".
- Help text:** "Please specify mapped attributes e.g. accountname+ipaddress transactionstring(50)+accountname(1,3) emailsender()+filename"

PERFORM ENRICHMENT:

- Extract value from:** A dropdown menu with "Owner" selected.
- Store In:** A dropdown menu with "Create Enrichment Attribute" selected.

There is a green plus icon and a red minus icon at the bottom right of the configuration area.

For Condition:

Attribute: AccountName | **Operator:** Equal To | **Value:** NULL.

Enrich from Asset Metadata:

- Match Condition:** Check the selected asset metadata datasource against the specified attribute in the event data.
 - Select Asset Metadata:** Select available datasource from dropdown. Example: DallasAssetMetadata.
 - Matches:** Specify the mapped attribute to match to the asset metadata. Example: Source Hostname.

b. **Perform Enrichment:** Add an additional attribute to event data when the previous condition is met.

- **Extract Value from:** Use dropdown to select an existing attribute from which to extract asset metadata value. Example: Owner.
- **Store In:** Select an existing enrichment attribute value from dropdown OR **Create Enrichment Attribute.**

- **+/-:** Click to add/remove enrichment rules.

Perform IP Address Attribution

When above conditions are met, perform IP address attribution to detect an account for an IP Address. In this example, attribute an IP to the user who logged into a destination host name such as a proxy when account name is null.



Note: This differs from IP Attribute Mapping, as ArcSight UBA will only perform IP address attribution on events when specific conditions are met, rather than for a specified duration of time on all events.

For Condition:

- a. **Attribute:** Account Name | **Operator:** Equal to | **Value:** NULL.

Perform IP Address Attribution:

- a. **Detect the Account for an IP Address?:** Toggle to **Yes** to enable. Requires IP address to user relationship.
- b. **Select IPAddress Attribute:** Select an attribute to which to attribute an IP Address from drop-down.
- c. **Select Hostname Attribute:** Select a hostname attribute to attribute from dropdown.

Click **Save** for each **Action Filter**.

Drop Events

When above conditions are met, drop events with the above matching conditions.

ADD CONDITIONS

Attribute	Operator	Value	Condition	Add/Remove
URL	Equal To	mycompany.com	AND	+ -

Do you want to drop Events that do not get correlated?

☐ NO

If yes then above conditions will be evaluated after correlation of event data.

SELECT ACTIONS FOR ABOVE CONDITIONS

+ Click on + icon to add actions

DROP_EVENTS REMOVE ACTION

Do you want to drop events?

☐ NO

Events with above matching conditions will be dropped.

CANCEL SAVE

For Condition:

- a. **Attribute:** URL | **Operator:** Equal to | **Value:** mycompany.com.

Do you want to drop events?: Set slide to **YES** or **NO**.

IP Address to Account Name Relationship

Enable IP Address to Account Name Relationship to record the account name using an IP address and use it for associating the events that do not have account name information. For example, proxy or firewall logs. IP Address to Account Name Relationship maintains relationships between account names from authentication datasources such as Active Directory and dynamic IP addresses for a specified duration of time.

To enable IP Address to Account Name Relationship, complete the following steps:

1. Toggle to **Yes** to **Enable Storage of IP Address to Account Name Information**.

IP ADDRESS TO ACCOUNT NAME RELATIONSHIP

Enable Storage of IP Address to Account Name Information

YES

Record the account name using an IP Address and use it for associating the events that do not have account name information.

Events Matching Criteria:

Transaction Attribute	Transaction
-Select-	

Choose Attributes holding IPAddress & Hostname:

IP Address Attribute	Host Name Attribute
-Select-	-Select-

Choose Attributes holding Account Name:

Account Name Attribute

Sender

Expiry Duration (In Minutes)

480

IP Addresses assigned via DHCP may expire after a time period. Provide an expiry time for the Account name - IP Address information recorded.

SAVE

- Events Matching Criteria:**
 - Transaction Attribute:** Select an available attribute from dropdown and enter a value. Example: transactionstring1.
 - Transaction:** Enter a value for the datasource from which you want to attribute IP Addresses. Example: 4624: An Account was successfully logged on (Active Directory).

b. **Choose Attributes holding IP Address and Hostname:**

a. **IP Address Attribute:** Select an available attribute from dropdown.

Example: IP Address.

b. **Host Name Attribute:** Select an available attribute from

dropdown: Example: Destination Host Name.

c. **Choose Attributes holding Account Name:**

a. **Account Name Attribute:** Select the attribute that holds an account name.

Example: Accountname.

d. **Expiry duration (In Minutes):** Enter the duration of time in which to maintain the IP Address to Account Name Relationship. Example: 1,440 (24hrs).

Derived Fields

If you would like to include a file name in activity events but the field is not included in the mapped attributes for this datasource, you can include a Derived Field to extract the information from the event data.



Note: You may only extract attributes which exist in the event data. If you select an attribute that does not exist in the event data, the field will be left blank in the raw event and results on the UI and in Spotter.

Click **+ Add New** to define custom parsing rules for log events and **Save**.

- **Attribute Name:** Specifies the name of the attribute in the datasource. Map With: Select a corresponding attribute from the dropdown.
- **Format:** Specify a DATETIME format if required or proceed to next field.
- **Description:** Enter a brief a description of the attribute.
- **Indexed?:** Toggle to **Yes** to index the attribute in Solr to be available in Spotter search results. Toggle to No to exclude the field from Spotter search results.
- **Display on UI?:** Toggle to **Yes** to display the attribute in results on the UI. Select No to exclude the field from results on the UI.
- **Is Multivalued?:** Toggle to **Yes** if the attribute has multiple values separated by a delimiter and specify **Delimiter**.
- **Populate Using Function:** Click **Select Function** to view and select available functions/formulas to perform operations on attribute values.

To populate derived fields using functions, complete the following:

1. Click the function you would like to use to populate the field in the dialog window.
2. Click **field** for each attribute to be populated.
3. Select an **Activity Attribute** from the dropdown OR enter a **Constant** value.
4. Click **Add**.
5. Click **Add** on Populate Using Function.

For a complete list of available functions, see [Appendix B: Functions](#).

Example: Extract a file name from an activity event

To use functions to extract a file name from an activity event, complete the following steps:

1. Click **Add New** in the Derived Fields section.
2. Enter an Attribute Name: Example: FileName.
3. Select the attribute to Map With. Example: filename.
4. Enter a brief **Description** (optional).
5. Click **Select Function** for Populate Using Function.

The screenshot shows a modal window titled "DERIVED FIELDS (AVAILABLE:0)" with a green "+ Add New" button. The modal contains the following fields and options:

- Attribute Name:** A text input field.
- Map With:** A dropdown menu currently showing "-Select-".
- Description:** A text input field.
- Populate Using Function:** A section with a blue "SELECT FUNCTION" link and a blue "X" icon.
- Indexed?:** A toggle switch set to "YES".
- Display on UI?:** A toggle switch set to "YES".
- Is Multivalued?:** A toggle switch set to "NO".
- Save:** A blue button at the bottom right.

6. Click **String Functions**.

Populate Using Function ✕

i Function/Formula are used to perform operations on attribute value. You can create Formula or select Function from below.

Logical Functions Math Functions Other Functions **String Functions** Formula

TO_UPPER	Converts the string read to upper case. Only one parameter which is the attribute name of the parameter to convert. E.g. : TO_UPPER(attr1)
TO_LOWER	Converts the string read to lower case. Only one parameter which is the attribute name of the parameter to convert. E.g. : TO_LOWER(attr1)
CONCATENATE	Concatenate the list attributes or constant. Pipe separated list of attributes and/or constants. E.g. : CONCATENATE(attr1 'abc' attr3)
CONSTANT	Replaces the destination attribute to a given constant. E.g. : CONSTANT('abc')
TRIM	Trims the given attribute. Only one parameter which is the attribute name of the parameter to convert. E.g. : TRIM(attr1)
REGEX_TOKEN	Returns the first token match for the given string. Two parameter first being the attribute name and second being the regex token. E.g. : REGEX_TOKEN(attr1 'fo+(o.*)'(r)')
TOP_LEVEL_DOMAIN	Extracts the top level domain of any url. Only one parameter which contains the hostname. E.g. TOP_LEVEL_DOMAIN
FILE_EXTENSION_EXTRACTOR	Get file extension.(c:/temp/test.txt returns txt) Only one parameter which is the attribute name of the parameter to convert. E.g. : FILE_EXTENSION_EXTRACTOR(attr1)

7. Select FILE_NAME_EXTRACTOR from list.

Populate Using Function ✕

CONSTANT	E.g. : CONSTANT('abc')
TRIM	Trims the given attribute. Only one parameter which is the attribute name of the parameter to convert. E.g. : TRIM(attr1)
REGEX_TOKEN	Returns the first token match for the given string. Two parameter first being the attribute name and second being the regex token. E.g. : REGEX_TOKEN(attr1 'fo+(o.*)'(r)')
TOP_LEVEL_DOMAIN	Extracts the top level domain of any url. Only one parameter which contains the hostname. E.g. TOP_LEVEL_DOMAIN
FILE_EXTENSION_EXTRACTOR	Get file extension.(c:/temp/test.txt returns txt) Only one parameter which is the attribute name of the parameter to convert. E.g. : FILE_EXTENSION_EXTRACTOR(attr1)
FILE_NAME_EXTRACTOR	Get file name.(c:/temp/test.txt returns test). Only one parameter which is the attribute name of the parameter to convert. E.g. : FILE_NAME_EXTRACTOR(attr1)
FILE_PATH_EXTRACTOR	Get file path.(c:/temp/test.txt returns c:/temp) Only one parameter which is the attribute name of the parameter to convert. E.g. : FILE_PATH_EXTRACTOR(attr1)
LENGTH	Replaces the destination attribute to the length of given attribute. Only one parameter which is the attribute name of the parameter to convert. E.g. : LENGTH(attr1)

8. Scroll back to the top of the dialog box.

- Click **Field**.

Populate Using Function

Function/Formula are used to perform operations on attribute value. You can create Formula or select Function from below.

FILE.EXTENSION_EXTRACTOR(field)

Logical Functions Math Functions Other Functions String Functions Formula

- Select a Field from the Select Activity Attribute dropdown. Example: DocTitle.

Select Field

DocTitle

DestinationFolderID

DestinationFolderTitle

DocID

DocOwner

DocTitle

DocType

- Click **Add**.
- Click **Add** on the **Populate Using Function** screen.
- Enable **Indexed?** to index the attribute in Solr to be available in Spotter search results. Disable to exclude the field from Spotter search results.
- Enable **Display on UI?** to display the attribute in results on the UI. Disable to exclude the field from results on the UI.

The Derived Field will show the available attribute. To remove the Derived Field, click **Delete**.

DERIVED FIELDS (AVAILABLE:1)

+ Add New

FileName

filename

Attribute Name

FileName

Map With

filename

Description

Populate Using Function

FILE_NAME_EXTRACTOR(\\") X

Indexed?

YES

Display on UI?


YES

DELETE Save

Click **Save & Next** when all Action Filters are configured to proceed to [Step 4: Configuring Identity Attribution](#).

Step 4: Configuring Identity Attribution

The ArcSight UBA application associates events with user identities according to correlation rules. You can use account names that appear in event IP Addresses to perform this association. If you specify multiple rules, the rules are evaluated in the order in which they appear. ArcSight UBA stores the correlation rules you create so you can apply them to multiple data feeds.

 **Note:** You can view correlated and uncorrelated accounts for the data source in **Menu > Views > Resources**. See [Views](#) in the User Guide for more information about Resources.

This section describes how to create correlation rules to attribute identities to events.

Correlation Rules

4

Resource Type Information

Parsing & Normalization

Conditional Actions

Identity Attribution

Summary

Associate events to user identities by specifying rules below. You can use account names that appear in events IP addresses to perform this association. If you specify multiple rules, the rules are evaluated in the order in which they appear.

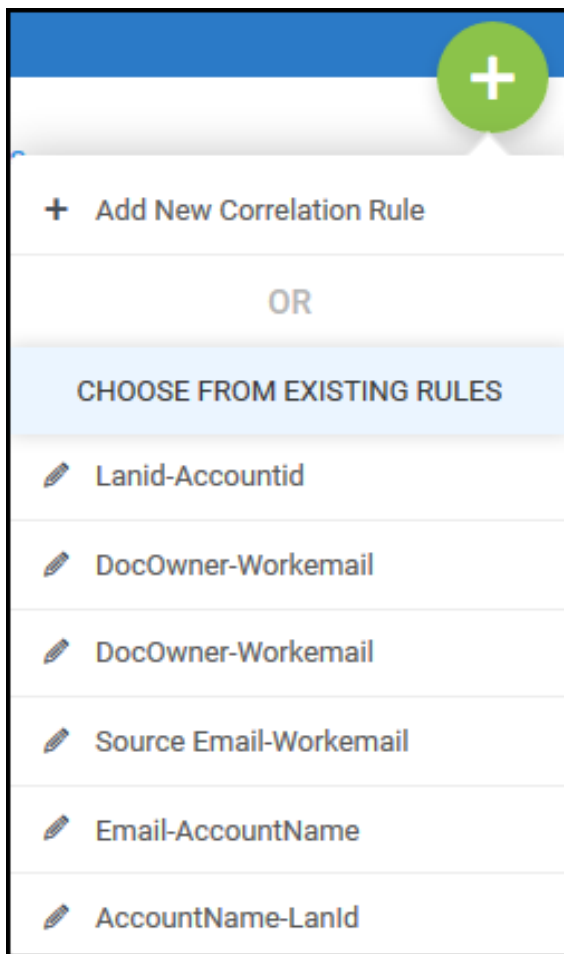
+

Correlation Rules

Employeeid_Workemail

Synchronized with HBase

1. Click **+** to add a **Correlation Rule**.



2. Select **Add New Correlation Rule** or **Choose from Existing Rules**:

a. **Add New Correlation Rule:**

CORRELATION RULE

Correlation Rule Name: Select Event Field:

CORRELATE EVENTS TO USER USING RULE

User Attribute	Operation	Parameter	Condition	Separator	Add/Delete
<input type="text" value="firstname"/>	<input type="text" value="Postfix"/>	<input type="text" value="."/>	<input type="text" value="AND"/>	<input type="checkbox"/>	
<input type="text" value="lastname"/>	<input type="text" value="Select an Option"/>	<input type="text"/>	<input type="text" value="Select an Option"/>	<input type="checkbox"/>	

[CANCEL](#) [SAVE](#)

- Correlation Rule Name:** Enter a descriptive name for the correlation rule.
- Select Event Field:** Select an event to which to correlate users. Example: Email.
- Correlate Event to User Using Rule:**
 - User Attribute:** Select the user attribute from the dropdown. Example: employeeid.
 - Operation:** Select an operation from the dropdown. Examples: Trim Right, Trim Left, Prefix, Postfix.
 - Parameter:** Enter a parameter if you select an **Operation**.
 - Condition:** Select a condition from the dropdown. Default AND.
 - Separator:** Click check box to specify a separator and enter separator value.
 - +/-:** Add/remove rules.

b. **Choose from Existing Rules:** Complete any edits.

CORRELATION RULE

Select Event Field:

CORRELATE EVENTS TO USER USING RULE

User Attribute	Operation	Parameter	Condition	Separator	Add/Delete
<input type="text" value="employeeid"/>	<input type="text" value="None"/>		<input type="text" value="AND"/>	<input type="checkbox"/>	




[CANCEL](#) [SAVE](#)

- Click **Save** to save rules.
- View **Correlation Rules** applied to this datasource in the left navigation pane.

Associate events to user identities by specifying rules below. You can use account names that appear in events IP addresses to perform this association. If you specify multiple rules, the rules are evaluated in the order in which they appear.

Correlation Rules




Employeeid_Workemail
Synchronized with HBase



Note: The correlation rule is automatically synchronized and stored in HBase.

You can perform the following actions for the Correlation Rule:

	Re-Sync rule with HBase.
	Edit correlation rule.
	Remove rule from datasource. Note: This will not delete the rule from HBase. The rule will be available for other datasources.

- Click **Save & Next** to proceed to [Step 5: Reviewing Import Summary](#).

Step 5: Reviewing Import Summary

This section describes the features of the **Summary** screen and how to run the activity data import job.

Activity Import Summary

Save Template

DEVICE TYPE INFORMATION

Datasource Name	IP Address
PaloAlto	
Vendor	Functionality
Palo Alto Networks	Firewall / NGFW / WAF
Resource Type	
Firewall	

COLLECTION METHOD

Method
file
All Files Matching Condition
Prefix : pal
Show more

LINE FILTERS

Search

All Lines

No of Fields : 19

YES

POLICIES

CREATE

YES	Suspicious Network Activity TOR	
YES	Suspicious Bytes Out Bytes In ratio Proxy	
NO	Communication to Proxy Anonymizer Sites-27	
	This policy looks for any successful communication to a proxy anonymizing site	
NO	Network Firewall: Communication over Anomalous Ports-28	
NO	Possible Flight Risk Users-28	
NO	High Number of Blocked Attempts in an Hour-28	
NO	High Amount of Data Exfiltrated to Storage Sites-28	
NO	Spike in Amount of Data Uploaded-28	
NO	Potential beaconing activity	
NO	Connection to malicious destination	
NO	Spike in high number of bytes out	
NO	Possible Flight Risk User	
NO	Flight Risk User watchlist	
NO	Communication to malicious website	

The **Summary** screen displays the **Activity Import Summary** which includes the following:

- Device Type Information
- Collection Method
- Line Filters
- Correlation Rules
- Action Filters
- Policies
- Threat Models

From this screen, you can complete the following actions:

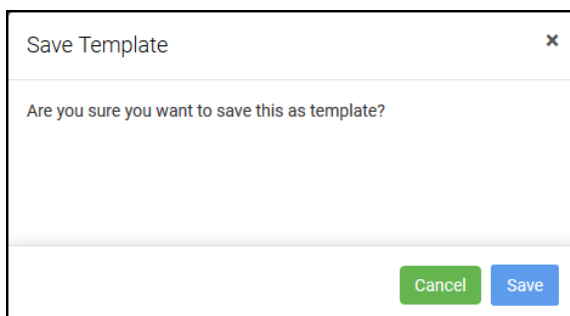
- Review the import
- Save the import template
- Enable/disable line filters
- Create a policy for this datasource
- Schedule the job

Review the Import

1. Review the **Device Type Information, Policies, Behavior Profiles, Collection Method, Line Filters, Correlation Rules, and Action Filters.**
2. Click **Prev** to return to any screens you wish to edit.

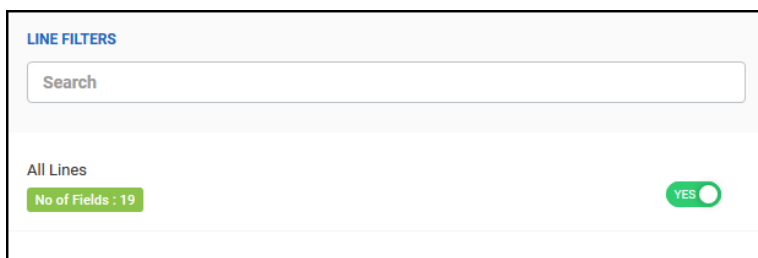
Save the Import Template

1. Click **Save Template.**
2. Click **Save** to confirm in the pop up window.



Enable/Disable Line Filters

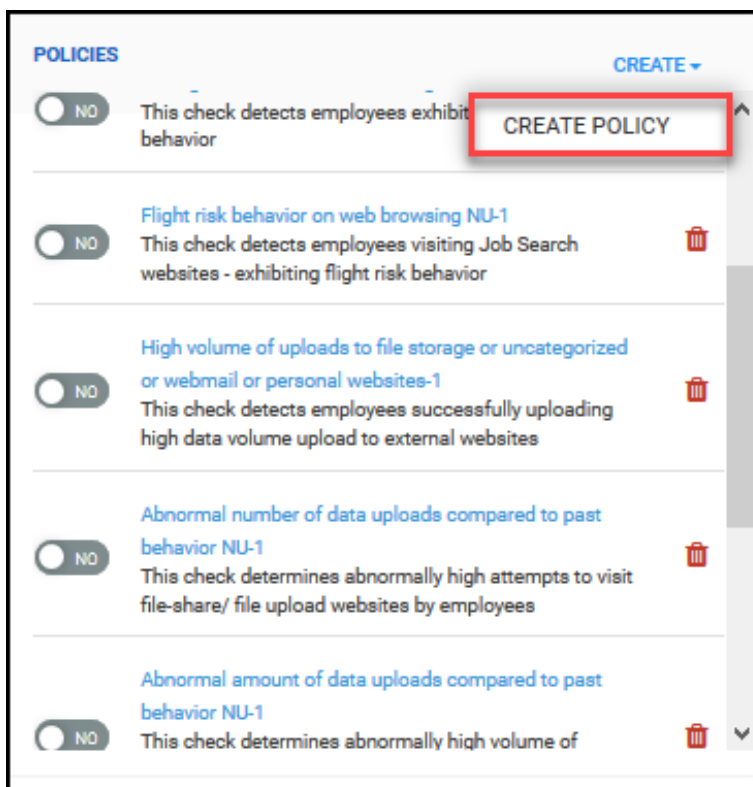
1. Set slider to **YES** or **NO** to enable or disable line filters.



Activity Data

Create a Policy

1. Click **Create** in the **Policies** section and select **Create Policy** from dropdown.



2. Complete the Create Policy form.

DEFINE POLICY

Policy Name*

Provide unique name which will describe what type of violation it detects. Special characters are not allowed. Example: (- (bracket), ' - (single quote) are not allowed

Description

Criticality

Low

Select the criticality of the policy. The criticality affects the risk score for the user. None=0.0, Low=0.2, Medium=0.6 and High=1.0

Do you want to save violations and calculate risk scores for this policy?

YES

If Yes, violations will be searchable in Spotter and risk scores will be calculated for violators. If No, violations will not be searchable and risk scores will not be calculated for violators of this policy.

Do you want to escalate this policy as a Threat?

YES

If Yes, this policy will be escalated as a Threat instead of a Violation and will appear under Top Threats in Security Command Center. If no, this policy will appear under the Top Violations widget.

Select Violation Entity*

-Select-

Select the entity that the risk should apply to?

Users - Returns list of users violating policy. Orphan accounts(or uncorrelated accounts) will be ignored.Users cannot be used in behavior based policy.

ActivityAccount - Returns list of activity accounts (both correlated and uncorrelated) violating the policy.

Resources - Returns list of resources violating the policy.

Resource Group Account - Returns list of activity accounts across datasources (both correlated and uncorrelated) violating the policy.

Do you want to run the policy on a

☒ Datasource
☐ Functionality



Note: For information about how to configure policies for datasources, see [Policy Violations](#).

Step 6: Running the Job


Complete the following steps to schedule and run the activity import job:

JOB SCHEDULING INFORMATION

☒ Do you want to run job Once ?

☐ Do you want to run this job every seconds ?

☐ Do you want to schedule this job for future ?

 Job will be scheduled according to the server time. Current server time is - 5/1/2017 15:12:46

JOB DETAILS

Job Name

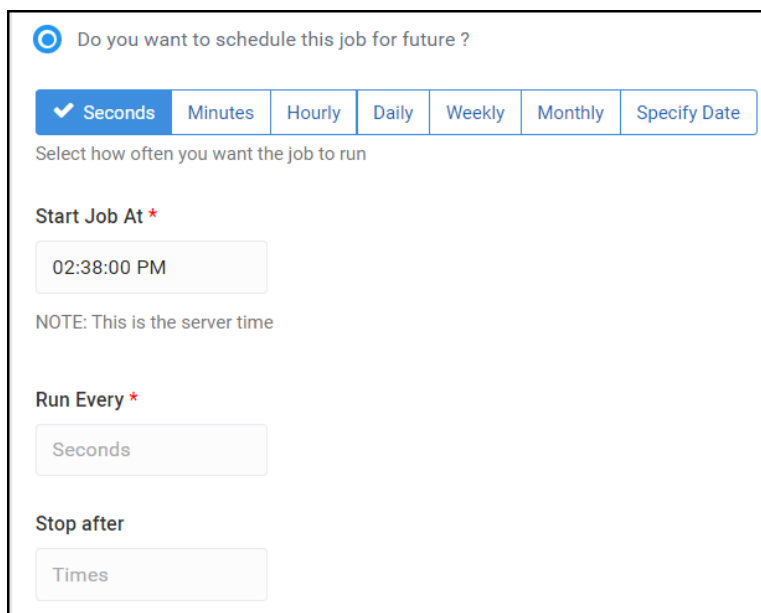
Enable Job Related Notifications

☐ NO

Set job related notifications to "Yes" if you want to send emails upon job success/failure.

Job Scheduling Information

1. Select when you would like the job to run.
 - Select **Do you want to run job Once?** to run now.
 - Select **Do you want to run this job every [10] seconds?** and fill in a value to run the job incrementally.
 - Select **Do you want to schedule this job for future?** to run the job later and complete the relevant fields.



The screenshot shows a web form titled "Do you want to schedule this job for future ?". It features a row of tabs: "Seconds" (selected with a checkmark), "Minutes", "Hourly", "Daily", "Weekly", "Monthly", and "Specify Date". Below the tabs is the instruction "Select how often you want the job to run". The form has three main sections: "Start Job At *" with a text input field containing "02:38:00 PM" and a note "NOTE: This is the server time"; "Run Every *" with a text input field containing "Seconds"; and "Stop after" with a text input field containing "Times".

Job Details

1. Enter a unique **Job Name** or use the default name.
2. Toggle **Increment Import** to **Yes** if you would like to run the job in increments.
3. **Enable Job Related Notifications** if you would like to receive email notifications when the job is run.
 - a. If **No**: Proceed without entering additional information.
 - b. If **Yes**:
 - **On Success**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template.
 - **On Failure**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template.

- **On Misfired:** Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template.
- **On Completed with Errors:** Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template:

Create New Email Template

Sender Name* ⓘ

Template Name* ⓘ

Description

To* ⓘ

From*

test@securonix.com

CC ⓘ

BCC ⓘ

Subject ⓘ

HTML Enabled

☒ YES

Store in Outbox prior to sending?

☒ YES

Use this template for *

Job Misfired

Owner ⓘ

Administrators

SECURITYOPERATIONS

Email Body ⓘ

[Add Email Template Variables](#)

Rich text editor toolbar with icons for bold, italic, underline, text color, background color, bulleted list, numbered list, link, unlink, insert image, insert video, insert table, insert code, undo, redo, and other formatting options.

4. Click **Save & Run**.

Review Job Status

Review the job status to ensure data was loaded successfully:

Job Name	Creation Date	Start Date	Next Trigger Date	Job Status
CERNER HEALTHCARE DATA_DELIMITED-SEMICOLON_10_30_2017_06_55_24_PM CREATED BY: ADMIN / JOB TYPE: ACTIVITY IMPORT EDIT JOB RE-RUN JOB DELETE JOB	MON, 30 OCT 2017 @ 06:55:26.000 PM	START DATE: MON, 30 OCT 2017 @ 06:55:26.000 PM	NOT SCHEDULED	NOT AVAILABLE
CERNER HEALTHCARE DATA_DELIMITED-SEMICOLON_10_30_2017_06_49_51_PM CREATED BY: ADMIN / JOB TYPE: ACTIVITY IMPORT EDIT JOB RE-RUN JOB DELETE JOB	MON, 30 OCT 2017 @ 06:49:54.000 PM	START DATE: MON, 30 OCT 2017 @ 06:49:54.000 PM	NOT SCHEDULED	NOT AVAILABLE
DIGITAL GUARDIAN USB_DELIMITED-PIPE_10_30_2017_06_46_30_PM CREATED BY: ADMIN / JOB TYPE: ACTIVITY IMPORT EDIT JOB RE-RUN JOB DELETE JOB	MON, 30 OCT 2017 @ 06:46:32.000 PM	START DATE: MON, 30 OCT 2017 @ 06:46:32.000 PM	NOT SCHEDULED	NOT AVAILABLE
CERNER HEALTHCARE DATA_DELIMITED-SEMICOLON_10_30_2017_06_39_10_PM CREATED BY: ADMIN / JOB TYPE: ACTIVITY IMPORT EDIT JOB RE-RUN JOB DELETE JOB	MON, 30 OCT 2017 @ 06:39:13.000 PM	START DATE: MON, 30 OCT 2017 @ 06:39:13.000 PM	NOT SCHEDULED	NOT AVAILABLE

Search using Spotter

Upon successful import, the event data will be available for searching in Spotter. To search events in Spotter, complete the following steps:

1. Navigate to **Menu > Security Center > Spotter**.
2. Click the datasource name on the Spotter **Summary** screen.

AVAILABLE VIOLATIONS		AVAILABLE DATASOURCES	
Access to Java Files by Non-Engineering Dept [O-DRV]	1,230,700	GDriveLogs	16,914,470
Drive Permissions to External Domain [O-DRV]	1,230,690	GoogleDriveLogs	2,938,799
Access to License Files by Sales Department [O-DRV]	1,230,690	Securonix Palo Alto Traffic	436,006
Drive Permission Set to Self [O-DRV]	488,528	AD Events	70,715
Activities on Sensitive Files [O-DRV]	7,007	Securonix Amazon Web Services	50,225
Logon Failure Database_testDB	232	GoogleLogin	15,099
AD Events - High no of logon failures by an account	112	TestDB	14,642
Proxy Landispeed Violation	4	VPNL	6,732
Detecting audit log tampering	4	Sophos	3,427
land speed violation Policy	2	SharepointCovTest	869



Note: Click for more information about searching [Spotter](#) or see the *ArcSight UBA User Guide*.

Third Party Intelligence

The ArcSight UBA application can use intelligence about IP addresses and hostnames that have been classified by open source trackers. Out of the box, the application comes with connectors to highly trusted Third Party Intelligence (TPI) sources to import IP addresses and the domain names that are malicious and black-listed. The main focus of this is to detect these hosts well in advance and avoid potential infections.

The ArcSight UBA application uses intelligence from third-party sources to add value to the events seen from sources like DLP, web gateways or proxies, and firewall. The ArcSight UBA application normalizes these different data feeds from the third-party sources using its built-in parsers and uses the normalized data in its Intelligence Engine.

The ArcSight UBA application brings in its intelligence by importing the list of malicious IP addresses and domains from these sources and looks for the presence of these addresses or domains in the activity events, adding additional value and enriching event data.

The connection details for the TPI data sources are provided out of the box with the ArcSight UBA application. Some of the data sources for the blacklisted IPs/domains are listed below:

- CIAmyIP lists
- ZeusIP and Domain lists
- SagaDC lists
- Palevo IP and Domains list
- Spyeye and Domains list

Third Party Intelligence is enabled during [Activity Data](#) during Step 3: Performing Conditional Actions.

You can import Third Party Intelligence from existing sources or create a new connection.

Steps to import from an existing source:

1. Preview input.
2. (Optional) Edit connection details and/or mapped attributes.
3. Schedule the job.

Steps to import a new Third Party Intelligence source:

1. Create a connection to import from the following sources:
 - [Importing TPI from a File](#)
 - [Importing TPI from the Web](#)
 - [Importing TPI from ThreatStream](#)
 - [Importing TPI from ThreatStream](#)
2. Map Attributes with corresponding ArcSight UBA attributes.
3. Schedule and run the job.

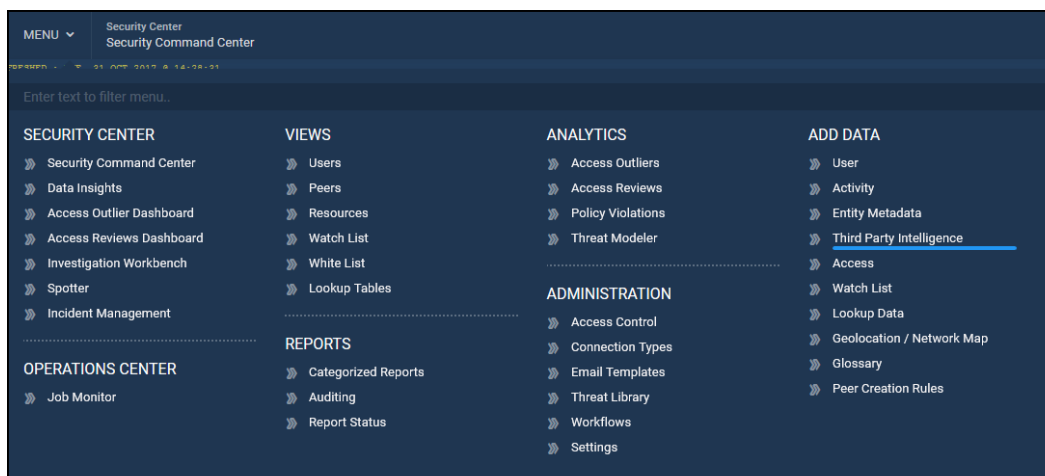
Ingesting Third Party Intelligence



Step 1: Importing Third Party Intelligence from an Existing Connection

To import TPI Data from an existing pre-configured source, complete the following steps:

1. Navigate to **Menu > Add Data > Third Party Intelligence**.



2. Click the name of the datasource from which you would like to import TPI or search existing connections.




3. **Preview Input** on the right side of the screen.
4. Click **Save and Next** to Proceed to [Step 3: Scheduling the Job](#).

(Optional) Editing an Existing Connection

To edit an existing connection, complete the following steps:



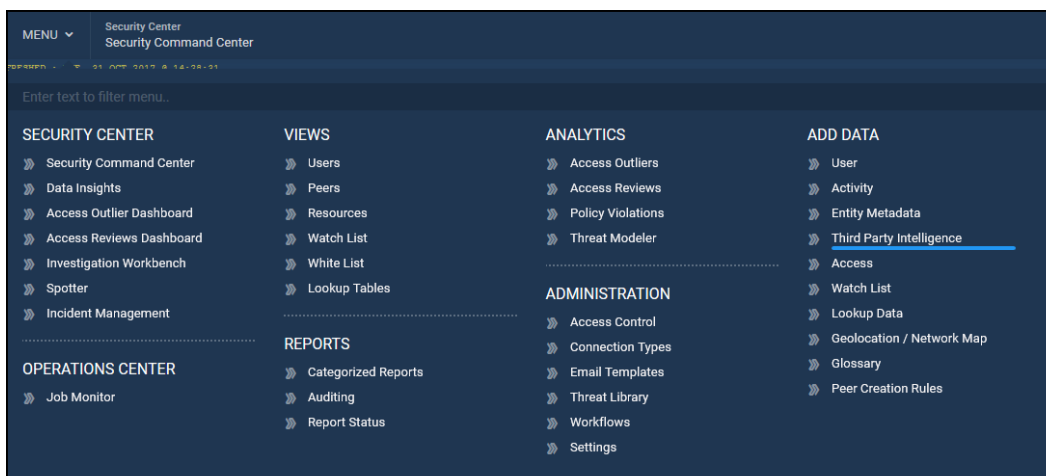
1. Click  icon to edit details.
2. Edit information for **Connection Properties**. For information about how to configure the connection, see [Importing TPI from the Web](#)
3. Edit information for **Attribute Mapping**. For information about how to map attributes, see [Step 2: Mapping Attributes](#).
4. Proceed to [Step 3: Scheduling the Job](#).

Step 1: Creating a New Connection

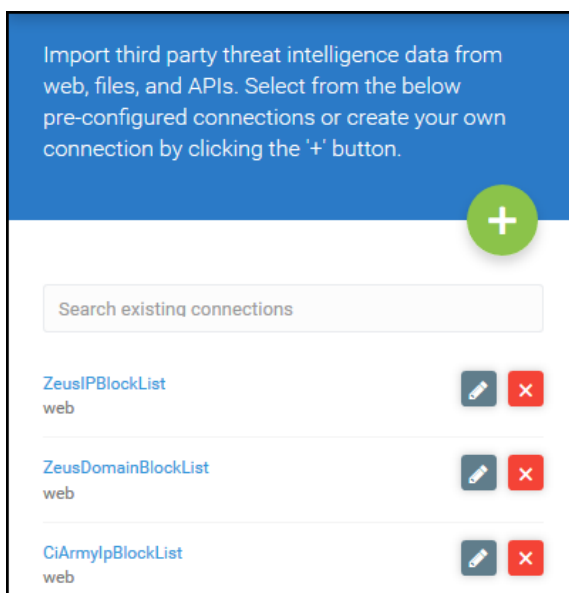
You can import Third Party Intelligence from web, files, and APIs using pre-configured connections or by creating your own connection.

To import Third Party Intelligence, complete the following steps:

1. Navigate to **Menu > Add Data > Third Party Intelligence**.



2. Click **+** to add a new connection.



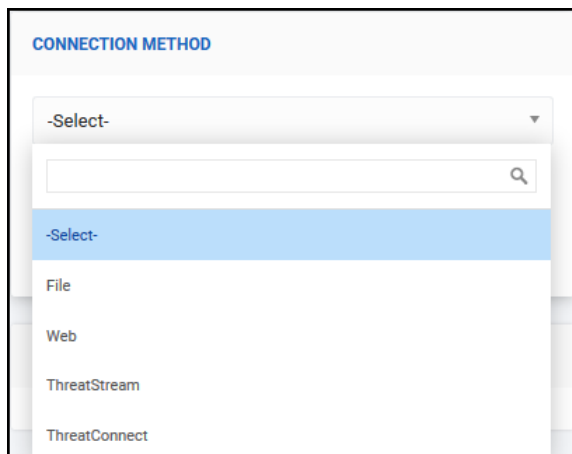
Connection Name

Enter a unique **Connection Name**.

A screenshot of the 'New Connection' form in the ArcSight Security Center. The form has a light gray background. At the top, it says 'CONNECTION NAME' in blue. Below that is a text input field with the placeholder text 'New Connection'. At the bottom, there is a note: 'Provide a name to uniquely identify this connection.'

Connection Method

Select a **Connection Method** from the dropdown.



Note: The Collection Method determines the steps to configure Connection Properties.

Importing TPI from a File

To import TPI from a file, first complete the previous steps for [Step 1: Creating a New Connection](#).

Connection Properties

Complete the following information:

CONNECTION PROPERTIES

File Name*

Name of the file to be downloaded from web or to be imported. The file needs to be located at:
\${SECURONIX_HOME}/import/in

TPI Type*

Malicious Domain ▼

Type of the intelligence data to be imported.

Parser Type*

Delimited ▼

Type of parser to be used to parse the data.

Delimiter*

Contains Quote Character

☐ NO

Values in the delimited file enclosed by a quote.

**Indicates required field*

- a. **File name:** Enter the file name to be imported. Example: maliciousdomains.csv.



Note: The file must be located in \${SECURONIX_HOME}/import/in

- b. **TPI Type:** Select a type of third party intelligence from the dropdown. Example: Malicious Domain.
- c. **Parser type:** Select from the dropdown.
- Delimited:** Specify a **Delimiter**. Example: , (comma).
 - RegEx:** Specify a **Regular Expression**. Example: ^(\S+)\$.

Additional Settings

Complete the following information:

ADDITIONAL SETTINGS

Exclude Header
☒ YES
Include/Exclude Headers from input file.

Header Lines

Exclude Footer
☐ NO
Include/Exclude Footers from input file.

Criticality*

Assign a confidence for the threat data to be imported [None=0.0, Low=0.3, Medium=0.6, High=1.0].

Modify Criticality?
☒ YES

Modify Criticality?
☒ YES

Modification Type

-Select-

Normalize

String

a. **Exclude Header?:** Toggle to **Yes** to exclude headers from input file.

a. **No:** Proceed to next step. Header will be included.

b. **Yes:** Specify the number of **Header Lines** to exclude.

b. **Criticality:** Select a criticality from the dropdown. Example: High.



Note: Criticality assigns a confidence for the threat data to be imported on the following scale: None=0.0, Low=0.3, Medium=0.6, High=1.0.

c. **Modify Criticality?:** Toggle to **Yes** to modify the criticality.

a. **No:** Proceed to **More Settings**.

b. **Yes:** Select a **Modification Type** from the dropdown and set criticality.

- **Normalize:** When the criticality is provided as a numerical value, if the input file has ratings from 0-10 indicating criticality, the following configuration will normalize the criticality rating to None for 0, Low for 1-3, Medium for 4-6, and High for 7-10.

Modify Criticality?
☒ YES

Modification Type
Normalize ▼

Set None	When criticality is =0
Set Low	When criticality is >=1
Set Medium	When criticality is >=4
Set High	When criticality is >=7

**Indicates required field*

- **String:** When the criticality is provided as a string, the application will set the appropriate criticality for each of the criticality string conditions provided.

Modification Type

String ▼

Set None	When criticality is None
Set Low	When criticality is Low
Set Medium	When criticality is Medium
Set High	When criticality is High

**Indicates required field*

More Settings

Complete the following information:

MORE SETTINGS

`${SECURONIX_HOME}` is set to `/Securonix/tenants/four/snypr6/securonix_home`.
You can also replace `${SECURONIX_HOME}` below with the direct path to the folder where the file exists.
Example: `/Users/dev/files/`

Source Folder*

Enter the complete path to the directory where this file is located.

Success Folder*

Enter the complete path to the directory where this file must be moved once the import is completed successfully.

Failed Folder*

Enter the complete path to the directory where this file must be moved if the import job fails to complete.

***Indicates required field**

- Success Folder:** Specify the folder into which you would like the file to move upon successful upload. Default: `/Securonix/ArcSight/uba6/securonix_home/import/success/`
- Failed Folder:** Specify the folder into which you would like the file to move upon a failed upload. Default: `/Securonix/ArcSight/uba6/securonix_home/import/failed/`
- Staging Folder:** Specify the staging folder (required for data requiring preprocessing). Default: `/Securonix/ArcSight/uba6/securonix_home/import/in/`

Preview Input

1. **Preview Input** to ensure the data has uploaded successfully.

PREVIEW INPUT	GET PREVIEW
101.200.81.187	
103.19.89.118	
103.230.84.239	
103.26.128.84	
103.4.52.150	
103.7.59.135	
104.238.158.106	
107.161.186.90	
108.174.157.123	
109.127.8.242	
109.229.210.250	
109.229.36.65	
113.29.230.24	
120.31.134.133	
120.63.157.195	
123.30.129.179	

2. Click **Save and Next** to proceed to [Step 2: Mapping Attributes](#).

Importing TPI from the Web

To import TPI from the web, first complete the previous steps for [Step 1: Creating a New Connection](#).

Connection Properties

Complete the following information:

CONNECTION PROPERTIES

URL*

URL from which the data will be downloaded.

File Name*

Name of the file to be downloaded from web or to be imported. The file needs to be located at:
\${SECURONIX_HOME}/import/in

TPI Type*

Malicious Domain ▼

Type of the intelligence data to be imported.

Parser Type*

Regex ▼

Type of parser to be used to parse the data.

Regular Expression*

**Indicates required field*

- URL:** Enter the URL from which the data will be downloaded.
Example: https://zeustracker.abuse.ch/blocklist.php?download=domainblocklist.
- File Name:** Enter the name of the file to be downloaded. Example: zeusdomainblocklist.txt.
- TPI Type:** Select the type of third party intelligence from the dropdown. Example: Malicious Domain.
- Parser type:** Select from the dropdown.
 - Delimited:** Specify a **Delimiter**. Example: , (comma).
 - RegEx:** Specify a **Regular Expression**. Example: ^(\\S+)\$.

Additional Settings

Complete the following information:

ADDITIONAL SETTINGS

Exclude Header
☒ YES
Include/Exclude Headers from input file.

Header Lines

Exclude Footer
☐ NO
Include/Exclude Footers from input file.

Criticality*

Assign a confidence for the threat data to be imported [None=0.0, Low=0.3, Medium=0.6, High=1.0].

Modify Criticality?
☒ YES

Modify Criticality?
☒ YES

Modification Type

-Select-

Normalize

String

- a. **Exclude Header?:** Toggle to **Yes** to exclude headers from input file.
- a. **No:** Proceed to next step. Header will be included.
 - b. **Yes:** Specify the number of **Header Lines** to exclude.

- b. **Criticality:** Select a criticality from the dropdown. Example: High.



Note: Criticality assigns a confidence for the threat data to be imported on the following scale: None=0.0, Low=0.3, Medium=0.6, High=1.0.

- c. **Modify Criticality?:** Toggle to **Yes** to modify the criticality.
 - a. **No:** Proceed to **More Settings**.
 - b. **Yes:** Select a **Modification Type** from the dropdown and set criticality.

- **Normalize:** When the criticality is provided as a numerical value, if the input file has ratings from 0-10 indicating criticality, the following configuration will normalize the criticality rating to None for 0, Low for 1-3, Medium for 4-6, and High for 7-10.

Modify Criticality?
☒ YES

Modification Type
Normalize ▼

Set None	When criticality is =0
Set Low	When criticality is >=1
Set Medium	When criticality is >=4
Set High	When criticality is >=7

**Indicates required field*

- **String:** When the criticality is provided as a string, the application will set the appropriate criticality for each of the criticality string conditions provided.

Modification Type

String ▼

Set None	When criticality is None
Set Low	When criticality is Low
Set Medium	When criticality is Medium
Set High	When criticality is High

**Indicates required field*

More Settings

Complete the following information:

MORE SETTINGS

`${SECURONIX_HOME}` is set to `/Securonix/tenants/four/snypr6/securonix_home`.
You can also replace `${SECURONIX_HOME}` below with the direct path to the folder where the file exists.
Example: `/Users/dev/files/`

Source Folder*

Enter the complete path to the directory where this file is located.

Success Folder*

Enter the complete path to the directory where this file must be moved once the import is completed successfully.

Failed Folder*

Enter the complete path to the directory where this file must be moved if the import job fails to complete.

***Indicates required field**

- Success Folder:** Specify the folder into which you would like the file to move upon successful upload. Default: `/Securonix/ArcSight/uba6/securonix_home/import/success/`
- Failed Folder:** Specify the folder into which you would like the file to move upon a failed upload. Default: `/Securonix/ArcSight/uba6/securonix_home/import/failed/`
- Staging Folder:** Specify the staging folder (required for data requiring preprocessing). Default: `/Securonix/ArcSight/uba6/securonix_home/import/in/`

Preview Input

1. **Preview Input** to ensure the data has uploaded successfully.

PREVIEW INPUT	GET PREVIEW
039b1ee.netsoihost.com	
03a6b7a.netsoihost.com	
03a6f57.netsoihost.com	
03b6ec4.netsoihost.com	
0f1n16.org	
0x.x.gg	
1st.technology	
54g35546-5g5nbgffhb.sk	
76tgy6bh6gfrn7tg.su	
afobal.cl	
afrirent.net	
ahmedashid.com	
akdenizklima.com.tr	
aljazeera.kz	
allfortune777.biz	
analiticwebexperience.com	

2. Click **Save and Next** to proceed to [Step 2: Mapping Attributes](#).

Importing TPI from ThreatStream

ThreatStream combines threat data from feeds and other sources. ArcSight UBA accesses ThreatStream threat intelligence feed through Anomali API in JSON format.

Prerequisites for Importing TPI from ThreatStream

Ensure you have the following before importing TPI using the ThreatStream API:

- **API Username:** The unique username in email format for the Anomali API account.
- **API Key:** The 20-digit alphanumeric key for the Anomali API account.
- **API Base URL:** The base URL for your account.
- **API Resource:** The type of resource: intelligence, snapshot, or tipreport.
- **API Resource Version:** The version of the API resource: v1 or v2.
- (Optional) **API Query Conditions:** The optional query condition for filtering out data.
Example: itype=bot_ip.

To import TPI from ThreatStream, first complete the previous steps for [Step 1: Creating a New Connection](#)

Connection Properties

Complete the following information:

CONNECTION PROPERTIES

API Username*

Username to connect to the API.

API Key*

API Key tied to the Username above.

API Base URL*

Base URL of the API.

API Resource*

Resource from which the threat data needs to be imported.

API Resource Version*

Version of the Resource type

API Query Conditions

Conditions to filter out any data.

TPI Type*

ThreatStream import is always of the TPI type ThreatStream.

***Indicates required field**

- a. **API Username:** Enter the username for API account in email format.
- b. **API Key:** Enter the 20-digit alphanumeric key for the API account.
- c. **API Base URL:** Enter the base URL for the API account.
- d. **API Resource:** Select type of resource from the following options: intelligence, snapshot, tip-report.
- e. **API Resource Version:** Select the Resource version from the dropdown.
- f. (Optional) **API Query Conditions:** Enter an optional query condition. Example: itype=bot_ip.
- g. **TPI Type:** Proceed to next step. ThreatStream is always the TPI type for ThreatStream and is selected by default.

Additional Settings

Complete the following information:

ADDITIONAL SETTINGS

Exclude Header
☒ YES
Include/Exclude Headers from input file.

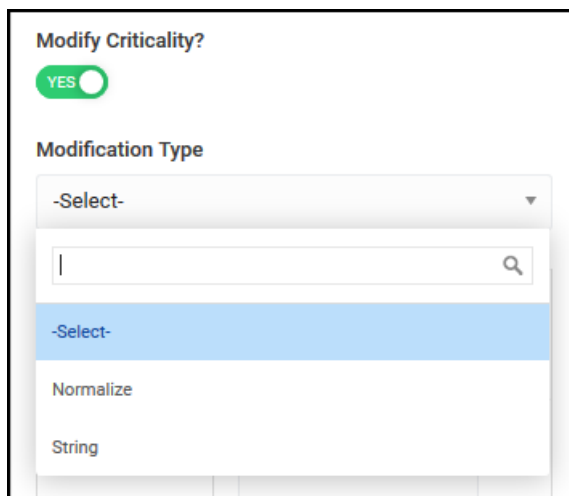
Header Lines

Exclude Footer
☐ NO
Include/Exclude Footers from input file.

Criticality*

Assign a confidence for the threat data to be imported [None=0.0, Low=0.3, Medium=0.6, High=1.0].

Modify Criticality?
☒ YES



Modify Criticality?

YES

Modification Type

-Select-

Normalize

String

- a. **Exclude Header?:** Toggle to **Yes** to exclude headers from input file.
 - a. **No:** Proceed to next step. Header will be included.
 - b. **Yes:** Specify the number of **Header Lines** to exclude.
- b. **Criticality:** Select a criticality from the dropdown. Example: High.



Note: Criticality assigns a confidence for the threat data to be imported on the following scale: None=0.0, Low=0.3, Medium=0.6, High=1.0.

- c. **Modify Criticality?:** Toggle to **Yes** to modify the criticality.
 - a. **No:** Proceed to **More Settings**.
 - b. **Yes:** Select a **Modification Type** from the dropdown and set criticality.

- **Normalize:** When the criticality is provided as a numerical value, if the input file has ratings from 0-10 indicating criticality, the following configuration will normalize the criticality rating to None for 0, Low for 1-3, Medium for 4-6, and High for 7-10.

Modify Criticality?
☒ YES

Modification Type
Normalize ▼

Set None	When criticality is =0
Set Low	When criticality is ≥1
Set Medium	When criticality is ≥4
Set High	When criticality is ≥7

**Indicates required field*

- **String:** When the criticality is provided as a string, the application will set the appropriate criticality for each of the criticality string conditions provided.

Modification Type

String

Set None	When criticality is None
Set Low	When criticality is Low
Set Medium	When criticality is Medium
Set High	When criticality is High

**Indicates required field*

Preview Input

1. **Preview Input** to ensure the data has uploaded successfully.

PREVIEW INPUT	GET PREVIEW
101.200.81.187	
103.19.89.118	
103.230.84.239	
103.26.128.84	
103.4.52.150	
103.7.59.135	
104.238.158.106	
107.161.186.90	
108.174.157.123	
109.127.8.242	
109.229.210.250	
109.229.36.65	
113.29.230.24	
120.31.134.133	
120.63.157.195	
123.30.129.179	

2. Click **Save and Next** to proceed to [Step 3: Scheduling the Job.](#)

Importing TPI from ThreatConnect

ThreatConnect aggregates threat intelligence from over 100 open source feeds, crowd-sourced intelligence, and the ThreatConnect Research Team.

Prerequisites for Importing TPI from ThreatConnect

Ensure you have the following before importing TPI using the ThreatStream API:

- **API Access ID:** The unique Access ID for the ThreatConnect API account.
- **API Secret Key:** The alphanumeric key for the ThreatConnect API account.
- **API URL:** The URL for your API account.
- **API Owner:** The owner for which the data is to be retrieved

To import TPI from ThreatConnect, first complete the previous steps for [Step 1: Creating a New Connection](#)

Connection Properties

Complete the following information:

CONNECTION PROPERTIES

API Access ID*

01234567899876543210

Access ID to connect to the API

API Secret Key*

Alphanumeric key

API Secret Key tied to the Access ID above.

API URL*

https://www.companyname.com

URL of the API.

API Owner*

Owner Name

Owner for which the data is to be retrieved.

Type of Data*

-Select-

Type of Data which needs to be imported.

TPI Type*

ThreatConnect

ThreatConnect import is always of the TPI type ThreatConnect.

*Indicates required field

- a. **API Access ID:** Enter the unique Access ID for the ThreatConnect API account.
- b. **API Secret Key:** Enter the alphanumeric key for the ThreatConnect API account.
- c. **API URL:** Enter the URL for your API account.
- d. **API Owner:** Enter the owner for which the data is to be retrieved.
- e. **Type of Data:** Select the type of data to be imported from the dropdown. Example: Threat Group.
- a. **TPI Type:** Proceed to next step. ThreatConnect is always the TPI type for ThreatConnect and is selected by default.

Additional Settings

Complete the following information:

ADDITIONAL SETTINGS

Exclude Header
☒ YES
Include/Exclude Headers from input file.

Header Lines

Exclude Footer
☐ NO
Include/Exclude Footers from input file.

Criticality*

Assign a confidence for the threat data to be imported [None=0.0, Low=0.3, Medium=0.6, High=1.0].

Modify Criticality?
☒ YES

Modify Criticality?
☒ YES

Modification Type

-Select-

Normalize

String

- a. **Exclude Header?:** Toggle to **Yes** to exclude headers from input file.
- a. **No:** Proceed to next step. Header will be included.
 - b. **Yes:** Specify the number of **Header Lines** to exclude.

- b. **Criticality:** Select a criticality from the dropdown. Example: High.



Note: Criticality assigns a confidence for the threat data to be imported on the following scale: None=0.0, Low=0.3, Medium=0.6, High=1.0.

- c. **Modify Criticality?:** Toggle to **Yes** to modify the criticality.
 - a. **No:** Proceed to **More Settings**.
 - b. **Yes:** Select a **Modification Type** from the dropdown and set criticality.

- **Normalize:** When the criticality is provided as a numerical value, if the input file has ratings from 0-10 indicating criticality, the following configuration will normalize the criticality rating to None for 0, Low for 1-3, Medium for 4-6, and High for 7-10.

Modify Criticality?
☒ YES

Modification Type
Normalize ▼

Set None	When criticality is <input type="text" value="=0"/>
Set Low	When criticality is <input type="text" value=">=1"/>
Set Medium	When criticality is <input type="text" value=">=4"/>
Set High	When criticality is <input type="text" value=">=7"/>

**Indicates required field*

- **String:** When the criticality is provided as a string, the application will set the appropriate criticality for each of the criticality string conditions provided.

Modification Type

String ▼

Set None	When criticality is None
Set Low	When criticality is Low
Set Medium	When criticality is Medium
Set High	When criticality is High

**Indicates required field*

Preview Input

1. **Preview Input** to ensure the data has uploaded successfully.

PREVIEW INPUT	GET PREVIEW
101.200.81.187	
103.19.89.118	
103.230.84.239	
103.26.128.84	
103.4.52.150	
103.7.59.135	
104.238.158.106	
107.161.186.90	
108.174.157.123	
109.127.8.242	
109.229.210.250	
109.229.36.65	
113.29.230.24	
120.31.134.133	
120.63.157.195	
123.30.129.179	

2. Click **Save and Next** to proceed to [Step 3: Scheduling the Job.](#)

Step 2: Mapping Attributes

ArcSight UBA extracts fields from the imported Third Party Intelligence based on the parsing technique selected in the previous screen. In this section, map attribute fields from the TPI data to their correct position in the file.



Note: For a complete list of attributes in ArcSight UBA, see [Appendix A: ArcSight UBA Attribute Schema](#).

To map attributes, complete the following steps:

Field Name	Position	Actions
tpi_domain	1	+

PREVIEW

First 10 lines from input file are shown below. Headers in the table correspond to column positions. Enter the position number above and select corresponding field to map to. You can choose not to map columns you do not wish to import.

1
039b1ee.netsoihost.com
03a6b7a.netsoihost.com
03a6f57.netsoihost.com
03b0ec4.netsoihost.com
0bf1n6.org
0x.x.gg
54g35546-5g5hbgg7fb.tk
76tgy9h6dgtt17tg.su
af0bat.cl
ahmedashid.com

1. Select a **Field Name** from the dropdown. Example: tpi_domain.
2. Indicate a **Position** for the attribute in the file.
3. Use **+/-** to add/remove attribute entries
4. Click **Save & Next** to proceed to [Step 3: Scheduling the Job](#).

Step 3: Scheduling the Job

JOB DETAILS

Job Name*
TPI_import_ZeusDomain@lockList_1508791455499

Job Description
Third Party Intelligence Import Job

Enable Job Related Notifications
☒ Yes ☐ No
Set job related notifications to "Yes" if you want to send emails upon job success/failure.

JOB SCHEDULING INFORMATION

Run Job

☒ Do you want to run job Once ?
☐ Do you want to schedule this job for future ?

Job will be scheduled according to the server time. Current server time is - 10/23/2017 15:45:03

1. Enter a unique **Job Name** or use the default name.
2. Enter a **Job Description** or use the default description.
3. Select when you would like the job to run.

JOB SCHEDULING INFORMATION

Run Job

☒ Do you want to run job Once ?

☐ Do you want to schedule this job for future ?

1 Job will be scheduled according to the server time. Current server time is - 5/1/2017 14:40:57

- Select **Do you want to run job Once?** to run now.
- Select **Do you want to schedule this job for future?** to run the job later and complete the relevant fields.

☒ Do you want to schedule this job for future ?

Select how often you want the job to run

Start Job At *

02:38:00 PM

NOTE: This is the server time

Run Every *

Seconds

Stop after

Times

4. **Save** job.
5. Click **Run**.
6. Review the job status to ensure data was loaded successfully.

The Job Monitor screen for this job will appear automatically. To find specific jobs, navigate to **Menu > Operations Center > Job Monitor** and select **Third Party Intelligence Import** from left navigation panel.

Job Name	Creation Date	Start Date	Next Trigger Date	Job Status
TPI_IMPORT_THREATSTREAM_1507676616048 CREATED BY: ADMIN / JOB TYPE: THIRD PARTY INTELLIGENCE JOB EDIT JOB REVIEW JOB DELETE JOB	TUE, 10 OCT 2017 @ 06:03:43.000 PM	START DATE: TUE, 10 OCT 2017 @ 06:03:43.000 PM END DATE: TUE, 10 OCT 2017 @ 06:04:17.000 PM	NOT SCHEDULED	COMPLETED
TPI_IMPORT_THREATSTREAM_150168845339 CREATED BY: ADMIN / JOB TYPE: THIRD PARTY INTELLIGENCE JOB EDIT JOB REVIEW JOB DELETE JOB	MON, 11 SEP 2017 @ 05:27:30.000 PM	START DATE: MON, 11 SEP 2017 @ 05:27:30.000 PM END DATE: MON, 11 SEP 2017 @ 05:27:46.000 PM	NOT SCHEDULED	COMPLETED

First 10 Last Show 10 Total results: 2 / Total pages: 1

Search Third Party Intelligence Data using Spotter

Upon successful import, the lookup data will be available for searching in Spotter. To search lookup data in Spotter, complete the following steps:

1. Navigate to **Menu > Security Center > Spotter**.
2. Type `index=tpi` in search bar and click search icon.

Timestamp	Event Details
MON, 6 MAR 2017 @ 06:00:11 PM	tpi_action = inactive , tpi_addr = 99.39.240.234 , tpi_category = bot_ip , tpi_country = US , tpi_criticality = 0.3 , tpi_date = 10/10/2017 18:03:34.202 , tpi_description = bfoicats_deactivated_on_2017-03-06_18:00:11.669191 , tpi_domain = 99.39.240.234 , tpi_dt_firstseen = 1481101746000 , tpi_dt_lastseen = 1488844811000 , tpi_latitude = 25.9102 , tpi_longitude = -80.3965 , tpi_src = ThreatStream , tpi_src_confidence = 75.0 , tpi_src_organization = AT&T Uverse , tpi_srckey = 2~99.39.240.234_ThreatStream , tpi_type = bot
WED, 8 MAR 2017 @ 07:00:20 PM	tpi_action = inactive , tpi_addr = 98.25.48.224 , tpi_category = bot_ip , tpi_country = US , tpi_criticality = 0.3 , tpi_date = 10/10/2017 18:03:34.202 , tpi_description = bfoicats_deactivated_on_2017-03-06_19:00:20.615115 , tpi_domain = 98.25.48.224 , tpi_dt_firstseen = 1481230449000 , tpi_dt_lastseen = 1489021220000 , tpi_latitude = 34.0402 , tpi_longitude = -80.8382 , tpi_src = ThreatStream , tpi_src_confidence = 75.0 , tpi_src_organization = Time Warner Cable , tpi_srckey = 2~98.25.48.224_ThreatStream , tpi_type = bot
MON, 6 MAR 2017 @ 06:00:11 PM	tpi_action = inactive , tpi_addr = 98.238.73.66 , tpi_category = bot_ip , tpi_country = US , tpi_criticality = 0.3 , tpi_date = 10/10/2017 18:03:34.202 , tpi_description = bfoicats_deactivated_on_2017-03-06_18:00:11.669191 , tpi_domain = 98.238.73.66 , tpi_dt_firstseen = 1481101746000 , tpi_dt_lastseen = 1488844811000 , tpi_latitude = 26.1338 , tpi_longitude = -81.7979 , tpi_src = ThreatStream , tpi_src_confidence = 75.0 , tpi_src_organization = Comcast Cable , tpi_srckey = 2~98.238.73.66_ThreatStream , tpi_type = bot
THU, 8 DEC 2016 @ 08:28:06 PM	tpi_action = falsepos , tpi_addr = 98.234.192.15 , tpi_category = bot_ip , tpi_country = US , tpi_criticality = 0.3 , tpi_date = 10/10/2017 18:03:34.202 , tpi_description = imported by user 1 Confirmed as false positive , tpi_domain = 98.234.192.15 , tpi_dt_firstseen = 1481230486000 , tpi_dt_lastseen = 1481230486000 , tpi_latitude = 37.8927 , tpi_longitude = -122.1978 , tpi_src = ThreatStream , tpi_src_confidence = 75.0 , tpi_src_organization = Comcast Cable , tpi_srckey = 2~98.234.192.15_ThreatStream , tpi_type = bot



Note: Click for more information about searching [Spotter](#) or see the ArcSight UBA User Guide.

Watch Lists

A watch list is a list of entities that need to be watched closely due to inherent risks. Watch lists in ArcSight UBA help to monitor users, activity accounts, activity IPs, and resources that are deemed problematic and require special attention.

For example, users who have received a poor performance review can be placed on a watch list so that their activity can be closely monitored. Alerts are sent out if a user on a watch list takes actions such as accessing information that they have never accessed before or uploading files to a personal file storage site. You could use a watch list to monitor activity IPs from which users clicked a phishing email to be notified if anomalous activity occurs on the IPs that suggests a malware infection.

The steps to import watch lists in ArcSight UBA include the following:

1. Configure a connection to import watch list data.
2. Map attributes for the watch list
3. Run the job to import the watch list data

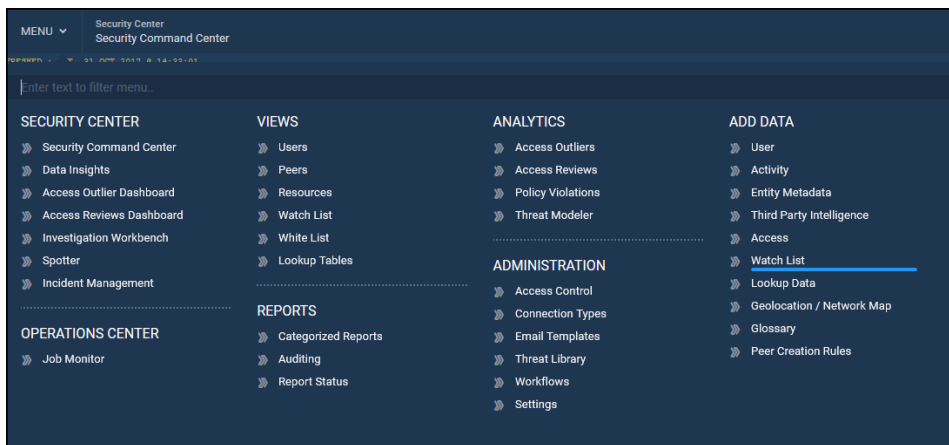
Ingesting Watchlist Data



Step 1: Configuring the Connection

Complete the following steps to configure a connection:

1. Navigate to **Menu > Add Data > Watch List**.



Connection

1. Select a connection:

Existing connection: Select from dropdown. Edit details as described in proceeding steps.

New Connection: Select a Connection Type from the drop down. Example: File Import.

The screenshot shows a dialog box titled 'Select Connection to import Watch List data. Create a new connection by selecting New Connection box or also select an existing connection. Every New Connection must have a new Watch List.' The dialog has two tabs: 'EXISTING CONNECTION' and 'NEW CONNECTION'. The 'NEW CONNECTION' tab is active. Below the tabs is a form with the following fields:

- CONNECTION** (Section Header)
- Connection Type*** (Dropdown menu): 'File Import' is selected.
- Connection Name*** (Text input): 'Watchlist_1508801156627' is entered.

2. Enter a unique **Connection Name**.

Connection Details

CONNECTION DETAILS

Watch List Name*

Watch List Type*

-Select-

Watch List Criticality*

-Select-

Upload a file?

☐ NO

File Name*

Name of the file containing data to import. Example: hrdata.csv, hrdata.log, hrdata.txt.
This file must be located in /Securonix/tenants/partnerdemo /securonix_home\import\in. You can change this location by clicking on [More Settings](#) below.

Delimiter*

Specify the delimiter between the fields in the input file. Example: , (comma) | (pipe)

Please choose the resource group with which the watchlist entities being imported are to be associated. *

Bluecoat Proxy

Exclude Header

☐ NO

1. Provide a unique **Watch List Name**. Example: PoorPerformanceReviewUsers.
2. Select an entity from Watch List Type dropdown. Example: Users.

3. Select a Watch List Criticality from the dropdown. Example: Medium.
4. Enable **Upload a File** to **YES** to add a file from your local machine.
5. Provide the **File Name** from which to import watch list data. Example: hrdata.csv.



Note: The file must be located in your \$securonix_home/import/in folder.

6. Specify the Delimiter between the fields in the input file. Example: , (comma).
7. Select a **Resource Group** with which the imported watch list entities will be associated from drop down. Example: Bluecoat Proxy.
8. Enable **Exclude Header** to **YES** to exclude the header of the input file.
 1. Specify **Number of lines to ignore**.

Connection Properties

CONNECTION PROPERTIES

Import from Remote Server?

☐ NO

Use FTP/SFTP/SCP to ingest file located in a remote location?

`${SECURONIX_HOME}` is set to `/Securonix/tenants/partnerdemo/securonix_home`.
You can also replace `${SECURONIX_HOME}` below with the direct path to the folder where the file exists.
Example: `/Users/dev/files/`

Source Folder*

`${SECURONIX_HOME}/import/in`

Enter the complete path to the directory where this file is located.

Success Folder*

`${SECURONIX_HOME}/import/success`

Enter the complete path to the directory where this file must be moved once the import is completed successfully.

Failed Folder*

`${SECURONIX_HOME}/import/failed`

Enter the complete path to the directory where this file must be moved if the import job fails to complete.

1. Enable **Import from Remote Server?** to use FTP/SFTP/SCP to ingest the file located on a remote location.

- a. If **No**: Proceed to next step.
- b. If **Yes**: Enter the following information:

CONNECTION PROPERTIES

Import from Remote Server?

☒ YES

Use FTP/SFTP/SCP to ingest file located in a remote location?

Remote Connection Type*

FTP ▼

Host IP Address*

<host>

Port Number*

21

Username

Password

Source directory

Proxy Server?

☐ NO

This is a server that all computers on the local network have to go through before accessing information on the Internet.

Test Remote Connection?

[TEST](#)

- a. Select a **Remote Connection Type** from the dropdown.
 - b. Enter the **Host IP Address** (for FTP, SFTP, etc.) or **URL** (for HTTP, HTTPS).
 - c. Enter the **Port Number** (for FTP, SFTP, etc.).
 - d. Enter the **Username**.
 - e. Enter the **Password**.
 - f. Enter the **Source Directory**.
 - g. Select **Yes** or **No** for **Proxy Server?**
 - a. If **No**: Proceed to next step.
 - b. If **Yes**: Enter **Proxy Server URL**, **Username**, and **Password**.
 - h. **Test** the remote connection.
2. Specify the **Source Folder** in which the file is located. Default \${SECURONIX_HOME}/import/in.

`${SECURONIX_HOME}` is set to `/Securonix/tenants/snypr6/securonix_home`.
 You can also replace `${SECURONIX_HOME}` below with the direct path to the folder where the file exists.
 Example: `/Users/dev/files/`

Source Folder*

`${SECURONIX_HOME}/import/in`

Enter the complete path to the directory where this file is located.

Success Folder*

`${SECURONIX_HOME}/import/success`

Enter the complete path to the directory where this file must be moved once the import is completed successfully.

Failed Folder*

`${SECURONIX_HOME}/import/failed`

Enter the complete path to the directory where this file must be moved if the import job fails to complete.



Note: `${SECURONIX_HOME}` is set to `/Securonix/tenants/snypr6/securonix_home`. You can replace `${SECURONIX_HOME}` with the direct path to the folder where the file exists. Example: `/Users/dev/files/`.

3. Specify the **Success Folder** into which to move the file once the import is completed successfully. Default `${SECURONIX_HOME}/import/success`.
4. Specify the **Failed Folder** into which to move the file if the import job fails to complete. Default `${SECURONIX_HOME}/import/failed`.
5. Click **Save and Next** to proceed to [Step 2: Mapping Attributes](#).

Step 2: Mapping Attributes

After configuring the connection for the watch list, map the attributes from the watch list file.

The first column shows the entity ID; the second column shows location; the third column shows the login information; and the fourth column shows the expiry data for the watch list. Based on this example, you can map the watch list fields as follows:

1. Review the fields in the input source, and determine which of the fields you want to map for the watch list.
2. Use drops downs to select the attributes to map to each position in the watch list.
 - a. Select ArcSight UBA attributes that correspond to the items in the watch list. Example: Entity Name corresponds to Entity ID.
 - b. Select **Watch List Item** to map items for which no corresponding ArcSight UBA attribute is available and specify the value. Example: Watch List Item: Location.

For example, the preview input shows the following data:

2276	los ángeles	InCorrectLoginGeo	03/25/2017
2257	new jersey	InCorrectLoginGeo	04/05/2017
2258	ethopia	MultipleLoginGeo	06/21/2017

Based on the input information shown in the example, map the attributes as follows:

1	Select Connection	Attribute Mapping	Run Job
Specify column positions in the input source that map to Watchlist Fields. Entity Name is the the first field which is mandatory and its position number can be changed.			
Field Mapping			
Position	Mapped With		
1	Entity Name		
2	Watch List Item	Location	
3	Watch List Item	LoginInfo	
4	Expiry Date	MM/dd/yyyy	

1. **Position 1:** Entity Name
 2. **Position 2:** Watch List Item with specified value Location
 3. **Position 3:** Login information (LoginInfo)
 4. **Position 4:** Expiry date
3. Click **Save and Next**.

Step 3: Running the Job

To schedule the job to run, complete the following steps:

JOB DETAILS		JOB SCHEDULING INFORMATION	
Job Name* WatchListConn_Contractors-UpComingTermination_1508861224450		Run Job ⓘ <input checked="" type="radio"/> Do you want to run job Once ? <input type="radio"/> Do you want to schedule this job for future ?	
Job Description Watch List Import Job		ⓘ Job will be scheduled according to the server time. Current server time is - 10/24/2017 11:09:15	
Enable Job Related Notifications ⓘ <input checked="" type="radio"/> YES			
ON SUCCESS Select Email Template to Use for Sending Notifications -Select- OR Override email address from template If we specify email address above then email addresses in email template will be overridden.	ON FAILURE Select Email Template to Use for Sending Notifications -Select- OR Override email address from template If we specify email address above then email addresses in email template will be overridden.	ON MISFIRE Select Email Template to Use for Sending Notifications -Select- OR Override email address from template If we specify email address above then email addresses in email template will be overridden.	ON COMPLETED WITH ERRORS Select Email Template to Use for Sending Notifications -Select- OR Override email address from template If we specify email address above then email addresses in email template will be overridden.

Job Details

1. Specify a **Job Name** or use auto-generated name.
2. Enter a **Job Description**.

3. **Enable Job Related Notifications** if you would like to receive email notifications when the job is run.
 - a. If **No**: Proceed without entering additional information.
 - b. If **Yes**:
 - **On Success**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template:
 - **On Failure**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template.
 - **On Misfired**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template.
 - **On Completed with Errors**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template:

Create New Email Template

Sender Name*

Template Name*

Description

To*

From*

test@securonix.com

CC

BCC

Subject

HTML Enabled

YES

Store in Outbox prior to sending?

YES

Use this template for *

Job Misfired

Owner

Administrators
SECURITYOPERATIONS

>
>>
<<
<

Email Body

Add Email Template Variables

B I U abc x² T• fT H• T_a [Y] [T]

[List Icon] [Text Icon] [Image Icon] [Link Icon] [Unlink Icon] [Table Icon] [Quote Icon] [Code Icon] [Print Icon] [Share Icon] [More Icon]

Job Scheduling Information

1. Select when you would like the job to run.

JOB SCHEDULING INFORMATION

Run Job

☒ Do you want to run job Once ?

☐ Do you want to schedule this job for future ?

Job will be scheduled according to the server time. Current server time is - 5/1/2017 14:40:57

- Select **Do you want to run job Once?** to run now.
- Select **Do you want to schedule this job for future?** to run the job later and complete the relevant fields.

☒ Do you want to schedule this job for future ?

Seconds Minutes Hourly Daily Weekly Monthly Specify Date

Select how often you want the job to run

Start Job At *

02:38:00 PM

NOTE: This is the server time

Run Every *

Seconds

Stop after

Times

1. Select when you would like the job to run.
2. **Save** job.

4. Review the job status to ensure data was loaded successfully.

The Job Monitor screen for this job will appear automatically. To find specific jobs, navigate to **Menu > Operations Center > Job Monitor** and select **Entity Metadata Import** from left nav-

igation panel.

Job Name	Creation Date	Start Date	Next Trigger Date	Job Status
WATCHLISTCONN_FCI ASSET_1505524773781 CREATED BY: ADMIN / JOB TYPE: WATCH LIST IMPORT EDIT JOB RE-RUN JOB DELETE JOB	FRI, 15 SEP 2017 @ 08:19:37.000 PM	START DATE: FRI, 15 SEP 2017 @ 08:19:37.000 PM END DATE: FRI, 15 SEP 2017 @ 08:19:37.000 PM	NOT SCHEDULED	COMPLETED
WATCHLISTCONN_VULNERABLE HOST_1505524653631 CREATED BY: ADMIN / JOB TYPE: WATCH LIST IMPORT EDIT JOB RE-RUN JOB DELETE JOB	FRI, 15 SEP 2017 @ 08:17:35.000 PM	START DATE: FRI, 15 SEP 2017 @ 08:17:35.000 PM END DATE: FRI, 15 SEP 2017 @ 08:17:35.000 PM	NOT SCHEDULED	COMPLETED
WATCHLISTCONN_HPAA SERVERS_1505524802323 CREATED BY: ADMIN / JOB TYPE: WATCH LIST IMPORT EDIT JOB RE-RUN JOB DELETE JOB	FRI, 15 SEP 2017 @ 08:15:04.000 PM	START DATE: FRI, 15 SEP 2017 @ 08:15:04.000 PM END DATE: FRI, 15 SEP 2017 @ 08:15:04.000 PM	NOT SCHEDULED	COMPLETED
WATCHLISTCONN_WATCHLIST_1505524147764_1505524266585 CREATED BY: ADMIN / JOB TYPE: WATCH LIST IMPORT EDIT JOB RE-RUN JOB DELETE JOB	FRI, 15 SEP 2017 @ 08:11:10.000 PM	START DATE: FRI, 15 SEP 2017 @ 08:11:10.000 PM END DATE: FRI, 15 SEP 2017 @ 08:11:10.000 PM	NOT SCHEDULED	COMPLETED

Total results : 4 | Total pages : 1

- Review the job status to ensure data was loaded successfully.

The Job Monitor screen for this job will appear automatically. To find specific jobs, navigate to **Menu > Operations Center > Job Monitor** and select **Entity Metadata Import** from left navigation panel.

Job Name	Creation Date	Start Date	Next Trigger Date	Job Status
WATCHLISTCONN_FCI ASSET_1505524773781 CREATED BY: ADMIN / JOB TYPE: WATCH LIST IMPORT EDIT JOB RE-RUN JOB DELETE JOB	FRI, 15 SEP 2017 @ 08:19:37.000 PM	START DATE: FRI, 15 SEP 2017 @ 08:19:37.000 PM END DATE: FRI, 15 SEP 2017 @ 08:19:37.000 PM	NOT SCHEDULED	COMPLETED
WATCHLISTCONN_VULNERABLE HOST_1505524653631 CREATED BY: ADMIN / JOB TYPE: WATCH LIST IMPORT EDIT JOB RE-RUN JOB DELETE JOB	FRI, 15 SEP 2017 @ 08:17:35.000 PM	START DATE: FRI, 15 SEP 2017 @ 08:17:35.000 PM END DATE: FRI, 15 SEP 2017 @ 08:17:35.000 PM	NOT SCHEDULED	COMPLETED
WATCHLISTCONN_HPAA SERVERS_1505524802323 CREATED BY: ADMIN / JOB TYPE: WATCH LIST IMPORT EDIT JOB RE-RUN JOB DELETE JOB	FRI, 15 SEP 2017 @ 08:15:04.000 PM	START DATE: FRI, 15 SEP 2017 @ 08:15:04.000 PM END DATE: FRI, 15 SEP 2017 @ 08:15:04.000 PM	NOT SCHEDULED	COMPLETED
WATCHLISTCONN_WATCHLIST_1505524147764_1505524266585 CREATED BY: ADMIN / JOB TYPE: WATCH LIST IMPORT EDIT JOB RE-RUN JOB DELETE JOB	FRI, 15 SEP 2017 @ 08:11:10.000 PM	START DATE: FRI, 15 SEP 2017 @ 08:11:10.000 PM END DATE: FRI, 15 SEP 2017 @ 08:11:10.000 PM	NOT SCHEDULED	COMPLETED

Total results : 4 | Total pages : 1

Viewing Watch Lists

Views

To view watch lists, Navigate to **Menu > Views > Watch List**.

Click the name of the watch list you want to view or manage. See [Views](#) in the ArcSight UBA User Guide for more information about what you can do from the Watch List view screen.

Entity Name	Watch List Type	Reason	Confidence Level (between 0 to 1)	expirydate	watchlistname	createdate	decayflag
DALGDC1619	Resources	PCI Assets	1.0	05/04/2018	PCI Assets	05/04/2017	false
DALGDC2229	Resources	PCI Assets	1.0	05/04/2018	PCI Assets	05/04/2017	false
DALGDC4657	Resources	PCI Assets	1.0	05/04/2018	PCI Assets	05/04/2017	false
DALGDC5857	Resources	PCI Assets	1.0	05/04/2018	PCI Assets	05/04/2017	false
DALGDC6321	Resources	PCI Assets	1.0	05/04/2018	PCI Assets	05/04/2017	false
DALGDC7426	Resources	PCI Assets	1.0	05/04/2018	PCI Assets	05/04/2017	false
DALGDC8132	Resources	PCI Assets	1.0	05/04/2018	PCI Assets	05/04/2017	false
DALGDC8945	Resources	PCI Assets	1.0	05/04/2018	PCI Assets	05/04/2017	false
DALGDC9260	Resources	PCI Assets	1.0	05/04/2018	PCI Assets	05/04/2017	false

Security Command Center

To manage watch lists from the Watchlist dashboard on the Security Command Center, navigate to **Menu > Security Center > Security Command Center**.

Watchlist	Entities
PART TIME EMPLOYEES	31
FLIGHT RISK USERS	13
PCI ASSET	8
HIPAA SERVERS	7
VULNERABLE HOST	5

Click the watch list you want to view or manage. See [Watchlists](#) for information about how to manage watch lists from this screen.

Entity Name	Watch List Type	Reason	Confidence Level (between 0 to 1)	expirydate	watchlistname	createdate	decayflag
1127	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
1128	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
1129	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
1130	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
1131	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
1132	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
1135	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
1136	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
1138	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
1139	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
1140	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false

Searching Watchlists in Spotter

Upon successful configuration, the watch list will be available for searching in Spotter. To search watchlist data in Spotter, complete the following steps:

1. Navigate to **Menu > Security Center > Spotter**.
2. Type `index=watchlist` in search bar and click search icon.

Field	Value
confidencefactor	1.0
decayflag	false
entityname	NJCUX12.scmx.com
expired	false
expirydate	09/15/2018 20:17:35.341
type	Resources
watchlistname	Vulnerable Host
watchlistuniquekey	2~2~Vulnerable Host(NJCUX12.scmx.com)



Note: Click for more information about searching [Spotter](#) or see the ArcSight UBA User Guide.

Lookup Tables

Lookup tables are used to save any data needed for reference, such as critical keywords, competitors, non-business domains, malicious file extensions, job portals, etc. The contents of a lookup table are used to make comparisons in policies.

The ArcSight UBA application includes some lookup tables by default. These tables do not contain data. This section will show you how to create new lookup tables and import data into existing tables.

Lookup tables are enabled during [Activity Data](#) during Step 3: Performing Conditional Actions.

Steps to create lookup tables:

1. Create a connection to import from file or database.
2. Map Attributes with corresponding ArcSight UBA attributes.
3. Schedule and run the job.

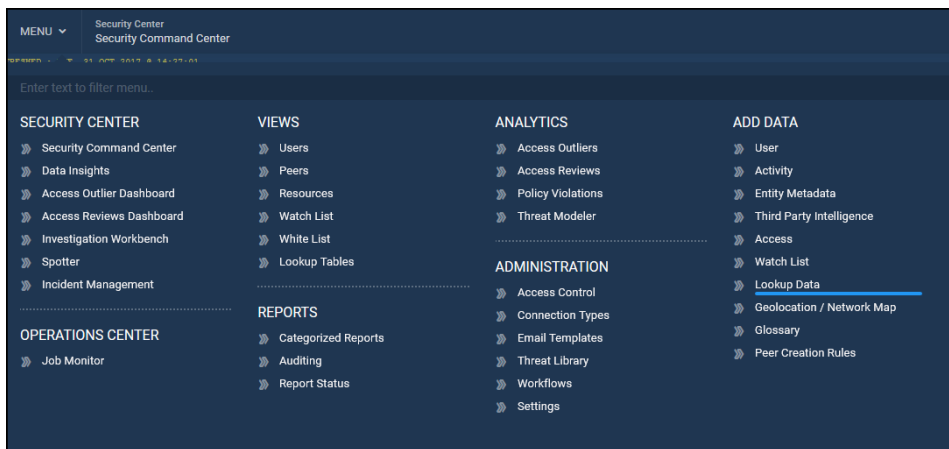
Ingesting Lookup Data



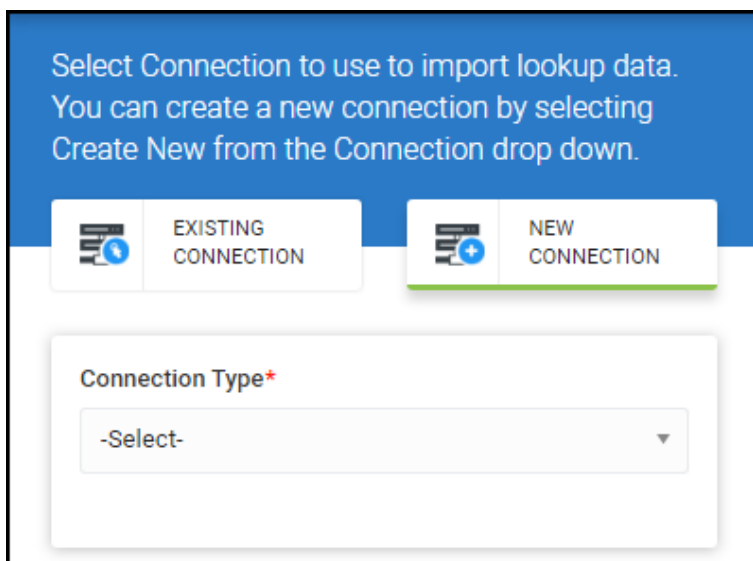
Step 1: Creating a New Connection

To create a new lookup table connection, complete the following steps:

1. Navigate to **Menu > Add Data > Lookup Tables**.





2. Click **New Connection**.



3. Select **Connection Type** from dropdown. Example: File Import.
4. Enter a unique name for **Create New Lookup Table**. Example: Non-Business Domains.

Select Connection to use to import lookup data.
You can create a new connection by selecting
Create New from the Connection drop down.

 EXISTING
CONNECTION

 NEW
CONNECTION

Connection Type*

File Import ▼

Create New Lookup Table*

Non-Business Domains

Importing Lookup Data from a File

Configure Connection

Connection Details

CONNECTION DETAILS

Upload a file?
☐ NO

File name*

Delimiter*

Specify the delimiter between the fields in the input file.
Example: , (comma) | (pipe)

Exclude Header
☒ YES
Number of header lines to be excluded from input file.

Number of lines to Ignore*

Number of lines to skip/ignore in a file.

Delete Old Lookup Data
☐ NO

1. Toggle **Upload a file?** to **Yes** to browse your local machine for a file.

OR

2. Enter a **File name**.



Note: You must place the file to import into the /securonix_home/import/in folder before importing into the ArcSight UBA application.

3. Specify the **Delimiter** for your file type. Default is comma (,).
4. Enable **Exclude Header** to exclude header from input and enter the **Number of Lines to Ignore**.
5. Enable **Delete Old Lookup Data** if you would like to delete data from an existing table. Default is **No**.

Enter a file name in **Select the File to Import** or use the **BROWSE** button to browse for the file.



Note: You must place the file to import into the /securonix_home/import/in folder before importing into the ArcSight UBA application.

Connection Properties

CONNECTION PROPERTIES

Import from Remote Server?

☐ NO

Use FTP/SFTP/SCP to ingest file located in a remote location?

`${SECURONIX_HOME}` is set to `/Securonix/tenants/four/snypr6/securonix_home`.
You can also replace `${SECURONIX_HOME}` below with the direct path to the folder where the file exists.
Example: `/Users/dev/files/`

Source Folder*

`${SECURONIX_HOME}/import/in`

Enter the complete path to the directory where this file is located.

Success Folder*

`${SECURONIX_HOME}/import/success`

Enter the complete path to the directory where this file must be moved once the import is completed successfully.

Failed Folder*

`${SECURONIX_HOME}/import/failed`

Enter the complete path to the directory where this file must be moved if the import job fails to complete.

1. Select whether you would like to **Import from Remote Server**.

- If **No**: Proceed without entering additional information.
- If **Yes**: Enter the following information:

Import from Remote Server?

YES

Use FTP/SFTP/SCP to ingest file located in a remote location?

Remote Connection Type*

FTP

Host IP Address*

<host>

Port Number*

21

Username

admin

Password

•••••

Source directory


Proxy Server?

NO

This is a server that all computers on the local network have to go through before accessing information on the Internet.

Test Remote Connection?

TEST

- a. Select **Remote Connection Type** from dropdown.
 - b. Enter **Host IP Address**.
 - c. Enter **Port Number**. Default 21.
 - d. Enter **Username**.
 - e. Enter **Password**.
 - f. Specify the **Source Directory**.
 - g. Enable **Proxy Server** slider if your information must pass through a proxy server.
 - a. If **No**: Proceed without entering additional information.
 - b. If **Yes**: Enter **Proxy Server URL**, **Username**, and **Password**.
 - h. Click **Test** to **Test Remote Connection**.
 2. Specify the complete path to the **Source Folder** from which you will import lookup data. Default is \${SECURONIX_HOME}/import/in.
-  **Note:** \${SECURONIX_HOME} is set to "/Securonix/tenants/snypr6/securonix_home". You can also replace \${SECURONIX_HOME} below with the direct path to the folder where the file exists. Example: "/Users/dev/files/"
3. Specify a complete path to the **Success Folder** into which to move the file once the import is successful. Default is \${SECURONIX_HOME}/import/success.
 4. Specify a complete path to the **Failed Folder** into which to move the file if the import job fails to complete. Default is \${SECURONIX_HOME}/import/failed.
 5. Specify a complete path to the **Staging Folder** (only required for data requiring preprocessing). Default is \${SECURONIX_HOME}/import/in.
 6. Review the input in the **Preview Input** pane.


- Click **Save and Next** to proceed to [Step 2: Mapping Attributes](#).


Importing Lookup Data from a Database

Configure Connection

Connection

Select Connection to use to import lookup data. You can create a new connection by selecting Create New from the Connection drop down.


EXISTING CONNECTION


NEW CONNECTION

Connection Type*

Database ▼

Create New Lookup Table*

Lookuptable_1494270977670

- Select **Database** in the **Connection Type** dropdown.
- Enter a unique name for Create New Lookup Table.

Connection Details

CONNECTION DETAILS

Delete Old Lookup Data

☐ NO

Query*

select domainname, domainkey from
lookuptable10

1. Enable **Delete Old Lookup Data** to remove previous data for this lookup table.
2. Enter the **Query**. Example: `select domainname, domainkey from lookuptable10.`

Connection Properties

CONNECTION PROPERTIES

Database Type *

MySQL

JDBC URL *

jdbc:mysql://<host>:<3306>/<database>

Connection string to connect to particular database.
 Example: jdbc:mysql://hostname:port/database_name

Driver Class *

com.mysql.jdbc.Driver

Database specific class

Database Username *

root

Database Password *

.....

1. Select the **Database Type** from the dropdown.
2. Enter the **JDBC URL** to connect to a particular database. Example: `jdbc:mysql://<host>:<3306>/<database>`.
3. Specify the database specific **Driver Class**. Example: `com.mysql.jdbc.Driver`.
4. Enter the **Database Username** and **Password**.
5. Review the input in the **Preview Input** pane.
6. Click **Save and Next** to proceed to Map Attributes.

Step 2: Mapping Attributes

1. Enter the **Position** of the column in the data file.

Configure Connection | **Attribute Mapping** | Run Job | Prev | Save & Next

Specify column positions in the input source that map to Lookup Fields

Position*	Mapped With*	Map as key*
1	Domain	YES


PREVIEW

First 10 lines from input file are shown below. Headers in the table correspond to column positions. Enter the position number above and select corresponding field to map to. You can choose not to map columns you do not wish to import.

Position	Value
1	dio.com
1	csps.com
1	buffnews.com
1	tfww.com
1	theprovider.com
1	wsou.net
1	ap.org
1	juno.com
1	telemundo.com
1	flashnews.com

2. Provide a value for **Mapped With** value from the dropdown. Example: Domain.
3. Toggle **Map as key** slider to **YES** if **Mapped With** value is the key.




4. Use  to add/remove entries.
5. Click **Save & Next**.


Step 3: Running Job

1. Enter a unique **Job Name** or use the default name.
2. Enter a **Job Description** or use the default description.
3. **Enable Job Related Notifications** if you would like to receive email notifications when the job is run.
 - a. If **No**: Proceed without entering additional information.
 - b. If **Yes**:
 - **On Success**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template:
 - **On Failure**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template.
 - **On Misfired**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template.
 - **On Completed with Errors**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications.


You can also create a new email template:

Create New Email Template

Sender Name* 


Template Name* 


Description


To* 

From*

test@securonix.com

CC 

BCC 

Subject 

HTML Enabled


☒ YES

Store in Outbox prior to sending?


☒ YES

Use this template for *

Job Misfired

Owner 

Administrators
SECURITYOPERATIONS

Email Body 

Add Email Template Variables

B **I** **U** **abc** **x** **x'** **T** **T'** **H** **H'** **T₀** **T₁** **T₂** **T₃** **T₄** **T₅** **T₆** **T₇** **T₈** **T₉** **T₁₀** **T₁₁** **T₁₂** **T₁₃** **T₁₄** **T₁₅** **T₁₆** **T₁₇** **T₁₈** **T₁₉** **T₂₀** **T₂₁** **T₂₂** **T₂₃** **T₂₄** **T₂₅** **T₂₆** **T₂₇** **T₂₈** **T₂₉** **T₃₀** **T₃₁** **T₃₂** **T₃₃** **T₃₄** **T₃₅** **T₃₆** **T₃₇** **T₃₈** **T₃₉** **T₄₀** **T₄₁** **T₄₂** **T₄₃** **T₄₄** **T₄₅** **T₄₆** **T₄₇** **T₄₈** **T₄₉** **T₅₀** **T₅₁** **T₅₂** **T₅₃** **T₅₄** **T₅₅** **T₅₆** **T₅₇** **T₅₈** **T₅₉** **T₆₀** **T₆₁** **T₆₂** **T₆₃** **T₆₄** **T₆₅** **T₆₆** **T₆₇** **T₆₈** **T₆₉** **T₇₀** **T₇₁** **T₇₂** **T₇₃** **T₇₄** **T₇₅** **T₇₆** **T₇₇** **T₇₈** **T₇₉** **T₈₀** **T₈₁** **T₈₂** **T₈₃** **T₈₄** **T₈₅** **T₈₆** **T₈₇** **T₈₈** **T₈₉** **T₉₀** **T₉₁** **T₉₂** **T₉₃** **T₉₄** **T₉₅** **T₉₆** **T₉₇** **T₉₈** **T₉₉** **T₁₀₀** **T₁₀₁** **T₁₀₂** **T₁₀₃** **T₁₀₄** **T₁₀₅** **T₁₀₆** **T₁₀₇** **T₁₀₈** **T₁₀₉** **T₁₁₀** **T₁₁₁** **T₁₁₂** **T₁₁₃** **T₁₁₄** **T₁₁₅** **T₁₁₆** **T₁₁₇** **T₁₁₈** **T₁₁₉** **T₁₂₀** **T₁₂₁** **T₁₂₂** **T₁₂₃** **T₁₂₄** **T₁₂₅** **T₁₂₆** **T₁₂₇** **T₁₂₈** **T₁₂₉** **T₁₃₀** **T₁₃₁** **T₁₃₂** **T₁₃₃** **T₁₃₄** **T₁₃₅** **T₁₃₆** **T₁₃₇** **T₁₃₈** **T₁₃₉** **T₁₄₀** **T₁₄₁** **T₁₄₂** **T₁₄₃** **T₁₄₄** **T₁₄₅** **T₁₄₆** **T₁₄₇** **T₁₄₈** **T₁₄₉** **T₁₅₀** **T₁₅₁** **T₁₅₂** **T₁₅₃** **T₁₅₄** **T₁₅₅** **T₁₅₆** **T₁₅₇** **T₁₅₈** **T₁₅₉** **T₁₆₀** **T₁₆₁** **T₁₆₂** **T₁₆₃** **T₁₆₄** **T₁₆₅** **T₁₆₆** **T₁₆₇** **T₁₆₈** **T₁₆₉** **T₁₇₀** **T₁₇₁** **T₁₇₂** **T₁₇₃** **T₁₇₄** **T₁₇₅** **T₁₇₆** **T₁₇₇** **T₁₇₈** **T₁₇₉** **T₁₈₀** **T₁₈₁** **T₁₈₂** **T₁₈₃** **T₁₈₄** **T₁₈₅** **T₁₈₆** **T₁₈₇** **T₁₈₈** **T₁₈₉** **T₁₉₀** **T₁₉₁** **T₁₉₂** **T₁₉₃** **T₁₉₄** **T₁₉₅** **T₁₉₆** **T₁₉₇** **T₁₉₈** **T₁₉₉** **T₂₀₀** **T₂₀₁** **T₂₀₂** **T₂₀₃** **T₂₀₄** **T₂₀₅** **T₂₀₆** **T₂₀₇** **T₂₀₈** **T₂₀₉** **T₂₁₀** **T₂₁₁** **T₂₁₂** **T₂₁₃** **T₂₁₄** **T₂₁₅** **T₂₁₆** **T₂₁₇** **T₂₁₈** **T₂₁₉** **T₂₂₀** **T₂₂₁** **T₂₂₂** **T₂₂₃** **T₂₂₄** **T₂₂₅** **T₂₂₆** **T₂₂₇** **T₂₂₈** **T₂₂₉** **T₂₃₀** **T₂₃₁** **T₂₃₂** **T₂₃₃** **T₂₃₄** **T₂₃₅** **T₂₃₆** **T₂₃₇** **T₂₃₈** **T₂₃₉** **T₂₄₀** **T₂₄₁** **T₂₄₂** **T₂₄₃** **T₂₄₄** **T₂₄₅** **T₂₄₆** **T₂₄₇** **T₂₄₈** **T₂₄₉** **T₂₅₀** **T₂₅₁** **T₂₅₂** **T₂₅₃** **T₂₅₄** **T₂₅₅** **T₂₅₆** **T₂₅₇** **T₂₅₈** **T₂₅₉** **T₂₆₀** **T₂₆₁** **T₂₆₂** **T₂₆₃** **T₂₆₄** **T₂₆₅** **T**

4. Select when you would like the job to run.

JOB SCHEDULING INFORMATION

Run Job?

☒ Do you want to run job Once ?

☐ Do you want to schedule this job for future ?

Job will be scheduled according to the server time. Current server time is - 5/1/2017 14:40:57

- Select **Do you want to run job Once?** to run now.
- Select **Do you want to schedule this job for future?** to run the job later and complete the relevant fields.

☒ Do you want to schedule this job for future ?

Select how often you want the job to run

Start Job At *

02:38:00 PM

NOTE: This is the server time

Run Every *

Seconds

Stop after

Times

5. **Save** job.
6. Click **Run**.
7. Review the job status to ensure data was loaded successfully.

The Job Monitor screen for this job will appear automatically. To find specific jobs, navigate to **Menu > Operations Center > Job Monitor** and select **Lookup Import** from left navigation panel.

JOBS FOR LOOKUP DATA IMPORT				
Job Name	Creation Date	Start Date	Next Trigger Date	Job Status
LOOKUPDATA_LOOKUPTABLE_LOOKUPTYPE_1493426190818 CREATED BY: ADMIN / JOB TYPE: LOOKUP DATA IMPORT EDIT JOB RELOAD JOB DELETE JOB	FRI, 28 APR 2017 @ 06:36:34.000 PM	START DATE: FRI, 28 APR 2017 @ 06:36:34.000 PM END DATE: FRI, 28 APR 2017 @ 06:36:34.000 PM	NOT SCHEDULED	COMPLETED


First 10 Last Show 10

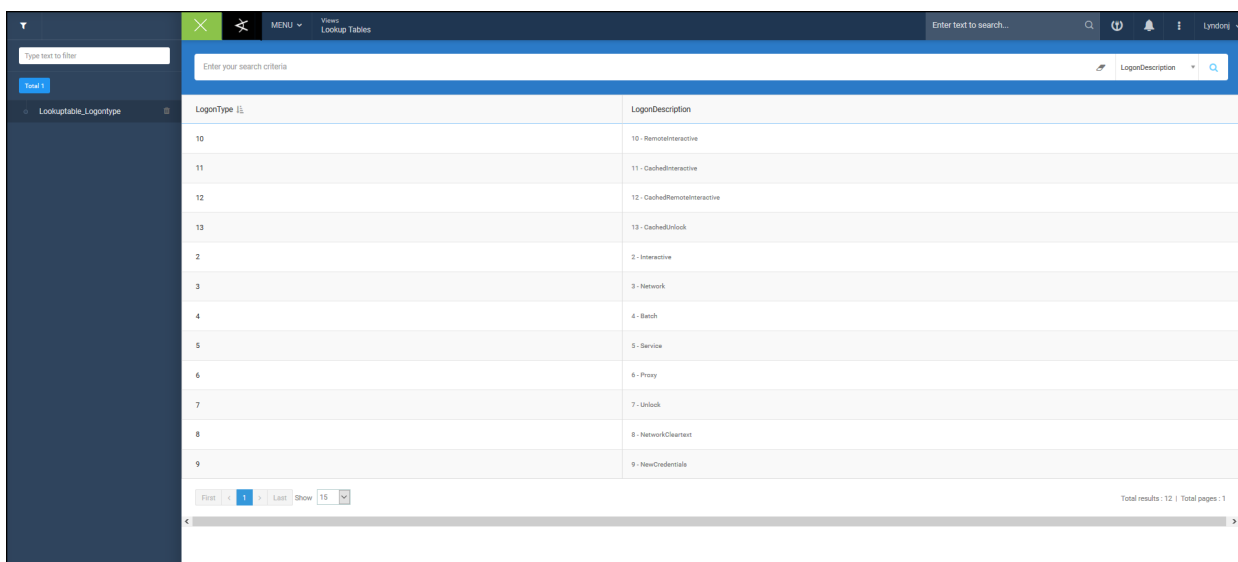
Total results: 1 | Total pages: 1

View Lookup Tables

1. Navigate to **Menu > Views > Lookup Tables** to check that the data was loaded successfully.



2. Click  to maximize the Lookup Tables left navigation menu.
3. Select the Lookup Table you created from the left navigation menu.



LogonType	LogonDescription
10	10 - RemoteInteractive
11	11 - CachedInteractive
12	12 - CachedRemoteInteractive
13	13 - CachedUnlock
2	2 - Interactive
3	3 - Network
4	4 - Batch
5	5 - Service
6	6 - Proxy
7	7 - Unlock
8	8 - NetworkClient
9	9 - NewCredentials



Note: For more information about [Views](#), see the ArcSight UBA User Guide.

Search Lookup Data using Spotter

Upon successful import, the lookup data will be available for searching in Spotter. To search lookup data in Spotter, complete the following steps:

1. Navigate to **Menu > Security Center > Spotter**.
2. Type `index=lookup` in search bar and click search icon.

key	lookupname	value_LogonDescription
9	LookupTable_LogonType	9-NewCredentials
8	LookupTable_LogonType	8-NetworkClearTest
7	LookupTable_LogonType	7-Unlock
6	LookupTable_LogonType	6-Proxy
5	LookupTable_LogonType	5-Service



Note: Click for more information about searching [Spotter](#) or see the ArcSight UBAUser Guide.

Geolocation/Network Map Data

Geolocation data represents the location information for IP addresses (city, state, country, etc.). The Network map represents the zone for the IP addresses (for example, LAN, DMZ, VPN, WIFI-contiguous IP addresses). The application indexes the geolocation/network map data and uses it to enrich event data. By inserting the geolocation/network map information in every event, the application can use this data for threat detection, reporting, and alerting. Geolocation data is typically imported from Maxmind (GeoIPCityLite DB) then normalized and indexed into the ipmapping core.

Geolocation/Network Map Data is enabled during [Activity Data](#) during Step 3: Performing Conditional Actions.

The geolocation import can be run as a scheduled job to get the latest available geolocation data from Maxmind.

The Network map is imported from a comma delimited flat file. The application supports CIDR (Classless Inter-Domain Routing), formatted IP addresses, and IP ranges (from-to).

Steps to import Geolocation/Network Map Data in ArcSight UBA:

1. Import Geolocation data from Maxmind
2. Import Network Map data.
3. Schedule and run the job.

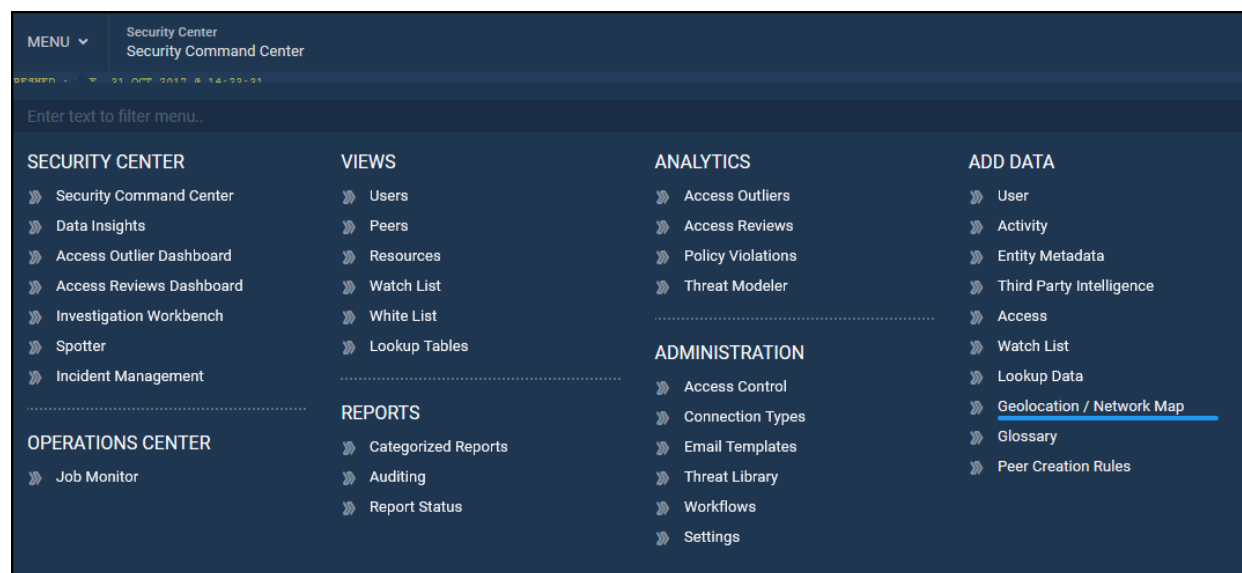
Ingesting Geolocation/Network Map Data



Step 1: Importing Geolocation Data from Maxmind

The application connects to the MaxMind geolocation site (http://geolite.maxmind.com/download/geoip/database/GeoLiteCity_CSV/GeoLiteCity-latest.zip) and downloads the latest geolocation mapping.

To import geolocation data from Maxmind navigate to **Menu > Add Data > Geolocation/Network Map** and complete the following steps.



Select Source Type

1. Select **Maxmind** from **Available Configurations** dropdown.
If Maxmind is not present, select **New Configuration** to create a new connection.

1 Select source type Run job

Select Connection to use to import lookup data.
You can create a new connection by selecting
Create New from the Connection drop down.

EXISTING CONNECTION NEW CONNECTION

AVAILABLE CONFIGURATIONS

Available configurations *


MaxMind

DELETE CONFIGURATION

AVAILABLE CONFIGURATIONS

Available configurations *

MaxMind

 **DELETE CONFIGURATION**

Configuration Name*

MaxMind


Select source from where to import the data







Select source type

Maxmind

Select source from where to import the data

For example -
Map's attributes like "IP From" whose format is "a.b.c.d" to position "1".

Attribute Mapping 

Position*	Name	
2	IP To (a.b.c.d)	 
1	IP From(a.b.c.d)	 
3	Country Code	 

Connection

Maxmind

Convert IP

YES ☒

2. Enter **Maxmind** for **Configuration Name** (if not present).
3. Select **Maxmind** for **Source Type**.
4. Set the **Position** and **Name** of attributes in **Attribute Mapping** as follows:
 - a. Position 1: IP From (a, b, c, d)
 - b. Position 2: IP To (a, b, c, d)
 - c. Position 3: Country Code



Use  to add/remove attributes.

5. Set **Connection Type** to Maxmind.
6. Enable **Convert IP** slider to **Yes**.
7. Click **Save and Next** to proceed to [Step 3: Running Job](#).

Step 2: Importing Network Map Data from a Delimited File

A network zone represents a contiguous block of IP addresses that is provided with a name. Generally, the network zones are provided in a CIDR notation. For example, the block 192.168.100.0 represents the 1024 IPv4 addresses from 192.168.100.0 to 192.168.103.255. The same information may be provided in the form of IP From, IP To, location, as this format is also supported.

When ingesting network map data in CIDR block format, the application converts the IP address block to a range of integers.

For example:

10.30.0.0/12 - USA will be converted to:

Start IP: 10.16.0.0 (168820736)

End IP: 10.31.255.255 (169869311)

10.30.150.0/24 - USA_Sanfrancisco will be converted to:

Start IP: 10.30.150.0 (168820736)

End IP: 10.30.150.255 (169869311)

If the application receives an IP address in an event, for example 10.30.150.10 (169776650), the query will look like this:

```
Get Country from IP_Mapping where Start_IP,169776650 and Last_IP>169776650
```

You will receive results for both USA and USA_Sanfrancisco, and the first result that you get will be associated with the country (USA).

Insert the network map into the ArcSight UBA application in this order so that the city is the first result from the query:

10.30.150.0/24 - USA_Sanfrancisco

10.30.150.8/29

10.30.0.0/12 - USA


To import network map data from a delimited file, navigate to **Menu > Add Data > Geolocation/Network Map** and complete the following steps:


1

Select source type

Run job

Select Connection to use to import lookup data.
You can create a new connection by selecting
Create New from the Connection drop down.

 EXISTING
CONNECTION

 NEW
CONNECTION

AVAILABLE CONFIGURATIONS

Configuration Name*

Select source from where to import the data

Select source type*

File ▼

Select source from where to import the data



Source Folder*

\$(SECURONIX_HOME)/import/in

Source File*
Enter Filename

BROWSE

Attribute Mapping

Position*	Name	
<div>1</div>	<div>IP From (a.b.c.d)▼</div>	<div> </div>

Specify which attribute value is at which column position.

1. Click **New Connection**.
2. Enter a **Configuration Name**.
3. Select **File** for **Source Type**.
4. Specify a **Source Folder**. Default \${SECURONIX_HOME}/import/in.



Note: You must place the file to import into the /securonix_home/import/in folder before importing into the ArcSight UBA application.

5. Enter name of the delimited file for **Source File** or **Browse** to select the file on a local machine (e.g. .cidr, .csv).
6. Set the **Position** and **Name** of attributes in **Attribute Mapping** as follows:
 - a. Position 1: Select from dropdown. Example: CIDR Field (a, b, c, d/24).
 - b. Position 2: Select from dropdown. Example: Location.



Use to add/remove attributes.

7. Enable **Delete Old Network Classification** slider to **Yes** if you would like to delete the old classification. Default **No**.
8. Click **Save and Next** to proceed to [Step 3: Running Job](#).

Step 3: Running Job

Geolocation/Network Map Data

Select source type Run job

Prev Save Run

JOB DETAILS

Job Name*

GeolocationImport_Maxmind_2017_5_1_14_37

Job Description

Geolocation Import Job

Enable Job Related Notifications

NO

JOB SCHEDULING INFORMATION

Run Job

Do you want to run job Once ?

Do you want to schedule this job for future ?

Job will be scheduled according to the server time. Current server time is - 5/1/2017 14:39:45

1. Enter a unique **Job Name** or use the default name.
2. Enter a **Job Description** or use the default description.
3. **Enable Job Related Notifications** if you would like to receive email notifications when the job is run.
 - a. If **No**: Proceed without entering additional information.
 - b. If **Yes**:
 - **On Success**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template:
 - **On Failure**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template.
 - **On Misfired**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template.
 - **On Completed with Errors**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications.

You can also create a new email template:

Create New Email Template

Sender Name* ⓘ

Template Name* ⓘ

Description

To* ⓘ

From*

test@securonix.com

CC ⓘ

BCC ⓘ

Subject ⓘ

HTML Enabled

☒ YES

Store in Outbox prior to sending?

☒ YES

Use this template for *

Job Misfired

Owner ⓘ

Administrators

SECURITYOPERATIONS

Email Body ⓘ

[Add Email Template Variables](#)

B I U abc x2 x3 T- T+ H+ T+

4. Select when you would like the job to run.

JOB SCHEDULING INFORMATION

Run Job ⓘ

☒ Do you want to run job Once ?

☐ Do you want to schedule this job for future ?

Job will be scheduled according to the server time. Current server time is - 5/1/2017 14:40:57

- Select **Do you want to run job Once?** to run now.
- Select **Do you want to schedule this job for future?** to run the job later and complete the relevant fields.

☒ Do you want to schedule this job for future ?

Select how often you want the job to run

Start Job At *

02:38:00 PM

NOTE: This is the server time

Run Every *

Seconds

Stop after

Times

5. **Save** job.

6. Click **Run**.

Review Job Status

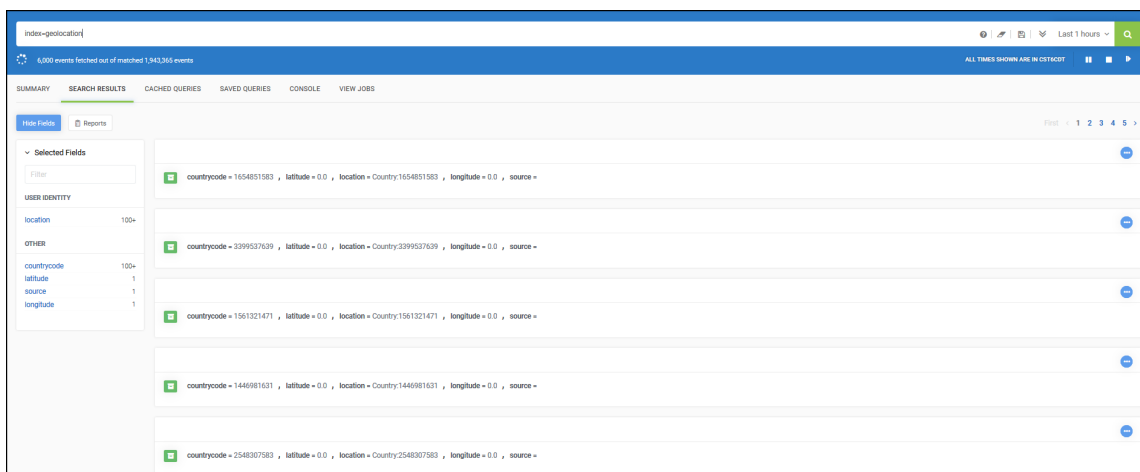
Review the job status to ensure data was loaded successfully:

Job Name	Creation Date	Start Date	Next Trigger Date	Job Status
GEOLOCATIONIMPORT_MAXMIND_2017_5_8_13_15_15 CREATED BY: ADMIN / JOB TYPE: POPULATE GEOLOCATION JOB EDIT JOB DELETE JOB	MON, 8 MAY 2017 @ 01:15:23.000 PM	START DATE: MON, 8 MAY 2017 @ 01:15:23.000 PM END DATE:	MON, 8 MAY 2017 @ 01:15:22.784 PM	IN-PROGRESS
BLUECOATPROXYIPT_DELIMITED-COMMA_05_07_2017_08_34_39_PM CREATED BY: ADMIN / JOB TYPE: ACTIVITY IMPORT EDIT JOB DELETE JOB	SUN, 7 MAY 2017 @ 08:34:48.000 PM	START DATE: SUN, 7 MAY 2017 @ 08:34:48.000 PM	NOT SCHEDULED	IN-PROGRESS
WINDOWSPID_DELIMITED-COMMA_05_07_2017_08_01_51_PM CREATED BY: ADMIN / JOB TYPE: ACTIVITY IMPORT EDIT JOB RE-RUN JOB DELETE JOB	SUN, 7 MAY 2017 @ 08:04:46.000 PM	START DATE: SUN, 7 MAY 2017 @ 08:04:46.000 PM	NOT SCHEDULED	COMPLETED
JSONH_JSON_05_05_2017_12_40_01_PM CREATED BY: ADMIN / JOB TYPE: ACTIVITY IMPORT EDIT JOB DELETE JOB	FRI, 5 MAY 2017 @ 12:40:05.000 PM	START DATE: FRI, 5 MAY 2017 @ 12:40:05.000 PM	NOT SCHEDULED	IN-PROGRESS
JSONH_JSON_05_04_2017_05_38_13_PM		START DATE:		

Search Geolocation Data using Spotter

Upon successful import, the entity metadata will be available for searching in Spotter. To search events in Spotter, complete the following steps:

1. Navigate to **Menu > Security Center > Spotter**.
2. Type `index=geolocation` in search bar and click search icon.



Note: Click for more information about searching [Spotter](#) or see the ArcSight UBA User Guide.

Entity Metadata

The ArcSight UBA application uses entity and asset metadata at the time of ingestion to transform raw events into meaningful information that easy to understand, search , and investigate. You can import entity meta-data to super enrich events for the following resources:

- Resources: The assets on your network such as workstations, laptops and servers.
- IP addresses: The IP addresses of the assets on your network.
- Activity Account: The user accounts performing activity on your network.

Steps to import Entity Metadata in ArcSight UBA:

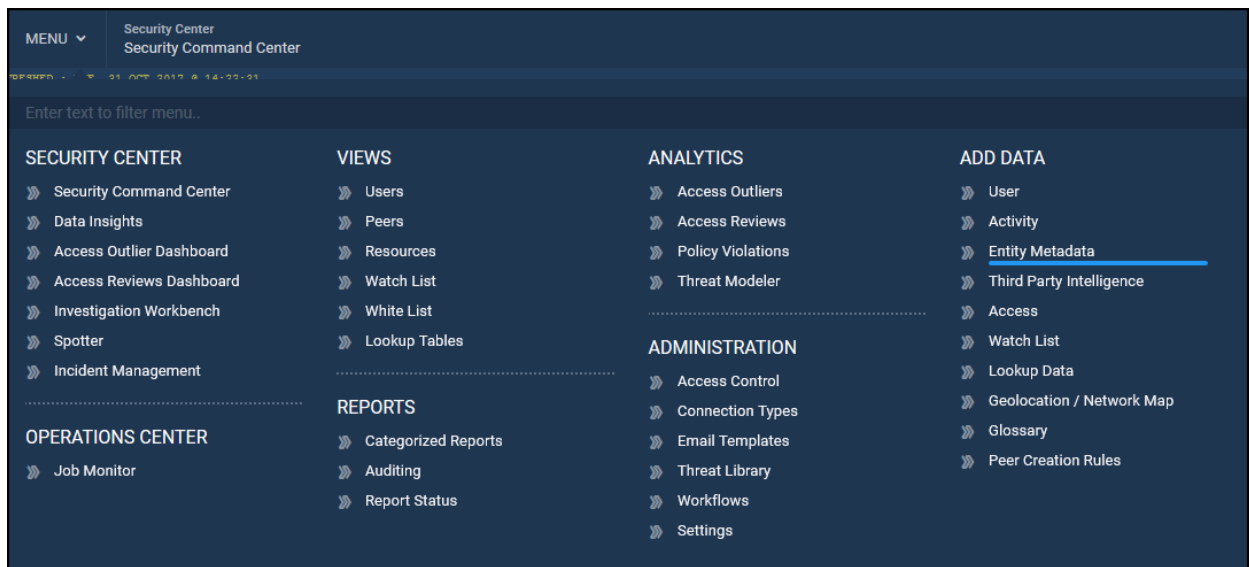
1. Create a connection to import from file or database.
2. Map Attributes with corresponding ArcSight UBA attributes.
3. Schedule and run the job.

Ingesting Entity Metadata



Step 1: Creating a Connection

1. Navigate to **Menu > Add Data > Entity Metadata**.



2. Click **New Connection** to create a new connection from a file or database.


1


Select Connection

Configure Attribute Mapping

Run job

Select Connection to import Entity meta-data. You can create a new connection or select a existing Connection from the drop down.

 EXISTING CONNECTION

 NEW CONNECTION

ENDPOINT RESOURCE INFORMATION

Connection Type*

-Select- ▼

Connection Name*

New Connection Name

MetaData Entity*

IP Address ▼

Select meta data entity for which you are importing data.

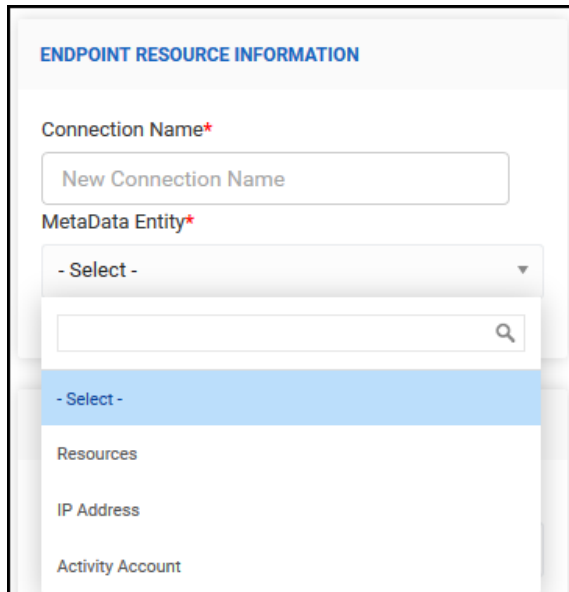
CONNECTION DETAILS

CONNECTION PROPERTIES

PREVIEW INPUT

Importing Entity Metadata from a File

Endpoint Resource Information



The screenshot shows a web form titled "ENDPOINT RESOURCE INFORMATION". It contains two main sections. The first section is labeled "Connection Name*" and has a text input field with the placeholder text "New Connection Name". The second section is labeled "MetaData Entity*" and features a dropdown menu. The dropdown menu is open, showing a search bar with a magnifying glass icon and a list of options: "- Select -", "Resources", "IP Address", and "Activity Account". The "Resources" option is currently selected and highlighted in blue.

1. Click **New Connection**.
2. Select **File Import** from **Connection Type** dropdown.
3. Enter a unique **Connection Name**.
4. Select a **MetaData Entity** from the dropdown:
 - Resources
 - IP Address
 - Activity Account

Connection Details

CONNECTION DETAILS

Upload a file?
☐ NO

File Name*

Name of the file containing data to import. Example: ad-dc-001.csv, ad-dc-001.log, ad-dc-001.txt.
This file must be located in /Securonix/tenants/partnerdemo /securonix_home/import/in.

Column Delimiter*

Specify the delimiter between the fields in the input file. Example: , (comma) | (pipe)

Exclude Header
☐ NO

Number of lines to Ignore

Delete Old Entity Metadata
☐ NO

1. Toggle **Upload a File?** slider:
YES: Browse to upload a file on your local machine.
NO: Specify the complete path to the folder in which the file to be imported is located. Default: \$securonix_home/import/in.
2. Specify the **Column Delimiter** if required for the file type.
3. Use slider to **Exclude Header**.
 - a. For **No**: Proceed to next step.
 - b. For **Yes**: Specify the number of lines to ignore.
4. Toggle **Delete Old Entity Metadata** to **Yes** to delete old data and replace with new import.

Connection Properties

Import from Remote Server?

☒ YES

Use FTP/SFTP/SCP to ingest file located in a remote location?

Remote Connection Type*

HTTP

Url*

Username

admin

Password

Source directory

Proxy Server?

☐ NO

This is a server that all computers on the local network have to go through before accessing information on the Internet.

Test Remote Connection?

TEST

1. Enable **Import from Remote Server?** to use FTP/SFTP/SCP to ingest the file located in a remote location.
 - a. If **No**: Proceed to next step.
 - b. If **Yes**: Enter the following information:
 - a. Select a **Remote Connection Type** from the dropdown.
 - b. Enter the **Host IP Address** (for FTP, SFTP, etc.) or **URL** (for HTTP, HTTPS).
 - c. Enter the **Port Number** (for FTP, SFTP, etc.). Default 22.
 - d. Enter the **Username**.
 - e. Enter the **Password**.
 - f. Enter the **Source Directory**.
 - g. Select **Yes** or **No** for **Proxy Server?**.
 - a. If **No**: Proceed to next step.
 - b. If **Yes**: Enter **Proxy Server URL, Username**, and **Password**.
 - h. **Test** the remote connection.
2. Specify the **Source Folder** in which the file is located. Default \${SECURONIX_HOME}/import/in.

`${SECURONIX_HOME}` is set to `/Securonix/tenants/snypr6/securonix_home`.
 You can also replace `${SECURONIX_HOME}` below with the direct path to the folder where the file exists.
 Example: `/Users/dev/files/`

Source Folder*

`${SECURONIX_HOME}/import/in`

Enter the complete path to the directory where this file is located.

Success Folder*

`${SECURONIX_HOME}/import/success`

Enter the complete path to the directory where this file must be moved once the import is completed successfully.

Failed Folder*

`${SECURONIX_HOME}/import/failed`

Enter the complete path to the directory where this file must be moved if the import job fails to complete.



Note: `${SECURONIX_HOME}` is set to `/Securonix/tenants/snypr6/securonix_home`. You can replace `${SECURONIX_HOME}` with the direct path to the folder where the file exists. Example: `/Users/dev/files/`.

3. Specify the **Success Folder** into which to move the file once the import is completed successfully. Default `${SECURONIX_HOME}/import/success`.
4. Specify the **Failed Folder** into which to move the file if the import job fails to complete. Default `${SECURONIX_HOME}/import/failed`.



5. Click  to **Preview Input**.

Select Connection to import Entity meta-data. You can create a new connection or select an existing Connection from the drop down.

EXISTING CONNECTION **NEW CONNECTION**

ENDPOINT RESOURCE INFORMATION

Connection*
Dallas Asset Inventory

MetaData Entity*
MetaData Entity

IP Address

Select meta data entity for which you are importing data.

CONNECTION DETAILS

Connection Type*
File Import

Upload a file?
☐

Exclude Header
☐

Include/Exclude Headers from input file.
Number of lines to ignore
1

PREVIEW INPUT

Device Name , Owner , IP Address , Device Vendor , Model , Operating System , OS Version , Processor , Memory , Serial Number ,
tanujmacbookpro-6.local , Gulati , Apple , MacBook Pro , Mac OS Sierra , 10.12.3 , 3.2 GHz Intel Core i7 , 16 Gb 1600 MHz DDR3 ,
Mac , Natarajan , Apple , MacBook Air , Mac OS Sierra , 10.12.3 , 1.4 GHz Intel Core i5 , 8 GB 1600 MHz DDR3 ,
Siddhant PC , Siddhant , DHCP , Dell , Dell Inspiron , Microsoft Windows , Windows 10 Pro , 2.4GHz Intel Core i7 , 16 GB 1600 MHz DDR3 ,
Joey's MacBook Air , Joey , dynamic IP , Apple , MacBook Air , Mac OS Sierra , 10.12.3 , 1.6 Gh Intel Core i5 , 8 GB 1600 MHz DDR3 , C1M
DESKTOP-BHRG08C , Satish , Dell , Dell Inspiron15 , Microsoft Windows , Windows 10 , 2.4GHz Intel Core i7 , 16GB ,
Ishan's MacBook Pro , Ishan , Apple , MacBook Pro , OS X El Capitan , 10.11.6 , 2.2 GHz Intel Core i7 , 16 GB 1600 MHz DDR3 ,
Akash-Socio-MacBook-Pro , Akash , Apple , MacBook Pro , Mac OS Sierra , 10.12.3 , 2.5 GHz Intel Core i7 , 16 GB ,
Rakesh's MacBook Pro , Rakesh , Apple , MacBook Pro , Mac OS Sierra , 10.12.3 , 2.2 GHz Intel Core i7 , 16 GB ,
Omkar's MacBook Pro , Omkar , Apple , MacBook Pro , OS X El Capitan , 10.11.6 , 2.2 GHz Intel Core i7 , 16 GB 1600 MHz DDR3 ,
Kamlesh'sMacBookPro , Kamlesh , Apple , MacBook Pro , OS X El Capitan , 10.11.1 , 2.2 GHz Intel Core i7 , 16 GB 1600 MHz DDR3 ,
MacBook-Pro-3.local , Praful , Apple , MacBook Pro (15-inch, 2016) , MacOS Sierra , 10.12.3 (16032) , 2.7 GHz Intel Core i7 , 16 GB 2133 MHz LPDDR3 ,
Dell Laptop , Preetham , Dell , Dell Latitude E5470 , Microsoft Windows , Windows 10 , 2.6 GHz Intel Core i7 , 16 GB ,

6. Click **Save and Next** to proceed to Configuring Attribute Mapping.

Importing Entity Metadata from a Database

Endpoint Resource Information

ENDPOINT RESOURCE INFORMATION

Connection Type*
Database Import

Connection*
DallasAssetInventory

MetaData Entity*
Resources

Select meta data entity for which you are importing data.

1. Click **New Connection**.
2. Select **Connection Type** from dropdown.
3. Enter a unique **Connection Name**.
4. Select a **MetaData Entity** from the dropdown.
 - Resources
 - IP Address
 - Activity Account

Connection Details

CONNECTION DETAILS

Delete Old Lookup Data

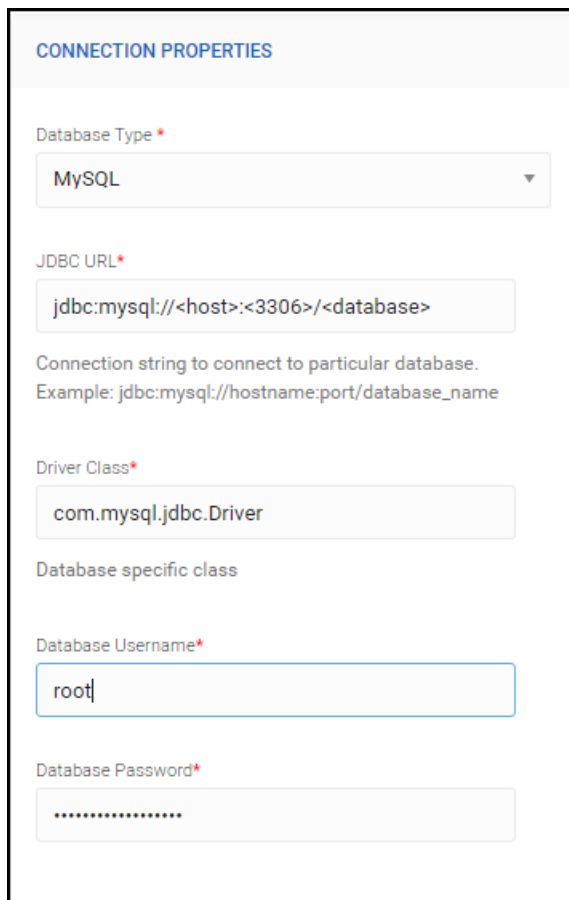
☐ NO

SQL Query*

```
select id, resourcename, ownerid, ownertype,
criticality from resources;
```

1. Toggle **Delete Old Lookup Data** to **Yes** to delete old data and replace with new metadata.
2. Enter the **Query**. Example: `select id, resourcename, ownerid, ownertype, criticality from resources;`

Connection Properties

A screenshot of a web form titled "CONNECTION PROPERTIES". The form contains several input fields: a dropdown menu for "Database Type" with "MySQL" selected; a text field for "JDBC URL" containing "jdbc:mysql://<host>:<3306>/<database>"; a text field for "Driver Class" containing "com.mysql.jdbc.Driver"; a text field for "Database Username" containing "root"; and a password field for "Database Password" with masked characters. There is also a small text block explaining the JDBC URL format with an example.

CONNECTION PROPERTIES

Database Type *

MySQL

JDBC URL *

jdbc:mysql://<host>:<3306>/<database>

Connection string to connect to particular database.
Example: jdbc:mysql://hostname:port/database_name

Driver Class *

com.mysql.jdbc.Driver

Database specific class

Database Username *

root

Database Password *

.....

1. Select the **Database Type** from the dropdown.
2. Enter the **JDBC URL** to connect to a particular database. Example: jdbc:mysql://<host>:<3306>/<database>.
3. Specify the database specific **Driver Class**. Example: com.mysql.jdbc.Driver.
4. Enter the **Database Username** and **Password**.
5. Review the input in the **Preview Input** pane.
6. Click **Save and Next** to proceed to [Step 2: Configure Attribute Mapping](#).

Importing Entity Metadata from Qualys

Prerequisite

To import Entity Metadata from Qualys, you must configure the required connection credentials:

1. Navigate to `../securonix_home/connectorapis/qualys/src` folder.
2. Open **config.txt**.
3. Enter connection credentials.

Endpoint Resource Information

ENDPOINT RESOURCE INFORMATION

Connection Type*

Qualys

Connection Name*

EntityMetadata_1508787316697

MetaData Entity*

Resources

Select meta data entity for which you are importing data.

1. Select **Qualys** from **Connection Type** dropdown.
2. Enter a unique **Connection Name**.
3. Select **MetaData Entity** from dropdown:
 - Resources
 - IP Address
 - Activity Account

Connection Details

CONNECTION DETAILS

NOTE

Please use the 'config.txt' file to fill in the required connection credentials. This file is present at `~/securonix_home/connectorapis/qualys/src/`

Date Launched After [Date format: yyyy-MM-dd]

2017-01-01

All the scans launched after this date will be retrieved. By default, all scans launched after 2017-01-01 will be retrieved.

1. Enter a **Date Launched After** in yyyy-MM-dd format. All scans launched after this date will be retrieved. Default: 2017-01-01.

Importing Entity Metadata from Tanium

Prerequisites

To import Entity Metadata from Tanium, you will need the following information for your Tanium server:

- **API Username:** User name to connect to the UI.
- **API Password:** Password associated with the API user name
- **API IP Address:** IP Address of the Server.

Endpoint Resource Information

ENDPOINT RESOURCE INFORMATION

Connection Type*

Tanium

Connection Name*

EntityMetadata_1508788261691

MetaData Entity*

Resources

Select meta data entity for which you are importing data.

1. Select **Tanium** from **Connection Type** dropdown.
2. Enter a unique **Connection Name**.
3. Select **MetaData Entity** from dropdown:
 - Resources
 - IP Address
 - Activity Account

Connection Details

CONNECTION DETAILS

API Username*

 Username to connect to the API.

API Password*

 Password associated with the above Username.

API IP Address*

 IP Address of the Server.

1. Enter **API Username**.
2. Enter **API Password** associated with the Username.
3. Enter the **API IP Address** of the Tanium server.

Step 2: Configure Attribute Mapping

3 Select Connection **Configure Attribute Mapping** Run job Prev Save & Next

Specify column positions in file that map to Meta data Fields


Position	Value	Is indexed key	Action
<input type="text" value="1"/>	<input type="text" value="Device Name"/>	<input type="checkbox"/> NO	+ -
<input type="text" value="10"/>	<input type="text" value="Serial Number"/>	<input type="checkbox"/> NO	+ -
<input type="text" value="2"/>	<input type="text" value="Owner"/>	<input type="checkbox"/> NO	+ -
<input type="text" value="3"/>	<input type="text" value="IP Address"/>	<input checked="" type="checkbox"/> YES	+ -
<input type="text" value="4"/>	<input type="text" value="Device Vendor"/>	<input type="checkbox"/> NO	+ -
<input type="text" value="5"/>	<input type="text" value="Model"/>	<input type="checkbox"/> NO	+ -
<input type="text" value="6"/>	<input type="text" value="Operating System"/>	<input type="checkbox"/> NO	+ -
<input type="text" value="7"/>	<input type="text" value="OS Version"/>	<input type="checkbox"/> NO	+ -
<input type="text" value="8"/>	<input type="text" value="Processor"/>	<input type="checkbox"/> NO	+ -
<input type="text" value="9"/>	<input type="text" value="Memory"/>	<input type="checkbox"/> NO	+ -



Note: For a complete list of attributes in ArcSight UBA, see [Appendix A: ArcSight UBA Attribute Schema](#).

1. Specify the column **Position** and **Value** for each column in the file that map to metadata fields.
2. Enable **Is indexed key** to specify the primary key for the table.



3. Use  to add/remove entries.
4. Click **Save and Next** when all metadata fields have been mapped to proceed to [Step 3: Running the Job](#).

Step 3: Running the Job

Job Details

1. Specify a **Job Name** or use auto-generated name.
2. Enter a **Job Description**.
3. **Enable Job Related Notifications** if you would like to receive email notifications when the job is run.
 - a. If **No**: Proceed without entering additional information.
 - b. If **Yes**:
 - **On Success**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template:
 - **On Failure**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template.

- **On Misfired:**Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template.
- **On Completed with Errors:** Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template:

Create New Email Template

Sender Name* ⓘ

Template Name* ⓘ

Description

To* ⓘ

From*
test@securonix.com

CC ⓘ

BCC ⓘ

Subject ⓘ

HTML Enabled
YES ☒

Store in Outbox prior to sending?
YES ☒

Use this template for *

Owner ⓘ
Administrators
SECURITYOPERATIONS

Email Body ⓘ
Add Email Template Variables

Rich text editor toolbar:

Job Scheduling Information

1. Select when you would like the job to run.

JOB SCHEDULING INFORMATION

Run Job ⓘ

☒ Do you want to run job Once ?

☐ Do you want to schedule this job for future ?

i Job will be scheduled according to the server time. Current server time is - 5/1/2017 14:40:57

- Select **Do you want to run job Once?** to run now.
- Select **Do you want to schedule this job for future?** to run the job later and complete the relevant fields.

☒ Do you want to schedule this job for future ?

✓ Seconds Minutes Hourly Daily Weekly Monthly Specify Date

Select how often you want the job to run

Start Job At *

02:38:00 PM

NOTE: This is the server time

Run Every *

Seconds

Stop after

Times

2. **Save** job.
4. Review the job status to ensure data was loaded successfully.
The Job Monitor screen for this job will appear automatically. To find specific jobs, navigate to **Menu > Operations Center > Job Monitor** and select **Entity Metadata Import** from left nav-

igation panel.

Job Name	Creation Date	Start Date	Next Trigger Date	Job Status
RESOURCEDATA_DEMOSERVER_NAME_2017_9_6_22_37_25 CREATED BY: ADMIN / JOB TYPE: ENTITY METADATA EDIT JOB RE-RUN JOB DELETE JOB	THU, 7 SEP 2017 @ 12:37:27.000 AM	START DATE: THU, 7 SEP 2017 @ 12:37:27.000 AM END DATE: THU, 7 SEP 2017 @ 12:37:27.000 AM	NOT SCHEDULED	COMPLETED
RESOURCEDATA_WORKSTATION_IPADDRESS_2017_9_6_17_8_38 CREATED BY: ADMIN / JOB TYPE: ENTITY METADATA EDIT JOB RE-RUN JOB DELETE JOB	WED, 6 SEP 2017 @ 07:00:44.000 PM	START DATE: WED, 6 SEP 2017 @ 07:00:44.000 PM END DATE: WED, 6 SEP 2017 @ 07:00:44.000 PM	NOT SCHEDULED	COMPLETED

Total results : 2 | Total pages : 1

- Review the job status to ensure data was loaded successfully.

The Job Monitor screen for this job will appear automatically. To find specific jobs, navigate to **Menu > Operations Center > Job Monitor** and select **Entity Metadata Import** from left navigation panel.

Job Name	Creation Date	Start Date	Next Trigger Date	Job Status
RESOURCEDATA_DEMOSERVER_NAME_2017_9_6_22_37_25 CREATED BY: ADMIN / JOB TYPE: ENTITY METADATA EDIT JOB RE-RUN JOB DELETE JOB	THU, 7 SEP 2017 @ 12:37:27.000 AM	START DATE: THU, 7 SEP 2017 @ 12:37:27.000 AM END DATE: THU, 7 SEP 2017 @ 12:37:27.000 AM	NOT SCHEDULED	COMPLETED
RESOURCEDATA_WORKSTATION_IPADDRESS_2017_9_6_17_8_38 CREATED BY: ADMIN / JOB TYPE: ENTITY METADATA EDIT JOB RE-RUN JOB DELETE JOB	WED, 6 SEP 2017 @ 07:00:44.000 PM	START DATE: WED, 6 SEP 2017 @ 07:00:44.000 PM END DATE: WED, 6 SEP 2017 @ 07:00:44.000 PM	NOT SCHEDULED	COMPLETED

Total results : 2 | Total pages : 1

Search using Spotter

Upon successful import, the entity metadata will be available for searching in Spotter. To search events in Spotter, complete the following steps:

1. Navigate to **Menu > Security Center > Spotter**.
2. Type `index=asset` in search bar and click search icon.

index=asset

782 events fetched out of matched 782 events

ALL TIMES SHOWN ARE IN CST/CDT

SUMMARY SEARCH RESULTS CACHED QUERIES SAVED QUERIES CONSOLE VIEW JOBS

Hide Fields Reports

Selected Fields

Filter

OTHER

key_Serveripaddress 100+

key_ServerOS 94

key_Servermacaddress 100+

key_Id 100+

key_Servernetworkname 3

key_Serverfqdn 100+

entityname 100+

key_Workstation_MacAddr... 100+

key_Servercategory 6

entitytype 1

key_Workstation_Name 100+

key_Workstation_Owner 100+

key_Workstation_OS 2

entityname = 2*-RWC0DC0896 , entitytype = Resources , key_ServerOS = Cent-OS 5.6 , key_Servercategory = POS , key_Serverfqdn = RWC-9896.scmx.com , key_Serveripaddress = 10.0.1.164 , key_Servermacaddress = 4:15:4C:96:27:47:47 , key_Servernetworkname = Redwood City Data Center , key_Id = 66

entityname = 2*-RWC0DC0893 , entitytype = Resources , key_ServerOS = RHEL 6.8 , key_Servercategory = PCI Assets , key_Serverfqdn = RWC-8953.scmx.com , key_Serveripaddress = 10.0.1.141 , key_Servermacaddress = 3:34:6C:53:12:11:0 , key_Servernetworkname = Redwood City Data Center , key_Id = 43

entityname = 2*-RWC0DC08177 , entitytype = Resources , key_ServerOS = Cent-OS 6.2 , key_Servercategory = PCI Assets , key_Serverfqdn = RWC-8177.scmx.com , key_Serveripaddress = 10.0.1.105 , key_Servermacaddress = 11:22:9C:77:3:45:56 , key_Servernetworkname = Redwood City Data Center , key_Id = 7

entityname = 2*-RWC0DC0725 , entitytype = Resources , key_ServerOS = Cent-OS 7.2 , key_Servercategory = PCI Assets , key_Serverfqdn = RWC-7725.scmx.com , key_Serveripaddress = 10.0.1.145 , key_Servermacaddress = 1:32:1C:25:1:57:22 , key_Servernetworkname = Redwood City Data Center , key_Id = 47



Note: Click for more information about searching [Spotter](#) or see the ArcSight UBA User Guide.

Access Data

The ArcSight UBA application is designed to support the access privilege schema of nearly any application. By importing access privileges and correlating the accounts on these systems with the user identity, ArcSight UBA enables the centralized monitoring of user access.

Typical sources of access privilege data include:

- Operating Systems
- Databases
- Commercial Applications (SAP, Siebel, Oracle Financials, Peoplesoft, etc.)
- Custom Applications (homegrown apps)
- Directories (including Active Directory)
- Network Devices
- Identity Management Systems (Oracle Identity Manager, Sun Identity Manager, Tivoli Identity Manager)
- Access Governance products (Oracle Identity Analytics, Sailpoint, Aveksa, CA Role and Compliance Manager)

Example

User is a member of multiple Groups in Active Directory that allows the user to get access to the Windows Desktop, VPN Access, Remote Desktop, Internet Access, Exchange Mailbox etc. The Groups are the access privileges for the User on Active Directory. Similarly, each application/platform has an access control model that ensures that the user is only able to access certain functionality/views within the application.

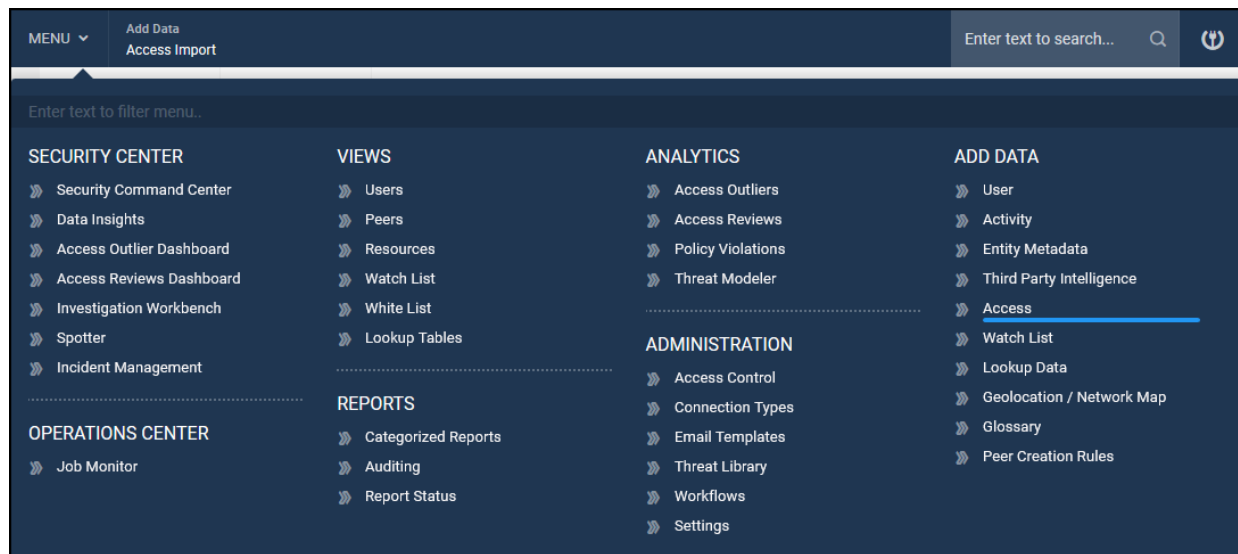
Access-related data for employees can be imported from different log files generated by different vendor tools. The Access Scanner can pull in these access files and import the data. To clarify:

- **Resource/Device** refers to the actual device itself.
- **Resource/Device Type** refers to applications, operating systems, server hosts, desktops, proxy servers, for example. The resource type may also represent the vendor name/-product/version whose device is being monitored (example: Bluecoat Proxy Server, Microsoft Windows 2008, IBM AIX5.1)
- **Resource Group** refers to the source of the event data. Resource Groups can be used to group resources together.

This section shows you how to import Access Data from the following sources:

- Active Directory
- Aveksa
- Database
- Files

To import Access Data into ArcSight User Behavior Analytics, navigate to **Menu > Add Data > Access**.



Complete the following steps.

Step 1: Selecting the Datasource

You can import access data from a variety of data sources using traditional connectors such as file and database, as well as API connectors such as Google Report. See the following for examples of specific datasources from which to import access data:

- [Importing from Active Directory](#)
- [Importing from Aveksa](#)
- [Importing from Database](#)
- [Importing from Files](#)

Importing Access Data

Importing from Active Directory

1. Click **Select Datasource** to select an existing datasource from the dropdown to edit OR **Create New Datasource** to create a new datasource.
2. Complete the following information:

General Details

GENERAL DETAILS

Datasource Name*

Provide a name to uniquely identify this connection.

IP Address

Specify IP address or hostname for the datasource

Select Device Type

Selection of existing Resource Type will automatically create the fields needed to store the event attributes and also the parsers to normalize the events. You may also create custom resource type by selecting the Create New Type option.

Input file format for the selected resource type is LDAP

- a. **Datasource Name:** Provide a unique name for the datasource.
- b. **IP Address:** Specify the IP Address or hostname for the datasource, if required.
- c. **Select Device Type:** Select from dropdown. Selection of an existing Device Type will automatically create the fields needed to store the event attributes and the parsers to normalize events. To create a custom resource type, complete the following:
 1. Select **Create a new type**.
 2. Enter the **Data Source Vender**. Example: Microsoft.
 3. Enter the **Data Source Functionality**. Example: Identity/Access Management.
 4. Provide the **Datasource Type**. Example: Active Directory.
 5. Select the **Format** from the dropdown. Example: File.
 6. Click **Save**.

Access Connection Details

ACCESS CONNECTION DETAILS

Connection Name*

Access_Data_ACCESS

Active_Directory_ACCESS

Provide a unique name for this connection. Do not use any white space in the name. Connections can also be managed from Configure->Connection Types.

Select a Connection Type*

Active Directory

Select the source from which to import data. You can import data from a delimited file (csv, pipe delimited etc), Active Directory or any other listed sources.

Select a Connection Type*

Active Directory ▼

Select the source from which to import data. You can import data from a delimited file (csv, pipe delimited etc), Active Directory or any other listed sources.

SSL?

☐ NO

Hostname*

ldap://10.0.1.250:389

Host name/IP address of LDAP server. Example:
ldap://10.1.12.123:389

LDAP Username*

test_A1

LDAP Password*

●●●●●●●●

Base Context *

DC=test,DC=securonix,DC=com

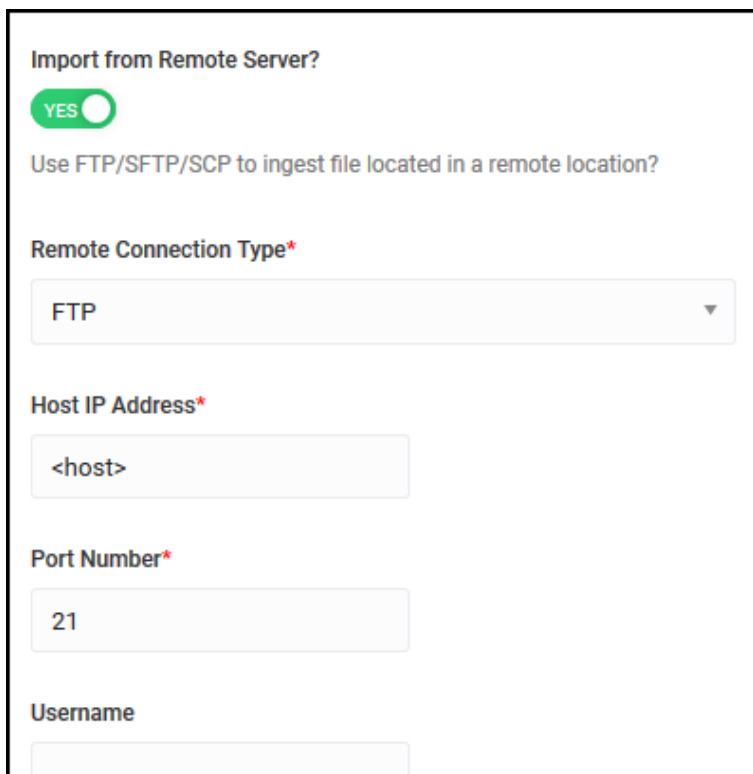
Specify the DNS name prefixed with DC. Example:
DC=Americas,DC=securonix,DC=com

Filter*

(&(objectCategory=person)(objectClass=User))

Specify search filter to search for users. Example:
(&(objectCategory=person)(objectClass=User)) will search

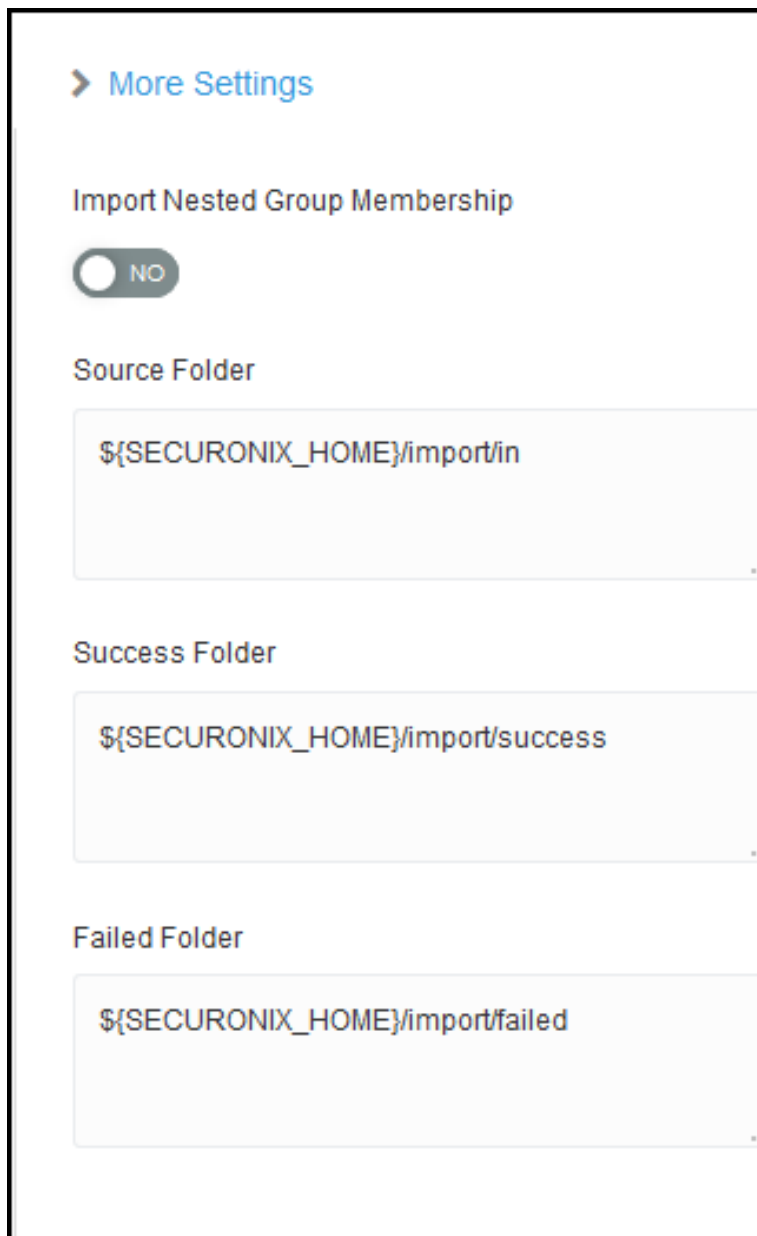
- a. **Connection Name:** Click inside the box to auto-populate or select an existing connection from the dropdown.
- b. **Select Connection Type:** Select Active Directory from dropdown.
- c. **Import from Remote Server?:** Enable to enter remote server details:



The screenshot shows a configuration form titled "Import from Remote Server?". At the top, there is a green toggle switch labeled "YES" which is currently turned on. Below the toggle is the text "Use FTP/SFTP/SCP to ingest file located in a remote location?". Underneath, there is a section for "Remote Connection Type*" with a dropdown menu currently set to "FTP". Below that is a text input field for "Host IP Address*" containing the placeholder "<host>". Next is a text input field for "Port Number*" containing the value "21". At the bottom, there is a text input field for "Username" which is currently empty.

1. If **No**: Proceed to next step.
2. If **Yes**: Enter the following information:
 - a. Select a **Remote Connection Type** from the dropdown.
 - b. Enter the **Host IP Address** (for FTP, SFTP, etc.) or **URL** (for HTTP, HTTPS).
 - c. Enter the **Port Number** (for FTP, SFTP, etc.). Default 22.
 - d. Enter the **Username**.
 - e. Enter the **Password**.
 - f. Enter the **Source Directory**.
 - g. Select **Yes** or **No** for **Proxy Server?**.
 - a. If **No**: Proceed to next step.
 - b. If **Yes**: Enter **Proxy Server URL**, **Username**, and **Password**.
 - h. **Test** the remote connection.

More Settings



> More Settings

Import Nested Group Membership

☐ NO

Source Folder

`${SECURONIX_HOME}/import/in`

Success Folder

`${SECURONIX_HOME}/import/success`

Failed Folder

`${SECURONIX_HOME}/import/failed`

- a. **Import Nested Group Membership:** Set to **YES** if access data contains nested groups.
- b. **Source Folder:** Specify the folder in which the file is located. Default `${SECURONIX_HOME}/import/in`.
- c. **Success Folder:** Specify the folder into which to move the file once the import is completed successfully.
- d. **Failed Folder:** Specify the folder into which to move the file if the import job fails to complete.

Default \${SECURONIX_HOME}/import/failed.

- e. (Optional) **Keep existing Access Data while Access Import:** Enable to retain existing access data during the new access data import.



- f. Click  to **Preview Input**.

Click **Save And Next** to proceed to [Step 2: Configuring the Import](#).

Importing from Aveksa

Aveksa's products are built to manage the user access lifecycle, including initial access request, approval, fulfillment, review, certification, and remediation. Aveksa Compliance Manager provides visibility of entitlements across applications, platforms and data sources in the enterprise, and manages the overall process for compliance reviews.

ArcSight UBA integrates with Aveksa Compliance Manager to import user and access entitlements. ArcSight UBA analyzes the access entitlements assigned to each user and detects rogue access privileges. These rogue access privileges can be sent for certification by using Aveksa Compliance Manager reducing the workload for certifiers since they only need to certify the access privileges that are outliers and suspicious.

Prerequisites

1. Create a service account with read-only privileges to the Aveksa database.
2. Collect the JDBC URL for the connection to the Aveksa database (IP Address or hostname, Database name, Port number, SID).
 - **Database Type:** Oracle11g
 - **Driver:** oracle.jdbc.driver.OracleDriver
 - **URL:** jdbc:oracle:thin:@servename:1521:aveksadb
 - **Username** (example: aveksadbuser)/**Password**

To import access data from Aveksa, complete the following steps:

1. Click **Select Datasource** to select an existing datasource from the dropdown to edit OR **Create New Datasource** to create a new datasource.
2. Complete the following information:

General Details

GENERAL DETAILS

Datasource Name*

Provide a name to uniquely identify this connection.

IP Address

Specify IP address or hostname for the datasource

Select Device Type

aveksa ▼

Selection of existing Resource Type will automatically create the fields needed to store the event attributes and also the parsers to normalize the events. You may also create custom resource type by selecting the Create New Type option.

Input file format for the selected resource type is Database

- a. **Datasource Name:** Provide a unique name for the datasource.
- b. **IP Address:** Specify the IP Address or hostname for the datasource, if required.
- c. **Select Device Type:** Select from dropdown. Selection of an existing Device Type will automatically create the fields needed to store the event attributes and the parsers to normalize events. To create a custom resource type, complete the following:
 1. Select **Create a new type**.
 2. Enter the **Data Source Vender**. Example: Aveksa
 3. Enter the **Data Source Functionality**. Example: Identity/Access Management.
 4. Provide the **Datasource Type**. Example: Aveksa.
 5. Select the **Format** from the dropdown. Example: Database.
 6. Click **Save**.

Access Connection Details

ACCESS CONNECTION DETAILS

Connection Name*

Access_Data_ACCESS

Aveksa_ACCESS

Provide a unique name for this connection. Do not use any white space in the name. Connections can also be managed from Configure->Connection Types.

Select a Connection Type*

Database

Select the source from which to import data. You can import data from a delimited file (csv, pipe delimited etc), Active Directory or any other listed sources.

Import from Remote Server?

YES

Use FTP/SFTP/SCP to ingest file located in a remote location?

Remote Connection Type*

FTP

Host IP Address*

<host>

Port Number*

21

Username

- a. **Connection Name:** Click inside the box to auto-populate or select an existing connection from the dropdown.
- b. **Select Connection Type:** Select Database from dropdown.
- c. **Source Folder:** Specify the folder in which the file is located. Default \${SECURONIX_HOME}/import/in.

Source Folder*

`${SECURONIX_HOME}/import/in`

Enter the complete path to the directory where this file is located.

Success Folder*

`${SECURONIX_HOME}/import/success`

Enter the complete path to the directory where this file must be moved once the import is completed successfully.

Failed Folder*

`${SECURONIX_HOME}/import/failed`

Enter the complete path to the directory where this file must be moved if the import job fails to complete.

Keep existing Access Data while Access Import (optional)

☐ NO

- d. **Success Folder:** Specify the folder into which to move the file once the import is completed successfully. Default `${SECURONIX_HOME}/import/success`.
- e. **Failed Folder:** Specify the folder into which to move the file if the import job fails to complete. Default `${SECURONIX_HOME}/import/failed`.
- f. **SQL Query:** Provide a query to import the data. Example:

```
Select Application_Name, User_ID, Full_Name, Entitlement_Type,
Entitlement_Name from (select nvl( app.ALT_NAME, app.NAME ) AS
Application_Name, tmeu.USER_ID as User_ID, tmeu.LAST_NAME
||', '|| tmeu.FIRST_NAME As Full_Name, xue.ENTITLEMENT_TYPE as
Entitlement_Type, ar.NAME as Entitlement_Name from AVUSER.T_AV_
EXPLODEDUSERENTITLEMENTS xue join AVUSER.T_MASTER_ENTERPRISE_
USERS tmeu on tmeu.id=xue.entitled_id join AVUSER.T_ENTITLEMENT_
GROUPS ar on ar.id=xue.entitlement_id join AVUSER.T_APPLICATIONS
app on app.id=xue.APPLICATION_ID join AVUSER.T_DATA_COLLECTORS
dc on dc.ID = xue.DC_ID left outer join AVUSER.T_AV_BUSINESS_
UNITS BU ON BU.ID = app.BUSINESS_UNIT_ID left outer join
AVUSER.T_AV_ACCOUNTS acc on acc.id=xue.ENTITLED_DERIVED_FROM_ID
and xue.ENTITLED_DERIVED_FROM_TYPE='account' left outer join
(select distinct entitlement_id from ( select entitlement_id
from AVUSER.t_av_explodeduserentitlements x where entitlement_
type='app-role' and entitled_type='user' and (entitlement_
derived_from_type not in ('explicit') or entitled_derived_from_
type not in ('explicit','account')) and x.deletion_date is null
union all select entitlement_id from AVUSER.V_AV_
INROLEENTITLEMENTS where entitlement_type='app-role' )) model on
model.entitlement_id = xue.entitlement_id where xue.ENTITLED_
DERIVED_FROM_TYPE in ('explicit','account') and xue.ENTITLEMENT_
DERIVED_FROM_TYPE in ('explicit') and xue.entitlement_type='app-
role' and xue.entitled_type='user' and xue.deletion_date is null
and model.entitlement_id is null and app.classification =
'APPNAME' Union all select nvl( app.ALT_NAME, app.NAME ) AS
Application_Name, tmeu.USER_ID as User_ID, tmeu.LAST_NAME
||', '|| tmeu.FIRST_NAME As Full_Name, xue.ENTITLEMENT_TYPE as
Entitlement_Type, (RESOURCE_NAME || ' : ' || ACTION_NAME) as
Entitlement_Name from AVUSER.T_AV_EXPLODEDUSERENTITLEMENTS xue
join AVUSER.T_ENTITLEMENTS ent on ent.id=xue.entitlement_id join
AVUSER.T_RESOURCES res on res.id=ent.RESOURCE_ID join AVUSER.T_
APPLICATIONS app on app.id=xue.APPLICATION_ID join AVUSER.T_
DATA_COLLECTORS dc on dc.ID = xue.DC_ID join AVUSER.T_MASTER_
ENTERPRISE_USERS tmeu on tmeu.id=xue.entitled_id left outer join
AVUSER.T_AV_BUSINESS_UNITS BU ON BU.ID = app.BUSINESS_UNIT_ID
left outer join AVUSER.T_AV_ACCOUNTS acc on acc.id=xue.ENTITLED_
DERIVED_FROM_ID and xue.ENTITLED_DERIVED_FROM_TYPE='account'
left outer join (select distinct entitlement_id from ( select
entitlement_id from AVUSER.t_av_explodeduserentitlements x where
entitlement_type='ent' and entitled_type='user' and
(entitlement_derived_from_type not in ('explicit') or entitled_
derived_from_type not in ('explicit','account')) and x.deletion_
date is null union all select entitlement_id from AVUSER.V_AV_
```

```
INROLEENTITLEMENTS where entitlement_type='ent' )) model on
model.entitlement_id = xue.entitlement_id where xue.ENTITLED_
DERIVED_FROM_TYPE in ('explicit','account') and xue.ENTITLEMENT_
DERIVED_FROM_TYPE in ('explicit') and xue.entitlement_type='ent'
and xue.entitled_type='user' and xue.deletion_date is null and
model.entitlement_id is null and app.classification = 'APPNAME')
```

- g. (Optional) **Keep existing Access Data while Access Import:** Enable to retain existing access data during the new access data import.



- h. Click  to **Preview Input**.

Click **Save And Next** to proceed to [Step 2: Configuring the Import](#).

Importing from Database

To import access data from a database, complete the following steps:

1. Navigate to **Menu > Add Data > Access**.
2. Complete the following information:

General Details

GENERAL DETAILS

Datasource Name*

Database

Provide a name to uniquely identify this connection.

IP Address

Specify IP address or hostname for the datasource

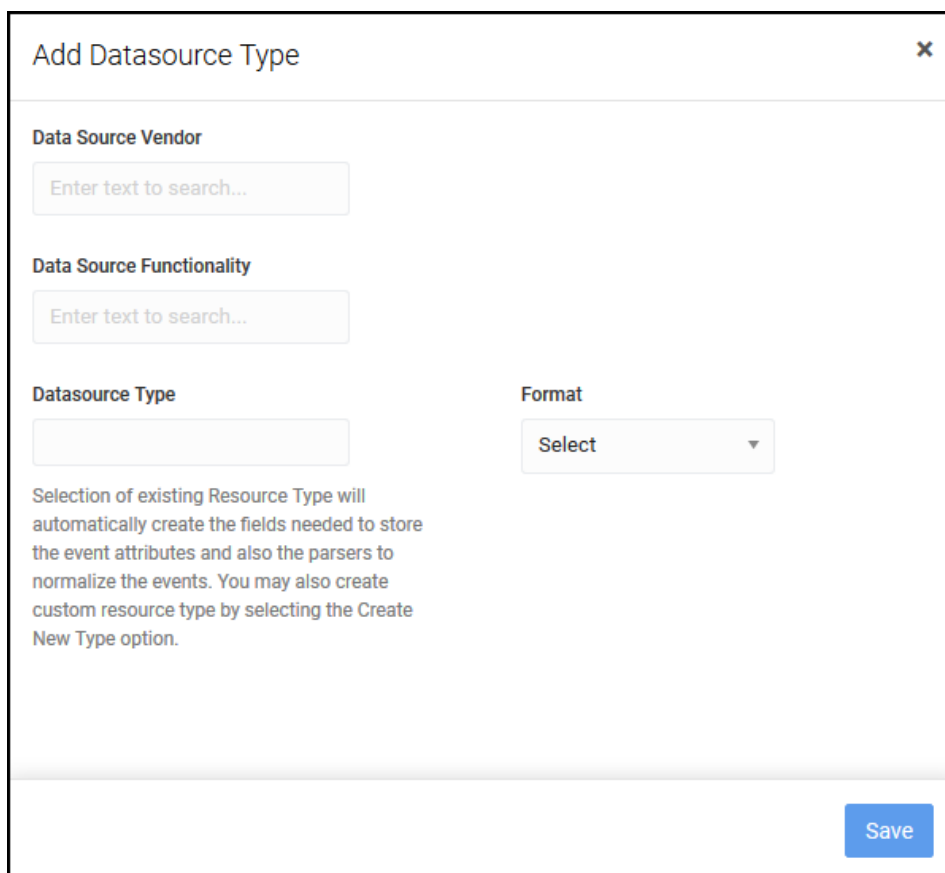
Select Device Type

Create a new type ▼

Selection of existing Resource Type will automatically create the fields needed to store the event attributes and also the parsers to normalize the events. You may also create custom resource type by selecting the Create New Type option.

- a. **Datasource Name:** Provide a unique name for the datasource.

- a. **IP Address:** Specify the IP Address or hostname for the datasource, if required.
- b. **Select Device Type:** Select from dropdown. Selection of an existing Device Type will automatically create the fields needed to store the event attributes and the parsers to normalize events. To create a custom resource type, complete the following:



The screenshot shows a dialog box titled "Add Datasource Type" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Data Source Vendor:** A text input field with the placeholder text "Enter text to search..."
- Data Source Functionality:** A text input field with the placeholder text "Enter text to search..."
- Datasource Type:** A text input field.
- Format:** A dropdown menu with the text "Select" and a downward arrow.

Below the input fields, there is a paragraph of text: "Selection of existing Resource Type will automatically create the fields needed to store the event attributes and also the parsers to normalize the events. You may also create custom resource type by selecting the Create New Type option."

At the bottom right of the dialog, there is a blue button labeled "Save".

1. Select **Create a new type**.
2. Enter the **Data Source Vendor**.
3. Enter the **Data Source Functionality**.
4. Provide the **Datasource Type**.
5. Select **Database** from the **Format** dropdown.
6. Click **Save**.

Access Connection Details

ACCESS CONNECTION DETAILS

Connection Name*

Create New Connection ▼

Database_ACCESS

Provide a unique name for this connection. Do not use any white space in the name. Connections can also be managed from Configure->Connection Types.

Select a Connection Type*

Database ▼

Select the source from which to import data. You can import data from a delimited file (csv, pipe delimited etc), Active Directory or any other listed sources.

Database Type *

MySQL ▼

JDBC URL*

Connection string to connect to particular database. Example:
jdbc:mysql://hostname:port/database_name

Driver Class*

Database specific class


Database Username*

- a. **Connection Name:** Click inside the box to auto-populate or select an existing connection from the dropdown.
- b. **Select Connection Type:** Select **Database** from dropdown.
- c. **Database Type:** Select from the dropdown. Example: My SQL
- d. **JDBC URL:** Example: jdbc:mysql://<host>:<3306>/<database>.
- e. **Driver Class:** Specify the database specific driver class. Example: com.mysql.jdbc.Driver.
- f. **Database User Name:** Provide the user name for the database.
- g. **Database Password:** Provide the password associated with the user name.
- h. **SQL Query:** Provide a query to import the data. Example:

```
SELECT DISTINCT
aa.accountname,aav.accessvalue1,aav.accessvalue2 from Access_
Attribute_Values aav, Access_Account_Attributes aaa, Access_
Account aa where aa.id = aaa.accountid and
aaa.accessvalueid=aav.id
```

- i. (Optional) **Keep existing Access Data while Access Import:** Enable to retain existing access data during the new access data import.



- j. Click  to **Preview Input**.

Click **Save and Next** to proceed to [Step 2: Configuring the Import](#).

Importing from Files

To import access data from a file, complete the following steps:

1. Navigate to **Menu > Add Data > Access**.
2. Complete the following information:

General Details

GENERAL DETAILS

Datasource Name*

Access File

Provide a name to uniquely identify this connection.

IP Address

Specify IP address or hostname for the datasource

Select Device Type

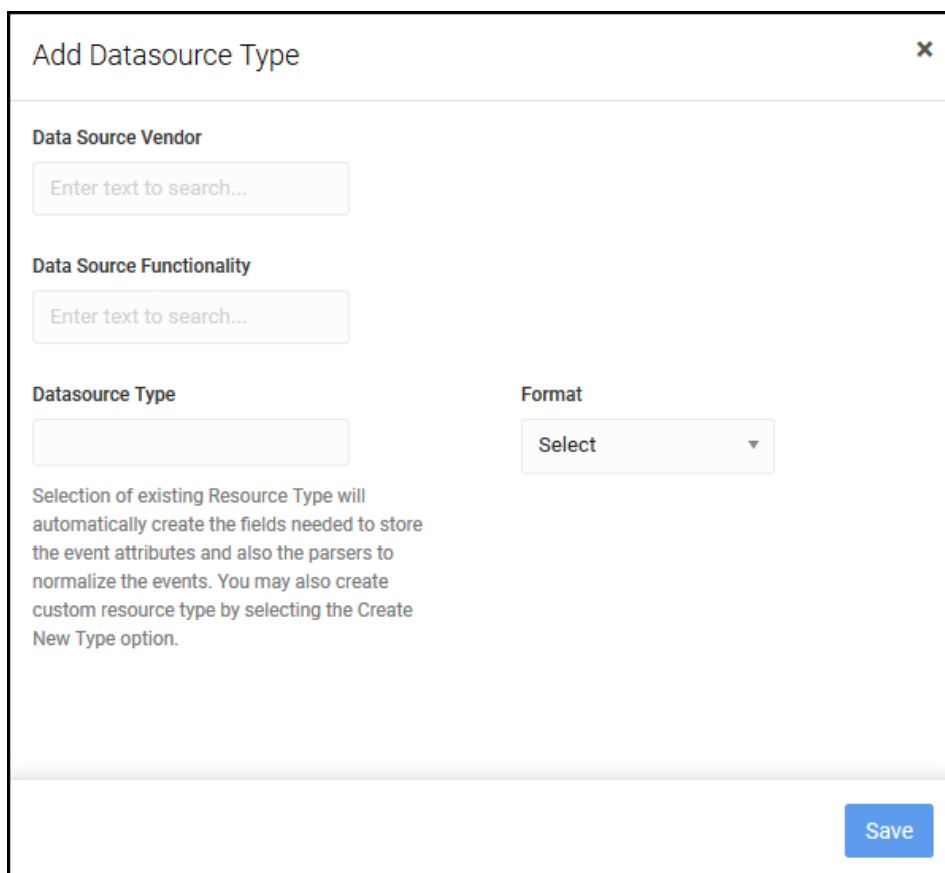
Create a new type ▼

Selection of existing Resource Type will automatically create the fields needed to store the event attributes and also the parsers to normalize the events. You may also create custom resource type by selecting the Create New Type option.

Input file format for the selected resource type is file

- a. **Datasource Name:** Provide a unique name for the datasource.

- a. **IP Address:** Specify the IP Address or hostname for the datasource, if required.
- b. **Select Device Type:** Select from dropdown. Selection of an existing Device Type will automatically create the fields needed to store the event attributes and the parsers to normalize events. To create a custom resource type, complete the following:



The screenshot shows a dialog box titled "Add Datasource Type" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Data Source Vendor:** A text input field with the placeholder text "Enter text to search..."
- Data Source Functionality:** A text input field with the placeholder text "Enter text to search..."
- Datasource Type:** A text input field.
- Format:** A dropdown menu with the text "Select" and a downward arrow.

Below the input fields, there is a paragraph of text: "Selection of existing Resource Type will automatically create the fields needed to store the event attributes and also the parsers to normalize the events. You may also create custom resource type by selecting the Create New Type option."

At the bottom right of the dialog, there is a blue button labeled "Save".

1. Select **Create a new type**.
2. Enter the **Data Source Vender**.
3. Enter the **Data Source Functionality**.
4. Provide the **Datasource Type**.
5. Select **File** from the **Format** dropdown.
6. Click **Save**.

Access Connection Details

ACCESS CONNECTION DETAILS

Connection Name*

Create New Connection ▼

Access_File_ACCESS

Provide a unique name for this connection. Do not use any white space in the name. Connections can also be managed from Configure->Connection Types.

Select a Connection Type*

File Import ▼

Select the source from which to import data. You can import data from a delimited file (csv, pipe delimited etc), Active Directory or any other listed sources.

Upload a file?

☐ NO

File Prefix

Specify file name prefix. All files matching this prefix will be imported. Example: AIX_.

File Postfix

Specify file name postfix. All files matching this postfix will be imported. Example: .csv

Column Delimiter*

Exclude Header
☐ NO
Number of header lines to be excluded from input file.

Import from Remote Server?
☒ YES
Use FTP/SFTP/SCP to ingest file located in a remote location?

Remote Connection Type*

FTP ▼

Host IP Address*

<host>

Port Number*

21

Username

Password

Source directory

Proxy Server?
☐ NO
This is a server that all computers on the local network have to go

- a. **Connection Name:** Click inside the box to auto-populate or select an existing connection from the dropdown.
- b. **Select Connection Type:** Select **File Import** from dropdown.
- c. **Upload a File?:** Toggle slider to **YES** to browse for a file on the local machine.
- d. **File Prefix:** Specify the file prefix. All matching files with this prefix will be imported. Example: AIX_.
- e. **File Postfix:** Specify the file postfix. Example: .csv.
- f. **Column Delimiter:** Specify the delimiter between the fields in the input file. Example: , (comma).
- g. **Exclude Header:** Toggle to **YES** to exclude the header.
 - a. For **No**: Proceed to next step.
 - b. For **Yes**: Specify the number of lines to ignore.
- h. **Import from Remote Server?:** Enable to enter remote server details:

Import from Remote Server?
☒ YES
Use FTP/SFTP/SCP to ingest file located in a remote location?

Remote Connection Type*

FTP ▼

Host IP Address*

<host>

Port Number*

21

Username

1. If **No**: Proceed to next step.
2. If **Yes**: Enter the following information:
 - a. Select a **Remote Connection Type** from the dropdown.
 - b. Enter the **Host IP Address** (for FTP, SFTP, etc.) or **URL** (for HTTP, HTTPS).
 - c. Enter the **Port Number** (for FTP, SFTP, etc.). Default 22.
 - d. Enter the **Username**.
 - e. Enter the **Password**.
 - f. Enter the **Source Directory**.
 - g. Select **Yes** or **No** for **Proxy Server?**
 - a. If **No**: Proceed to next step.
 - b. If **Yes**: Enter **Proxy Server URL, Username**, and **Password**.
 - h. **Test** the remote connection.
- i. **Source Folder**: Specify the folder in which the file is located. Default \${SECURONIX_HOME}/import/in.

`${SECURONIX_HOME}` is set to `/Securonix/tenants/partnerdemo/securonix_home`.
You can also replace `${SECURONIX_HOME}` below with the direct path to the folder where the file exists.
Example: `/Users/dev/files/`

Source Folder*

`${SECURONIX_HOME}/import/in`

Enter the complete path to the directory where this file is located.

Success Folder*

`${SECURONIX_HOME}/import/success`

Enter the complete path to the directory where this file must be moved once the import is completed successfully.

Failed Folder*

`${SECURONIX_HOME}/import/failed`

Enter the complete path to the directory where this file must be moved if the import job fails to complete.

Keep existing Access Data while Access Import (optional)

☐ NO

- j. **Success Folder:** Specify the folder into which to move the file once the import is completed successfully. Default `${SECURONIX_HOME}/import/success`.
- k. **Failed Folder:** Specify the folder into which to move the file if the import job fails to complete. Default `${SECURONIX_HOME}/import/failed`.

- l. (Optional) **Keep existing Access Data while Access Import:** Enable to retain existing access data during the new access data import.



m. Click  to **Preview Input**.

Click **Save And Next** to proceed to [Step 2: Configuring the Import](#).

Step 2: Configuring the Import

To configure the access data import, complete the following steps:

Attribute Mapping

Map the attributes in the input file to the attributes that will appear in ArcSight UBA for the data-source.

ATTRIBUTE MAPPING

Add Attributes Remove Attributes Edit Attributes

Map input file columns to Datasource attributes. Specify numerical values for column positions starting from 1.

Input Source Column Position	Datasource Fields	Is Multi-valued?	Delimiter	Is Account Name?	Is Resource Name?	Add/Remove
1	sAMAccountName	NO		YES	NO	+ -
2	homeMTA	NO			NO	+ -
3	memberOf	YES	;		NO	+ -
4	manager	NO			NO	+ -
5	employeeID	NO			NO	+ -
6	employeeType	NO			NO	+ -
7	primaryGroupID	NO			NO	+ -
8	userAccountControl	NO			NO	+ -

1. Complete the following to map attributes for the datasource:
 - a. **Input Source Column Position:** Map the numerical value of the column position to the corresponding attribute in the input file.
 - b. **Datasource Fields:** Select the attribute that corresponds to the column position from the dropdown.
 - c. **Is Multi-Valued?:** Toggle to **YES** if the attribute has multiple values separated by a delimiter and specify **Delimiter**.
 - d. **Is Account Name?:** Toggle to **YES** if the attribute corresponds to an account name.
 - e. **Is Resource Name?:** Toggle to **YES** if the attribute corresponds to a resource name.
 - f. **Add/Remove:** Click to add or remove an attribute to map.
2. Click **Add Attributes** to specify custom attributes.

Attribute Name *	Parent Attribute	Populate Using Formula/Function	Use in Outlier Detection	Actions
<input type="text"/>	-Select-	Populate Using Function ✕	<input type="checkbox"/> NO	+ -

Create Attribute

- a. **Attribute Name:** Provide a name to uniquely identify the new attribute.
 - b. **Parent Attribute:** Select the parent attribute for the new attribute from the dropdown.
 - c. **Populate Using Formula/Function:** Click to use Functions to populate attribute field. For a complete list of functions in ArcSight UBA, see [Appendix B: Functions](#).
 - d. **Use In Outlier Detection:** Toggle to **YES** to include the new attribute in access outlier detection. See [Access Outliers](#) for information about how to run access outlier jobs.
 - e. **Actions:** Click +/- to add/remove Actions to populate attributes.
 - f. **Create Attribute:** Click to create the new attribute.
3. Click **Remove Attributes** to select mapped attributes to remove from the datasource.

Remove Access Attribute ✕

Remove Attributes

	Attribute Name	Parent Attribute	High Privileged	Use In Outlier Detection
<input type="checkbox"/>	accountExpires		<input type="radio"/> NO	<input type="radio"/> NO
<input type="checkbox"/>	displayName		<input type="radio"/> NO	<input type="radio"/> NO
<input type="checkbox"/>	distinguishedName		<input type="radio"/> NO	<input type="radio"/> NO
<input type="checkbox"/>	employeeID		<input type="radio"/> NO	<input type="radio"/> NO
<input type="checkbox"/>	employeeType		<input type="radio"/> NO	<input type="radio"/> NO
<input type="checkbox"/>	givenName		<input type="radio"/> NO	<input type="radio"/> NO
<input type="checkbox"/>	groupType		<input type="radio"/> NO	<input type="radio"/> NO
<input type="checkbox"/>	homeMTA		<input type="radio"/> NO	<input type="radio"/> NO
<input type="checkbox"/>	lastLogonTimestamp		<input type="radio"/> NO	<input type="radio"/> NO

4. Click **Edit Attributes** edit the following details:

Edit Access Attribute ✕

	Attribute Name	Parent Attribute	High Privileged	Use In Outlier Detection	Edit
<input type="checkbox"/>	accountExpires		<input type="radio"/> NO	<input type="radio"/> NO	
<input type="checkbox"/>	displayName		<input type="radio"/> NO	<input type="radio"/> NO	
<input type="checkbox"/>	distinguishedName		<input type="radio"/> NO	<input type="radio"/> NO	
<input type="checkbox"/>	employeeID		<input type="radio"/> NO	<input type="radio"/> NO	
<input type="checkbox"/>	employeeType		<input type="radio"/> NO	<input type="radio"/> NO	
<input type="checkbox"/>	givenName		<input type="radio"/> NO	<input type="radio"/> NO	
<input type="checkbox"/>	groupType		<input type="radio"/> NO	<input type="radio"/> NO	
<input type="checkbox"/>	homeMTA		<input type="radio"/> NO	<input type="radio"/> NO	
<input type="checkbox"/>	lastLogonTimestamp		<input type="radio"/> NO	<input type="radio"/> NO	

- a. **High Privileged:** Enable if attribute has High Privilege.
- b. **Use in Outlier Detection:** Enable to include attribute in Access Outlier detection. See [Access Outliers](#) for details.
- c. **Edit:** Click edit icon to edit the following details about the attribute:

- a. **Attribute Name:** Provide a name to uniquely identify the new attribute.
- b. **Parent Attribute:** Select the parent attribute for the new attribute from the dropdown.
- c. **Populate Using Formula/Function:** Click to use Functions to populate attribute field. For a complete list of functions in ArcSight UBA, see [Appendix B: Functions](#).
- d. **High Privileged:** Enable if attribute has High Privilege.
- e. **Use In Outlier Detection:** Toggle to YES to include the new attribute in access outlier detection. See [Access Outliers](#) for information about how to run access outlier jobs.

Correlation Rules

Create or edit rules to correlate an event to a user identity. ArcSight UBA provides a comprehensive and feature-rich correlation engine with the following features:

- **Ability to specify multiple correlation rules:** Many organizations have different conventions for creating account IDs for users on different applications. The ArcSight UBA correlation engine allows for the specification of multiple correlation rules. The correlation rules are evaluated in the order in which they are specified. When the account ID is matched to a user identity within the organization, the correlation rule engine stops processing the other rules.
- **Ability to specify multiple operations on the identity data:** The Correlation engine allows the following operations to be performed on any identity attribute. The identity attribute generated after the operator is applied can be concatenated with other identity attributes.

- Trim Left
- Trim Right
- Prefix
- Postfix
- Substring
- Prefix and Postfix

Example: An application uses the convention of first initial of first name + first 2 initials of last-name + employeeid.

In the correlation engine this rule can be constructed by:



- Perform substring operation on first name with 1,1 (start from first character and extract the first character).
 - Perform substring operation on last name with 1,2 (start from first character and extract the first 2 characters).
 - Concatenate with Employee ID.
- **Ability to prioritize rules:** You can assign weights to rules to prioritize them. Rules are processed based on the weightage assigned to them.
 - **Ability to request for suggested matches:** The ArcSight UBA application utilizes special comparators that perform the following types of matches:
 - **Phonetics:** The comparator provides results for words that sound like each other.
 - **Character Swapping:** The comparator provides results by swapping characters (Sean misspelled to Saen will match).
 - **Closest Match:** jsmith01 and jsmith02 will match to jsmith.
 - **Ability to filter users:** You can select all users for correlation or filter users by specifying user selection for correlation.

To add correlation rules, complete the following steps:

CORRELATION RULES

Create/Edit rules to correlate an event to a user identity. You can create multiple correlation rules. For example, use the account name attribute to correlate to the user identity's employeeid.

+ Add Correlation Rule
More Settings...

Rule Name	Resource Attribute	Expression	Actions
sAMAccountname-EmpID	sAMAccountName	Expression	 

1. Click **Add Correlation Rule** to add rules by which to correlate user identities.

Add Correlation Rule

Correlation Rule Name

Weight

0.0

Datasource Attribute



sAMAccountName

Select the Event Field that you want to use to correlate to a user identity. Example: AccountName

Relation

EXACT MATCH

Event Field value either exact match with user attribute condition below or contains user attribute condition below.

User Attribute	Operation	Parameter	Condition	Separator	Add/Delete
employeeid	None		AND	<input type="checkbox"/>	 

Enable Comparators

NO

Set to "Yes" if you want to enable comparators for computing suggested matches. Set to "No" if you do not want suggested matches.

Save

- Correlation Rule Name:** Provide a unique name for the correlation rule.
- Weight:** Specify a weight for the rule.
- Datasource Attribute:** Select the attribute with which to correlate user identity from the dropdown. Example: sAMAccountName.
- Relation:** Select EXACT MATCH or CONTAINS from dropdown.
- User Attribute:** Select the [User Data](#) attribute to correlate to the selected Access Data attribute.
- Operation:** Select from dropdown. Example: Trim Left.
- Parameter:** Specify if required:
 - None: Proceed to Condition.
 - Trim Left/Right: Use Parameter is used for number of characters to trim.
 - Pre-/Post-fix: Use Parameter is used for the pre/post fix string.
 - Substring: Use Parameters for the start position and length of the substring.
 - Pre and Postfix: Use Parameters to set the pre and postfix strings.

- h. **Condition:** Select from dropdown.
- i. **Separator:** Check to enter a separator character.
- j. **+/-:** Add or remove user attributes to correlate to access data attribute.
- k. **Enable Comparators:** Toggle to **YES** to enable comparators for suggesting matches.

Add Correlation Rule
✕

Enable Comparators
☒ YES
Set to "Yes" if you want to enable comparators for computing suggested matches. Set to "No" if you do not want suggested matches.

Min Threshold

Comparison result must cross this value to show up as a suggested match.

Max Threshold

If Comparison result crosses this value then it is considered 100% Match

Weight

Available Comparators	Enabled?	Discredit	Delimiter	Regex
Alphanumeric Comparator	<input type="radio"/> NO	<input type="text" value="0.0"/>	<input type="text"/>	<input type="text"/>
CondensedString Comparator	<input type="radio"/> NO	<input type="text" value="0.0"/>	<input type="text"/>	<input type="text"/>
Transpose Comparator	<input type="radio"/> NO	<input type="text" value="0.0"/>	<input type="text"/>	<input type="text"/>

Save

- l. **Min Threshold:** Enter a threshold the comparison result must cross to appear as a suggested match.
- m. **Max Threshold:** Enter a threshold the comparison result must cross to be considered a 100% match.
- n. **Weight:** Provide the weight of the comparator.
- o. **Available Comparators:** Enable any of the following comparators:

- **Alphanumeric Comparator:** Looks at the similarity in a range of characters at the beginning of the strings. Use: Ideal for alphanumeric account IDs, identities derived from SSN, and birth dates.
 - **Condensed String Comparator:** Handles special diacritical characters. (A diacritical is a glyph added to a letter, or basic glyph.)
 - Some diacritical marks, such as the acute (´) and grave (`) are often called accents.
 - Diacritical marks may appear above or below a letter, or in some other position such as within the letter or between two letters).
 - Takes into account misspelled characters as well as visual memory errors.
 - Effective for both alphabetical and alphanumeric strings. Use: Effective for data sets containing special characters.
 - **Transpose Comparator:** Transpose a given pair of strings and find distances amongst strings. Handles transposition of strings and accounts for misspelled strings. Use: Effective for user identities derived from first name, last name, and account ID.
 - **Bigram:** A Bigram algorithm compares two strings using all combinations of two consecutive characters within each string. For example, the word “bigram” contains the following bigrams: “bi”, “ig”, “gr”, “ra”, and “am”. Bigrams handle minor typographical or 'fat fingering'. Use: More efficient in alphabetical comparison.
- p. **Discredit:** Assign a value between 0 to 1 to reduce the weight for each comparator.
 - q. **Delimiter:** Specify a delimiter if required.
 - r. **Regex:** Specify a Regex if required.
 - s. **Save:** Click to save the Correlation Rule.
2. Click Edit or Delete icons to edit or delete existing Correlation Rules.
 3. Click **More Settings** to add additional settings by which to correlate user identities.

MORE SETTINGS

Prioritize Rules

☐ NO

When set to "Yes", correlation rules can be prioritized by assigning weights on the create/edit correlation rules screens. Rules with higher weights will be given more priority. When set to "No", all correlation rules are given the same priority.

Force Suggested Match



☐ NO

When set to "Yes", suggested matches for an account will be evaluated even after a 100% match is found for the same account. Enable this option if you want to store both matched and suggested matches for the same account. When set to "No", suggested matches for an account are not evaluated after a 100% match is found.

Filter Users

☒ YES

Set to "Yes" to specify user selection criteria for correlation. When set to "No", all users will be considered for correlation.

Attribute	Condition	Value	Condition	Add/Remove
approveremployeeid	Equal To		AND	 

[Save](#)

- a. **Prioritize Rules:** Toggle to **YES** to prioritize correlation rules by weights assigned to the rule. Rules with higher weights will be given higher priority. If disabled to **NO**, all correlation rules will be assigned the same priority.
 - b. **Force Suggested Match:** Toggle to **YES** to store both matched and suggested matches for the same account. When enabled, suggested matches for an account will be evaluated even after a 100% match is found for the same account. If disabled to **NO**, suggested matches for an account will not be evaluated after a 100% match is found.
 - c. **Filter Users:** Toggle to **YES** to specify user selection criteria for correlation. Disable to **NO** to consider all users for correlation.
 - **NO:** Proceed to next step.
 - **YES:** Specify the **Attribute**, **Condition**, **Value**, and **Condition** for each user selection criteria. Use +/- to add/remove user selection criteria.
4. Click Save to proceed to [Step 3: Running the Job](#).

Step 3: Running the Job

To preview the identity correlation results and run the Access Data Import job, complete the following steps:

Preview Correlation Results

Preview the results of the identity correlation.

PREVIEW CORRELATION RESULTS			
Account	Employeeid	Firstname	Lastname
DB1080-2			
DB1080	1080	Demetria	Bridges
DBRIDGES			
DV1080			
ADM-DB1080			
RH1095	1095	Rosalyn	Harding

If no results exist, return to Step 2 to verify configuration.

Job Details

JOB DETAILS

Job Name*

AccessImport_ActiveDirectory_2017_11_1_16_4

Job Description

Access Import Job

Enable Job Related Notifications

YES

JOB SCHEDULING INFORMATION

Run Job

☒ Do you want to run job Once ?

☐ Do you want to schedule this job for future ?

i Job will be scheduled according to the server time. Current server time is - 11/1/2017 16:41:42

ON SUCCESS

Name*

-Select- OR

Override email address from template

ON FAILURE

Select Email Template to Use for Sending Notifications

-Select- OR

Override email address from template

ON MISFIRED

Select Email Template to Use for Sending Notifications

-Select- OR

Override email address from template

ON COMPLETED WITH ERRORS

Name*


-Select- OR


Override email address from template

1. Specify a **Job Name** or use auto-generated name.
2. Enter a **Job Description**.


3. **Enable Job Related Notifications** if you would like to receive email notifications when the job is run.
 - a. If **No**: Proceed without entering additional information.
 - b. If **Yes**:
 - **On Success**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template:
 - **On Failure**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template.
 - **On Misfired**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template.
 - **On Completed with Errors**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template:

Create New Email Template

Sender Name* 


Template Name* 


Description


To* 

From*

test@securonix.com

CC 

BCC 


Subject 

HTML Enabled ☒


Store in Outbox prior to sending? ☒

Use this template for *



















Job Misfired

Owner 

Administrators
SECURITYOPERATIONS

Email Body 

Add Email Template Variables

B I U abc x² T• fT• H• T•                  

Job Scheduling Information

1. Select when you would like the job to run.

JOB SCHEDULING INFORMATION

Run Job

☒ Do you want to run job Once ?

☐ Do you want to schedule this job for future ?

i Job will be scheduled according to the server time. Current server time is - 5/1/2017 14:40:57

- Select **Do you want to run job Once?** to run now.
- Select **Do you want to schedule this job for future?** to run the job later and complete the relevant fields.

☒ Do you want to schedule this job for future ?

Seconds Minutes Hourly Daily Weekly Monthly Specify Date

Select how often you want the job to run

Start Job At *

02:38:00 PM

NOTE: This is the server time

Run Every *

Seconds

Stop after

Times

2. **Save** job.
4. Review the job status to ensure data was loaded successfully.
The Job Monitor screen for this job will appear automatically. To find specific jobs, navigate to **Menu > Operations Center > Job Monitor** and select **Access Import** from left navigation

panel.

The screenshot shows the ArcSight Job Monitor interface. On the left is a navigation panel with 'DATA IMPORT JOBS' expanded, showing options like User Import, Activity Import, Access Import, Lookup Import, WatchList Import, Entity Metadata Import, Third Party Intelligence Import, Geolocation/Network Map Import, and Peer Creation Import. Below these are 'JOB STATUS' and 'JOB SCHEDULE'. The main area has a header with 'Operations Center Job Monitor > All Jobs' and a search bar. Below the header is a table titled 'JOBS FOR ACCESS IMPORT'. The table has columns: Job Name, Creation Date, Start Date, Next Trigger Date, and Job Status. A single job is listed: 'ACCESSIMPORT_ACCESS DATA_2017_10_2_15_2_35', created by 'ADMIN' on 'MON, 2 OCT 2017 @ 05:02:42.000 PM'. The status is 'COMPLETED'. The table also shows 'START DATE' and 'END DATE' as 'MON, 2 OCT 2017 @ 05:02:42.000 PM' and 'MON, 2 OCT 2017 @ 05:02:46.000 PM' respectively. At the bottom, there are pagination controls showing 'Total results : 1 | Total pages : 1'.

Job Name	Creation Date	Start Date	Next Trigger Date	Job Status
ACCESSIMPORT_ACCESS DATA_2017_10_2_15_2_35 CREATED BY : ADMIN / JOB TYPE : ACCESS IMPORT	MON, 2 OCT 2017 @ 05:02:42.000 PM	START DATE : MON, 2 OCT 2017 @ 05:02:42.000 PM END DATE : MON, 2 OCT 2017 @ 05:02:46.000 PM	NOT SCHEDULED	COMPLETED

- Review the job status to ensure data was loaded successfully.

The Job Monitor screen for this job will appear automatically. To find specific jobs, navigate to **Menu > Operations Center > Job Monitor** and select **Access Import** from left navigation panel.

This screenshot is identical to the one above, showing the same Job Monitor interface with the 'JOBS FOR ACCESS IMPORT' table containing one job with a 'COMPLETED' status.

Job Name	Creation Date	Start Date	Next Trigger Date	Job Status
ACCESSIMPORT_ACCESS DATA_2017_10_2_15_2_35 CREATED BY : ADMIN / JOB TYPE : ACCESS IMPORT	MON, 2 OCT 2017 @ 05:02:42.000 PM	START DATE : MON, 2 OCT 2017 @ 05:02:42.000 PM END DATE : MON, 2 OCT 2017 @ 05:02:46.000 PM	NOT SCHEDULED	COMPLETED

8. Navigate to **Menu > Views > Resources** to review the access import information.
9. Select the datasource and from the left navigation pane.

The screenshot shows the 'Resources' view in the ArcSight interface. The left navigation pane lists various data sources. The main area displays a table of resources with the following columns: Name, Type, IP Address, Category, Vendor, Last Event Date, and Last Import Access Date. Two resources are listed:

Name	Type	IP Address	Category	Vendor	Last Event Date	Last Import Access Date
Access Data	Active Directory			Active Directory	Active Directory	Oct 02, 2017 17:02:43
Active Directory	Active Directory		Identity Access Management	Microsoft Corporation	Microsoft Corporation	-

At the bottom, it shows 'Total results: 2 | Total pages: 1'.

10. Select **Monitor Access > Accounts** to view Correlated, Uncorrelated, and Soft Link Accounts. See [Views](#) in the User Guide for more information about what you can do from this screen.

The screenshot shows the 'Accounts' view in the ArcSight interface. The left navigation pane is expanded to 'Monitor Access > Accounts'. The main area displays a table of accounts with the following columns: Criticality, Account Name, Description, Employee ID, First Name, Last Name, Account Type, Account Status, Actions, and Create Date. Three accounts are listed:

Criticality	Account Name	Description	Employee ID	First Name	Last Name	Account Type	Account Status	Actions	Create Date
	AB2518		2518	Ashling	Barrett	User	Active	Assign To	2017-10-17 17:02:43
	AB2639		2639	Andreas	Baker	User	Active	Assign To	2017-10-17 17:02:43
	AC1073		1073	Anika	Charles	User	Active	Assign To	2017-10-17 17:02:43

Analytics

Why use Security Analytics

Three primary factors drive the need for Security Analytics:

1. Attack sophistication has increased: Normal vs abnormal patterns.
2. Attack surface has increased: Perimeter to endpoints, users, and applications.
3. Volume and type of event data has increased: Impossible for a person to review for threats.

What is Increased Sophistication

APT (advanced persistent threat) actors use sophisticated multi-vector attacks to bypass the defenses put in place by organizations. These multi-vector attacks exploit vulnerabilities to get in the IT systems of organizations, become resident in the environment, aggregate critical data for exfiltration or perform harmful actions. Unfortunately, the defenses put in place by organizations focus on the patching of vulnerabilities to prevent APT actors from entering the environment. Once the bad actor is inside the environment, few defenses exist to detect the resident actor and prevent the actor from performing the exfiltration attempt.

With Security Analytics, organizations can perform a more holistic analysis of the environment to detect malicious actions indicative of an attack. By using techniques to identify abnormalities in each system/application and aggregating these abnormalities in the context of risk to the organization, security analytics can detect threats that may not have been detected by other defenses.

Signature-based defense systems rely on the notion that the indicators exhibited by the attack have been seen before and all subsequent attacks will exhibit the same pattern. cyberattackers easily bypass these signature-based techniques by making slight modifications to their code from randomly generating function names to the behavior exhibited by the code. Since the triggers for the signatures do not get fired, the signature-based detection systems are rendered useless.

On the other hand, behavior based anomaly detection systems may get triggered on every change in the environment and provide thousands of false positives. Use the behavior based anomaly detection system for finding threat indicators and then combine multiple threat indicators in the context of the overall risk of the compromise.

What are Access Outliers

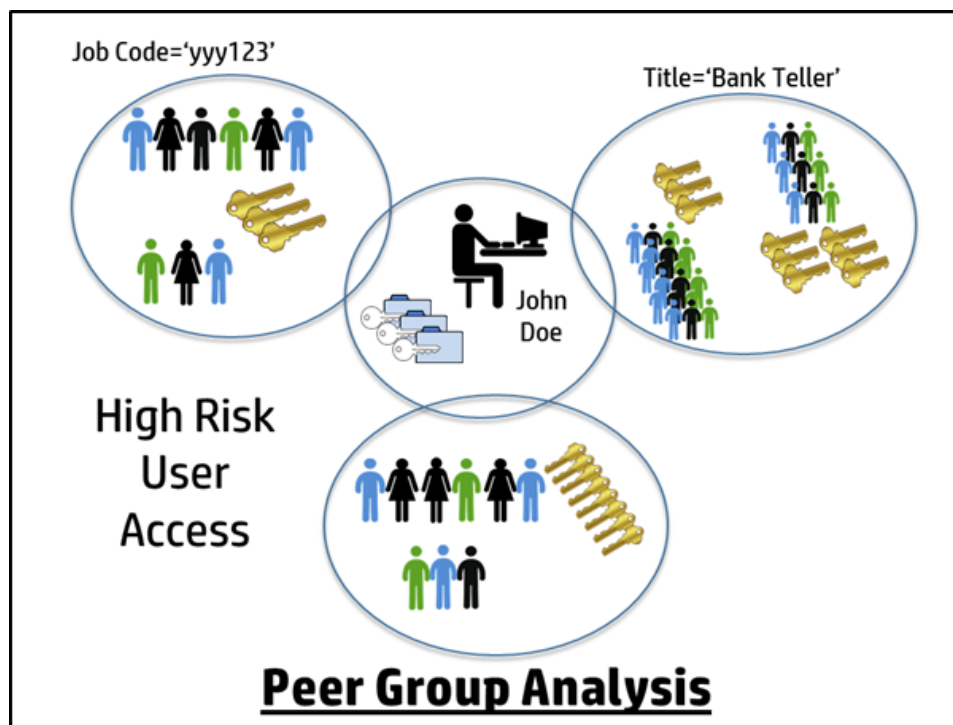
With more than 80% of data residing in electronic form, organizations have a pressing need to manage the access privileges held by users to their IT assets. Managing user access privileges across the hundreds and thousands of applications, databases, directories and hosts is a daunting task.

Organizations utilize various access control models to limit their exposure to rogue access. However, it becomes very difficult to determine the right access privileges required by users, more so when users are transferred between organizations or change job functions. Even with a role-based access control model, users end up having access to thousands of exceptions because there is always something special the user needs for the job they are doing. Most access provided as an exception is never cleaned up and the user carries the access throughout the organization.

It is also very difficult to take a hardline approach to enforcing access control models, as this hampers business. It is counterproductive to prevent a sales representative from generating a sales quote for a customer because it violates an access control policy.

What is Peer Group Analysis

The credit card industry uses Peer Group Analysis extensively to detect fraudulent transactions in credit card use. When users use their credit card in a fashion that does not align with the usage patterns of their “peers,” the transactions are flagged and require further investigation. A similar approach is used by ArcSight UBA to detect rogue access held by users.



How Peer Group Analysis Works

Users are assigned to one or multiple peer groups based on their identity attributes. As shown above, John Doe, a user within the organization, belongs to three peer groups based on his job code, title, and manager. Peers group that the user belongs to, have other set of users with access privileges assigned to them.

Step 1: Determine which peer groups are valid against which to compare the user

The access privileges held by users belonging to other peer groups may or may not be similar to each other. The “cohesiveness factor” determines how many access privileges are common amongst members of the peer group. The greater the number of common entitlements, the higher the cohesiveness value for the peer group. If the peer group is not cohesive enough, we do not have a high level of confidence in the user’s entitlement being an outlier in that peer group.

Step 2: Determine access “outlierness” of each entitlement held by a user

Each access privilege held by a user is compared across the members of each Peer group to determine the number of users that hold the same access privilege. The greater the number of users that hold the same entitlement, the less the probability of the access privilege being an outlier. The entitlement is determined to be an outlier if it crosses a threshold for “outlierness.”

Step 3: Determine access risk for the user

Each user within the organization may have one or multiple access privileges that are outliers. The greater the number of access privileges that are outliers, the higher the overall access risk for the user.

How to Interpret Outlier Analysis Results

Peer group cohesiveness and access outlier risk are the two major indicators of access risk that security administrators and risk analysts must analyze to determine the appropriate access risk threshold.

- **Peer Group Cohesiveness:** The peer group cohesiveness is an indicator of the number of access entitlements that are held by the majority of the members of the peer group. The peer group-cohesiveness factor takes into account the fact that most entitlements are not held by all users in a peer group.
- **Access Outlier Risk:** The access outlier risk indicates how many users in the peer group have the access privilege. A high value indicates fewer members in the peer group that have that access privilege.

What Threat Detection Techniques are Available

ArcSight UBA provides purpose-built analytics techniques to detect threats and risk rank events. By applying these techniques, the application reduces the number of events for security analysts to investigate. The risk ranking algorithms employed ensure that security analysts can focus their attention on key threats and actors behind the threats.

Analytical techniques supported by ArcSight UBA:

Analytical Technique	Description
User behavior-based anomaly	Detects unusual spike in volume of activity from established baselines for the user
Resource account behavior-based anomaly	Detects unusual spike in volume of activity from established baselines across all users
Peer behavior-based anomaly	Detects unusual spike in volume of activity from established baselines for peer group of user
Amount behavior-based anomaly for user	Detects unusual spike in amounts found within some activity attribute compared to user, peer group or user population
Rare events	Detects activities or IP addresses and even accounts that have not been observed before
Peer-based activity outlier	Detects outliers in activity performed by user compared to peers
Third-party intelligence	Checks for existence in third-party intelligence data
String comparators	Compares two strings to determine how closely they match

Peer Groups contain sets of users with access privileges assigned to them. ArcSight UBA compares each access privilege held by a user with all members of the Peer Group to determine the number of users holding the same access privilege. A privilege may be determined to be an outlier if very few other Peer Group members hold the same privilege.

Activity Outliers

Security Administrators are inundated with log data generated from applications, security devices, operating systems, databases, and network devices. Most organizations use log management, database monitoring, security incident, and event monitoring technologies to correlate this immense amount of data and run this log data against signature for known attacks to determine if their organization is under siege from hackers, malware, and other malicious attacks.

A signature-based approach for detecting fraudulent user actions is not effective in combating actions taken by insiders. Users from within the perimeter of the organization's IT structure can conduct reconnaissance missions seeking sensitive data, the loss of which can be detrimental to the organization, whether intellectual property, customer and employee private data, or information that can be sold to competitors.

The only way to prevent and detect these kinds of attacks is by employing a behavior based approach to anomaly detection. Activity conducted by insiders must be checked against the past behavior of these users and the behavior of their peers to detect anomalous activities that may be detrimental to the organization.

Behavior Profiles

Behavior profiling refers to mining activity log data for usage characteristics. Behavior Profiles are generated for Users, Peer Groups and Resources. Behavior-based anomaly detection techniques detect indicators of compromise by finding deviations from normal. To do this, the application first extracts normal or valid behavior extracted from reference data. The repeated observation of the same characteristics for an entity (typically a user or device) form the behavior for the entity. The characteristics the system must observe depend on the use case you are trying to solve.

Behavior Profiles are generated for Users, Peer Groups, and Resources by establishing a baseline observed over a period of time. See [Behavior Profiles](#) for more information.

These baselines consider four major characteristics:

- Time Slices
- Activities
- Network Source
- Baseline Frequency

Example behavior profile characteristics and associated data

Time Slices	Activities	Network Source	Baseline Frequency
Day of Week	Add User	10.27.226.12	30
Time of Day	Create User	10.27.226.22	25
Holidays	Approve Loan	10.27.226.17	10
Weekends	Database Backup	10.27.101.2	2
Daily	Create Invoices	10.27.226.17	10
Weekly	Issue Purchase Orders	10.27.226.12	12
Monthly	Read Customer Credit Reports	10.27.226.12	5

As shown in the previous table, ArcSight UBA derives the baseline frequency using clustering techniques that can mine for generic behavior of users and remove noise from the data set. Activities are considered anomalous when they deviate from the normal baseline for each of the time slices. The amount of deviation, criticality of activity, and the number of checks that the activity fails adds to the risk score for the activity.

The following section describes how to create Activity Outlier policies, including:

- **Behavior Based Outliers:** Detect anomalous behaviors compared to baseline frequency or behaviors that are rare for users or accounts.
- **Peer Group Based Outliers:** Detects anomalous behaviors compared to peer behavior for activity accounts.
- **Peer Group Based Activity IP Outliers:** Detects anomalous behaviors compared to peer behavior for network addresses.
- **Peer Group Based Resource Outliers:** Detects anomalous behaviors compared to peer behavior for resources.

Behavior Profiles

Behavior profiling analyzes what users do on your network by collecting all user privileges, resources, and activities, determining what is "normal", and then identifying the abnormal or "outlier" behaviors to bring to the attention of security administrators.

How Behavior Profiles Work in ArcSight UBA

The Event Indexer job reads the data from the enriched topic, indexes every event based on the configuration specified in the data source, and then stores the events in Solr Cloud. The Behavior Analytics job uses Securonix's patented behavior profile algorithm to analyze the data in enriched topic and generate clusters. The cluster details are stored in HBase. This job also runs the behavior based outlier/policies and saves the violations to Solr Cloud. The Behavior Profile job analyzes the cluster information stored by the Behavior Analytics job in HBase, generates behavior profiles, and stores them in HBase.

Why Monitor Behavior?

- Single events seldom detect threats but are indicators of compromise. A combination of multiple indicators of compromise will highlight true threats.
- Risky behavior is detected by watching for new and unusual events:
 - Never before seen transactions (e.g. interactive login on a domain controller, payment authorization, accessing files never used before)
 - Never before used hosts (e.g. new IP)
 - High Volume of transactions (e.g. high number of failed logons, high number of TCP Firewall Denies, transfers of \$0.01 a billion times, accessing 1,000 patient/client/customer records)
 - High total amounts (e.g. 10GB firewall transfer, \$50,000 payment)

About Behavior Profiles

Signature-based approaches do not work well to detect zero-day attacks, and signature-based detection techniques are easy to circumvent by changing any single dimension of the attack sequence.

- Use Behavior Profiles to detect an unusual spike in volume of activity.
- Use Behavior Profiles to detect an unusual spike in amounts.

Examples for using behavior based anomaly detection include the following:

Threat Indicators	Explanation	Use of Behavior Profiling
Insider threat	Users operating from within the perimeter of an organization perform data reconnaissance over an extended period and slowly exfiltrate data	Run behavior-based analytics on the volume of data accessed and exfiltrated daily, weekly or monthly to detect suspiciously high data transfer rates
Lateral movement	Malware trying to infiltrate the network establishes connections to multiple devices	Run behavior analysis to detect suspiciously high volume of data connections or transfers
Brute force attacks	Brute force attacks attempt to access applications and systems by using multiple user name and password combinations	Identify suspiciously high volume of logon failures or failed connection attempts
Denial-of-service attacks	DoS attacks overwhelm the resources of a system using repeated service requests	Identify a suspiciously higher volume of requests than normal service by the system
Network reconnaissance mission	Attempts to detect vulnerabilities in network by scanning multiple devices for available services	Identify a suspiciously high volume of connection attempts across multiple ports
Data reconnaissance mission	Attempts to find important data across multiple data stores	Identify suspiciously high volume of data accessed by an account
Discount fraud/insurance claim fraud	User providing several type of discounts/claims to the same customer	Identify a suspiciously higher volume of discounts or claims than is normal in the peer population
Small amount fraud	User withdraws small amounts from customer accounts in order to stay under the threshold for triggering audits	Identify a suspiciously higher volume of transactions than normal in the peer population

What are Behavior Profiles?

Behavior based anomaly detection techniques detect indicators of compromise by finding deviations from normal. In doing so, the normal or valid behavior must first be extracted from reference data. The repeated observation of the same characteristics for an entity (typically a user or device) form the behavior for the entity. The characteristics to observe on the system depend on the use case involved.

Behavior profiling is mining usage characteristics from activity log data. Behavior profiles generated for users, peer groups and resources establish baseline observed over a period. These baselines have five major characteristics: time slices, activities, network sources, activity, attributes, and frequency.

How are Behavior Baselines Established?

The application generates behavior baselines by mining historical data. Generally, a minimum of 10 occurrences of a characteristic are required to generate a behavior baseline. These 10 occurrences may appear over a period of 10 days or even 10 weeks. Since the application uses the number of occurrences as one of the parameters when determining the risk rating of a suspicious event, there is a much lower probability of receiving false alerts.

Example: Determining baselines for number of Logon Failures

Acme Corp has three employees: John Doe, James Smith and Jane Brown.

Day #	Account Name	Number of Logon Failures
1	JOHN DOE	2
2	JOHN DOE	3
2	JAMES SMITH	2
2	JANE BROWN	1
3	JOHN DOE	3
3	JAMES SMITH	2
4	JOHN DOE	4
4	JAMES SMITH	3
5	JOHN DOE	1
5	JAMES SMITH	4
6	JOHN DOE	1
6	JAMES SMITH	3
7	JOHN DOE	20
7	JAMES SMITH	4
8	JOHN DOE	2
8	JAMES SMITH	6
9	JANE BROWN	2
9	JAMES SMITH	2
10	JANE BROWN	1
10	JAMES SMITH	3
11	JOHN DOE	4
11	JAMES SMITH	2
12	JOHN DOE	1
12	JAMES SMITH	3

Day #	Account Name	Number of Logon Failures
13	JOHN DOE	2
13	JAMES SMITH	3
14	JOHN DOE	4
14	JAMES SMITH	5
15	JOHN DOE	1
15	JAMES SMITH	3

Based on the 15 days of data presented above, the occurrence matrix for John Doe, James Smith and Jane Brown is presented in the following table:

Number of Logon Failures	John Doe	James Smith	Jane Brown
1 to 3 Logon Failures	9	10	3
4 to 6 Logon Failures	3	4	0
7 to 9 Logon Failures	0	0	0
10 to 12 Logon Failures	0	0	0
13 and higher Logon Failures	1	0	0

Conclusions:

- John Doe and James Smith generally experience 1 to 3 logon failures in a day.
- Jane has experienced only 3 occurrences, so her behavior baseline is inconclusive.
- Users generally perform 0 to 3 logon failures in a day.
- Users sometimes perform 4 to 6 logon failures in a day.
- John has performed a much higher number of logon failures on 1 day. This number is higher than is usual for him or his peers, and the entire user population.

What attributes should I choose to run behavior on?

Choose attributes for generating behavior based on the use case as described in the following example.

Example: SAP application logs authentication failure event

```
01/01/2014 10:23:00 JohnDoe 192.168.1.10 Action:Logon Failure  
Reason Code: Bad Password 01/01/2014 10:24:00 JohnDoe 192.168.1.10  
Action:Logon Failure Reason Code: Invalid Username 01/01/2014  
10:25:00 JohnDoe 192.168.1.20 Action:Logon Failure Reason Code:  
Account Locked 01/01/2014 10:26:00 JohnDoe 192.168.1.30  
Action:Logon Failure Reason Code: Insufficient Privileges
```

In this example, if you want to detect a brute force attack, choose to run behavior only on the Action. The reason code is not important in this case.

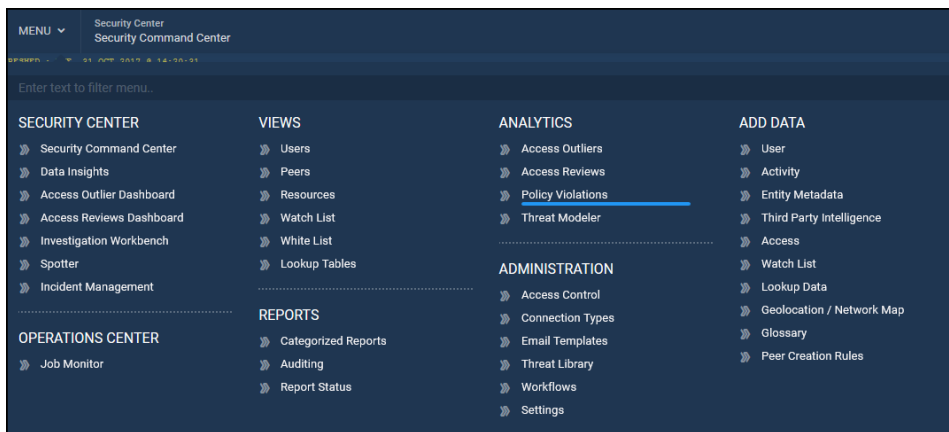
However, if you want to detect the behavior baseline for bad password, choose the Action and the Reason Code.

If you want to detect the behavior baseline for the number of failed logon attempts by IP Address, choose the Action and the IP Address.

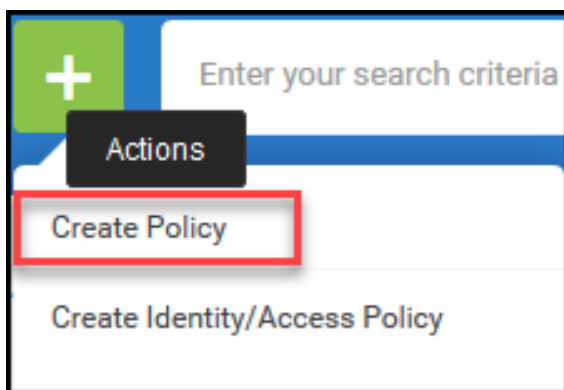
Creating Behavior Profiles

You can create Behavior Profiles when creating a behavior-based policy. To create Behavior Profiles when creating [Policy Violations](#) during Step 2: Provide Conditions, complete the following steps:

1. Navigate to **Menu > Analytics > Policy Violations:**



2. Click +.
3. Select **Create Policy**.



4. Complete **Step 1: Enter Policy Details**.
5. Proceed to **Step 2: Provide Conditions**.

What do you want to detect?

1. Select one of the following behavior-based analytics.

WHAT DO YOU WANT TO DETECT ?

1 Rare Behavior : Detects rare events compared to past behavior. Example : If an account uses ip address which is never used before.

RARE BEHAVIOR SPIKE IN NUMBER OF OCCURRENCES SPIKE IN VOLUME/AMOUNT ENUMERATION BEHAVIOR ABNORMAL ACTIVITY COMPARED TO PEERS INDIVIDUAL EVENT ANALYTICS AGGREGATED EVENT ANALYTICS LAND SPEED DETECTION TRAFFIC ANALYZER PHISHING

BATCHED ANALYTICS

- Rare Behavior
- Spike in Number of Occurrences
- Spike in Volume/Amount
- Enumeration Behavior
- Abnormal Activity Compared to Peers



Note: The fields described below may vary based on the analytical type selected in this step.

Choose the Features for Generating Behavior

1. Select the attributes from the panel on which to run the behavior profile.

CHOOSE THE FEATURES FOR GENERATING BEHAVIOR

☒ destinationhostnamecountry
☒ Filetype
☒ Method
☒ sourcehostnamelongitude
☒ Process_Name
☒ resourcehostnamepostalcode
☒ sessionid
☒ eventlatitude
☒ ResponseCode
☒ Referrer
☒ destinationhostnamepostalcode
☒ resourcehostnamecountry
☒ destinationhostnamecountry
☒ destinationhostnamecountry

Select the attributes from above panel

Selected features

1 Choose one or more features to generate behavior profiles. Behavior profiles will be generated on a combination of selected features.

Behavior Information

1. Provide a **Behavior Name** for this profile.
2. Choose a **Time Window** on which to run the profile.

BEHAVIOR INFORMATION

Behavior Name

Provide unique name for this behavior

Choose Time Window

☐ Hourly ☒ Daily ☐ Weekly ☐ Monthly ☐ Day of Week

Behavior will be generated according to time window selected

What Should get Flagged as Violations?

WHAT SHOULD GET FLAGGED AS VIOLATIONS ?

Number of occurrences of selected features is unusually higher than behavior baseline for :

☐ Self ☐ Other Accounts ☐ Peer Groups

Choose the Analytical Technique to run

-Select-

Flag as Violations when Rarity crosses Sigma Threshold Value

Slight Deviation High Deviation

0.85

1. Select an option for **Number of Occurrences of selected features is usually higher than behavior baseline for:**

Example 1:

- Self
- Other Accounts
- Peer Groups

Example 2:

- Department
- Division
- Location

2. Select from drop down for **Choose the Analytical Technique to run**. Example: Transaction Occurrence Abnormally higher than User's Daily Behavior.
3. Use slider to specify the Deviation from Slight to High for Flag as Violations when Rarity crosses Sigma Threshold Value. Example: 0.85.



Note: Sigma (standard deviation) threshold is calculated using inputs such as deviation from baseline, cluster confidence, number of valid and invalid clusters, and baseline value.

10. Proceed to Filter Conditions to finish creating policy. See [Policy Violations](#) for more information about how to create policies.

Viewing Behavior Profiles

You can view behavior profiles for policies from **Menu > Views > Users** or behavior profiles for specific datasources from **Menu > Views > Resources**.



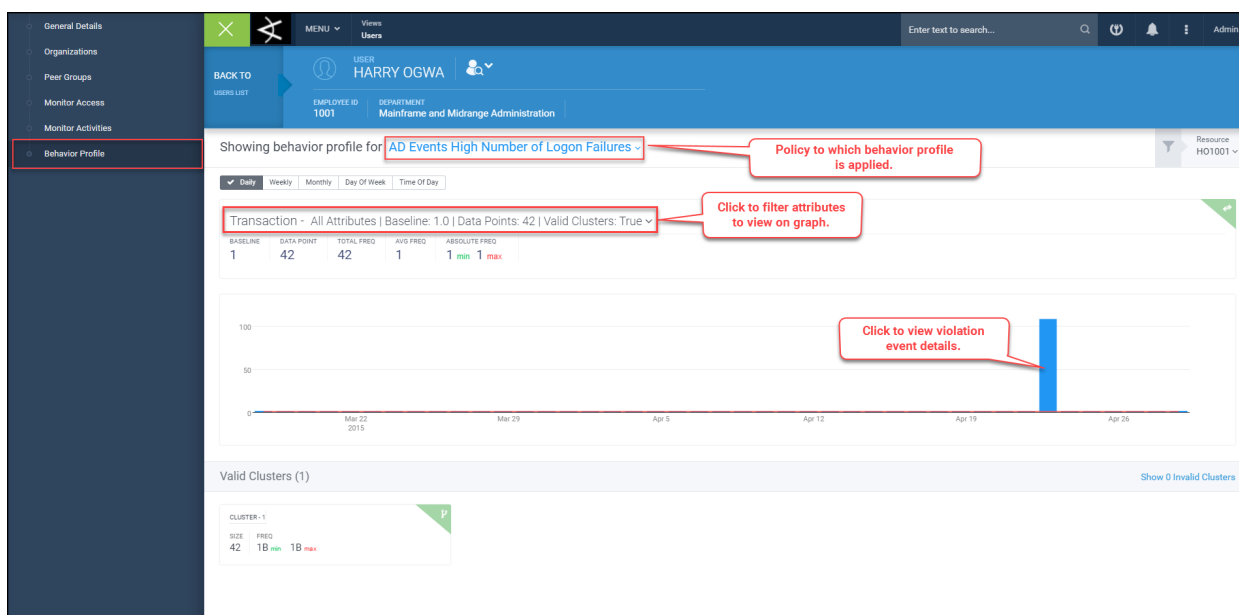
Note: See [Views](#) in the User Guide for more information about the types of views available.

Users

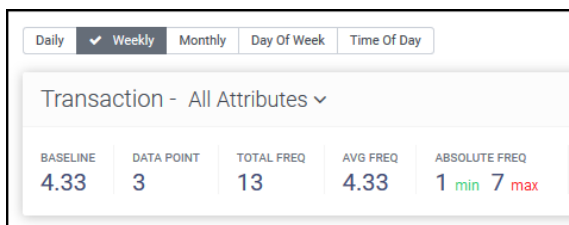
1. Click the **Employee ID** of the user you would like to view.

	Employee ID	First Name	Last Name	Manager Employee ID	Email	Department	Division	Title	Employee Type
<input type="checkbox"/>	1080	Demetria	Bridges	1070	Demetria.Bridges@scnx.com	Advertising	Global Marketing, Branding and Corporate Affairs	Vice President Advertising	FT
<input type="checkbox"/>	1095	Rosalyn	Harding	1080	Rosalyn.Harding@scnx.com	Advertising	Global Marketing, Branding and Corporate Affairs	Associate Vice President Advertising	FT
<input type="checkbox"/>	1099	Yeo	Twist	1080	Yeo.Twist@scnx.com	Advertising	Global Marketing, Branding and Corporate Affairs	Associate Advertising	FT
<input type="checkbox"/>	1130	Amena	Parker	1080	Amena.Parker@scnx.com	Advertising	Global Marketing, Branding and Corporate Affairs	Associate Advertising	FT
<input type="checkbox"/>	1131	Montana	Bean	1080	Montana.Bean@scnx.com	Advertising	Global Marketing, Branding and Corporate Affairs	Associate Advertising	FT
<input type="checkbox"/>	1136	Jelani	Charles	1080	Jelani.Charles@scnx.com	Advertising	Global Marketing, Branding and Corporate Affairs	Associate Advertising	FT
<input type="checkbox"/>	1345	Annie	Wong	1080	Annie.Wong@scnx.com	Advertising	Global Marketing, Branding and Corporate Affairs	Associate Advertising	FT
<input type="checkbox"/>	1349	Yann	Bernard	1080	Yann.Bernard@scnx.com	Advertising	Global Marketing, Branding and Corporate Affairs	Associate Advertising	FT
<input type="checkbox"/>	1380	Anh	Tran	1080	Anh.Tran@scnx.com	Advertising	Global Marketing, Branding and Corporate Affairs	Associate Advertising	FT
<input type="checkbox"/>	1381	Jeanine	Wong	1080	Jeanine.Wong@scnx.com	Advertising	Global Marketing, Branding and Corporate Affairs	Associate Advertising	FT

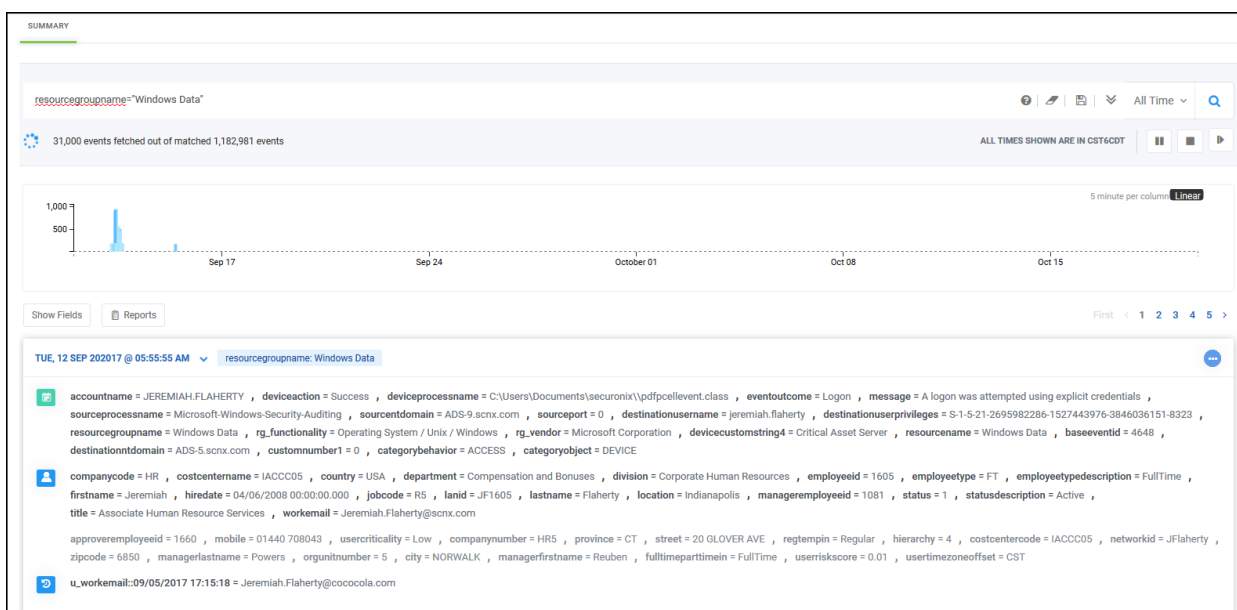
2. Click **Behavior Profile** from the left navigation pane.



3. Select a time range in which to view the behavior baseline: daily, weekly, monthly, day of week, or time of day. These options display the number of times the user performed a particular activity within the specified time range.



4. Filter **Transaction** attributes as needed from dropdown.
5. View a Summary of the events associated with the behavior profile you are viewing. Click any data point on the baseline to view specific events or enter a custom Spotter query. For more information about what you can do in this section, see [Spotter](#).

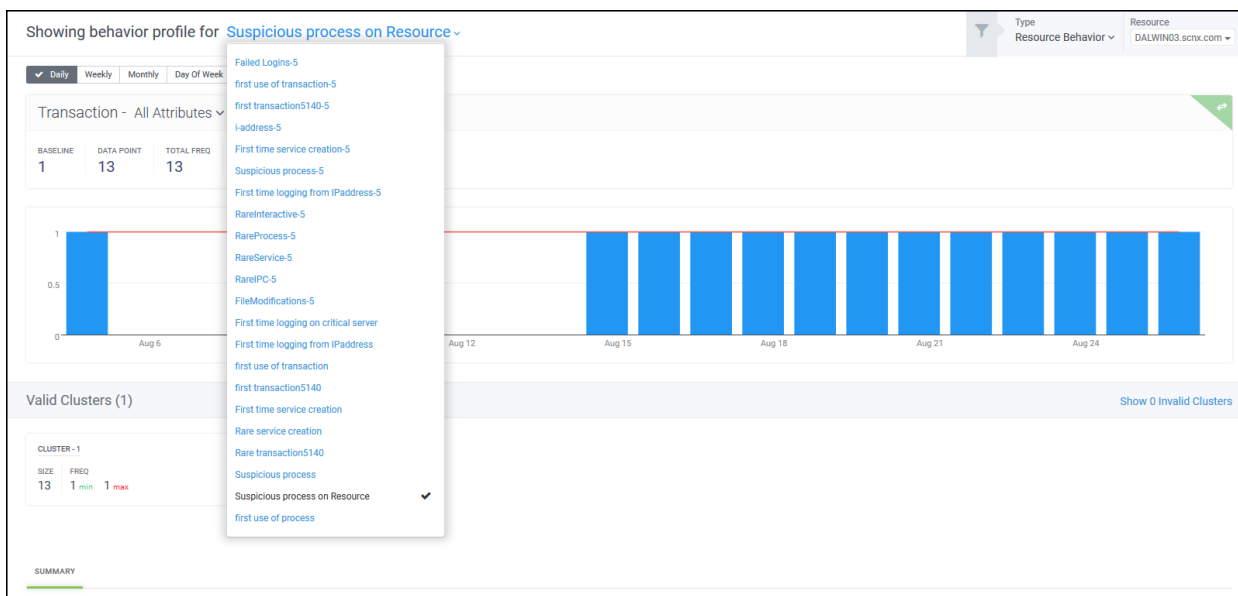


Resources

1. Click the **Name** of the Resource you would like to view.

Name	Type	IP Address	Category	Vendor	Last Event Date	Last Import Access Date
ADEvents	WindowsAD			Microsoft Corporation	-	-
BhanuTPI	BHANUTPI			Securonix	-	-
BluecoatProxy	Bluecoat			Symantec / Blue Coat Systems	-	-
BFSecurum4DatabaseAudit					-	-
DBAUDIT					-	-
GDnetLogs	GoogleD			Google	-	-
GoogleDriveLogs			Firewall/VPN	Palo Alto Networks	-	-
GoogleLogin	google			Google	-	-

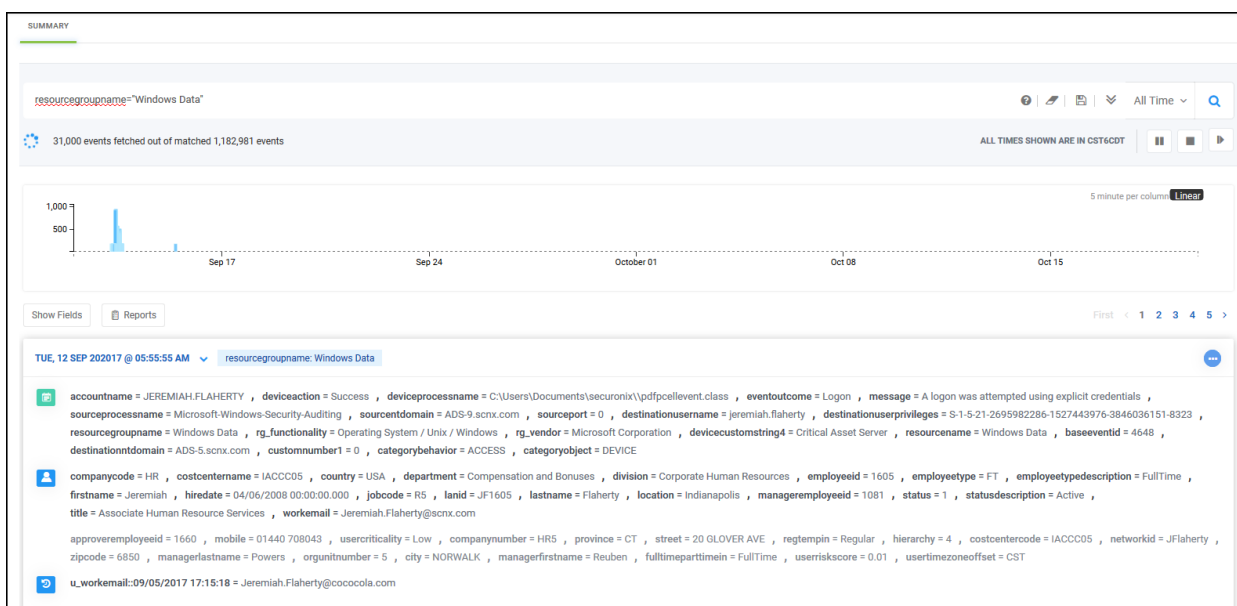
2. Click **Behavior Profile** from the left navigation pane.
3. Select a policy that has been configured for the datasource for which to view the behavior profile.



4. Select a time range in which to view the behavior baseline: daily, weekly, monthly, day of week, or time of day.

Daily	Weekly	Monthly	Day Of Week	Time Of Day
Transaction - All Attributes ▾				
BASILINE	DATA POINT	TOTAL FREQ	AVG FREQ	ABSOLUTE FREQ
4.33	3	13	4.33	1 min 7 max

5. View a Summary of the events associated with the behavior profile you are viewing. Click any data point on the baseline to view specific events or enter a custom Spotter query. For more information about what you can do in this section, see [Spotter](#).



Access Outliers

Users, such as employees and contractors, access company IT assets based on their user identities and roles. Besides individual access, users may be assigned to one or more peer groups depending on their identity attributes. Users that belong to a peer group (for example, Finance) share a common set of access privileges to function within the peer group. These peer groups exhibit distinct patterns of behavior. If a rogue activity is detected that breaks from the distinct pattern of the peer group, the user is considered an outlier.

ArcSight UBA analyzes the following factors to detect access risk:

- **Peer Group Cohesiveness:** Indicates the number of access entitlements that are held by the majority of the members of the peer group. The peer group cohesiveness factor takes into account the fact that most entitlements are not held by all users in a peer group.
- **Access Outlier Risk:** Indicates how many users in the peer group have the access privilege. A high value indicates fewer members in the peer group have that access privilege.

How Peer Group Analysis Works

Users are assigned to one or multiple peer groups based on their identity attributes. As shown above, John Doe, a user within the organization, belongs to three peer groups based on his job code, title, and manager. Peer groups that the user belongs to have other set of users with access privileges assigned to them.

Step 1: Determine which peer groups are valid against which to compare the user:

The access privileges held by users belonging to other peer groups may or may not have similar access privileges to each other. The “cohesiveness factor” determines how many access privileges are common amongst members of the peer group. The greater the number of common entitlements, the higher the cohesiveness value for the peer group. If the peer group is not cohesive enough, we do not have a high level of confidence in the user’s entitlement being an outlier in that peer group.

Step 2: Determine access “outlierness” of each entitlement held by a user:

Each access privilege held by a user is compared across the members of each peer group to determine the number of users that hold the same access privilege. The greater the number of users that hold the same entitlement, the less the probability of the access privilege being an outlier. The entitlement is determined to be an outlier if it crosses a threshold for “outlierness.”

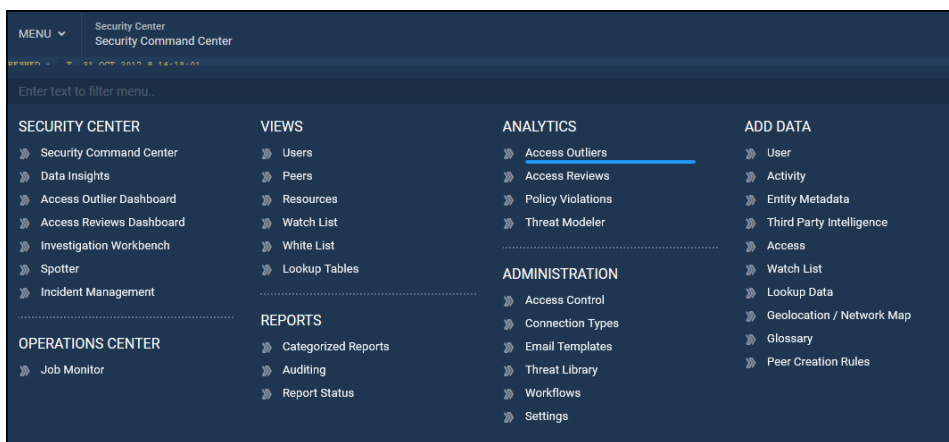
Step 3: Determine access risk for the user:

Each user within the organization may have one or multiple access privileges that are outliers. The greater the number of access privileges that are outliers, the higher the overall access risk for the user.

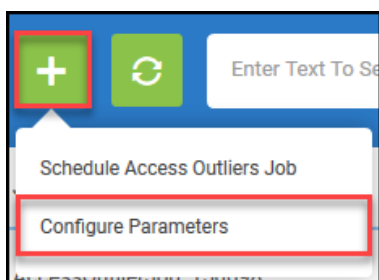
Configuring Variables for Outlier Detection and Peer Group Cohesiveness

To configure variables for outlier detection and peer group cohesiveness, complete the following steps:

1. Navigate to **Menu > Analytics > Access Outliers**.



2. Click **+**.
3. Click **Configure Parameters**.



4. Configure the following parameters:

Outlier Detection Risk Variables

OUTLIER DETECTION RISK VARIABLES

Certify All Entitlements?
☒ NO

Entitlement Cutoff

Any entitlement whose risk value crosses this cutoff value will be deemed as an Outlier.

Transaction Capacity Ceiling

If members of a peer have a large cumulative set of entitlements, the Transaction Capacity Ceiling looks for smaller subsets that are held by the members of that peer in order to counter for small clusters within a large population, a ceiling is set for the smaller population size. When this value is set as 10, the Outlier Analysis will form micro-clusters within a large population if the entitlement is held by 1 out of every 10 members in the Peer Group.

- **Certify All Entitlements?:** Set to **YES** to automatically set the next two parameters to look at all entitlements.
- **Entitlement Cutoff:** Enter or use slider to set a value between 0 and 1. An entitlement whose risk value exceeds the selected cutoff limit is considered an outlier.
- **Transaction Capacity Ceiling:** Use slider to set a value. If members of a peer group have a large cumulative set of entitlements, the Transaction Capacity Ceiling looks for smaller subsets that are held by the members of that group. For example, when this value is set as 10, the Outlier Analysis will form micro-clusters within a large population if the entitlement is held by 1 out of every 10 members in the Peer Group.

Peer Group Cohesiveness Variables

PEER GROUP COHESIVENESS VARIABLES

Peer Entitlement Strength*

0.8

When Calculating Peer Group Cohesiveness, an Access Privilege must be held by atleast these many users for it to contribute to the Cohesiveness of the Peer Group. A value of 0.5 indicates that atleast 50% of the Users in a Peer Group must have the Entitlement. The more the number of these entitlements the higher the Cohesiveness of the Peer Group.

Peer Capacity Ceiling*

10.0

For an entitlement to contribute towards Peer Cohesiveness, it is not necessary for all users within the Peer group to have the entitlement. Smaller populations within the peer group may have the same entitlement. Setting this value as 10, means that if 10% of entitlements are above Peer Entitlement Strength then peer cohesiveness is 1.

Min Peer Population*

10

A Peer Group must have atleast these many members in it for it to be considered during Outlier Analysis. If the Peer Group does not have enough members, it will not be considered during Peer Group Analysis.

Peer Cohesiveness Cutoff*

0.5

The Peer Group is considered during Outlier Analysis only if the cohesiveness value of the Peer Group crosses this threshold value. Peer Groups with low cohesiveness values means that the members of that Peer Group do not have similar entitlements. Keep this value low if you want all Peer Groups to be considered irrespective of their cohesiveness.

- **Peer Entitlement Strength:** Enter or use slider to set a value between 0 and 1. To calculate Peer Group Cohesiveness, an access privilege must be held by at least as many users (set by the value) for it to contribute to the cohesiveness of the peer group. A value of 0.5 indicates that at least 50% of the Users in a Peer Group have the Entitlement. The higher the number of these entitlements, the higher the cohesiveness of the peer group.
- **Peer Capacity Ceiling:** Enter or use slider to set a value between 0 and 10. This parameter calculates the Peer Capacity Ceiling value needed for peer cohesiveness. An entitlement can contribute towards Peer Cohesiveness even if not all users within the peer group have the entitlement. If this value is set to 10, this indicates that 10% of entitlements are above Peer Entitlement Strength then peer cohesiveness is 1.
- **Min Peer Population:** Enter or use slider to set a value. The peer group must have at least this number of members for it to be considered during Outlier Analysis. If the peer group does not
- **Peer Cohesiveness Cutoff:** Enter or use slider to set a value between 0 and 1. The peer group is considered during Outlier Analysis only if the cohesiveness value of the peer group crosses

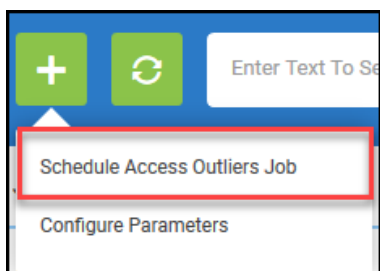
this threshold value. Low cohesiveness values indicate that the members of that peer group do not have similar entitlements. Keep this value low if you want all peer groups to be considered irrespective of their cohesiveness.

5. Click **Save**.

Running Access Outlier Analysis

To run the Access Outlier Analysis job, complete the following steps:

1. Navigate to **Menu > Analytics > Access Outliers**.
2. Click **+**.
3. Click **Schedule Access Outliers Job**.



Selection Criteria

Select one of the following user selection criteria:

i Select the user population whose access entitlements should be analyzed.

Click to choose one of the user selection criteria below



✓ All Peer Groups	Peer Criteria	Selected Peer Groups	All Users	Users Criteria	Selected Users
-------------------	---------------	----------------------	-----------	----------------	----------------

All Peer Groups will be selected for outlier analysis.









- **All Peer Groups:** Select all Peer Groups for outlier analysis. Proceed to next step.
- **Peer Criteria:** Select Peer Groups based on specified filter criteria. Complete the following steps:
 1. Enter filter criteria:

Click to choose one of the user selection criteria below

Enter filter criteria for Peer Groups below. Click on Preview to preview results. Ex. Select all Peer Groups of type

Attribute	Condition	Value	Operator	
location	Equal To	*	AND	 

[Preview](#)

<input type="checkbox"/>	Peer Name	Member Count	Location	Peer Group Type	
<input type="checkbox"/>	Advertising	12		Department	
<input type="checkbox"/>	Branding	2		Department	
<input type="checkbox"/>	Capital Markets	12		Department	
<input type="checkbox"/>	Cash Planning and Management	33		Department	
<input type="checkbox"/>	Client Development Group	4		Department	
<input type="checkbox"/>	Commodities	14		Department	
<input type="checkbox"/>	Compensation and Bonuses	20		Department	
<input type="checkbox"/>	Compliance Risk	11		Department	

Click to launch Investigation Workbench

- **Attribute:** Select a peer group attribute for analysis. Example: Location.
- **Condition:** Select from dropdown. Example: Equal To.
- **Value:** Enter the value of the peer group attribute. Example: Dallas.
- **Operator:** Select AND/OR from dropdown.
- **+/-:** Click to add/remove filters.
- **Preview:** Click to preview the peer groups that will be included in the analysis.
- **Selected Peer Groups:** Select specific peer groups to include in the outlier analysis. Complete the following steps:

1. Click **Add Peer Groups(s)**.

Select the user population whose access entitlements should be analyzed.

Click to choose one of the user selection criteria below

Select specific Peer Groups for outlier analysis. Click on **Add Peer Group(s)** button below to search and select Peer Groups. Only users belonging to selected peer groups will be considered for outlier analysis

Criticality	Peer Name	Member Count	Location	Peer Group Type

2. Enter search criteria to find specific Peer Groups in Add Peer Groups dialogue box.

Add Peer Groups ✕

5 membercount Q

<input type="checkbox"/>		Peer Name	Member Count	Location	Peer Group Type		
<input type="checkbox"/>		Associate Consumer Loan Specialist	5		Title		
<input type="checkbox"/>		Associate Enterprise Loans	15		Title		
<input type="checkbox"/>		Associate Marketing Analyst	5		Title		
<input type="checkbox"/>		Consumer and small business Loans	15		Department		



- Click to select one or multiple peer groups.
 - Click **Add Selected Peer Groups**.
 - Click **Remove Peer Groups(s)** to remove selected peer groups from analysis.
- All Users:** Select all users for outlier analysis. Proceed to next step.
 - Users Criteria:** Select users based on specified filter criteria. Complete the following steps:

1. Enter filter criteria:








Select the user population whose access entitlements should be analyzed.

Click to choose one of the user selection criteria below

Enter filter criteria for Users below. Click on Preview to preview results. Ex. Select all Users in location

Attribute	Condition	Value	Operator	
division	Equal To	Business Banking	AND	 

[Preview](#)

<input type="checkbox"/>	Employee ID	First Name	Last Name	Manager Employee ID	Email	Department	Division	Title	Employee Type	
<input type="checkbox"/>	1068	Amal	Wolfe	1025	Amal.Wolfe@scnx.com	Executive Management	Business Banking	Managing Dir. Business Development	FT	
<input type="checkbox"/>	1097	Katell	Blake	1068	Katell.Blake@scnx.com	Client Development Group	Business Banking	Vice President Business Development	FT	
<input type="checkbox"/>	1104	Olivia	Williams	1097	Olivia.Williams@scnx.com	Client Development Group	Business Banking	Associate Client Relations	FT	
<input type="checkbox"/>	1129	Ray	Hutchinson	1097	Ray.Hutchinson@scnx.com	Client Development Group	Business Banking	Associate Client Relations	FT	
<input type="checkbox"/>	1142	Anastasia	Morgan	1097	Anastasia.Morgan@scnx.com	Client Development Group	Business Banking	Associate Client Relations	FT	
<input type="checkbox"/>	1160	Hollie	Richardson	1068	Hollie.Richardson@scnx.com	Processing and Fulfillment	Business Banking	Vice President Business Services	FT	
<input type="checkbox"/>	1176	Aquila	Wynn	1160	Aquila.Wynn@scnx.com	Processing and Fulfillment	Business Banking	Associate Business Services	FT	

- **Attribute:** Select a peer group attribute for analysis. Example: division.
- **Condition:** Select from dropdown. Example: Equal To.
- **Value:** Enter the value of the peer group attribute. Example: Business Banking.
- **Operator:** Select AND/OR from dropdown.
- **+/-:** Click to add/remove filters.
- **Preview:** Click to preview the users that will be included in the analysis.

- **Selected Users:** Select specific users to include in the outlier analysis. Complete the following steps:

1. Click **Add User(s)**.

Select the user population whose access entitlements should be analyzed.

Click to choose one of the user selection criteria below

Only selected Users will be considered for outlier analysis. Click on **Add User(s)** button below to search and select Users.

Criticality	Employee ID	First Name	Middle Name	Last Name	Manager	Email	Title	Employee Type	Risk Score
-------------	-------------	------------	-------------	-----------	---------	-------	-------	---------------	------------

2. Enter search criteria to find specific Users in Add Users dialogue box.

Add Users

PT

employee type

<input type="checkbox"/>	Criticality	Employee ID	First Name	Middle Name	Last Name	Manager	Email	Title	Emp
<input type="checkbox"/>		1006	MEL		GIBSON	1001	MEL.GIBSON@scnx.com	Associate Mainframe Administrator	PT
<input type="checkbox"/>		1007	RAJESH		RAO	1001	RAJESH.RAO@scnx.com	Associate Mainframe Administrator	PT
<input type="checkbox"/>		1008	AKON		SHIATSU	1001	AKON.SHIATSU@scnx.com	Associate Mainframe Administrator	PT

Add Selected Users

3. Click to select one or multiple users.
4. Click **Add Selected Users**.
5. Click **Remove User(s)** to remove selected peer groups from analysis.

Click **Save and Next**.

Select Resource(s)

Select one of the following options to include in the outlier analysis:

2 Selection Criteria Select Resource(s) Run Job

Prev Save & Next

Select the criteria based on which user population will be selected for outlier analysis.

All Resources will be selected for outlier analysis.

- **All Resources:** Select all resources on which to run outlier analysis.
- **Selected Resources:** Select specific resources to be considered for outlier analysis. Complete the following steps:

1. Click **Add Resource(s)**.

Select the criteria based on which user population will be selected for outlier analysis.

Click to choose one of the user selection criteria below

Only selected Resources will be considered for outlier analysis. Click on **Add Resource(s)** button to search and selected Resources.

Criticality	Resource Name	Datasource Name	Resource Type	Resource Owner	Source IP	Risk Score
-------------	---------------	-----------------	---------------	----------------	-----------	------------

2. Enter search criteria to find specific Resources in Add Resources dialogue box.

Add Resources ✕

<input type="checkbox"/>	Criticality	Resource Name	Datasource	Hostname	IP Address	Type	Owner	Last Run D
<input checked="" type="checkbox"/>		Access Data	Access Data			Active Directory		

Show

Total results : 1 | Total pages : 1

3. Click to select one or multiple resources.
4. Click **Add Selected Resources**.
5. Click **Remove Resource(s)** to remove selected peer groups from analysis.

Click **Save and Next**.

Running the Job

1. Enter value or use slider to select Manually or specify a value between 0.95 (top 5%) and 0.0 (100%) for **How many entitlements would you like to review?** For example, 0.9 will return the top 10% of entitlements.

Job Details

1. Specify a **Job Name** or use auto-generated name.
2. Enter a **Job Description**.
3. **Enable Job Related Notifications** if you would like to receive email notifications when the job is run.
 - a. If **No**: Proceed without entering additional information.
 - b. If **Yes**:
 - **On Success**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template:
 - **On Failure**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template.
 - **On Misfired**: Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template.

ate a new email template.

- **On Completed with Errors:** Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template:

Create New Email Template

Sender Name* ⓘ

Template Name* ⓘ

Description

To* ⓘ

From*
test@securonix.com

CC ⓘ

BCC ⓘ

Subject ⓘ

HTML Enabled
☒ YES

Store in Outbox prior to sending?
☒ YES

Use this template for *

Owner ⓘ
Administrators
SECURITYOPERATIONS

Email Body ⓘ
Add Email Template Variables

Rich text editor toolbar: Bold, Italic, Underline, Bulleted List, Numbered List, Indent Left, Indent Right, Undo, Redo, Link, Unlink, Image, Video, Table, Quote, Code Block, Full Screen, Print.

Job Scheduling Information

1. Select when you would like the job to run.

JOB SCHEDULING INFORMATION

Run Job ⓘ

☒ Do you want to run job Once ?

☐ Do you want to schedule this job for future ?

i Job will be scheduled according to the server time. Current server time is - 5/1/2017 14:40:57

- Select **Do you want to run job Once?** to run now.
- Select **Do you want to schedule this job for future?** to run the job later and complete the relevant fields.

☒ Do you want to schedule this job for future ?

✓ Seconds Minutes Hourly Daily Weekly Monthly Specify Date

Select how often you want the job to run

Start Job At *

02:38:00 PM

NOTE: This is the server time

Run Every *

Seconds

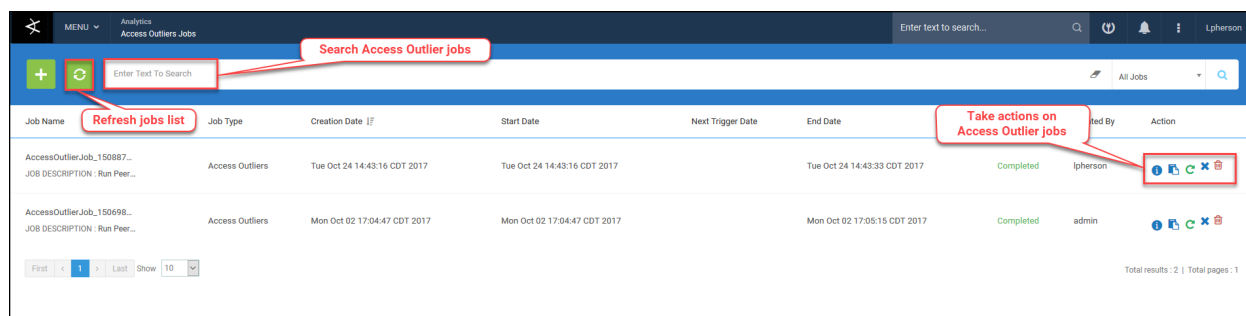
Stop after

Times

1. Select when you would like the job to run.
2. **Save** job.
3. Click **Run**.






Reviewing Access Outlier Jobs

To review and manage Access Outlier jobs, navigate to **Menu > Analytics > Access Outliers**. The recent access outlier jobs appear.



You can perform the following actions on Access Outlier Jobs:

Actions

	Show job details
	Review Access Outliers
	Re-run job
	Delete Access Outliers
	Delete job



Note: The available actions for Access Outlier jobs vary depending on the user's role. For example, non-admin users may only be able to delete jobs.

Review Access Outlier Job Details

The Access Outlier Job Details screen displays the following information:

- Resources selected for the job.
- Details about the each user with outlier access including the following:
 - Employee ID
 - First and Last Name
 - Account Name
 - Access Outlier Probability
 - Mapped Attributes

Outlier Probability Cut Off: 0.8

Adjust outlier threshold by moving the slider above (or typing into the box) to the desired percentage and click Preview Results to view results based on threshold selected. Click on the finalize button to send results to the security dashboard.

Employee ID	First Name	Last Name	Account	Access Outlier Probability	Mapped Attribute(s)
1593	Walter	Molony	WM1593	0.99	memberOf: CN=HR_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com
1593	Walter	Molony	WM1593	0.99	memberOf: CN=Portal_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com
1593	Walter	Molony	WM1593	0.99	memberOf: CN=CRM_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com
1593	Walter	Molony	WM1593	0.99	memberOf: CN=BankSoft_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com
1852	Colm	Murphy	CM1852	0.99	memberOf: CN=PAY_User,OU=Applications,OU=Corporate,DC=scnx,DC=com
1811	Audrey	Feighery	AF1811	0.99	memberOf: CN=AP_User,OU=Applications,OU=Corporate,DC=scnx,DC=com
2657	Ciara	Prasad	CP2657	0.99	memberOf: CN=BUDGET_APPROVER,OU=Applications,OU=Corporate,DC=scnx,DC=com
2667	Stuart	Brennan	SB2667	0.99	memberOf: CN=COMPTROLLER_UPDATE,OU=Applications,OU=Corporate,DC=scnx,DC=com

To view Access Outlier Job Details, complete the following steps:

1. Click **Review Access Outliers** icon.
2. Click a Resource name to view outliers for that resource.
3. (Optional) Adjust **Outlier Probability Cut Off** slider to desired percentage. For example, 0.9 will return the top 10% of entitlements.
4. Click **Preview Results** to view results based on the Probability Cut Off.
5. Click **+** to view the following details about each user including the following:

	Employee ID	First Name	Last Name	Account	Access Outlier Probability ⓘ	ⓘ Mapped Attribute(s)	
☰	1593	Walter	Molony	WM1593	0.99	memberOf: CN=BankSoft_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com	
Peer Name				Type	Cohesiveness	Risk Value ⓘ	Users With Entitlement
Compensation and Bonuses				Department	0.98639	1.0	1/20
Corporate Human Resources				Division	0.98639	1.0	1/51
Associate Human Resource Services				Title	0.98639	1.0	1/14
R5				Job Code	0.98639	1.0	1/17
Reuben_Powers_1081				Manager	0.98639	1.0	1/19

- **Peer Name:** Peer Groups to which the user belongs. Example: Compensation and Bonuses.
- **Type:** Types of Peer Groups to which the user belongs. Example: Department.
- **Cohesiveness:** Peer Cohesiveness of the Peer Groups to which the user belongs. Example: 0.98639.
- **Risk Value:** Value of the risk. Example: 1.0.
- **Users with Entitlement:** Number of users in the peer group with the entitlement compared to the number of users without access.

Click to view Users With Access and Users Without Access.

Users with access 136						
<div> <div>Users With Access</div> <div>Users Without Access</div> </div>						
Criticality	Employee ID	First Name	Last Name	Manager	Email	Department
	1593	Walter	Molony	1081	Walter.Molony@scnx.com	Compensation and Bonuses
<div> <div>First</div> <div>< 1 ></div> <div>Last</div> <div>Show 10</div> <div>Total results : 1 Total pages : 1</div> </div>						

- Click an **Employee ID** to view details about the user.

Walter Molony [1593] Details

General Details

Organizations

Peer Groups

Monitor Access

Monitor Activities

Behavior Profile

GENERAL DETAILS

USER ID	EMPLOYEE ID	FIRST NAME	MIDDLE NAME
-	1593	Walter	-
LAST NAME	JOB CODE	DOMESTIC/INTERNATIONAL	ORGANIZATION UNIT NUMBER
Molony	R5	-	5
EMPLOYEE TYPE	PROMOTED	EMPLOYEE TYPE DESCRIPTION	LAST PERFORMANCE REVIEW DATE
FT	-	FullTime	-
FULL TIME/PART TIME	COST CENTER NAME	COST CENTER CODE	SHIFT CODE
FullTime	IACCC05	IACCC05	-
ORGANIZATION UNIT NUMBER	MAIL CODE	NAME PREFIX	USER GROUP
5	-	-	-
STANDARD HOURS	DEPARTMENT	LAST PERFORMANCE REVIEW RESULT	REGULAR/TEMPORARY
-	Compensation and Bonuses	-	Regular
CRITICALITY	NETWORK ID	COMPANY CODE	NAME SUFFIX
Low	VMolony	HR	-
COMPANY NUMBER	PREFERRED NAME	HIERARCHY	TITLE
HR5	-	4	Associate Human Resource Services
STATUS	DIVISION	STATUS DESCRIPTION	COMMENTS
1	Corporate Human Resources	Active	-

General Details

Contact Details

Workflow Details

Employment History

Custom Properties

Change History

- Click **Finalize/Send for Access Review** to send results to the Access Outlier Dashboard.
- View the new job on the Access Outlier Jobs screen.

Job Name	Job Type	Creation Date	Start Date	Next Trigger Date	End Date	Status	Created By	Action
Access Outlier Job_150887... JOB DESCRIPTION : Access Outlier Review	Access Outlier Review	Tue Oct 24 15:48:13 CDT 2017	Tue Oct 24 15:48:13 CDT 2017		Tue Oct 24 15:48:14 CDT 2017	Completed	lpherson	
AccessOutlierJob_150887... JOB DESCRIPTION : Run Peer...	Access Outliers	Tue Oct 24 14:43:16 CDT 2017	Tue Oct 24 14:43:16 CDT 2017		Tue Oct 24 14:43:33 CDT 2017	Completed	lpherson	
AccessOutlierJob_150698... JOB DESCRIPTION : Run Peer...	Access Outliers	Mon Oct 02 17:04:47 CDT 2017	Mon Oct 02 17:04:47 CDT 2017		Mon Oct 02 17:05:15 CDT 2017	Completed	admin	

First < 1 > Last Show 10

Total results : 3 | Total pages : 1



Note: You can delete this job, but other actions are unavailable.

Viewing Access Outlier Results

View Access Outlier results on the [Access Outliers Dashboard](#).

See the ArcSight UBA User Guide for more information about what you can do from this dashboard.

MENU

Security Center

Access Outliers Dashboard

Enter text to search...

Lpherson

High Risk Users

17

Rogue Access Detac...

15

Enter Criteria

Click to refresh results

Click to export outliers as a PDF

Search for specific users with outlier access

employeeid

Employee ID	First Name	Last Name	Manager Employee ID	Email	Department	Title	Risk Score
1067	Rigel	Rodgers	1067	Rigel.Rodgers@scnx.com	Credit Evaluation	Associate Credit Products	4.94
1044	Francis	Gallagher	1044	Francis.Gallagher@scnx.com	Consumer Risk	Associate Consumer Risk	4.22
1081	Walter	Molony	1081	Walter.Molony@scnx.com	Compensation and Bonuses	Associate Human Resource Services	3.97
1091	Brady	Pierce	1091	Brady.Pierce@scnx.com	Mortgage Products	Vice President Mortgage Products	3.69
1086	Kennedy	Harding	1086	Kennedy.Harding@scnx.com	Capital Markets	Associate Vice President Capital Markets	3.41
1810	Audrey	Feighery	1810	Audrey.Feighery@scnx.com	Consumer and small business Loans	Vice President Consumer and SBA Loans	0.99
1852	Colm	Murphy	1811	Colm.Murphy@scnx.com	Consumer and small business Loans	Associate Consumer Loan Specialist	0.99
2590	Graham	O'Sullivan	2588	Graham.O'Sullivan@scnx.com	Debt Planning and Management	Associate Debt Management	0.99
2655	Sally	Flynn	2588	Sally.Flynn@scnx.com	Debt Planning and Management	Associate Debt Management	0.99
2657	Ciana	Prasad	2588	Ciana.Prasad@scnx.com	Debt Planning and Management	Associate Debt Management	0.99

First

<

1

2

>

Last

Show

10

Total results : 17 | Total pages : 2

Access Reviews

Ensuring that users have the right access for their job is both necessary for demonstrating compliance and also the last line of defense for protecting against a data breach or sabotage attempt.

Users with unnecessary, excessive or inappropriate access rights increase the risk of data breach, compromising sensitive information and sabotage. Effective access governance requires organizations to establish policies and procedures to manage access rights, especially if they are subject to industry or government regulations such as SOX, HIPAA, GLBA, PCI DSS, BASEL II and others.

ArcSight UBA automates the access compliance management lifecycle, enabling organizations to strengthen controls and demonstrate compliance easily, while reducing the time and costs involved.

Simplified entitlement reviews are designed for business users and IT or security administrators.

ArcSight UBA allows authorized users to review business-friendly entitlements definitions and easily certify, modify, or revoke user access rights. Integration with leading DLP and SIEM tools correlates sensitive data alerts (generated by DLP) or user activity alerts (from SIEM) with user access rights to provide the manager with a comprehensive user profile, including what data the user has access to, as well as previous activity patterns. ArcSight UBA highlights instances where access rights violate policy, such as access to sensitive data that is not part of the individual's business role, or Segregation of Duties (SOD) violations. The authorized business managers can review user access rights to any enterprise platform or application and directly change, disable, or delete inappropriate rights and entitlements.

Types of Certifications

ArcSight UBA provides the ability to schedule several different types of certifications. The administrator responsible for running the certification can choose the type of certification and the user population to include in the certification, and decide which systems or applications to include in the certification.

The following broad categories of certifications are available:

1. **Based on the certifier:** Based on who will perform the review, certifications can be scheduled for:
 - User's direct manager
 - System or application owner
 - Data owner
2. **Based on the data to certify:** Based on what will be certified, certifications can be scheduled for:
 - All accounts and underlying entitlements
 - Accounts and roles
 - High risk entitlements

3. **Based on which user will be certified:** Based on which user will be certified:

- All users
- Only high risk users
- Only transferred users
- Users belonging to specific department, title, job code or any other condition

ArcSight UBA allows any combination of the above three broad categories. This means there are more than 50 different combinations from which to choose.

Access Review Checklist

Before performing access reviews/certifications, there are some processes and procedures to perform within the organization.

Certification Requirements

1. What applications and systems are in scope?
2. Do you want to certify accounts and entitlements?
3. How often must the certification occur?
4. Who is responsible for launching and administering reviews?
5. Who is responsible for certifying access?
6. Do you want to certify all or only high risk access?
7. Who will train the certifier?
8. How often should the reviewer be notified and reminded of the certification?
9. What happens to the certifications that are not completed in time?
10. What are the reporting requirements from the certification?

Data Collection

Identity Data

- What is the best source for identity data?
- How often must identity data be collected?

Access Data

- Will the application or system export the access data?
- Is a direct connection required to the application to extract access data?
- What is the rule to correlate account names to identity data?
- What access attributes must be extracted from the system or application?

Perform Certification

- When should reviews be triggered?
- Are the reviewers trained on how to perform the certification?

Managing Incomplete and Bad Certifications

- What should be done with orphaned certifications (certifications that don't have an existing certifier)?
- What should be done with certifications not completed by the due date?

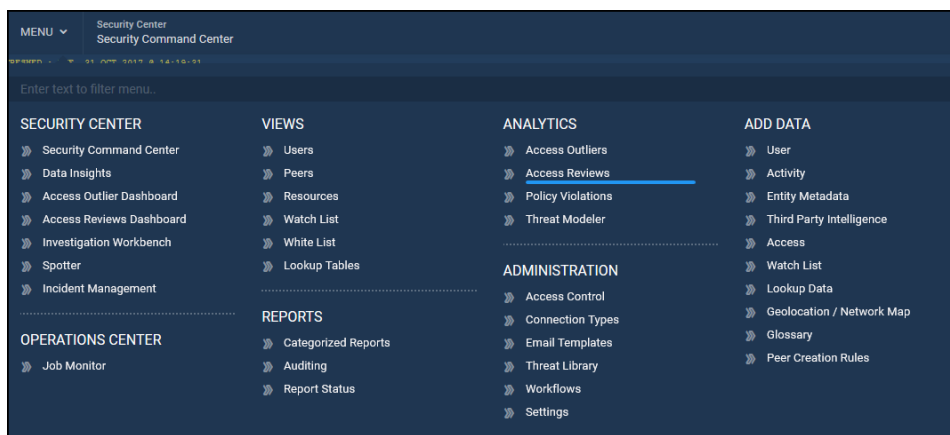
Act on Certification Results

- What happens to the access entitlements that are revoked by the reviewer?

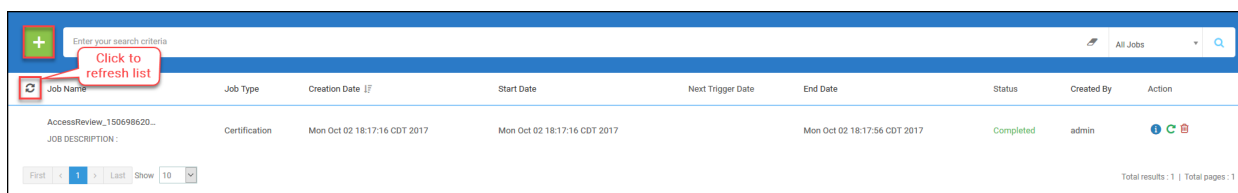
Scheduling Access Review Jobs

To configure schedule an Access Review job, complete the following steps:

1. Navigate to **Menu > Analytics > Access Reviews**.



2. Click +.



Selection Criteria

Select one of the following user selection criteria:

1

Selection Criteria

Select Resource(s)

Run Job

Select the user population whose access entitlements should be analyzed.

✓ All Peer Groups

Peer Criteria

Selected Peer Groups

All Users

Users Criteria

Selected Users

Transferred Users

All Peer Groups will be selected for outlier analysis.

- **All Peer Groups:** Select all Peer Groups for access review. Proceed to next step.
- **Peer Criteria:** Select Peer Groups based on specified filter criteria. Complete the following steps:
 1. Enter filter criteria:

Select the user population whose access entitlements should be analyzed.

All Peer Groups

✓ Peer Criteria

Selected Peer Groups

All Users

Users Criteria

Selected Users

Transferred Users

Enter filter criteria for Peer Groups below. Click on **Preview** to preview results. Ex. Select all Peer Groups of type

Object	Attribute	Condition	Value	Operator	
Peer Group	name	Equal To	Compliance Risk	AND	⊕ ⊖

☐ Peer Name
 ☐ Compliance Risk

Member Count
11

Location

Peer Group Type
Department

First 1 Last Show 10

Total results: 1 | Total pages: 1

- **Object:** Select an object for review. Example: Peer Group.
- **Attribute:** Select a peer group attribute for review. Example: name.
- **Condition:** Select from dropdown. Example: Equal To.
- **Value:** Enter the value of the peer group attribute. Example: Compliance Risk.
- **Operator:** Select AND/OR from dropdown.
- **+/-:** Click to add/remove filters.
- **Preview:** Click to preview the peer groups that will be included in the review.
- **Selected Peer Groups:** Select specific peer groups to include in the access review. Complete the following steps:

1. Click **Add Peer Groups(s)**.

Select the user population whose access entitlements should be analyzed.

Click to choose one of the user selection criteria below

Select specific Peer Groups for outlier analysis. Click on **Add Peer Group(s)** button below to search and select Peer Groups. Only users belonging to selected peer groups will be considered for outlier analysis

Criticality	Peer Name	Member Count	Location	Peer Group Type

2. Enter search criteria to find specific Peer Groups in Add Peer Groups dialogue box.

Add Peer Groups ✕

5 membercount Q

<input type="checkbox"/>		Peer Name	Member Count	Location	Peer Group Type		
<input type="checkbox"/>		Associate Consumer Loan Specialist	5		Title		
<input type="checkbox"/>		Associate Enterprise Loans	15		Title		
<input type="checkbox"/>		Associate Marketing Analyst	5		Title		
<input type="checkbox"/>		Consumer and small business Loans	15		Department		

3. Click to select one or multiple peer groups.

4. Click **Add Selected Peer Groups**.5. Click **Remove Peer Groups(s)** to remove selected peer groups from analysis.

- **All Users:** Select all users for access review. Proceed to next step.
- **Users Criteria:** Select users based on specified filter criteria. Complete the following steps:

1. Enter filter criteria:

1 Selection Criteria Select Resource(s) Run Job [Save And Next](#)

Select the user population whose access entitlements should be analyzed.

All Peer Groups Peer Criteria Selected Peer Groups All Users **Users Criteria** Selected Users Transferred Users

Enter filter criteria for Users below. Click on **Preview** to preview results. Ex. Select all Users in location

Object	Attribute	Condition	Value	Operator		
User	department	Equal To	Finance	AND		

[Preview](#)

<input type="checkbox"/>	Employee ID	First Name	Last Name	Manager Employee ID	Email	Department	Division	Title	Employee Type	
<input type="checkbox"/>	1087	Ulla	Hines	1074	Ulla.Hines@scnx.com	Finance	Finance and Accounting	Vice President Financial Accounting	FT	A
<input type="checkbox"/>	1098	Donovan	Lyons	1087	Donovan.Lyons@scnx.com	Finance	Finance and Accounting	Associate Vice President Financial Accounting	FT	A
<input type="checkbox"/>	1105	Lillith	Mueller	1087	Lillith.Mueller@scnx.com	Finance	Finance and Accounting	Associate Financial Accounting	FT	A
<input type="checkbox"/>	1154	Kyra	Chan	1087	Kyra.Chan@scnx.com	Finance	Finance and Accounting	Associate Financial Accounting	FT	A
<input type="checkbox"/>	1188	Geraldine	Clements	1087	Geraldine.Clements@scnx.com	Finance	Finance and Accounting	Associate Financial Accounting	FT	A
<input type="checkbox"/>	1192	Hayley	Coleman	1087	Hayley.Coleman@scnx.com	Finance	Finance and Accounting	Associate Financial Accounting	FT	A

- **Object:** Select the object on which to run the analysis. Example: User.
- **Attribute:** Select a peer group attribute for analysis. Example: division.
- **Condition:** Select from dropdown. Example: Equal To.
- **Value:** Enter the value of the peer group attribute. Example: Business Banking.
- **Operator:** Select AND/OR from dropdown.
- **+/-:** Click to add/remove filters.
- **Preview:** Click to preview the users that will be included in the analysis.
- **Selected Users:** Select specific users to include in the access review. Complete the following steps:

1. Click **Add User(s)**.

Select the user population whose access entitlements should be analyzed.

Only selected Users will be considered for outlier analysis. Click on **Add User(s)** button below to search and select Users.

	Criticality	Employee ID	First Name	Middle Name	Last Name	Manager	Email	Title	Employee Type	Risk Score

2. Enter search criteria to find specific Users in Add Users dialogue box.

Add Users

PT

employee type

<input type="checkbox"/>	Criticality	Employee ID	First Name	Middle Name	Last Name	Manager	Email	Title	Err
<input type="checkbox"/>		1006	MEL		GIBSON	1001	MEL.GIBSON@scnx.com	Associate Mainframe Administrator	PT
<input type="checkbox"/>		1007	RAJESH		RAO	1001	RAJESH.RAO@scnx.com	Associate Mainframe Administrator	PT
<input type="checkbox"/>		1008	AKON		SHIATSU	1001	AKON.SHIATSU@scnx.com	Associate Mainframe Administrator	PT

Add Selected Users

3. Click to select one or multiple users.

4. Click **Add Selected Users**.5. Click **Remove User(s)** to remove selected peer groups from access review.

- **Transferred Users:** Select only transferred users to include in the access review. Proceed to next step.

Click **Save and Next**.

Select Resource(s)

Step 1: Select one of the following options to include in the access review:

2 Selection Criteria Select Resource(s) Run Job Prev Save & Next

Select the criteria based on which user population will be selected for outlier analysis.

All Resources will be selected for outlier analysis.

- **All Resources:** Select all resources on which to run access review.
- **Selected Resources:** Select specific resources to be considered for access review. Complete the following steps:

1. Click **Add Resource(s)**.

2. Enter search criteria to find specific Resources in Add Resources dialogue box.

3. Click to select one or multiple resources.
4. Click **Add Selected Resources**.
5. Click **Remove Resource(s)** to remove selected peer groups from analysis.

Step 2: Click **Configure Parameters** to specify Certification Risk Variables and Peer Cohesiveness Group Variables for selected Resources.

Configure Parameters

Certification Risk Variables

Note: You have selected all resources. Configuration will be updated for all resources. Previous configuration will be over-written.

Entitlement Cutoff *

0.5

Any entitlement whose risk value crosses this cutoff value will be deemed as an Outlier.

Transaction Capacity Ceiling *

10.0

If members of a peer have a large cumulative set of entitlements, the Transaction Capacity Ceiling looks for smaller subsets that are held by the members of that

Save

Certification Risk Variables:

- **Entitlement Cutoff:** Enter or use slider to set a value between 0 and 1. An entitlement whose risk value exceeds the selected cutoff limit is considered an outlier.
- **Transaction Capacity Ceiling:** Use slider to set a value. If members of a peer group have a large cumulative set of entitlements, the Transaction Capacity Ceiling looks for smaller subsets that are held by the members of that group. For example, when this value is set as 10, the Outlier Analysis will form micro-clusters within a large population if the entitlement is held by 1 out of every 10 members in the Peer Group.

Peer Group Cohesiveness Variables:

- **Peer Entitlement Strength:** Enter or use slider to set a value between 0 and 1. To calculate Peer Group Cohesiveness, an access privilege must be held by at least as many users (set by the value) for it to contribute to the cohesiveness of the peer group. A value of 0.5 indicates that at least 50% of the Users in a Peer Group have the Entitlement. The higher the number of these entitlements, the higher the cohesiveness of the peer group.
- **Peer Capacity Ceiling:** Enter or use slider to set a value between 0 and 10. This parameter calculates the Peer Capacity Ceiling value needed for peer cohesiveness. An entitlement can contribute towards Peer Cohesiveness even if not all users within the peer group have the entitlement. If this value is set to 10, this indicates that 10% of entitlements are above Peer Enti-

tlement Strength then peer cohesiveness is 1.

- **Peer Cohesiveness Cutoff:** Enter or use slider to set a value between 0 and 1. The peer group is considered during Outlier Analysis only if the cohesiveness value of the peer group crosses this threshold value. Low cohesiveness values indicate that the members of that peer group do not have similar entitlements. Keep this value low if you want all peer groups to be considered irrespective of their cohesiveness.

Step 3: Click **Save and Next**.

Running the Job

Provide the following information:

Run Job

Access Review Type

✓ Manager Data Owner User

Do you want to run a Access Review on all entitlements or only outlier entitlements?

✓ All Entitlements Outlier Entitlements

Min Peer Population

10

A Peer Group must have atleast these many members in it for it to be considered during Outlier Analysis.If the Peer Group does not have enough members, it will not be considered during Peer Group Analysis.

Access Review End Date *

Reminder Dates. You can set up to 3 reminders.

Reminder Date 1

Reminder Date 2

Reminder Date 3

Send Access Review Emails?

NO

Select 'Yes' if you want to send emails to Manager/Data Owner/User for access reviews

- **Access Review Type:** Select one of the following options:
 - **Manager:** Review by Manager.
 - **Data Owner:** Review by Data Owner.
 - **User:** Review by User
- **Do you want to run an Access Review on all entitlements or only outlier entitlements?:** Select one of the following:
 - **All Entitlements:** Run review on all entitlements.
 - **Outlier Entitlements:** Run review only on outlier entitlements.

- **Min Peer Population:** Enter or use slider to set a value. The peer group must have at least this number of members for it to be considered during Outlier Analysis. If the peer group does not have enough members, it will not be considered during Peer Group Analysis.
- **Access Review End Date:** Click to select a date on which the access review will end.
- **Reminder Dates:** Click to set up reminders for this access review. You can set up to three reminders.
- **Send Access Review Emails?:** Select **YES** to send emails to the Manager/Data Owner/User to certify the access review.
 - Select **Email Template:** Select from dropdown. Example: Access Certification Email.

The screenshot displays the configuration interface for an Access Review job, divided into two main sections: **JOB DETAILS** and **JOB SCHEDULING INFORMATION**.

JOB DETAILS includes:

- Access Review Name:** A text field containing "AccessReview_1508883355644".
- Description:** A large text area for job description.
- Enable Job Related Notifications:** A toggle switch set to "YES".

JOB SCHEDULING INFORMATION includes:

- Run Job:** Radio buttons for "Do you want to run job Once?" (selected) and "Do you want to schedule this job for future?".
- Scheduling Note:** A message stating "Job will be scheduled according to the server time. Current server time is - 10/24/2017 18:06:03".

Below these sections are four columns for notification templates:

- ON SUCCESS:** Select Email Template to Use for Sending Notifications (dropdown), OR Override email address from template (text field).
- ON FAILURE:** Select Email Template to Use for Sending Notifications (dropdown), OR Override email address from template (text field).
- ON MISFIRE:** Select Email Template to Use for Sending Notifications (dropdown), OR Override email address from template (text field).
- ON COMPLETED WITH ERRORS:** Select Email Template to Use for Sending Notifications (dropdown), OR Override email address from template (text field).

Each column has a note: "If we specify email address above then email addresses in email template will be overridden."

Job Details

1. Specify a **Job Name** or use auto-generated name.
2. Enter a **Job Description**.
3. **Enable Job Related Notifications** if you would like to receive email notifications when the job is run.
 - a. If **No**: Proceed without entering additional information.
 - b. If **Yes**:
 - **On Success:** Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template:
 - **On Failure:** Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template.

- **On Misfired:** Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template.
- **On Completed with Errors:** Select an email template from the dropdown to send notifications to your default email address or enter an email address to send notifications. You can also create a new email template:

Create New Email Template

Sender Name*

Template Name*

Description

To*

From*

test@securonix.com

CC

BCC

Subject

HTML Enabled

YES

Store in Outbox prior to sending?

YES

Use this template for *

Job Misfired

Owner

Administrators

SECURITYOPERATIONS

>

>>

<<

<

Email Body

Add Email Template Variables

B

I

U

abc

x

x'

T

rt

HI

T

Job Scheduling Information

1. Select when you would like the job to run.

JOB SCHEDULING INFORMATION

Run Job

☒ Do you want to run job Once ?

☐ Do you want to schedule this job for future ?

Job will be scheduled according to the server time. Current server time is - 5/1/2017 14:40:57

- Select **Do you want to run job Once?** to run now.
- Select **Do you want to schedule this job for future?** to run the job later and complete the relevant fields.

☒ Do you want to schedule this job for future ?

Select how often you want the job to run

Start Job At *

02:38:00 PM

NOTE: This is the server time

Run Every *

Seconds

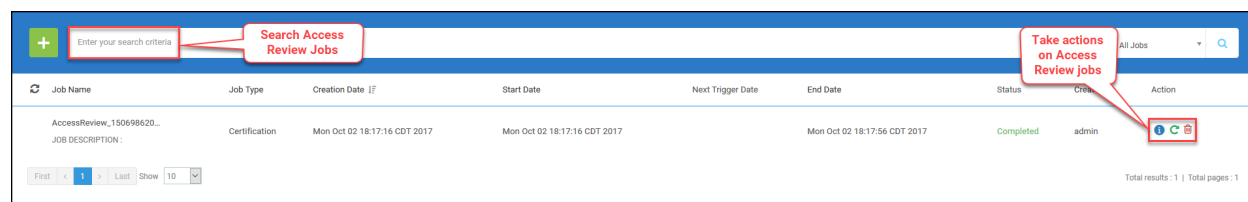
Stop after

Times

1. Select when you would like the job to run.
2. **Save** job.
3. Click **Run**.


Reviewing Access Review Jobs

To review and manage Access Outlier jobs, navigate to **Menu > Analytics > Access Reviews**. The recent access review jobs appear.



You can perform the following actions on Access Review Jobs:

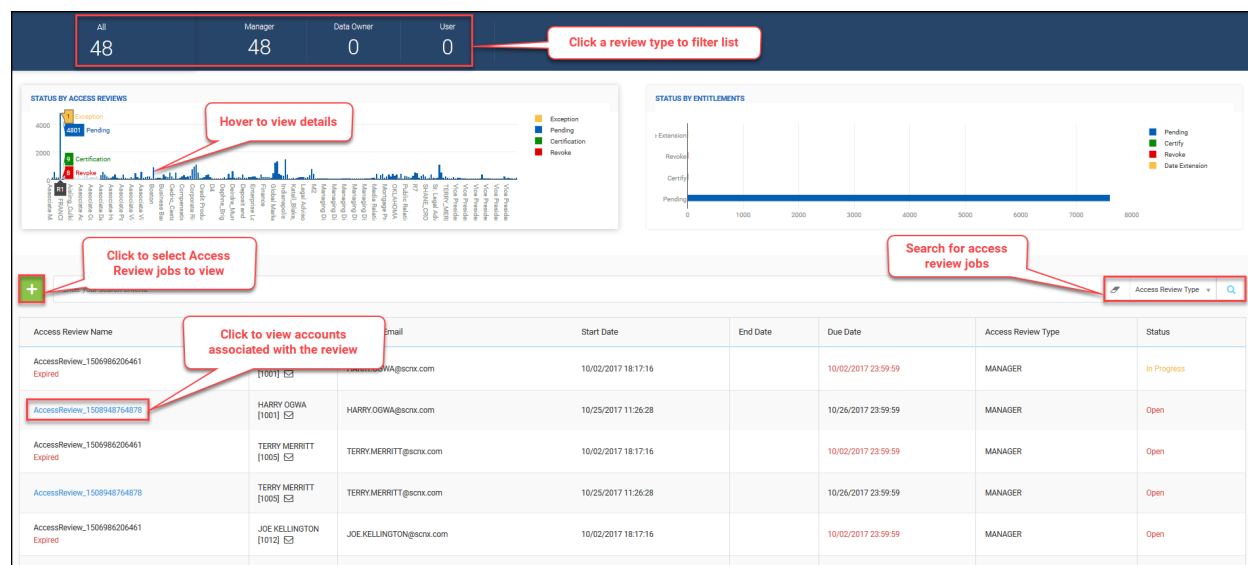
Actions

	Show job details
	Re-run job
	Delete job

Viewing Access Review Results

View Access Review results on the [Access Reviews Dashboard](#).

See the ArcSight UBA User Guide for more information about what you can do from this dashboard.



Traffic Analyzer

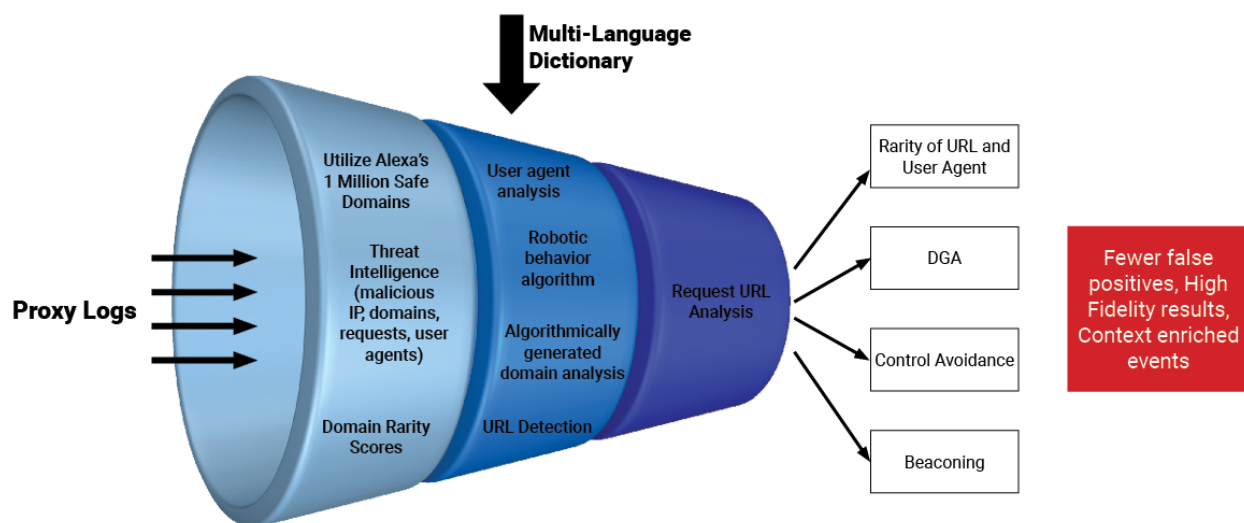
The ArcSight UBA Traffic Analyzer performs specific checks against proxy traffic to detect rare domains, user agents, and algorithmically generated domains, as well as patterns of malicious or robotic behavior that indicate a sophisticated cyber attack. The ArcSight UBA Traffic Analyzer performs the following checks:

- [Rare Domain Visited](#)
- [Rare User Agent](#)
- [Detection of possible control avoidance](#)
- [Multiple Protocols used on URL](#)
- [Traffic to Algorithmically Generated Domains \(DGA\)](#)
- [Detection of possible control avoidance](#)
- [Detection of beaconing behavior \(All proxy traffic\)](#)

This document offers an overview of how the ArcSight UBA Traffic Analyzer works and explains the configuration details for the Traffic Analyzer checks described above.

Traffic Analyzer Overview

To detect rare domains, user agents, and algorithmically generated domains, control avoidance, and beaconing behavior, the Traffic Analyzer checks proxy logs against safe domains such as Alexa's 1 Million Safe Domains, threat intelligence, and domain rarity scores generated based on the organization's baseline proxy traffic behavior; compares domains to multi-language dictionary words to detect algorithmically generated domains; and analyzes request URLs.



Traffic Analyzer Checks

Rare Domain Visited

This Traffic Analyzer check uses **Traffic Analyzer Check: URL Visited by Visitors** to track proxy traffic to domains that are rare compared to the organization's typical browsing behavior. The rarity of the domain is a direct measure of the number of users visiting that pay level domain (PLD), and the rarity score is assigned on a scale of 0-1, with 1 implying the domain is rare.

The check

Configuration for this Check

The following configuration is used for this check:

The screenshot shows the 'TRAFFIC ANALYZER CHECKS' configuration page. The 'URL VISITED BY VISITORS' tab is selected. The configuration for this check includes:

- Select URL Attribute:** Destination HostName
- Select Visitor Attribute:** Account Name
- Number of Visitors:** 20
- Threshold:** A slider ranging from Low to High, currently set at 0.85.
- Check Against Alexa:** YES (checked)
- Select Domain Attribute:** Destination HostName

Key Configuration Parameters

- **Select URL Attribute: Destination Hostname** refers to the URL of the destination.
- **Select Visitor Attribute: Account Name** refers to the name of the account visiting the Destination Hostname.
- **Number of Visitors:** Refers to the number of visitors per destination hostname to be considered for rare domain. If the number is exceeded, the domain is no longer considered rare and is whitelisted.
- **Threshold:** Refers to the number of days of base-lining (**0.85**: 30 days) before a violation is

flagged. See [Reference: Threshold configuration](#) for threshold values.

- **Check Against Alexa:** Value **YES** Excludes domains matching the Alexa 1M list from the check.
 - **Select Domain Attribute: Destination Hostname** refers to the URL of the destination to check against Alexa.

Rare User Agent

This Traffic Analyzer check uses **Traffic Analyzer Check: Useragent Visited by Visitors** to track proxy traffic to domains that are rare compared to the organization's typical browsing behavior. The rarity of a user agent is a direct measure of the number of accounts per use agent, and the rarity score is assigned on a scale of 0-1, with 1 implying the domain is rare.

Configuration for this Check

The following configuration is used for this check:

The screenshot shows the 'TRAFFIC ANALYZER CHECKS' configuration page. The 'USERAGENT VISITED BY VISITORS' tab is selected. The configuration for this check includes:

- Select User Agent:** dropdown menu set to 'requestclientapplication'.
- Select Visitor Attribute:** dropdown menu set to 'requestclientapplication'.
- Number of Visitors:** input field set to '5'.
- Threshold:** a slider between 'Low' and 'High' with a value of '0.22'.
- Check Against Alexa:** a radio button set to 'NO'.

Key Configuration Parameters

- **Select User Agent: requestclientapplication** refers to the user agent.
- **Select Visitor Attribute: requestclientapplication** refers to the user agent.
- **Number of Visitors:** The value **5** refers to the number of accounts per user agent to be considered for rare user agent. If the number is exceeded, the user agent is no longer considered rare and is whitelisted.
- **Threshold:** The value **0.22** refers to the number of days (4) of base-lining before a violation is flagged. See [Reference: Threshold configuration](#) for threshold values.

Detection of possible control avoidance

This Traffic Analyzer check uses **Traffic Analyzer Check: Ports Used on URL** to track avoidance of proxy controls such as if the same hostname has been both allowed and blocked. The check uses the deviceaction field provided by the proxy logs.

Configuration for this Check

The following configuration is used for this check:

The screenshot shows the 'TRAFFIC ANALYZER CHECKS' interface. The 'PORTS USED ON URL' tab is selected. The configuration for this check is as follows:

- Select URL Attribute:** Destination HostName
- Select Port Attribute:** Device Action
- No of Ports Allowed:** 1
- Threshold:** A slider is positioned between 'LOW' and 'High', with a value of 0.22 displayed.
- Check Against Alexa:** YES (indicated by a green circle)
- Select Domain Attribute:** Destination HostName



Note: A pre-requisite to check if the domain is rare is recommended.

Key Configuration Parameters

- **Select URL Attribute: Destination Hostname** refers to the URL of the destination.
- **Select Port Attribute: Device Actions** refers to actions of the device such as allowing or blocking a **Destination Hostname**.
- **No of Ports Allowed:** Value **1** refers to the number of **Device Actions** present for a **Destination Hostname**. If the number exceeds **1**, the check will flag the domain.

Multiple Protocols used on URL

This Traffic Analyzer check uses **Traffic Analyzer Check: Protocols used on URL** to track when a specified number of protocols used across a specified number of says has been exceeded.

Configuration for this Check

The following configuration is used for this check:

TRAFFIC ANALYZER CHECKS

URL VISITED BY VISITORS USERAGENT VISITED BY VISITORS PORTS USED ON URL **PROTOCOLS USED ON URL** RANDOMLY GENERATED URL BEACONING

Protocols used on URL

Select URL Attribute: Destination HostName Select Protocol Attribute: transportprotocol

No of Protocols Allowed: 10 Threshold: 0.85 (Low to High slider)

Check Against Alexa: ☐ NO



Note: A pre-requisite to check if the domain is rare is recommended.

Key Configuration Parameters

- **Select URL Attribute: Destination Hostname** refers to the URL of the destination.
- **Select Protocol Attribute:** Example: **transportprotocol** refers to the type of protocol used to transfer data to or from a **Destination Hostname**.
- **No of Protocols Allowed:** Value **10** refers to the number of **transportprotocols** present for a **Destination Hostname**. If the number exceeds **10**, the check will flag the domain.
- **Threshold:** Refers to the number of days of base-lining (**0.85**: 30 days) before a violation is flagged. See [Reference: Threshold configuration](#) for threshold values.

Traffic to Algorithmically Generated Domains (DGA)

This Traffic Analyzer check uses **Traffic Analyzer Check: Randomly Generated URL** to track traffic to domains that look algorithmically generated.

Configuration for this Check

The following configuration is used for this check:

TRAFFIC ANALYZER CHECKS

URL VISITED BY VISITORS USERAGENT VISITED BY VISITORS PORTS USED ON URL PROTOCOLS USED ON URL RANDOMLY GENERATED URL BEACONING

URL Visited by Visitors

Select URL Attribute: Destination HostName

Select Visitor Attribute: Account Name

Number of Visitors: 20

Threshold: 0.85

Randomly generated URL

Select URL Attribute: Destination HostName

DGA score: 3

Check Against Alexa: YES

Key Configuration Parameters

- **Recommended Prerequisite:**

- **Traffic Analyzer: URL Visited by Visitors** to check the rarity of a domain.

- **Select URL Attribute: Destination Hostname** refers to the URL of the destination.
 - **Select Visitor Attribute: Account Name** refers to the name of the account visiting the Destination Hostname.
 - **Number of Visitors:** Refers to the number of visitors per destination hostname to be considered for rare domain. If the number is exceeded, the domain is no longer considered rare and is whitelisted.
 - **Threshold:** Refers to the number of days of base-lining (**0.85**: 30 days) before a violation is flagged. See [Reference: Threshold configuration](#) for threshold values.
 - **Check Against Alexa:** Value **YES** Excludes domains matching the Alexa 1M list from the check.
 - **Select Domain Attribute: Destination Hostname** refers to the URL of the destination to check against Alexa.

- **Select URL Attribute: Destination Hostname** refers to the URL of the destination.
 - **DGA Score** value **3 (Low)** refers to the DGA score computed for the domain. Any DGA score greater than the DGA Score value is flagged. The check is performed only across the PLD.

Detection of beaconing behavior (to possible malicious domains)

This Traffic Analyzer check uses **Traffic Analyzer Check: Beaconing** to detect beaconing traffic behavior between a source and a destination on proxy logs. This check builds behavior profiles for every combination of source IP and destination hostname seen on the proxy logs, and alerts if the cluster quality of the behavior is on the high side, indicating a possible beaconing pattern.

Configuration for this Check

The following configuration is used for this check:

The screenshot shows the configuration interface for the 'Beaconing' check. At the top, there is a condition bar with a green plus icon, a dropdown menu set to 'TPI Category', and a value of 'Malicious'. Below this is a '+ ADD GROUP' button. The main section is titled 'TRAFFIC ANALYZER CHECKS' and contains several tabs: 'URL VISITED BY VISITORS', 'USERAGENT VISITED BY VISITORS', 'PORTS USED ON URL', 'PROTOCOLS USED ON URL', 'RANDOMLY GENERATED URL', and 'BEACONING' (which is highlighted in orange). The 'Beaconing' configuration panel includes three dropdown menus: 'Select Source Attribute' (set to 'Account Name'), 'Select Destination Attribute' (set to 'Destination HostName'), and 'Select Request Uri Attribute' (set to 'Request Uri'). Below these is a 'Number of Distinct Destinations allowed' field set to '5'. To the right is a 'Confidence factor' slider ranging from 'Low' to 'High', with a value of '0.60' displayed. At the bottom left, there is a 'Check Against Alexa' checkbox which is currently unchecked.



Note: When configuring the check from the UI, add condition to filter for domains falling under the usual malware categories.

Key Configuration Parameters

- **Select Source Attribute: Account Name** refers to the name of the account requesting or visiting a destination URL.
- **Select Destination Attribute: Destination Hostname** refers to the URL of the destination.
- **Request URL Attribute: Request URL** refers to the URL requested by the source.
- **Number of Distinct Destination allowed:** For value **5**, only the destination domains for which the URL variations are less than **5** will be published as violations.
- **Confidence Factor:** Refers to the cluster quality, which is a direct measure of the beaconing behavior. For value **0.60**, only accounts with cluster confidence factor greater than **0.60** will be considered for analysis.

Detection of beaconing behavior (All proxy traffic)

This Traffic Analyzer check uses **Traffic Analyzer Check: Beaconing** to detect beaconing traffic behavior between a source and a destination in proxy logs. This check builds behavior profiles for every combination of source IP and destination hostname seen on the proxy logs, and alerts if the cluster quality of the behavior is on the higher side, indicating a possible beaconing pattern.

Configuration for this Check

The following configuration is used for this check:

The screenshot shows the 'TRAFFIC ANALYZER CHECKS' interface. At the top, there are several tabs: 'URL VISITED BY VISITORS', 'USERAGENT VISITED BY VISITORS', 'PORTS USED ON URL', 'PROTOCOLS USED ON URL', 'RANDOMLY GENERATED URL', and 'BEACONING'. The 'BEACONING' tab is selected and highlighted in orange. Below the tabs, there are two configuration panels. The top panel is titled 'Beaconing' and contains three dropdown menus: 'Select Source Attribute' (set to 'IPAddress'), 'Select Destination Attribute' (set to 'Destination HostName'), and 'Select Request Url Attribute' (set to 'Destination HostName'). Below these is a 'Number of Distinct Destinations allowed' field set to '5' and a 'Confidence factor' slider ranging from 'Low' to 'High' with a value of '0.85'. The bottom panel is titled 'URL Visited by Visitors' and contains two dropdown menus: 'Select URL Attribute' (set to 'Destination HostName') and 'Select Visitor Attribute' (set to 'Account Name'). Below these is a 'Number of Visitors' field set to '10' and a 'Threshold' slider ranging from 'Low' to 'High' with a value of '0.85'.

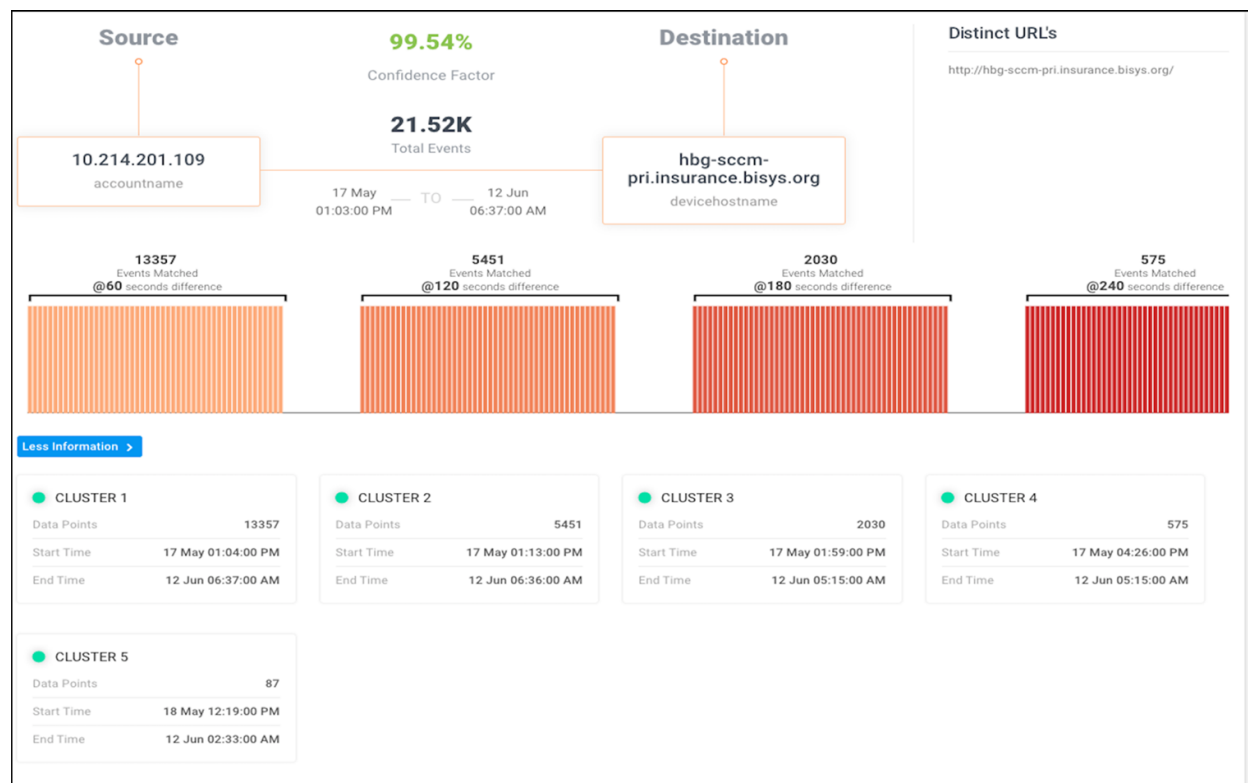


Note: The pre-requisite for this check is to run a domain rarity analysis. It also excludes white-listed domains present in Redis from analysis.

Key Configuration Parameters

- **Select Source Attribute: IPAddress** refers to the IP Address requesting or visiting a destination URL.
- **Select Destination Attribute: Destination Hostname** refers to the URL of the destination.
- **Request URL Attribute: Destination Hostname** refers to the URL of the destination requested by the source IP Address.
- **Number of Distinct Destination allowed:** For value **5**, only the destination domains for which the URL variations are less than **5** will be published as violations.
- **Confidence Factor:** Refers to the cluster quality, which is a direct measure of the beaconing behavior. For value **0.85**, only accounts with cluster confidence factor greater than **0.85** will be considered for analysis.

Example Beaconing Violation



Reference: Threshold configuration

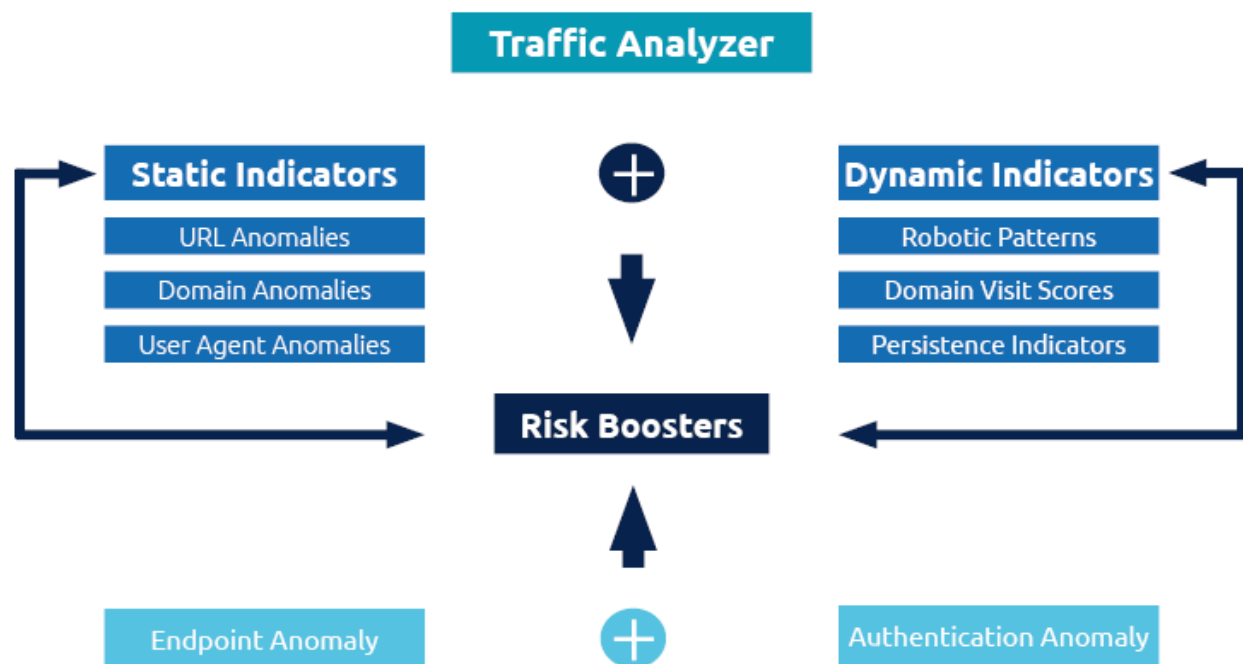
The following table maps the number of days required for baselining to the threshold value that should be specified in the Traffic Analyzer configuration.

Days	0	1	2	3	4	5	6	7	8	9	10	1-1	12	13	14	15	16	17
Threshold	0-0	0-06	0-12	0-17	0-22	0-27	0-31	0-35	0-39	0-43	0-46	0-5	0-53	0-56	0-58	0-61	0-63	0-65

Days	18	19	20	21	22	23	24	25	2-6	27	28	29	30	31	32	33	34
Threshold	0.6-7	0.6-9	0.7-1	0.7-3	0.7-5	0.7-6	0.7-8	0.7-9	0.8-8	0.8-1	0.8-3	0.8-4	0.8-5	0.8-6	0.8-6	0.8-7	0.8-8

Traffic Analyzer Threat Model: Persistent Malware Communication

Traffic Analyzer checks can be used in threat models to predict, detect, and contain the sequence of events that could be part of an advanced attack. The Persistent Malware Communication Threat Model uses Traffic Analyzer checks to analyze static indicators (URL Anomalies, Domain Anomalies, and User Agent Anomalies) **plus** Dynamic Indicators (Robotic Patterns, Domain Visit Scores, and Persistence Indicators) **plus** a combination of Endpoint and Authentication Anomalies to boost the risk score for these behaviors.



Violation Result

User Details

EmployeeID: ozkang01

NetworkID: 10.198.26.281

Threat	Domain	Violation Behavior
Domain Presence/Rarity	miledaughter.ru	Only IP in the network seen to attempt communicating to all domains
	s0ibspyxb7by8.ru	
	3uorg03dxfy.ru	
	n46gd0nenr1az.ru	
	dmud3vysja6me4.ru	
	cbbze5u2m65vg8.ru	
DGA	s0ibspyxb7by8.ru	Domains detected to be DGA with successful traffic
	3uorg03dxfy.ru	
	n46gd0nenr1az.ru	
	dmud3vysja6me4.ru	
	cbbze5u2m65vg8.ru	
Robotic Communication	miledaughter.ru	Observed about 300 events every 15 minutes (3 days, steady stream of bytes, unusual time of day compared to past behavior)
Robotic Communication Bytes Analysis	miledaughter.ru	Bytes being transmitted were always around 2001 bytes or 160 bytes
Suspicious URL Communication	n46gd0nenr1az.ru	Domains seen to exhibit proxy avoidance by changing connection from HTTP to TCP to pass through proxy control
	s0ibspyxb7by8.ru	
Suspicious Packet Drop	dmud3vysja6me4.ru	Domains seen to have a successful TCP packet with a size > account general baseline of 5 KB.
	s0ibspyxb7by8.ru	

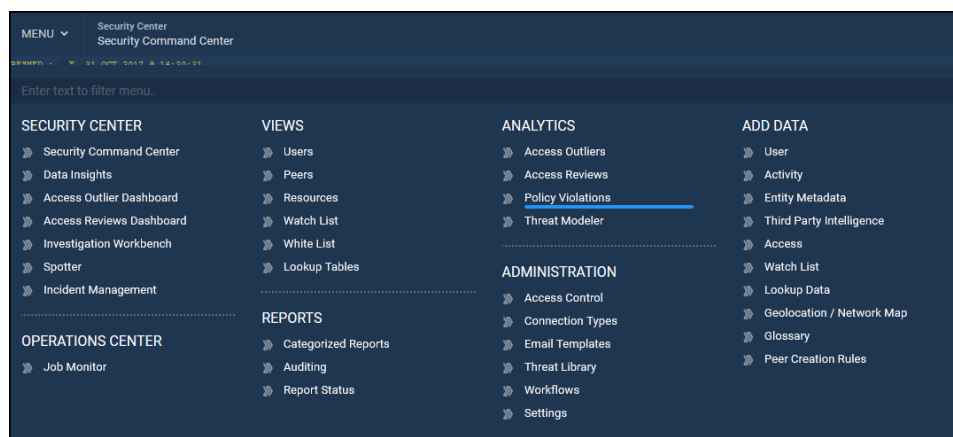
Policy Violations

Policies are predefined sets of rules. ArcSight UBA provides a very flexible policy engine that can be used to run checks against Identity, Access, Events, Resources, and Activity IP data. ArcSight UBA comes pre-packaged with a variety of policies, or you can create custom policies. Policies are used for the following:

- Checking for known bad signatures (rules)
- Managing separation of duties
- Checking against business specific rules
- Managing compliance and regulatory requirements

A violation occurs when a user performs an action that contradicts a policy.

To create a new policy, navigate to **Menu > Analytics > Policy Violations**.



Click **+** to create a new policy.

The screenshot shows the ArcSight Policy Violations page. A red box highlights the '+' button in the top left corner, which is used to create a new policy. The page displays a table of policy violations with columns: Type, Datasource, Last Update Date, Violation Entity, Enabled?, and Actions.

Type	Datasource	Last Update Date	Violation Entity	Enabled?	Actions
Abnormal high number of attempts to upload files-59	Tier 2 Behavior Summary		Activity Account	YES	
Abnormal high number of attempts to upload files-60	Tier 2 Behavior Summary		Activity Account	YES	
Abnormal high volume of uploads-59	Tier 2 Behavior Summary		Activity Account	YES	
Abnormal high volume of uploads-60	Tier 2 Behavior Summary		Activity Account	YES	
Accounts that belong to terminated user	Identity Policy	2015-04-02 22:11:20.0	Access Account	YES	
Accounts that dont have Users	Identity Policy	2015-04-02 22:11:43.0	Access Account	YES	
Accounts where user dont have manager	Identity Policy	2015-04-02 22:12:15.0	Access Account	YES	
Accounts with Domain Admin Access	Identity Policy	2015-04-02 22:21:56.0	Access Account	YES	

The following options are available:

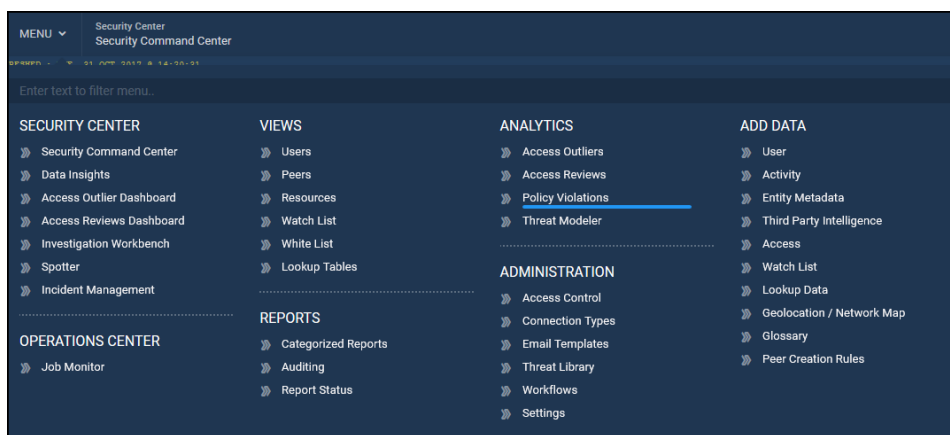
- [Creating Policies](#): Select this option to create real time policies that flag single or multiple events that result in a violation, and behavior-based policies that perform frequency and rarity checks to detect behavior-based or peer-based outliers.
- [Creating Identity /Access Policies](#): Select this option to create policies using a built-in template. Templates store the underlying joins to facilitate the execution of a policy.

Creating Policies

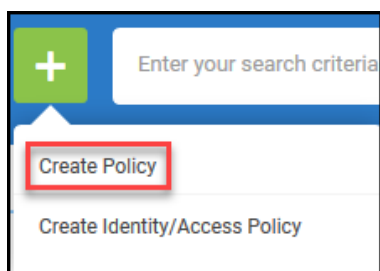
Create a policy to flag single or multiple events that result in a violation, or behavior-based policies that perform frequency and rarity checks to detect behavior-based or peer-based outliers. This section includes how to create policies for single and multiple events using frequency and rarity checks; conditions; analytical checks against active lists, lookup tables, watchlists, and TPI; directives; and risk boosters.

To create a policy, complete the following steps:

1. Navigate to **Menu > Analytics > Policy Violations**:



2. Click +.
3. Select **Create Policy**.



Enter Policy Details

In this section, configure the policy name, criticality, entity against which the policy will run, and the datasource to which the policy will be applied, as well as designating the owner and remediator of the policy in order to restrict what users may view the policy violations. Define the category and indicator of threat.

Define Policy

Complete the following information:

DEFINE POLICY

Policy Name*

Provide unique name which will describe what type of violation it detects. Special characters are not allowed. Example: (- (bracket), ' - (single quote) are not allowed

Description

Criticality

Low

Select the criticality of the policy. The criticality affects the risk score for the user. None=0.0, Low=0.2, Medium=0.6 and High=1.0

Do you want to save violations and calculate risk scores for this policy?

☒ YES ☐ NO

If Yes, violations will be searchable in Spotter and risk scores will be calculated for violators. If No, violations will not be searchable and risk scores will not be calculated for violators of this policy.

Do you want to escalate this policy as a Threat?

☒ YES ☐ NO

If Yes, this policy will be escalated as a Threat instead of a Violation and will appear under Top Threats in Security Command Center. If no, this policy will appear under the Top Violations widget.

Select Violation Entity*

Select the entity that the risk should apply to?

"Users" - Returns list of users violating policy. Orphan accounts(or uncorrelated accounts) will be ignored.Users cannot be used in behavior based policy.

"ActivityAccount" - Returns list of activity accounts (both correlated and uncorrelated) violating the policy.

"Resources" - Returns list of resources violating the policy.

"Resource Group Account" - Returns list of activity accounts across datasources (both correlated and uncorrelated) violating the policy.

Do you want to run the policy on a

☒ Datasource ☐ Functionality

- a. **Policy Name:** Provide a unique name to describe the type of violation the policy detects.
- b. **Description:** Enter a brief description of the policy.
- c. **Criticality:** Use slider to select the criticality of the policy.



Note: This will affect the risk score for the user. None=0.0, Low=0.2, Medium=0.6, and High=1.0.

- d. **Do you want to save violations and calculate risk scores for this policy?:** Toggle to **YES** to make violations for this policy searchable in Spotter and to calculate risk scores for violators. If disabled, violations will not be searchable and risk scores will not be calculated.
- e. **Do you want to escalate this policy as a Threat?:** Toggle to **YES** to escalate the policy to a threat rather than a policy violation. Violations will appear under Top Threats in the Security Command Center. If **NO**, view violations will appear in the Top Violations dashboard.
- f. **Select Violation Entity:** Select from dropdown.

- **Users:** Returns list of users violating policy. Uncorrelated accounts will be ignored.
- **Activity Account:** Returns list of activity accounts (both correlated and uncorrelated) violating the policy.
- **Network Addresses:** Returns list of network addresses violating policy.
- **Resources:** Returns list of resources violating policy.



Note: Resources refers to assets on the network imported as [Entity Metadata](#).

- **Resource Group Account:** Returns list of activity accounts (correlated and uncorrelated) violating the policy across data sources.



Note: Resource Group refers to all the data sources imported for a **Device Type**. For example, the Resource Group **Blue Coat Proxy** could include the data sources BlueCoat1, BlueCoat2, and BlueCoatLandspeed. For this entity type, select the Resource Group from the **Functionality** dropdown in the next step.

- g. **Do you want to run the policy on a:** Select one:
 - Datasource:** Select a specific datasource from the dropdown. Example: BlueCoat1.
 - Functionality:** Select a functionality or resource group to run policy on all available data sources that perform a specific function. Example: Web Proxy or Blue Coat Proxy.

Additional Details

ADDITIONAL DETAILS

Owner

Select the owner of the policy. This can be used for sending notifications and case management. The category widget on the security dashboard is visible to policy owners.

Remediator

Select the remediator for the policy. The remediator can be sent notifications and used in case management.

- a. **Owner:** Click search icon to select an owner for the policy. This can be used to send notifications and manage cases.

Add/Change Owner

*
username

	User Name	First Name	Last Name	E-Mail	Enabled?
<input type="radio"/>	1001	HARRY	OGWA	HARRY.OGWA@scnx.com	true
<input type="radio"/>	1005	TERRY	MERRITT	TERRY.MERRITT@scnx.com	true
<input type="radio"/>	1012	JOE	KELLINGTON	JOE.KELLINGTON@scnx.com	true
<input type="radio"/>	1013	ROBERT	WELLINGTON	ROBERT.WELLINGTON@scnx.com	true
<input type="radio"/>	1025	Ted	Thomson	ted.thomson@scnx.com	true
<input type="radio"/>	1044	NORA	LEWIS	NORA.LEWIS@scnx.com	true
<input type="radio"/>	1045	FAHAD	WALKER	FAHAD.WALKER@scnx.com	true
<input type="radio"/>	1063	Meredith	COLEMAN	Meredith.COLEMAN@scnx.com	true
<input type="radio"/>	1064	Cedric	Castaneda	Cedric.Castaneda@scnx.com	true
<input type="radio"/>	1065	Ainsley	Moses	Ainsley.Moses@scnx.com	true

Add Selected Owner

- b. **Remediator:** Click search icon to select a remediator for the policy. This can be used to send notifications and manage cases.

Define Risk and Threat

Complete the following information:

DEFINE RISK AND THREAT

Category*

Create New Policy Category

None
+
-

Category is displayed on dashboard as a widget and risk will be aggregated for policies with the same category. All violations of the same category will be available in the widget.

Threat Indicator*

Create New Threat Indicator

Edit Killchain Stage and Response Actions

-Select-

Violations detected are indicative of threat

a. **Category:**

a. Select from dropdown.

OR

b. **Create New Policy Category.**

Create New Policy Category

Category

Save

c. Click +/- to add/remove categories.

b. **Threat Indicator:**

- a. Select from dropdown.
- OR
- b. **Create New Threat Indicator.**

The screenshot shows a 'Create New Threat Indicator' window. It includes a text input for the name, a category dropdown menu with a search bar, and a list of stages: Recon Stage, Delivery Stage, Exploit Stage, Execute Stage, and Exfiltration Stage. The 'Recon Stage' is highlighted. Below the stages is a section for selecting associated playbooks, and a 'Save' button is at the bottom right.

- a. **Threat Indicator Name:** Enter a descriptive name for the threat indicator.
- b. **Category:** Select a threat kill chain stage from the dropdown:
 - **Recon Stage:** Stage in which attackers gathers information before an attack in an attempt to find a vulnerable point in the network. Example: Phishing emails.
 - **Delivery Stage:** Stage in which attackers deliver a malicious package to gain access to a network. Example: User clicks a link within a phishing email and downloads malware from the malicious site.
 - **Exploit Stage:** Stage in which attackers find a vulnerable point of entry into the network and gain access. Example: Zero-day attack.
 - **Execute Stage:** Stage in which attackers escalate access to execute the attack using admin privileges. Example: Escalating privileges or stealing admin credentials, lateral movement.
 - **Exfiltration Stage:** Stage in which the attackers can move freely around the network and access or remove any sensitive data at will. Example: An insider uploading customer information to a personal file sharing/storage site.

Each stage represents a step in the threat kill chain. To view violations by threat stage on the Kill Chain Analysis, navigate to **Menu > Security Center > Security Command Center**. See [Security Command Center](#) for more information.

<

- c. **Threat Response Playbook:** Enter the steps to take to remediate this threat. Use HTML to control the way the steps are displayed on the Violation Summary screen. Example:

<0|>

Review the Account Name and Domain Name fields, that identify the user who cleared the log

Additional fields of interest: Security ID, Logon ID, Subject

- Login ID allows you to correlate backwards to the logon events as well as with other events logged during the same logon session

[Submit a ticket to investigate](supportticketsite.com)

Threat Response Playbook

```
<ol>  
<li>Review the Account Name and Domain Name fields, that identify the  
user who cleared the log</li>  
<li>Additional fields of interest: Security ID, Logon ID, Subject</li>  
<li>Login ID allows you to correlate backwards to the logon events as well  
as with other events logged during the same logon session</li>  
<li><a href="supportticketsite.com">Submit a ticket to investigate</a></li>  
</ol>
```

The Remediation Steps will appear on the Violation Summary screen:

VIOLATION SUMMARY		VIOLATION EVENTS	REMEDIATION STEPS
1	Check the initial level privileges		
2	Contact ITOps Administrator to get more insight into his privileges		
3	Submit a ticket to investigate further		

- d. **Select to Associate Playbooks:** Select the play books to associate with the threat indicator. Example: VirusTotal ScanIP.

For information about how playbooks work in ArcSight UBA, see [Automated Response](#).

Edit Threat Indicator

Select To Associate Playbooks

<input type="checkbox"/>	SNYPR SendAlertCEF Send violation alerts as CEF	<input type="radio"/> NO AUTO PLAY
<input checked="" type="checkbox"/>	VirusTotal ScanIP VirusTotal ScanIP and fetch results	<input type="radio"/> NO AUTO PLAY
<input checked="" type="checkbox"/>	VirusTotal ScanURL VirusTotal ScanURL and fetch results	<input type="radio"/> NO AUTO PLAY
<input checked="" type="checkbox"/>	VirusTotal ScanDomain VirusTotal ScanDomain and fetch results	<input type="radio"/> NO AUTO PLAY
<input checked="" type="checkbox"/>	VirusTotal ScanFile VirusTotal ScanFile and fetch results	<input type="radio"/> NO AUTO PLAY
<input checked="" type="checkbox"/>	Nessus LaunchScan Launch a Nessus Scan	<input type="radio"/> NO AUTO PLAY

Save



Note: You may select multiple playbooks for the threat indicator.

- e. Enable Auto Play to automatically launch play book tasks upon violation.

If Auto Play is disabled, you can launch play book tasks manually from the violation summary screen when an incident occurs.

For information about how playbooks work in ArcSight UBA, see [Automated Response](#).

Edit Threat Indicator

Select To Associate Playbooks

<input type="checkbox"/>	SNYPR SendAlertCEF Send violation alerts as CEF	<div><div>NO</div><div>AUTO PLAY</div></div>
<input checked="" type="checkbox"/>	VirusTotal ScanIP VirusTotal ScanIP and fetch results	<div><div>YES</div><div>AUTO PLAY</div></div>
<input checked="" type="checkbox"/>	VirusTotal ScanURL VirusTotal ScanURL and fetch results	<div><div>NO</div><div>AUTO PLAY</div></div>
<input checked="" type="checkbox"/>	VirusTotal ScanDomain VirusTotal ScanDomain and fetch results	<div><div>NO</div><div>AUTO PLAY</div></div>
<input checked="" type="checkbox"/>	VirusTotal ScanFile VirusTotal ScanFile and fetch results	<div><div>YES</div><div>AUTO PLAY</div></div>
<input checked="" type="checkbox"/>	Nessus LaunchScan Launch a Nessus Scan	<div><div>NO</div><div>AUTO PLAY</div></div>

Save

- c. **Edit Killchain Stage and Response Actions:** Click to edit the details described above.

Click **Save & Next** to proceed to [Provide Conditions](#).

Provide Conditions

In this section, set the rules for the policy to enable its functions. Select the analytical technique, create groups of rules to determine what the policy will check against the data, configure analytical checks to add additional data processing, and select risk boosters to increase or decrease the risk score of violators based on specified conditions.

What do you want to detect?

ArcSight UBA provides purpose-built analytics techniques to detect threats and risk rank events. Select one of the following analytical techniques:

- **Rare behavior:** Detects rare events compared to past behavior. Example : An account uses an IP address never used before.
- **Spike in number of occurrences:** Detects unusual spike in number of events from established baselines in a particular time window for the user or across all users. Example: If user does 'x' number of logon failures within a day (which is never happened in past).
- **Spike in Volume/Amount:** Detects unusual spike in volume/amount of data from establishing baselines in a particular time window for the user or across all users. Example: If user uploads 'x' volume of data to personal storage site within a day (which never happened in the past).
- **Enumeration Behavior:** Detects behavior of an event attribute distinct from established baselines in a particular time window for the user or across all users. Example: If user transfer 'x' amount of file size within a day (which is never happened in past).
- **Abnormal activity compared to peers:** Detects unusual spike in amounts found within some activity attribute compared to user, peer group or user population. Example: If user modifies files from other department and this activity has never been done by other peer members.

- **Individual Event Analytics:** Checks for specified conditions and additional analytics for a single event. Example: If user from 'x' country login to 'y' server and modify 'z' file.
- **Aggregated Event Analytics:** Runs additional analytics on aggregated events passed from Filter Conditions and Additional Event Analytics. Example: If user logon successful after 'x' number of logon failure with different IP addresses.
- **Land Speed Detection:** Flags activity accounts performing successful login attempts from different geographic locations within unusual or impossible periods of time. Example: If user logs on to 'x' server multiple times from multiple countries within short period of time.
- **Traffic Analyzer:** Uses ArcSight UBA Traffic Analyzer performs specific checks against proxy traffic to detect rare domains, user agents, and algorithmically generated domains, as well as patterns of malicious or robotic behavior.
- **Phishing:** Detects emails purporting to be from reputable companies in order to induce individuals to reveal personal information.
- **Batched Analytics:** Allows you to use Spotter or HDFS search terms to configure rules for a policy.

Rare Behavior

Select rare behavior to detect activities or IP addresses and accounts that have not been observed before. For example, first use of a transaction by an account.

Choose the Features for Generating Behavior

Click to choose one or more features to generate a behavior profile. Behavior profiles are generated on a combination of the selected features. For more information about how behavior profiles work, see [Behavior Profiles](#).



Note: Features are available based on the attributes mapped for the data source or data source type selected in the previous step.

WHAT DO YOU WANT TO DETECT ?

i Rare Behavior : Detects rare events compared to past behavior. Example : If an account uses ip address which

RARE BEHAVIOR
SPIKE IN NUMBER OF OCCURRENCES
SPIKE IN VOLUME/AMOUNT
ENUMERATION BEHAVIOR

BATCHED ANALYTICS

CHOOSE THE FEATURES FOR GENERATING BEHAVIOR

☒ destinationhostnamecountry
☒ Filetype
☒ Method
☒ sourcehostnamelongitude
☒ Process_Name
☒ resourcehostnamepostalcode
☒ sessionid
☒ eventlatitude
☒ Response_Code
☒ Referer
☒ destinationhostnamepostalcode
☒ resourcehostnamecountry
☒ destinationhostnameecity

Select the attributes from above panel
Selected features

Behavior Information:

Provide a unique name for the behavior profile.

What should get flagged as violations?

1.

1. Select an option for **Number of occurrences of selected features is unusually higher than behavior baseline for:**

Examples:

- First use of IPAddress by Account
- First use of Transaction by Account
- First use of IPAddress on Resource (Flag Account)
- First use of Transaction on Resource (Flag Account)

- First use of Account on Resource
2. Use slider to specify a value for **Flag as Violations when Rarity Crosses Sigma Threshold Value**. Example: 0.85 Highly Rare.



Note: Sigma (standard deviation) threshold is calculated using inputs such as deviation from baseline, cluster confidence, number of valid and invalid clusters, and baseline value.

Spike in Number of Occurrences

Select Spike in Number of Occurrences to detects unusual spikes in the number of events from established baselines for a user or across all users. For example, transaction occurrence abnormally higher than peer's daily behavior.

Choose the Features for Generating Behavior

WHAT DO YOU WANT TO DETECT ?

Spike in number of occurrences : Detects spike in number of events in particular time window. Example : If

RARE BEHAVIOR

SPIKE IN NUMBER OF OCCURRENCES

SPIKE IN VOLUME/AMOUNT

ENUMERATION B

BATCHED ANALYTICS

CHOOSE THE FEATURES FOR GENERATING BEHAVIOR

☒ destinationhostnamecountry
 ☒ Filetype
 ☒ Method
 ☒ sourcehostnamelongitude
 ☒ Process_Name
 ☒ resourcehostnamepostalcode
 ☒ sessionid
 ☒ eventlatitude
 ☒ Response_Code
 ☒ Referer
 ☒ destinationhostnamepostalcode
 ☒ resourcehostnamecountry
 ☒ destinationhostnamecity

Select the attributes from above panel

sourcehostnamelongitude
 Process_Name
 eventlatitude
 destinationhostnamepostalcode
 Referer
 Response_Code
 Method
 Filetype

Selected features

Choose one or more features to generate a behavior profile. Behavior profiles are generated on a combination of the selected features. For more information about how behavior profiles work, see [Behavior Profiles](#).



Note: Features are available based on the attributes mapped for the data source selected in the previous step.

Behavior Information

BEHAVIOR INFORMATION

Behavior Name

Provide unique name for this behavior

Choose Time Window

☐ Hourly
☐ Daily
☐ Weekly
☐ Monthly
☐ Day of Week

Behavior will be generated according to time window selected

1. Provide a unique **Behavior Name**.
2. **Choose Time Window** for which to generate the behavior.

What should get flagged as violations?

WHAT SHOULD GET FLAGGED AS VIOLATIONS ?

Number of occurrences of selected features is unusually higher than behavior baseline for :

☐ Self
☐ Other Accounts
☐ Peer Groups

Choose the Analytical Technique to run

-Select-

Flag as Violations when Rarity crosses Sigma Threshold Value

Slight Deviation

High Deviation

0.85

1. Select an option for **Number of occurrences of selected features is unusually higher than behavior baseline for:**
 - Self
 - Other Accounts
 - Peer Groups
2. **Choose the Analytical Technique to run** from the dropdown. Example: Transaction Occurrence Abnormally higher than User's Weekly Behavior.
3. Use slider to specify a value for **Flag as Violations when Rarity Crosses Sigma Threshold Value**. Example: 0.85 Highly Rare.



Note: Sigma (standard deviation) threshold is calculated using inputs such as deviation from baseline, cluster confidence, number of valid and invalid clusters, and baseline value.

Spike in Volume/Amount

Select Spike in Volume/Amount to detects unusual spikes in the volume of data from established baselines for a user or across all users. For example, volume of data downloaded abnormally higher than peer's daily behavior.

Choose the Features for Generating Behavior

WHAT DO YOU WANT TO DETECT ?

i Spike in Volume/Amount : Detects spike in amount of event attribute in particular time window. Example :

RARE BEHAVIOR
SPIKE IN NUMBER OF OCCURRENCES
SPIKE IN VOLUME/AMOUNT
ENUMERATION B

BATCHED ANALYTICS

CHOOSE THE FEATURES FOR GENERATING BEHAVIOR

☒ destinationhostnamecountry
☒ Filetype
☒ Method
☒ sourcehostnamelongitude
☒ Process_Name
☒ resourcehostnamepostalcode
☒ sessionid
☒ eventlatitude
☒ Response_Code
☒ Referer
☒ destinationhostnamepostalcode
☒ resourcehostnamecountry
☒ destinationhostnameecity
☒ destinationhostname...

sourcehostnamelongitude
Process_Name
eventlatitude
destinationhostnamepostalcode
Referer
Response_Code
Method
Filetype

Select the attributes from above panel
Selected features

Choose one or more features to generate a behavior profile. Behavior profiles are generated on a combination of the selected features. For more information about how behavior profiles work, see [Behavior Profiles](#).



Note: Features are available based on the attributes mapped for the data source selected in the previous step.

Behavior Information

BEHAVIOR INFORMATION

Behavior Name

Provide unique name for this behavior

Choose Time Window

☐ Hourly
☐ Daily
☐ Weekly
☐ Monthly
☐ Day of Week

Behavior will be generated according to time window selected

1. Provide a unique **Behavior Name**.
2. **Choose Time Window** for which to generate the behavior.

What should get flagged as violations?

WHAT SHOULD GET FLAGGED AS VIOLATIONS ?

Number of occurrences of selected features is unusually higher than behavior baseline for :

☐ Self
☐ Other Accounts
☐ Peer Groups

Choose the Analytical Technique to run

-Select-

Flag as Violations when Rarity crosses Sigma Threshold Value

Slight Deviation

High Deviation

0.85

1. Select an option for **Number of occurrences of selected features is unusually higher than behavior baseline for:**
 - Self
 - Other Accounts
 - Peer Groups
2. **Choose the Analytical Technique to run** from the dropdown. Example: Transaction Occurrence Abnormally higher than User's Weekly Behavior.
3. Use slider to specify a value for **Flag as Violations when Rarity Crosses Sigma Threshold Value**. Example: 0.85 Highly Rare.



Note: Sigma (standard deviation) threshold is calculated using inputs such as deviation from baseline, cluster confidence, number of valid and invalid clusters, and baseline value.

Enumeration Behavior

Select Enumeration Behavior to detect behavior of an event attribute distinct from established baselines in a particular time window for the user or across all users. Example: Filetype never seen before.

Choose the Features for Generating Behavior

WHAT DO YOU WANT TO DETECT ?

Enumeration Behavior : Detects distinct behavior of event attribute in particular time window.

RARE BEHAVIOR

SPIKE IN NUMBER OF OCCURRENCES

SPIKE IN VOLUME/AMOUNT

ENUMERATION BEHAVIOR

BATCHED ANALYTICS

CHOOSE THE FEATURES FOR GENERATING BEHAVIOR

☒ destinationhostnamecountry

☒ Filetype

☒ Method

☒ sourcehostnamelongitude

☒ Process_Name

☒ resourcehostnamepostalcode

☒ sessionid

☒ eventlatitude

☒ Response_Code

☒ Referer

☒ destinationhostnamepostalcode

☒ resourcehostnamecountry

☒ destinationhostnamecity

sourcehostnamelongitude

Process_Name

eventlatitude

destinationhostnamepostalcode

Referer

Response_Code

Method

Filetype

Select the attributes from above panel

Selected features

Select the event attribute for which to generate a behavior for distinct values of this attribute

destinationhostnamecountry

1. Choose one or more features to generate a behavior profile. Behavior profiles are generated on a combination of the selected features. For more information about how behavior profiles work, see [Behavior Profiles](#).
2. **Select the event attribute for which to generate a behavior for distinct values of this attribute** from dropdown. Example: Filetype.



Note: Features are available based on the attributes mapped for the data source selected in the previous step.

Behavior Information

The screenshot shows a form titled "BEHAVIOR INFORMATION". It contains a "Behavior Name" label above a text input field. Below the input field is the instruction "Provide unique name for this behavior". Underneath is a "Choose Time Window" section with five radio button options: "Hourly", "Daily", "Weekly", "Monthly", and "Day of Week". At the bottom of this section is the text "Behavior will be generated according to time window selected".

1. Provide a unique **Behavior Name**.
2. **Choose Time Window** for which to generate the behavior.

What should get flagged as violations?

The screenshot shows a form titled "WHAT SHOULD GET FLAGGED AS VIOLATIONS ?". It contains a section "Number of occurrences of selected features is unusually higher than behavior baseline for :" with three radio button options: "Self", "Other Accounts", and "Peer Groups". Below this is a "Choose the Analytical Technique to run" section with a dropdown menu currently showing "-Select-". At the bottom is a "Flag as Violations when Rarity crosses Sigma Threshold Value" section. It features a horizontal slider with a green bar on the left and a grey bar on the right. The green bar is labeled "Slight Deviation" and the grey bar is labeled "High Deviation". A circular slider knob is positioned on the green bar. To the right of the slider is a text box containing the value "0.85".

1. Select an option for **Number of occurrences of selected features is unusually higher than behavior baseline for:**
 - Self
 - Other Accounts
 - Peer Groups
2. **Choose the Analytical Technique to run** from the dropdown. Example: Abnormally higher amount than Peer's Daily Behavior.
3. Use slider to specify a value for **Flag as Violations when Rarity Crosses Sigma Threshold Value**. Example: 0.85 Highly Rare.



Note: Sigma (standard deviation) threshold is calculated using inputs such as deviation from baseline, cluster confidence, number of valid and invalid clusters, and baseline value.

Abnormal Activity Compared to Peers

Select Abnormal Activity Compared to Peers to detect unusual spike in amounts found within some activity attribute compared to user, peer group or user population. For example, transactions performed by user not seen for other members of peer group.

Choose the Features for Generating Behavior

WHAT DO YOU WANT TO DETECT ?

1 Abnormal Activity Compared to Peers : Detects activity which is never performed by other peer members. Example : If user modifies files from other department and

RARE BEHAVIOR
SPIKE IN NUMBER OF OCCURRENCES
SPIKE IN VOLUME/AMOUNT
ENUMERATION BEHAVIOR
ABNORMAL ACTIVITY COMPARED TO PEERS
BATCHED ANALYTICS

CHOOSE THE FEATURES FOR GENERATING BEHAVIOR

☒ destinationhostnameecountry
☒ Filetype
☒ Method
☒ sourcehostnamelongitude
☒ Process_Name
☒ resourcehostnamepostalcode
☒ sessionid
☒ eventlatitude
☒ Response_Code
☒ Referer
☒ destinationhostnamepostalcode
☒ resourcehostnameecountry
☒ destinationhostnameecity

sourcehostnamelongitude
Process_Name
eventlatitude
destinationhostnamepostalcode
Referer
Response_Code
Method
Filetype

Select the attributes from above panel
Selected features

Choose one or more features to generate a behavior profile. Behavior profiles are generated on a combination of the selected features. For more information about how behavior profiles work, see [Behavior Profiles](#).



Note: Features are available based on the attributes mapped for the data source selected in the previous step.

Behavior Information

BEHAVIOR INFORMATION

Behavior Name

Provide unique name for this behavior

Provide a unique name for the behavior profile.

What should get flagged as violations?

□

1. Click to select attributes from panel for **Number of occurrences of selected features is unusually higher than behavior baseline for:** Example: Department.
2. Use slider to specify a value for **Flag as Violations when Rarity Crosses Sigma Threshold Value.** Example: 0.85 Highly Rare.



Note: Sigma (standard deviation) threshold is calculated using inputs such as deviation from baseline, cluster confidence, number of valid and invalid clusters, and baseline value.

Individual Event Analytics

Select Individual Event Analytics to checks single events against specified conditions and additional analytics:

- [Criteria to Filter Events](#)
- [Additional Event Analytics](#)
- [Risk Boosters](#)

WHAT DO YOU WANT TO DETECT ?

Individual Event Analytics : Detects activities with specified criteria. Example : If user from 'x' country login to 'y' server and modify 'z' file.

RARE BEHAVIOR
SPIKE IN NUMBER OF OCCURRENCES
SPIKE IN VOLUME/AMOUNT
ENUMERATION BEHAVIOR
ABNORMAL ACTIVITY COMPARED TO PEERS
INDIVIDUAL EVENT ANALYTICS

BATCHED ANALYTICS

Aggregated Event Analytics

Select Aggregated Event Analytics to runs additional analytics on multiple aggregated events passed from Filter Conditions and Additional Event Analytics. Aggregated Event Analytics use Directives to specify single or multiple events that result in a violation. Directives allow you to specify the count and duration of the events that are to be flagged as violations. For example, four failed transactions with a credit card followed by a successful transaction within one hour.

WHAT DO YOU WANT TO DETECT ?

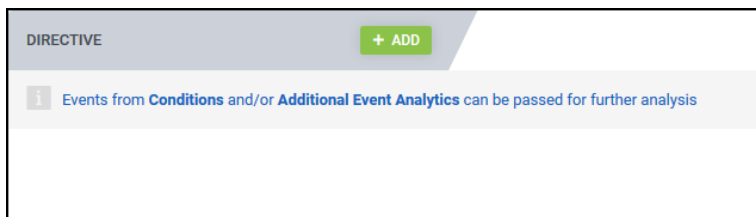
Aggregated Event Analytics : Detects bunch of activities with specific sequence. Example : If user logon succesful after 'x' number of logon failure with different ip addresses.

RARE BEHAVIOR
SPIKE IN NUMBER OF OCCURRENCES
SPIKE IN VOLUME/AMOUNT
ENUMERATION BEHAVIOR
ABNORMAL ACTIVITY COMPARED TO PEERS
INDIVIDUAL EVENT ANALYTICS
AGGREGATED EVENT ANALYTICS

BATCHED ANALYTICS

To use Directives in aggregated events, complete the following steps:

1. Click **Aggregated Event Analytics**.
2. Click **Add** under Directive.



3. Click **Configure**.



Note: The Details window will appear.

4. Enter directive Details. See [Example Directive: Three failed transactions with a credit card followed by a successful transaction within one hour](#) for details.
5. Click **+ Child** to add child directives.

Example Directive: Three failed transactions with a credit card followed by a successful transaction within one hour

1. Configure details for the parent directive **Failed Transactions** as follows:



Note: For this example, CustomString 2 is the attribute that was mapped to Credit Card Issuer Response Code during [Activity Data](#) for the datasource. The Values for this attribute are set by the datasource. Examples: 14=Invalid Card Number. 5=Do Not Honor.

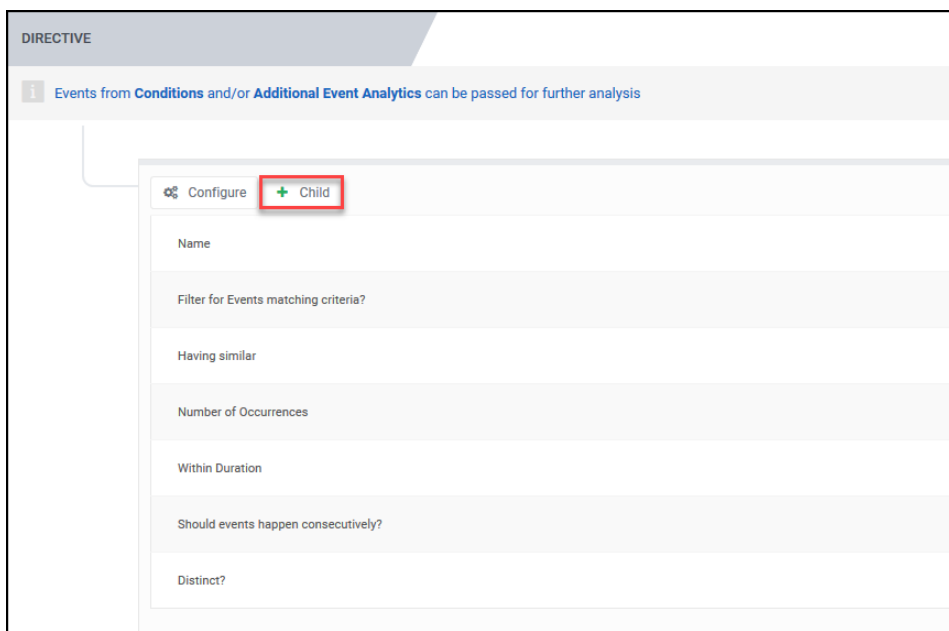
The screenshot shows the 'Details' configuration window for the 'Failed Transactions' directive. The settings are as follows:

- Name:** Failed Transactions
- Filter for Events matching criteria?:** YES (toggle). Below it, a table shows two conditions:

Attribute	Condition	Value	AND
CustomString 2	Equal To	14	AND
CustomString 2	Equal To	5	AND
- Filter for Amount matching criteria?:** NO (toggle).
- Having similar:** Account Name (dropdown).
- Number of Occurrences:** At least 3 (dropdown). Within Duration: 01:00:00 (text input). A 'Choose Duration' panel is open on the right, showing sliders for Hour, Minute, and Second, with the total duration set to 01:00:00.
- Should events happen consecutively?:** NO (toggle).
- Distinct?:** NO (toggle).
- Buttons:** Save (blue), Done (grey).

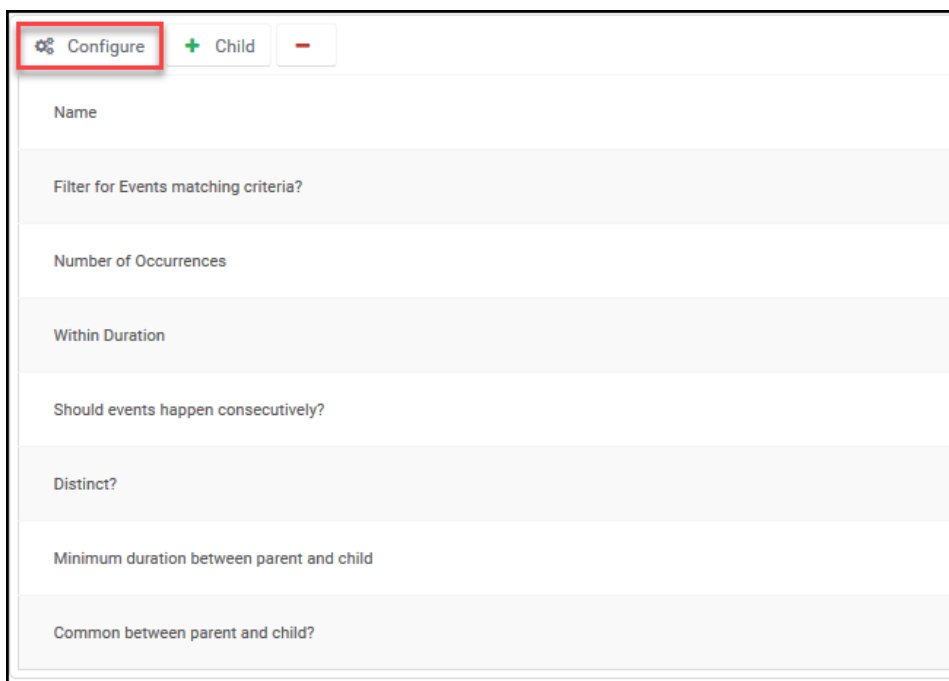
- Name:** Provide the unique name Failed Transactions.
- Filter for Events matching criteria?:**
 - Toggle to **Yes** to provide conditions.
 - Select the attribute from dropdown. Example: CustomString2.
 - Select condition from dropdown. Example: Equal To.
 - Enter value for attribute. Example: 14.
 - Use **+/-** to add/remove conditions. Example: CustomString2 Equal To 14 + CustomString2 Equal to 5.
- Filter for Amount matching criteria?:** Enable this option if you want to filter for amount matching criteria, select the attribute, and provide the value.
- Having Similar:** Select an attribute from dropdown. Example: Account Name.
- Number of Occurrences:** Select the rate at which an event is repeated over a period of time. Example: At least 3.
 - Within Duration:** Select a duration using sliders. Example: 01:00:00 Hour.
- Should events happen consecutively?:** Toggle to **Yes** if events must occur consecutively to flag the violation.
- Distinct?:** Toggle to **Yes** to select a distinct attribute to apply to the condition.

2. Click **Save**.
3. Click **+ Child** to create the child directive Successful Transaction.



The screenshot shows the 'DIRECTIVE' configuration page. At the top, there is a header 'DIRECTIVE' and a message: 'Events from Conditions and/or Additional Event Analytics can be passed for further analysis'. Below this, there is a 'Configure' button with a gear icon and a '+ Child' button with a plus icon. The '+ Child' button is highlighted with a red box. Below the buttons, there are several input fields: 'Name', 'Filter for Events matching criteria?', 'Having similar', 'Number of Occurrences', 'Within Duration', 'Should events happen consecutively?', and 'Distinct?'.

4. Click **Configure** to edit the details of the newly created child directive.



The screenshot shows the 'DIRECTIVE' configuration page. At the top, there is a header 'DIRECTIVE' and a message: 'Events from Conditions and/or Additional Event Analytics can be passed for further analysis'. Below this, there is a 'Configure' button with a gear icon and a '+ Child' button with a plus icon. The 'Configure' button is highlighted with a red box. Below the buttons, there are several input fields: 'Name', 'Filter for Events matching criteria?', 'Number of Occurrences', 'Within Duration', 'Should events happen consecutively?', 'Distinct?', 'Minimum duration between parent and child', and 'Common between parent and child?'.

5. Configure details of the child directive as follows:



Note: For this example, CustomString 2 is the attribute that was mapped to Credit Card Issuer Response Code during [Activity Data](#) for the datasource. The Values for this attribute are set by the datasource. Example: 00=Approved.

- a. **Name:** Provide the unique name Successful Transaction.
 - b. **Filter for Events matching criteria?:**
 - a. Toggle to **Yes** to provide conditions.
 - b. Select the attribute from dropdown. Example: CustomString2.
 - c. Select condition from dropdown. Example: Equal To.
 - d. Enter value for attribute. Example: 00.
 - e. Use **+/-** to add/remove conditions.
 - c. **Filter for Amount matching criteria?:** Enable this option if you want to filter for amount matching criteria, select the attribute, and provide the value.
 - d. **Number of Occurrences:** Select the rate at which an event is repeated over a period of time. Example: At least 3.
 - a. **Within Duration:** Select a duration using sliders. Example: 01:00:00 Hour.
 - e. **Should events happen consecutively?:** Toggle to **Yes** if events must occur consecutively to flag the violation.
 - f. **Minimum duration between parent and child:** Select a duration using sliders. Example: 01:00:00 Hour.
 - g. **Common between parent and child?:** Select an attribute from dropdown. Example: Account Name.
 - h. **Distinct?:** Toggle to **Yes** to select a distinct attribute to apply to the condition.
6. Click **Save**.

The overall configuration will appear similar to the following:

Configure + Child	
Name	Failed Transactions
Filter for Events matching criteria?	customstring2(CONDITION_EQUALS)14.AND.customnumber2(CONDITION_EQUALS)5
Having similar	accountname
Number of Occurrences	3
Within Duration	01:00:00
Should events happen consecutively?	false
Distinct?	NA

Configure + Child -	
Name	Successful Transactions
Filter for Events matching criteria?	customstring2(CONDITION_EQUALS)00
Number of Occurrences	1
Within Duration	01:00:00
Should events happen consecutively?	false
Distinct?	NA
Minimum duration between parent and child	01:00:00
Common between parent and child?	accountname

Land Speed Detection

Land Speed Detection is an aggregated event analytical check that uses geolocation data and advanced analytics to compute land speed to flag accounts performing activity from different geographic locations within unusual or impossible periods of time. See [Example Real Time Policy: Check Land Speed](#) for more information about how ArcSight UBA uses analytical check to detect compromised accounts.



Note: To use this analytical check, you must first import geolocation data from MaxMind and enable geolocation attributes for the selected datasource during [Activity Data](#) Step: 3 Perform Conditional Actions.

To detect land speed violations, complete the following steps:

1. Click **Land Speed Detection**.

WHAT DO YOU WANT TO DETECT ?

1 Land Speed Detection : Detects bunch of activities with different geographical location within specific time range. Example : If user logon to 'x' server multiple times from multiple countries within short period of time.

RARE BEHAVIOR SPIKE IN NUMBER OF OCCURRENCES SPIKE IN VOLUME/AMOUNT ENUMERATION BEHAVIOR ABNORMAL ACTIVITY COMPARED TO PEERS INDIVIDUAL EVENT ANALYTICS AGGREGATED EVENT ANALYTICS **LAND SPEED DETECTION**

BATCHED ANALYTICS

2. Configure the following to specify the total distance or maximum speed after which to flag violations on similar attributes:

LAND SPEED DETECTION

1 Events from **Conditions** and/or **Additional Event Analytics** can be passed for further analysis

Flag as Violation if Greater Than Value (Miles) IP Address Attribute Having similar

MAX_SPEED 60 ipaddress Account Name

- Flag as Violation if:** Select Total_Distance or Max_Speed from dropdown.
- Greater than Value (Miles):** Enter a value in miles. Example: 60.0.
- IP Address Attribute:** Select an attribute from the drop down. Example: ipaddress.
- Having similar:** Select an attribute from the drop down. Example: Account Name.

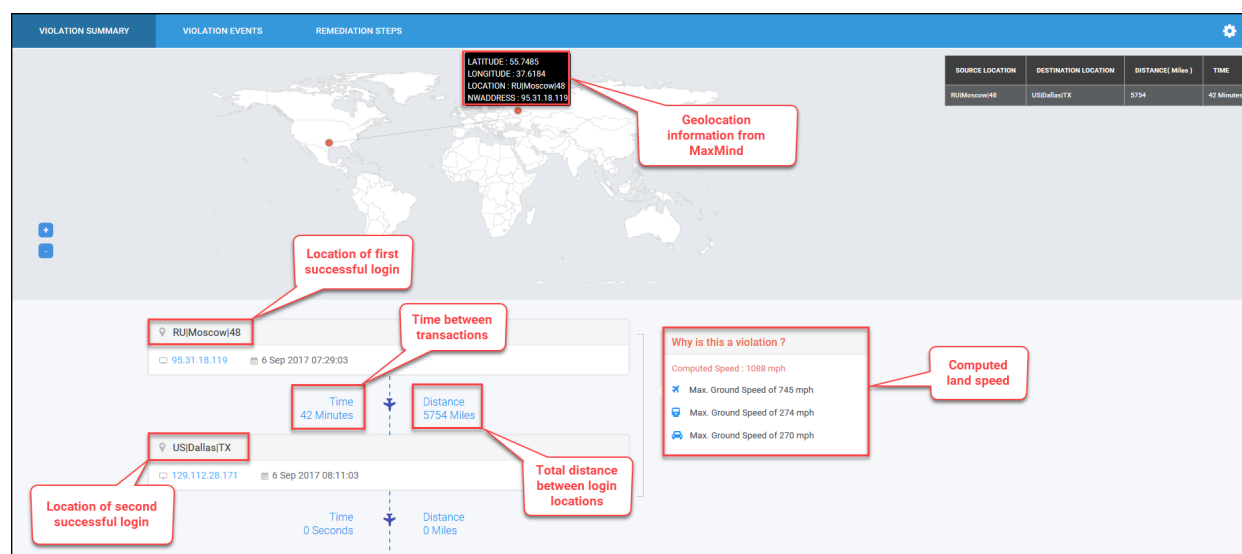
Example

To detect land speed violations for account performing successful account login transactions from different geolocations within an unusual period of time, use the following conditions:

Condition: Attribute: TransactionString1 | **Condition:** Contains | **Value:** Authentication: successful

Land Speed Violation: Flag as Violation if: MAX_SPEED | **Greater than Value (Miles):** 60.0 | **Having similar:** Account Name.

Resulting violations will appear as follows:



Traffic Analyzer

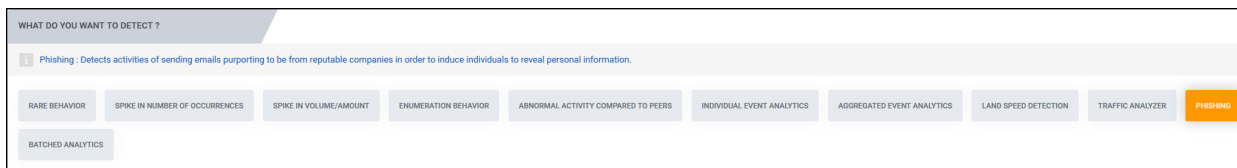
The following traffic analyzer checks are part of the ArcSight UBA Traffic Analyzer:

- **URL Visited by Visitors**
- **Useragent Visited by Visitors**
- **Ports used on URL**
- **Protocols user on URL**
- **Randomly Generated URL**
- **Beaconing**

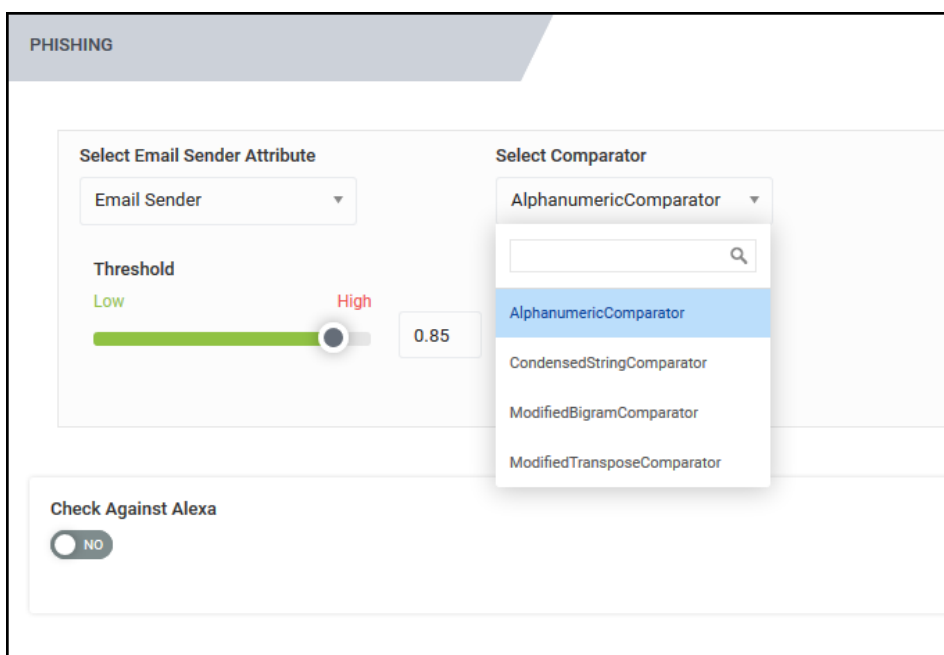
See [Traffic Analyzer](#) for details about these checks and examples of specific configurations.


Phishing

Phishing detection checks email senders against comparators to detect emails purporting to be from reputable companies in order induce individuals to reveal personal information. Email senders can also be checked against Alexa's 1 Million Safe Domains to eliminate safe senders from the check. To detect phishing emails, complete the following steps:

1. Click **Phishing**.

2. Configure the following to specify email sender attribute and comparator against which to check the attribute:



- **Select Email Sender Attribute:** Select from dropdown. Example: Email Sender.
 - **Select Comparator:** Select from dropdown. Example: Alphanumeric Comparator.
 - **Threshold:** Use slider to specify a threshold of match between the email sender attribute and the comparator after which to flag the violation.
-  **Note:** Sigma (standard deviation) threshold is calculated using inputs such as deviation from baseline, cluster confidence, number of valid and invalid clusters, and baseline value.
- **Check Against Alexa:** Enable slider to YES to check email sender against Alexa's 1M Safe Domains.

Batched Analytics

Select Batched Analytics to use Spotter or HDFS search terms to configure rules for a policy.

Spotter

Spotter Query allows you to use Spotter search terms to configure rules for a policy. To use Spotter Query, complete the following steps:

1. Click **Spotter**.



Note: Query replaces **Filter Conditions**.

2. Enter a search **Query**. Example: `resourcegroupname = "GoogleDriveLogs"` and `userriskscore = "0.10"`

3. Enable **Do you want to query on violation data?** to include the policy on the Spotter Summary screen as in the following image:

AVAILABLE VIOLATIONS	TOTAL VIOLATED EVENTS: 23.64K
Excessive number of emails to personal email address-42	20,180
Potential beaconing activity	2,368
Excessive number of emails to personal email address	468
Possible Flight Risk Users-28	179
Spam Email	92
Possible Flight Risk User	87
Spike in high number of bytes out	77
Potential Data Snooping Activity	77
Flight Risk User watchlist	29
Communication to malicious website	23
Critical File Exfiltrated via USB	16

AVAILABLE DATASOURCES	TOTAL EVENTS: 45.94M
Microsoft Windows Event	14,710,349
Infoblox	7,537,171
Google	6,854,092
Unix OS	6,850,826
Digital Guardian Send Mail	2,526,746
Sophos Endpoint Protection	1,974,761
CitrixVPN	1,270,422
PaloAlto	1,045,784
Digital Guardian USB	670,005
Google_Login	29,971
Bro DHCP	29,708

HDFS

Select **HDFS** to check historical data stored in HDFS to find violations for the specified rule.

WHAT DO YOU WANT TO DETECT ?

1 HDFS : Detects activities which are returned by HDFS query.

RARE BEHAVIOR SPIKE IN NUMBER OF OCCURRENCES SPIKE IN VOLUME/AMOUNT ENUMERATION BEHAVIOR ABNORMAL ACTIVITY COMPARED TO PEERS INDIVIDUAL EVENT ANALYTICS AGGREGATED EVENT ANALYTICS LAND SPEED DETECTION TRAFFIC ANALYZER PHISHING

HDFS

1. Click **HDFS**.
2. Enter a **Query** using 'where' clauses as the condition. Example: `where employeeid='xyz'`

CRITERIA TO FILTER EVENTS

1 Conditions contains either set of rules or set of subgroups.Set of Groups and Rules will decide which data will be marked as violation.

Query*

Enter HDFS Query to catch violations. Note : - Please enter only 'where' clause, that is condition part.
e.g : where employeeid='xyz'

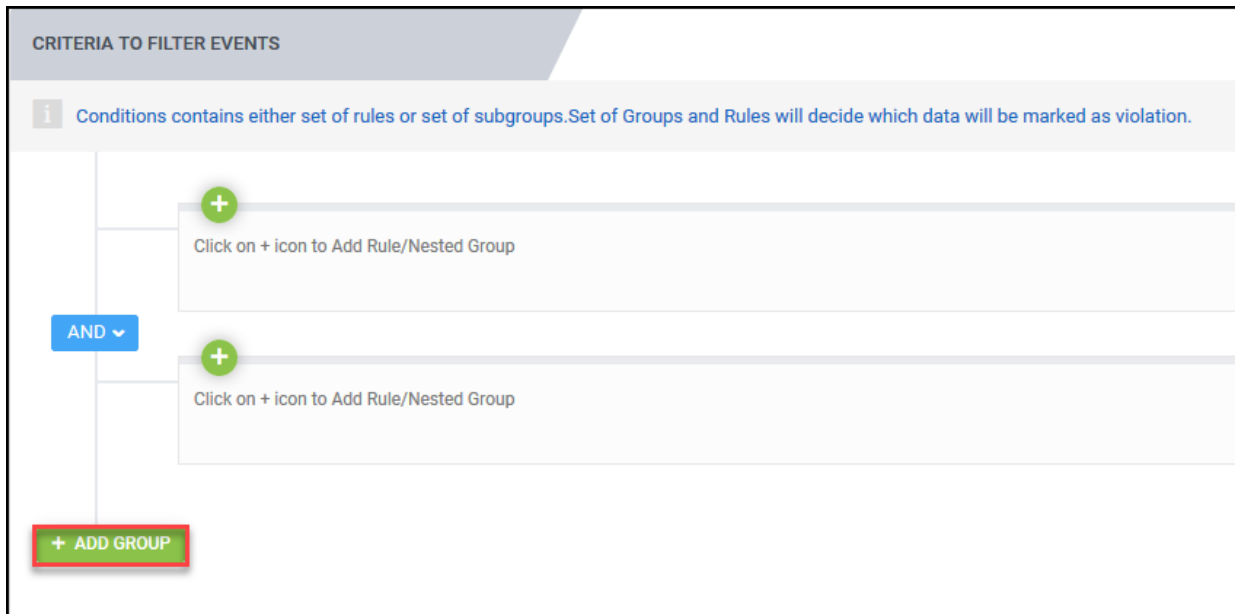


Note: See [Appendix A: ArcSight UBA Attribute Schema](#) for a list of the attributes you can use to search in place of * in the previous example.

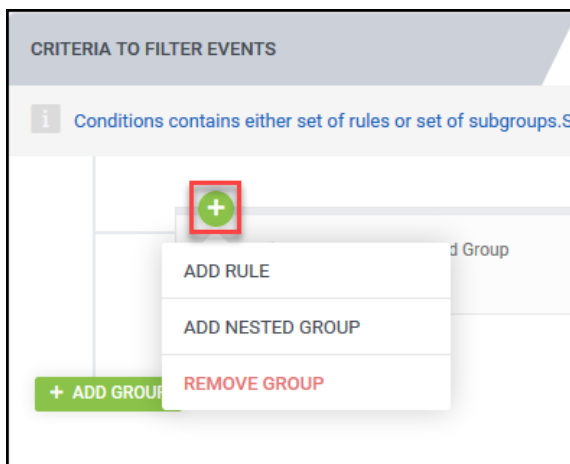
Criteria to Filter Events

Criteria to Filter Events contain sets of rules or sets of nested groups called conditions. Conditions decide which data will be marked as a violation. Complete these steps to create conditions to filter events. For more information and examples of how to use conditions to filter events, see [Conditions](#).

1. Click **Add Group** for each condition group you would like to add.



2. Click + to **Add Rule** to group or **Remove Group** of rules.



- **Add Rule:** Complete the following information in pop up window:

- Select Event Attribute:** Select an attribute from the dropdown. Example: Email Recipient Domain.



Note: Event Attributes are organized by Object. Example: **Object:** EVENT-EMAIL | **Event Attribute:** Email Recipient Domain.

OR

Click **Use Operator Expression** to configure the operator. See [Operators](#) for more information about how to use operators. .

- Select Condition:** Select from the dropdown. Example: Equal To.
- Value:**

- Provide a value to match to the source criteria. Example: competitor.com.
OR
- Click **Select Event Attribute** to select an attribute from the dropdown. Example: TPI domain.
OR
- Click **Use Operator Expression** to select **Show Available Operators**.

The screenshot shows a rule configuration interface. On the left, there's a sidebar with a blue circle containing the letter 'B'. The main area has three tabs: 'Value', 'Select Event Attribute', and 'Use Operator Expression'. The 'Use Operator Expression' tab is active. Below the tabs is a large empty box. To the right of this box is a panel titled 'Available Operators' containing a list of operators and their descriptions: DAY_OF_MONTH (Day of month), DAY_OF_WEEK (Day of week), STRING_DAY_OF_WEEK (String day of week), MONTH_OF_YEAR (Month of year), YEAR_OF_TIME (Year), SUM (Sum), and MUL (Multiply). At the bottom left of the main area, a button labeled 'Show Available Operators' is highlighted with a red rectangular box. Below this button is the text '@rightsideside'.

- d. **Add:** Click to add the rule to the group.
- **Add Nested Group:** Click to add a nested group of rules within the group.
 - **Remove Group:** Click to remove groups.



Note: Removing a Group will delete all Rules within the Group.

Additional Event Analytics

Additional Event Analytics perform additional processing after violations have been detected by a set of Filter Conditions. Event analytics check individual events against data such as Active Lists, Lookup Tables, Watchlists, Geolocation, Domain Age, and Third Party Intelligence.

The screenshot shows the 'ADDITIONAL EVENT ANALYTICS' configuration screen. At the top, there's a header bar with the title 'ADDITIONAL EVENT ANALYTICS' and a toggle switch for 'Do you want to flag as a violation ONLY when it matches all the selected Analytical Checks?' set to 'NO'. Below the header, there's a section titled 'Events Matching Conditions pass to Additional Event Analytics'. Under this section, there are several buttons for different analytics: 'CHECK AGAINST ACTIVE LIST', 'CHECK AGAINST LOOKUP TABLE', 'CHECK AGAINST THIRD PARTY INTELLIGENCE', 'CHECK AGAINST WATCHLIST', 'CHECK DOMAIN AGE', 'CHECK NETWORK ADDRESS', 'CUSTOM FUNCTION', 'EMAIL SENT TO SELF', 'MATCH STRING', and 'SPOTTER QUERY'. At the bottom left, there's a button labeled 'SQL QUERY'.

To perform additional processing using Additional Event Analytics, complete the following steps:

1. Click each Additional Event Analytics you would like to add.
2. Enable **Do you want to flag as a violation ONLY when it matches all the selected Analytical Checks?** if you want to restrict violations to exact matches to Analytical Checks.
3. Complete fields for each selected function.
4. Click red **X** to remove functions.

Check Against Active List

Check Against Active List checks activity data against Active Lists. Active Lists are used in ArcSight UBA to maintain a history of activity on specified attributes for each event for a specified duration of time for faster processing and analytical checks. Active lists are also configured during [Activity Data](#) import and stored in Redis in-memory database.

Use **Check Against Active Lists** in policies to check against only the specified attributes in the active list, rather than every attribute in the event, when the conditions configured in the previous step are met.

Example:

Condition: Attribute: filename | Condition: Contains | value: customer.

Active List: accountname (1,3)+transactionstring1(50)+filename | Duration: 24 hrs

Event 1: **DateTime:**03 May 2017 2:28:11 PM | **accountname:** JRedding@sec.com | **transactionstring1:** Download | **filename:** Customer CCs.

Event 2: **DateTime:**03 May 2017 3:03:02 AM **accountname:** JRedding@sec.com | **transactionstring1:** Download | **filename:** Customer SSNs.

Event 3: **DateTime:**04 May 2017 11:52:33 AM **accountname:** JRedding@sec.com | **transactionstring1:** Upload to file sharing/storage site | **filename:** Customer CCs.

Event 4: **DateTime:**04 May 2017 11:53:04 AM **accountname:** JRedding@sec.com | **transactionstring1:** Upload to file sharing/storage site | **filename:** Customer SSNs.

Configure **Check Against Active List** as follows:

1. Select **Check Against Active List**.

The screenshot shows the 'ADDITIONAL EVENT ANALYTICS' section. A message states: 'Events Matching Conditions pass to Additional Event Analytics'. Below this, there are four buttons: 'CHECK AGAINST ACTIVE LIST' (highlighted in orange), 'CHECK AGAINST LOOKUP TABLE', 'CHECK AGAINST THIRD PARTY INTELLIGENCE', and 'CHECK AGAINST...'. Below these are 'SPOTTER QUERY' and 'SQL QUERY' buttons. A line connects the 'CHECK AGAINST ACTIVE LIST' button to a modal window titled 'Check Against Active List'. Inside the modal, there is a section 'Specify rule to check against Activelist' with a large text input area. Below the input area, it says: 'Please specify mapped attributes, e.g. accountname+ipaddress', 'transactionstring1(50)+accountname(1,3)', and 'emailsender+(.)+filename'. At the bottom, there is a 'Select Activelist' dropdown menu with '-Select-' as the current selection.

2. Provide the following information:

- a. **Specify rule to check against Activelist:** Specify attributes mapped in the datasource to check against. Example: accountname+transactionstring1(50)+accountname(1,3).



Note: For attribute transactionstring1 (50), the (50) refers to the maximum number of characters to be held in Redis.

For attribute accountname (1,3), the (1,3) instructs the active list to store the first character of the first name, and the first three in the last name. Example: HRUI will pick up hrui@sec.com or HECTORRUIZ.

OR

- b. **Select Activelist:** Select an existing Active List from the dropdown. Example: accountname+Filename.

Check Against Lookup Table


Check Against Lookup Table compares attributes in events against lookup tables added during [Lookup Tables](#) import.

Configure **Check Against Lookup Data** as follows:

1. Select **Check Against Lookup Table** from menu.

The screenshot shows the 'CHECK AGAINST LOOKUP TABLE' configuration interface. At the top, there's a header 'ADDITIONAL EVENT ANALYTICS' and a sub-header 'Events Matching Conditions pass to Additional Event Analytics'. Below this, there are several tabs: 'CHECK AGAINST ACTIVE LIST', 'CHECK AGAINST LOOKUP TABLE' (which is highlighted in orange), 'CHECK AGAINST THIRD PARTY INTELLIGENCE', 'CHECK AGAINST WATCHLIST', 'CHECK DOMAIN AGE', 'CHECK LENGTH', and 'CHECK NETWORK A'. Under the 'CHECK AGAINST LOOKUP TABLE' tab, there are two buttons: 'SPOTTER QUERY' and 'SQL QUERY'. The main configuration area is titled 'CHECK AGAINST LOOKUP TABLE' and contains three dropdown menus: 'Select The Field To Check Against Lookup Table' (set to 'TransactionString 1'), 'Select Condition' (set to 'Equal To'), and 'Select Lookup Table To Check' (set to 'Lookuptable_Logontype'). Below these, there's a toggle switch for 'Do you want to provide additional criteria on Lookup Table Attributes?' which is currently set to 'YES'. Under this toggle, there's a table with columns: 'Select The Field To Check Against Lookup Table Attribute', 'Select Condition', 'Select Lookup Table Attribute', and a final column for logical operators. The first row shows 'TransactionNumber 2' as the field, 'Equal To' as the condition, 'LogonDescription' as the attribute, and 'AND' as the operator. There are also '+' and '-' icons at the end of the row to add or remove criteria.

2. Provide the following information:
 - a. **Select the Field to Check Against Lookup Table:** Select an attribute from the dropdown. Example: Transactionstring1.
 - b. **Select Condition:** Select a condition from the dropdown. Example: Equal To.
 - c. **Select Lookup Table to Check:** Select a lookup table from the dropdown against which to check the selected attribute. Example: Lookuptable_Logontype.

 **Note:** Only lookup tables into which you have added data will appear.

 - d. **Do you want to provide additional criteria on Lookup Table Attribute?:** Toggle to **Yes** to select a field to check against attributes mapped in the Lookup Table.
 - a. **Select The Field Against Lookup Table Attribute:** Select an attribute to check against an attribute from the lookup table from the dropdown. Example: TransactionNumber 2.
 - b. **Select Condition:** Select from the dropdown. Example: Equal To.
 - c. **Select Lookup Table Attribute:** Select an attribute within the lookup table mapped during Lookup Data import from the dropdown. Example: LogonDescr
 - d. **And/Or:** Specify from the dropdown.
 - e. **+/-:** Use to add/ remove criteria.

Check Against Third Party Intelligence

Check against Third Party Intelligence compares attributes in events against Third Party Intelligence added during TPI import.

Configure **Check Against Third Party Intelligence** as follows:

1. Select **Check Against Third Party Intelligence**.

The screenshot shows the 'ADDITIONAL EVENT ANALYTICS' section of a configuration page. It features a header with an information icon and the text 'Events Matching Conditions pass to Additional Event Analytics'. Below this are five buttons: 'CHECK AGAINST ACTIVE LIST', 'CHECK AGAINST LOOKUP TABLE', 'CHECK AGAINST THIRD PARTY INTELLIGENCE' (highlighted in orange), 'SPOTTER QUERY', and 'SQL QUERY'. A line connects the highlighted button to a detailed configuration panel titled 'CHECK AGAINST THIRD PARTY INTELLIGENCE'. This panel contains two columns of dropdown menus. The first column is labeled 'Field To Check Against TPI' and has one dropdown with 'Destination HostName' selected. The second column is labeled 'TPI Src To Check' and has one dropdown with 'threatstream' selected. To the right of the 'TPI Src To Check' dropdown is a button with a plus icon and the text '+ Add TPI Src'. Below the first dropdown is another 'Field To Check Against TPI' dropdown, also with 'threatstream' selected. To the right of this second dropdown is a red minus icon.

2. Select attribute from **Field to Check Against TPI** dropdown. Example: Destination HostName.
3. Select **TPI to Check** from dropdown. Example: threatstream.
4. Click **+ TPI Src** to add additional **TPI Src** fields to check.
5. Use **-** to remove TPI cores to check.

Check Against Watchlist

Check Against Watchlist compares attributes in events against watch lists added during Watchlist creation.

Configure **Check Against Watchlist Data** as follows:

1. Select **Check Against Watchlist**.

The screenshot shows the 'ADDITIONAL EVENT ANALYTICS' configuration page. At the top, a message states 'Events Matching Conditions pass to Additional Event Analytics'. Below this, there are several tabs: 'CHECK AGAINST ACTIVE LIST', 'CHECK AGAINST LOOKUP TABLE', 'CHECK AGAINST THIRD PARTY INTELLIGENCE', 'CHECK AGAINST WATCHLIST' (which is highlighted in orange), and 'CHECK DOMAIN AGE'. Below the tabs, there are two buttons: 'SPOTTER QUERY' and 'SQL QUERY'. The 'CHECK AGAINST WATCHLIST' section is expanded, showing three fields: 'Select The Field To Check Against Watchlist' with a dropdown menu showing 'Account Name', 'Select Watchlist' with a dropdown menu showing 'Privileged Users (Users)', and a toggle switch for 'Do you want to flag as Violation if it is not found in Watchlist?' which is currently set to 'NO'.

2. Select attribute from **Field to Check Against Watchlist** dropdown. Example: Account Name.
3. **Select Watchlist** from dropdown. Example: Privileged Users (Users).
4. **Do you want to flag as Violation if it is not found in Watchlist?**: Toggle to **Yes** if you would like to flag as violations even if the account name is not found on a watchlist.

Check Domain Age

Check Domain Age compares attributes against an age in days.

Configure **Check Domain Age** as follows:

1. Select **Check Domain Age**:

The screenshot shows the 'ADDITIONAL EVENT ANALYTICS' configuration page. At the top, a message states 'Events Matching Conditions pass to Additional Event Analytics'. Below this, there are several tabs: 'CHECK AGAINST ACTIVE LIST', 'CHECK AGAINST LOOKUP TABLE', 'CHECK AGAINST THIRD PARTY INTELLIGENCE', 'CHECK AGAINST WATCHLIST', and 'CHECK DOMAIN AGE' (which is highlighted in orange). Below the tabs, there are two buttons: 'SPOTTER QUERY' and 'SQL QUERY'. The 'CHECK DOMAIN AGE' section is expanded, showing two fields: 'Select Field' with a dropdown menu showing 'Destination Network Domain' and 'Age (In Days)' with a text input field containing '750'. Below the input field, there is a label 'Enter Age in days'. At the bottom of the section, there is a note: 'If domain age is greater than specified value(in days) then mark as violation'.

2. **Select Field** against which to check age. Example: Destination Network Domain.
3. Specify the **Age (In Days)**. Example: 750.

Check Network Address

Check Network Address checks for a specific event attribute and flags the event as a violation if the attribute is not found in the event.

Configure **Check Network Address** as follows:

1. Select **Check Network Address** from the menu.

The screenshot shows the 'ADDITIONAL EVENT ANALYTICS' configuration interface. At the top, a status bar indicates '1 Events Matching Conditions pass to Additional Event Analytics'. Below this, a row of buttons includes 'CHECK AGAINST ACTIVE LIST', 'CHECK AGAINST LOOKUP TABLE', 'CHECK AGAINST THIRD PARTY INTELLIGENCE', 'CHECK AGAINST WATCHLIST', 'CHECK DOMAIN AGE', and 'CHECK NETWORK ADDRESS' (which is highlighted in orange). To the left of these buttons is a 'SQL QUERY' button. Below the 'CHECK NETWORK ADDRESS' button, a configuration panel is expanded. It contains a 'Network address field' dropdown menu with 'Destination Network Domain' selected. To the right of this dropdown is a 'Violate If Not Found' toggle switch, which is currently set to 'YES' (indicated by a green circle). Below the dropdown, there is a text prompt 'Select a Network Address field'.

2. Select attribute from **Network address field** from dropdown. Example: Destination Network Domain.
3. Toggle **Violate if Not Found** to **Yes** to flag the event as a violation if the address field is not found.

Custom Function

You can create a custom Additional Event Analytic function as follows:

1. Select **Custom Function**.

The screenshot shows the 'ADDITIONAL EVENT ANALYTICS' configuration interface. The 'CUSTOM FUNCTION' button is highlighted in orange. The configuration panel below it is expanded, showing a 'Class Name' text input field with the value 'PolicyViolatorScore.class' entered.

2. Enter a unique **Class Name**. Example: PolicyViolatorScore.class.



Note: When you have defined the Class Name, the class file must be placed in the respective path. Example: (\$\$/apache-tomcat-8.0.33/webapps/Snypr/WEB-INF/classes/com/securonix/snyper/).

Email Sent to Self

Email Sent to Self checks events for email recipients against the email sender using a match threshold.

Configure **Email Sent to Self** as follows:

1. Select **Email Sent To Self**.

The screenshot shows the 'ADDITIONAL EVENT ANALYTICS' configuration interface. At the top, a status bar indicates '1 Events Matching Conditions pass to Additional Event Analytics'. Below this, a row of buttons includes 'CHECK AGAINST ACTIVE LIST', 'CHECK AGAINST LOOKUP TABLE', 'CHECK AGAINST THIRD PARTY INTELLIGENCE', 'CHECK AGAINST WATCHLIST', 'CHECK DOMAIN AGE', 'CHECK NETWORK ADDRESS', 'CUSTOM FUNCTION', and 'EMAIL SENT TO SELF' (highlighted in orange). A 'SQL QUERY' button is also present. The 'EMAIL SENT TO SELF' configuration panel is open, showing a dropdown for 'Select Field for Email Recipient' with 'Email Sender' selected, and a 'Match Threshold (0 to 1)' input field with '0.8' entered. Below these are labels 'Select a field for email recipient' and 'Enter Threshold'.

2. **Select Field for Email Recipient** to check against from dropdown. Example: Email Sender.
3. Specify a **Match Threshold** from 0-1. Default: 0.8.

Match String

Match String matches attribute values in an event using a match threshold.

Configure **Match String** as follows:

1. Select **Match String**.

The screenshot shows the 'ADDITIONAL EVENT ANALYTICS' configuration interface. At the top, a status bar indicates '1 Events Matching Conditions pass to Additional Event Analytics'. Below this, a row of buttons includes 'CHECK AGAINST ACTIVE LIST', 'CHECK AGAINST LOOKUP TABLE', 'CHECK AGAINST THIRD PARTY INTELLIGENCE', 'CHECK AGAINST WATCHLIST', 'CHECK DOMAIN AGE', 'CHECK NETWORK ADDRESS', 'CUSTOM FUNCTION', 'EMAIL SENT TO SELF', and 'MATCH STRING' (highlighted in orange). A 'SQL QUERY' button is also present. The 'MATCH STRING' configuration panel is open, showing two dropdowns: 'Select First Field to compare' with 'Email Sender Domain' selected and 'Select Second Field to compare' with 'TPI Domain' selected. A 'Match Threshold (0 to 1)' input field has '0.8' entered. Below these are labels 'Select a field to compare', 'Select a field to compare', and 'Enter Threshold'.

2. **Select First Field to Compare** from dropdown. Example: Email Sender Domain.
3. **Select Second Field to Compare** from dropdown. Example: TPI Domain.
4. Specify a **Match Threshold** from 0-1. Default: 0.8.

Spotter Query

Spotter Query allows you to enter a Spotter search query to check against specific information within Solr collection cores.

Configure **Spotter** as follows:

1. Select **Spotter Query**.

The screenshot shows a web interface titled "ADDITIONAL EVENT ANALYTICS". Below the title, a message states: "1 Events Matching Conditions pass to Additional Event Analytics". There are five buttons in a row: "CHECK AGAINST ACTIVE LIST", "CHECK AGAINST LOOKUP TABLE", "CHECK AGAINST THIRD PARTY INTELLIGENCE", "CHECK AGAINST WATCHLIST", and "CHECK DOMAIN AGE". Below these buttons are two more buttons: "SPOTTER QUERY" (highlighted in orange) and "SQL QUERY". A line connects the "SPOTTER QUERY" button to a configuration box below. The configuration box is titled "SPOTTER QUERY" and contains two sections: "Query" and "Core". The "Query" section has a text input field containing "transactionstring2 = 'Failed Login'" and a placeholder "Enter Query". The "Core" section has a dropdown menu currently showing "ACTIVITY" and a placeholder "Select Core".

2. Enter a **Spotter** Query. For search help, see [Spotter Search Help](#). Example: transactionstring2 = "Failed Login".
3. Select a **Core** data collection core from the dropdown. Example: ACTIVITY.

SQL Query

SQL allows you to run a SQL query on specific information for a policy.

Configure **SQL** as follows:

1. Select **SQL Query**.

2. Enter the following information:

- a. **Database Type:** Select from dropdown. Example: MySQL.
- b. **JDBC URL:** Enter the URL to connect to the database. Default: jdbc:mysql://<host>:<3306>/<database>.
- c. **Driver Class:** Enter the database specific class. Default: com.mysql.jdbc.Driver.
- d. **Database Username:** Enter the username for the database. Example: root.
- e. **Database Password:** Enter the password for the database.
- f. **Query:** Enter the query to run on the policy. Example: select id,userid, accountname, activitytransaction,applicationprotocol, filesize, bytsesin, bystesout from policyviolationevents.

Risk Boosters

Risk Boosters increase or decrease risk scores for a policy based on specified criteria.

You can enable the following Risk Boosters:

Match Criteria

Match Criteria increases or decreases the risk score of the policy when a source criteria matches a destination criteria.

Configure **Match Criteria** as follows:

1. Select **Match Criteria**.

RISK BOOSTERS

Risk Booster will increase/decrease risk scores for specified criteria

MATCH CRITERIA | WATCHLIST ENTITIES | AFTER HOURS ACTIVITY | LOOKUP TABLE

Source Column	Condition	Destination Column/Value	Operator	
filename	Contains	confidential	AND	+ -

Increase/Decrease Risk?
increase

Increase/Decrease Riskscore for the above mentioned criteria

Adjustment Factor*
100

Factor by which to increase/decrease riskscore

2. Provide the following information:

- Source Column:** Select an attribute from the dropdown. Example: filename.
 - Condition:** Select a condition from the dropdown. Example: Contains.
 - Destination Column/Value:**
 - Provide a value to match to the source criteria. Example: confidential.
- OR



- Click  to select from the dropdown.

filepermission

|

filepermission

filehash

filepermission

filehash

oldfilepermission

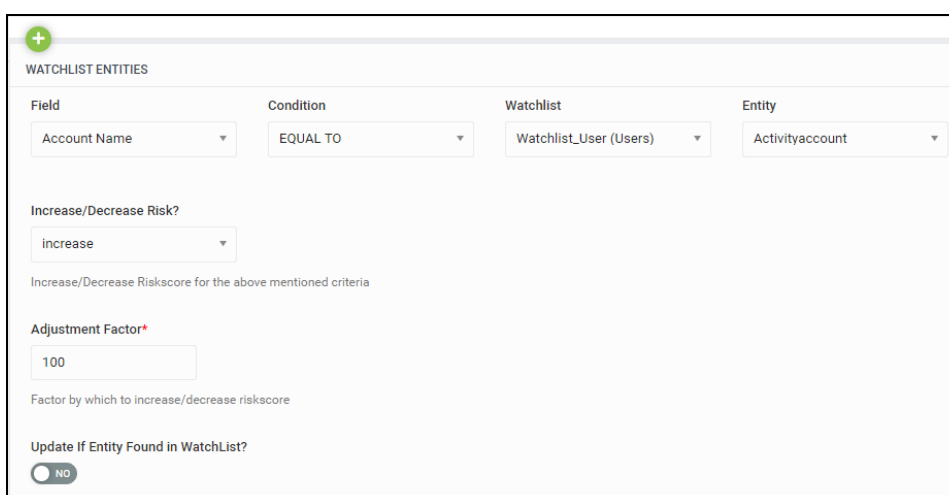
- d. **Operator:** Select AND or OR.
- e. **+/-:** Click to add/remove conditions.
- f. **Increase/Decrease Risk?:** Select one from the dropdown.
- g. **Adjustment Factor:** Enter a numerical value to adjust the risk. Example: 100.

Watchlist Entities

Watchlist Entities increases or decreases the risk score if a specific attribute matches a specified watchlist.

Configure **Watchlist Entities** as follows:

1. Select **Watchlist Entities**.



WATCHLIST ENTITIES

Field	Condition	Watchlist	Entity
Account Name	EQUAL TO	Watchlist_User (Users)	Activityaccount

Increase/Decrease Risk?

Increase

Increase/Decrease Riskscore for the above mentioned criteria


Adjustment Factor*

100

Factor by which to increase/decrease riskscore

Update If Entity Found in WatchList?

NO

2. Provide the following information:
 - a. **Field:** Select a field to check against the watchlist from the dropdown. Example: Account Name
 - b. **Condition:** Select a condition from the dropdown. Example: Equal To.
 - c. **Watchlist:** Select a Watchlist from the dropdown. Example: Bad Performance Review (Users).
 -  **Note:** You must have added Watchlist data to use this risk booster function.
 - d. **Entity:** Select the entity for this watchlist. Example: Users.
 - e. **Increase/Decrease Risk?:** Select one from the dropdown.
 - f. **Adjustment Factor:** Enter a numerical value to adjust the risk. Example: 100.
 - g. **Update if entity found in watchlist?:** Toggle to **Yes** if you would like to update the watchlist if the entity is found.

After Hours Activity

After Hours Activity increases or decreases the risk score if events occur within a specified time range.

Configure **After Hours Activity** as follows:

1. Select **After Hours Activity**.

The screenshot shows the 'RISK BOOSTERS' configuration page. At the top, there is a header 'RISK BOOSTERS' and a sub-header 'Risk Booster will increase/decrease risk scores for specified criteria'. Below this, there are four tabs: 'MATCH CRITERIA', 'WATCHLIST ENTITIES', 'AFTER HOURS ACTIVITY' (which is highlighted in orange), and 'LOOKUP TABLE'. A line connects the 'AFTER HOURS ACTIVITY' tab to a detailed configuration panel below. This panel has the title 'AFTER HOURS ACTIVITY' and contains the following fields:

- After Hours Start Time***: A text input field with '2000' and a unit dropdown set to 'hrs'.
- After Hours End Time ***: A text input field with '0700' and a unit dropdown set to 'hrs'.
- Increase/Decrease Risk?**: A dropdown menu currently set to 'increase'.
- Adjustment Factor***: A text input field with '1000'.

Below the fields, there is explanatory text: 'Increase/Decrease Riskscore for the above mentioned criteria' and 'Factor by which to increase/decrease riskscore'.

2. Provide the following information:
 - a. **After Hours Start Time:** Enter the start time for after hours activity on a 24-hour clock. Example: 2000 hours (8:00 P.M.).
 - b. **After Hours End Time:** Enter the end time for after hours activity on a 24-hour clock. Example: 0700 hours (7:00 A.M.).
 - c. **Increase/Decrease Risk?:** Select one from the dropdown.
 - d. **Adjustment Factor:** Enter a numerical value to adjust the risk. Example: 1000.

Lookup Table

Lookup Table increases or decreases the risk score if events contain Lookup Table data.

Configure **Lookup Data** as follows:

1. Select **Lookup Table**.

The screenshot shows the 'RISK BOOSTERS' configuration page. At the top, there's a header 'RISK BOOSTERS' and a sub-header 'Risk Booster will increase/decrease risk scores for specified criteria'. Below this are four tabs: 'MATCH CRITERIA', 'WATCHLIST ENTITIES', 'AFTER HOURS ACTIVITY', and 'LOOKUP TABLE' (which is highlighted in orange). The 'LOOKUP TABLE' tab is active, showing a form with the following fields:

- Lookup Table:** A dropdown menu with 'Lookuptable_Logontype' selected.
- Row Key:** A section with two dropdowns: 'Select Condition' (set to 'Equal To') and 'Select The Field To Check Against Lookup Table Attribute' (set to 'TransactionString 2').
- Value:** A section with two dropdowns: 'Select Condition' (set to 'Equal To') and 'Select The Field To Check Against Lookup Table Attribute' (set to 'Source User Privileges'). To the right of these is a dropdown set to 'AND' and a green plus icon.
- Increase/Decrease Risk?:** A dropdown menu set to 'increase'.
- Adjustment Factor*:** A text input field containing '100'.

Below the 'Adjustment Factor' field, there is a small text label: 'Factor by which to increase/decrease riskscore'.

2. Provide the following information:

- a. **Lookup Table:** Select a pre-configured lookup table from the dropdown.

Example: Lookuptable_Logontype.



Note: You must have imported lookup table data to use this risk booster function.

- b. **Row Key:**

- a. **Select Condition:** Select from dropdown. Example: Equal To.

- b. **Select the Field to Check Against Lookup Table Attribute:** Select a from the dropdown. Example: Transactionstring2.

c. **Value:**

- a. **Select Condition:** Select from dropdown. Example: Equal To.
- b. **Select the Field to Check Against Lookup Table Attribute:** Select from dropdown. Example: Source User Privileges.
- c. **Operator:** Select AND or OR.
- d. **+/-:** Click to add/remove values.
- d. **Increase/Decrease Risk?:** Select one from the dropdown.
- e. **Adjustment Factor:** Enter a numerical value to adjust the risk. Example: 100.

When all conditions are provided, click **Save & Next** to proceed to [Configure The Violation Information Summary](#).

Configure The Violation Information Summary

In this section, determine what actions the application will take for violations of this policy. Create actions to generate cases, assign workflow, export data in CEF format, and configure a violation summary to specify what attributes to include in the violation summary for the [Policies](#).

Complete the following information to appear on the Violation Summary screen that can be accessed from the [Security Command Center](#):

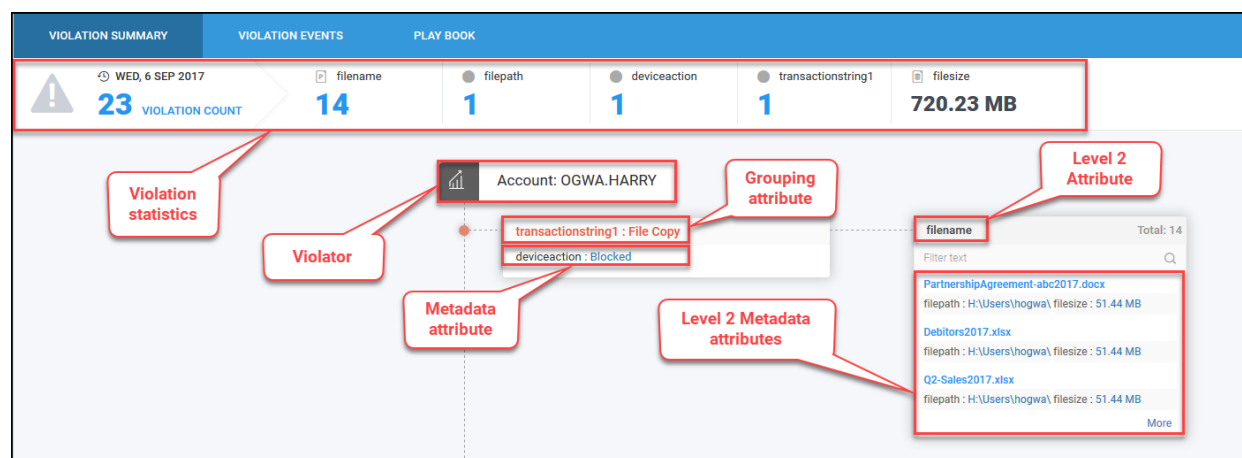
- a. (Optional) **Provide the verbose template for violation summary:** Enter a verbose template to specify custom attributes to display in the violation summary. Example: Account \${accountname!"ACCOUNTNAME"} performed \${transactionstring1!"ACTIVITY"} from ipaddress \${ipaddress!"UNKNOWN"}.



Note: You must include the ! in the attribute. For example: \${resource!\"Unknown\"} initiated a suspicious process will work but \${resource} initiated a suspicious process will not. For a complete list of available attributes, see [Appendix C: Verbose Template Attributes](#).

- b. **Grouping Attribute:** Select an attribute under which to group the information in the summary.
- c. **Metadata Attributes:** Select up to three metadata attributes to view within the grouping attribute in the summary.
- d. **Level 2 Attribute:** Select a high-level attribute to view independent of the Grouping Attribute.
- e. **Level 2 Metadata Attributes:** Select up to three metadata attributes to view within the Level 2 attribute in the summary.

The Violation Summary will appear as follows on the Violations Summary screen:



Violation Action

1. Complete the following steps to choose the action to be taken on the violations flagged by the policy:

VIOLATION ACTION

Daily Violation Threshold

When a violations exceeds the threshold, it will be skipped for scoring and saving.

Do you want to generate incident for policy violators?

☐ NO

Send Notification

☐ NO

Add Policy Violators to Watchlist?

Add Policy Violators to Active list?

☐ NO

CEF Output

☐ NO

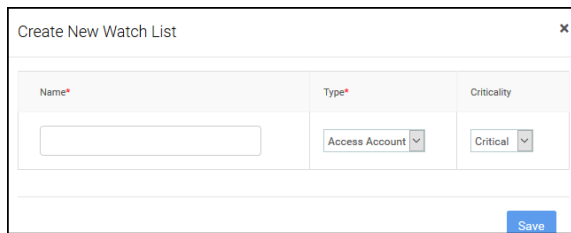
RSA Archer CEF Output

☐ NO

RSA Netwitness CEF Output

☐ NO

- a. **Daily Violations Threshold:** Enter a value after which to stop flagging violations for the policy.
- b. **Do you want to generate cases for policy violators?:** Set to **YES** to generate a case for each policy violator.
Cases can also be created manually from the Security Command Center.
 - a. **Select workflow to trigger when generating cases:** Set to **Yes** to select a workflow from the dropdown.
- c. **Send Notification:** Toggle to **YES** to **Select Email Template** from dropdown to receive notifications of violations for this policy.
- d. **Add Policy Violators to Watchlist?:** Select from dropdown or **Create a New Watchlist**.



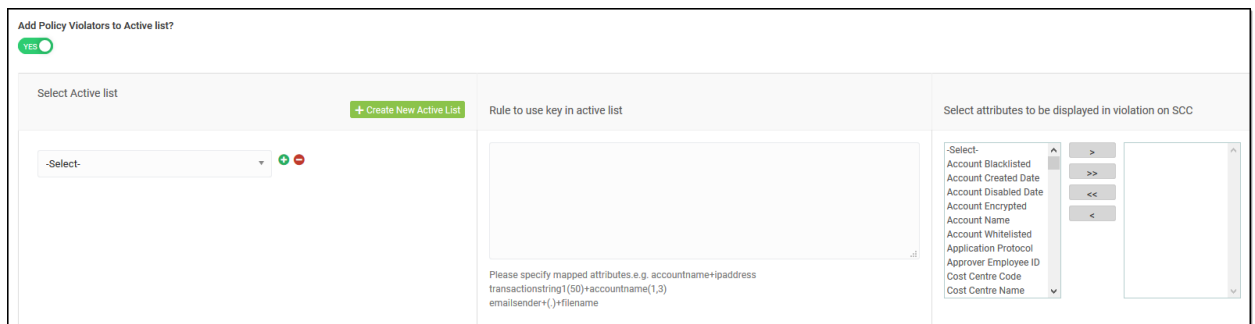
Create New Watch List

Name*	Type*	Criticality
<input type="text"/>	Access Account	Critical

Save

Complete the following:

- Confidence Factor:** Enter a value from 0 to 1 to indicate how confident you are the violator should be on the watchlist.
- Confidence Incremental Factor:** Enter a value from 0 to 1 to indicate how confident you are the violation should be on the watchlist for each subsequent violation.
- Rule to Remove Violators from Watchlist:** Enable to specify a time frame after which to **Remove Violators from Watchlist**.
- Add Policy Violators to Active List?:** Toggle to **YES** to complete the following information:



Add Policy Violators to Active list?

YES ☒

<p>Select Active list</p> <p>+ Create New Active List</p> <p>-Select-</p>	<p>Rule to use key in active list</p> <p>Please specify mapped attributes e.g. accountname+ipaddress transactionstring(150)+accountname(1,3) emailsender()+filename</p>	<p>Select attributes to be displayed in violation on SCC</p> <p>-Select- Account Blacklisted Account Created Date Account Disabled Date Account Encrypted Account Name Account Whitelisted Application Protocol Approver Employee ID Cost Centre Code Cost Centre Name</p>
---	---	--

- Select Active list:** Select from dropdown or Create New Active List as described in [Check Against Active List](#).
- Rule to use key in active list:** Specify mapped attributes to include in the check as described in [Check Against Active List](#).
- Select attributes to be displayed in violation on SCC:** Use > or >> to add the attributes to include in the violation summary on the [Security Command Center](#).

f. **CEF Output:** Toggle to **Yes** to produce output in CEF format. If **Yes**:

a. **Select Connection** from dropdown.



Note: You must configure your connections for CEF output in [Connection Types](#) before you can export from ArcSight UBA.

b. Click **Output Mapping** to configure output.

CEF Field	Constant?	Mapped With
act	YES	deviceaction
app	YES	applicationprotocol
dhost	YES	destinationhostname
dpid	YES	destinationprocessid
dmac	YES	destinationmacaddress
dntdom	YES	destinationntdomain

Save

a. **CEF Field:** Specify field. Example: act.

b. **Constant?:** Toggle to **Yes** or **No**.

c. **Mapped With:** Enter a value using +/- to add/remove attributes.
Example: deviceaction

g. **RSA Archer CEF Output:** Toggle to **Yes** to produce output in CEF format. If **Yes**, see **CEF Output**.



Note: You must configure your connections for RSA Archer CEF output before you can export from ArcSight UBA.

h. **RSA Netwitness CEF Output:** Toggle to **Yes** to produce output in CEF format. If **Yes**, see **CEF Output**.



Note: You must configure your connections for RSA Netwitness CEF output before you can export from ArcSight UBA.

Example Real Time Policy: Check Land Speed

This real time policy uses geolocation data and advanced analytics to compute land speed to flag activity accounts performing successful login attempts from different geographic locations within unusual or impossible periods of time. This indicates account misuse.

Prerequisites

Before enabling this policy, you must complete the following:

1. Import Geolocation data from MaxMind. For more information about importing from MaxMind, see [Geolocation/Network Map Data](#).
2. Enable Geolocate_Attributes for the datasource during activity import **Step 3: Provide Conditions**. For more information about using action filters, see [Activity Data](#).

The screenshot displays the ArcSight policy configuration interface. On the left, the 'ACTION FILTERS' panel lists various actions with toggle switches and icons. The 'Geolocate_Attributes' action is highlighted. The main area is titled 'ADD CONDITIONS' and contains a table for defining conditions. Below this, there is a section for 'SELECT ACTIONS FOR ABOVE CONDITIONS' with a red box highlighting the 'GEOLOCATE_ATTRIBUTES' action configuration. This configuration includes a list of fields to be geolocated, with 'ClientIP' selected and a dropdown menu showing options like 'Destination Domain' and 'Hostname'.

Attribute	Operator	Value	Condition	Add/Remove
src_ip	Is Not Null		AND	+ -

Do you want to drop Events that do not get correlated?
☒ NO
 If yes then above conditions will be evaluated after correlation of event data.

SELECT ACTIONS FOR ABOVE CONDITIONS

Click on + icon to add actions

GEOLOCATE_ATTRIBUTES REMOVE ACTION

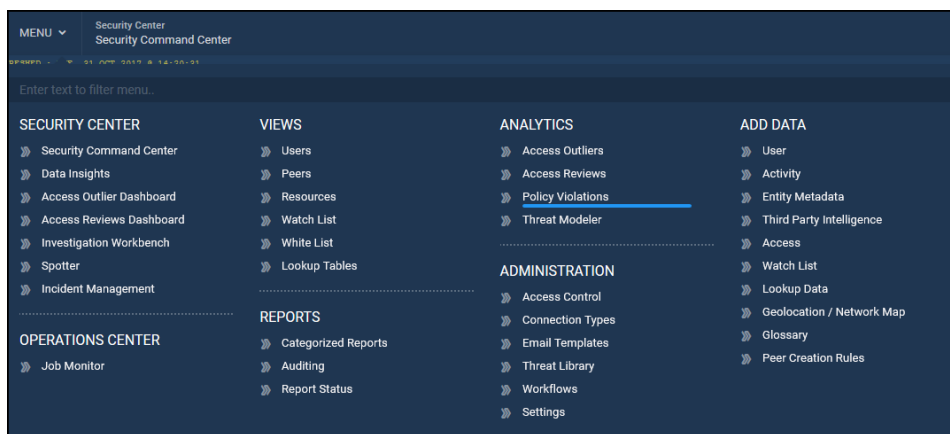
Specify fields to get Geolocated

ClientIP

Destination Domain
 Destination Domain
 Destination Domain
 Destination Domain
 Hostname

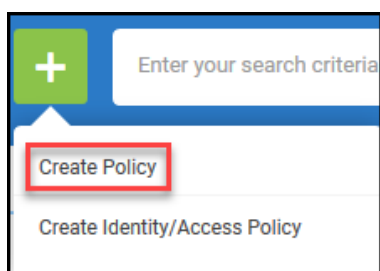
To configure the policy, complete the following steps:

1. Navigate to **Menu > Analytics > Policy Violations**:



2. Click **+**.

3. Select **Create Policy**.



Enter Policy Details

In this section, configure the policy name, criticality, entity against which the policy will run, and the datasource to which the policy will be applied, as well as designating the owner and remediator of the policy in order to restrict what users may view the policy violations. Define the category and indicator of threat.

Define Policy

Complete the following information:

DEFINE POLICY

Policy Name*

Provide unique name which will describe what type of violation it detects. Special characters are not allowed. Example: (- (bracket), ' - (single quote) are not allowed

Description

Criticality

Low

Select the criticality of the policy. The criticality affects the risk score for the user. None=0.0, Low=0.2, Medium=0.6 and High=1.0

Do you want to save violations and calculate risk scores for this policy?

YES

If Yes, violations will be searchable in Spotter and risk scores will be calculated for violators. If No, violations will not be searchable and risk scores will not be calculated for violators of this policy.

Do you want to escalate this policy as a Threat?

YES

If Yes, this policy will be escalated as a Threat instead of a Violation and will appear under Top Threats in Security Command Center. If no, this policy will appear under the Top Violations widget.

Select Violation Entity*

Activity Account

Select the entity that the risk should apply to?

Users - Returns list of users violating policy. Orphan accounts(or uncorrelated accounts) will be ignored.

ActivityAccount - Returns list of activity accounts (both correlated and uncorrelated) violating the policy.

Resources - Returns list of resources violating the policy.

Do you want to run the policy on a

✓ Datasource

Functionality

Citrix VPN [Citrix VPN]


- Policy Name:** Provide a unique name to describe the policy: Land Speed Violation Policy.
- Description:** Enter a brief description of the policy. Example: Flag a user who violates land speed by logging in to different IP addresses within an unusual period of time.
- Criticality:** Use slider to select the criticality of the policy: Medium.



Note: This will affect the risk score for the user. None=0.0, Low=0.2, Medium=0.6, and High=1.0.

- Do you want to save violations and calculate risk scores for this policy?:** Toggle to **YES** to make violations for this policy searchable in Spotter and to calculate risk scores for violators. If disabled, violations will not be searchable and risk scores will not be calculated.

- e. **Do you want to escalate this policy as a Threat?:** Toggle to **YES** to escalate the policy to a threat rather than a policy violation. Violations will appear under Top Threats in the Security Command Center. If **NO**, view violations will appear in the Top Violations dashboard.
- f. **Select Violation Entity:** Select from dropdown: Activity Account.
 - **Activity Account:** Returns list of activity accounts (both correlated and uncorrelated) violating policy.
- g. **Do you want to run the policy on a:** Select **Datasource** and use dropdown to select the datasource the policy should run on: Citrix VPN

 **Note:** Geolocation attributes must be enabled for this datasource prior to running this policy.
- h. **Owner:** Click search icon to select an owner for the policy: None selected.
- i. **Remediator:** Click search icon to select a remediator for the policy: None selected.

Define Risk and Threat

1. Complete the following information:

DEFINE RISK AND THREAT

Category*

Create New Policy Category

Account Misuse ▼ + -

Category is displayed on dashboard as a widget and risk will be aggregated for policies with the same category. All violations of the same category will be available in the widget.

Threat Indicator*

Create New Threat Indicator Edit Killchain Stage and Response Actions

Landspeed Violation Detected ▼

Violations detected are indicative of threat

- a. **Category:** Select from dropdown: Account Misuse.
- b. **Threat Indicator:**
 - a. Select from dropdown: Landspeed Violation Detected
 - OR
 - b. **Create New Threat Indicator** as described in [Creating Policies](#).
2. Click **Save & Next** to proceed to Provide Conditions.

Provide Conditions

What do you want to detect?

Select **Land Speed Detection**.

WHAT DO YOU WANT TO DETECT ?

1 Land Speed Detection : Detects bunch of activities with different geographical location within specific time range. Example : If user login to 'x' server multiple times from multiple countries within short period of time.

RARE BEHAVIOR SPIKE IN NUMBER OF OCCURRENCES SPIKE IN VOLUME/AMOUNT ENUMERATION BEHAVIOR ABNORMAL ACTIVITY COMPARED TO PEERS INDIVIDUAL EVENT ANALYTICS AGGREGATED EVENT ANALYTICS **LAND SPEED DETECTION**

BATCHED ANALYTICS

Filter Conditions

1. Click +.
2. Click **Add Rule**.
3. Use dropdowns to create the following rule:

CRITERIA TO FILTER EVENTS

1 Conditions contains either set of rules or set of subgroups. Set of Groups and Rules will decide which data will be marked as violation.

+ ADD GROUP

TransactionString 1 CONTAINS default SSLVPN LOGIN EDIT DELETE

EDIT RULE

Select Event Attribute OR Use Operator Expression

TransactionString 1 @leftside

Select Condition

Contains @middlecondition

Value OR Select Event Attribute OR Use Operator Expression

default SSLVPN LOGIN @rightside

CANCEL Add

LAND SPEED DETECTION

1. **Attribute:** Transactionstring1 | **Conditions:** Contains | **Value:** default SSLVPN LOGIN.

Land Speed Detection

1. Configure the following:

- a. **Flag as Violation if:** Max_Speed.
 - b. **Greater than Value (Miles):** 60.0 (miles).
 - c. **Having similar:** Account Name.
2. Click **Save & Next** to proceed to [Choose Action for Violation Results](#).

Choose Action for Violation Results

In this section, determine what actions the application will take for violations of this policy. Create actions to generate cases, assign workflow, export data in CEF format, and configure a violation summary to specify what attributes to include in the Violation Summary for [Policies](#).

1. Complete the following information to appear on the Violation Summary screen that can be accessed from the [Security Command Center](#):

- a. (Optional) **Provide the verbose template for violation summary:** Enter a verbose template to specify custom attributes to display in the violation summary. Example: Account `${accountname!"ACCOUNTNAME"}` performed `${transactionstring1!"ACTIVITY"}` from ipaddress `${ipaddress!"UNKNOWN"}`.



Note: You must include the **!** in the attribute. For example: `${resource!"Unknown"}` initiated a suspicious process **will work** but `${resource}` initiated a suspicious process **will not**. For a complete list of available attributes, see [Appendix C: Verbose Template Attributes](#).

- b. **Grouping Attribute:** Select an attribute under which to group the information in the summary. Example: Source.
- c. **Metadata Attributes:** Select up to three metadata attributes to view within the grouping attribute in the summary.
- d. **Level 2 Attribute:** Select a high-level attribute to view independent of the Grouping Attribute. Example: Destination.
- e. **Level 2 Metadata Attributes:** Select up to three metadata attributes to view within the Level 2 attribute in the summary.

Violation Action

1. Complete the following steps to choose the action to be taken on the violations flagged by the policy:

VIOLATION ACTION

Daily Violation Threshold

When a violations exceeds the threshold, it will be skipped for scoring and saving.

Do you want to generate incident for policy violators?

☐ NO

Send Notification

☐ NO

Add Policy Violators to Watchlist?

Add Policy Violators to Active list?

☐ NO

CEF Output

☐ NO

RSA Archer CEF Output

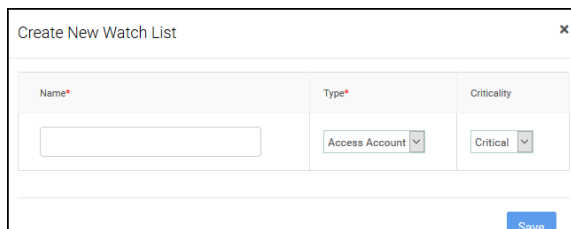
☐ NO

RSA Netwitness CEF Output

☐ NO

- a. **Daily Violations Threshold:** Enter a value after which to stop flagging violations for the policy.
- b. **Do you want to generate cases for policy violators?:** Set to **YES** to generate a case for each policy violator.
Cases can also be created manually from the Security Command Center.
 - a. **Select workflow to trigger when generating cases:** Set to **Yes** to select a workflow from the dropdown.
- c. **Send Notification:** Toggle to **YES** to **Select Email Template** from dropdown to receive notifications of violations for this policy.

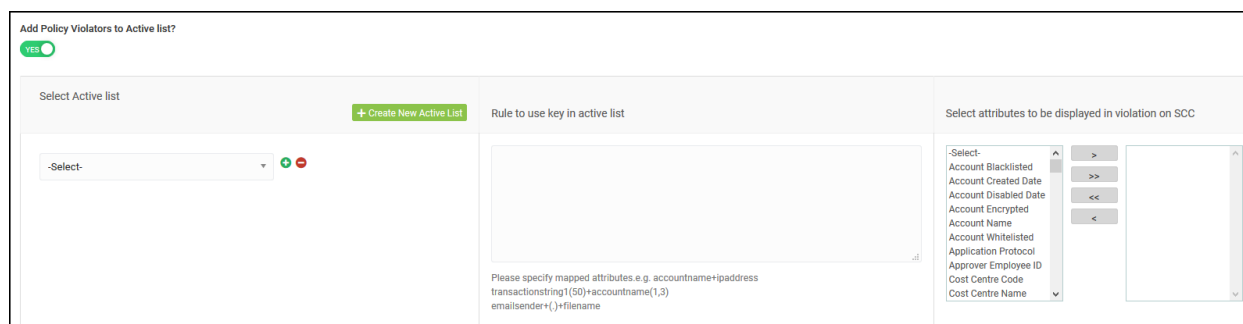
- d. **Add Policy Violators to Watchlist?:** Select from dropdown or **Create a New Watchlist**.



The 'Create New Watch List' dialog box contains three input fields: 'Name*' (a text box), 'Type*' (a dropdown menu with 'Access Account' selected), and 'Criticality' (a dropdown menu with 'Critical' selected). A 'Save' button is located at the bottom right.

Complete the following:

- Confidence Factor:** Enter a value from 0 to 1 to indicate how confident you are the violator should be on the watchlist.
- Confidence Incremental Factor:** Enter a value from 0 to 1 to indicate how confident you are the violation should be on the watchlist for each subsequent violation.
- Rule to Remove Violators from Watchlist:** Enable to specify a time frame after which to **Remove Violators from Watchlist**.
- Add Policy Violators to Active List?:** Toggle to **YES** to complete the following information:



The 'Add Policy Violators to Active list?' configuration screen has a 'YES' toggle at the top left. It is divided into three main sections:

- Select Active list:** Includes a dropdown menu (currently showing '-Select-'), a '+ Create New Active List' button, and a green/red status indicator.
- Rule to use key in active list:** A large text area for defining rules. Below it, a note says: 'Please specify mapped attributes e.g. accountname+ipaddress', followed by examples: 'transactionstring(150)+accountname(1,3)' and 'emailsender()+filename'.
- Select attributes to be displayed in violation on SCC:** A list of attributes on the left (Account Blacklisted, Account Created Date, Account Disabled Date, Account Encrypted, Account Name, Account Whitelisted, Application Protocol, Approver Employee ID, Cost Centre Code, Cost Centre Name) and a set of navigation buttons (>, >>, <<, <) to move them to a selection box on the right.

- Select Active list:** Select from dropdown or Create New Active List as described in [Check Against Active List](#).
- Rule to use key in active list:** Specify mapped attributes to include in the check as described in [Check Against Active List](#).
- Select attributes to be displayed in violation on SCC:** Use > or >> to add the attributes to include in the violation summary on the [Security Command Center](#).

e. **CEF Output:** Toggle to **Yes** to produce output in CEF format. If **Yes**:

a. **Select Connection** from dropdown.



Note: You must configure your connections for CEF output in [Connection Types](#) before you can export from ArcSight UBA.

b. Click **Output Mapping** to configure output.

CEF Field	Constant?	Mapped With
act	YES	deviceaction
app	YES	applicationprotocol
dhost	YES	destinationhostname
dpid	YES	destinationprocessid
dmac	YES	destinationmacaddress
dntdom	YES	destinationntdomain

Save

a. **CEF Field:** Specify field. Example: act.

b. **Constant?:** Toggle to **Yes** or **No**.

c. **Mapped With:** Enter a value using +/- to add/remove attributes.
Example: deviceaction

f. **RSA Archer CEF Output:** Toggle to **Yes** to produce output in CEF format. If **Yes**, see **CEF Output**.



Note: You must configure your connections for RSA Archer CEF output before you can export from ArcSight UBA.

g. **RSA Netwitness CEF Output:** Toggle to **Yes** to produce output in CEF format. If **Yes**, see **CEF Output**.



Note: You must configure your connections for RSA Netwitness CEF output before you can export from ArcSight UBA.

Violation Action

1. Complete the following steps to choose the action to be taken on the violations flagged by the policy:

VIOLATION ACTION
Daily Violation Threshold

When a violations exceeds the threshold, it will be skipped for scoring and saving.
Do you want to generate incident for policy violators?
☐ NO
Send Notification
☐ NO
Add Policy Violators to Watchlist?

Add Policy Violators to Active list?
☐ NO
CEF Output
☐ NO
RSA Archer CEF Output
☐ NO
RSA Netwitness CEF Output
☐ NO

- a. **Daily Violations Threshold:** Enter a value after which to stop flagging violations for the policy.
- b. **Do you want to generate cases for policy violators?:** Set to **YES** to generate a case for each policy violator.
Cases can also be created manually from the Security Command Center.
 - a. **Select workflow to trigger when generating cases:** Set to **Yes** to select a workflow from the dropdown.

- c. **CEF Output:** Toggle to **Yes** to produce output in CEF format. If **Yes**:

- a. **Select Connection** from dropdown.



Note: You must configure your connections for CEF output in [Connection Types](#) before you can export from ArcSight UBA.

- b. Click **Output Mapping** to configure output.

Output Field Mapping
×

CEF Field	Constant?	Mapped With	
<input type="text" value="act"/>	<input checked="" type="checkbox"/> YES	<input type="text" value="deviceaction"/>	+ -
<input type="text" value="app"/>	<input checked="" type="checkbox"/> YES	<input type="text" value="applicationprotocol"/>	+ -
<input type="text" value="dhost"/>	<input checked="" type="checkbox"/> YES	<input type="text" value="destinationhostname"/>	+ -
<input type="text" value="dpid"/>	<input checked="" type="checkbox"/> YES	<input type="text" value="destinationprocessid"/>	+ -
<input type="text" value="dmac"/>	<input checked="" type="checkbox"/> YES	<input type="text" value="destinationmacaddress"/>	+ -
<input type="text" value="dntdom"/>	<input checked="" type="checkbox"/> YES	<input type="text" value="destinationntdomain"/>	+ -

Save

- a. **CEF Field:** Specify field. Example: act.
- b. **Constant?:** Toggle to **Yes** or **No**.
- c. **Mapped With:** Enter a value using **+/-** to add/remove attributes.
Example: deviceaction
- d. **RSA Archer CEF Output:** Toggle to **Yes** to produce output in CEF format. If **Yes**, see **CEF Output**.



Note: You must configure your connections for RSA Archer CEF output before you can export from ArcSight UBA.

- e. **RSA Netwitness CEF Output:** Toggle to **Yes** to produce output in CEF format. If **Yes**, see **CEF Output**.



Note: You must configure your connections for RSA Netwitness CEF output before you can export from ArcSight UBA.

3. Click **Save** to proceed to [Viewing, Enabling, and Editing Policies](#).
4. View or search for violations on Spotter:
 1. Navigate to **Menu > Security Center > Spotter** or click **F2**.
 2. Click the policy name from **Available Violations** or the datasource from **Available Data-sources** to view events.

The screenshot shows the Spotter interface with a search bar at the top containing "resourcegroupname = 'Citrix VPN'". Below the search bar, there are tabs for SUMMARY, SEARCH RESULTS, CACHED QUERIES, SAVED QUERIES, CONSOLE, and VIEW JOBS. The main area is divided into two sections: AVAILABLE VIOLATIONS and AVAILABLE DATASOURCES. In the AVAILABLE VIOLATIONS section, "Landspeed Violation - VPN" is highlighted with a red box, showing a count of 2. In the AVAILABLE DATASOURCES section, "Citrix VPN" is highlighted with a red box, showing a total of 317,468 events.

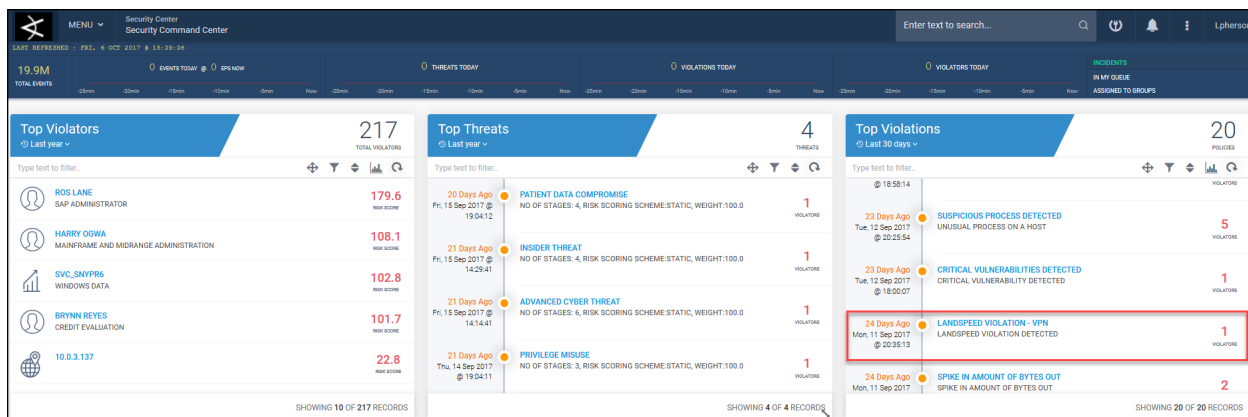
OR

Search Spotter using the following syntax: `policyname=" [policyname] "`.

The screenshot shows the Spotter interface with a search bar at the top containing "policyname = 'Landspeed Violation - VPN'". Below the search bar, there are tabs for SUMMARY, SEARCH RESULTS, CACHED QUERIES, SAVED QUERIES, CONSOLE, and VIEW JOBS. The main area displays a timeline graph and a list of search results. The first result is highlighted with a red box, showing details for a Landspeed Violation - VPN event. The event details include: accountname = MARA ROONEY, transactionstring1 = default SSLVPN LOGIN, ipaddress = 129.112.28.171, sourceport = 57261, resourcegroupname = Citrix VPN, resource = Citrix VPN, destinationaddress = 10.1.2.123, destinationport = 37422, eventcity = Dallas, eventcountry = US, eventaltitude = 32.8326, eventlongitude = -96.8467, eventregion = TX, category = ACCOUNT MISUSE, policyname = Landspeed Violation - VPN, riskthreatname = Landspeed Violation Detected, violator = Activityaccount, companycode = PAY, costcentername = IACCD06, country = USA, department = Payroll Processing, division = Corporate Human Resources, employeeid = 1691, employeetype = FT, employeetypedescription = FullTime, firstname = Mara, hiredate = 06/12/2009 00:00:00.000, jobcode = R6, landid = MR1691, lastname = Rooney, location = Indianapolis, manageremployeeid = 1083, status = 1, statusdescription = Active, title = Associate Payroll Processing Admin, workemail = Mara.Rooney@scnx.com, workphone = 294-680-8318, approveremployeeid = 1090, mobile = 020 8681 5800, userlocality = Low, companynumber = PAY6, province = KS, street = 6900 COLLEGE BLVD, regtempln = Regular, costcentercode = IACCD06, networkid = MRooney, zipcode = 66211, orgunitnumber = 6, city = OVERLAND PARK, managerfirstname = GRIFFIN, fulltimeparttime = PartTime, userriskscore = 0.01, usertimezoneoffset = CST.

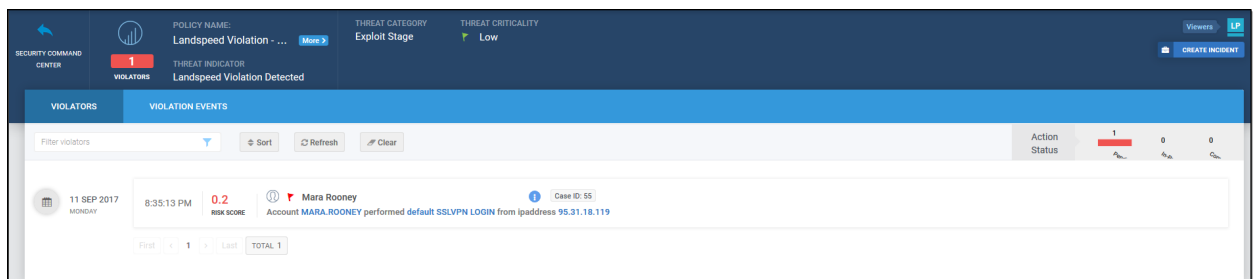
5. Find violations in the Security Command Center:

1. Navigate to **Menu > Security Center > Security Command Center** or click ArcSight UBA logo.

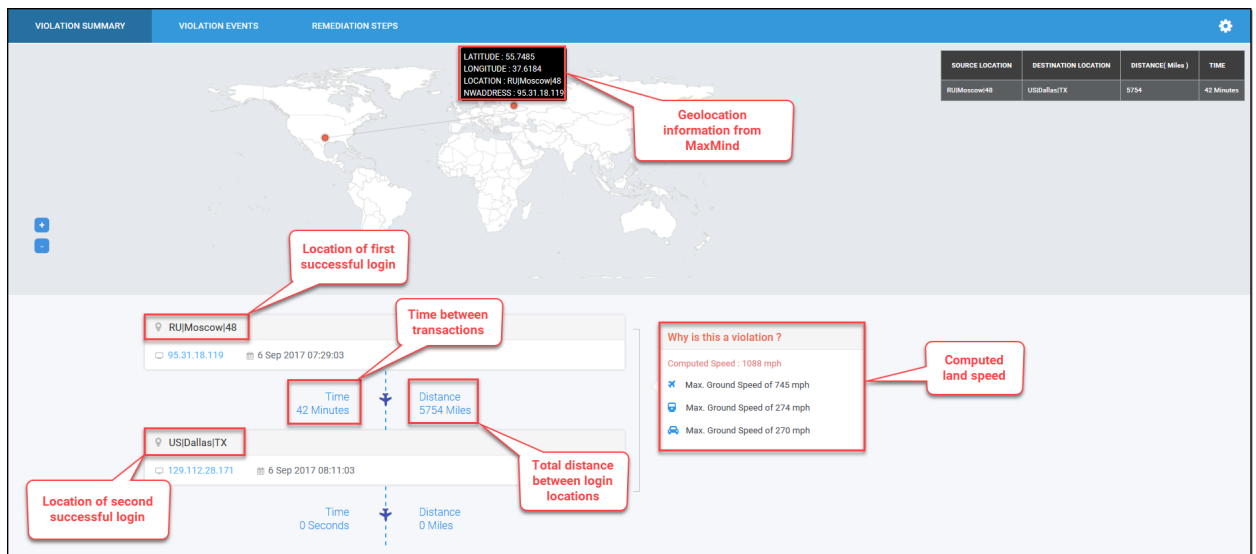


Note: Policies will only appear in the Security Command Center if violations exist for

2. Click the policy name to view activity accounts associated with the violations.
For more information about this screen, see [Policies](#).



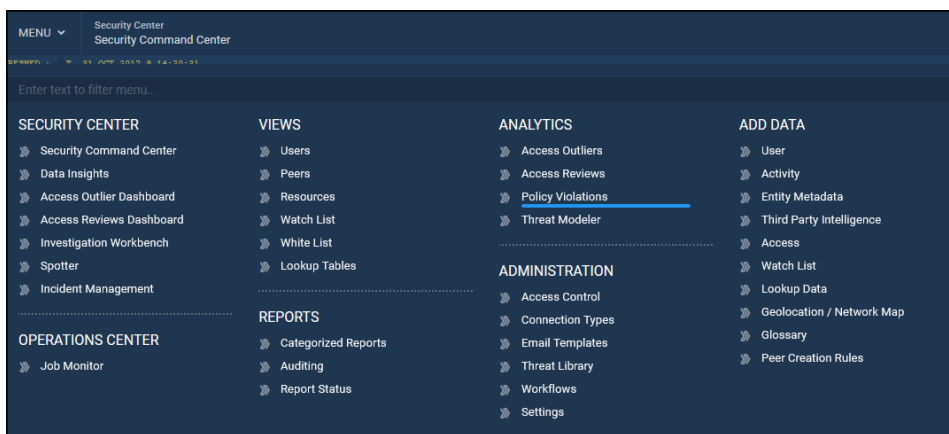
3. Click the violator name to view the a summary of the violation.



Example Directives-Based Policy: Flight Risk User - Job Search

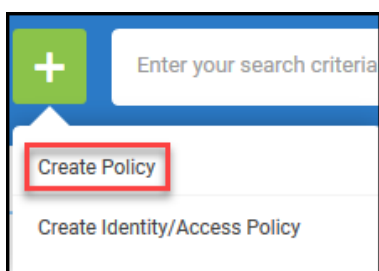
This directives-based policy uses web proxy to detect when users exhibit exiting behaviors such as searching for jobs."

1. Navigate to **Menu > Analytics > Policy Violations**:



2. Click +.

3. Select **Create Policy**.



Enter Policy Details

In this section, configure the policy name, criticality, entity against which the policy will run, and the datasource to which the policy will be applied, as well as designating the owner and remediator of the policy in order to restrict what users may view the policy violations. Define the category and indicator of threat.

Define Policy

Complete the following information:

DEFINE POLICY

Policy Name*

Provide unique name which will describe what type of violation it detects. Special characters are not allowed. Example: (- (bracket), ' - (single quote) are not allowed

Description

Criticality

None

Select the criticality of the policy. The criticality affects the risk score for the user. None=0.0, Low=0.2, Medium=0.6 and High=1.0

Do you want to save violations and calculate risk scores for this policy?

YES

If Yes, violations will be searchable in Spotter and risk scores will be calculated for violators. If No, violations will not be searchable and risk scores will not be calculated for violators of this policy.

Do you want to escalate this policy as a Threat?

YES

If Yes, this policy will be escalated as a Threat instead of a Violation and will appear under Top Threats in Security Command Center. If no, this policy will appear under the Top Violations widget.

Select Violation Entity*

Activity Account

Select the entity that the risk should apply to?

Users - Returns list of users violating policy. Orphan accounts(or uncorrelated accounts) will be ignored.

ActivityAccount - Returns list of activity accounts (both correlated and uncorrelated) violating the policy.


Resources - Returns list of resources violating the policy.

Do you want to run the policy on a

Datasource
Functionality

Bluecoat Proxy [Bluecoat Proxy]

- Policy Name:** Provide a unique name to describe the policy: Flight Risk Users - Job Search
- Description:** Enter a brief description of the policy. Example: Detect users exhibiting flight risk behavior.
- Criticality:** Use slider to select the criticality of the policy: None.


Note: This will affect the risk score for the user. None=0.0, Low=0.2, Medium=0.6, and High=1.0.
- Do you want to save violations and calculate risk scores for this policy?:** Toggle to **YES** to make violations for this policy searchable in Spotter and to calculate risk scores for violators. If disabled, violations will not be searchable and risk scores will not be calculated.

- e. **Do you want to escalate this policy as a Threat?:** Toggle to **YES** to escalate the policy to a threat rather than a policy violation. Violations will appear under Top Threats in the Security Command Center. If **NO**, view violations will appear in the Top Violations dashboard.
- f. **Select Violation Entity:** Select from dropdown: Activity Account.
 - **Activity Account:** Returns list of activity accounts (both correlated and uncorrelated) violating policy.
- g. **Do you want to run the policy on a:** Select **Datasource** to use the dropdown to select the datasource on which the policy should run: Bluecoat proxy.

Additional Details

ADDITIONAL DETAILS

Owner

Select the owner of the policy. This can be used for sending notifications and case management. The category widget on the security dashboard is visible to policy owners.

Remediator

Select the remediator for the policy. The remediator can be sent notifications and used in case management.

- a. **Owner:** Click search icon to select an owner for the policy: None selected.
- b. **Remediator:** Click search icon to select a remediator for the policy: None selected.

Define Risk and Threat

1. Complete the following information:

DEFINE RISK AND THREAT

Category*

Create New Policy Category

DATA EXFILTRATION ▼ + -

Category is displayed on dashboard as a widget and risk will be aggregated for policies with the same category. All violations of the same category will be available in the widget.

Threat Indicator*

Create New Threat Indicator Edit Killchain Stage and Response Actions

Possible Flight Risk Users ▼

Violations detected are indicative of threat

- Category:** Select from dropdown: Data Exfiltration.
 - Threat Indicator:**
 - Select from dropdown: Possible Flight Risk Users.

OR

 - Create New Threat Indicator** as described in [Creating Policies](#).
2. Click **Save & Next** to proceed to [Provide Conditions](#).

Provide Conditions

What do you want to detect?

Select **Aggregated Event Analytics**.

WHAT DO YOU WANT TO DETECT ?

Individual Event Analytics : Detects activities with specified criteria. Example : If user from 'x' country login to 'y' server and modify 'z' file.

RARE BEHAVIOR SPIKE IN NUMBER OF OCCURRENCES SPIKE IN VOLUME/AMOUNT ENUMERATION BEHAVIOR ABNORMAL ACTIVITY COMPARED TO PEERS **INDIVIDUAL EVENT ANALYTICS**

BATCHED ANALYTICS

Criteria to Filter Conditions

1. Click **+** to select **Add Rule** under Filter Conditions.
2. Use dropdowns to create the following rules:

The screenshot shows a web interface titled "CRITERIA TO FILTER EVENTS". At the top, there is a grey header bar with the title. Below the header, a light blue box contains an information icon and the text: "Conditions contains either set of rules or set of subgroups. Set of Groups and Rules will decide which data will be marked as violation." Below this, there is a list of criteria. A green plus icon is visible next to the first criterion. The first criterion is displayed as a row with the following elements: "Device Event Category", a grey button labeled "CONTAINS", the value "job", and two buttons labeled "EDIT" (in blue) and "DELETE" (in red). At the bottom left of the criteria list, there is a green button labeled "+ ADD GROUP".

1. **Attribute:** Device Event Category | **Condition:** Contains | **Value:** job

Directives

1. Click **+ Add**.
2. Configure the following directive:

Details

Name

FlightRisk

Do you want to filter events based on certain

Filter for Events matching criteria?

☒ YES

Do you want to filter events based on certain criteria?

Attribute	Condition	Value	
Device Event Category	Contains	job	AND

Filter for Amount matching criteria?

☐ NO

Do you want to filter events based on certain amount criteria?

Having similar

Account Name

Events will have same attribute value selected

Number of Occurrences

Atleast 3 Within Duration 23:59:59

The rate at which event occurs or is repeated over a particular period of time.

- **Name:** FlightRisk
- **Filter for Events Matching Criteria?:** YES.
- **Attribute:** Device Event Category | **Condition:** Contains | **Value:** job
- **Filter for Amount matching criteria?:** NO.
- **Having similar:** Account Name.
- **Number of Occurrences:** Atleast 3.
- **Within Duration:** 23:59:59
- **Should events happen consecutively?:** NO.
- **Distinct?:** NO.

3. Click **Save**.

4. Click Save & Next to proceed to [Choose Action for Violation Results](#).

Choose Action for Violation Results

In this section, determine what actions the application will take for violations of this policy. Create actions to generate cases, assign workflow, export data in CEF format, and configure a violation summary to specify what attributes to include in the Violation Summary for [Policies](#).

1. **Configure Your Violation Summary:** Complete the following information to appear on the Violation Summary screen that can be accessed from the [Security Command Center](#).

CONFIGURE THE VIOLATION INFORMATION SUMMARY

1 Based on selected attributes, violation summary will be generated that can be viewed on **Summary** from the Security Command center.

Account \${accountname!ACCOUNTNAME} performed \${transactionstring1!ACTIVITY} from ipaddress \${ipaddress!UNKNOWN}

VIOLATOR

GROUPING ATTRIBUTE

CATEGORY

Metadata Attributes

1 METHOD

2 RESPONSE_CODE

3 SELECT

Level 2 Attribute

Destination Domain

Metadata Attributes

1 URL

2 SELECT

3 SELECT

- a. **Provide the verbose template for violation summary:** Enter a verbose template to specify custom attributes to display in the violation summary (optional.) Example: Account \${accountname!"ACCOUNTNAME"} performed \${transactionstring1!"ACTIVITY"} from ipaddress \${ipaddress!"UNKNOWN"}.



Note: You must include the ! in the attribute. For example: \${resource! "Unknown"} initiated a suspicious process will work but \${resource} initiated a suspicious process will not. For a complete list of available attributes, see [Appendix C: Verbose Template Attributes](#).

- b. **Grouping Attribute:** Select an attribute under which to group the information in the summary. Example: Category.
 - c. **Metadata Attributes:** Select up to three metadata attributes to view within the grouping attribute in the summary. Example: Method, Response_Code.
 - d. **Level 2 Attribute:** Select a high-level attribute to view independent of the Grouping Attribute. Example: Destination Domain.
 - e. **Level 2 Metadata Attributes:** Select up to three metadata attributes for the Level 2 Attribute. Example: URL.
2. Complete the following steps to choose the action to be taken on the violations flagged by the policy:

VIOLATION ACTION

Daily Violation Threshold

When a violations exceeds the threshold, it will be skipped for scoring and saving.

Do you want to generate incident for policy violators?

☐ NO

Send Notification

☐ NO

Add Policy Violators to Watchlist?

Add Policy Violators to Active list?

☐ NO

CEF Output

☐ NO

RSA Archer CEF Output

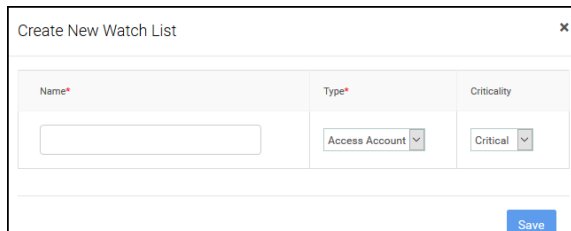
☐ NO

RSA Netwitness CEF Output

☐ NO

- a. **Daily Violations Threshold:** Enter a value after which to stop flagging violations for the policy.
- b. **Do you want to generate cases for policy violators?:** Set to **YES** to generate a case for each policy violator.
Cases can also be created manually from the Security Command Center.
 - a. **Select workflow to trigger when generating cases:** Set to **Yes** to select a workflow from the dropdown.
- c. **Send Notification:** Toggle to **YES** to **Select Email Template** from dropdown to receive notifications of violations for this policy.

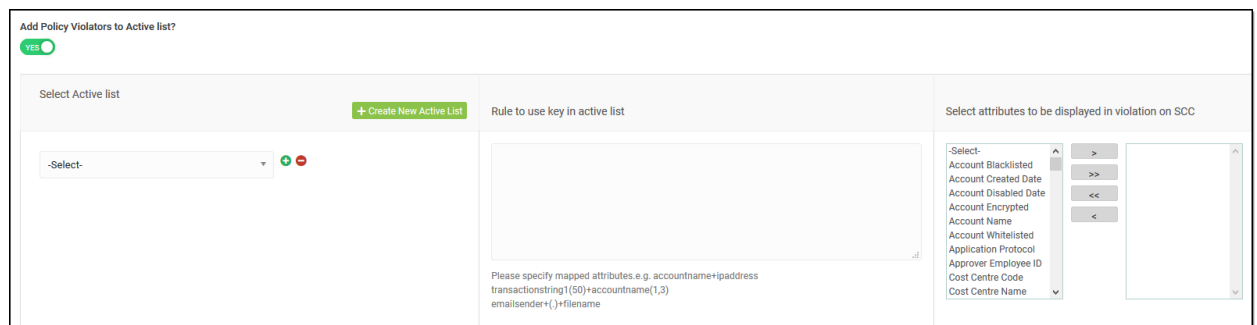
- d. **Add Policy Violators to Watchlist?:** Select from dropdown or **Create a New Watchlist**.



The 'Create New Watch List' dialog box contains three input fields: 'Name*' (a text box), 'Type*' (a dropdown menu with 'Access Account' selected), and 'Criticality' (a dropdown menu with 'Critical' selected). A 'Save' button is located at the bottom right.

Complete the following:

- Confidence Factor:** Enter a value from 0 to 1 to indicate how confident you are the violator should be on the watchlist.
- Confidence Incremental Factor:** Enter a value from 0 to 1 to indicate how confident you are the violation should be on the watchlist for each subsequent violation.
- Rule to Remove Violators from Watchlist:** Enable to specify a time frame after which to **Remove Violators from Watchlist**.
- Add Policy Violators to Active List?:** Toggle to **YES** to complete the following information:



The 'Add Policy Violators to Active list?' configuration screen has a 'YES' toggle at the top left. It is divided into three main sections:

- Select Active list:** Includes a dropdown menu (currently showing '-Select-'), a '+ Create New Active List' button, and a green/red status indicator.
- Rule to use key in active list:** A large text area for defining rules. Below it, a note says: 'Please specify mapped attributes e.g. accountname+ipaddress', followed by examples: 'transactionstring(150)+accountname(1,3)' and 'emailsender()+filename'.
- Select attributes to be displayed in violation on SCC:** A list of attributes on the left (Account Blacklisted, Account Created Date, Account Disabled Date, Account Encrypted, Account Name, Account Whitelisted, Application Protocol, Approver Employee ID, Cost Centre Code, Cost Centre Name) and a set of navigation buttons (>, >>, <<, <) to move them to a selection box on the right.

- Select Active list:** Select from dropdown or Create New Active List as described in [Check Against Active List](#).
- Rule to use key in active list:** Specify mapped attributes to include in the check as described in [Check Against Active List](#).
- Select attributes to be displayed in violation on SCC:** Use > or >> to add the attributes to include in the violation summary on the [Security Command Center](#).

e. **CEF Output:** Toggle to **Yes** to produce output in CEF format. If **Yes**:

a. **Select Connection** from dropdown.



Note: You must configure your connections for CEF output in [Connection Types](#) before you can export from ArcSight UBA.

b. Click **Output Mapping** to configure output.

CEF Field	Constant?	Mapped With
act	YES	deviceaction
app	YES	applicationprotocol
dhost	YES	destinationhostname
dpid	YES	destinationprocessid
dmac	YES	destinationmacaddress
dntdom	YES	destinationntdomain

Save

a. **CEF Field:** Specify field. Example: act.

b. **Constant?:** Toggle to **Yes** or **No**.

c. **Mapped With:** Enter a value using +/- to add/remove attributes.
Example: deviceaction

f. **RSA Archer CEF Output:** Toggle to **Yes** to produce output in CEF format. If **Yes**, see **CEF Output**.



Note: You must configure your connections for RSA Archer CEF output before you can export from ArcSight UBA.

g. **RSA Netwitness CEF Output:** Toggle to **Yes** to produce output in CEF format. If **Yes**, see **CEF Output**.



Note: You must configure your connections for RSA Netwitness CEF output before you can export from ArcSight UBA.

3. Navigate to **Menu > Security Center > Spotter** or click **F2**.

Click the policy name from **Available Violations** or the datasource from **Available Data-sources** to view events.

The screenshot displays the ArcSight Security Center Spotter interface. The top navigation bar includes a search bar, a filter for 'Last 1 hours', and a search icon. Below the navigation bar, there are tabs for SUMMARY, SEARCH RESULTS, CACHED QUERIES, SAVED QUERIES, CONSOLE, and VIEW JOBS. The main content area is divided into two panels: 'AVAILABLE VIOLATIONS' on the left and 'AVAILABLE DATASOURCES' on the right. The 'AVAILABLE VIOLATIONS' panel shows a list of violations with their counts. The 'AVAILABLE DATASOURCES' panel shows a list of datasources with their event counts. Both panels have a 'TOTAL' count at the top right.

AVAILABLE VIOLATIONS	TOTAL VIOLATED EVENTS
Spike in amount of bytes out	1,180
Robotic beaconing traffic detected	379
Spam Email	193
Spike in Number of Records accessed by an Employee	120
Critical vulnerabilities detected	114
Excessive number of emails to personal email address	104
Flight Risk User - Job Search	31
File Copy Blocked By DLP	23
Potential Data Snooping Activity	18
Suspicious Process Detected	5
LandSpeed Violation - VPN	2
Privilege Escalation	2
Rare Login to Critical Server	1

AVAILABLE DATASOURCES	TOTAL EVENTS
Unix Data	6,238,743
Infoblox	5,930,539
Digital Guardian Send Mail	5,561,322
Bluecoat Proxy	1,039,572
Windows Data	711,524
Citrix VPN	317,468
Windchill Data	158,453
Google Login	24,282
Nessus Data	9,436
Cerner Healthcare Data	2,824
Ironport Data	1,103
Digital Guardian USB	24

OR

Search Spotter using the following syntax: `polycname=" [polycname] "`.

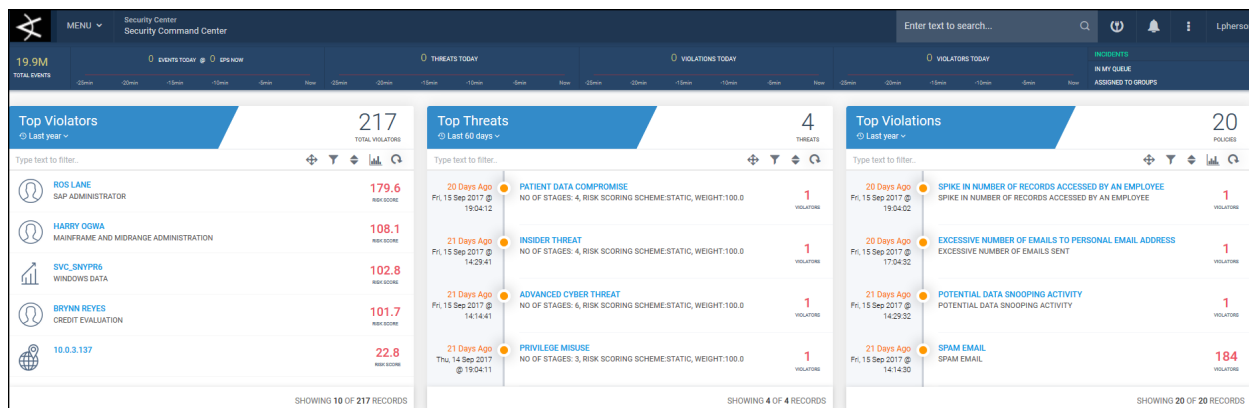
The screenshot displays the ArcSight Security Center Spotter interface showing search results for the policy 'Flight Risk User - Job Search'. The top navigation bar includes a search bar with the query 'polycname="Flight Risk User - Job Search"', a filter for 'Last 90 days', and a search icon. Below the navigation bar, there are tabs for SUMMARY, SEARCH RESULTS, CACHED QUERIES, SAVED QUERIES, CONSOLE, and VIEW JOBS. The main content area is divided into two panels: a left panel for 'Selected Fields' and a right panel for 'Search Results'. The 'Selected Fields' panel shows a list of fields including DEVICE, SOURCE ACCOUNT, and TRANSACTION. The 'Search Results' panel shows a list of search results with their details. The first result is highlighted with a red box.

Selected Fields
DEVICE
SOURCE ACCOUNT
TRANSACTION

Search Results
<p>WED, 30 AUG 2017 @ 08:35:51 PM resourcegroupname: Bluecoat Proxy polycname: Flight Risk User - Job Search</p> <p>accountname = OGWA.HARRY , bytesin = 6946 , bytesout = 488 , destinationservice = none , eventoutcome = 200 , message = allowed , applicationprotocol = ssl , ipaddress = 10.0.1.61 , sourceaddress = 10.91.252.94 , resourcegroupname = Bluecoat Proxy , resource = Bluecoat Proxy , destinationaddress = 10.91.252.94 , destinationhostname = https://quintiles.taleo.net , destinationdomain = , destinationport = 8443 , requesturl = https://quintiles.taleo.net/careersection/10080/jobdetail.ftit?job=1704064&lang=en&src=JB-11S , filetype = , customnumber1 = 16200 , customstring2 = unavailable , categorybehavior = communication , categoryobject = device , deviceeventcategory = Job Search</p> <p>category = ACCOUNT MISUSE , polycname = Flight Risk User - Job Search , riskthreatname = Possible Flight Risk Users , violator = Activityaccount</p> <p>companycode = TECH , costcentername = INFCCC12 , country = USA , department = Mainframe and Midrange Administration , division = Global Technology , employeid = 1001 , employetype = FT , employetypedescription = FullTime , firstname = HARRY , hiredate = 08/08/2009 00:00:00.000 , jobcode = RT , land = HO1001 , lastname = OGWA , location = DALLAS , manageremployeid = 1012 , middlename = A , status = 1 , statusdescription = Active , title = Vice President Mainframe and Midrange , workemail = HARRY.OGWA@scnx.com , workphone = 9723451278</p> <p>approveremployeid = 1082 , mobile = 0151 709 7593 , lastperformanceevaluationdate = 04/01/2014 00:00:00.000 , usercriticality = Low , companynumber = TECH12 , province = FL , street = 9000 SOUTHSIDE BLVD BLDG 600 , regtempin = Regular , lastperformanceevaluationresult = Poor , costcentercode = INFCCC12 , networkid = HOGWA , zipcode = 32256 , orgunitnumber = 12 , city = JACKSONVILLE , managerfirstname = Joe , fulltimeparttimein = FullTime , userriskscore = 0.01 , usertimezoneoffset = CST</p>

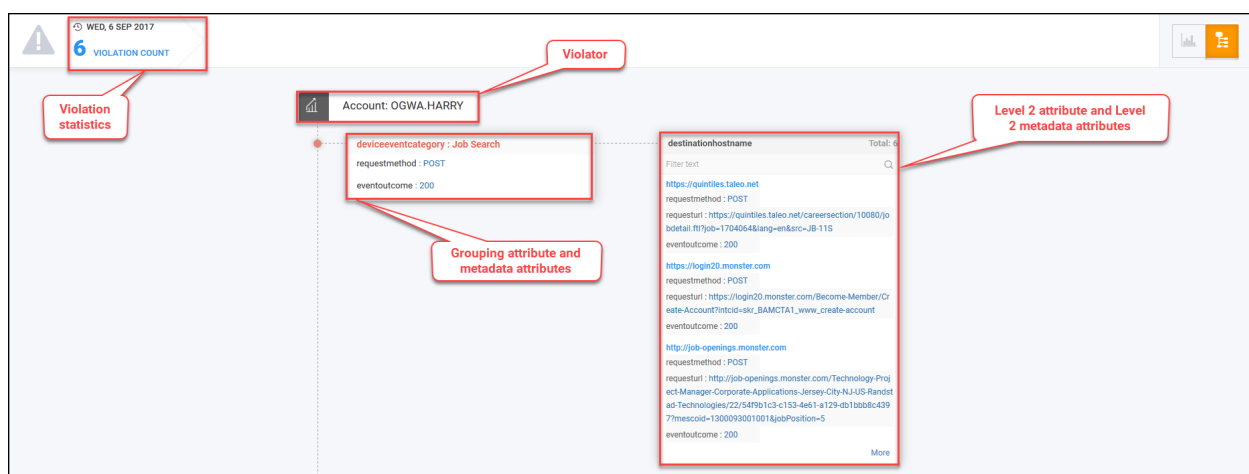
4. Find violations in the Security Command Center:

1. Navigate to **Menu > Security Center > Security Command Center** or click ArcSight UBA logo.



Note: Policies will only appear in the Security Command Center if violations exist for those policies.

2. Click the policy name to view activity accounts associated with the violations.
3. Click the violator name to view the a summary of the violation.

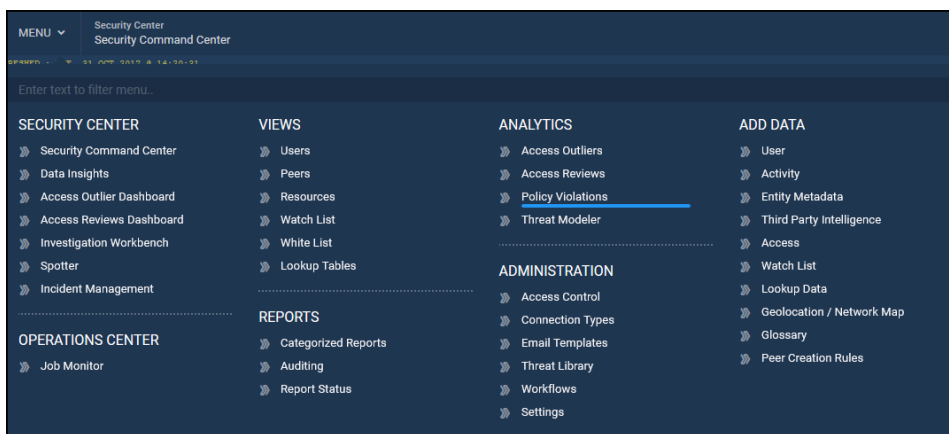


For more information about this screen, see [Policies](#).

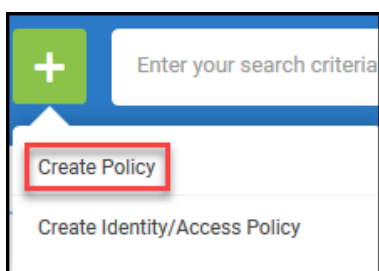
Example Behavior-Based Policy: Abnormal amount of data uploads compared to past behavior

This behavior-based policy uses web proxy data to detect when users have uploaded an abnormally high volume of data compared to their normal baseline behavior.

1. Navigate to **Menu > Analytics > Policy Violations**:



2. Click +.
3. Select **Create Policy**.



Enter Policy Details

In this section, configure the policy name, criticality, entity against which the policy will run, and the datasource to which the policy will be applied, as well as designating the owner and remediator of the policy in order to restrict what users may view the policy violations. Define the category and indicator of threat.

Define Policy

Complete the following information:

DEFINE POLICY

Policy Name*

Provide unique name which will describe what type of violation it detects. Special characters are not allowed. Example: (- (bracket), ' - (single quote) are not allowed

Description

Criticality

Low

Select the criticality of the policy. The criticality affects the risk score for the user. None=0.0, Low=0.2, Medium=0.6 and High=1.0

Do you want to save violations and calculate risk scores for this policy?
☒ YES ☐ NO

If Yes, violations will be searchable in Spotter and risk scores will be calculated for violators. If No, violations will not be searchable and risk scores will not be calculated for violators of this policy.

Do you want to escalate this policy as a Threat?
☒ YES ☐ NO

If Yes, this policy will be escalated as a Threat instead of a Violation and will appear under Top Threats in Security Command Center. If no, this policy will appear under the Top Violations widget.

Select Violation Entity*

Select the entity that the risk should apply to?

"Users" - Returns list of users violating policy. Orphan accounts(or uncorrelated accounts) will be ignored.


"ActivityAccount" - Returns list of activity accounts (both correlated and uncorrelated) violating the policy.

"Resources" - Returns list of resources violating the policy.

Do you want to run the policy on a

☒ Datasource
☐ Functionality

- Policy Name:** Provide a unique name to describe the policy: Abnormal amount of data uploads compared to past behavior.
- Description:** Enter a brief description of the policy. Example: This check determines abnormally high volume of uploads by employees compared to their normal baseline behavior.
- Criticality:** Use slider to select the criticality of the policy: Low.


Note: This will affect the risk score for the user. None=0.0, Low=0.2, Medium=0.6, and High=1.0.
- Do you want to save violations and calculate risk scores for this policy?:** Toggle to **YES** to make violations for this policy searchable in Spotter and to calculate risk scores for violators. If disabled, violations will not be searchable and risk scores will not be calculated.

- e. **Do you want to escalate this policy as a Threat?:** Toggle to **YES** to escalate the policy to a threat rather than a policy violation. Violations will appear under Top Threats in the Security Command Center. If **NO**, view violations will appear in the Top Violations dashboard.
- f. **Select Violation Entity:** Select from dropdown: Activity Account.
 - **Activity Account:** Returns list of activity accounts (both correlated and uncorrelated) violating policy.
- g. **Do you want to run the policy on a:** Select **Datasource** to use the dropdown to select the datasource on which the policy should run: Bluecoat proxy.

Additional Details

ADDITIONAL DETAILS

Owner

Select the owner of the policy. This can be used for sending notifications and case management. The category widget on the security dashboard is visible to policy owners.

Remediator

Select the remediator for the policy. The remediator can be sent notifications and used in case management.

- a. **Owner:** Click search icon to select an owner for the policy: None selected.
- b. **Remediator:** Click search icon to select a remediator for the policy: None selected.

Define Risk and Threat

1. Complete the following information:

DEFINE RISK AND THREAT

Category*

Create New Policy Category

DATA EXFILTRATION - 1.0

+

-

Category is displayed on dashboard as a widget and risk will be aggregated for policies with the same category. All violations of the same category will be available in the widget.

Threat Indicator*

Create New Threat Indicator

Edit Killchain Stage and Response Actions

Abnormal amount of data uploads compared to past behavior

Violations detected are indicative of threat

- a. **Category:** Select from dropdown: Data Exfiltration.
- b. **Threat Indicator:** Abnormal amount of data uploads compared to past behavior
 - a. Select from dropdown.
OR
 - b. **Create New Threat Indicator** as described in [Creating Policies](#).

2. Click **Save & Next** to proceed to Provide Conditions.

Provide Conditions

What do you want to detect?

Select **Rare Behavior**.

WHAT DO YOU WANT TO DETECT ?

i Rare Behavior : Detects rare events compared to past behavior. Example : If an account uses ip address which

RARE BEHAVIOR SPIKE IN NUMBER OF OCCURRENCES SPIKE IN VOLUME/AMOUNT ENUMERATION BEHAVIOR

BATCHED ANALYTICS

CHOOSE THE FEATURES FOR GENERATING BEHAVIOR

☒ destinationhostnameecountry
☒ Filetype
☒ Method
☒ sourcehostnamelongitude
☒ Process_Name
☒ resourcehostnamepostalcode
☒ sessionid
☒ eventlatitude
☒ Response_Code
☒ Referer
☒ destinationhostnamepostalcode
☒ resourcehostnameecountry
☒ destinationhostnameecity
☒ destinationhostnameecountry

☐ Bytes_Sent

Select the attributes from above panel Selected features

Choose the Features for Generating Behavior

Click **Bytes_Sent** to select the feature for generating the behavior profile.

CHOOSE THE FEATURES FOR GENERATING BEHAVIOR

☒ destinationhostnameecountry
☒ Filetype
☒ Method
☒ sourcehostnamelongitude
☒ Process_Name
☒ resourcehostnamepostalcode
☒ sessionid
☒ eventlatitude
☒ Response_Code
☒ Referer
☒ destinationhostnamepostalcode
☒ resourcehostnameecountry
☒ destinationhostnameecity
☒ destinationhostnameecountry

☒ Bytes_Sent

Select the attributes from above panel Selected features

Behavior Information

Provide a unique **Behavior Name**. Example: BP_High_Amount_Uploads_volume-1

What should get flagged as violations?

Set **Flag as Violations when Rarity crosses Sigma Threshold Value** to **0.85 (Highly Rare)**.


WHAT SHOULD GET FLAGGED AS VIOLATIONS ?

Number of occurrences of selected features is unusually higher than behavior baseline for :

- ☐ First use of IPAddress by Account
- ☐ First use of Transaction by Account
- ☐ First use of IPAddress on Resource (Flag Account)
- ☐ First use of Transaction on Resource (Flag Account)
- ☐ First use of Account on Resource

Flag as Violations when Rarity crosses Sigma Threshold Value

Slightly Rare Highly Rare

 0.85

Criteria to Filter Events

Complete the following steps to add filter conditions for volume of uploads.

CRITERIA TO FILTER EVENTS

1 Conditions contains either set of rules or set of subgroups. Set of Groups and Rules will decide which data will be marked as violation.

+

bytesout GREATER THAN 1 EDIT DELETE

AND

eventoutcome EQUAL TO 200 EDIT DELETE

+

requestmethod EQUAL TO POST EDIT DELETE

OR

requestmethod EQUAL TO PUT EDIT DELETE

+

Device Event Category CONTAINS webmail EDIT DELETE

OR

Device Event Category CONTAINS uncategorized EDIT DELETE

OR

Device Event Category CONTAINS personal EDIT DELETE

OR

Device Event Category EQUAL TO storage EDIT DELETE

1. Click **+** to select **Add Rule** under Filter Conditions.
2. Use dropdowns to create the following rules:
 1. **Attribute:** bytesout | **Condition:** Greater Than | **Value:** 1
 2. **Attribute:** eventoutcome | **Condition:** Equal to | **Value:** 200
3. Click **+ Add Group** to add a new rule group.
4. Use dropdowns to create the following rules:
 1. **Attribute:** requestmethod | **Condition:** Equal to | **Value:** POST
 2. **Attribute:** requestmethod | **Condition:** Equal to | **Value:** PUT
5. Click **+ Add Group** to add a new rule group.
6. Use dropdowns to create the following rules:
 1. **Attribute:** Device Event Category | **Condition:** Contains | **Value:** webmail
 2. **Attribute:** Device Event Category | **Condition:** Contains | **Value:** uncategorized
 3. **Attribute:** Device Event Category | **Condition:** Contains | **Value:** personal
 4. **Attribute:** Device Event Category | **Condition:** Contains | **Value:** storage

Choose Action for Violation Results

In this section, determine what actions the application will take for violations of this policy. Create actions to generate cases, assign workflow, export data in CEF format, and configure a violation summary to specify what attributes to include in the Violation Summary for [Policies](#).

1. **Configure Your Violation Summary:** Complete the following information to appear on the Violation Summary screen that can be accessed from the [Security Command Center](#).

CONFIGURE THE VIOLATION INFORMATION SUMMARY

1 Based on selected attributes, violation summary will be generated that can be viewed on **Summary** from the Security Command center.

Account \${accountname!'ACCOUNTNAME'} performed \${transactionstring1!'ACTIVITY'} from ipaddress \${ipaddress!'UNKNOWN'}

VIOLATOR

GROUPING ATTRIBUTE

CATEGORY

Metadata Attributes

1 METHOD

2 RESPONSE_CODE

3 SELECT

Level 2 Attribute

Destination Domain

Metadata Attributes

1 URL

2 SELECT

3 SELECT

- a. **Provide the verbose template for violation summary:** Enter a verbose template to specify custom attributes to display in the violation summary (optional.) Example: Account \${accountname!'ACCOUNTNAME'} performed \${transactionstring1!'ACTIVITY'} from ipaddress \${ipaddress!'UNKNOWN'}.



Note: You must include the **!** in the attribute. For example: \${resource!name!'Unknown'} initiated a suspicious process **will work** but \${resource!name} initiated a suspicious process **will not**. For a complete list of available attributes, see [Appendix C: Verbose Template Attributes](#).

- b. **Grouping Attribute:** Select an attribute under which to group the information in the summary. Example: Category.
- c. **Metadata Attributes:** Select up to three metadata attributes to view within the grouping

- attribute in the summary. Example: Method, Response_Code.
- d. **Level 2 Attribute:** Select a high-level attribute to view independent of the Grouping Attribute. Example: Destination Domain.
 - e. **Level 2 Metadata Attributes:** Select up to three metadata attributes for the Level 2 Attribute. Example: URL.
2. Complete the following steps to choose the action to be taken on the violations flagged by the policy:

VIOLATION ACTION

Daily Violation Threshold

100000

When a violations exceeds the threshold, it will be skipped for scoring and saving.

Do you want to generate incident for policy violators?

☐ NO

Send Notification

☐ NO

Add Policy Violators to Watchlist?

Add Policy Violators to Active list?

☐ NO

CEF Output

☐ NO

RSA Archer CEF Output

☐ NO

RSA Netwitness CEF Output

☐ NO

1.

- a. **Daily Violations Threshold:** Enter a value after which to stop flagging violations for the policy.
- b. **Do you want to generate cases for policy violators?:** Set to **YES** to generate a case for each policy violator.

Cases can also be created manually from the Security Command Center.

- a. **Select workflow to trigger when generating cases:** Set to **Yes** to select a workflow from the dropdown.
- c. **Send Notification:** Toggle to **YES** to **Select Email Template** from dropdown to receive notifications of violations for this policy.
- d. **Add Policy Violators to Watchlist?:** Select from dropdown or **Create a New Watchlist**.

Complete the following:

- a. **Confidence Factor:** Enter a value from 0 to 1 to indicate how confident you are the violator should be on the watchlist.
- b. **Confidence Incremental Factor:** Enter a value from 0 to 1 to indicate how confident you are the violation should be on the watchlist for each subsequent violation.
- c. **Rule to Remove Violators from Watchlist:** Enable to specify a time frame after which to **Remove Violators from Watchlist**.
- e. **Add Policy Violators to Active List?:** Toggle to **YES** to complete the following information:

- a. **Select Active list:** Select from dropdown or Create New Active List as described in [Check Against Active List](#).
- b. **Rule to use key in active list:** Specify mapped attributes to include in the check as described in [Check Against Active List](#).
- c. **Select attributes to be displayed in violation on SCC:** Use > or >> to add the attributes to include in the violation summary on the [Security Command Center](#).
- e. **CEF Output:** Toggle to **Yes** to produce output in CEF format. If **Yes**:
 - a. **Select Connection** from dropdown.



Note: You must configure your connections for CEF output in [Connection Types](#) before you can export from ArcSight UBA.

- b. Click **Output Mapping** to configure output.

Output Field Mapping
✕

CEF Field	Constant?	Mapped With	
act	<input checked="" type="checkbox"/> YES	deviceaction	+ -
app	<input checked="" type="checkbox"/> YES	applicationprotocol	+ -
dhost	<input checked="" type="checkbox"/> YES	destinationhostname	+ -
dpid	<input checked="" type="checkbox"/> YES	destinationprocessid	+ -
dmac	<input checked="" type="checkbox"/> YES	destinationmacaddress	+ -
dntdom	<input checked="" type="checkbox"/> YES	destinationntdomain	+ -

Save

- a. **CEF Field:** Specify field. Example: act.
- b. **Constant?:** Toggle to **Yes** or **No**.
- c. **Mapped With:** Enter a value using +/- to add/remove attributes.
Example: deviceaction
- f. **RSA Archer CEF Output:** Toggle to **Yes** to produce output in CEF format. If **Yes**, see **CEF Output**.



Note: You must configure your connections for RSA Archer CEF output before you



can export from ArcSight UBA.

- g. **RSA Netwitness CEF Output:** Toggle to **Yes** to produce output in CEF format. If **Yes**, see **CEF Output**.



Note: You must configure your connections for RSA Netwitness CEF output before you can export from ArcSight UBA.

3. View or search for violations on Spotter:

1. Navigate to **Menu > Security Center > Spotter** or click **F2**.
2. Click the policy name from **Available Violations** or the datasource from **Available Data-sources** to view events.

OR

Search Spotter using the following syntax: `polycyname="[polycyname]"`.

4. Find violations in the Security Command Center:

1. Navigate to **Menu > Security Center > Security Command Center** or click ArcSight UBA logo.



Note: Policies will only appear in the Security Command Center if violations exist for those policies.

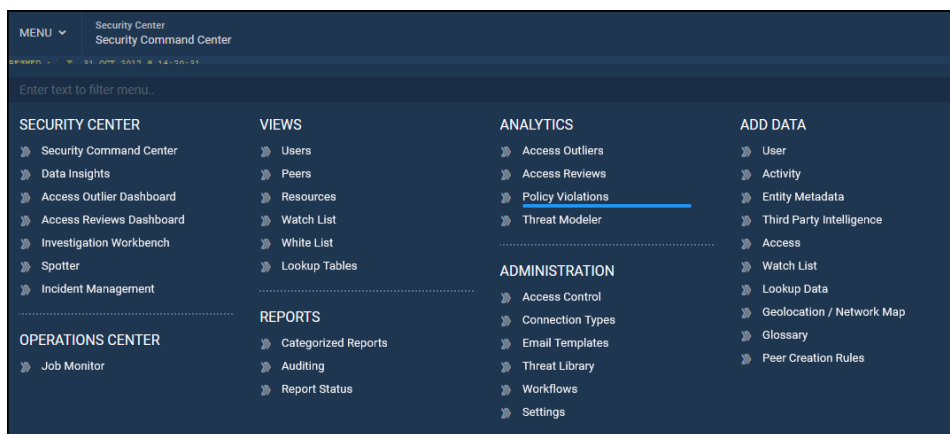
2. Click the policy name to view activity accounts associated with the violations.
3. Click the violator name to view the a summary of the violation.

For more information about this screen, see [Policies](#).

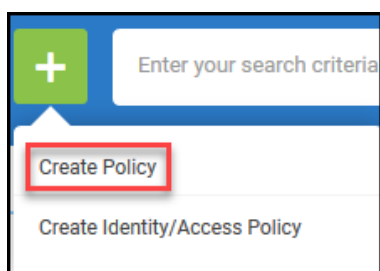
Example Peer-Based Activity Outlier Policy: Only Member in Peer Group Accessing Application

This behavior-based policy uses application data to detect when users have performed a health-care violation by accessing an application not accessed by the members of their peer group.

1. Navigate to **Menu > Analytics > Policy Violations**:



2. Click +.
3. Select **Create Policy**.



Enter Policy Details

In this section, configure the policy name, criticality, entity against which the policy will run, and the datasource to which the policy will be applied, as well as designating the owner and remediator of the policy in order to restrict what users may view the policy violations. Define the category and indicator of threat.

Define Policy

Complete the following information:

DEFINE POLICY

Policy Name*

Provide unique name which will describe what type of violation it detects. Special characters are not allowed. Example: (- (bracket), ' - (single quote) are not allowed

Description

Criticality

Low

Select the criticality of the policy. The criticality affects the risk score for the user. None=0.0, Low=0.2, Medium=0.6 and High=1.0

Do you want to save violations and calculate risk scores for this policy?

YES

If Yes, violations will be searchable in Spotter and risk scores will be calculated for violators. If No, violations will not be searchable and risk scores will not be calculated for violators of this policy.

Do you want to escalate this policy as a Threat?

YES

If Yes, this policy will be escalated as a Threat instead of a Violation and will appear under Top Threats in Security Command Center. If no, this policy will appear under the Top Violations widget.

Select Violation Entity*

Activity Account

Select the entity that the risk should apply to?

"Users" - Returns list of users violating policy. Orphan accounts(or uncorrelated accounts) will be ignored.

"ActivityAccount" - Returns list of activity accounts (both correlated and uncorrelated) violating the policy.


"Resources" - Returns list of resources violating the policy.

Do you want to run the policy on a

✓ Datasource
Functionality

Cerner Healthcare Data [Cerner Data]

- Policy Name:** Provide a unique name to describe the policy: Only Member in Peer Group Accessing Application.
- Description:** Enter a brief description of the policy. Example: This check compares behavior to behavior of members of peer group to determine if an activity account is accessing application not accessed by peers.
- Criticality:** Use slider to select the criticality of the policy: Low.


Note: This will affect the risk score for the user. None=0.0, Low=0.2, Medium=0.6, and High=1.0.
- Do you want to save violations and calculate risk scores for this policy?:** Toggle to **YES** to make violations for this policy searchable in Spotter and to calculate risk scores for violators. If disabled, violations will not be searchable and risk scores will not be calculated.

- e. **Do you want to escalate this policy as a Threat?:** Toggle to **YES** to escalate the policy to a threat rather than a policy violation. Violations will appear under Top Threats in the Security Command Center. If **NO**, view violations will appear in the Top Violations dashboard.
- f. **Select Violation Entity:** Select from dropdown: Activity Account.
 - **Activity Account:** Returns list of activity accounts (both correlated and uncorrelated) violating policy.
- g. **Do you want to run the policy on a:** Select **Datasource** to use the dropdown to select the datasource on which the policy should run: Cerner Healthcare Data.

Additional Details

ADDITIONAL DETAILS

Owner

Select the owner of the policy. This can be used for sending notifications and case management. The category widget on the security dashboard is visible to policy owners.

Remediator

Select the remediator for the policy. The remediator can be sent notifications and used in case management.

- a. **Owner:** Click search icon to select an owner for the policy: None selected.
- b. **Remediator:** Click search icon to select a remediator for the policy: None selected.

Define Risk and Threat

1. Complete the following information:

DEFINE RISK AND THREAT

Category*

Create New Policy Category

HEALTHCARE VIOLATION

+

-

Category is displayed on dashboard as a widget and risk will be aggregated for policies with the same category. All violations of the same category will be available in the widget.

Threat Indicator*

Create New Threat Indicator

Edit Killchain Stage and Response Actions

Account performing activity never conducted by peer

Violations detected are indicative of threat

- a. **Category:** Select from dropdown: Healthcare Violation.
- b. **Threat Indicator:**
 - a. Select from dropdown: Account performing activity never conducted by peer.
OR
 - b. **Create New Threat Indicator** as described in [Creating Policies](#).

2. Click **Save & Next** to proceed to Provide Conditions.

Provide Conditions

What do you want to detect?

Select **Abnormal Activity Compared to Peers**.

WHAT DO YOU WANT TO DETECT ?

1 Abnormal Activity Compared to Peers : Detects activity which is never performed by other peer members. Example : If user modifies files from other department and

RARE BEHAVIOR SPIKE IN NUMBER OF OCCURRENCES SPIKE IN VOLUME/AMOUNT ENUMERATION BEHAVIOR **ABNORMAL ACTIVITY COMPARED TO PEERS**

BATCHED ANALYTICS

CHOOSE THE FEATURES FOR GENERATING BEHAVIOR

☒ destinationhostnamecountry
☒ Filetype
☒ Method
☒ sourcehostnamelongitude
☒ Process_Name
☒ resourcehostnamepostalcode
☒ sessionid
☒ eventlatitude
☒ Response_Code
☒ Referer
☒ destinationhostnamepostalcode
☒ resourcehostnamecountry
☒ destinationhostnamecity

☒ sourcehostnamelongitude
☒ Process_Name
☒ eventlatitude
☒ destinationhostnamepostalcode
☒ Referer
☒ Response_Code
☒ Method
☒ Filetype

Select the attributes from above panel Selected features

Choose the Features for Generating Behavior

Click the following attributes to select the features for generating the behavior profile:

CHOOSE THE FEATURES FOR GENERATING BEHAVIOR

☒ Age
☒ Distance
☒ DEVICE
☒ Aging Baseline
☒ Distance Label
☒ ENCOUNTER_TYPE
☒ APPL_CTX
☒ ADMIT_DT_TM
☒ PATIENT_NAME
☒ AUDIT_SRC
☒ DEPARTMENT_SIZE
☒ Age Baseline
☒ EMPLOYEE_DEPARTMENT
☒ DISCHARGE_DT_TM

☒ EVENT_NAME
☒ APPLICATION
☒ EVENT_TYPE

Select the attributes from above panel Selected features

- **EVENT_NAME**
- **APPLICATION**
- **EVENT_TYPE**

Behavior Information

Provide a unique **Behavior Name**. Example: ApplicationAccessedByPeerGroupMember

What should get flagged as violations?

1. Select **Transaction performed by User not seen for other Peer Members** for **Number of occurrences of selected features is unusually higher than behavior baseline for:**
2. Set **Flag as Violations when Rarity crosses Sigma Threshold Value** to **0.15 (Slightly Rare)**.

WHAT SHOULD GET FLAGGED AS VIOLATIONS ?

Number of occurrences of selected features is unusually higher than behavior baseline for :

☒ Transaction performed by User not seen for other Peer Members
☐ Multiple Entities performing activity never conducted by other Peer Members before

☒ Department
☒ Division
☒ Location
☒ Title
☒ Job Code
☒ Manager

Department
Division

Select the peertypes from above panel Selected peertypes

Flag as Violations when Rarity crosses Sigma Threshold Value

Slightly Rare Highly Rare

0.15

Choose Action for Violation Results

In this section, determine what actions the application will take for violations of this policy. Create actions to generate cases, assign workflow, enable notifications, and configure a violation summary to specify what attributes to include in the Violation Summary for [Policies](#).

1. **Configure Your Violation Summary:** Complete the following information to appear on the Violation Summary screen that can be accessed from the [Security Command Center](#):

CONFIGURE THE VIOLATION INFORMATION SUMMARY

i Based on selected attributes, violation summary will be generated that can be viewed on **Summary** from the Security Command center.

VIOLATOR

GROUPING ATTRIBUTE

APPLICATION ▼

Metadata Attributes

1 EVENT_NAME ▼

2 SELECT ▼

3 SELECT ▼

Level 2 Attribute


PATIENT_NAME ▼

Metadata Attributes

1 PATIENT_ID ▼

2 SELECT ▼

3 SELECT ▼

- a. **Provide the verbose template for violation summary:** Enter a verbose template to specify custom attributes to display in the violation summary (optional.) Example: Account \${accountname!"ACCOUNTNAME"} performed \${transactionstring1!"ACTIVITY"} from ipaddress \${ipaddress!"UNKNOWN"}.
-  **Note:** You must include the **!** in the attribute. For example: \${resource!"Unknown"} initiated a suspicious process **will work** but \${resource} initiated a suspicious process **will not**. For a complete list of available attributes, see [Appendix C: Verbose Template Attributes](#).
- b. **Grouping Attribute:** Select an attribute under which to group the information in the summary. Example: Application.
 - c. **Metadata Attributes:** Select up to three metadata attributes to view within the grouping attribute in the summary. Example: EVENT_NAME.
 - d. **Level 2 Attribute:** Select a high-level attribute to view independent of the Grouping Attribute. Example: PATIENT_NAME.
 - e. **Level 2 Metadata Attributes:** Select up to three metadata attributes for the Level 2 Attribute. Example: PATIENT_ID.
2. Complete the following steps to choose the action to be taken on the violations flagged by the policy:

VIOLATION ACTION

Daily Violation Threshold

When a violations exceeds the threshold, it will be skipped for scoring and saving.

Do you want to generate incident for policy violators?

☐ NO

Send Notification

☐ NO

Add Policy Violators to Watchlist?

Add Policy Violators to Active list?

☐ NO

CEF Output

☐ NO

RSA Archer CEF Output

☐ NO

RSA Netwitness CEF Output

☐ NO

Daily Violations Threshold: Enter a value after which to stop flagging violations for the policy.

- b. **Do you want to generate cases for policy violators?:** Set to **YES** to generate a case for each policy violator.

Cases can also be created manually from the Security Command Center.

- a. **Select workflow to trigger when generating cases:** Set to **Yes** to select a workflow from the dropdown.
- c. **Send Notification:** Toggle to **YES** to **Select Email Template** from dropdown to receive notifications of violations for this policy.

- d. **Add Policy Violators to Watchlist?:** Select from dropdown or **Create a New Watchlist**.

Complete the following:

- Confidence Factor:** Enter a value from 0 to 1 to indicate how confident you are the violator should be on the watchlist.
- Confidence Incremental Factor:** Enter a value from 0 to 1 to indicate how confident you are the violation should be on the watchlist for each subsequent violation.
- Rule to Remove Violators from Watchlist:** Enable to specify a time frame after which to **Remove Violators from Watchlist**.
- Add Policy Violators to Active List?:** Toggle to **YES** to complete the following information:

- Select Active list:** Select from dropdown or Create New Active List as described in [Check Against Active List](#).
- Rule to use key in active list:** Specify mapped attributes to include in the check as described in [Check Against Active List](#).
- Select attributes to be displayed in violation on SCC:** Use > or >> to add the attributes to include in the violation summary on the [Security Command Center](#).

e. **CEF Output:** Toggle to **Yes** to produce output in CEF format. If **Yes**:

a. **Select Connection** from dropdown.



Note: You must configure your connections for CEF output in [Connection Types](#) before you can export from ArcSight UBA.

b. Click **Output Mapping** to configure output.

CEF Field	Constant?	Mapped With
act	YES	deviceaction
app	YES	applicationprotocol
dhost	YES	destinationhostname
dpid	YES	destinationprocessid
dmac	YES	destinationmacaddress
dntdom	YES	destinationntdomain

Save

a. **CEF Field:** Specify field. Example: act.

b. **Constant?:** Toggle to **Yes** or **No**.

c. **Mapped With:** Enter a value using +/- to add/remove attributes.
Example: deviceaction

f. **RSA Archer CEF Output:** Toggle to **Yes** to produce output in CEF format. If **Yes**, see **CEF Output**.



Note: You must configure your connections for RSA Archer CEF output before you can export from ArcSight UBA.

g. **RSA Netwitness CEF Output:** Toggle to **Yes** to produce output in CEF format. If **Yes**, see **CEF Output**.



Note: You must configure your connections for RSA Netwitness CEF output before you can export from ArcSight UBA.

3. View or search for violations on Spotter:

1. Navigate to **Menu > Security Center > Spotter** or click **F2**.
2. Click the policy name from **Available Violations** or the datasource from **Available Data-sources** to view events.

OR

Search Spotter using the following syntax: `polycyname="[polycyname]"`.

4. Find violations in the Security Command Center:

1. Navigate to **Menu > Security Center > Security Command Center** or click ArcSight UBA logo.



Note: Policies will only appear in the Security Command Center if violations exist for those policies.

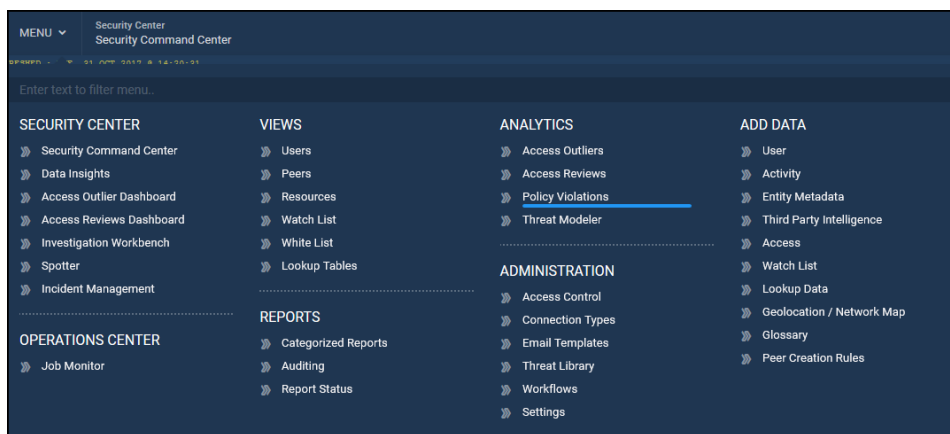
2. Click the policy name to view activity accounts associated with the violations.
3. Click the violator name to view the a summary of the violation.

For more information about this screen, see [Policies](#).

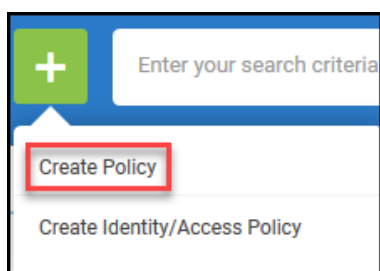
Example Behavior-Based Activity Outlier Policy: Spike in Number of Records accessed by an Employee

This behavior-based activity outlier policy uses application data to detect when users have committed a healthcare violation by accessing an abnormal number of records compared to their baseline behavior.

1. Navigate to **Menu > Analytics > Policy Violations**:



2. Click +.
3. Select **Create Policy**.



Enter Policy Details

In this section, configure the policy name, criticality, entity against which the policy will run, and the datasource to which the policy will be applied, as well as designating the owner and remediator of the policy in order to restrict what users may view the policy violations. Define the category and indicator of threat.

Define Policy

Complete the following information:

DEFINE POLICY

Policy Name*

Provide unique name which will describe what type of violation it detects. Special characters are not allowed. Example: (- (bracket), ' - (single quote) are not allowed

Description

Criticality
Medium

Select the criticality of the policy. The criticality affects the risk score for the user. None=0.0, Low=0.2, Medium=0.6 and High=1.0

Do you want to save violations and calculate risk scores for this policy?
☒ YES

If Yes, violations will be searchable in Spotter and risk scores will be calculated for violators. If No, violations will not be searchable and risk scores will not be calculated for violators of this policy.

Do you want to escalate this policy as a Threat?
☒ YES

If Yes, this policy will be escalated as a Threat instead of a Violation and will appear under Top Threats in Security Command Center. If no, this policy will appear under the Top Violations widget.

Select Violation Entity*

Select the entity that the risk should apply to?


Users - Returns list of users violating policy. Orphan accounts(or uncorrelated accounts) will be ignored.

ActivityAccount - Returns list of activity accounts (both correlated and uncorrelated) violating the policy.

Resources - Returns list of resources violating the policy.

Do you want to run the policy on a
☒ Datasource ☐ Functionality

- Policy Name:** Provide a unique name to describe the policy: Spike in Number of Records accessed by an Employee.
- Description:** Enter a brief description of the policy. Example: This check detects spikes in number of records accessed by an employee compared to baseline behavior.
- Criticality:** Use slider to select the criticality of the policy: Medium.


Note: This will affect the risk score for the user. None=0.0, Low=0.2, Medium=0.6, and High=1.0.
- Do you want to save violations and calculate risk scores for this policy?:** Toggle to **YES** to make violations for this policy searchable in Spotter and to calculate risk scores for violators. If disabled, violations will not be searchable and risk scores will not be calculated.

- e. **Do you want to escalate this policy as a Threat?:** Toggle to **YES** to escalate the policy to a threat rather than a policy violation. Violations will appear under Top Threats in the Security Command Center. If **NO**, view violations will appear in the Top Violations dashboard.
- f. **Select Violation Entity:** Select from dropdown: Activity Account.
 - **Activity Account:** Returns list of activity accounts (both correlated and uncorrelated) violating policy.
- g. **Do you want to run the policy on a:** Select **Datasource** to use the dropdown to select the datasource on which the policy should run: Cerner Healthcare Data.

Additional Details

ADDITIONAL DETAILS

Owner

Select the owner of the policy. This can be used for sending notifications and case management. The category widget on the security dashboard is visible to policy owners.

Remediator

Select the remediator for the policy. The remediator can be sent notifications and used in case management.

- a. **Owner:** Click search icon to select an owner for the policy: None selected.
- b. **Remediator:** Click search icon to select a remediator for the policy: None selected.

Define Risk and Threat

1. Complete the following information:

DEFINE RISK AND THREAT

Category*

Create New Policy Category

HEALTHCARE VIOLATION

+

-

Category is displayed on dashboard as a widget and risk will be aggregated for policies with the same category. All violations of the same category will be available in the widget.

Threat Indicator*

Create New Threat Indicator

Edit Killchain Stage and Response Actions

Spike in Number of Records accessed by an Employee

Violations detected are indicative of threat

- a. **Category:** Select from dropdown: Healthcare Violation.
 - b. **Threat Indicator:** Spike in Number of Records accessed by an Employee.
 - a. Select from dropdown.
OR
 - b. **Create New Threat Indicator** as described in [Creating Policies](#).
2. Click **Save & Next** to proceed to [Provide Conditions](#).

Provide Conditions

What do you want to detect?

Select **Spike in Number of Occurrences**.

WHAT DO YOU WANT TO DETECT ?

i Spike in number of occurrences : Detects spike in number of events in particular time window. Example : If

CHOOSE THE FEATURES FOR GENERATING BEHAVIOR

☒ destinationhostnameecountry
☒ Filetype
☒ Method
☒ sourcehostnamelongitude
☒ Process_Name
☒ resourcehostnamepostalcode
☒ sessionid
☒ eventlatitude
☒ Response_Code
☒ Referer
☒ destinationhostnamepostalcode
☒ resourcehostnameecountry
☒ destinationhostnameecity

sourcehostnamelongitude
Process_Name
eventlatitude
destinationhostnamepostalcode
Referer
Response_Code
Method
Filetype

Select the attributes from above panel Selected features

Choose the Features for Generating Behavior

Click the following attributes to select the features for generating the behavior profile:

CHOOSE THE FEATURES FOR GENERATING BEHAVIOR

☒ Age
☒ Distance
☒ DEVICE
☒ Aging Baseline
☒ Distance Label
☒ ENCOUNTER_TYPE
☒ APPL_CTX
☒ ADMIT_DT_TM
☒ PATIENT_NAME
☒ AUDIT_SRC
☒ DEPARTMENT_SIZE
☒ Age Baseline
☒ EMPLOYEE_DEPARTMENT
☒ DISCHARGE_DT_TM

EVENT_NAME

Select the attributes from above panel Selected features

- **EVENT_NAME**

Behavior Information

1. Provide a unique **Behavior Name**. Example: NumberOfRecordsAccessedByEmployee.
2. Select **Daily** for **Choose Time Window** to check against the activity account's typical daily behavior.

What should get flagged as violations?

1. Select **Self** for **Number of occurrences of selected features is unusually higher than behavior baseline for:**
2. Select **Transaction Occurrence Abnormally higher than User's Daily Behavior** from **Choose the Analytical Technique to run** dropdown.
3. Set **Flag as Violations when Rarity crosses Sigma Threshold Value** to **0.22 (Slight Deviation)**.

WHAT SHOULD GET FLAGGED AS VIOLATIONS ?

Number of occurrences of selected features is unusually higher than behavior baseline for :

☒ Self ☐ Other Accounts ☐ Peer Groups

Choose the Analytical Technique to run

Transaction Occurrence Abnormally higher than User's Daily Be...

Flag as Violations when Rarity crosses Sigma Threshold Value

Slight Deviation High Deviation 0.22

Choose Action for Violation Results

In this section, determine what actions the application will take for violations of this policy. Create actions to generate cases, assign workflow, export data in CEF format, and configure a violation summary to specify what attributes to include in the Violation Summary for [Policies](#).

1. **Configure Your Violation Summary:** Complete the following information to appear on the Violation Summary screen that can be accessed from the [Security Command Center](#).

CONFIGURE THE VIOLATION INFORMATION SUMMARY

1 Based on selected attributes, violation summary will be generated that can be viewed on **Summary** from the Security Command center.

VIOLATOR

GROUPING ATTRIBUTE

EVENT_NAME ▼

Metadata Attributes

1 EVENT_TYPE ▼

2 APPLICATION ▼

3 SELECT ▼

Level 2 Attribute


PATIENT_NAME ▼

Metadata Attributes

1 PATIENT_PRIVILEGES ▼

2 ENCOUNTER_TYPE ▼

3 SELECT ▼

- Provide the verbose template for violation summary:** Enter a verbose template to specify custom attributes to display in the violation summary (optional.) Example: Account \${accountname!"ACCOUNTNAME"} performed \${transactionstring1!"ACTIVITY"} from ipaddress \${ipaddress!"UNKNOWN"}.
-  **Note:** You must include the ! in the attribute. For example: \${resource!"Unknown"} initiated a suspicious process **will work** but \${resource} initiated a suspicious process **will not**. For a complete list of available attributes, see [Appendix C: Verbose Template Attributes](#).
- Grouping Attribute:** Select an attribute under which to group the information in the summary. Example: EVENT_NAME.
 - Metadata Attributes:** Select up to three metadata attributes to view within the grouping attribute in the summary. Example: EVENT_TYPE, APPLICATION.
 - Level 2 Attribute:** Select a high-level attribute to view independent of the Grouping Attribute. Example: PATIENT_NAME.
 - Level 2 Metadata Attributes:** Select up to three metadata attributes for the Level 2 Attribute. Example: PATIENT_PRIVILEGES, ENCOUNTER_TYPE.
- Complete the following steps to choose the action to be taken on the violations flagged by the policy:

VIOLATION ACTION

Daily Violation Threshold

When a violations exceeds the threshold, it will be skipped for scoring and saving.

Do you want to generate incident for policy violators?

☐ NO

Send Notification

☐ NO

Add Policy Violators to Watchlist?

Add Policy Violators to Active list?

☐ NO

CEF Output

☐ NO

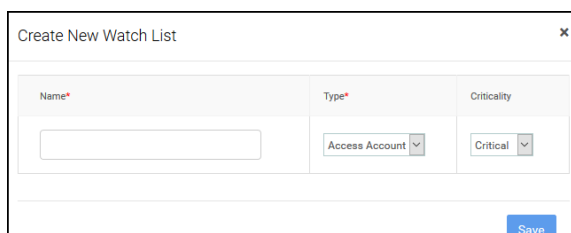
RSA Archer CEF Output

☐ NO

RSA Netwitness CEF Output

☐ NO

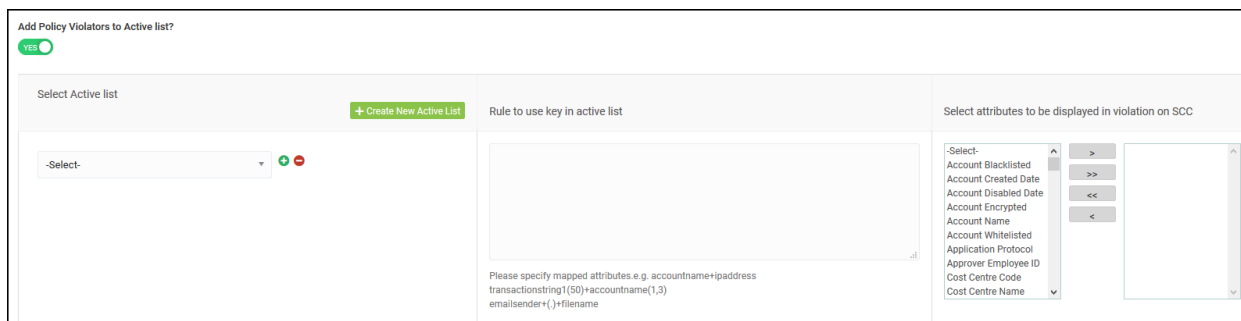
- a. **Daily Violations Threshold:** Enter a value after which to stop flagging violations for the policy.
- b. **Do you want to generate cases for policy violators?:** Set to **YES** to generate a case for each policy violator.
- c. Cases can also be created manually from the Security Command Center.
 - a. **Select workflow to trigger when generating cases:** Set to **Yes** to select a workflow from the dropdown.
- d. **Send Notification:** Toggle to **YES** to **Select Email Template** from dropdown to receive notifications of violations for this policy.
- e. **Add Policy Violators to Watchlist?:** Select from dropdown or **Create a New Watchlist**.



The 'Create New Watch List' form contains three main input fields: 'Name*' (a text box), 'Type*' (a dropdown menu with 'Access Account' selected), and 'Criticality' (a dropdown menu with 'Critical' selected). A 'Save' button is located at the bottom right of the form.

Complete the following:

- Confidence Factor:** Enter a value from 0 to 1 to indicate how confident you are the violator should be on the watchlist.
- Confidence Incremental Factor:** Enter a value from 0 to 1 to indicate how confident you are the violation should be on the watchlist for each subsequent violation.
- Rule to Remove Violators from Watchlist:** Enable to specify a time frame after which to **Remove Violators from Watchlist**.
- Add Policy Violators to Active List?:** Toggle to **YES** to complete the following information:



The 'Add Policy Violators to Active List' form has a 'YES' toggle at the top left. It is divided into three main sections:

- Select Active list:** Includes a dropdown menu (currently showing '-Select-') and a '+ Create New Active List' button.
- Rule to use key in active list:** A large text area for defining rules. Below it, a note says 'Please specify mapped attributes, e.g. accountname+ipaddress' followed by examples: 'transactionstring(50)+accountname(1,3)' and 'emailsender()+filename'.
- Select attributes to be displayed in violation on SCC:** A list of attributes on the left (Account Blacklisted, Account Created Date, Account Disabled Date, Account Encrypted, Account Name, Account Whitelisted, Application Protocol, Approver Employee ID, Cost Centre Code, Cost Centre Name) and a set of navigation buttons (>, >>, <<, <) to move them to a display area on the right.

- Select Active list:** Select from dropdown or Create New Active List as described in [Check Against Active List](#).
- Rule to use key in active list:** Specify mapped attributes to include in the check as described in [Check Against Active List](#).
- Select attributes to be displayed in violation on SCC:** Use > or >> to add the attributes to include in the violation summary on the [Security Command Center](#).

f. **CEF Output:** Toggle to **Yes** to produce output in CEF format. If **Yes**:

a. **Select Connection** from dropdown.



Note: You must configure your connections for CEF output in [Connection Types](#) before you can export from ArcSight UBA.

b. Click **Output Mapping** to configure output.

CEF Field	Constant?	Mapped With
act	YES	deviceaction
app	YES	applicationprotocol
dhost	YES	destinationhostname
dpid	YES	destinationprocessid
dmac	YES	destinationmacaddress
dntdom	YES	destinationntdomain

Save

a. **CEF Field:** Specify field. Example: act.

b. **Constant?:** Toggle to **Yes** or **No**.

c. **Mapped With:** Enter a value using +/- to add/remove attributes.
Example: deviceaction

g. **RSA Archer CEF Output:** Toggle to **Yes** to produce output in CEF format. If **Yes**, see **CEF Output**.



Note: You must configure your connections for RSA Archer CEF output before you can export from ArcSight UBA.

h. **RSA Netwitness CEF Output:** Toggle to **Yes** to produce output in CEF format. If **Yes**, see **CEF Output**.



Note: You must configure your connections for RSA Netwitness CEF output before you can export from ArcSight UBA.

3. View or search for violations on Spotter:

1. Navigate to **Menu > Security Center > Spotter** or click **F2**.
2. Click the policy name from **Available Violations** or the datasource from **Available Data-sources** to view events.

The screenshot shows the Spotter interface with two main panels: **AVAILABLE VIOLATIONS** and **AVAILABLE DATASOURCES**. Both panels have a search bar and a 'Count' dropdown set to 10. The **AVAILABLE VIOLATIONS** panel shows a list of violations with a total of 2.2K. The **AVAILABLE DATASOURCES** panel shows a list of data sources with a total of 19.99M events.

AVAILABLE VIOLATIONS	TOTAL VIOLATED EVENTS: 2.2K
Spike in amount of bytes out	1,180
Robotic beaconing traffic detected	379
Spam Email	193
Spike in Number of Records accessed by an Employee	120
Critical vulnerabilities detected	114
Excessive number of emails to personal email address	104
Flight Risk User - Job Search	31
File Copy Blocked By DLP	23
Potential Data Snooping Activity	18
Suspicious Process Detected	5
Landsped Violation - VPN	2
Privilege Escalation	2
Rare Login to Critical Server	1

AVAILABLE DATASOURCES	TOTAL EVENTS: 19.99M
Unix Data	6,238,743
Infoblox	5,930,539
Digital Guardian Send Mail	5,561,322
Bluecoat Proxy	1,039,572
Windows Data	711,524
Citrix VPN	317,468
Windchill Data	158,453
Google Login	24,282
Nessus Data	9,436
Cerner Healthcare Data	2,824
Ironport Data	1,103
Digital Guardian USB	24

OR

Search Spotter using the following syntax: `poli c yname=" [poli c yname] "`.

The screenshot shows the Spotter interface with the search bar containing the query: `poli c yname="Spike in Number of Records accessed by an Employee"`. The search results show 151 events fetched out of 151 matched events. The results are displayed in a table with columns for accountname, destination, device, and source account.

Selected Fields	Device	Source Account	Destination Account
accountname	BR1082	IMFGCC10	BR1082
destination	Day Surgery	USA	Day Surgery
device	SCX231 Data Logs	Credit Evaluation	SCX231 Data Logs
source account	Cerner Healthcare Data	Credit Evaluation	Cerner Healthcare Data

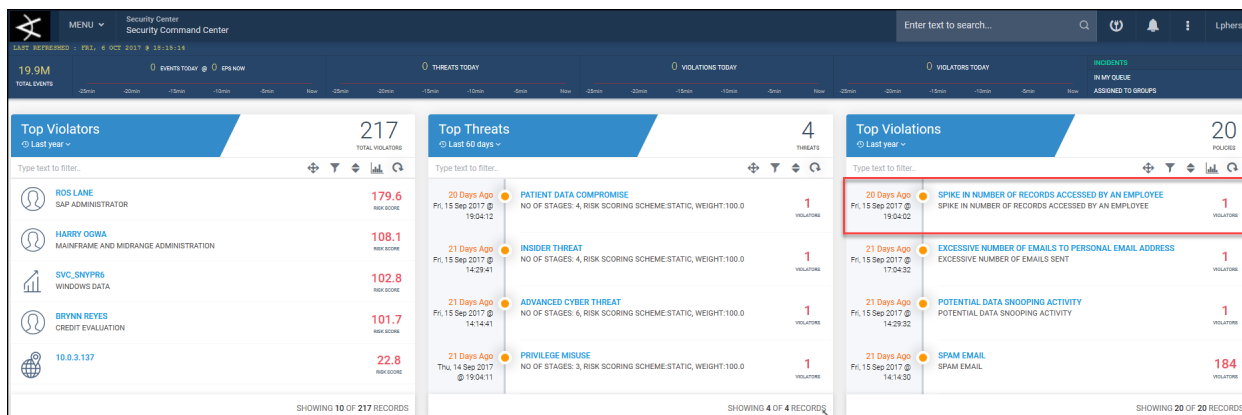
The search results also include a detailed view of the event, showing the following details:

- Category:** HEALTHCARE VIOLATION
- Policy Name:** Spike in Number of Records accessed by an Employee
- Risk Threat Name:** Spike in Number of Records accessed by an Employee
- Violator:** Activityaccount

The event details also include a list of fields such as accountname, destination, device, source account, and destination account, along with their respective values.

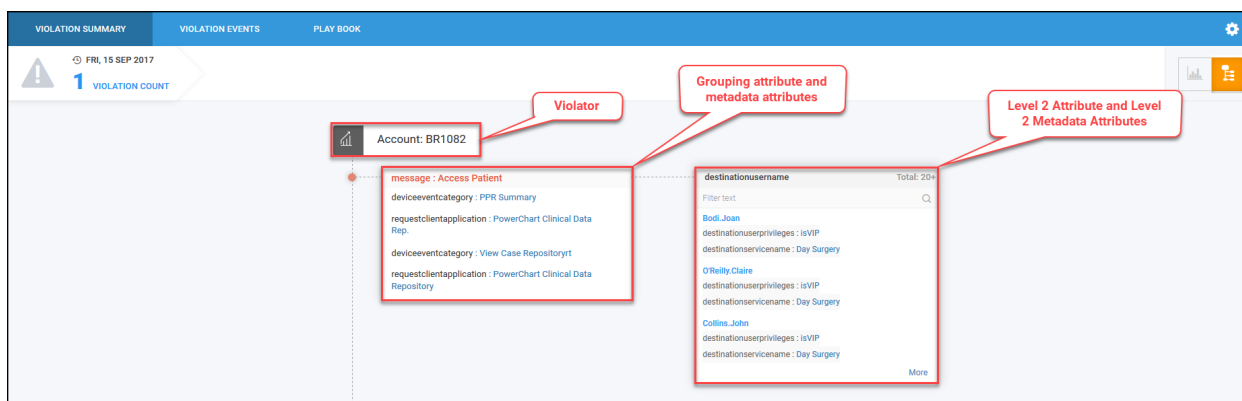
4. Find violations in the Security Command Center:

1. Navigate to **Menu > Security Center > Security Command Center** or click ArcSight UBA logo.



Note: Policies will only appear in the Security Command Center if violations exist for those policies.

2. Click the policy name to view activity accounts associated with the violations.
3. Click the violator name to view the a summary of the violation.



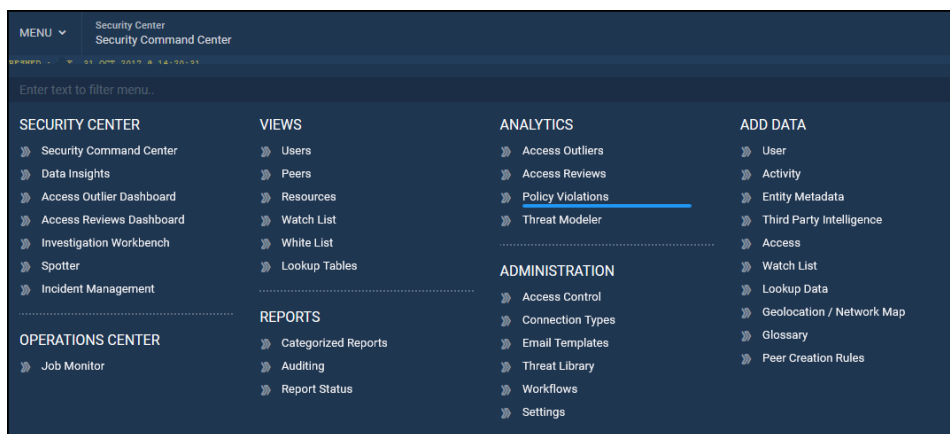
For more information about this screen, see [Policies](#).

Creating Identity / Access Policies

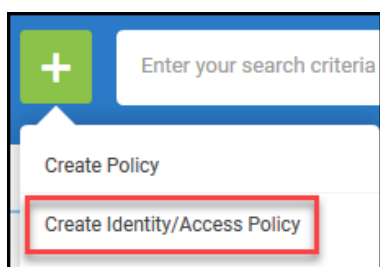
Create a rule based policy to flag events or entities that violate a specific rule based on a built-in template. This section includes how to create this type of policy and provides specific examples of Identity Policies.

To create an Identity/Access Policy, complete the following steps:

1. Navigate to **Menu > Analytics > Policy Violations**:



2. Click +.
3. Select **Create Identity/Access Policy**.



Enter Policy Details

In this section, configure the policy name, criticality, entity against which the policy will run, and the datasource to which the policy will be applied, as well as designating the owner and remediator of the policy in order to restrict what users may view the policy violations. Define the category and indicator of threat.

Define Policy

Complete the following information:

DEFINE POLICY


Policy Name*

Provide unique name which will describe what type of violation it detects. Special characters are not allowed. Example: (- (bracket), ' - (single quote) are not allowed

Description

Criticality

Low



Select the criticality of the policy. The criticality affects the risk score for the user. None=0.0, Low=0.2, Medium=0.6 and High=1.0

Select Violation Entity*

-Select-


Select the entity that the risk should apply to?

"Users" - Returns list of users violating policy. Orphan accounts(or uncorrelated accounts) will be ignored.

Datasource

Select the datasource that this policy should run on. For policies that do not run on any data source, you can leave this as blank (Example: Users with upcoming termination date).

- a. **Policy Name:** Provide a unique name to describe the type of violation the policy detects.
- b. **Description:** Enter a brief description of the policy.
- c. **Criticality:** Use slider to select the criticality of the policy.



Note: This will affect the risk score for the user. None=0.0, Low=0.2, Medium=0.6, and High=1.0.
- d. **Select Violation Entity:** Select from dropdown.
 - **Users:** Returns list of users violating policy. Uncorrelated accounts will be ignored. A new option will appear:
 - **Access Account:** Returns list of access accounts (both correlated and uncorrelated) violating policy.
- e. **Datasource:** Use search icon to select the datasource the policy should run on.



Note: For policies that do not run on any data source, such as Users with Upcoming Terminations, etc., you can leave this blank.

	Datasource Name	Select Device Type
<input type="radio"/>	Access Data	Active Directory
<input type="radio"/>	Bluecoat Proxy	Bluecoat Proxy
<input type="radio"/>	Cerner Healthcare Data	Cerner Data
<input type="radio"/>	Citrix VPN	Citrix_VPN
<input type="radio"/>	Digital Guardian Send Mail	Digital Guardian Send Mail
<input type="radio"/>	Digital Guardian USB	Digital Guardian USB
<input type="radio"/>	Google Admin	Google Admin
<input checked="" type="radio"/>	Google Login	Google Login
<input type="radio"/>	Infoblox	Infoblox
<input type="radio"/>	Ironport Data	Cisco Ironport Email

- a. Click radio button to select datasource.



Note: You may edit datasources by clicking the name of the datasource.

- b. Click **Assign**.

Additional Details

ADDITIONAL DETAILS

Would you like to Aggregate Risk Score on Each Run?

☒ YES

If set to yes, the risk score will be incremented each time the policy is run.

Owner

Select the owner of the policy. This can be used for sending notifications and case management. The category widget on the security dashboard is visible to policy owners.

Remediator

Select the remediator for the policy. The remediator can be sent notifications and used in case management.

Stop when violations are greater than

- a. **Would you like to Aggregate Risk Score on Each Run?:** Set to **Yes** to increment the risk score each time the policy is run. Default **Yes**.
- b. **Owner:** Click search icon to select an owner for the policy. This can be used to send notifications and manage cases.

Add/Change Owner

username

	User Name	First Name	Last Name	E-Mail	Enabled?
<input type="radio"/>	1001	HARRY	OGWA	HARRY.OGWA@scnx.com	true
<input type="radio"/>	1005	TERRY	MERRITT	TERRY.MERRITT@scnx.com	true
<input type="radio"/>	1012	JOE	KELLINGTON	JOE.KELLINGTON@scnx.com	true
<input type="radio"/>	1013	ROBERT	WELLINGTON	ROBERT.WELLINGTON@scnx.com	true
<input type="radio"/>	1025	Ted	Thomson	ted.thomson@scnx.com	true
<input type="radio"/>	1044	NORA	LEWIS	NORA.LEWIS@scnx.com	true
<input type="radio"/>	1045	FAHAD	WALKER	FAHAD.WALKER@scnx.com	true
<input type="radio"/>	1063	Meredith	COLEMAN	Meredith.COLEMAN@scnx.com	true
<input type="radio"/>	1064	Cedric	Castaneda	Cedric.Castaneda@scnx.com	true
<input type="radio"/>	1065	Ainsley	Moses	Ainsley.Moses@scnx.com	true

Add Selected Owner

- c. **Remediator:** Click search icon to select a remediator for the policy. This can be used to send notifications and manage cases.
- d. **Stop when violations are greater than:** Specify a number to put a limit on the number of violations flagged by the policy. Default 1,000,000.

Define Risk and Threat

1. Complete the following information:

DEFINE RISK AND THREAT

Category*

Create New Policy Category

None

+

-

Category is displayed on dashboard as a widget and risk will be aggregated for policies with the same category. All violations of the same category will be available in the widget.

Threat Indicator*

Create New Threat Indicator

Edit Killchain Stage and Response Actions

-Select-

Violations detected are indicative of threat

- a. **Category:**

- a. Select from dropdown.

OR

- b. **Create New Policy Category.**

Create New Policy Category

Category

Save

- c. Click **+/-** to add/remove categories.

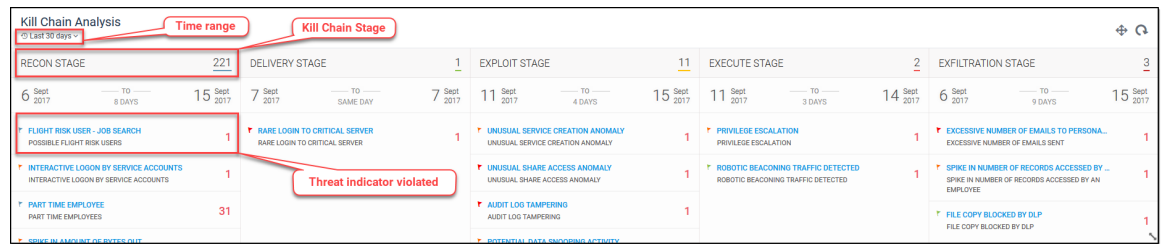
- b. **Threat Indicator:**

- a. Select from dropdown.
- OR
- b. **Create New Threat Indicator.**

The screenshot shows a 'Create New Threat Indicator' window. It includes a text field for the name, a category dropdown menu currently showing 'Recon Stage', and a list of other stages: Delivery Stage, Exploit Stage, Execute Stage, and Exfiltration Stage. At the bottom, there is a section for selecting associated playbooks and a 'Save' button.

- a. **Threat Indicator Name:** Enter a descriptive name for the threat indicator.
- b. **Category:** Select a threat kill chain stage from the dropdown:
 - **Recon Stage:** Stage in which attackers gathers information before an attack in an attempt to find a vulnerable point in the network. Example: Phishing emails.
 - **Delivery Stage:** Stage in which attackers deliver a malicious package to gain access to a network. Example: User clicks a link within a phishing email and downloads malware from the malicious site.
 - **Exploit Stage:** Stage in which attackers find a vulnerable point of entry into the network and gain access. Example: Zero-day attack.
 - **Execute Stage:** Stage in which attackers escalate access to execute the attack using admin privileges. Example: Escalating privileges or stealing admin credentials, lateral movement.
 - **Exfiltration Stage:** Stage in which the attackers can move freely around the network and access or remove any sensitive data at will. Example: An insider uploading customer information to a personal file sharing/storage site.

Each stage represents a step in the threat kill chain. To view violations by threat stage on the Kill Chain Analysis, navigate to **Menu > Security Center > Security Command Center**. See [Security Command Center](#) for more information.



- c. **Threat Response Playbook:** Enter the steps to take to remediate this threat. Use HTML to control the way the steps are displayed on the Violation Summary screen. Example:

```
<ol>
```

```
<li>Review the Account Name and Domain Name fields, that identify the user who cleared the log</li><br>
```

```
<li>Additional fields of interest: Security ID, Logon ID, Subject</li><br>
```

```
<li>Login ID allows you to correlate backwards to the logon events as well as with other events logged during the same logon session</li><br>
```

```
<li><a href="supportticketsite.com">Submit a ticket to investigate</a></li>
```

```
</ol>
```

The screenshot shows the 'Threat Response Playbook' input field. It contains the following HTML code:

```
<ol>
<li>Review the Account Name and Domain Name fields, that identify the user who cleared the log</li>
<li>Additional fields of interest: Security ID, Logon ID, Subject</li>
<li>Login ID allows you to correlate backwards to the logon events as well as with other events logged during the same logon session</li>
<li><a href="supportticketsite.com">Submit a ticket to investigate</a></li>
</ol>
```

The Remediation Steps will appear on the Violation Summary screen:

VIOLATION SUMMARY	VIOLATION EVENTS	REMEDIALTION STEPS
<ol style="list-style-type: none"> 1 Check the initial level privileges 2 Contact ITOps Administrator to get more insight into his privileges 3 Submit a ticket to investigate further 		

- d. **Select to Associate Playbooks:** Select the play books to associate with the threat indicator. Example: VirusTotal ScanIP.

For information about how playbooks work in ArcSight UBA, see [Automated Response](#).

Edit Threat Indicator

Select To Associate Playbooks

☐ **SNYPR SendAlertCEF**
Send violation alerts as CEF

☐ NO
AUTO PLAY

☒ **VirusTotal ScanIP**
VirusTotal ScanIP and fetch results

☐ NO
AUTO PLAY

☒ **VirusTotal ScanURL**
VirusTotal ScanURL and fetch results

☐ NO
AUTO PLAY

☒ **VirusTotal ScanDomain**
VirusTotal ScanDomain and fetch results

☐ NO
AUTO PLAY

☒ **VirusTotal ScanFile**
VirusTotal ScanFile and fetch results

☐ NO
AUTO PLAY

☒ **Nessus LaunchScan**
Launch a Nessus Scan

☐ NO
AUTO PLAY

Save



Note: You may select multiple playbooks for the threat indicator.

- e. Enable Auto Play to automatically launch play book tasks upon violation.
If Auto Play is disabled, you can launch play book tasks manually from the violation summary screen when an incident occurs.
For information about how playbooks work in ArcSight UBA, see [Automated Response](#).

Select To Associate Playbooks		
<input type="checkbox"/>	SNYPR SendAlertCEF Send violation alerts as CEF	<input type="radio"/> NO AUTO PLAY
<input checked="" type="checkbox"/>	VirusTotal ScanIP VirusTotal ScanIP and fetch results	<input checked="" type="radio"/> YES AUTO PLAY
<input checked="" type="checkbox"/>	VirusTotal ScanURL VirusTotal ScanURL and fetch results	<input type="radio"/> NO AUTO PLAY
<input checked="" type="checkbox"/>	VirusTotal ScanDomain VirusTotal ScanDomain and fetch results	<input type="radio"/> NO AUTO PLAY
<input checked="" type="checkbox"/>	VirusTotal ScanFile VirusTotal ScanFile and fetch results	<input checked="" type="radio"/> YES AUTO PLAY
<input checked="" type="checkbox"/>	Nessus LaunchScan Launch a Nessus Scan	<input type="radio"/> NO AUTO PLAY

Save

- c. Click **Edit Killchain Stage and Response Actions** to edit the information described in the previous step.
2. Click **Save & Next** to proceed to [Select Policy Template](#).

Select Policy Template

In this section, enable a template to determines the attributes against which to run the policy. For example, user attributes, access account attributes, and resource attributes.

1. Select the template for this policy from the list.

Click **Filter template** to filter list. Set the filter criteria by checking the boxes in the top selection area.

Enter Policy Details | **Select Policy Template** | Provide Conditions | Choose Action for Violation Results

Templates combine a group of tables which would be used in the query.

Template Name	Template Description	Objects Available
Enables policies based on USER attributes	1) Terminated Users (User Termination Date < Today's Date) 2) Users with Upcoming Termination Date (User Termination Date < Today's Date + 30 Days) 3) Users with Bad Performance Reviews (User Performance Review="Poor")	USER
Users with defined account types on Resource	Enables policies that include User attributes, Access account attributes and Resource attributes	USER,RESOURCE,ACCESS ACCOUNT
Accounts with defined Access Privileges on Resource	Enables policies that include Access account attributes and Resource attributes	RESOURCE,ACCESS ACCOUNT,RESOURCEACCESSMETADATA,ACCESS VALUES,ACCESS ACCOUNT USER
Separation of Duties Checks (Access Based)	Enables policies that include User attributes, Resource attributes, Accessaccount attributes and access values	USER,RESOURCE,ACCESS ACCOUNT,RESOURCEACCESSMETADATA,ACCESS VALUES
Users with defined Access Privileges on Resource	Enables policies that include User attributes, Access account attributes and Resource attributes	USER,RESOURCE,ACCESS ACCOUNT,RESOURCEACCESSMETADATA,ACCESS VALUES
Accounts that dont have Users	Orphaned Accounts	RESOURCE,ACCESS ACCOUNT,ACCESS ACCOUNT USER
SOD-User - Accessaccount - Resource - Access Values	Enables policies that include User attributes, Resource attributes, Accessaccount attributes and access values	USER,RESOURCE,ACCESS ACCOUNT,ACCESS VALUES

Filter templates

Access

☐ ACCESS ACCOUNT ☐ ACCESS VALUES

☐ RESOURCEACCESSMETADATA ☐ ACCESS ACCOUNT USER

Entities

☒ USER

2. Click **Save & Next** to proceed to [Provide Conditions](#).

Provide Conditions

In this section, set the rules for the policy to enable its functions. Create groups of rules to determine what the policy will check against the data, configure post process functions to add additional data processing, and select risk boosters to increase or decrease the risk score of violators based on specified conditions.

Enter Policy Details | Select Policy Template | **Provide Conditions** | Choose Action for Violation Results

Add new group

Enable attribute functions: ☒ No ☐ Yes

Enable value functions: ☒ No ☐ Yes

Object	Attributes	Condition	Value
USER	CUSTOM FIELD 20	Equal To	*
AND			
Remove group	Add new group		
Object	Attributes	Condition	Value
USER	CUSTOM FIELD 20	Equal To	*
AND			

Preview

Conditions

The Objects displayed in the **Object** dropdown are from the policy template. The attributes associated with the object are listed in the **Attributes** dropdown. Objects are the database tables and attributes are the respective columns for that table.

To add a new group of objects and attributes, complete following steps:

1. Click **Add new group**.

This displays another set of object, attributes, conditions, and value dropdowns to enable adding additional conditions to the query.

The screenshot shows the 'Add new group' interface with two rows of configuration. The first row has Object: USER, Attributes: CUSTOM FIELD 20, Condition: Equal To, and Value: *. The second row has Object: ACTIVITY ACCOUNT, Attributes: ACCOUNT TYPE, Condition: Equal To, and Value: *. Both rows have an AND operator and status icons (green and red).

2. Select the **Object**, **Attributes**, **Condition** and **Value** for that attribute.

- **Object:** Auto-filled based on the entity selected during **Enter Policy Details**.
- **Attributes:** Select from dropdown. Note: Based on the Object.
- **Condition:** Select from dropdown.
- **Value:** Select from dropdown. Note: Based on the Attribute.
- **+/-:** Add/remove rules.

This translates the rule into a HQL query with the format `[Object.Attributes <condition> Value]` (e.g. For the following settings: Object = "User", Attributes = "City", Condition="Equal To", Value="dallas", the resulting query is: "user-s.city = 'dallas'")



Note: For more information about groups and rules, see [Conditions](#).

3. **Enable Attribute Functions / Enable value functions** to display the respective dropdowns to select the functions to use on an attribute or value.



Note: For more information about using functions, see [Appendix B: Functions](#).

The screenshot shows the 'Add new group' interface with two rows of configuration. The first row has Object: USER, Attributes: CUSTOM FIELD 20, Function On Attribute: -Select-, Condition: Equal To, Value: *, and Function On Value: -Select- Function Type. The second row has Object: USER, Attributes: CUSTOM FIELD 20, Function On Attribute: -Select-, Condition: Equal To, Value: *, and Function On Value: -Select- Function Type. Both rows have an AND operator and status icons (green and red).

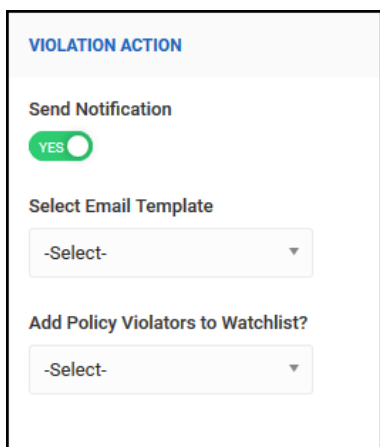
1. Click **Preview** to see the HQL query that will run based on your selections.

2. Click **Save & Next** to proceed to [Choose Action for Violation Results](#).

Choose Action for Violation Results

In this section, determine what actions the application will take for violations of this policy. Create actions to generate cases, assign workflow, enable notifications, and configure a violation summary to specify what attributes to include in the Violation Summary for [Policies](#).

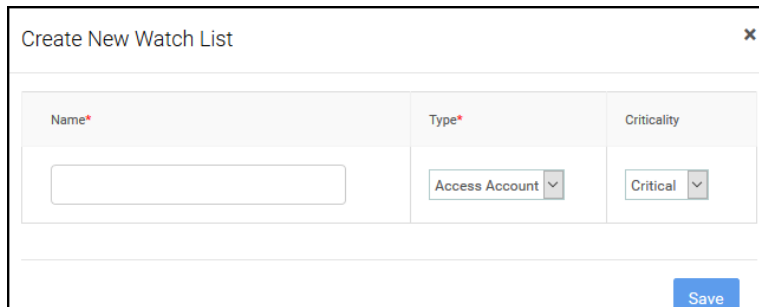
2. Complete the following steps to choose the action to be taken on the violations flagged by the policy:



The screenshot shows a configuration panel titled "VIOLATION ACTION". It contains three sections: "Send Notification" with a green "YES" toggle switch, "Select Email Template" with a dropdown menu showing "-Select-", and "Add Policy Violators to Watchlist?" with a dropdown menu showing "-Select-".

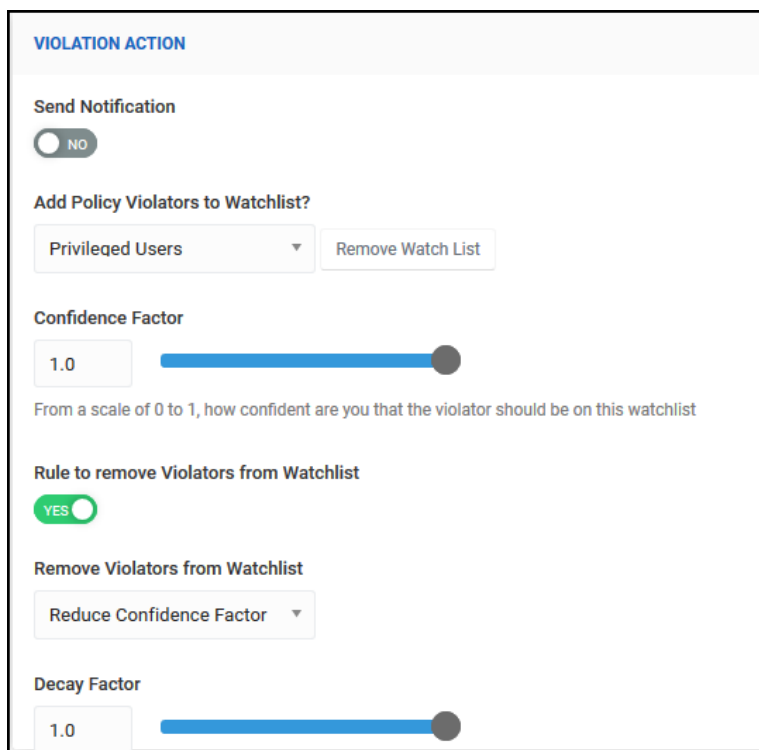
- a. **Send Notifications:** Toggle slider to **YES** to send notifications.
- a. **Select Email Template:** Select a template from the dropdown or click **Create New Email Template**.

- a. **Add Policy Violators to Watchlist?**: Select from dropdown or **Create a New Watchlist**.



The 'Create New Watch List' dialog box contains three input fields: 'Name*' (a text box), 'Type*' (a dropdown menu with 'Access Account' selected), and 'Criticality' (a dropdown menu with 'Critical' selected). A blue 'Save' button is located at the bottom right.

If you selected a Watchlist, complete the following:



The 'VIOLATION ACTION' panel includes the following settings:

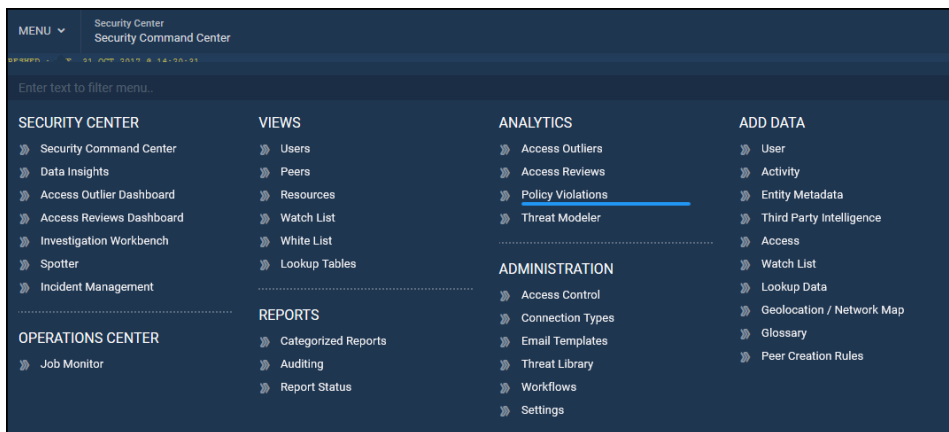
- Send Notification**: A toggle switch set to 'NO'.
- Add Policy Violators to Watchlist?**: A dropdown menu showing 'Privileged Users' and a 'Remove Watch List' button.
- Confidence Factor**: A slider set to 1.0. Below it, text reads: 'From a scale of 0 to 1, how confident are you that the violator should be on this watchlist'.
- Rule to remove Violators from Watchlist**: A toggle switch set to 'YES'.
- Remove Violators from Watchlist**: A dropdown menu showing 'Reduce Confidence Factor'.
- Decay Factor**: A slider set to 1.0.

- a. **Confidence Factor**: Indicate a value from 0 to 1 how confident you are the violator should be placed on the selected watch list.
 - b. **Rule to Remove Violators from Watchlist**: Enable to specify a rule to remove violators from the watch list. Example: **Reduce Confidence Factor** by **Decay Factor 1.0**.
3. Click **Save** to proceed to [Creating Identity /Access Policies](#).

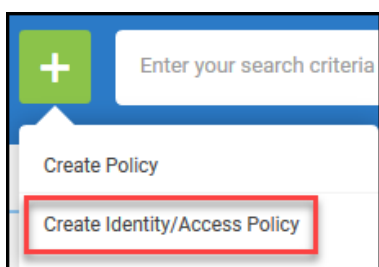
Example Identity Policy: Employees with Upcoming Terminations within 30 Days

This Identity Policy flags employees/users with upcoming terminations within the next 30 days. This policy is applied to user data. Use the following steps to create this policy:

1. Navigate to **Menu > Analytics > Policy Violations**:



2. Click +.
3. Select **Create Identity Policy**.



Enter Policy Details

Define Policy

1. Complete the following information:

DEFINE POLICY

Policy Name*

Employees with upcoming terminations within 30 days

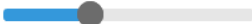
Provide unique name which will describe what type of violation it detects. Special characters are not allowed. Example: (- (bracket), ' - (single quote) are not allowed

Description

Detect employees with termination date within next 30 days

Criticality

Low



Select the criticality of the policy. The criticality affects the risk score for the user. None=0.0, Low=0.2, Medium=0.6 and High=1.0


Select Violation Entity*


Users

Select the entity that the risk should apply to?

Users - Returns list of users violating policy. Orphan accounts(or uncorrelated accounts) will be ignored.

Datasource





Select the datasource that this policy should run on. For policies that do not run on any data source, you can leave this as blank (Example: Users with upcoming termination date).

- a. **Policy Name:** Employees with upcoming termination within 30 days.
- b. **Description:** Detect employees with termination date within the next 30 days.
- c. **Criticality:** Low.
- d. **Select Violation Entity:** Users.
- e. **Datasource:** None.

Additional Details

ADDITIONAL DETAILS

Would you like to Aggregate Risk Score on Each Run?

YES ☒

If set to yes, the risk score will be incremented each time the policy is run.

Owner

Select the owner of the policy. This can be used for sending notifications and case management. The category widget on the security dashboard is visible to policy owners.

Remediator

Select the remediator for the policy. The remediator can be sent notifications and used in case management.

Stop when violations are greater than

- Would you like to Aggregate Risk Score on Each Run?:** Yes.
- Owner:** None.
- Remediator:** None.
- Stop when violation are greater than:** 10,000.

Define Risk and Threat

- Complete the following:

DEFINE RISK AND THREAT

Category*

Create New Policy Category

INSIDER THREAT	+	-
Account Misuse	+	-
Data Exfiltration	+	-

Category is displayed on dashboard as a widget and risk will be aggregated for policies with the same category. All violations of the same category will be available in the widget.

Threat Indicator*

Create New Threat Indicator

Identity-Upcoming Termination

Violations detected are indicative of threat

- Category:** Insider Threat + Account Misuse + Data Exfiltration.
- Threat Indicator:** Identity-Upcoming Termination.

- Click **Save & Next** to proceed to **Select Policy Template**.

Select Policy Template

- Select the following template: **Enables policies based on USER attributes**.

2 Enter Policy Details Select Policy Template Provide Conditions Choose Action for Violation Results			Prev Save & Next
Templates combine a group of tables which would be used in the query.			Filter templates
Template Name	Template Description	Objects Available	
<input checked="" type="radio"/> Enables policies based on USER attributes	1) Terminated Users (User Termination Date < Today's Date) 2) Users with Upcoming Termination Date (User Termination Date < Today's Date + 30 Days) 3) Users with Bad Performance Reviews (User Performance Review = "Poor")	USER	
<input type="radio"/> Users with defined account types on Resource	Enables policies that include User attributes, Access account attributes and Resource attributes	USER, RESOURCE, ACCESS ACCOUNT	
<input type="radio"/> Separation of Duties Checks (Access Based)	Enables policies that include User attributes, Resource attributes, Access account attributes and access values	USER, RESOURCE, ACCESS ACCOUNT, RESOURCE, ACCESS METADATA, ACCESS VALUES	
<input type="radio"/> Users with defined Access Privileges on Resource	Enables policies that include User attributes, Access account attributes and Resource attributes	USER, RESOURCE, ACCESS ACCOUNT, RESOURCE, ACCESS METADATA, ACCESS VALUES	
<input type="radio"/> SOD-User - Access account - Resource - Access Values	Enables policies that include User attributes, Resource attributes, Access account attributes and access values	USER, RESOURCE, ACCESS ACCOUNT, ACCESS VALUES	

- Click **Save & Next** to proceed to **Provide Conditions**.

Provide Conditions

- Click **+ New Group**.
- Enable value functions:** Yes.
- Enable attribute functions:** No.
- Use dropdown to add the following rules:

13

Enter Policy Details

Select Policy Template

Provide Conditions

Choose Action for Violation Results

Prev

Save & Next

Add new group

Enable attribute functions: NO

Enable value functions: YES

Object	Attributes	Condition	Value	Function On Value		
USER	EMPLOYEE TYPE	Equal To	FT	-Select- Function Type	AND	<div><div></div><div></div></div>
USER	TERMINATION DATE	Greater Than	\$CURRENT_DATE	-Select- Function Type	AND	<div><div></div><div></div></div>
USER	TERMINATION DATE	Less Than Or Equal	\$CURRENT_DATE	<div>DATE_ADD</div> <div>Interval Period30Interval TypeDAY</div>	AND	<div><div></div><div></div></div>

- Object:** User | **Attribute:** Employee Type | **Condition:** Equal To | **Value:** FT
- Object:** User | **Attribute:** Termination Date | **Condition:** Greater Than | **Value:** \$CURRENT_DATE
- Object:** User | **Attribute:** Termination Date | **Condition:** Greater Than | **Value:** \$CURRENT_DATE | **Function on Value:** Date_Add: **Interval Period:** 30 Day.
- Click **Preview** to view the HQL query.
- Click **Save & Next** to proceed to **Choose Action for Violation Results**.

Choose Action for Violation Results

1. Complete the following information:

The screenshot shows a web form titled "VIOLATION ACTION". It contains several sections for configuring how violations are handled:

- Send Notification:** A toggle switch is set to "NO".
- Add Policy Violators to Watchlist?:** A dropdown menu is set to "Employees-UpComing Termi..." and a "Remove Watch List" button is visible.
- Confidence Factor:** A slider is set to 1.0. Below it, text reads: "From a scale of 0 to 1, how confident are you that the violator should be on this watchlist".
- Rule to remove Violators from Watchlist:** A toggle switch is set to "YES".
- Remove Violators from Watchlist:** A dropdown menu is set to "Specify Number of Days".
- Number Of Days:** A text input field contains the value "30".

- a. **Send notification:** No.
 - b. **Add Policy Violators to Watchlist?:** Employees-Upcoming Terminations.
 - c. **Confidence Factor:** 1.
 - d. **Rule to remove Violators from Watchlist:** Yes.
 - a. **Remove Violators from Watchlist:** Specify Number of Days.
 - b. **Number of Days:** 30.
2. Click **Save** to proceed to [Viewing, Enabling, and Editing Policies](#).
 3. View or search for violations on Spotter:
 1. Navigate to **Menu > Security Center > Spotter**.
 2. Click the policy name from **Available Violations** or the datasource from **Available Data-sources** to view events.

OR

Search Spotter using the following syntax: `polycyname="[polycyname]"`.

4. Find violations in the Security Command Center:

1. Navigate to **Menu > Security Center > Security Command Center** or click ArcSight UBA logo.



Note: Policies will only appear in the Security Command Center if violations exist for those policies.

2. Click the policy name to view activity accounts associated with the violations.

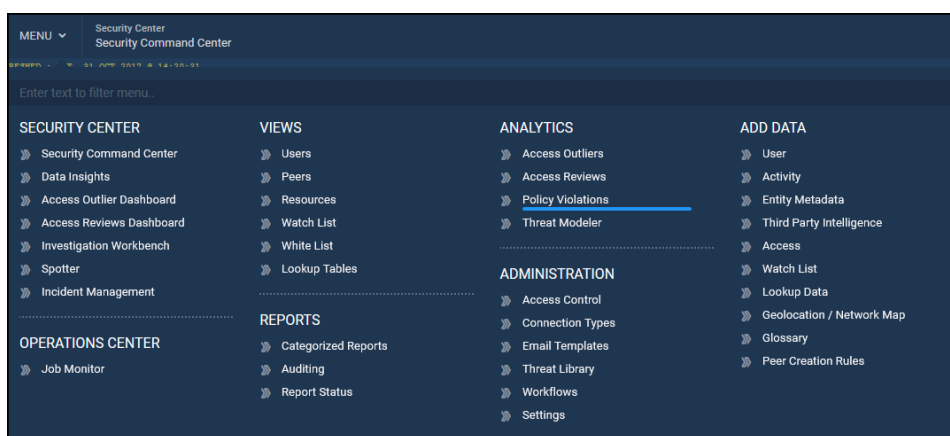
For more information about this screen, see [Policies](#).

3. Click the violator name to view the a summary of the violation.

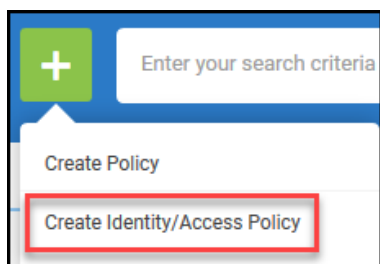
Example Identity Policy: Part Time Employee

This Identity Policy uses user attributes to flag employees who work for the organization part time. This policy is applied to user data. Use the following steps to create this policy:

1. Navigate to **Menu > Analytics > Policy Violations**:



2. Click +.
3. Select **Create Identity Policy**.



Enter Policy Details

Define Policy


1. Complete the following information:

DEFINE POLICY

Policy Name*

Provide unique name which will describe what type of violation it detects. Special characters are not allowed. Example: (- (bracket), ' - (single quote) are not allowed

Description

Criticality
None


Select the criticality of the policy. The criticality affects the risk score for the user. None=0.0, Low=0.2, Medium=0.6 and High=1.0

Select Violation Entity*

Select the entity that the risk should apply to?

Users - Returns list of users violating policy. Orphan accounts(or uncorrelated accounts) will be ignored.

Datasource

Select the datasource that this policy should run on. For policies that do not run on any data source, you can leave this as blank (Example: Users with upcoming termination date).

- a. **Policy Name:** Part Time Employee.
- b. **Description:** Flags employees who work for the organization part time.
- c. **Criticality:** Low.
- d. **Select Violation Entity:** Users.
- e. **Datasource:** None.

Additional Details

- a. **Would you like to Aggregate Risk Score on Each Run?:** Yes.
- b. **Owner:** None.
- c. **Remediator:** None.
- d. **Stop when violation are greater than:** 10,000.

Define Risk and Threat

5. Complete the following:

- a. **Category:** Example: HEALTHCARE VIOLATION.
 - b. **Threat Indicator:** Part Time Employees.
6. Click **Save & Next** to proceed to **Select Policy Template**.

Select Policy Template

1. Select the following template: **Enables policies based on USER attributes.**

Template Name	Template Description	Objects Available
Enables policies based on USER attributes	1) Terminated Users (User Termination Date < Today's Date) 2) Users with Upcoming Termination Date (User Termination Date < Today's Date + 30 Days) 3) Users with Bad Performance Reviews (User Performance Review="Poor")	USER
Users with defined account types on Resource	Enables policies that include User attributes, Access account attributes and Resource attributes	USER,RESOURCE,ACCESS ACCOUNT
Separation of Duties Checks (Access Based)	Enables policies that include User attributes, Resource attributes, Access account attributes and access values	USER,RESOURCE,ACCESS ACCOUNT,RESOURCE,ACCESSMETADATA,ACCESS VALUES
Users with defined Access Privileges on Resource	Enables policies that include User attributes, Access account attributes and Resource attributes	USER,RESOURCE,ACCESS ACCOUNT,RESOURCE,ACCESSMETADATA,ACCESS VALUES
SOD-User - Accessaccount - Resource - Access Values	Enables policies that include User attributes, Resource attributes, Accessaccount attributes and access values	USER,RESOURCE,ACCESS ACCOUNT,ACCESS VALUES

2. Click **Save & Next** to proceed to **Provide Conditions**.

Provide Conditions

1. Click **+ New Group**.
2. **Enable attribute functions:** No.
3. **Enable value functions:** No.
4. Use dropdown to add the following rules:

Object	Attributes	Condition	Value
USER	EMPLOYEE TYPE DESCRIPTION	Equal To	PartTime

1. **Object:** User | **Attribute:** Employee Type Description | **Condition:** Equal To | **Value:** PartTime
5. Click **Preview** to view the HQL query.
6. Click **Save & Next** to proceed to **Choose Action for Violation Results**.

Choose Action for Violation Results

1. Complete the following information:

VIOLATION ACTION

Send Notification
☐ NO

Add Policy Violators to Watchlist?

Part Time Employees ▼ Remove Watch List

Confidence Factor

1.0

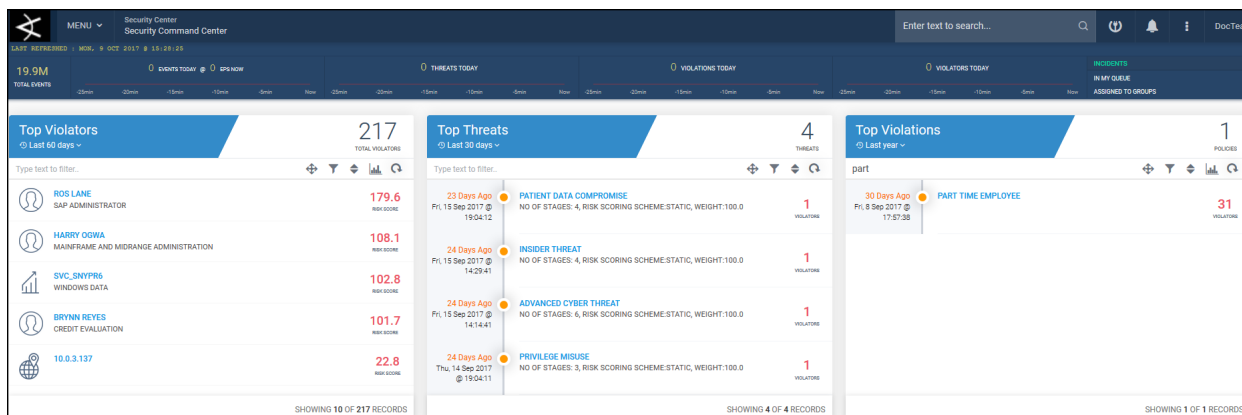
From a scale of 0 to 1, how confident are you that the violator should be on this watchlist

Rule to remove Violators from Watchlist
☐ NO

- a. **Send notification:** No.
 - b. **Add Policy Violators to Watchlist?:** Part Time Employees.
 - c. **Confidence Factor:** 1.
 - d. **Rule to remove Violators from Watchlist:** No.
2. Click **Save** to proceed to [Viewing, Enabling, and Editing Policies](#).

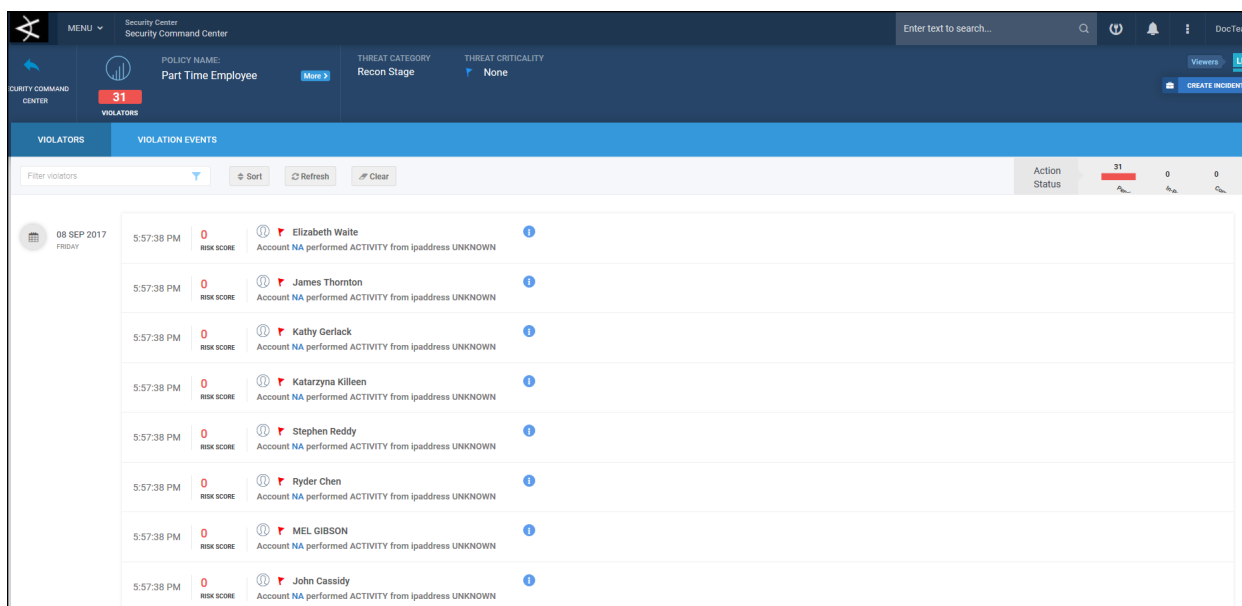
3. Find violations in the Security Command Center:

1. Navigate to **Menu > Security Center > Security Command Center** or click ArcSight UBA logo.



Note: Policies will only appear in the Security Command Center if violations exist for those policies.

2. Click the policy name to view activity accounts associated with the violations.



For more information about this screen, see [Policies](#).

4. View and manage users in Watch list:

1. Navigate to **Menu > Views > Users**.
2. Click Watch list name on left navigation panel (Part Time Employees).

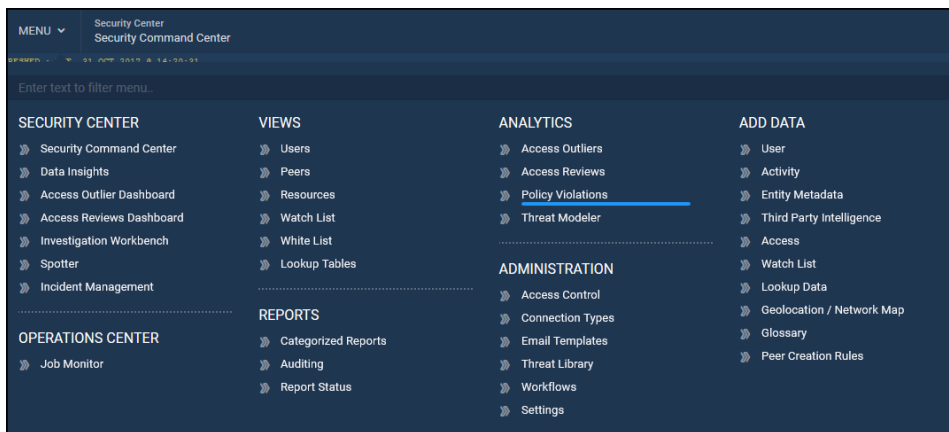
Entity Name	Watch List Type	Reason	Confidence Level (between 0 to 1)	expirydate	watchlistname	createdate	decayflag
1006	Users	Part Time Employee	1.0	09/06/2027 17:57:38	Part Time Employees	09/08/2017 17:57:40	false
1007	Users	Part Time Employee	1.0	09/06/2027 17:57:38	Part Time Employees	09/08/2017 17:57:40	false
1008	Users	Part Time Employee	1.0	09/06/2027 17:57:38	Part Time Employees	09/08/2017 17:57:40	false
1009	Users	Part Time Employee	1.0	09/06/2027 17:57:38	Part Time Employees	09/08/2017 17:57:40	false
1082	Users	Part Time Employee	1.0	09/06/2027 17:57:38	Part Time Employees	09/08/2017 17:57:40	false
1119	Users	Part Time Employee	1.0	09/06/2027 17:57:38	Part Time Employees	09/08/2017 17:57:40	false
1204	Users	Part Time Employee	1.0	09/06/2027 17:57:38	Part Time Employees	09/08/2017 17:57:40	false
1233	Users	Part Time Employee	1.0	09/06/2027 17:57:38	Part Time Employees	09/08/2017 17:57:40	false
1400	Users	Part Time Employee	1.0	09/06/2027 17:57:38	Part Time Employees	09/08/2017 17:57:40	false
1409	Users	Part Time Employee	1.0	09/06/2027 17:57:38	Part Time Employees	09/08/2017 17:57:40	false
1410	Users	Part Time Employee	1.0	09/06/2027 17:57:38	Part Time Employees	09/08/2017 17:57:40	false
1411	Users	Part Time Employee	1.0	09/06/2027 17:57:38	Part Time Employees	09/08/2017 17:57:40	false
1668	Users	Part Time Employee	1.0	09/06/2027 17:57:38	Part Time Employees	09/08/2017 17:57:40	false

For more information about this screen, see [Views](#).

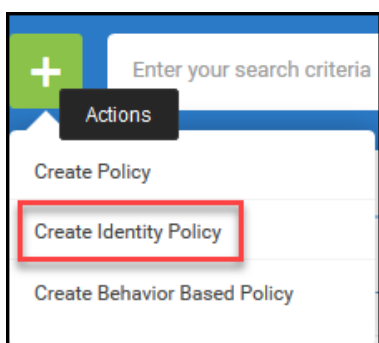
Example Access Policy: Accounts with Privileged Access on Active Directory

This Identity/Access Policy detects users belonging to privileged groups in Active Directory. This policy is applied to access accounts. Use the following steps to create this policy:

1. Navigate to **Menu > Analytics > Policy Violations**:



2. Click +.
3. Select **Create Identity Policy**.



Enter Policy Details

Define Policy

1. Complete the following information:

DEFINE POLICY

Policy Name*

Accounts with Privileged Access on Active Directory

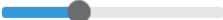
Provide unique name which will describe what type of violation it detects. Special characters are not allowed. Example: { - (bracket), ' - (single quote) are not allowed

Description

Users belonging to privileged groups in Active Directory

Criticality

Low



Select the criticality of the policy. The criticality affects the risk score for the user. None=0.0, Low=0.2, Medium=0.6 and High=1.0



Select Violation Entity*

Access Account

Select the entity that the risk should apply to?

Users - Returns list of users violating policy. Orphan accounts(or uncorrelated accounts) will be ignored.

Datasource

Select the datasource that this policy should run on. For policies that do not run on any data source, you can leave this as blank (Example: Users with upcoming termination date).

- a. **Policy Name:** Accounts with Privileged Access on Active Directory.
- b. **Description:** Users belonging to privileged groups in Active Directory.
- c. **Criticality:** Low.
- d. **Select Violation Entity:** Access Account.
- e. **Datasource:** Active Directory.

Additional Details

ADDITIONAL DETAILS

Owner

Select the owner of the policy. This can be used for sending notifications and case management. The category widget on the security dashboard is visible to policy owners.

Remediator

Select the remediator for the policy. The remediator can be sent notifications and used in case management.

Stop when violations are greater than

- Owner:** None.
- Remediator:** None.
- Stop when violation are greater than:** 10,000.

Define Risk and Threat

- Complete the following:

DEFINE RISK AND THREAT

Category*
Create New Policy Category

Category is displayed on dashboard as a widget and risk will be aggregated for policies with the same category. All violations of the same category will be available in the widget.

Threat Indicator*
Create New Threat Indicator Edit Killchain Stage and Response Actions

Violations detected are indicative of threat

- Category:**Account Misuse.
 - Threat Indicator:** Example: Rare Login to Critical Server.
- Click **Save & Next** to proceed to **Select Policy Template**.

Select Policy Template

1. Select the following template: **Accounts with defined Access Privileges on Resource.**

Enter Policy Details | **Select Policy Template** | Provide Conditions | Choose Action for Violation Results

Templates combine a group of tables which would be used in the query.

Filter templates

Template Name	Template Description	Objects Available
Users with defined account types on Resource	Enables policies that include User attributes, Access account attributes and Resource attributes	USER,RESOURCE,ACCESS ACCOUNT
Accounts with defined Access Privileges on Resource	Enables policies that include Access account attributes and Resource attributes	RESOURCE,ACCESS ACCOUNT,RESOURCEACCESSMETADATA,ACCESS VALUES,ACCESS ACCOUNT USER
Separation of Duties Checks (Access Based)	Enables policies that include User attributes, Resource attributes, Accessaccount attributes and access values	USER,RESOURCE,ACCESS ACCOUNT,RESOURCEACCESSMETADATA,ACCESS VALUES
Users with defined Access Privileges on Resource	Enables policies that include User attributes, Access account attributes and Resource attributes	USER,RESOURCE,ACCESS ACCOUNT,RESOURCEACCESSMETADATA,ACCESS VALUES
Accounts that dont have Users	Orphaned Accounts	RESOURCE,ACCESS ACCOUNT,ACCESS ACCOUNT USER
SOD-User - Accessaccount - Resource - Access Values	Enables policies that include User attributes, Resource attributes, Accessaccount attributes and access values	USER,RESOURCE,ACCESS ACCOUNT,ACCESS VALUES

2. Click **Save & Next** to proceed to **Provide Conditions.**

Provide Conditions

1. Click **+ New Group**.
2. **Enable attribute functions:** No.
3. **Enable value functions:** No.
4. Use dropdown to add the following rules:

Enter Policy Details | Select Policy Template | **Provide Conditions** | Choose Action for Violation Results

Enable attribute functions: ☐ No ☒ Yes

Enable value functions: ☐ No ☒ Yes

+ Add new group

Object	Attributes	Condition	Value	AND/OR	Enable
RESOURCEACCESSMETADA...	ATTRIBUTE	Equal To	MemberOf	AND	Yes
ACCESS VALUES	ACCESS LEVEL 1	Contains	CN=Account Operators	OR	Yes
ACCESS VALUES	ACCESS LEVEL 1	Contains	CN=Administrators	OR	Yes
ACCESS VALUES	ACCESS LEVEL 1	Contains	CN=Domain Admins	OR	Yes
ACCESS VALUES	ACCESS LEVEL 1	Contains	CN=Enterprise Admins	OR	Yes
ACCESS VALUES	ACCESS LEVEL 1	Contains	CN=Backup Operators	OR	Yes
ACCESS VALUES	ACCESS LEVEL 1	Contains	CN=Distributed COM Ut	OR	Yes
ACCESS VALUES	ACCESS LEVEL 1	Contains	CN=Cert Publishers	OR	Yes
ACCESS VALUES	ACCESS LEVEL 1	Contains	CN=DnsAdmins	OR	Yes

1. **Object:** ResourceAccessMetadata | **Attribute:** Attribute | **Condition:** Equal To | **Value:** MemberOf
5. Click **Add New Group** to add a group with the following rules:

1. **Object:** Access Values | **Attribute:** Access Level 1 | **Condition:** Contains | **Value:** CN=A-account Operators
 2. **Object:** Access Values | **Attribute:** Access Level 1 | **Condition:** Contains | **Value:** CN=A-Administrators
 3. **Object:** Access Values | **Attribute:** Access Level 1 | **Condition:** Contains | **Value:** CN=D-Domain Admins
 4. **Object:** Access Values | **Attribute:** Access Level 1 | **Condition:** Contains | **Value:** CN=D-Domain Admins
 5. **Object:** Access Values | **Attribute:** Access Level 1 | **Condition:** Contains | **Value:** CN=Backup Operators
 6. **Object:** Access Values | **Attribute:** Access Level 1 | **Condition:** Contains | **Value:** CN=Distributed COM Users
 7. **Object:** Access Values | **Attribute:** Access Level 1 | **Condition:** Contains | **Value:** CN=Cert Publishers
 8. **Object:** Access Values | **Attribute:** Access Level 1 | **Condition:** Contains | **Value:** CN=D-DnsAdmins
 9. **Object:** Access Values | **Attribute:** Access Level 1 | **Condition:** Contains | **Value:** CN=Group Policy Creator Owners
 10. **Object:** Access Values | **Attribute:** Access Level 1 | **Condition:** Contains | **Value:** CN=DHCP Administrators
 11. **Object:** Access Values | **Attribute:** Access Level 1 | **Condition:** Contains | **Value:** CN=Incoming Forest Trust Builders
 12. **Object:** Access Values | **Attribute:** Access Level 1 | **Condition:** Contains | **Value:** CN=Network Configuration Operators
 13. **Object:** Access Values | **Attribute:** Access Level 1 | **Condition:** Contains | **Value:** CCN-N=Print Operators
 14. **Object:** Access Values | **Attribute:** Access Level 1 | **Condition:** Contains | **Value:** CN=-Schema Admins
 15. **Object:** Access Values | **Attribute:** Access Level 1 | **Condition:** Contains | **Value:** CN=Server Operators
 16. **Object:** Access Values | **Attribute:** Access Level 1 | **Condition:** Contains | **Value:** CN=WinRMRemoteWMIUsers
6. Click **Preview** to view the HQL query.
7. Click **Save & Next** to proceed to **Choose Action for Violation Results**.

Choose Action for Violation Results

1. Complete the following information:

VIOLATION ACTION

Send Notification

☐ NO

Add Policy Violators to Watchlist?

Privileged Accounts

Remove Watch List

Confidence Factor

1.0

From a scale of 0 to 1, how confident are you that the violator should be on this watchlist

Rule to remove Violators from Watchlist

☒ YES

Remove Violators from Watchlist

Reduce Confidence Factor

Decay Factor

1.0

- a. **Send notification:** No.
 - b. **Add Policy Violators to Watchlist?:** Privileged Accounts.
 - c. **Confidence Factor:** 1.
 - d. **Rule to remove Violators from Watchlist:** YES.
 - a. **Remove Violators from Watchlist:** Reduce Confidence Factor.
 - b. **Decay Factor:** 1.0.
2. Click **Save** to proceed to [Viewing, Enabling, and Editing Policies](#).
 3. Find violations in the **Security Command Center**.
 4. View and manage users in Watch list:
 1. Navigate to **Menu > Views > Users**.
 2. Click Watch list name on left navigation panel Privileged Accounts.


Viewing, Enabling, and Editing Policies

From the **Menu > Analytics > Policy Violations** main screen, you can view information for all policies, search for a specific policy, enable or disable policies, take actions on policies, and edit policies.

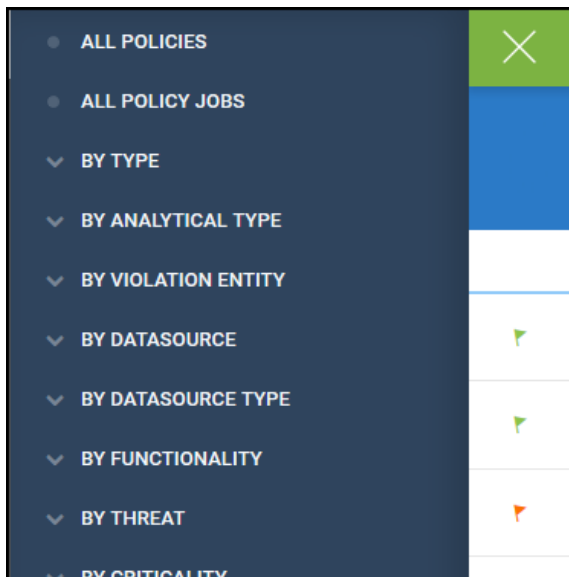
Enter your search criteria									
Name	Type	Analytical Type	Datasource	Datasource Type	Functionality	Last Update Date	Violation Entity	Enabled?	Actions
Abnormal amount of data uploads compared to past behavior NU-1	Real Time Policy	Tier 2 Behavior Summary	Bluecoat Proxy	Bluecoat Proxy			Activity Account	<input type="checkbox"/>	
Abnormal number of data uploads compared to past behavior NU-1	Real Time Policy	Tier 2 Behavior Summary	Bluecoat Proxy	Bluecoat Proxy			Activity Account	<input type="checkbox"/>	
Accounts that belong to terminated user	Identity Policy	-				2017-10-02 14:11:58.0	Access Account	<input checked="" type="checkbox"/>	
Accounts that dont have Users	Identity Policy	-				2015-04-02 22:11:43.0	Access Account	<input checked="" type="checkbox"/>	
Accounts where user dont have manager	Identity Policy	-				2015-04-02 22:12:15.0	Access Account	<input checked="" type="checkbox"/>	
Accounts with Domain Admin Access	Identity Policy	-				2015-04-02 22:21:56.0	Access Account	<input checked="" type="checkbox"/>	
Accounts with Privileged Access on Active Directory	Identity Policy	-				2015-04-02 22:21:18.0	Access Account	<input checked="" type="checkbox"/>	
Activity by terminated user - Windows-5	Real Time Policy	-	Windows Data	OS			Activity Account	<input type="checkbox"/>	
Admin activity by non-admin accounts-5	Real Time Policy	-	Windows Data	OS			Activity Account	<input type="checkbox"/>	
Age Based Anomaly-7	Real Time Policy	-	Cerner Healthcare Data	Cerner Data			Activity Account	<input type="checkbox"/>	
Audit log tampering	Real Time Policy	-	Windows Data	OS		2017-09-11 20:35:58.0	Activity Account	<input type="checkbox"/>	
Contractors with remote login access	Identity Policy	-				2015-02-09 18:20:12.0	Access Account	<input checked="" type="checkbox"/>	
Contractors with upcoming						2015-04-02		<input checked="" type="checkbox"/>	

Policy Violations

View Policies

1. Click  to open left navigation menu.

Click X to collapse the menu.



2. Select a menu option and click on the main screen.

- **All Policies:** View all available policies.
- **All Policy Jobs:** View and perform actions on policy jobs.

ALL POLICIES

ALL POLICY JOBS

BY TYPE

BY ANALYTICAL TYPE

BY VIOLATION ENTITY

Users

Activity Account

Access Account

Resources

Network Address

BY DATASOURCE

BY DATASOURCE TYPE

BY FUNCTIONALITY

BY THREAT

BY CRITICALITY

Analytics
Policy Violations

Enter text to search...

Refresh

Name	Creation Date	Start Date	Next Trigger Date	End Date	Status	Created By	Actions
Test Watchlist Removal_1506553163242	Wed Sep 27 17:59:25 CDT 2017	Wed Sep 27 17:59:25 CDT 2017		Wed Sep 27 17:59:26 CDT 2017	Completed	admin	<div><div></div><div></div><div></div></div>
Test Employee 89_1506553008703	Wed Sep 27 17:56:58 CDT 2017	Wed Sep 27 17:56:58 CDT 2017		Wed Sep 27 17:56:58 CDT 2017	Completed	admin	<div><div></div><div></div><div></div></div>
Test Watchlist Removal_1506552843597	Wed Sep 27 17:54:06 CDT 2017	Wed Sep 27 17:54:06 CDT 2017		Wed Sep 27 17:54:07 CDT 2017	Completed	admin	<div><div></div><div></div><div></div></div>
Test Watchlist Removal_1506551937228	Wed Sep 27 17:39:02 CDT 2017	Wed Sep 27 17:39:02 CDT 2017		Wed Sep 27 17:39:03 CDT 2017	Completed	admin	<div><div></div><div></div><div></div></div>
Test Watchlist Removal_1506551256288	Wed Sep 27 17:27:43 CDT 2017	Wed Sep 27 17:27:43 CDT 2017		Wed Sep 27 17:27:47 CDT 2017	Completed	admin	<div><div></div><div></div><div></div></div>
Part Time Employee_1504911456258	Fri Sep 08 17:57:39 CDT 2017	Fri Sep 08 17:57:39 CDT 2017		Fri Sep 08 17:57:41 CDT 2017	Completed	admin	<div><div></div><div></div><div></div></div>

First

<

1

>

Last

Show

10

Total results : 6 | Total pages : 1

Actions

	View job details
	Re-run job
	Delete job

- **By Type:** Select an option to view only policies of the selected policy type.
Example: Behavior based policy.
- **By Analytical Type:** Select an option to view only policies of the selected analytical type configured during Provide Conditions step. Example: Flag Violators Based on Peers.
- **By Violation Entity:** Select an option to view only policies with the selected violation entity.
Example: Users.
- **By Datasource:** Select an option to view only policies that run on the selected datasource.
Example: Bluecoat Proxy.
- **By Datasource Type:** Select an option to view only policies that run on the selected data-source type. Example: Bluecoat Proxy [Regex]

- **By Functionality:** Select an option to view policies that run on the selected functionality type. Example: Web Proxy.
- **By Threat:** Select an option to view only policies with the selected threat indicator configured during Enter Policy Details step. Example: Critical Data Exfiltrated.
- **By Criticality:** Select an option to view only policies configured with the selected criticality. Example: High.

Enable Policies

By default, policies are enabled to run against imported data unless they are disabled. To disable or enable a policy, complete the steps:

Name ⓘ	Type	Analytical Type	Datasource	Datasource Type	Functionality	Last Update Date	Violation Entity	Enabled?	Actions
Abnormal amount of data uploads compared to past behavior NU-1	Real Time Policy	Tier 2 Behavior Summary	Bluecoat Proxy	Bluecoat Proxy			Activity Account	<input type="checkbox"/>	
Abnormal number of data uploads compared to past behavior NU-1	Real Time Policy	Tier 2 Behavior Summary	Bluecoat Proxy	Bluecoat Proxy			Activity Account	<input type="checkbox"/>	
Accounts that belong to terminated user	Identity Policy	-				2017-10-02 14:11:58.0	Access Account	<input checked="" type="checkbox"/>	

1. Toggle **Enabled?** to **Yes** or **No**.

- **No:** Policies will not run against imported data.
- **Yes:** Policies will run against imported data.

Take Action on Policies

You can take the following actions on policies on the Policy Violations main screen:

	Run policy Note: This option is only available for policies that have been enabled.
	Delete policy

Edit Policies

To edit an existing policy, click the policy name from the Policy Violations main screen and complete the following steps as needed:

1. Edit policy details.
2. Edit templates.
3. Edit conditions.
4. Edit actions for violation results.

Searching Policies using Spotter

Navigate to **Menu > Security Center > Spotter** to view the policies you configured to appear in the Summary and search for violations for specific policies.



Note: See [Spotter](#) for complete details about searching.

View the number of violations for the policies you configured to appear on the Summary screen in the previous steps.

The screenshot shows the Spotter interface with a search bar at the top. Below the search bar, there are two main sections: "AVAILABLE VIOLATIONS" and "AVAILABLE DATASOURCES".

AVAILABLE VIOLATIONS: This section lists various violation types with their respective counts. A red box highlights the following violations:

Violation Type	Count
Spike in amount of bytes out	1,180
Robotic beaconing traffic detected	379
Spam Email	193
Spike in Number of Records accessed by an Employee	120
Critical vulnerabilities detected	114
Excessive number of emails to personal email address	104
Flight Risk User - Job Search	31
File Copy Blocked By DLP	23
Potential Data Snooping Activity	18
Suspicious Process Detected	5
LandSpeed Violation - VPN	2
Privilege Escalation	2
Rare Login to Critical Server	1

AVAILABLE DATASOURCES: This section lists data sources with their respective event counts.

Data Source	Total Events
Infoblox	5,967,763
Ironport Data	1,103

Click a policy to view the available violations for that policy OR search for a specific policy using the following syntax: `polycname = [policy name]`. Example: `polycname = "Flight Risk User - Job Search"`.

The screenshot shows the Spotter interface with a search bar containing the query `polycname = "Flight Risk User - Job Search"`. Below the search bar, there is a bar chart showing the number of events over time. The search results are displayed in a table format.

Search Results:

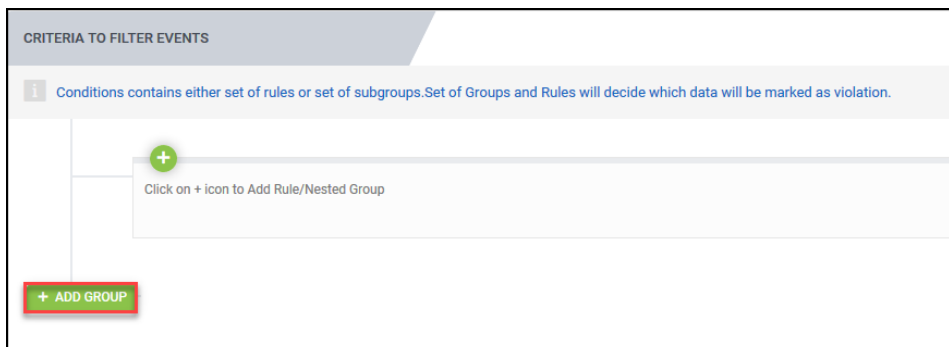
Field	Value
accountname	OGWA.HARRY
bytesin	6946
bytesout	488
destinationhostname	https://quintiles.taleo.net
destinationport	8443
requestclientapplication	Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.112 Safari/537.36
requesturl	https://quintiles.taleo.net/careersection/10080/jobdetail.ft?job=1704064&lang=en&src=JB-118
requestmethod	POST
deviceeventcategory	Job Search
category	ACCOUNT MISUSE
polycname	Flight Risk User - Job Search
riskthreatname	Possible Flight Risk Users
violation	Activityaccount
companycode	TECH
costcentername	INFCCC12
country	USA
department	Mainframe and Midrange Administration
division	Global Technology
employeid	1001
employeetype	FT
employeetypedescription	FullTime
firstname	HARRY
hiredate	08/08/2009 00:00:00.000
jobcode	R1
land	HO1001
lastname	OGWA
location	DALLAS
manageremployeid	1012
middlename	A
status	1
statusdescription	Active
title	Vice President Mainframe and Midrange
workemail	HARRY.OGWA@sonix.com
workphone	9723451278
approveremployeid	1082
mobile	0151 709 7593
lastperformanceviewdate	04/01/2014 00:00:00.000
usercriticality	Low
companynumber	TECH12
province	FL
street	9000 SOUTHSIDE BLVD BLDG 600
regtempin	Regular
lastperformanceviewresult	Poor
costcentercode	INFCCC12
networkid	HOGWA
zipcode	32256
orgunitnumber	12
city	JACKSONVILLE
managerfirstname	Joe
fulltimeparttimein	FullTime
userriskscore	0.01
usertimezoneoffset	CST

Conditions

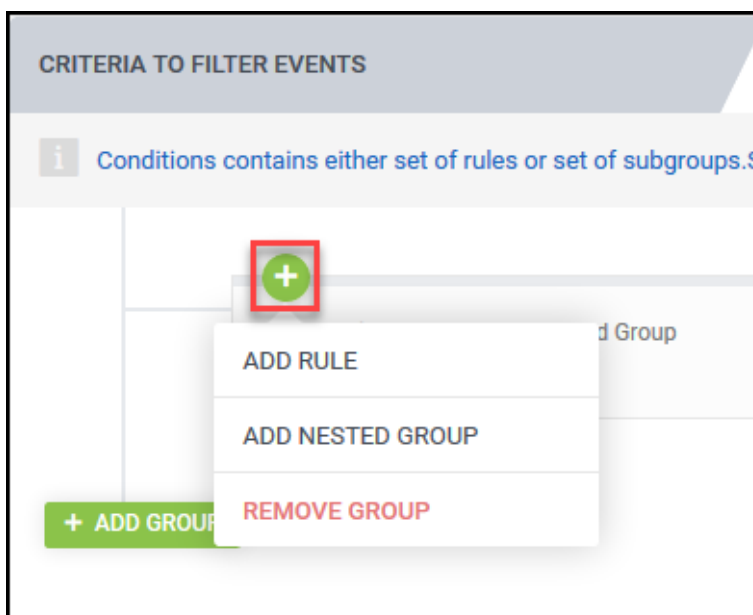
Conditions contain a set of rules or set of nested groups of rules. Sets of groups and rules decide which data will be marked as a violation.

To configure Conditions during [Policy Violations](#) **Step 2: Providing Conditions > Criteria to Filter Events**, complete the following steps:

1. Click **Add Group** for each condition group you would like to add.



2. Click + to **Add Rule** or **Add Nested Group**.



- **Add Rule:** Complete the following information in pop up window:

- Select Event Attribute:** Select an attribute from the dropdown.
Example: Email Recipient Domain.



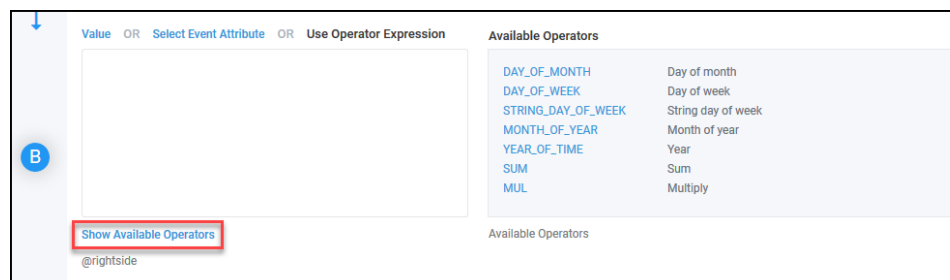
Note: Event Attributes are organized by Object. Example: **Object:** EVENT-EMAIL |
Event Attribute: Email Recipient Domain.

OR

Click **Use Operator Expression** to configure the operator. See [Operators](#) for more information.

- Select Condition:** Select from the dropdown. Example: Equal To.
- Value:**
 - Provide a value to match to the source criteria. Example: competitor.com.
OR
 - Click **Select Event Attribute** to select an attribute from the dropdown.
Example: Email Recipient.
OR

- Click **Use Operator Expression** to configure the operator.



- Add Nested Group:** Click **Add Rule** to add rules within each group.
- Remove Group:** Click to remove groups.



Note: Deleting a Group will delete all Rules within the Group.

Example 1: One Rule

To configure a single group with one rule, complete the following steps:

1. Click **Add Group**.
2. Click **+**.
3. Click **Add Rule**.
4. Complete the following information:

The screenshot shows the 'CREATE NEW RULE' dialog box. It has a title bar with a green '+' icon and a '< BACK' button. The main area is divided into three sections, each with a blue circle icon (A, B, and C) and a downward arrow. Section A is labeled 'Select Event Attribute OR Use Operator Expression' and contains a dropdown menu with 'Email Recipient Domain' selected and a placeholder '@leftside'. Section B is labeled 'Select Condition' and contains a dropdown menu with 'Equal To' selected and a placeholder '@middlecondition'. Section C is labeled 'Value OR Select Event Attribute OR Use Operator Expression' and contains a text input field with 'competitor.com' and a placeholder '@rightside'. At the bottom right, there are 'Cancel' and 'Add' buttons.

- a. **Select Event Attribute:** Select an event attribute from the dropdown.
Example: Email Recipient Domain.



Note: Event Attributes are organized by Object. Example: **Object:** EVENT-EMAIL | **Event Attribute:** Email Recipient Domain. The available objects depend on the attributes mapped for the selected data source or data source type.

OR

Operator: Click **User Operator Expression** to configure the operator. See [Operators](#) for more information.

- b. **Condition:** Select from the dropdown. Example: Equal To.
- c. **Value:**

- Provide a value to match to the source criteria. Example: competitor.com.

OR

- Click **Select Event Attribute**
 - Select an attribute from the dropdown. Example: Email Recipient.

OR

Operator: Click **User Operator Expression** to configure the operator.

Example 2: Multiple Groups with Multiple Rules

To configure a multiple groups with multiple rules, complete the following:

Group 1

1. Click **Add Group**.
2. Click **+ > Add Rule** to add each rule to the Group.



Note: Click EDIT to edit existing rules. Click DELETE to delete existing rules.

3. Complete the following for the first Group:

Conditions contains either set of rules or set of subgroups. Set of Groups and Rules will decide which data will be marked as violation.

+

Resource Group Name EQUAL TO Active Directory EDIT DELETE

AND

Account Owner EQUAL TO MemberOf EDIT DELETE

AND

Source User Privileges EQUAL TO Accounts Receivable EDIT DELETE

AND

+

Resource Group Name EQUAL TO Active Directory EDIT DELETE

AND

Account Owner EQUAL TO MemberOf EDIT DELETE

AND

Source User Privileges EQUAL TO Accounts Payable EDIT DELETE

Rule 1

- a. **Select Event Attribute:** Select dropdown. Example: Resource Group Name.

OR

Operator: Click **User Operator Expression** to configure the operator. See [Operators](#) for more information.

- b. **Condition:** Select from the dropdown. Example: Equal To.

- c. **Value:**

- Provide a value to match to the source criteria. Example: Active Directory.

OR

- Click **Select Event Attribute** to select an attribute from the dropdown.

OR

Operator: Click **User Operator Expression** to configure the operator.

Rule 2

- a. **Select Event Attribute:** Select dropdown. Example: Account Owner.

OR

Operator: Click **User Operator Expression** to configure the operator.

- b. **Condition:** Select from the dropdown. Example: Equal To.

- c. **Value:**

- Provide a value to match to the source criteria. Example: MemberOf.

OR

- Click **Select Event Attribute** to select an attribute from the dropdown.

OR

Operator: Click **User Operator Expression** to configure the operator.

Rule 3

- a. **Attribute:** Select dropdown. Example: Source User Privileges.

OR

Operator: Click **User Operator Expression** to configure the operator.

- b. **Condition:** Select from the dropdown. Example: Equal To.

- c. **Value:**

- Provide a value to match to the source criteria. Example: Account Receivable.

OR

- Click **Select Event Attribute** to select an attribute from the dropdown.

OR

Operator: Click **User Operator Expression** to configure the operator.

Group 1

1. Click **Add Group**.
2. Click **+ > Add Rule** to add each rule to the Group.
3. Complete the following for the second Group:

The screenshot shows the 'Conditions' configuration page. At the top, a message states: 'Conditions contains either set of rules or set of subgroups. Set of Groups and Rules will decide which data will be marked as violation.' Below this, there are two rule groups. The first group contains three rules: 'Resource Group Name EQUAL TO Active Directory', 'Account Owner EQUAL TO MemberOf', and 'Source User Privileges EQUAL TO Accounts Receivable'. The second group, which is highlighted with a red box, contains three rules: 'Resource Group Name EQUAL TO Active Directory', 'Account Owner EQUAL TO MemberOf', and 'Source User Privileges EQUAL TO Accounts Payable'. Each rule has 'EDIT' and 'DELETE' links. Between the groups and at the end of each group is an 'AND' dropdown menu. A green plus icon is visible at the top of each group's rule list.

Rule 1

- Select Event Attribute:** Select dropdown. Example: Resource Group Name.
OR
Operator: Click **User Operator Expression** to configure the operator. See [Operators](#) for more information.
- Condition:** Select from the dropdown. Example: Equal To.
- Value:**
 - Provide a value to match to the source criteria. Example: Active Directory.
OR
 - Click **Select Event Attribute** to select an attribute from the dropdown.
OR
 - Operator:** Click **User Operator Expression** to configure the operator.

Rule 2

- a. **Attribute:** Select dropdown. Example: Account Owner.
OR
Operator: Click **User Operator Expression** to configure the operator.
- b. **Condition:** Select from the dropdown. Example: Equal To.
- c. **Value:**
 - Provide a value to match to the source criteria. Example: MemberOf.OR
 - Click **Select Event Attribute** to select an attribute from the dropdown.OR
Operator: Click **User Operator Expression** to configure the operator.

Rule 3

- a. **Attribute:** Select dropdown. Example: Source User Privileges.
OR
Operator: Click **User Operator Expression** to configure the operator.
- b. **Condition:** Select from the dropdown. Example: Equal To.
- c. **Value:**
 - Provide a value to match to the source criteria. Example: Account Payable.OR
 - Click **Select Event Attribute** to select an attribute from the dropdown.OR
Operator: Click **User Operator Expression** to configure the operator.

Operators

You can use operators in place of attributes or values. To use an operator in place of an attribute or value, click **User Operator Expression**.

CREATE NEW RULE

< BACK

A

↓

↓

B

Select Event Attribute OR **Use Operator Expression**

-Select-

@leftside

Select Condition

Equal To

@middlecondition

Value OR Select Event Attribute OR **Use Operator Expression**

@rightside

Cancel

Add

The **Operator** field will appear.

CREATE NEW RULE

< BACK

A

↓

↓

B

Select Event Attribute OR Use Operator Expression

Show Available Operators

@leftside

Select Condition

Equal To ▼

@middlecondition

Value OR Select Event Attribute OR Use Operator Expression

@rightside

Cancel

Add

Click **Show Available Operators** to select an operator.

CREATE NEW RULE

< BACK

A

Select Event Attribute OR Use Operator Expression

Show Available Operators

@leftside

↓

B

Value OR Select Event Attribute OR Use Operator Expression

@rightside

Available Operators

DAY_OF_MONTH	Day of month
DAY_OF_WEEK	Day of week
STRING_DAY_OF_WEEK	String day of week
MONTH_OF_YEAR	Month of year
YEAR_OF_TIME	Year
SUM	Sum
MUL	Multiply

Available operator info

Select Condition

Equal To

@middlecondition

Cancel

Add

ArcSight UBA includes the following operators:

Conditions

Day of Month

1. Select **Day of Month** from **Available Operators**.

CREATE NEW RULE

< BACK

Select Event Attribute OR Use Operator Expression

DAY_OF_MONTH(Epoch Time Long 1)

Show Available Operators
@leftside

Available Operators

DAY_OF_MONTH	Day of month
DAY_OF_WEEK	Day of week
STRING_DAY_OF_WEEK	String day of week
MONTH_OF_YEAR	Month of year
YEAR_OF_TIME	Year
SUM	Sum
MUL	Multiply

Available operator info

Select Condition

Equal To

@middlecondition

Value OR Select Event Attribute OR Use Operator Expression

@rightside

Cancel

Add

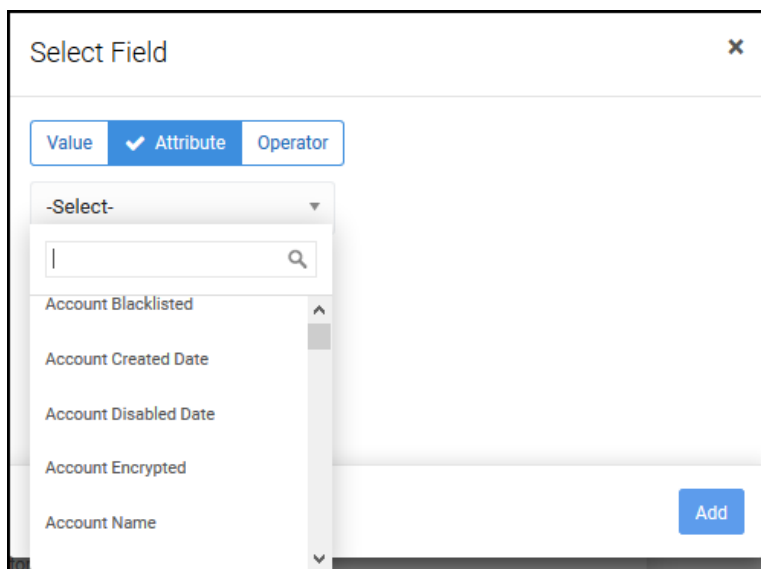
2. Click **Epoch Time Long 1** to select one of the following:

- **Value:** Enter a value. Example: 28.



The screenshot shows a dialog box titled "Select Field" with a close button (X) in the top right corner. Inside the dialog, there are three tabs: "Value" (which is selected and has a checkmark), "Attribute", and "Operator". Below the tabs is a large, empty text input field. At the bottom right of the dialog is a blue "Add" button.

- **Attribute:** Select from dropdown.



The screenshot shows the same "Select Field" dialog box, but now the "Attribute" tab is selected and has a checkmark. A dropdown menu is open below the tabs, showing a search bar with a magnifying glass icon and a list of attributes: "Account Blacklisted", "Account Created Date", "Account Disabled Date", "Account Encrypted", and "Account Name". The dropdown menu has up and down arrow icons on its right side. The "Add" button is still visible at the bottom right.

- **Operator:** Click to add an operator nested inside the Day_of_Month operator. Click the field to specify the value of the nested operator.

Select Field
✕

ValueAttributeOperator

DAY_OF_MONTHDay of month
DAY_OF_WEEKDay of week
STRING_DAY_OF_WEEKString day of week
MONTH_OF_YEARMonth of year
YEAR_OF_TIMEYear
SUMSum
MULMultiply
DIVDivide
SUBSubtract
BETWEENRange

Conditions

Day of Week

1. Select **Day of Week** from **Available Operators**.

CREATE NEW RULE

< BACK

A

↓

B

Select Event Attribute OR Use Operator Expression

DAY_OF_WEEK(Epoch Time Long 1)

Show Available Operators
@leftside

Select Condition

Equal To

@middlecondition

Value OR Select Event Attribute OR Use Operator Expression

@rightside

Available Operators

DAY_OF_MONTH	Day of month
DAY_OF_WEEK	Day of week
STRING_DAY_OF_WEEK	String day of week
MONTH_OF_YEAR	Month of year
YEAR_OF_TIME	Year
SUM	Sum
MUL	Multiply

Available operator info

Cancel

Add

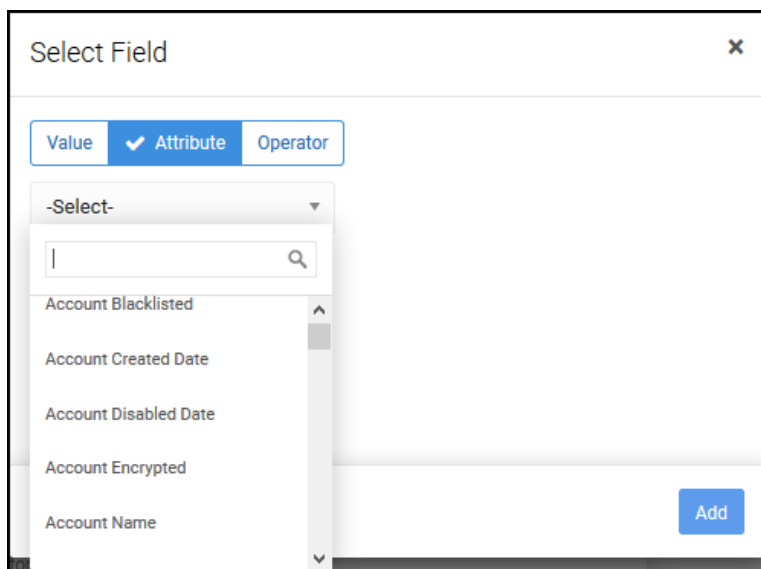
2. Click **Epoch Time Long 1** to select one of the following:

- **Value:** Enter a value. Example: 5.



The screenshot shows a dialog box titled "Select Field" with a close button (X) in the top right corner. Inside the dialog, there are three tabs: "Value" (which is selected and has a checkmark), "Attribute", and "Operator". Below the tabs is a large, empty text input field. At the bottom right of the dialog is a blue "Add" button.

- **Attribute:** Select from dropdown.



The screenshot shows the same "Select Field" dialog box, but now the "Attribute" tab is selected and has a checkmark. A dropdown menu is open below the tabs, showing a search bar and a list of attributes: "Account Blacklisted", "Account Created Date", "Account Disabled Date", "Account Encrypted", and "Account Name". The dropdown menu has a scroll bar on the right. The "Add" button is still visible at the bottom right.

- **Operator:** Click to add an operator nested inside the Day_of_Week operator. Click the field to specify the value of the nested operator.

Select Field

×

Value

Attribute

✓ Operator

DAY_OF_MONTHDay of month

DAY_OF_WEEKDay of week

STRING_DAY_OF_WEEKString day of week

MONTH_OF_YEARMonth of year

YEAR_OF_TIMEYear

SUMSum

MULMultiply

DIVDivide

SUBSubtract

BETWEENRange

Conditions

String Day of Week

1. Select **String Day of Week** from **Available Operators**.

CREATE NEW RULE < BACK

Select Event Attribute OR Use Operator Expression

STRING_DAY_OF_WEEK(Epoch Time Long 1)

Show Available Operators
@leftside

Available Operators

DAY_OF_MONTH	Day of month
DAY_OF_WEEK	Day of week
STRING_DAY_OF_WEEK	String day of week
MONTH_OF_YEAR	Month of year
YEAR_OF_TIME	Year
SUM	Sum
MUL	Multiply

Available operator info

Select Condition

Equal To ▼

@middlecondition

Value OR Select Event Attribute OR Use Operator Expression

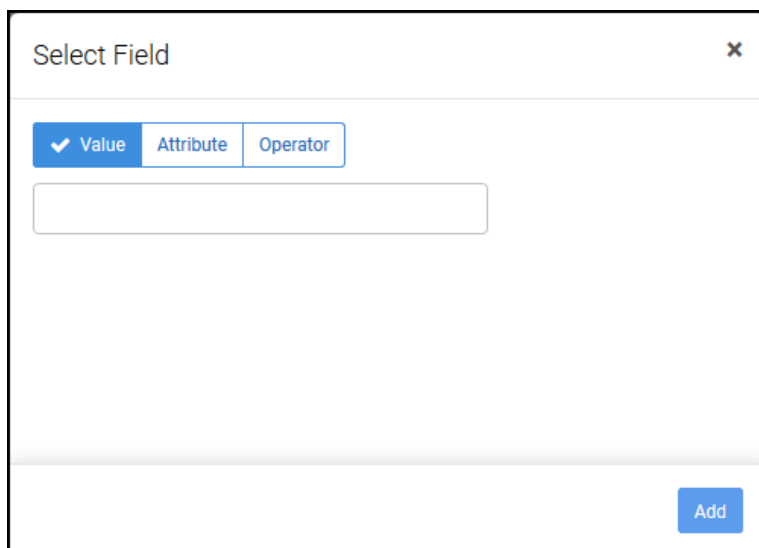
@rightside

Cancel

Add

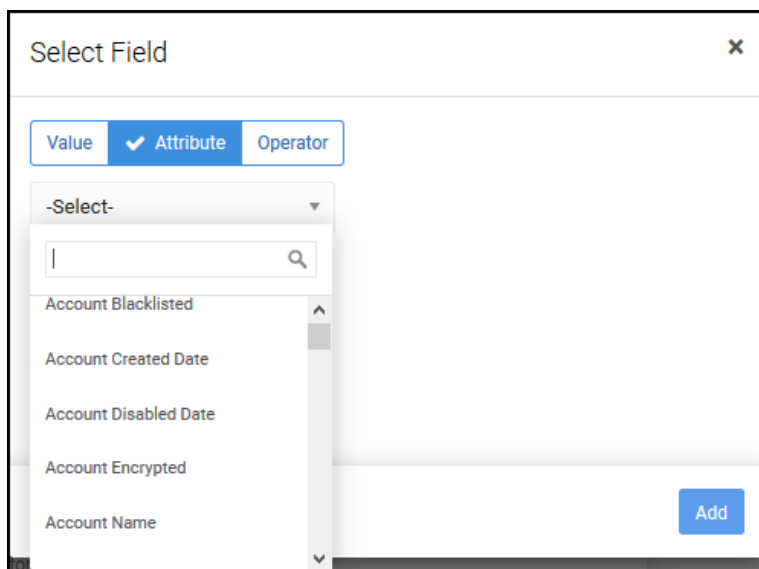
2. Click **Epoch Time Long 1** to select one of the following:

- **Value:** Enter a value. Example: SATURDAY



The screenshot shows a dialog box titled "Select Field" with a close button (X) in the top right corner. Inside the dialog, there are three tabs: "Value" (which is selected and has a checkmark), "Attribute", and "Operator". Below the tabs is a large, empty text input field. At the bottom right of the dialog is a blue "Add" button.

- **Attribute:** Select from dropdown.



The screenshot shows the same "Select Field" dialog box, but now the "Attribute" tab is selected and has a checkmark. A dropdown menu is open below the tabs, showing a search bar with a magnifying glass icon and a list of attributes: "Account Blacklisted", "Account Created Date", "Account Disabled Date", "Account Encrypted", and "Account Name". The dropdown menu has a scroll bar on the right. The "Add" button is still visible at the bottom right.

- **Operator:** Click to add an operator nested inside the String_Day_of_Week operator. Click the field to specify the value of the nested operator.

Select Field

×

Value

Attribute

✓ Operator

DAY_OF_MONTHDay of month

DAY_OF_WEEKDay of week

STRING_DAY_OF_WEEKString day of week

MONTH_OF_YEARMonth of year

YEAR_OF_TIMEYear

SUMSum

MULMultiply

DIVDivide

SUBSubtract

BETWEENRange

Conditions

Month of Year

1. Select **Month of Year** from **Available Operators**.

CREATE NEW RULE < BACK

Select Event Attribute OR Use Operator Expression

MONTH_OF_YEAR(Epoch Time Long 1)

Show Available Operators
@leftside

Available Operators

DAY_OF_MONTH	Day of month
DAY_OF_WEEK	Day of week
STRING_DAY_OF_WEEK	String day of week
MONTH_OF_YEAR	Month of year
YEAR_OF_TIME	Year
SUM	Sum
MUL	Multiply

Available operator info

Select Condition

Equal To

@middlecondition

Value OR Select Event Attribute OR Use Operator Expression

@rightside

Cancel Add

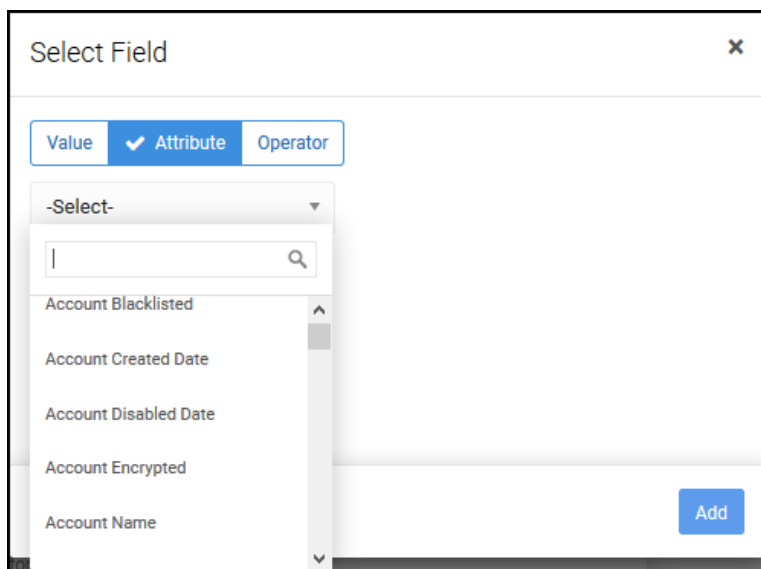
2. Click **Epoch Time Long 1** to select one of the following:

- **Value:** Enter a value. Example: 8.



The screenshot shows a dialog box titled "Select Field" with a close button (X) in the top right corner. Inside the dialog, there are three tabs: "Value" (which is selected and has a checkmark), "Attribute", and "Operator". Below the tabs is a large, empty text input field. At the bottom right of the dialog is a blue "Add" button.

- **Attribute:** Select from dropdown.



The screenshot shows the same "Select Field" dialog box, but now the "Attribute" tab is selected and has a checkmark. A dropdown menu is open below the tabs, showing a search bar and a list of attributes: "Account Blacklisted", "Account Created Date", "Account Disabled Date", "Account Encrypted", and "Account Name". The dropdown menu has a scroll bar on the right. The "Add" button is still visible at the bottom right.

- **Operator:** Click to add an operator nested inside the Month_of_Year operator. Click the field to specify the value of the nested operator.

Select Field
✕

Value	Attribute	✓ Operator
DAY_OF_MONTH	Day of month	
DAY_OF_WEEK	Day of week	
STRING_DAY_OF_WEEK	String day of week	
MONTH_OF_YEAR	Month of year	
YEAR_OF_TIME	Year	
SUM	Sum	
MUL	Multiply	
DIV	Divide	
SUB	Subtract	
BETWEEN	Range	

Conditions

Year of Time

1. Select **Year of Time** from **Available Operators**.

CREATE NEW RULE < BACK

Select Event Attribute OR Use Operator Expression

YEAR_OF_TIME(Epoch Time Long 1)

Show Available Operators
@leftside

Available Operators

DAY_OF_MONTH	Day of month
DAY_OF_WEEK	Day of week
STRING_DAY_OF_WEEK	String day of week
MONTH_OF_YEAR	Month of year
YEAR_OF_TIME	Year
SUM	Sum
MUL	Multiply

Available operator info

Select Condition

Equal To ▼

@middlecondition

Value OR Select Event Attribute OR Use Operator Expression

@rightside

Cancel Add

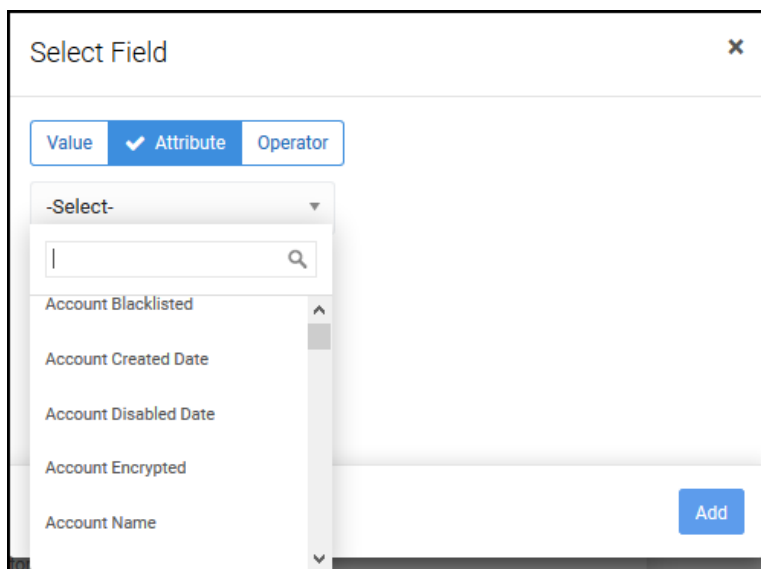
2. Click **Epoch Time Long 1** to select one of the following:

- **Value:** Enter a value. Example: 2017.



The screenshot shows a dialog box titled "Select Field" with a close button (X) in the top right corner. Inside the dialog, there are three tabs: "Value" (which is selected and has a checkmark), "Attribute", and "Operator". Below the tabs is a large, empty text input field. At the bottom right of the dialog is a blue "Add" button.

- **Attribute:** Select from dropdown.



The screenshot shows the same "Select Field" dialog box, but now the "Attribute" tab is selected and has a checkmark. A dropdown menu is open below the tabs, showing a search bar and a list of attributes: "Account Blacklisted", "Account Created Date", "Account Disabled Date", "Account Encrypted", and "Account Name". The dropdown menu has a scroll bar on the right. The "Add" button is still visible at the bottom right.

- **Operator:** Click to add an operator nested inside the Year_of_Time operator. Click the field to specify the value of the nested operator.

Select Field

✕

Value

Attribute

✓ Operator

DAY_OF_MONTH

Day of month

DAY_OF_WEEK

Day of week

STRING_DAY_OF_WEEK

String day of week

MONTH_OF_YEAR

Month of year

YEAR_OF_TIME

Year

SUM

Sum

MUL

Multiply

DIV

Divide

SUB

Subtract

BETWEEN

Range

Conditions

Sum

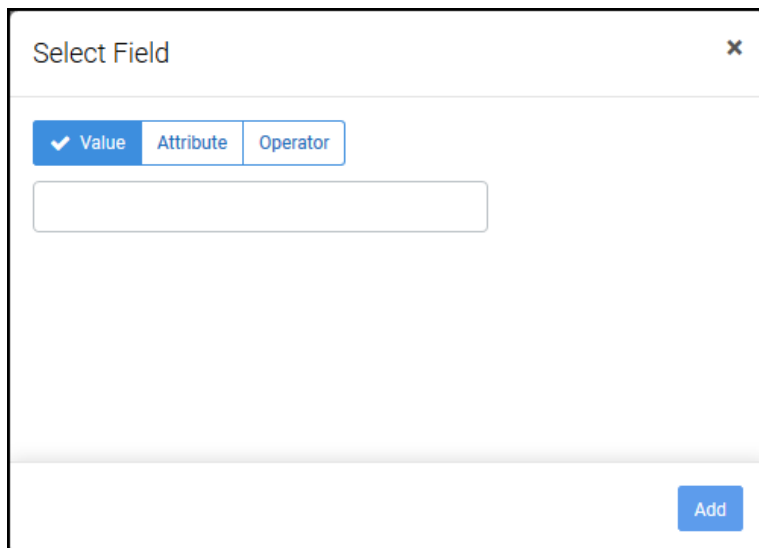
1. Select **Sum** from **Available Operators** to take the sum of three integers.

The screenshot shows the 'CREATE NEW RULE' interface. On the left, a vertical sidebar contains three blue circular buttons labeled 'A', a downward arrow, and 'B'. The main area is divided into three sections. The top section, labeled '@leftside', has tabs for 'Select Event Attribute' and 'Use Operator Expression'. The 'Use Operator Expression' tab is active, showing a text input with the expression 'SUM(Int 1 , Int 2 , Int n)'. To the right of this is a panel titled 'Available Operators' containing a table of operators. The middle section, labeled '@middlecondition', has a tab for 'Select Condition' with a dropdown menu set to 'Equal To'. The bottom section, labeled '@rightside', has tabs for 'Value', 'Select Event Attribute', and 'Use Operator Expression', with the 'Value' tab currently selected and an empty text input field. At the bottom right of the interface are 'Cancel' and 'Add' buttons.

Operator	Description
DAY_OF_MONTH	Day of month
DAY_OF_WEEK	Day of week
STRING_DAY_OF_WEEK	String day of week
MONTH_OF_YEAR	Month of year
YEAR_OF_TIME	Year
SUM	Sum
MUL	Multiply

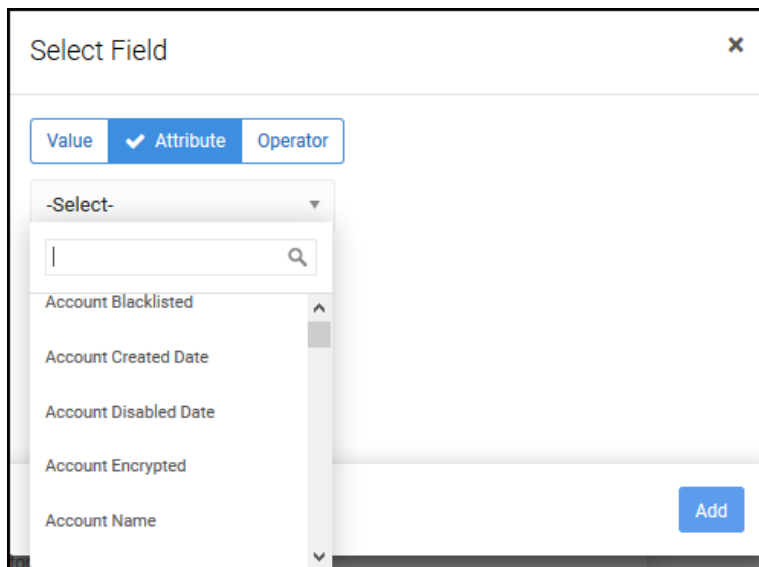
2. Click **INT 1** to select one of the following:

- **Value:** Enter a value.



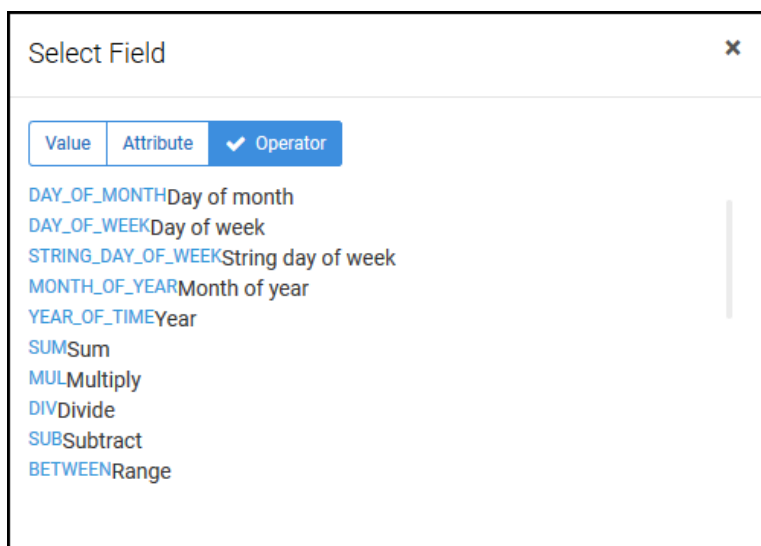
The screenshot shows a dialog box titled "Select Field" with a close button (X) in the top right corner. Inside the dialog, there are three tabs: "Value" (which is selected and has a checkmark), "Attribute", and "Operator". Below the tabs is a large, empty text input field. At the bottom right of the dialog is a blue "Add" button.

- **Attribute:** Select from dropdown.



The screenshot shows the same "Select Field" dialog box, but now the "Attribute" tab is selected and has a checkmark. A dropdown menu is open below the tabs, showing a search bar with a magnifying glass icon and a list of attributes: "Account Blacklisted", "Account Created Date", "Account Disabled Date", "Account Encrypted", and "Account Name". The dropdown menu has up and down arrow icons on its sides. The "Add" button is still visible at the bottom right.

- **Operator:** Click to add an operator nested inside the Sum operator. Click the field to specify the value of the nested operator.



3. Repeat to populate value of **INT 2** and **INT 3**.

Conditions

Mul

1. Select **Mul** from **Available Operators** to multiply integers.

CREATE NEW RULE

< BACK

Select Event Attribute OR Use Operator Expression

MUL(Int 1 , Int 2 , Int n)

Show Available Operators

@leftside

Available Operators

DAY_OF_MONTH	Day of month
DAY_OF_WEEK	Day of week
STRING_DAY_OF_WEEK	String day of week
MONTH_OF_YEAR	Month of year
YEAR_OF_TIME	Year
SUM	Sum
MUL	Multiply

Available operator info

Select Condition

Equal To

@middlecondition

Value OR Select Event Attribute OR Use Operator Expression

@rightside

Cancel

Add

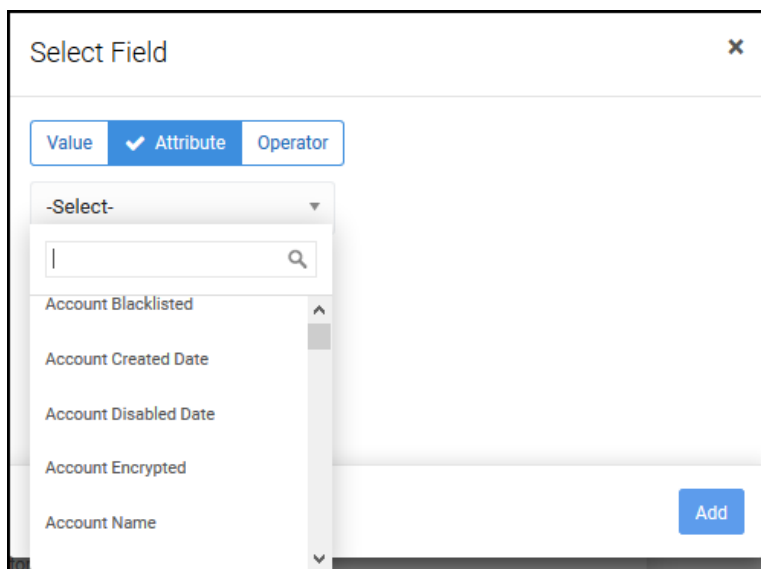
2. Click **INT 1** to select one of the following:

- **Value:** Enter a value.



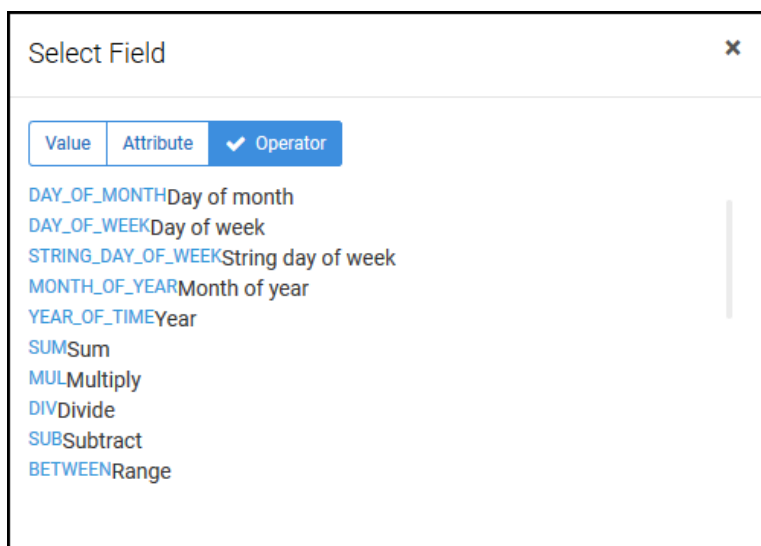
The screenshot shows a dialog box titled "Select Field" with a close button (X) in the top right corner. Inside the dialog, there are three tabs: "Value" (which is selected and has a checkmark), "Attribute", and "Operator". Below the tabs is a large, empty text input field. At the bottom right of the dialog is a blue "Add" button.

- **Attribute:** Select from dropdown.



The screenshot shows the same "Select Field" dialog box, but now the "Attribute" tab is selected and has a checkmark. A dropdown menu is open below the tabs, showing a search bar with a magnifying glass icon and a list of attributes: "Account Blacklisted", "Account Created Date", "Account Disabled Date", "Account Encrypted", and "Account Name". The dropdown menu has a scroll bar on the right. The "Add" button is still visible at the bottom right.

- **Operator:** Click to add an operator nested inside the Mul operator. Click the field to specify the value of the nested operator.



3. Repeat to populate value of **INT 2** and **INT 3**.

Conditions

Div

1. Select **Div** from Operators list to divide values.

CREATE NEW RULE

< BACK

A

Select Event Attribute OR Use Operator Expression

DIV(Double 1 , Double 2)

Show Available Operators @leftside

↓

Select Condition

Equal To

@middlecondition

↓

Value OR Select Event Attribute OR Use Operator Expression

@rightside

Available Operators

DAY_OF_MONTH	Day of month
DAY_OF_WEEK	Day of week
STRING_DAY_OF_WEEK	String day of week
MONTH_OF_YEAR	Month of year
YEAR_OF_TIME	Year
SUM	Sum
MUL	Multiply

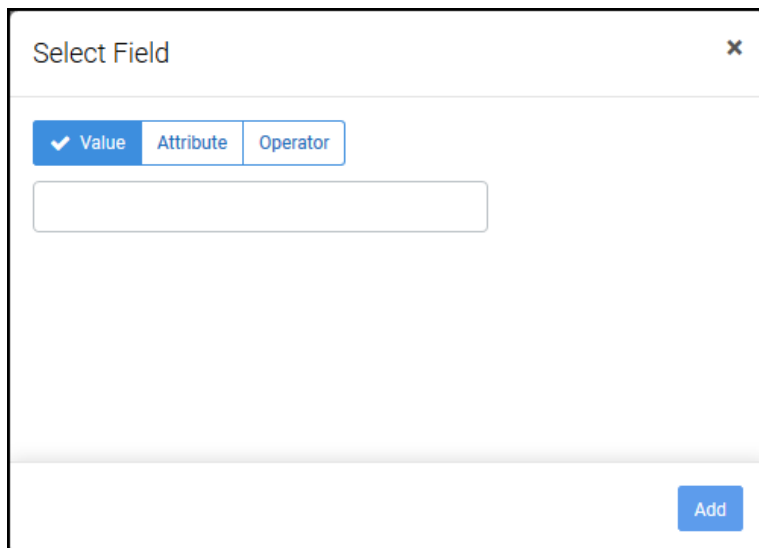
Available operator info

Cancel

Add

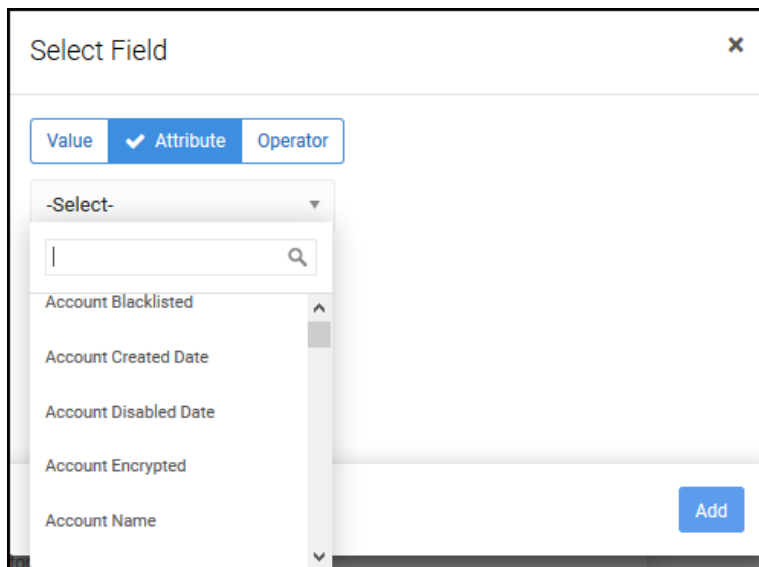
2. Click **Double 1** to select one of the following:

- **Value:** Enter a value.



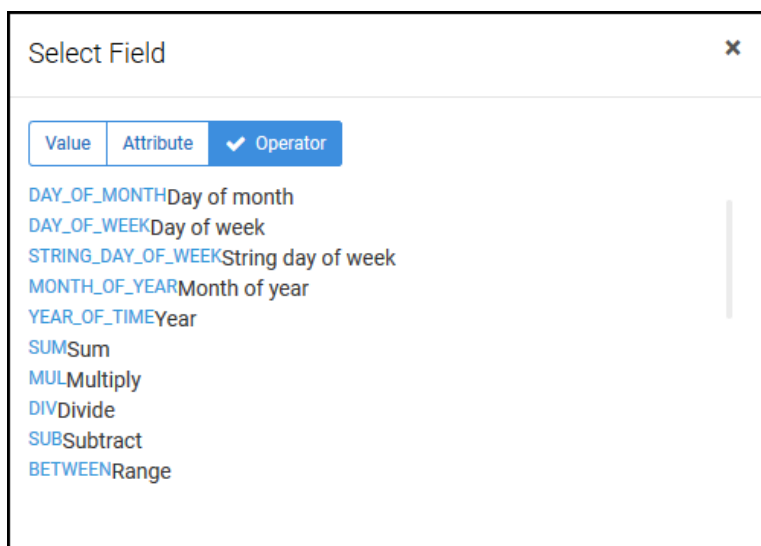
The screenshot shows a dialog box titled "Select Field" with a close button (X) in the top right corner. Inside the dialog, there are three tabs: "Value" (which is selected and has a checkmark), "Attribute", and "Operator". Below the tabs is a large, empty text input field. At the bottom right of the dialog is a blue "Add" button.

- **Attribute:** Select from dropdown.



The screenshot shows the same "Select Field" dialog box, but now the "Attribute" tab is selected and has a checkmark. A dropdown menu is open below the tabs, showing a search bar with a magnifying glass icon and a list of attributes: "Account Blacklisted", "Account Created Date", "Account Disabled Date", "Account Encrypted", and "Account Name". The dropdown menu has up and down arrow icons on its sides. The "Add" button is still visible at the bottom right.

- **Operator:** Click to add an operator nested inside the Div operator. Click the field to specify the value of the nested operator.



3. Repeat to populate value of **Double 2**.

Conditions

Sub

1. Select **Sub** from Operators list to subtract value of **Double 2** from value of **Double 1**.

CREATE NEW RULE < BACK

A

↓

B

Select Event Attribute OR Use Operator Expression

(SUB(Double 1 , Double 2))

Show Available Operators
@leftside

Select Condition

Equal To ▼

@middlecondition

Value OR Select Event Attribute OR Use Operator Expression

@rightside

Available Operators

DAY_OF_MONTH	Day of month
DAY_OF_WEEK	Day of week
STRING_DAY_OF_WEEK	String day of week
MONTH_OF_YEAR	Month of year
YEAR_OF_TIME	Year
SUM	Sum
MUL	Multiply

Available operator info

Cancel

Add

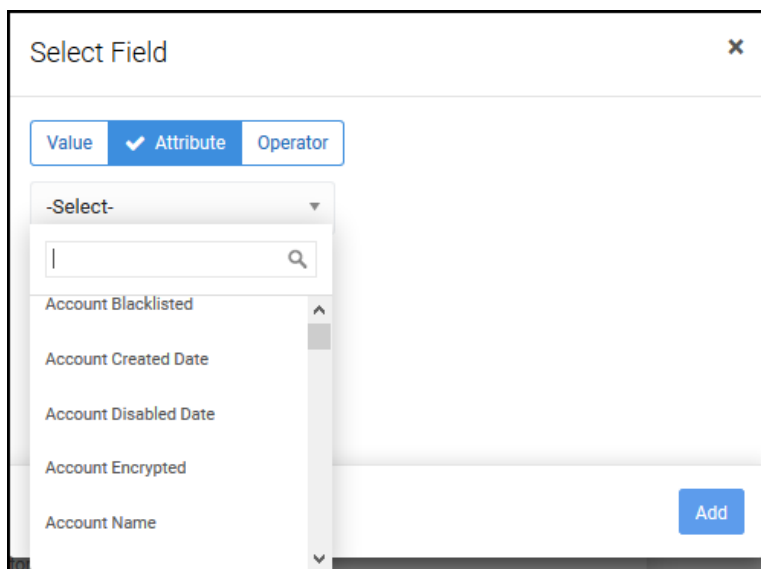
2. Click **Double 1** to select one of the following:

- **Value:** Enter a value.



The screenshot shows a dialog box titled "Select Field" with a close button (X) in the top right corner. Inside the dialog, there are three tabs: "Value" (which is selected and has a checkmark), "Attribute", and "Operator". Below the tabs is a large, empty text input field. At the bottom right of the dialog is a blue "Add" button.

- **Attribute:** Select from dropdown.



The screenshot shows the same "Select Field" dialog box, but now the "Attribute" tab is selected and has a checkmark. A dropdown menu is open below the tabs, showing a search bar with a magnifying glass icon and a list of attributes: "Account Blacklisted", "Account Created Date", "Account Disabled Date", "Account Encrypted", and "Account Name". The dropdown menu has up and down arrow icons on its right side. The "Add" button is still visible at the bottom right.

- **Operator:** Click to add an operator nested inside the Sub operator. Click the field to specify the value of the nested operator.

Select Field

ValueAttributeOperator

DAY_OF_MONTHDay of month

DAY_OF_WEEKDay of week

STRING_DAY_OF_WEEKString day of week

MONTH_OF_YEARMonth of year

YEAR_OF_TIMEYear

SUMSum

MULMultiply

DIVDivide

SUBSubtract

BETWEENRange

3. Repeat to populate value of **Double 2**.

Conditions

Between

1. Select **Between** from Operators list to specify range between **Start Date**, **End Date**, and **Date to check**.

CREATE NEW RULE

< BACK

A

↓

B

Select Event Attribute OR Use Operator Expression

(BETWEEN(Epoch Time Long Start Date , Epoch Time Long End Date , Epoch Time Long Date to check))

Show Available Operators
@leftside

Available Operators

DAY_OF_MONTH	Day of month
DAY_OF_WEEK	Day of week
STRING_DAY_OF_WEEK	String day of week
MONTH_OF_YEAR	Month of year
YEAR_OF_TIME	Year
SUM	Sum
MUL	Multiply

Available operator info

Select Condition

Equal To

@middlecondition

Value OR Select Event Attribute OR Use Operator Expression

@rightside

Cancel

Add

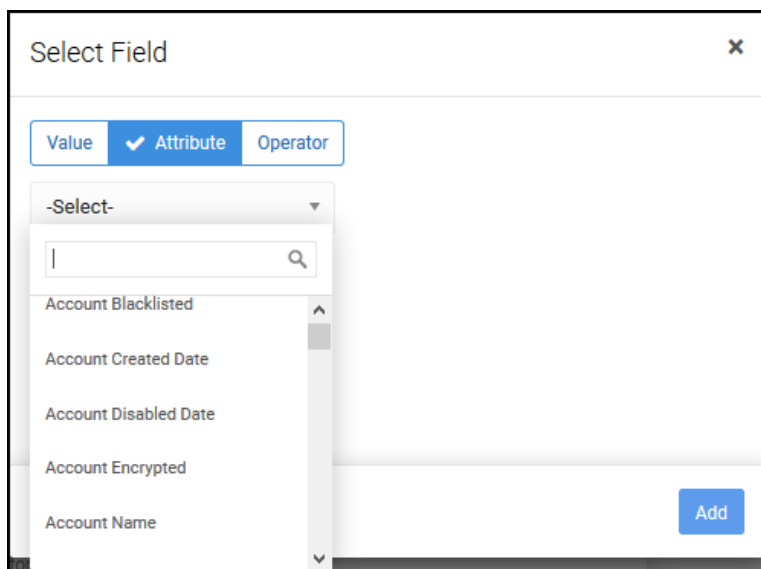
2. Click **Epoch Time Long Start Date** to select one of the following:

- **Value:** Enter a value.



The screenshot shows a dialog box titled "Select Field" with a close button (X) in the top right corner. Inside the dialog, there are three tabs: "Value" (which is selected and has a checkmark), "Attribute", and "Operator". Below the tabs is a large, empty text input field. At the bottom right of the dialog is a blue "Add" button.

- **Attribute:** Select from dropdown.



The screenshot shows the same "Select Field" dialog box, but now the "Attribute" tab is selected and has a checkmark. A dropdown menu is open below the tabs, showing a search bar and a list of attributes: "Account Blacklisted", "Account Created Date", "Account Disabled Date", "Account Encrypted", and "Account Name". The dropdown menu has a scroll bar on the right. The "Add" button is still visible at the bottom right.

- **Operator:** Click to add an operator nested inside the Between operator. Click the field to specify the value of the nested operator.

Select Field

ValueAttributeOperator

DAY_OF_MONTHDay of month
DAY_OF_WEEKDay of week
STRING_DAY_OF_WEEKString day of week
MONTH_OF_YEARMonth of year
YEAR_OF_TIMEYear
SUMSum
MULMultiply
DIVDivide
SUBSubtract
BETWEENRange

- Repeat to populate value of **Epoch Time Long End Date** and **Epoch Time Long Date to check**.

Conditions

DateDiff

1. Select **DateDiff** from Operators list to specify the difference between two dates.

CREATE NEW RULE

< BACK

Select Event Attribute OR Use Operator Expression

(DATEDIFF(Epoch Time Long1 , Epoch Time Long2)

Show Available Operators

@leftside

Select Condition

Equal To

@middlecondition

Value OR Select Event Attribute OR Use Operator Expression

@rightside

Available Operators

DAY_OF_MONTH	Day of month
DAY_OF_WEEK	Day of week
STRING_DAY_OF_WEEK	String day of week
MONTH_OF_YEAR	Month of year
YEAR_OF_TIME	Year
SUM	Sum
MUL	Multiply

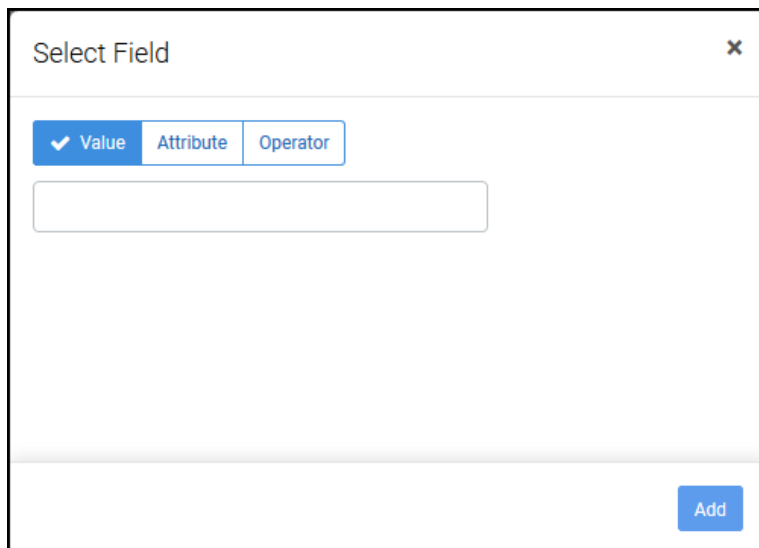
Available operator info

Cancel

Add

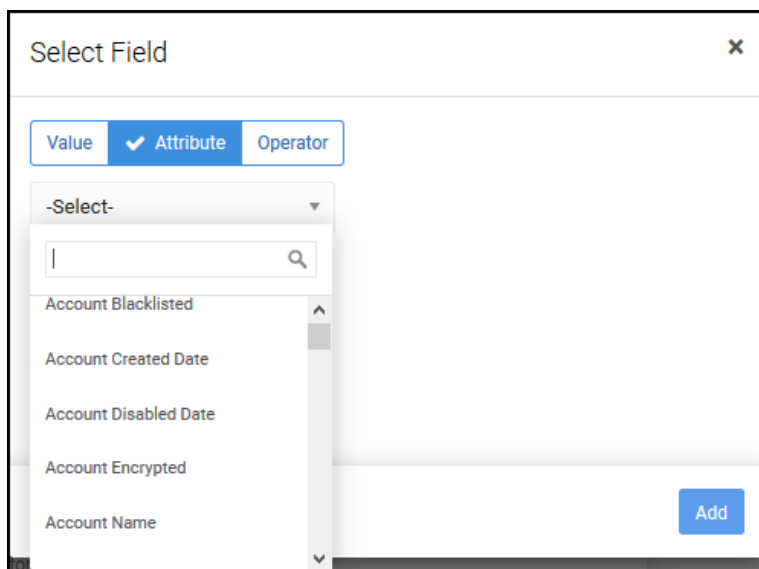
2. Click **Epoch Time Long1** to select one of the following:

- **Value:** Enter a value.



The screenshot shows a dialog box titled "Select Field" with a close button (X) in the top right corner. Inside the dialog, there are three tabs: "Value" (which is selected and has a checkmark), "Attribute", and "Operator". Below the tabs is a large, empty text input field. At the bottom right of the dialog is a blue "Add" button.

- **Attribute:** Select from dropdown.



The screenshot shows the same "Select Field" dialog box, but now the "Attribute" tab is selected and has a checkmark. A dropdown menu is open below the tabs, showing a search bar and a list of attributes: "Account Blacklisted", "Account Created Date", "Account Disabled Date", "Account Encrypted", and "Account Name". The dropdown menu has a scroll bar on the right. The "Add" button is still visible at the bottom right.

- **Operator:** Click to add an operator nested inside the DateDiff operator. Click the field to specify the value of the nested operator.

Select Field

×

Value

Attribute

✓ Operator

DAY_OF_MONTHDay of month

DAY_OF_WEEKDay of week

STRING_DAY_OF_WEEKString day of week

MONTH_OF_YEARMonth of year

YEAR_OF_TIMEYear

SUMSum

MULMultiply

DIVDivide

SUBSubtract

BETWEENRange

- Repeat to populate value of **Epoch Time Long2**.

Conditions

Greatest

1. Select **Greatest** from Operators list to specify the value of Time1, Time2, and Time3.

CREATE NEW RULE

< BACK

Select Event Attribute OR Use Operator Expression

(GREATEST(Epoch Time Long1 , Epoch Time Long2 , Epoch Time Long3))

Show Available Operators @leftside

Available Operators

DAY_OF_MONTH	Day of month
DAY_OF_WEEK	Day of week
STRING_DAY_OF_WEEK	String day of week
MONTH_OF_YEAR	Month of year
YEAR_OF_TIME	Year
SUM	Sum
MUL	Multiply

Available operator info

Select Condition

Equal To

@middlecondition

Value OR Select Event Attribute OR Use Operator Expression

@rightside

Cancel

Add

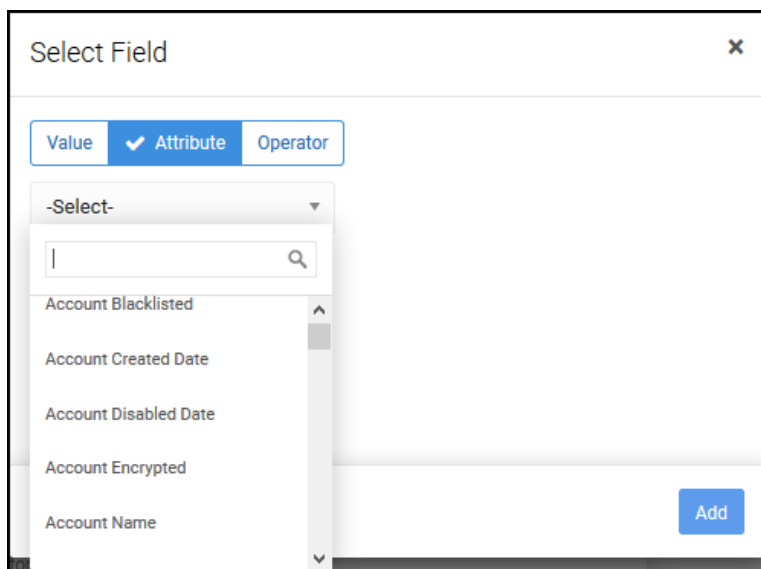
2. Click **Epoch Time Long1** to select one of the following:

- **Value:** Enter a value.



The screenshot shows a dialog box titled "Select Field" with a close button (X) in the top right corner. Inside the dialog, there are three tabs: "Value" (which is selected and has a checkmark), "Attribute", and "Operator". Below the tabs is a large, empty text input field. At the bottom right of the dialog is a blue "Add" button.

- **Attribute:** Select from dropdown.



The screenshot shows the same "Select Field" dialog box, but now the "Attribute" tab is selected and has a checkmark. A dropdown menu is open below the tabs, showing a search bar with a magnifying glass icon and a list of attributes: "Account Blacklisted", "Account Created Date", "Account Disabled Date", "Account Encrypted", and "Account Name". The "Add" button is visible at the bottom right.

- **Operator:** Click to add an operator nested inside the Greatest operator. Click the field to specify the value of the nested operator.

Select Field
×

Value
Attribute
Operator

DAY_OF_MONTHDay of month
DAY_OF_WEEKDay of week
STRING_DAY_OF_WEEKString day of week
MONTH_OF_YEARMonth of year
YEAR_OF_TIMEYear
SUMSum
MULMultiply
DIVDivide
SUBSubtract
BETWEENRange

- Repeat to populate value of **Epoch Time Long2** and **Epoch Time Long3**.

Conditions

Smallest

1. Select **Smallest** from Operators list to specify the value of Time1, Time2, and Time3.

CREATE NEW RULE

< BACK

A

↓

↓

B

Select Event Attribute OR Use Operator Expression

SMALLEST(Epoch Time Long1 , Epoch Time Long2 , Epoch Time Long3) |

Show Available Operators @leftside

Select Condition

Equal To ▾

@middlecondition

Value OR Select Event Attribute OR Use Operator Expression

@rightside

Available Operators

DAY_OF_MONTH	Day of month
DAY_OF_WEEK	Day of week
STRING_DAY_OF_WEEK	String day of week
MONTH_OF_YEAR	Month of year
YEAR_OF_TIME	Year
SUM	Sum
MUL	Multiply

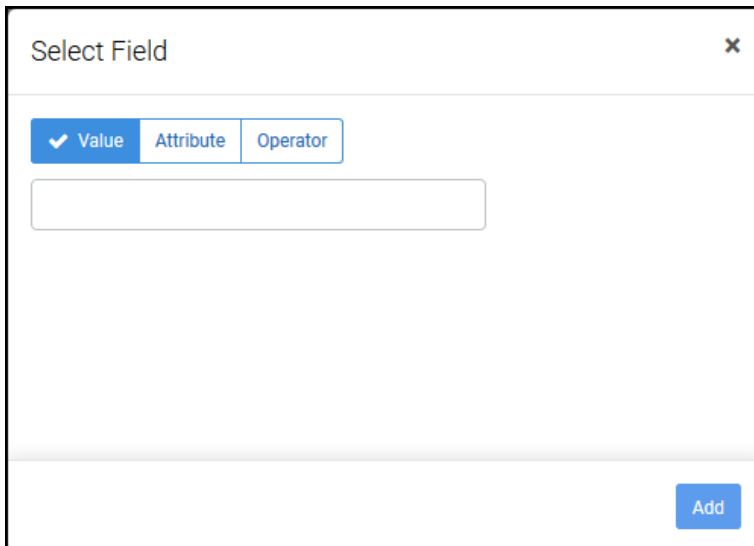
Available operator info

Cancel

Add

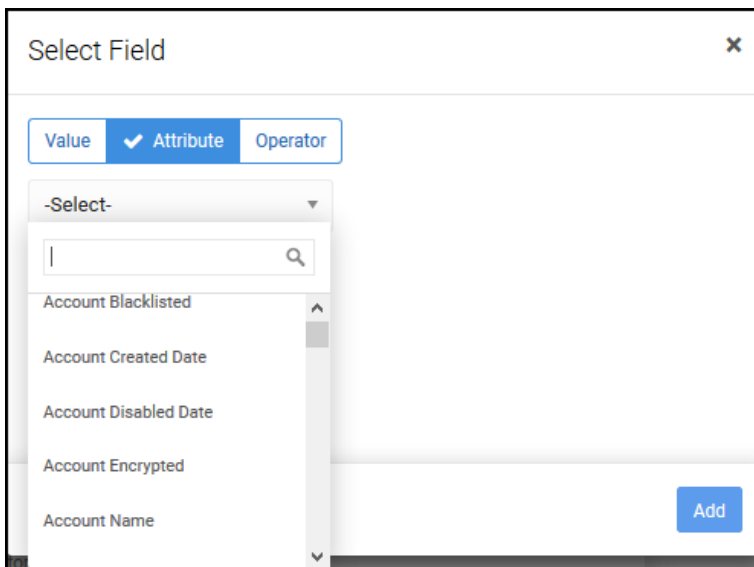
2. Click **Epoch Time Long1** to select one of the following:

- **Value:** Enter a value.



The screenshot shows a dialog box titled "Select Field" with a close button (X) in the top right corner. Inside the dialog, there are three tabs: "Value" (which is selected and has a checkmark), "Attribute", and "Operator". Below the tabs is a large, empty text input field. At the bottom right of the dialog is a blue "Add" button.

- **Attribute:** Select from dropdown.



The screenshot shows the same "Select Field" dialog box, but now the "Attribute" tab is selected and has a checkmark. A dropdown menu is open below the tabs, showing a search bar with a magnifying glass icon and a list of attributes: "Account Blacklisted", "Account Created Date", "Account Disabled Date", "Account Encrypted", and "Account Name". The dropdown menu has up and down arrow icons on its right side. The "Add" button is still visible at the bottom right.

- **Operator:** Click to add an operator nested inside the Smallest operator. Click the field to specify the value of the nested operator.

Select Field

Value

Attribute

Operator

DAY_OF_MONTHDay of month

DAY_OF_WEEKDay of week

STRING_DAY_OF_WEEKString day of week

MONTH_OF_YEARMonth of year

YEAR_OF_TIMEYear

SUMSum

MULMultiply

DIVDivide

SUBSubtract

BETWEENRange

- Repeat to populate value of **Epoch Time Long2** and **Epoch Time Long3**.

Conditions

*D*Sum

1. Select **DSum** from Operators list to specify the value of Time1, Time2, and Time3.

The screenshot shows the 'CREATE NEW RULE' interface. On the left, there are three blue circular buttons labeled A, B, and a downward arrow. The main area is divided into three sections:

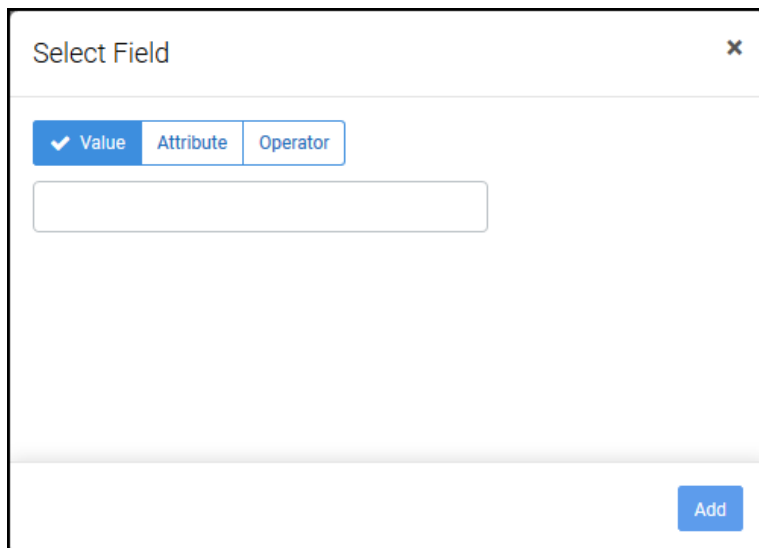
- Top Section:** Contains the text 'Select Event Attribute OR Use Operator Expression'. Below this is a text box with the expression `DSUM(Epoch Time Long1 , Epoch Time Long2 , Epoch Time Long3)`. To the right is a table of 'Available Operators':

Available Operators	
DAY_OF_MONTH	Day of month
DAY_OF_WEEK	Day of week
STRING_DAY_OF_WEEK	String day of week
MONTH_OF_YEAR	Month of year
YEAR_OF_TIME	Year
SUM	Sum
MUL	Multiply
- Middle Section:** Contains the text 'Select Condition'. Below this is a dropdown menu with 'Equal To' selected. To the right is the text 'Available operator info'.
- Bottom Section:** Contains the text 'Value OR Select Event Attribute OR Use Operator Expression'. Below this is a text box.

At the bottom right, there are 'Cancel' and 'Add' buttons.

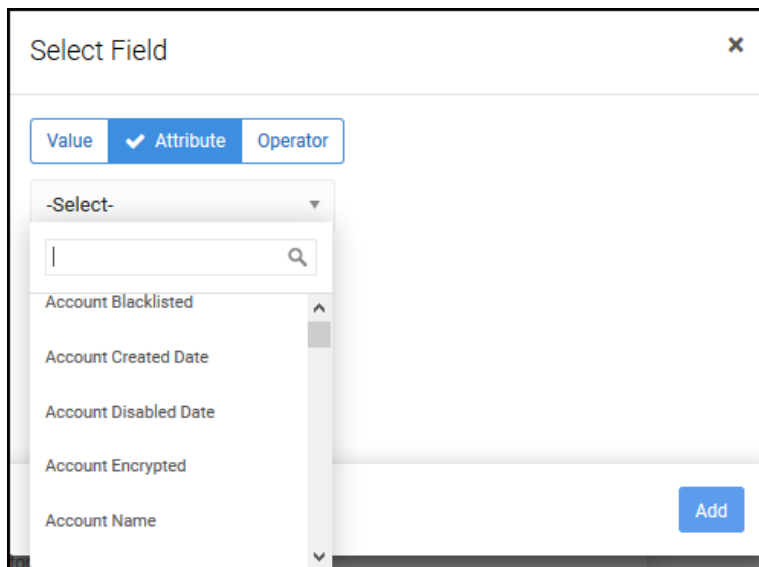
2. Click **Epoch Time Long1** to select one of the following:

- **Value:** Enter a value.



The screenshot shows a dialog box titled "Select Field" with a close button (X) in the top right corner. Inside the dialog, there are three tabs: "Value" (which is selected and has a checkmark), "Attribute", and "Operator". Below the tabs is a large, empty text input field. At the bottom right of the dialog is a blue "Add" button.

- **Attribute:** Select from dropdown.



The screenshot shows the same "Select Field" dialog box, but now the "Attribute" tab is selected and has a checkmark. A dropdown menu is open below the tabs, showing a search bar and a list of attributes: "Account Blacklisted", "Account Created Date", "Account Disabled Date", "Account Encrypted", and "Account Name". The dropdown menu has a scroll bar on the right. The "Add" button is still visible at the bottom right.

- **Operator:** Click to add an operator nested inside the DSum operator. Click the field to specify the value of the nested operator.

Select Field

×

Value

Attribute

✓ Operator

DAY_OF_MONTHDay of month

DAY_OF_WEEKDay of week

STRING_DAY_OF_WEEKString day of week

MONTH_OF_YEARMonth of year

YEAR_OF_TIMEYear

SUMSum

MULMultiply

DIVDivide

SUBSubtract

BETWEENRange

- Repeat to populate value of **Epoch Time Long2** and **Epoch Time Long3**.

Conditions

LCase

1. Select **LCase** from Operators list to specify the value of String.

CREATE NEW RULE

< BACK

Select Event Attribute OR Use Operator Expression

LCASE(String)

Show Available Operators @leftside

Available Operators

DAY_OF_MONTH	Day of month
DAY_OF_WEEK	Day of week
STRING_DAY_OF_WEEK	String day of week
MONTH_OF_YEAR	Month of year
YEAR_OF_TIME	Year
SUM	Sum
MUL	Multiply

Available operator info

↓

Select Condition

Equal To

@middlecondition

↓

Value OR Select Event Attribute OR Use Operator Expression

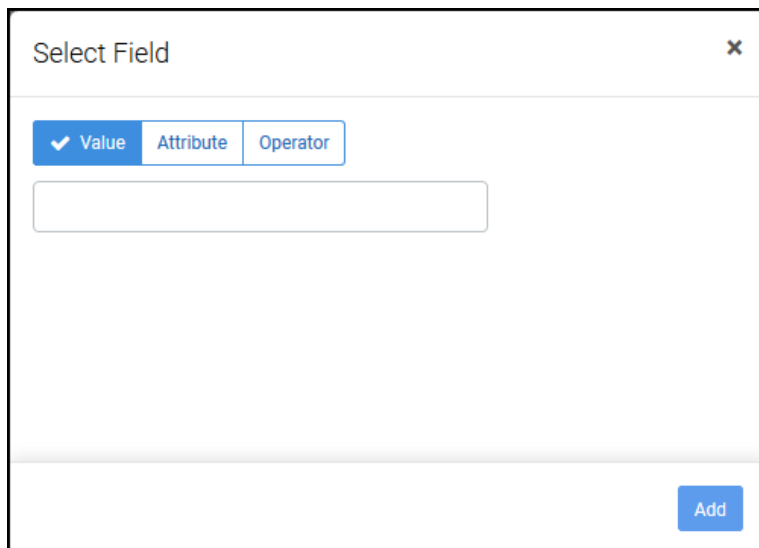
@rightside

Cancel

Add

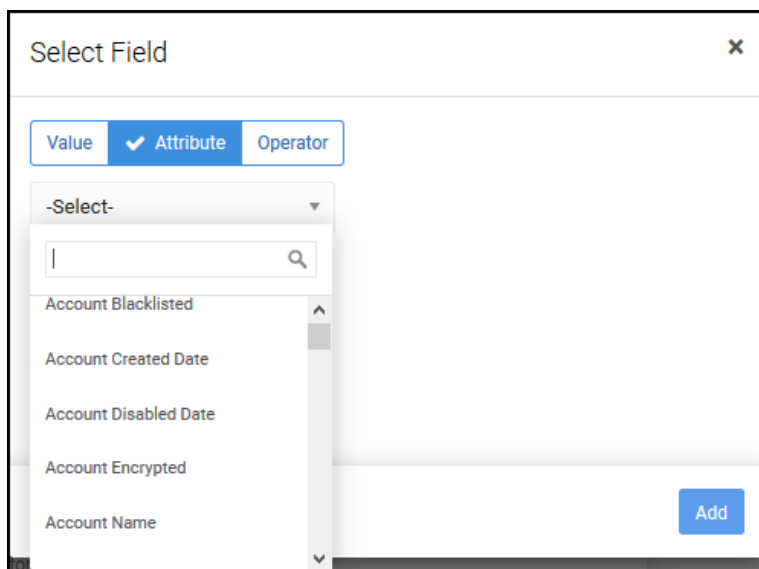
2. Click **String** to select one of the following:

- **Value:** Enter a value.



The screenshot shows a dialog box titled "Select Field" with a close button (X) in the top right corner. Inside the dialog, there are three tabs: "Value" (which is selected and has a checkmark), "Attribute", and "Operator". Below the tabs is a large, empty text input field. At the bottom right of the dialog is a blue "Add" button.

- **Attribute:** Select from dropdown.



The screenshot shows the same "Select Field" dialog box, but now the "Attribute" tab is selected and has a checkmark. A dropdown menu is open below the tabs, showing a search bar and a list of attributes: "Account Blacklisted", "Account Created Date", "Account Disabled Date", "Account Encrypted", and "Account Name". The dropdown menu has a scroll bar on the right. The "Add" button is still visible at the bottom right.

- **Operator:** Click to add an operator nested inside the LCase operator. Click the field to specify the value of the nested operator.

Select Field
✕

Value
Attribute
Operator

DAY_OF_MONTHDay of month
DAY_OF_WEEKDay of week
STRING_DAY_OF_WEEKString day of week
MONTH_OF_YEARMonth of year
YEAR_OF_TIMEYear
SUMSum
MULMultiply
DIVDivide
SUBSubtract
BETWEENRange

Conditions

UCase

1. Select **UCase** from Operators list to specify the value of String.

CREATE NEW RULE [← BACK](#)

Select Event Attribute OR Use Operator Expression

(UCASE(String))

Available Operators

DAY_OF_MONTH	Day of month
DAY_OF_WEEK	Day of week
STRING_DAY_OF_WEEK	String day of week
MONTH_OF_YEAR	Month of year
YEAR_OF_TIME	Year
SUM	Sum
MUL	Multiply

Show Available Operators @leftside Available operator info

Select Condition

Equal To @middlecondition

Value OR Select Event Attribute OR Use Operator Expression

@rightside

Cancel Add

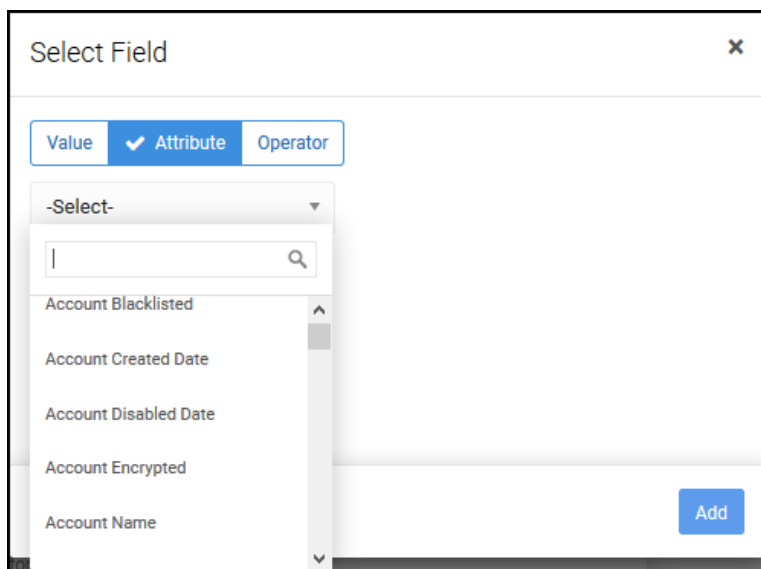
2. Click **String** to select one of the following:

- **Value:** Enter a value.



The screenshot shows a dialog box titled "Select Field" with a close button (X) in the top right corner. Inside the dialog, there are three tabs: "Value" (which is selected and has a checkmark), "Attribute", and "Operator". Below the tabs is a large, empty text input field. At the bottom right of the dialog is a blue "Add" button.

- **Attribute:** Select from dropdown.



The screenshot shows the same "Select Field" dialog box, but now the "Attribute" tab is selected and has a checkmark. A dropdown menu is open below the tabs, showing a search bar and a list of attributes: "Account Blacklisted", "Account Created Date", "Account Disabled Date", "Account Encrypted", and "Account Name". The dropdown menu has a scroll bar on the right. The "Add" button is still visible at the bottom right.

- **Operator:** Click to add an operator nested inside the UCase operator. Click the field to specify the value of the nested operator.

Select Field

×

Value

Attribute

✓ Operator

DAY_OF_MONTHDay of month

DAY_OF_WEEKDay of week

STRING_DAY_OF_WEEKString day of week

MONTH_OF_YEARMonth of year

YEAR_OF_TIMEYear

SUMSum

MULMultiply

DIVDivide

SUBSubtract

BETWEENRange

Conditions

Split

1. Select **Split** from Operators list to specify the values of Input **String**, **Delimited**, and **Limit**.

The screenshot shows the 'CREATE NEW RULE' interface with a sidebar on the left containing three blue circular buttons labeled 'A', a downward arrow, and 'B'. The main area is divided into three sections:

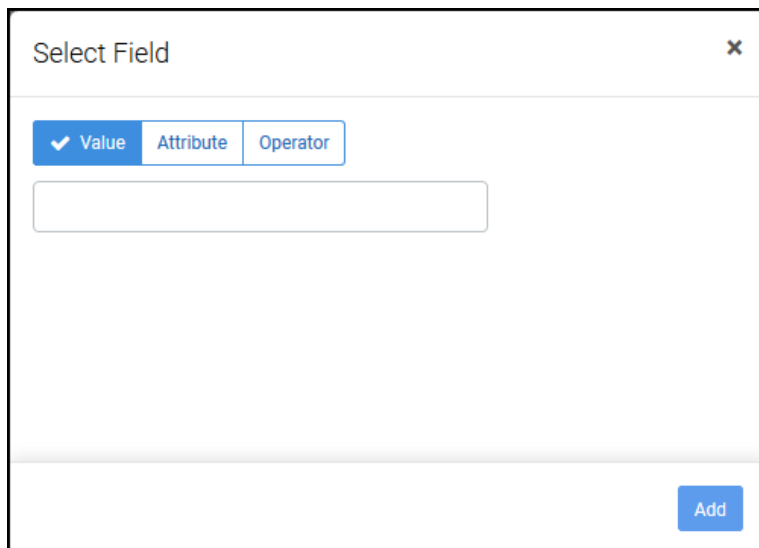
- Top Section:** Contains the text 'Select Event Attribute OR Use Operator Expression'. Below it is a text box with the expression 'SPLIT(Input String , Delimiter , Limit)'. To the right is a list of 'Available Operators' with two columns: the operator name and its description.

Available Operators	
DAY_OF_MONTH	Day of month
DAY_OF_WEEK	Day of week
STRING_DAY_OF_WEEK	String day of week
MONTH_OF_YEAR	Month of year
YEAR_OF_TIME	Year
SUM	Sum
MUL	Multiply
- Middle Section:** Contains the text 'Show Available Operators @leftside' and a 'Select Condition' dropdown menu set to 'Equal To'. Below the dropdown is the text '@middlecondition'.
- Bottom Section:** Contains the text 'Value OR Select Event Attribute OR Use Operator Expression' and an empty text box. Below the text box is the text '@rightside'.

At the bottom right of the interface are 'Cancel' and 'Add' buttons.

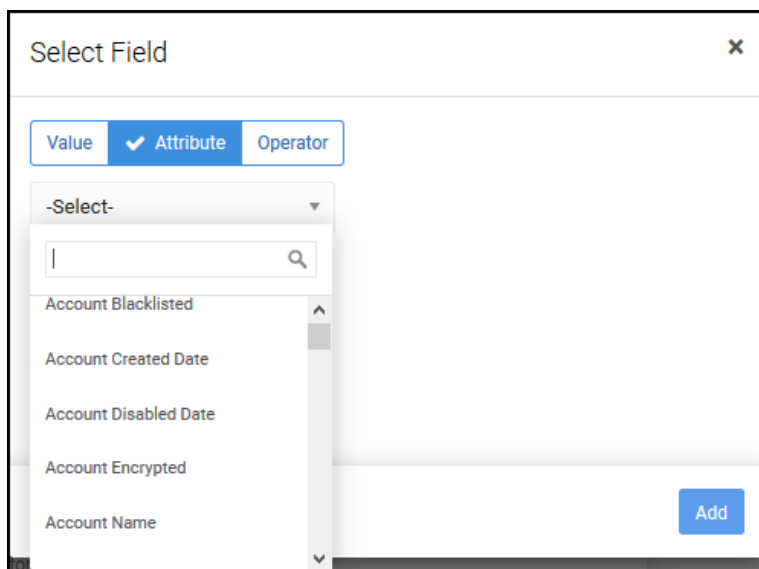
2. Click **String** to select one of the following:

- **Value:** Enter a value.



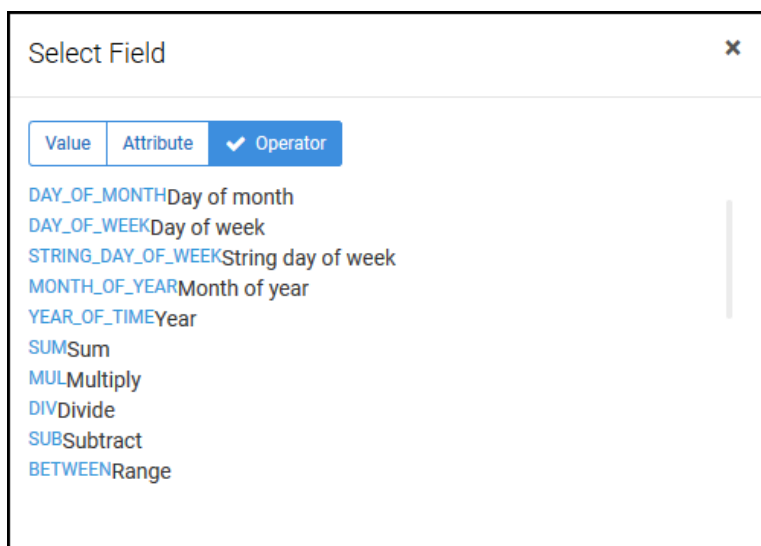
The screenshot shows a dialog box titled "Select Field" with a close button (X) in the top right corner. Inside the dialog, there are three tabs: "Value" (which is selected and has a checkmark), "Attribute", and "Operator". Below the tabs is a large, empty text input field. At the bottom right of the dialog is a blue "Add" button.

- **Attribute:** Select from dropdown.



The screenshot shows the same "Select Field" dialog box, but now the "Attribute" tab is selected and has a checkmark. A dropdown menu is open below the tabs, showing a search bar with a magnifying glass icon and a list of attributes: "Account Blacklisted", "Account Created Date", "Account Disabled Date", "Account Encrypted", and "Account Name". The dropdown menu has a scroll bar on the right. The "Add" button is still visible at the bottom right.

- **Operator:** Click to add an operator nested inside the Split operator. Click the field to specify the value of the nested operator.



3. Repeat to populate value of **Delimiter** and **Limit**.

Conditions

Concat

1. Select **Concat** from Operators list to concatenate String1 and String2 into StringN.

The screenshot shows the 'CREATE NEW RULE' interface with a sidebar on the left containing three blue circular buttons labeled 'A', a downward arrow, and 'B'. The main area is divided into three sections:

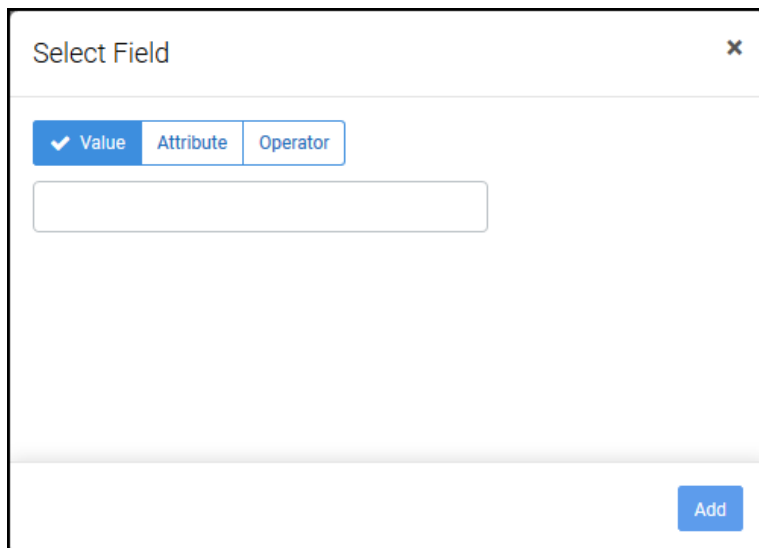
- Top Section:** Contains the text 'Select Event Attribute OR Use Operator Expression'. Below this is a text input field with the formula `CONCAT(String 1 , String 2 , String n)`. To the right is a table titled 'Available Operators'.
- Middle Section:** Contains the text 'Select Condition' and a dropdown menu currently set to 'Equal To'.
- Bottom Section:** Contains the text 'Value OR Select Event Attribute OR Use Operator Expression' and an empty text input field.

At the bottom right of the interface are 'Cancel' and 'Add' buttons.

Operator Name	Description
DAY_OF_MONTH	Day of month
DAY_OF_WEEK	Day of week
STRING_DAY_OF_WEEK	String day of week
MONTH_OF_YEAR	Month of year
YEAR_OF_TIME	Year
SUM	Sum
MUL	Multiply

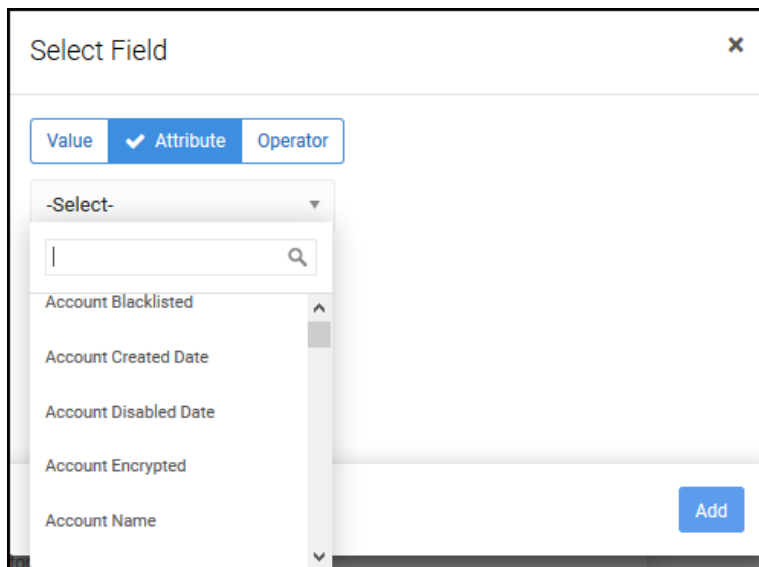
2. Click **String 1** to select one of the following:

- **Value:** Enter a value.



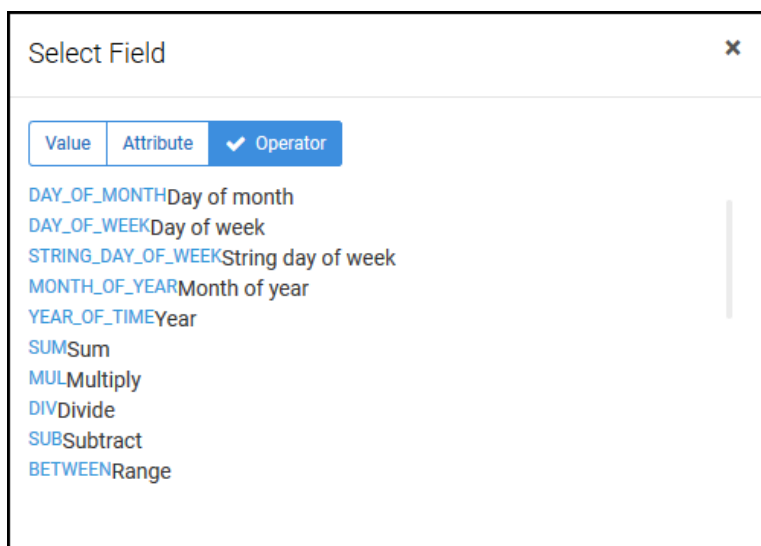
The screenshot shows a dialog box titled "Select Field" with a close button (X) in the top right corner. Inside the dialog, there are three tabs: "Value" (which is selected and has a checkmark), "Attribute", and "Operator". Below the tabs is a large, empty text input field. At the bottom right of the dialog is a blue "Add" button.

- **Attribute:** Select from dropdown.



The screenshot shows the same "Select Field" dialog box, but now the "Attribute" tab is selected and has a checkmark. A dropdown menu is open below the tabs, showing a search bar and a list of attributes: "Account Blacklisted", "Account Created Date", "Account Disabled Date", "Account Encrypted", and "Account Name". The dropdown menu has a scroll bar on the right. The "Add" button is still visible at the bottom right.

- **Operator:** Click to add an operator nested inside the Concat operator. Click the field to specify the value of the nested operator.



3. Repeat to populate value of **String 2** and **String N**.

Conditions

MOA

1. Select **MOA** from Operators list to specify **Input Array** and **Index** for Member of Array.

CREATE NEW RULE

< BACK

Select Event Attribute OR Use Operator Expression

CONCAT(String 1 , String 2 , String n)

Show Available Operators

@leftside

Available Operators

DAY_OF_MONTH	Day of month
DAY_OF_WEEK	Day of week
STRING_DAY_OF_WEEK	String day of week
MONTH_OF_YEAR	Month of year
YEAR_OF_TIME	Year
SUM	Sum
MUL	Multiply

Available operator info

Select Condition

Equal To

@middlecondition

Value OR Select Event Attribute OR Use Operator Expression

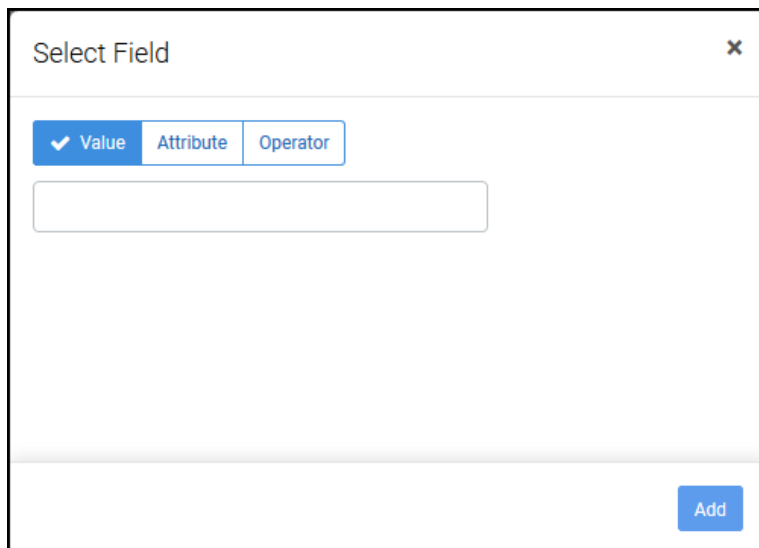
@rightside

Cancel

Add

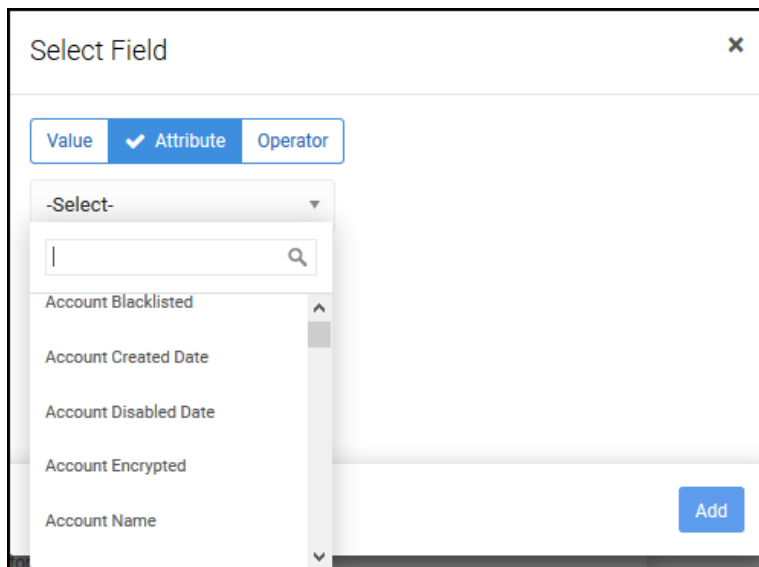
2. Click **Input Array** to select one of the following:

- **Value:** Enter a value.



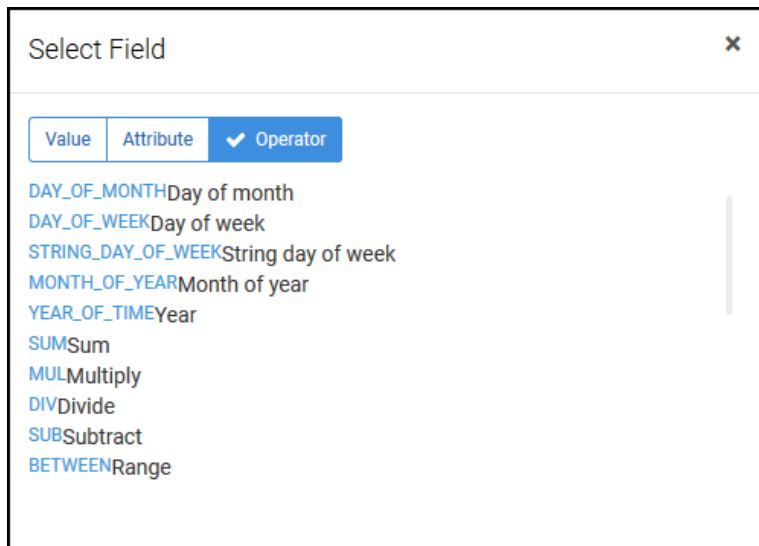
The screenshot shows a dialog box titled "Select Field" with a close button (X) in the top right corner. Inside the dialog, there are three tabs: "Value" (which is selected and has a checkmark), "Attribute", and "Operator". Below the tabs is a large, empty text input field. At the bottom right of the dialog is a blue "Add" button.

- **Attribute:** Select from dropdown.



The screenshot shows the same "Select Field" dialog box, but now the "Attribute" tab is selected and has a checkmark. A dropdown menu is open below the tabs, showing a search bar with a magnifying glass icon and a list of attributes: "Account Blacklisted", "Account Created Date", "Account Disabled Date", "Account Encrypted", and "Account Name". The dropdown menu has a scroll bar on the right. The "Add" button is still visible at the bottom right.

- **Operator:** Click to add an operator nested inside the MOA operator. Click the field to specify the value of the nested operator.



3. Repeat to populate value of **String 2** and **String N**.

Conditions

Substring

1. Select **Substring** from Operators list to specify **Input String**, **Start Index**, and **End Index**.

The screenshot shows the 'CREATE NEW RULE' interface with a sidebar on the left containing three blue circular buttons labeled 'A', a downward arrow, and 'B'. The main area is divided into three sections:

- Top Section:** Contains the text 'Select Event Attribute OR Use Operator Expression'. Below it is a text input field with the formula `SUBSTRING(Input String , Start Index , End Index)`. To the right is a table of 'Available Operators':

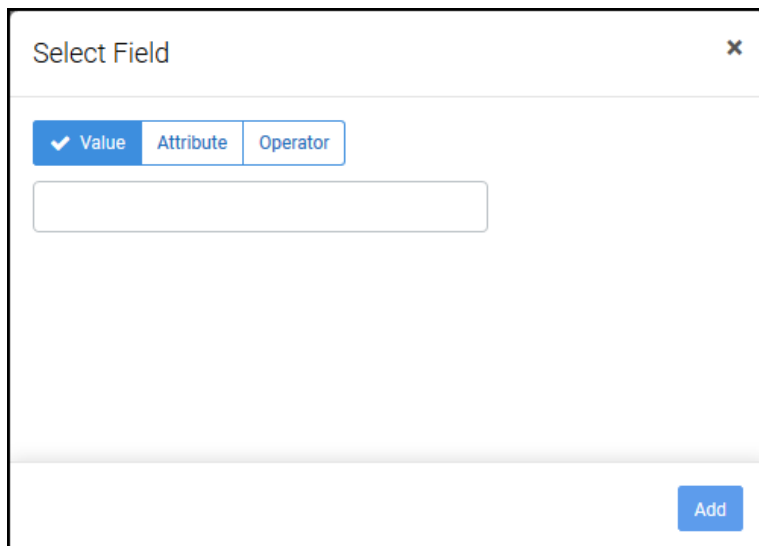
Available Operators	
DAY_OF_MONTH	Day of month
DAY_OF_WEEK	Day of week
STRING_DAY_OF_WEEK	String day of week
MONTH_OF_YEAR	Month of year
YEAR_OF_TIME	Year
SUM	Sum
MUL	Multiply

Below the table is a link 'Show Available Operators @leftside' and the text 'Available operator info'.
- Middle Section:** Contains the text 'Select Condition' and a dropdown menu set to 'Equal To'. Below it is the text '@middlecondition'.
- Bottom Section:** Contains the text 'Value OR Select Event Attribute OR Use Operator Expression' and an empty text input field. Below it is the text '@rightside'.

At the bottom right of the interface are 'Cancel' and 'Add' buttons.

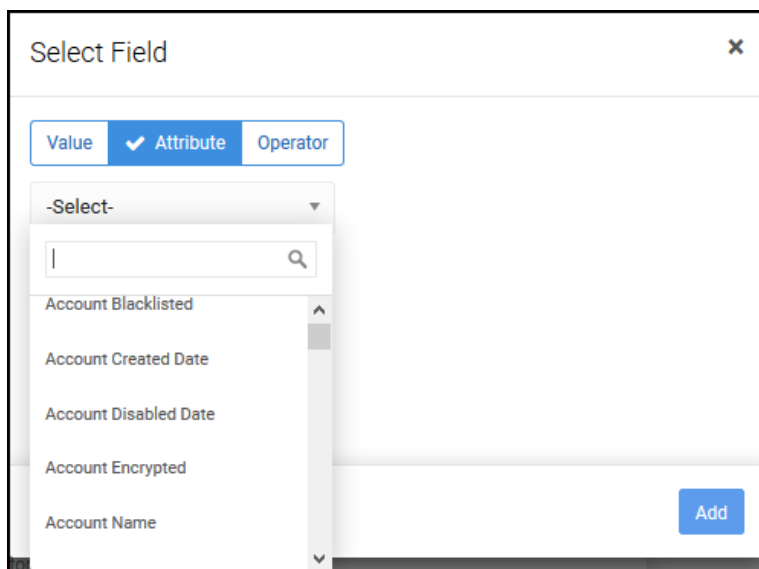
2. Click **Input String** to select one of the following:

- **Value:** Enter a value.



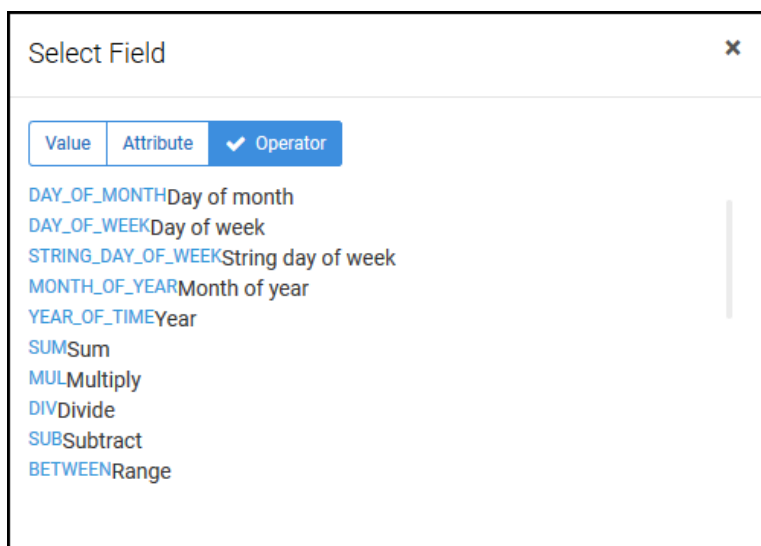
The screenshot shows a dialog box titled "Select Field" with a close button (X) in the top right corner. Inside the dialog, there are three tabs: "Value" (which is selected and has a checkmark), "Attribute", and "Operator". Below the tabs is a large, empty text input field. At the bottom right of the dialog is a blue "Add" button.

- **Attribute:** Select from dropdown.



The screenshot shows the same "Select Field" dialog box, but now the "Attribute" tab is selected and has a checkmark. A dropdown menu is open below the tabs, showing a search bar with a magnifying glass icon and a list of attributes: "Account Blacklisted", "Account Created Date", "Account Disabled Date", "Account Encrypted", and "Account Name". The dropdown menu has up and down arrow icons on its right side. The "Add" button is still visible at the bottom right.

- **Operator:** Click to add an operator nested inside the Substring operator. Click the field to specify the value of the nested operator.



3. Repeat to populate value of **Start Index** and **End Index**.

Conditions

RegEx

1. Select **Regex** from Operators list to specify a regex.

CREATE NEW RULE

< BACK

A

↓

B

Select Event Attribute OR Use Operator Expression

(REGEX(REGEX , Input string , Case sensitive , Negate result))

Show Available Operators

@leftside

Select Condition

Equal To

@middlecondition

Value OR Select Event Attribute OR Use Operator Expression

@rightside

Available Operators

DAY_OF_MONTH	Day of month
DAY_OF_WEEK	Day of week
STRING_DAY_OF_WEEK	String day of week
MONTH_OF_YEAR	Month of year
YEAR_OF_TIME	Year
SUM	Sum
MUL	Multiply

Available operator info

Cancel

Add

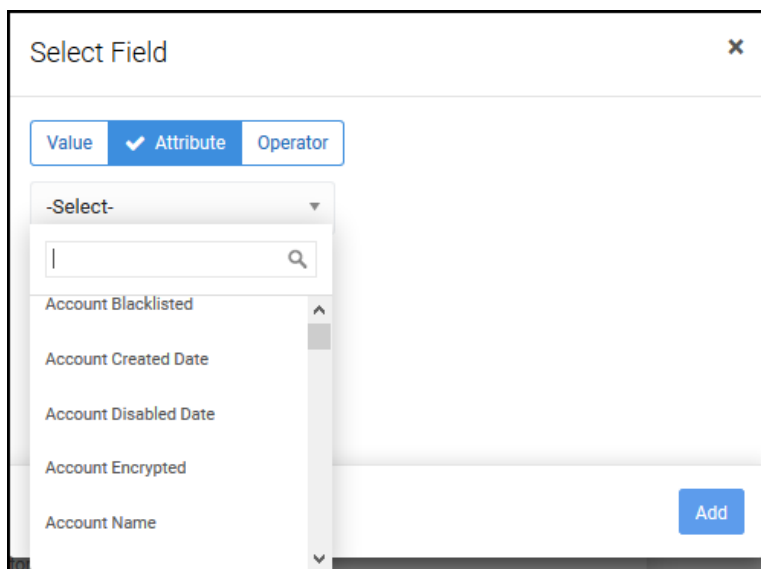
2. Click **Input String** to select one of the following:

- **Value:** Enter a value.



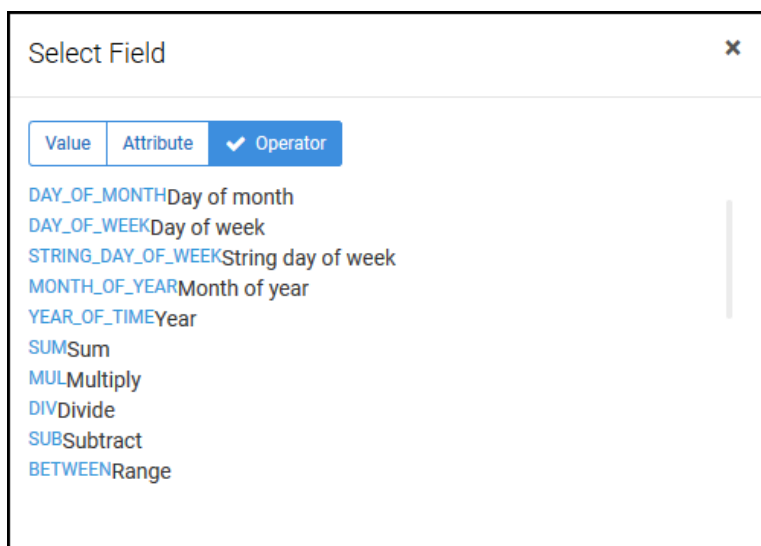
The screenshot shows a dialog box titled "Select Field" with a close button (X) in the top right corner. Inside the dialog, there are three tabs: "Value" (which is selected and has a checkmark), "Attribute", and "Operator". Below the tabs is a large, empty text input field. At the bottom right of the dialog is a blue "Add" button.

- **Attribute:** Select from dropdown.



The screenshot shows the same "Select Field" dialog box, but now the "Attribute" tab is selected and has a checkmark. A dropdown menu is open below the tabs, showing a search bar and a list of attributes: "Account Blacklisted", "Account Created Date", "Account Disabled Date", "Account Encrypted", and "Account Name". The dropdown menu has a scroll bar on the right. The "Add" button is still visible at the bottom right.

- **Operator:** Click to add an operator nested inside the Regex operator. Click the field to specify the value of the nested operator.



3. Repeat to populate value of **Input string**, **Case sensitive**, and **Negate result**.

Conditions

Web Extractor

1. Select **Web Extractor** from Operators list to extract a value from a URL.

CREATE NEW RULE

< BACK

A

Select Event Attribute OR Use Operator Expression

(REGEX(REGEX , Input string , Case sensitive , Negate result))

Show Available Operators

@leftside

↓

B

Select Condition

Equal To

@middlecondition

Value OR Select Event Attribute OR Use Operator Expression

@rightside

Available Operators

DAY_OF_MONTH	Day of month
DAY_OF_WEEK	Day of week
STRING_DAY_OF_WEEK	String day of week
MONTH_OF_YEAR	Month of year
YEAR_OF_TIME	Year
SUM	Sum
MUL	Multiply

Available operator info

Cancel

Add

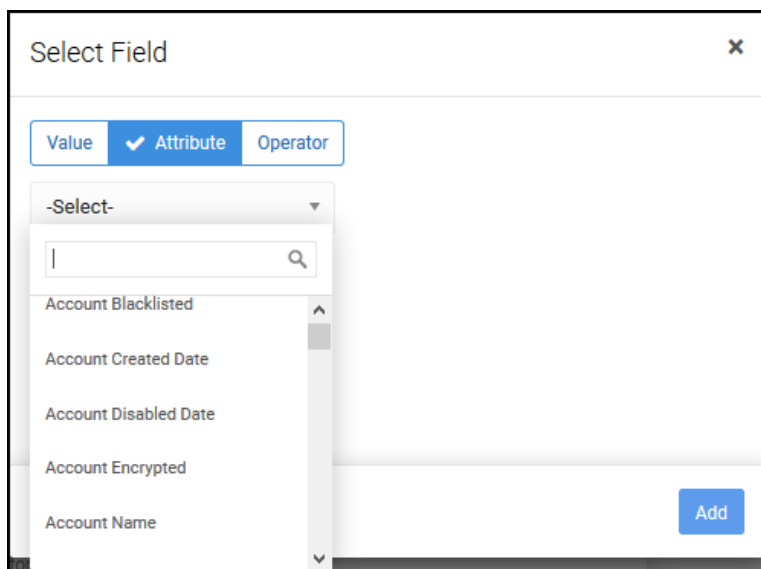
2. Click **URL** to select one of the following:

- **Value:** Enter a value.



The screenshot shows a dialog box titled "Select Field" with a close button (X) in the top right corner. Inside the dialog, there are three tabs: "Value" (which is selected and has a checkmark), "Attribute", and "Operator". Below the tabs is a large, empty text input field. At the bottom right of the dialog is a blue "Add" button.

- **Attribute:** Select from dropdown.



The screenshot shows the same "Select Field" dialog box, but now the "Attribute" tab is selected and has a checkmark. A dropdown menu is open below the tabs, showing a search bar and a list of attributes: "Account Blacklisted", "Account Created Date", "Account Disabled Date", "Account Encrypted", and "Account Name". The dropdown menu has a scroll bar on the right. The "Add" button is still visible at the bottom right.

- **Operator:** Click to add an operator nested inside the Web_Extractor operator. Click the field to specify the value of the nested operator.

Select Field

ValueAttributeOperator

DAY_OF_MONTHDay of month
DAY_OF_WEEKDay of week
STRING_DAY_OF_WEEKString day of week
MONTH_OF_YEARMonth of year
YEAR_OF_TIMEYear
SUMSum
MULMultiply
DIVDivide
SUBSubtract
BETWEENRange

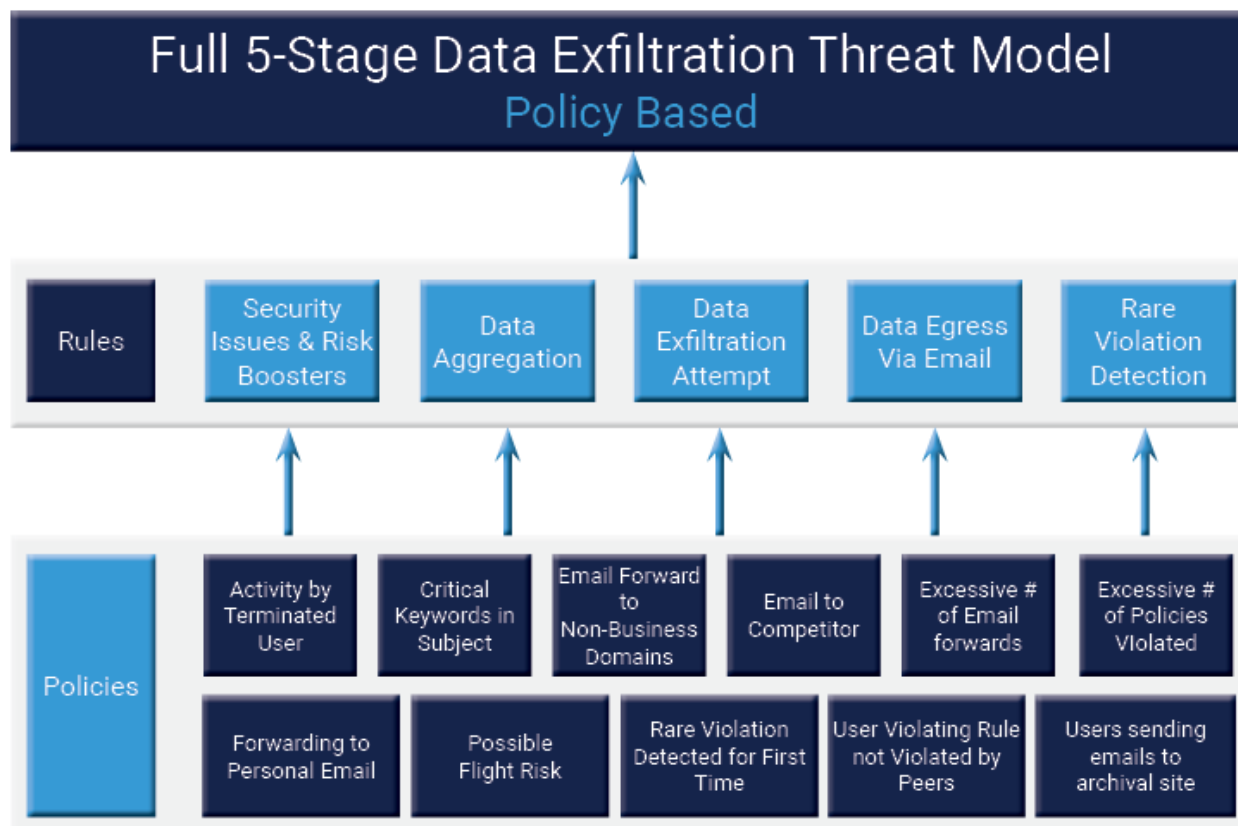
3. Repeat to populate value of **Value to Extract**.

Threat Modeler

ArcSight UBA uses Threat Models to boost the risk score of policies based on the policy category.

Threat Models

The Threat Modeler provides a security design that evaluates the possible goals of the adversary and the vulnerabilities that exist because of those goals.



The threat profile consists of the following main areas:

- Identify the threats
- Select the category, create the rule, and include the threats
- Investigate and analyze the threats
- Mitigate the vulnerabilities caused by the threats

Risk Scoring

- **Static Risk Scoring:** Model Score=Weight. Sets a static score for all users based on the weight selected. For example, if the weight specified is 10, all users will have a risk score of 10.
- **Exponential Scoring:** Model Score=(weight^(number of stages)). Uses predictive modeling to calculate a risk score based on the weight to the power of the number of stages. For Example, if the predictive scoring factor specified is 5 and the number of stages in the threat model is 3, users will have a risk score of 5^3 .



Note: While creating Stages in the Threat Model, the risk can be calculated for a user if the user violates *any one* of the policies. Similarly, the risk can be calculated for the user if the user violates *all* the policies.

Example

Category: Malware

Threat Model 1: Phishing attempt followed by visit to known malicious site

Policy A: Emails with same subject sent to several users

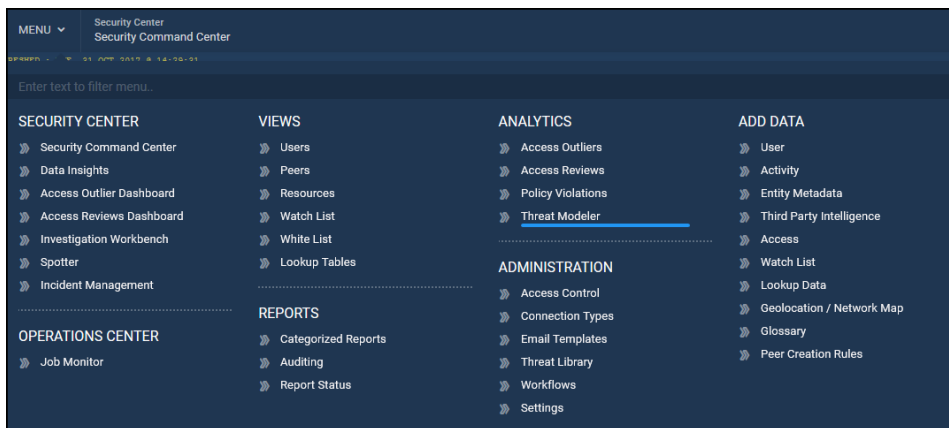
Policy B: Visit to malicious site

This section describes how to create Threat Models for Policies and Threat Models for Threats using the Threat Modeler.

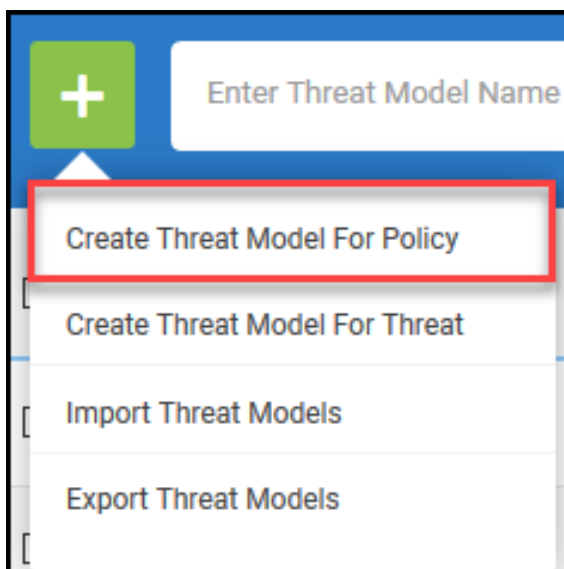
Creating a Threat Model for Policies

To create a Threat Model for Policies, complete the following steps:

1. Navigate to **Menu > Analytics > Threat Modeler**.



2. Click +.
3. Select **Create Threat Model for Policy**.



Threat Model Details

1. Complete the following information:

THREAT MODEL DETAILS

Threat Model Name*

Enter Threat Model Name

Threat Model Description

Enter Threat Model Description

Threat Model Violator *

Select

Select Threat Model Violator

Criticality

None

Set Criticality

Threat Response Playbook

Sample Template: <ul class=

Enter Threat Model Remediation Steps

Risk Scoring

Risk Scoring Scheme ⓘ

Static Risk Scoring Exponential Scoring

Static Score

0

Enter the score to be applied on Threat Model

Select To Associate Playbooks

<input type="checkbox"/> SNYPR SendAlertCEF Send violation alerts as CEF	<input type="checkbox"/> NO AUTO PLAY
<input type="checkbox"/> Demisto Incident playbook - Check URL Checks for Malicious URL in Virus Total	<input type="checkbox"/> NO AUTO PLAY
<input type="checkbox"/> Advanced Cyber Threat Incident Playbook Creates an incident in Demisto and blocks malicious IP addresses	<input type="checkbox"/> NO AUTO PLAY
<input type="checkbox"/> Tanium Extract Machine Info This playbook shows how to use automation scripts to interact with Tanium.	<input type="checkbox"/> NO AUTO PLAY
<input type="checkbox"/> Disable Account Disables the service or AD accounts	<input type="checkbox"/> NO AUTO PLAY
<input type="checkbox"/> Block IP Address Blocks the IP Address in Firewall	<input type="checkbox"/> NO AUTO PLAY

- Threat Model Name:** Provide a unique name for the threat model. Example: Advanced Cyber Threat.
- Threat Model Description:** Provide a brief description to indicate the purpose of the threat model.
- Threat Model Violator:** Select one of the following entities from the dropdown: Users, Activity Account, Resources, Activity IP.
- Criticality:** Use slider to set a criticality for the threat model.
- Threat Response Playbook:** Enter the steps to take to remediate this threat. Use HTML to control the way the steps are displayed on the Violation Summary screen. Example:

```
<ol>
```

```
<li>Review the Account Name and Domain Name fields, that identify the user who cleared the log</li><br>
```

```
<li>Additional fields of interest: Security ID, Logon ID, Subject</li><br>
```

```
<li>Login ID allows you to correlate backwards to the logon events as well as with other events logged during the same logon session</li><br>
```

```
<li><a href="supportticketsite.com">Submit a ticket to investigate</a></li>
```

```
</ol>
```

```

Threat Response Playbook

<ol>
<li>Review the Account Name and Domain Name fields, that identify the
user who cleared the log</li>
<li>Additional fields of interest: Security ID, Logon ID, Subject</li>
<li>Login ID allows you to correlate backwards to the logon events as well
as with other events logged during the same logon session</li>
<li><a href="supportticketsite.com">Submit a ticket to investigate</a></li>
</ol>

```

The Remediation Steps will appear on the Violation Summary screen:

VIOLATION SUMMARY	VIOLATION EVENTS	REMEDIATION STEPS
<ol style="list-style-type: none"> 1 Check the initial level privileges 2 Contact ITOps Administrator to get more insight into his privileges 3 Submit a ticket to investigate further 		

f. **Risk Scoring:**

- a. **Static Risk Scoring:** Provide a static risk score for the policy. Model Score = Weight.

Risk Scoring

Risk Scoring Scheme ⓘ

☒ Static Risk Scoring
 ☐ Exponential Scoring

Static Score

100

Enter the score to be applied on Threat Model

- b. **Exponential Scoring:** User slider or enter a weight exponent between 1 and 10. Model Score = Weight ^{^(number of stages)}.

Risk Scoring

Risk Scoring Scheme ⓘ

☐ Static Risk Scoring
 ☒ Exponential Scoring

100

^ Number of Stages

Enter weight value between 1 to 10

- g. **Select to Associate Playbooks:** Select the play books to associate with the threat indicator. Example: Disable Account.

For information about how playbooks work in ArcSight UBA, see [Automated Response](#).



Note: You may select multiple playbooks for the threat indicator.

- h. Enable **Auto Play** to automatically launch play book tasks upon violation.

If Auto Play is disabled, you can launch play book tasks manually from the violation summary screen when an incident occurs.

Stage Details

2. Complete the following information:

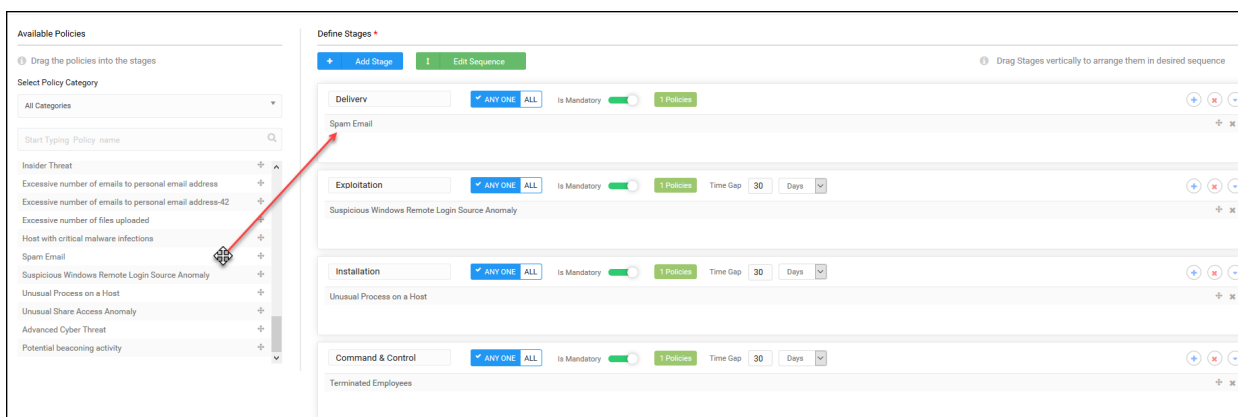
Available Policies

- a. **Select Policy Category:** Select from the dropdown to filter available policies. Available categories may vary based on the categories added or selected when creating Policies. Examples: Malware, Alert, Rogue Access Privileges, Insider Threat.

Define Stages

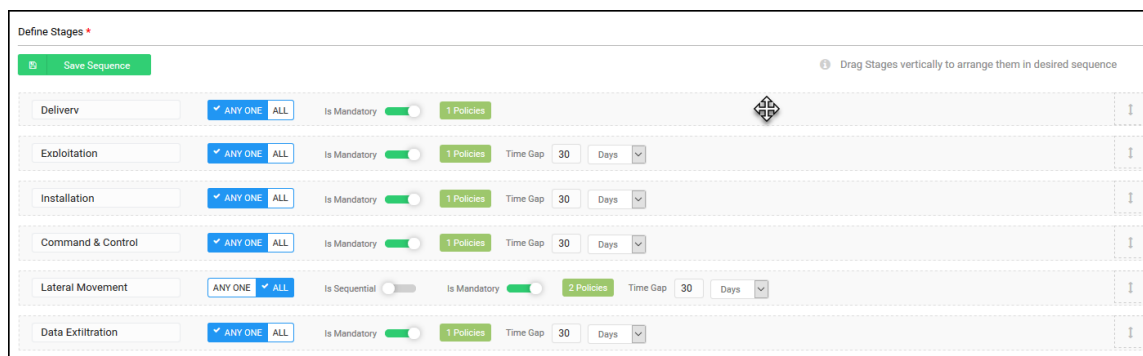
- a. **Add Stage:** Click to add stages to group policies together that define a threat.

- b. **Enter Stage Name:** Provide a unique name for the stage.
- c. **Any One/All:** Select to specify if risk will increase if they violate **Any One** of the policies in the stage, or if they must violate **All** policies in the stage to increase risk score.
3. Drag and drop policies from Available Policies into the each stage.



You can perform the following actions for stages:

- Rearrange policies within stages by dragging them into the preferred order.
- Click **Edit Sequence** to rearrange stages by dragging them into the preferred order.



- Click **Save Sequence** to save the new sequence.
- Click **+** or **Add Stage** to add stages to the threat model.
 - Specify if subsequent stage **Is Sequential** and specify a **Time Gap** in seconds, minutes, hours, or days.



- Click  to delete stages.

- Click **X** to delete policies.



- Click  to collapse or expand stages.

- Click **Save**.

- View the threat model from the Threat Modeler main screen.

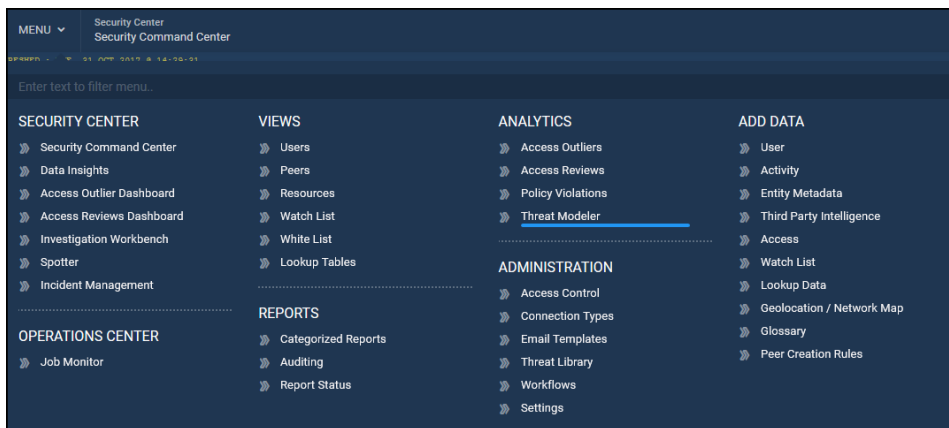
Name [1]	Category	Violation Entity	Weight Type [Weight]	Enabled?
<input type="checkbox"/> Advanced Cyber Threat	Category not selected	Activity/account	STATIC [100.0]	<input checked="" type="checkbox"/> YES
<input type="checkbox"/> Insider Threat	Category not selected	Users	STATIC [100.0]	<input type="checkbox"/> NO

6. Toggle **Enabled?** to **Yes** to enable the threat model. Default **Yes**.
7. Click trash icon to delete the threat model.

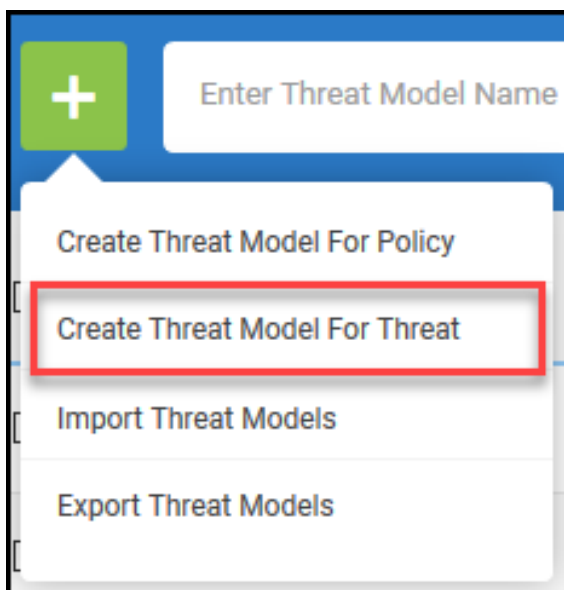
Creating a Threat Model for Threats

To create a Threat Model for Threats, complete the following steps:

1. Navigate to **Menu > Analytics > Threat Modeler**.



2. Click +.
3. Select **Create Threat Model for Threat**.



Threat Model Details

1. Complete the following information:

THREAT MODEL DETAILS

Threat Model Name*

Enter Threat Model Name

Threat Model Description

Enter Threat Model Description

Threat Model Violator *

Select

Select Threat Model Violator

Criticality

None

Set Criticality

Threat Response Playbook

Sample Template: <ul class=

Enter Threat Model Remediation Steps

Risk Scoring

Risk Scoring Scheme ⓘ

Static Risk Scoring Exponential Scoring

Static Score

0

Enter the score to be applied on Threat Model

Select To Associate Playbooks

<input type="checkbox"/> SNYPR SendAlertCEF Send violation alerts as CEF	<input type="checkbox"/> NO AUTO PLAY
<input type="checkbox"/> Demisto Incident playbook - Check URL Checks for Malicious URL in Virus Total	<input type="checkbox"/> NO AUTO PLAY
<input type="checkbox"/> Advanced Cyber Threat Incident Playbook Creates an incident in Demisto and blocks malicious IP addresses	<input type="checkbox"/> NO AUTO PLAY
<input type="checkbox"/> Tanium Extract Machine Info This playbook shows how to use automation scripts to interact with Tanium.	<input type="checkbox"/> NO AUTO PLAY
<input type="checkbox"/> Disable Account Disables the service or AD accounts	<input type="checkbox"/> NO AUTO PLAY
<input type="checkbox"/> Block IP Address Blocks the IP Address in Firewall	<input type="checkbox"/> NO AUTO PLAY

- Threat Model Name:** Provide a unique name for the threat model. Example: Advanced Cyber Threat.
- Threat Model Description:** Provide a brief description to indicate the purpose of the threat model.
- Threat Model Violator:** Select one of the following entities from the dropdown: Users, Activity Account, Resources, Activity IP.
- Criticality:** Use slider to set a criticality for the threat model.
- Threat Response Playbook:** Enter the steps to take to remediate this threat. Use HTML to control the way the steps are displayed on the Violation Summary screen. Example:

```
<ol>
```

```
<li>Review the Account Name and Domain Name fields, that identify the user who cleared the log</li><br>
```

```
<li>Additional fields of interest: Security ID, Logon ID, Subject</li><br>
```

```
<li>Login ID allows you to correlate backwards to the logon events as well as with other events logged during the same logon session</li><br>
```

```
<li><a href="supportticketsite.com">Submit a ticket to investigate</a></li>
```

```
</ol>
```

```

Threat Response Playbook

<ol>
<li>Review the Account Name and Domain Name fields, that identify the
user who cleared the log</li>
<li>Additional fields of interest: Security ID, Logon ID, Subject</li>
<li>Login ID allows you to correlate backwards to the logon events as well
as with other events logged during the same logon session</li>
<li><a href="supportticketsite.com">Submit a ticket to investigate</a></li>
</ol>

```

The Remediation Steps will appear on the Violation Summary screen:

VIOLATION SUMMARY	VIOLATION EVENTS	REMEDIATION STEPS
<ol style="list-style-type: none"> 1 Check the initial level privileges 2 Contact ITops Administrator to get more insight into his privileges 3 Submit a ticket to investigate further 		

f. **Risk Scoring:**

- a. **Static Risk Scoring:** Provide a static risk score for the policy. Model Score = Weight.

Risk Scoring

Risk Scoring Scheme ⓘ

☒ Static Risk Scoring
 ☐ Exponential Scoring

Static Score

100

Enter the score to be applied on Threat Model

- b. **Exponential Scoring:** User slider or enter a weight exponent between 1 and 10. Model Score = Weight ^ (number of stages).

Risk Scoring

Risk Scoring Scheme ⓘ

☐ Static Risk Scoring
 ☒ Exponential Scoring

100

^ Number of Stages

Enter weight value between 1 to 10

- g. **Select to Associate Playbooks:** Select the play books to associate with the threat indicator. Example: Disable Account.

For information about how playbooks work in ArcSight UBA, see [Automated Response](#).



Note: You may select multiple playbooks for the threat indicator.

- h. Enable **Auto Play** to automatically launch play book tasks upon violation.

If Auto Play is disabled, you can launch play book tasks manually from the violation summary screen when an incident occurs.

Stage Details

2. Complete the following information:

Available Policies

- a. **Select Threat Category:** Select from the dropdown to filter available Threats. Available threat categories may vary based on the categories added or selected when creating Policies. Examples: Data Exfiltration, Account Misuse, Exploit, Fraud.

Define Stages

- a. **Add Stage:** Click to add stages to group threats together.
- b. **Enter Stage Name:** Provide a unique name for the stage.
- c. **Any One/All:** Select to specify if risk will increase if they violate **Any One** of the threats in the stage, or if they must violate **All** threats in the stage to increase risk score.
3. Drag and drop threats from Available Threats into the each stage.

You can perform the following actions for stages:

- a. Rearrange policies within stages by dragging them into the preferred order.
- b. Click **Edit Sequence** to rearrange stages or policies by dragging them into the preferred order.

Click **Save Sequence** to save the new sequence.

- c. Click **+** or **Add Stage** to add stages to the threat model.
 - a. Specify if subsequent stage **Is Sequential** and specify a **Time Gap** in seconds, minutes, hours, or days.



- d. Click  to delete stages.

- e. Click **X** to delete threats.



- f. Click  to collapse or expand stages.

4. Click **Save**.
5. View the threat model from the Threat Modeler main screen.

+ Enter Threat Model Name ✎ 🔍						
<input type="checkbox"/>	Name ⓘ	Category	Violation Entity	Weight Type [Weight]	Enabled?	Actions
<input type="checkbox"/>	Advanced Cyber Threat	Category not selected	Users	STATIC [100.0]	YES	
<input type="checkbox"/>	Insider Threat	Category not selected	Users	STATIC [100.0]	YES	
<input type="checkbox"/>	Patient Data Compromise	Category not selected	Users	STATIC [100.0]	YES	
<input type="checkbox"/>	Privilege Misuse	Category not selected	Activityaccount	STATIC [100.0]	YES	

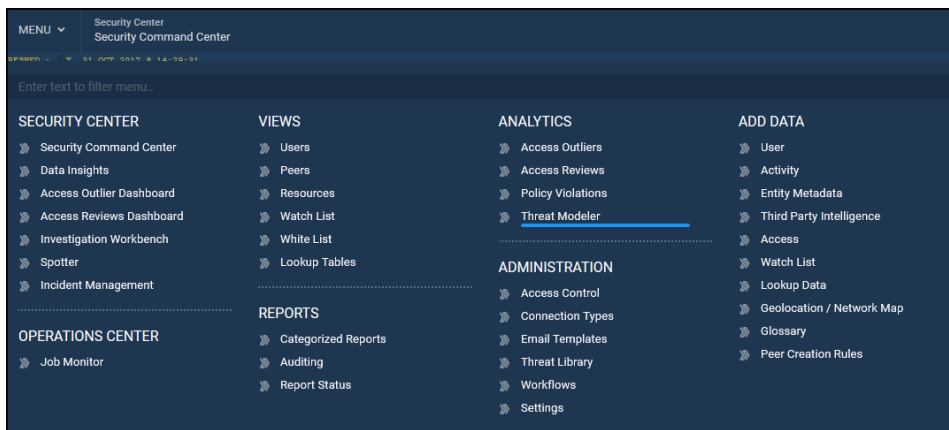
First < 1 > Last Show 15 Total results : 4 | Total pages

6. Toggle **Enabled?** to **Yes** to enable the threat model. Default **Yes**.
7. Click trash icon to delete the threat model.

Importing Threat Models

To import updates to existing threat models, complete the following steps:

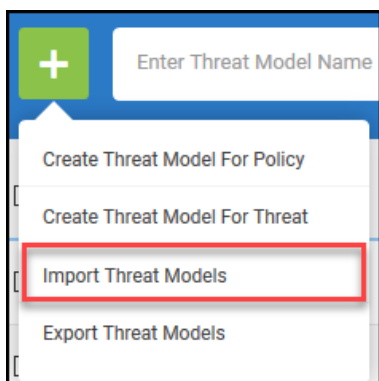
1. Navigate to **Menu > Analytics > Threat Modeler**.



2. Check the threat models to import from list of available threat models.

Enter Threat Model Name				
Name	Category	Violation Entity	Weight Type [Weight]	Enabled?
<input checked="" type="checkbox"/> Account Misuse	ACCOUNT MISUSE	Activityaccount	MULTIPLIER [5.0]	<input checked="" type="checkbox"/> YES
<input type="checkbox"/> Data Exfiltration 1	INSIDER THREAT	Users	MULTIPLIER [5.0]	<input type="checkbox"/> NO
<input checked="" type="checkbox"/> LandSpeedViolation_DrivePermission	Category not selected	Activityaccount	EXPONENTIAL [5.0]	<input checked="" type="checkbox"/> YES

3. Click **+**.
4. Click **Import Threat Models**.



The Threat Models window displays the threat models available for import.

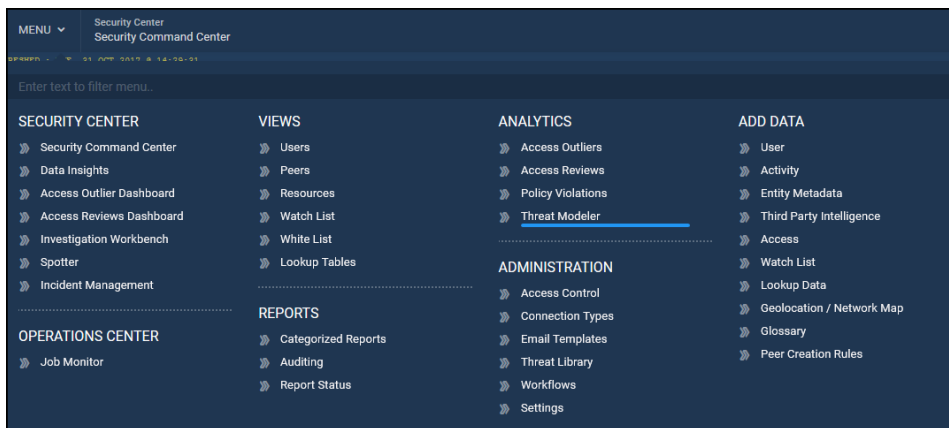
The screenshot shows a web interface titled "Threat Models" with a close button (X) in the top right corner. Below the title is an "Override" section with a radio button labeled "NO". A blue horizontal bar contains a search input field with the placeholder text "Enter your search criteria" and a magnifying glass icon. Below this is a table with a single header row labeled "Threat Model Name". Under the table header are navigation buttons: "First", "<", ">", and "Last". At the bottom right of the interface is a button labeled "Import Threat Models".

5. Enable **Override** to override existing models with imported models.
6. Click **Import Threat Models**.

Exporting Threat Models

To export threat models to the local database, complete the following steps:

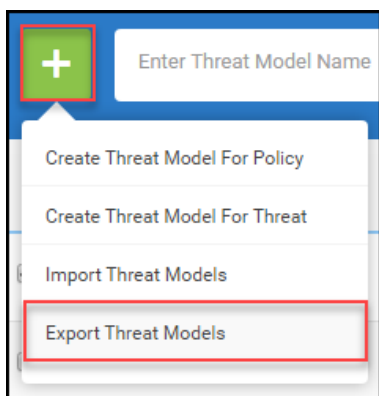
1. Navigate to **Menu > Analytics > Threat Modeler**.



2. Check the threat models to export from list of available threat models.

Enter Threat Model Name				
Name	Category	Violation Entity	Weight Type [Weight]	Enabled?
<input checked="" type="checkbox"/> Account Misuse	ACCOUNT MISUSE	Activityaccount	MULTIPLIER [5.0]	<input checked="" type="checkbox"/>
<input type="checkbox"/> Data Exfiltration 1	INSIDER THREAT	Users	MULTIPLIER [5.0]	<input type="checkbox"/>
<input checked="" type="checkbox"/> LandSpeedViolation_DrivePermission	Category not selected	Activityaccount	EXPONENTIAL [5.0]	<input checked="" type="checkbox"/>

3. Click **+**.
4. Click **Export Threat Models**.



You will receive the message **Threat Models Exported Successfully** to indicate the threat models have been exported to the local database.

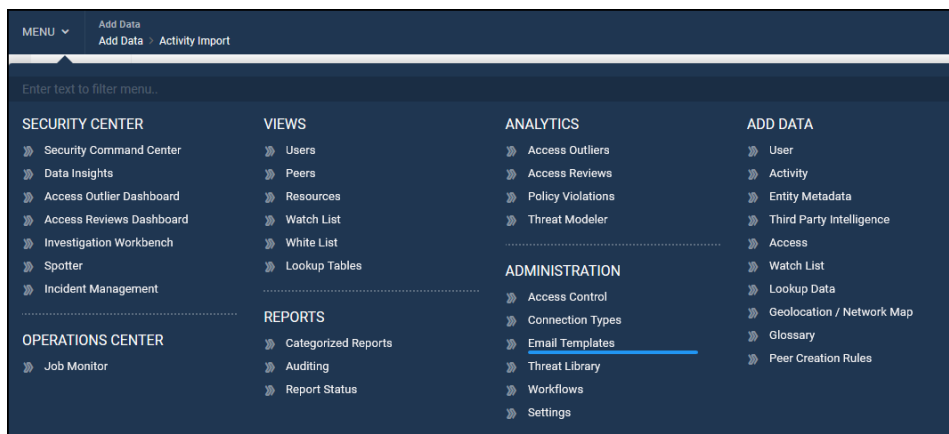
+ Enter Threat Model Name				
Threat Models exported successfully				
Name	Category	Violation Entity	Weight Type [Weight]	Enabled
<input checked="" type="checkbox"/> Account Misuse	ACCOUNT MISUSE	Activityaccount	MULTIPLIER [5.0]	<input checked="" type="checkbox"/>
<input type="checkbox"/> Data Exfiltration 1	INSIDER THREAT	Users	MULTIPLIER [5.0]	<input type="checkbox"/>
<input checked="" type="checkbox"/> LandSpeedviolation_DrivePermission	Category not selected	Activityaccount	EXPONENTIAL [5.0]	<input checked="" type="checkbox"/>

Email Templates

The ArcSight UBA application provides default email templates that are readily available for different modules. Customize these templates so that they can be used to notify users about jobs updates, password resets or about policy violations, for example.

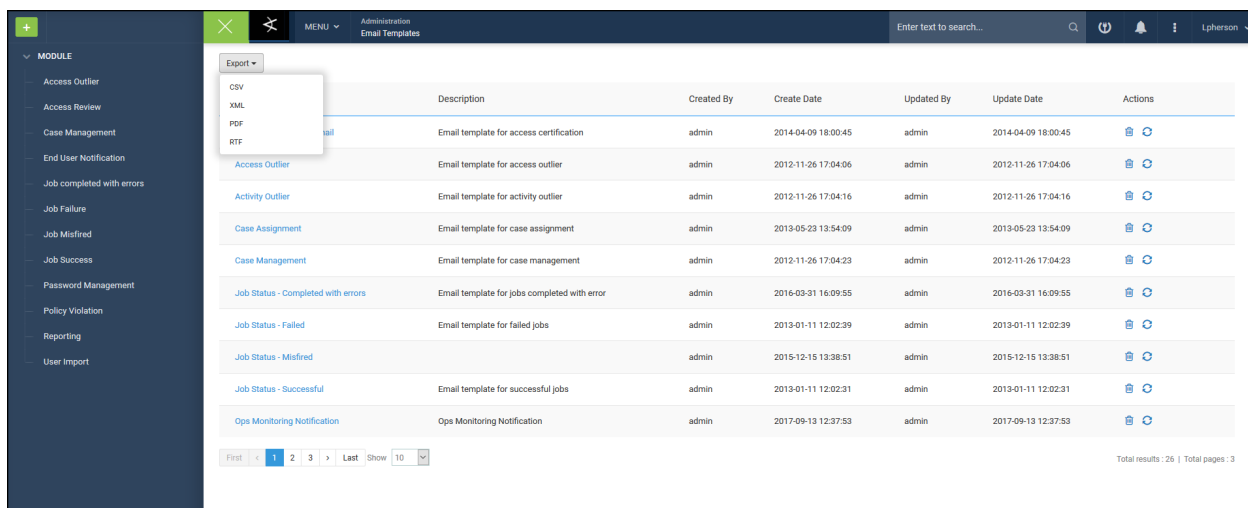
Using Email Templates

To access the email templates, navigate to **Menu > Administration > Email Templates**.



Viewing and Editing Email Templates

The Email Template screen shows the **Modules** in the left panel and a variety of default templates on the right.



Click on a module or directly on a template name to display the editable template.

ENTER EMAIL TEMPLATE INFORMATION

Sender Name*

Template Name*

Description

To*

From*

CC

Store in Outbox prior to sending?
☒ YES

Use this template for
 Access Review

Email Body

Add Email Template Variables

The main part of an email message containing the actual, arbitrary data such as text or images.

Save

The email template offers hover help for additional information on fields. For example, for the **To** field for email, you can use commas to separate more than one email address. The **Email Body** contains variables in the email text that are contextual to the module. To learn more about a variable or add a new variable for that specific module, click the **Add Email Template Variables**.

Customize the template as needed per the instructions in [Adding Email Templates](#).

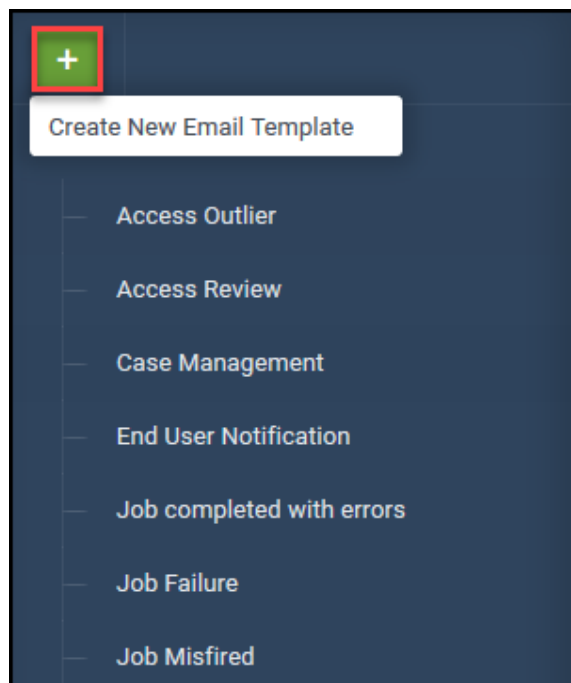
Click **Save**.

The updated email template is used, for example, when an access certification job is pending a review.

Adding Email Templates

To add an email template, complete the following steps:

Click **+** from the left navigation panel.



Complete the following information:



- **Sender Name:** Enter the name of the sender.
- **Template Name:** Enter a unique name for the template.
- **Description:** Enter a description of the template.
- **To:** Enter the email address of the recipient.
- **From:** Skip. Default sender address will be auto-filled.
- **CC:** Enter email addresses of the carbon copy recipients separated by commas.
- **BCC:** Enter email address of the blind carbon copy recipients separated by commas.

[illegible]

- **Subject:** Enter a subject for the email template.
- **HTML Enabled:** Toggle to **YES** to enable HTML.
- **Store in Outbox prior to sending?:** Toggle to **YES** to store outgoing messages in the outbox prior to sending.



Note: View the Outbox from the collapsed menu on the top navigation menu.

- **Use this template for:** Select a module for the template.
- **Email Body:** Enter and format text AND/OR click **Add Email Template Variables** to include variables:

Email			
<input type="checkbox"/>	Variable Name	Description	Module
<input type="checkbox"/>	\${access_history}	Access history	Access Review
<input type="checkbox"/>	\${access_value}	Access value	Access Outlier
<input type="checkbox"/>	\${account_name}	Account name	Event Import Quick Alerts
<input type="checkbox"/>	\${approver_email}	Approver Email	User Import
<input type="checkbox"/>	\${approver_firstname}	Approver Firstname	User Import
<input type="checkbox"/>	\${approver_lastname}	Approver Lastname	User Import
<input type="checkbox"/>	\${assignee_first_name}	Assignee first name	Case Management
<input type="checkbox"/>	\${assignee_last_name}	Assignee last name	Case Management
<input type="checkbox"/>	\${assignee_manager}	Assignee's manager	Case Management
<input type="checkbox"/>	\${attributes}	Attributes	Event Import Quick Alerts
<input type="checkbox"/>	\${attribute_value}	Attribute value	Access Outlier
<input type="checkbox"/>	\${av_group_owner_department}	Group owner department	Access Outlier
<input type="checkbox"/>	\${av_group_owner_email}	Group owner email id	Access Outlier
<input type="checkbox"/>	\${av_group_owner_employee_id}	Group owner employee id	Access Outlier

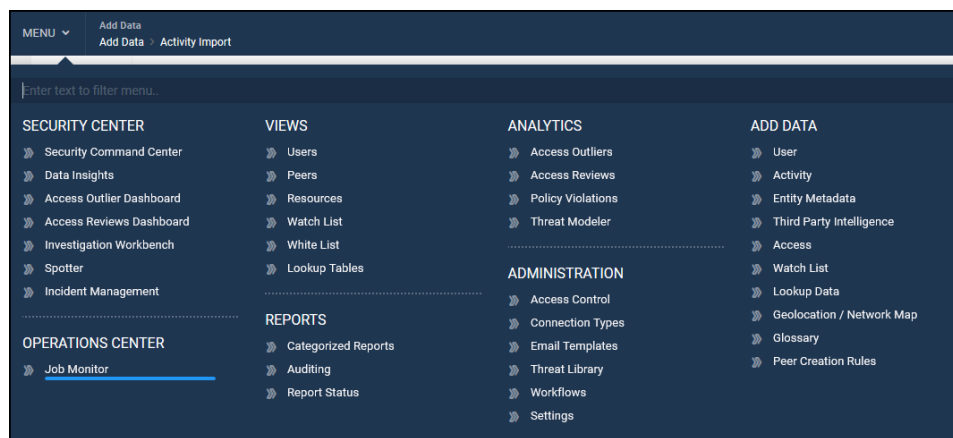
Click **Save**.

Job Monitor

The Job Monitor provides a centralized view of all data import and policy violation jobs in ArcSight UBA.

Monitoring Jobs

To access the Job Monitor, navigate to **Menu > Operations Center > Job Monitor**.



The Job Monitor screen displays a list of the latest jobs with additional details including the following:

- Job Details
- Schedule Details
- Today's Run Statistics
- Published Events History

By default, jobs are displayed by data import type.

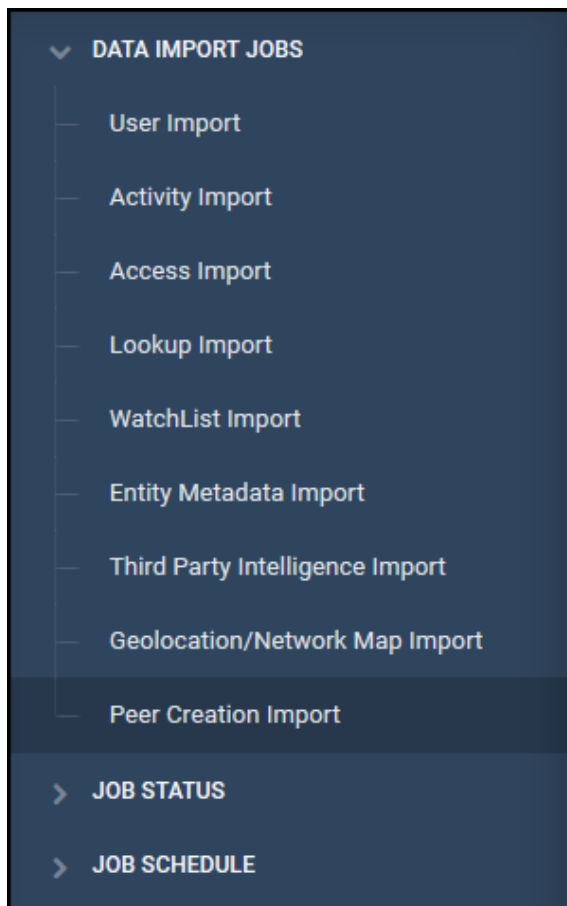
Jobs Details		Schedule Details	Today's Run Statistics					Published Events History
ACTIVITY IMPORT DATASOURCE NAME: BLUESOCK NATIVE PROXY DEVICE TYPE: BLUESOCK NATIVE EDIT VIEW CONFIG VIEW JOBS		SCHEDULE: ONCE LAST RUN: WED, OCT 25 2017 @ 17:12:12 NEXT RUN: -	542 PUBLISHED	297 PASSED	245 UNPUBLISHED	297 RECEIVED	297 STORED	NO PUBLISHED EVENTS FOR LAST 7 DAYS
		SCHEDULE: ONCE LAST RUN: FRI, OCT 13 2017 @ 18:56:33 NEXT RUN: -	0 PUBLISHED	0 PASSED	0 UNPUBLISHED	0 RECEIVED	0 STORED	NO PUBLISHED EVENTS FOR LAST 7 DAYS
		SCHEDULE: ONCE LAST RUN: THU, OCT 12 2017 @ 15:22:44 NEXT RUN: -	0 PUBLISHED	0 PASSED	0 UNPUBLISHED	0 RECEIVED	0 STORED	NO PUBLISHED EVENTS FOR LAST 7 DAYS
		SCHEDULE: ONCE LAST RUN: WED, OCT 11 2017 @ 17:39:26 NEXT RUN: MON, OCT 9 @ 03:44:30:000	0 PUBLISHED	0 PASSED	0 UNPUBLISHED	0 RECEIVED	0 STORED	NO PUBLISHED EVENTS FOR LAST 7 DAYS
		SCHEDULE: ONCE LAST RUN: WED, OCT 11 2017 @ 15:46:15 NEXT RUN: -	0 PUBLISHED	0 PASSED	0 UNPUBLISHED	0 RECEIVED	0 STORED	NO PUBLISHED EVENTS FOR LAST 7 DAYS
		SCHEDULE: ONCE LAST RUN: WED, OCT 11 2017 @ 15:46:15 NEXT RUN: -	0 PUBLISHED	0 PASSED	0 UNPUBLISHED	0 RECEIVED	0 STORED	NO PUBLISHED EVENTS FOR LAST 7 DAYS

You can perform the following actions from this screen:

Click Filter icon to select one of the following:

- **Jobs List:** Expands the left navigation panel.

View jobs by the following:



- **Data Import Jobs:** Select a data import type.
- **Job Status:** Select a job status.
- **Job Schedule:** Select a job schedule.
- **Jobs by Datasource:** Display jobs by datasource:

Job Name	Creation Date	Start Date	Next Trigger Date	Job Status
BLUECOAT NATIVE PROXY_REGEX_10_25_2017_05_12_10_PM CREATED BY: ADMIN / JOB TYPE: ACTIVITY IMPORT EDIT JOB RE-RUN JOB DELETE JOB	WED, 25 OCT 2017 @ 05:12:12.000 PM	START DATE: WED, 25 OCT 2017 @ 05:12:12.000 PM	NOT SCHEDULED	NOT AVAILABLE
BLUECOAT NATIVE PROXY_REGEX_10_25_2017_04_43_34_PM CREATED BY: ADMIN / JOB TYPE: ACTIVITY IMPORT EDIT JOB RE-RUN JOB DELETE JOB	WED, 25 OCT 2017 @ 04:43:26.000 PM	START DATE: WED, 25 OCT 2017 @ 04:43:26.000 PM	NOT SCHEDULED	NOT AVAILABLE
BLUECOAT NATIVE PROXY_REGEX_10_25_2017_03_59_05_PM CREATED BY: ADMIN / JOB TYPE: ACTIVITY IMPORT EDIT JOB RE-RUN JOB DELETE JOB	WED, 25 OCT 2017 @ 03:59:45.000 PM	START DATE: WED, 25 OCT 2017 @ 03:59:45.000 PM	NOT SCHEDULED	NOT AVAILABLE
BLUECOAT NATIVE PROXY_REGEX_10_25_2017_03_38_52_PM CREATED BY: ADMIN / JOB TYPE: ACTIVITY IMPORT EDIT JOB RE-RUN JOB DELETE JOB	WED, 25 OCT 2017 @ 03:38:57.000 PM	START DATE: WED, 25 OCT 2017 @ 03:38:57.000 PM	NOT SCHEDULED	NOT AVAILABLE
DIGITAL GUARDIAN USB_DELIMITED_PIPE_10_13_2017_06_56_36_PM CREATED BY: ADMIN / JOB TYPE: ACTIVITY IMPORT EDIT JOB RE-RUN JOB DELETE JOB	FRI, 13 OCT 2017 @ 06:56:33.000 PM	START DATE: FRI, 13 OCT 2017 @ 06:56:33.000 PM	NOT SCHEDULED	NOT AVAILABLE

Click Refresh icon to refresh list.

Click a data import type to filter the list. Click **X** to remove a filter.

Jobs Details	Schedule Details	Today's Run Statistics	Published Events History
THIRD PARTY INTELLIGENCE CONNECTION TYPE: THREATSTREAM EDIT VIEW JOBS	SCHEDULE: ONCE LAST RUN: TUE, OCT 10 2017 @ 18:04:17 NEXT RUN: -	<div>0 PUBLISHED</div> <div>0 STORED</div> <div>0 INDEXED</div>	EVENTS HISTORY TREND
THIRD PARTY INTELLIGENCE CONNECTION TYPE: NSA EDIT VIEW JOBS	SCHEDULE: ONCE LAST RUN: MON, SEP 11 2017 @ 17:27:46 NEXT RUN: -	<div>0 PUBLISHED</div> <div>0 STORED</div> <div>0 INDEXED</div>	EVENTS HISTORY TREND

First 1 Last Show 10

Total results: 2 | Total pages: 1

Click a Datasource Name to view Today's Statistics for the datasource.

ACTIVITY IMPORT	
DATASOURCE NAME	BLUECOAT NATIVE PROXY
TODAY'S STATICS	
PUBLISHED	542
PARSED	297
UNPARSED	245
INDEXED	297
STORED	297
CORRELATED	297
VIOLATIONS	10

Click **Edit** to be redirected to the data import screen to edit the data import configuration.

Jobs Details

ACTIVITY IMPORT

DATASOURCE NAME : BLUECOAT NATIVE PROXY

DEVICE TYPE : BLUECOAT NATIVE

EDIT

VIEW CONFIG

VIEW JOBS

Click **View Config** to view and edit the configuration for the data import job.

Configuration

Activity Import Summary

DEVICE TYPE INFORMATION

Datasource Name	IP Address
Bluecoat Native Proxy	
Vendor	Functionality
Blue Coat Systems	Web Proxy
Resource Type	
Bluecoat Native	

COLLECTION METHOD

Method	
file	
All Files Matching Condition	
Prefix : final_bluecoat_sample_test.txt	
Show more	

POLICIES

YES

Traffic to proxy anonymizing websites-17

This check detects attempts to bypass proxy controls by the use of anonymizing utilities

YES

High volume of uploads to storage sites-17

This check detects high amounts of data uploads to external sites indicating a possible exfiltration activity

YES

Flight risk behavior on web browsing-17

This check detects employees exhibiting signs of possible flight risk behavior

NO

Web browsing activity from terminated accounts-17

This check determines web browsing activity by users post their termination

NO

Abnormal number of failed attempts to storage sites compared to past behavior-17

This check detects high number of attempts to visit mass storage sites indicating a possible data exfiltration attempt

NO

Rare domain visited by account-17

This check detects an entity visiting a rare domain which is relative to the organization's web visit behavior

THREAT MODELS

No Threat Models Available to configure Policy

Click **View Jobs** to filter list by job type. Click **Back to Jobs by All Types** to return to the previous screen.

JOBS FOR : BLUECOAT NATIVE PROXY					Back to Jobs by All Types
Job Name	Creation Date	Start Date	Next Trigger Date	Job Status	
BLUECOAT NATIVE PROXY_REGEX_10_25_2017_05_12_10_PM CREATED BY : ADMIN / JOB TYPE : ACTIVITY IMPORT EDIT JOB RERUN JOB DELETE JOB	WED, 25 OCT 2017 @ 05:12:12.000 PM	START DATE : WED, 25 OCT 2017 @ 05:12:12.000 PM	NOT SCHEDULED	NOT AVAILABLE	
BLUECOAT NATIVE PROXY_REGEX_10_25_2017_04_43_34_PM CREATED BY : ADMIN / JOB TYPE : ACTIVITY IMPORT EDIT JOB RERUN JOB DELETE JOB	WED, 25 OCT 2017 @ 04:43:26.000 PM	START DATE : WED, 25 OCT 2017 @ 04:43:26.000 PM	NOT SCHEDULED	NOT AVAILABLE	
BLUECOAT NATIVE PROXY_REGEX_10_25_2017_03_59_05_PM CREATED BY : ADMIN / JOB TYPE : ACTIVITY IMPORT EDIT JOB RERUN JOB DELETE JOB	WED, 25 OCT 2017 @ 03:59:45.000 PM	START DATE : WED, 25 OCT 2017 @ 03:59:45.000 PM	NOT SCHEDULED	NOT AVAILABLE	
BLUECOAT NATIVE PROXY_REGEX_10_25_2017_03_38_52_PM CREATED BY : ADMIN / JOB TYPE : ACTIVITY IMPORT EDIT JOB RERUN JOB DELETE JOB	WED, 25 OCT 2017 @ 03:38:57.000 PM	START DATE : WED, 25 OCT 2017 @ 03:38:57.000 PM	NOT SCHEDULED	NOT AVAILABLE	

First

<

1

>

Last


Show

10

Total results : 4 | Total pages : 1

Click **Pause** or **Stop** to pause or stop an active job.

ACTIVITY IMPORT

DATASOURCE NAME : INFOBLOX 

DEVICE TYPE : INFOBLOX

EDIT

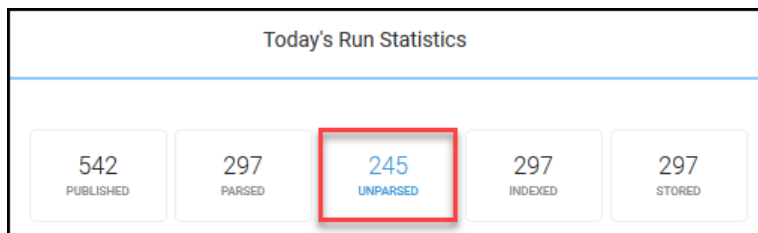
VIEW CONFIG

VIEW JOBS


PAUSE


STOP


Click **Unparsed** events from Today's Run Statistics to view unparsed events for the datasource.




You can take the following actions from the dialogue box:

Invalid Events 

Date
 10/26/2017

Job List
Select an Option 

Download Events For Job
 Download Events

Event	Error Message Count
No Records Found	

- Select an option from **Job List** dropdown to filter list.
- **Download Events for Job.**

Appendix A: ArcSight UBA Attribute Schema

ArcSight UBA stores and indexes data using an open data model. Using the following attribute schema, enriched events are compressed and stored in JSON format in HDFS as database accessible log data, and indexed in Solr collections for searching in Spotter.

Attributes are mapped during data ingestion. See Importing [User Data](#), [Activity Data](#), [Access Data](#), [Geolocation/Network Map Data](#), and [Third Party Intelligence](#) for more information about data ingestion.

Attributes in ArcSight UBA

Type	Attribute
Date Attributes	eventtime
Date Attributes	year
Date Attributes	week
Date Attributes	month
Date Attributes	dayofyear
Date Attributes	dayofweek
Date Attributes	dayofmonth
Date Attributes	hour
Date Attributes	minute
Date Attributes	categorizedtime
Date Attributes	endtime
Date Attributes	starttime
Date Attributes	devicecustomdate1
Date Attributes	devicecustomdate2
Account & User Event Attributes	accountname
Account & User Event Attributes	accounttype
Account & User Event Attributes	accountowner
Account & User Event Attributes	accountstatus
Account & User Event Attributes	accountcriticality
Account & User Event Attributes	accountcreateddate
Account & User Event Attributes	accountdisableddate
Account & User Event Attributes	accountwhitelisted
Account & User Event Attributes	accountblacklisted

Type	Attribute
Account & User Event Attributes	accountencrypted
Account & User Event Attributes	sourceuserid
Account & User Event Attributes	sourceusername
Account & User Event Attributes	sourceuserprivileges
Account & User Event Attributes	destinationuserprivileges
Account & User Event Attributes	destinationuserid
Account & User Event Attributes	destinationusername
User Identity Attributes	u_id
User Identity Attributes	u_employeeid
User Identity Attributes	u_firstname
User Identity Attributes	u_middlename
User Identity Attributes	u_lastname
User Identity Attributes	u_department
User Identity Attributes	u_division
User Identity Attributes	u_location
User Identity Attributes	u_manageremployeeid
User Identity Attributes	u_workemail
User Identity Attributes	u_workphone
User Identity Attributes	u_title
User Identity Attributes	u_employeetype
User Identity Attributes	u_status
User Identity Attributes	u_uniquecode
User Identity Attributes	u_riskscore

Type	Attribute
User Identity Attributes	u_customfield1
User Identity Attributes	u_customfield2
User Identity Attributes	u_customfield3
User Identity Attributes	u_customfield4
User Identity Attributes	u_customfield5
User Identity Attributes	u_customfield6
User Identity Attributes	u_customfield7
User Identity Attributes	u_customfield8
User Identity Attributes	u_customfield9
User Identity Attributes	u_customfield10
User Identity Attributes	u_customfield11
User Identity Attributes	u_customfield12
User Identity Attributes	u_customfield13
User Identity Attributes	u_customfield14
User Identity Attributes	u_customfield15
User Identity Attributes	u_customfield16
User Identity Attributes	u_customfield17
User Identity Attributes	u_customfield18
User Identity Attributes	u_customfield19
User Identity Attributes	u_customfield20
User Identity Attributes	u_customfield21
User Identity Attributes	u_customfield22
User Identity Attributes	u_customfield23

Type	Attribute
User Identity Attributes	u_customfield24
User Identity Attributes	u_customfield25
User Identity Attributes	u_customfield26
User Identity Attributes	u_customfield27
User Identity Attributes	u_customfield28
User Identity Attributes	u_customfield29
User Identity Attributes	u_customfield30
User Identity Attributes	u_promoted
User Identity Attributes	u_createdate
User Identity Attributes	u_usergroup
User Identity Attributes	u_street
User Identity Attributes	u_city
User Identity Attributes	u_province
User Identity Attributes	u_zipcode
User Identity Attributes	u_userstate
User Identity Attributes	u_region
User Identity Attributes	u_country
User Identity Attributes	u_approveremployeeid
User Identity Attributes	u_delegateemployeeid
User Identity Attributes	u_technicalapproverid
User Identity Attributes	u_extension
User Identity Attributes	u_fax
User Identity Attributes	u_mobile

Type	Attribute
User Identity Attributes	u_pager
User Identity Attributes	u_jobcode
User Identity Attributes	u_comments
User Identity Attributes	u_createdby
User Identity Attributes	u_costcentername
User Identity Attributes	u_costcentercode
User Identity Attributes	u_enabledate
User Identity Attributes	u_disabledate
User Identity Attributes	u_deletedate
User Identity Attributes	u_updatedate
User Identity Attributes	u_sunrisedate
User Identity Attributes	u_sunsetdate
User Identity Attributes	u_criticality
User Identity Attributes	u_domintlin
User Identity Attributes	u_nameprefix
User Identity Attributes	u_namesuffix
User Identity Attributes	u_preferredname
User Identity Attributes	u_secondaryphone
User Identity Attributes	u_statusdescription
User Identity Attributes	u_vacationstart
User Identity Attributes	u_vacationend
User Identity Attributes	u_networkid
User Identity Attributes	u_workpager

Type	Attribute
User Identity Attributes	u_workextensionnumber
User Identity Attributes	u_workfax
User Identity Attributes	u_employeestatuscode
User Identity Attributes	u_locationcode
User Identity Attributes	u_locationname
User Identity Attributes	u_mailcode
User Identity Attributes	u_hiredate
User Identity Attributes	u_rehiredate
User Identity Attributes	u_recenthiredate
User Identity Attributes	u_terminationdate
User Identity Attributes	u_lastdayworked
User Identity Attributes	u_contractstartdate
User Identity Attributes	u_contractenddate
User Identity Attributes	u_employeetypedescription
User Identity Attributes	u_regtempin
User Identity Attributes	u_fulltimeparttimein
User Identity Attributes	u_managerfirstname
User Identity Attributes	u_managerlastname
User Identity Attributes	u_managemiddlename
User Identity Attributes	u_orgunitnumber
User Identity Attributes	u_companycode
User Identity Attributes	u_companynumber
User Identity Attributes	u_hierarchy

Type	Attribute
User Identity Attributes	u_lastperformancereviewdate
User Identity Attributes	u_lastperformancereviewresult
User Identity Attributes	u_standardhours
User Identity Attributes	u_shiftcode
User Identity Attributes	u_shiftname
User Identity Attributes	u_lanid
User Identity Attributes	u_userid
User Identity Attributes	u_transferreddate
User Identity Attributes	u_datasourceid
User Identity Attributes	u_timezoneoffset
User Identity Attributes	u_encrypted
User Identity Attributes	u_encryptedfields
User Identity Attributes	u_maskedfields
User Identity Attributes	u_masked
User Identity Attributes	u_lastsynctime
User Identity Attributes	u_mergeuniquecode
User Identity Attributes	u_skipencryption
Resource Group Attributes	rg_id
Resource Group Attributes	rg_name
Resource Group Attributes	rg_type
Resource Group Attributes	rg_vendor
Resource Group Attributes	rg_functionality
Resource Group Attributes	rg_ownerid

Type	Attribute
Resource Group Attributes	rg_riskscore
Resource Group Attributes	rg_criticality
Resource Group Attributes	rg_deviceid
Resource Group Attributes	rg_timezoneoffset
Resource Group Attributes	rg_aggregatelevel
Resource Group Attributes	rg_resourcetypeid
Resource Group Attributes	rg_clusterid
Resource Group Attributes	rg_ipaddress
Resource Group Attributes	rg_category
Resource Group Attributes	rg_amountroundupvalue
Resource Group Attributes	rg_syslogenabled
Resource Group Attributes	rg_syslogport
Resource Group Attributes	rg_customerid
Resource Group Attributes	rg_parentstatus
Resource Group Attributes	rg_parentid
Resource Group Attributes	rg_retainedaccessentitlements
Resource or Device Attributes	resourcename
Resource or Device Attributes	resourcetype
Resource or Device Attributes	resourcecomments
Resource or Device Attributes	resourcecustomfield1
Resource or Device Attributes	resourcecustomfield2
Resource or Device Attributes	resourcecustomfield3
Resource or Device Attributes	resourcecustomfield4

Type	Attribute
Resource or Device Attributes	resourcecustomfield5
Resource or Device Attributes	resourcecustomfield6
Resource or Device Attributes	resourcecustomfield7
Resource or Device Attributes	resourcecustomfield8
Resource or Device Attributes	resourcehierarchy
Resource or Device Attributes	resourcehierarchyname
Resource or Device Attributes	resourcestatus
Resource or Device Attributes	resourcehostname
Network	ipaddress
Network	sourcehostname
Network	sourceaddress
Network	sourceport
Network	sourcemacaddress
Network	sourcecntdomain
Network	sourcednsdomain
Network	destinationhostname
Network	destinationaddress
Network	destinationport
Network	destinationmacaddress
Network	destinationntdomain
Network	deviceaddress
Network	devicehostname
Network	devicemacaddress

Type	Attribute
Network	devicentdomain
Network	devicednsdomain
Network	devicedirection
Network	devicefacility
Network	deviceinboundinterface
Network	deviceoutboundinterface
Network	destinationdnsdomain
Network	applicationprotocol
Network	translatedipaddress
Network	translatedport
Network	destinationtranslatedaddress
Network	destinationtranslatedport
Event Identifiers	baseeventid
Event Identifiers	sessionid
Event Identifiers	alertid
Event Identifiers	deviceexternalid
Event Identifiers	siemid
Event Identifiers	flowsiemid
Event Identifiers	baseeventcount
Process Information	sourceprocessid
Event Identifiers	sourceprocessname
Event Identifiers	sourceservicename
Event Identifiers	destinationprocessid

Type	Attribute
Event Identifiers	destinationprocessname
Event Identifiers	destinationservicename
Event Identifiers	deviceprocessid
Event Identifiers	deviceprocessname
Email Attributes	emailsubject
Email Attributes	emailsender
Email Attributes	emailsenderdomain
Email Attributes	emailrecipient
Email Attributes	emailrecipientdomain
Email Attributes	emailrecipienttype
File Attributes	filename
File Attributes	filepath
File Attributes	filetype
File Attributes	filesize
File Attributes	filehash
File Attributes	filepermission
File Attributes	filecreatetime
File Attributes	filemodificationtime
File Attributes	oldfilename
File Attributes	oldfilepath
File Attributes	oldfiletype
File Attributes	oldfilesize
File Attributes	oldfilehash

Type	Attribute
File Attributes	oldfilepermission
File Attributes	oldfilecreatetime
File Attributes	oldfileid
File Attributes	oldfilemodificationtime
Message	message
Message	transactionstring1
Message	transactionstring2
Message	transactionstring3
Message	transactionstring4
Message	transactionstring5
Message	transactionstring6
Message	transactionnumber1
Message	transactionnumber2
Message	transactionnumber3
Message	transactionnumber4
Message	transactionnumber5
Message	devicecustomstring1
Message	devicecustomstring2
Message	devicecustomstring3
Message	devicecustomstring4
Message	devicecustomstring5
Message	devicecustomstring6
Message	customstring1

Type	Attribute
Message	customstring2
Message	customstring3
Message	customnumber1
Message	customnumber2
Message	customnumber3
Message	devicecustomipv6address1
Message	devicecustomipv6address2
Message	devicecustomipv6address3
Message	devicecustomipv6address4
Message	devicecustomfloatingpoint1
Message	devicecustomfloatingpoint2
Message	devicecustomfloatingpoint3
Message	devicecustomfloatingpoint4
Message	devicecustomfloatingpoint1label
Message	devicecustomfloatingpoint2label2
Message	devicecustomfloatingpoint3label3
Message	devicecustomfloatingpoint4label4
Web or Traffic	bytesin
Web or Traffic	bytesout
Web or Traffic	transportprotocol
Web or Traffic	requesturl
Web or Traffic	requestclientapplication
Web or Traffic	requestcontext

Type	Attribute
Web or Traffic	requestmethod
Outcome & Categorization	eventoutcome
Outcome & Categorization	deviceaction
Outcome & Categorization	deviceeventcategory
Outcome & Categorization	categoryobject
Outcome & Categorization	categorybehavior
Outcome & Categorization	deviceseverity
Miscellaneous	others
Miscellaneous	eventcount
Miscellaneous	zone
Miscellaneous	classification
GEOLOCATION attributes for mapped Ip address	eventcountry
GEOLOCATION attributes for mapped Ip address	eventregion
GEOLOCATION attributes for mapped Ip address	eventcity
GEOLOCATION attributes for mapped Ip address	eventlatitude
GEOLOCATION attributes for mapped Ip address	eventlongitude
GEOLOCATION attributes for mapped Ip address	postalcode
GEOLOCATION attributes for source hostname	sourcehostnameecountry
GEOLOCATION attributes for source hostname	sourcehostnameregion
GEOLOCATION attributes for source hostname	sourcehostnameecity
GEOLOCATION attributes for source hostname	sourcehostnamelatitude
GEOLOCATION attributes for source hostname	sourcehostnamelongitude
GEOLOCATION attributes for source hostname	sourcehostnamepostalcode

Type	Attribute
GEOLOCATION attributes for destination hostname	destinationhostnameecountry
GEOLOCATION attributes for destination hostname	destinationhostnameregion
GEOLOCATION attributes for destination hostname	destinationhostnameecity
GEOLOCATION attributes for destination hostname	destinationhostnamelatitude
GEOLOCATION attributes for destination hostname	destinationhostnamelongitude
GEOLOCATION attributes for destination hostname	destinationhostnamepostalcode
GEOLOCATION attributes for resource hostname	resourcehostnameecountry
GEOLOCATION attributes for resource hostname	resourcehostnameregion
GEOLOCATION attributes for resource hostname	resourcehostnameecity
GEOLOCATION attributes for resource hostname	resourcehostnamelatitude
GEOLOCATION attributes for resource hostname	resourcehostnamelongitude
GEOLOCATION attributes for resource hostname	resourcehostnamepostalcode
GEOLOCATION attributes for device hostname	devicehostnameecountry
GEOLOCATION attributes for device hostname	devicehostnameregion
GEOLOCATION attributes for device hostname	devicehostnameecity
GEOLOCATION attributes for device hostname	devicehostnamelatitude
GEOLOCATION attributes for device hostname	devicehostnamelongitude
GEOLOCATION attributes for device hostname	devicehostnamepostalcode
TPI attributes	tpi_addr
TPI attributes	tpi_domain
TPI attributes	tpi_type
TPI attributes	tpi_src
TPI attributes	tpi_date

Type	Attribute
TPI attributes	tpi_text
TPI attributes	tpi_category
TPI attributes	tpi_reason
TPI attributes	tpi_description
TPI attributes	tpi_filename
TPI attributes	tpi_action
TPI attributes	tpi_criticality
TPI attributes	tpi_version
TPI attributes	tpi_malware
TPI attributes	tpi_risk
TPI attributes	tpi_recommendation
TPI attributes	tpi_resolution
TPI attributes	tpi_indicators

Appendix B: Functions

Functions

Functions are used to perform operations on attribute values. This section contains the available functions to populate attribute fields.

About Functions

Config Stored in DB

Config for operators is in resource attributes table. Below is the details of column used and their purpose:

- `operationclass` – Contains the class of the operator for the Predefine Operation. Eg `REPLACE,TO_UPPER,GELOCATION` etc
- `operationdata` – Stores data specific for the operation used. For Mathematical expression it contains function as it is. Eg $(attr1+attr2)^3$, $\tan(attr1/attr2)$. For predefined operations this stores pipe separated list of arguments. Eg `attr1 | "abc"` (This would be stored for concatenate function where we need to concatenate abc to attr1)
- `Operationtype` – Stores operationtype. This can be either `MATHEMATICAL_EXPRESSION` or `PREDEFINE_OPERATIONS`

Main Class Files

- `Attributeoperationconstants` – File which contains constants for activity operations
- `com.securonix.application.matcher.reader.operations.Operators` – File which should be extended by every predefined operation
- `com.securonix.application.matcher.reader.operations.*` -This package contains files for all predefined operations
- `Activityattributeoperationutil` – Util class which is used by activity import for applying operators

Case When Hadoop is Enabled

- `com.securonix.eventparser`
- `EventParser` - initialization for operators functionality for resourcegroupID
- `FilterConfiguration` `config = map.get(resourceGroupId)` - Get resource group configuration from the memory
- `config.operatorsinitialized` - If operator initialized then apply that operator on the attribute.
- `config.activityAttributeOperationUtil.execute` - Set/apply the value of attribute by executing the execute method for that operator

Workflow

- UI populates the data in columns specific to operators in resourceattribute table
- Activityattributeoperationutil.initialize method is called in starting of activity import. It loads the details regarding which operators are need to be applied
- Activityattributeoperationutil.execute method is called from generate chain. This method accepts a map of attributename to existing value from file. And returns the same map with new values after applying operators

Implementing a New Predefined Operator

Create a file which extends Operator class and implement the method process.

The following are the details of process method args:

- OldData – Map containing attributeName to values for this event.
- ParamValues – Every predefine operator takes as input one or more arguments. An argument can either be other attributename or some constant. Eg Concatenate(attr1,"abc"), here attr1 is attributename and "abc" is constant.
- Paramvalues contains a list of string in order of arguments specified in operator,wherein, value of attribute is replaced with its value for that specific event.
- AttributeToSet – attributeName on which this operator needs to be applied.

In the end, every operator should set the updated value in map for attributetToSet.

Tables used to Store Configuration

- resourceattributes

Logical Functions

Function	Operator Functionality	Parameters	Description	Example
IF_GREATER_OR_EQUAL	This implements the condition if (A>=B) then C else D .	4 pipe separated attributes/constants which are in order of A,B,C,D from the above description.	This implements the condition if(A>=B) then C else D . 4 pipe separated attributes/constants which are in order of A,B,C,D from the above description.	Attribute - Transaction (Criticality) Original value Transaction = 120 Apply operator : - IF_GREATER_OR_EQUAL (Transaction ""120"" ""MEDIUM"" ""LOW"") Result : - Transaction = OK
IF_THEN_ELSE	This implements the condition if (A.equals(B)) then C else D.(A and B are matched as string).	4 pipe separated attributes/constants which are in order of A,B,C,D from the above description.	This implements the condition if(A.equals(B)) then C else D.(A and B are matched as string). 4 pipe separated attributes/constants which are in order of A,B,C,D from the above description. E.g. : IF_THEN_ELSE (attr1 '100' 'OK' 'NOT OK')	Attribute - Transaction Original value Transaction = COMPLETED Apply operator : - IF_THEN_ELSE(Transaction ""COMPLETED"" ""OK"" - ""Not OK"") Result : - Transaction = OK

Function	Operator Functionality	Parameters	Description	Example
SIMPLE_MAP	This function replaces the value found on the basis of pre-configured values found from map.	List of pipe separated parameters, first parameter is attribute name whose value needs to be checked and updated. Others "=" separated key value pairs.	This function replaces the value found on the basis of preconfigured values found from map. List of pipe separated parameters, first parameter is attribute name whose value needs to be checked and updated. Others "=" separated key value pairs. E.g. : SIMPLE_MAP (attr1 'foo=100' 'bar=200')	Attribute - Transaction Original value Transaction = COMPLETED,TRIGGERED Apply operator : - SIMPLE_MAP(Transaction ""COMPLETED=Completed running"" ""TRIGGERED=In process"") Result : - Transaction = OK
SEVERITY_NUMERIC_RANGE	Severity is set according to the numeric range.	Two parameters first being the attribute name, second is a comma separated 4 specifying the range of severity. (order is LOW,MEDIUM,HIGH,VERY HIGH,CRITICAL)	Severity is set according to the numeric range. Two parameters first being the attribute name, second is a comma separated 4 specifying the range of severity. (order is LOW,MEDIUM,HIGH,VERY HIGH,CRITICAL) E.g. : SEVERITY_NUMERIC_RANGE (attr1 '100,200,300,400')	Attribute - Transaction Original value Transaction = 110 Apply operator : - SEVERITY_NUMERIC_RANGE(Transaction ""100,200,300,400"") Result : - Transaction = MEDIUM

Function	Operator Functionality	Parameters	Description	Example
SEVERITY_STRING_MATCHER	Severity is set according to the string encountered.	List of pipe separated parameters, first parameter is attribute name whose value needs to be checked and updated. Others "=" separated key value pairs (value can be multivalued separated by comma)	Severity is set according to the string encountered. List of pipe separated parameters, first parameter is attribute name whose value needs to be checked and updated. Others "=" separated key value pairs (value can be multivalued separated by comma) E.g. : SEVERITY_STRING_MATCHER (attr1 'HIGH=foo1,foo2' 'LOW=foo3')	" Attribute - Transaction Original value Transaction1 = 50 [ANOTHER VALUE = 120] Apply operator : - SEVERITY_STRING_MATCHER(Transaction 'HIGH=foo1,foo2' 'LOW=foo3') Result : - Transaction1 = LOW [ANOTHER VALUE = HIGH] "

Math Functions

Function	Operator Functionality	Parameters	Description	Example
SUM	Addition of all the given attributes/constants.	Pipe separated list of attributes and/or constants.	Addition of all the given attributes/constants. Pipe separated list of attributes and/or constants. E.g. : SUM(attr1 '100')	Attribute - Customstring1 Original value Customstring1 = 1234 Apply operator : - SUM(customstring1 '10000') Result : - Customstring1 = 11234

Function	Operator Functionality	Parameters	Description	Example
PRODUCT	Product of all the given attributes/constants.	Pipe separated list of attributes and/or constants.	Product of all the given attributes/constants. Pipe separated list of attributes and/or constants. E.g. : PRODUCT (attr1 '100')	Attribute - Customstring1 Original value Customstring1 = 1234 Apply operator : - PRODUCT (customstring1 ""10000"") Result : - Customstring1 = 12340000
SUBTRACT	Subtraction of all the given attributes/constants.	Pipe separated two attributes and/or constants.	Returns result for param1 - param2. Pipe separated two attributes and/or constants. E.g. : SUBTRACT (attr1 '100')	Attribute - Customstring1 Original value Customstring1 = 1234 Apply operator : - SUBTRACT (customstring1 ""1000"") Result : - Customstring1 = 234
DIVIDE	Division of all the given attributes/constants.	Pipe separated two attributes and/or constants.	Returns result for param1/param2. Pipe separated two attributes and/or constants. E.g. : DIVIDE(attr1 '10')	Attribute - Customstring1 Original value Customstring1 = 1234 Apply operator : - DIVIDE(customstring1 ""10"") Result : - Customstring1 = 12.34
GB_TO_KB	Operations are used for bytes conversion.	Only one parameter which is the attribute name of the parameter to convert.	Operations are used for bytes conversion. Only one parameter which is the attribute name of the parameter to convert. E.g. : GB_TO_KB(attr1)	Attribute - Transaction Original value Transaction in GB = 1 Apply operator : - GB_TO_KB (Transaction) Result : - Transaction in KB = 1000000

Function	Operator Functionality	Parameters	Description	Example
GB_TO_MB	Operations are used for bytes conversion.	Only one parameter which is the attribute name of the parameter to convert.	Operations are used for bytes conversion. Only one parameter which is the attribute name of the parameter to convert. E.g. : GB_TO_MB(attr1)	Attribute - Transaction Original value Transaction in GB = 1 Apply operator : - GB_TO_MB (Transaction) Result : - Transaction in MB = 1000
KB_TO_GB	Operations are used for bytes conversion.	Only one parameter which is the attribute name of the parameter to convert.	Operations are used for bytes conversion. Only one parameter which is the attribute name of the parameter to convert. E.g. : KB_TO_GB(attr1)	Attribute - Transaction Original value Transaction in KB = 1000000 Apply operator : - KB_TO_GB(Transaction) Result : - Transaction in GB = 1
KB_TO_MB	Operations are used for bytes conversion.	Only one parameter which is the attribute name of the parameter to convert.	Operations are used for bytes conversion. Only one parameter which is the attribute name of the parameter to convert. E.g. : KB_TO_MB(attr1)	Attribute - Transaction Original value Transaction in KB = 1000000 Apply operator : - KB_TO_MB(Transaction) Result : - Transaction in MB = 1000
MB_TO_KB	Operations are used for bytes conversion.	Only one parameter which is the attribute name of the parameter to convert.	Operations are used for bytes conversion. Only one parameter which is the attribute name of the parameter to convert. E.g. : MB_TO_KB(attr1)	Attribute - Transaction Original value Transaction in MB = 1000 Apply operator : - MB_TO_KB(Transaction) Result : - Transaction in KB = 1000000

Function	Operator Functionality	Parameters	Description	Example
MB_TO_GB	Operations are used for bytes conversion.	Only one parameter which is the attribute name of the parameter to convert.	Operations are used for bytes conversion. Only one parameter which is the attribute name of the parameter to convert. E.g. : MB_TO_GB(attr1)	Attribute - Transaction Original value Transaction in MB = 1000 Apply operator : - MB_TO_GB(Transaction) Result : - Transaction in GB = 1

Other Functions

Function	Operator Functionality	Parameters	Description	Example
DOUBLE_TO_IP	Converts the double number to IP Address.	Only one parameter which is the attribute name of the parameter to convert.	Converts the double number to IP_Address. Only one parameter which is the attribute name of the parameter to convert. E.g. :DOUBLE_TO_IP(attr1)	Attribute - Transaction Original value Transaction = 12345 Apply operator : - DOUBLE_TO_IP(Transaction) Result : - Transaction = 0.0.48.57
NS_LOOKUP	Get Hostname from Ipaddress.	Only one parameter which is the attribute name of the parameter to convert.	Get Hostname from Ipaddress. Only one parameter which is the attribute name of the parameter to convert.	NS_LOOKUP(attr1)

Function	Operator Functionality	Parameters	Description	Example
GEO_LOCATION	Get location name from the IP address.	Only one parameter which is the attribute name of the parameter to convert.	Get location name from the IP address. Only one parameter which is the attribute name of the parameter to convert.	GEO_LOCATION(attr1)
CORRELATED_USER	Gets the correlated user from the given field.	Only one parameter which is the attribute name of the parameter to convert.	Gets the correlated user from the given field. Only one parameter which is the attribute name of the parameter to convert.	CORRELATED_USER (attr1)

Function	Operator Functionality	Parameters	Description	Example
DOMAIN_CATEGORIZER	Checks for a domain in a core and returns given value if found.	It takes 3 params. First core-name (from securonix_home/solr folder), Second is field-name value of which should be checked in core, Third being value to return if domain is found in core.	Checks for a domain in a core and returns given value if found. It takes 3 params. First corename (from securonix_home/solr folder), Second is fieldname value of which should be checked in core, Third being value to return if domain is found in core. E.g. : DOMAIN_CATEGORIZER ('tpiCategoryDomainUrl',nwaddr,'Spam Email')	DOMAIN_CATEGORIZER ('tpiCategoryDomainUrl',nwaddr,'Spam Email')

Function	Operator Functionality	Parameters	Description	Example
TIME_CATEGORIZER	Checks given attribute against given time range and returns mapped value if found.	First field is attribute name, next fields are label and time range mappings separated by "=".	Checks given attribute against given time range and returns mapped value if found. First field is attribute name, next fields are label and time range mappings separated by '='. E.g. : TIME_CATEGORIZER (time 'Morning Shift=09:00:00-14:00:00' 'Evening Shift=15:00:00-20:00:00')	TIME_CATEGORIZER (time "Morning Shift-t=09:00:00-14:00:00" "Evening Shift=15:00:00-20:00:00")
EPOCHTIME_TO_DATE	Converts the epoch time to human readable date format.	Only one parameter is required which is the epoch time.	Converts the epoch time to human readable date format. Only one parameter is required which is the epoch time. For example : If epoch time is 1439923678000 then it will be converted into 08/18/2015 13:47:58	If epoch time is 1439923678000 then it will be converted into 08/18/2015 13:47:58

Function	Operator Functionality	Parameters	Description	Example
QUANTIFIED_DOMAIN_NAME	Extracts the CN field (Common Name) from quantified domain name.	Only one parameter which is the attribute name of the parameter to convert.	Extracts the CN field (Common Name) from quantified domain name. For example, if quantified domain name is CN=Demetria Bridges,CN=N=Users,DC=identric,DC=com extracted CN will become Demetria Bridges	if quantified domain name is CN=Demetria Bridges,CN=Users,DC=identric,DC=com extracted CN will become Demetria Bridges
QUERY	Execute the SQL statement	Only one parameter which is the attribute name of the parameter.	resource.activityAttribute.operator.func.QUERY	

String Functions

Function	Operator Functionality	Parameters	Description	Example
TO_UPPER	Converts the string read to upper case.	Takes only one parameter i.e. the attribute name on which the action is to be applied.	Converts the string read to upper case. Only one parameter which is the attribute name of the parameter to convert. E.g. : TO_UPPER(attr1)	Attribute - Transaction Original value Action = ""triggered"" Apply operator : - TO_UPPER(Transaction) Result : - Action = ""TRIGGERED""
TO_LOWER	Converts the string read to lower case.	Takes only one parameter i.e. the attribute name on which the action is to be applied.	Converts the string read to lower case. Only one parameter which is the attribute name of the parameter to convert. E.g. : TO_LOWER(attr1)	Attribute - Transaction Original value Action = ""TRIGGERED"" Apply operator : - TO_LOWER(Transaction) Result : - Action = ""triggered""
CONCATENATE	Concatenate the list attributes or constant.	Takes pipe separated list of attributes and/or constants.	Concatenate the list attributes or constant. Pipe separated list of attributes and/or constants. E.g. : CONCATENATE(attr1 "abc" attr3)	Attribute - Transaction Original value Action = ""TRIGGERED"" Apply operator : - TO_LOWER(Transaction) Result : - Action = ""triggered""

Function	Operator Functionality	Parameters	Description	Example
CONSTANT	Replaces the destination attribute to a given constant.	Takes single parameter.	Replaces the destination attribute to a given constant. E.g. : CONSTANT ('abc')	Attribute - Transaction Original value Action = ""TRIGGERED"" Constant value = ""COMPLETED"" Apply operator : - CONSTANT(Transaction) Result : - Action = ""COMPLETED""
TRIM	Trims the given attribute.	Only one parameter which is the attribute name of the parameter to convert	Trims the given attribute. Only one parameter which is the attribute name of the parameter to convert. E.g. : TRIM(attr1)	Attribute - Transaction Original value Action = ""TRIGGERED"" Apply operator : - TRIM(Transaction) Result : - Action = ""TRIGGERED""
REGEX_TOKEN	Returns the first token match for the given string.	Two parameter first being the attribute name and second being the regex token.	Returns the first token match for the given string. Two parameter first being the attribute name and second being the regex token. E.g. : REGEX_TOKEN(attr1 "fo+(o.)*(r)")	REGEX_TOKEN(field field)

Function	Operator Functionality	Parameters	Description	Example
TOP_LEVEL_DOMAIN	Extracts the top level domain of any url	Only one parameter which contains the hostname.	Extracts the top level domain of any URL. Only one parameter which contains the hostname. E.g. TOP_LEVEL_DOMAIN(attr1)	Attribute - Transaction Original value Action = ""xyz@securonix.com"" Apply operator : - TOP_LEVEL_DOMAIN(Transaction) Result : - com
FILE_EXTENSION_EXTRACTOR	Get file extension. (c:/temp/test.txt returns txt)	Only one parameter which is the attribute name of the parameter to convert.	Get file extension.(c:/temp/test.txt returns txt) Only one parameter which is the attribute name of the parameter to convert. E.g. : FILE_EXTENSION_EXTRACTOR(attr1)	Attribute - Transaction Original value Action = ""C:/temp/test.txt"" Apply operator : - FILE_EXTENSION_EXTRACTOR(Transaction) Result : - Transaction = ""txt""
FILE_NAME_EXTRACTOR	Get file name. (c:/temp/test.txt returns test).	Only one parameter which is the attribute name of the parameter to convert.	Get file name.(c:/temp/test.txt returns test). Only one parameter which is the attribute name of the parameter to convert. E.g. : FILE_NAME_EXTRACTOR(attr1)	Attribute - Transaction Original value Action = ""C:/temp/test.txt"" Apply operator : - FILE_NAME_EXTRACTOR(Transaction) Result : - Transaction = ""test""

Function	Operator Functionality	Parameters	Description	Example
FILE_PATH_EXTRACTOR	Get file path. (c:/temp/test.txt returns c:/temp)	Only one parameter which is the attribute name of the parameter to convert.	Get file path.(c:/temp/test.txt returns c:/temp) Only one parameter which is the attribute name of the parameter to convert. E.g. : FILE_PATH_EXTRACTOR(attr1)	Attribute - Transaction Original value Action = "C:/temp/test.txt" Apply operator : - FILE_PATH_EXTRACTOR (Transaction) Result : - Transaction = "C:/temp"
LENGTH	Replaces the destination attribute to the length of given attribute.	Only one parameter which is the attribute name of the parameter to convert.	Replaces the destination attribute to the length of given attribute. Only one parameter which is the attribute name of the parameter to convert. E.g. : LENGTH(attr1)	Attribute - Transaction Original value Action = "triggered" Apply operator : - LENGTH(Transaction) Result : - 9
HASH	Gets the hash of the value.	Only one parameter which is the attribute name of the parameter to convert.	Returns a unique hash value Example: HASH (email)	Attribute - Transaction Original value Action = "www.securonix.com" Apply operator : - HASH (Transaction) Result : - 1533434266 (Hash value returned)

Function	Operator Functionality	Parameters	Description	Example
REPLACE	Replace a value find in attribute with different string	Replace can have 3 or more params. first param being the attribute, second being the value to replace with other params are for values to replace.	Replace a value find in attribute with different string. Replace can have 3 or more params. first param being the attribute, second being the value to replace with other params are for values to replace. E.g. : REPLACE(transaction, 'command=', 'args=')	Attribute - IPAddress Original value = ""10.78.2.242"" Replace with = ""1.1.1.1"" Apply operator : - REPLACE (IPAd- dress ""10.78.2.242"" ""1.1.1.1"") Result : - IPAddress = ""1.1.1.1""
EXTRACT_EMAIL_DOMAIN	Used to extract the email domain.	Only one parameter which is the attribute name of the parameter to convert.	Extract domain name from email. Example: EXTRACT_EMAIL_DOMAIN(email)	Attribute - Transaction Original value Action = ""xyz@securonix.com"" Apply operator : - EXTRACT_EMAIL_DOMAIN (Transaction) Result : - securonix.com

Function	Operator Functionality	Parameters	Description	Example
USER_ENVIRONMENT_DETAILS	Gives the information about the browser, browser version and OS and if not found returns NA.		Extracts user environment details using User Agent Utils. For example, USER_ENVIRONMENT_DETAILS(user-AgentString,'BROWSER') Will extract browser details of user. You can extract BROWSER,BROWSER_VERSION and OPERATING_SYSTEM are supported.	USER_ENVIRONMENT_DETAILS(field field)

Formula

Function	Operator Functionality	Parameters	Description	Example
Exp			Exponent	
Abs			Absolute value	
ASin			Inverse sine	
Tan	Returns logarithm of given number		Tangent function	"Attribute - Transaction Original value Action = 45 Apply operator : - Tan(Transaction) * 1000 Result : - Action = 1000"
Sqrt	Returns logarithm of given number		Square root	"Attribute - Transaction Original value Action = 4 Apply operator : - Sqrt(Transaction) * 1000 Result : - Action = 2000"
ATan			Inverse tangent	

Function	Operator Functionality	Parameters	Description	Example
ACos			Inverse cosine	
Log10			Log Base 10	
Log	Returns logarithm of given number		Natural logarithm for a specific float expression	"Attribute - Transaction Original value Action = 2 Apply operator : - Log(Transaction) * 1000 Result : - Action = 301.02"
Π			Inserts pi	
Factorial			Product of an integer and all the integers below (ex. $4! = 1 \times 2 \times 3 \times 4 = 24$)	
Cos			Cosine function	
Sin			Sine function	
e			Exponential	
<			Less than	
>			Greater than	
&			And	
			pipe	
,			Comma	
!			Indicates factorial	
(Starting parenthesis	
)			Ending parenthesis	
/			Divide	
%			Percent	

Function	Operator Functionality	Parameters	Description	Example
*			Multiply	
"			Enclose specific text values	
-			Subtract	
^			Raise to the power of	
+			Add	
=			Equals	

Appendix C: Verbose Template Attributes

You can select custom attributes to populate the violation summary for a policy. Example: Account `${accountname!"ACCOUNTNAME"}` performed `${transactionstring1!"ACTIVITY"}` from ipaddress `${customerid!"UNKNOWN"}`.

Type	Attribute
Event	\${eventid!"Unknown"}
Event	\${eventtime!"Unknown"}
Event	\${jobid!"Unknown"}
Event	\${jobstarttime!"Unknown"}
Event	\${accountname!"Unknown"}
Event	\${invalidEventAction!"Unknown"}
Event	\${directImport!"Unknown"}
Event	\${year!"Unknown"}
Event	\${week!"Unknown"}
Event	\${month!"Unknown"}
Event	\${dayofyear!"Unknown"}
Event	\${dayofweek!"Unknown"}
Event	\${dayofmonth!"Unknown"}
Event	\${hour!"Unknown"}
Event	\${minute!"Unknown"}
Event	\${tenantid!"Unknown"}
Event	\${tenantname!"Unknown"}
Event	\${ingestionnodeid!"Unknown"}
Event	\${collectionmethod!"Unknown"}
Event	\${collectiontimestamp!"Unknown"}
Event	\${encrypted!"Unknown"}
Event	\${mediatype!"Unknown"}
Event	\${customfield1!"Unknown"}

Type	Attribute
Event	\${customfield2!"Unknown"}
Event	\${customfield3!"Unknown"}
Event	\${tenantTz!"Unknown"}
Event	\${rawevent!"Unknown"}
Event	\${invalid!"Unknown"}
Event	\${errormessage!"Unknown"}
Event	\${ignored!"Unknown"}
Event	\${u_id!"Unknown"}
Event	\${u_employeeid!"Unknown"}
Event	\${u_firstname!"Unknown"}
Event	\${u_middlename!"Unknown"}
Event	\${u_lastname!"Unknown"}
Event	\${u_department!"Unknown"}
Event	\${u_division!"Unknown"}
Event	\${u_location!"Unknown"}
Event	\${u_manageremployeeid!"Unknown"}
Event	\${u_workemail!"Unknown"}
Event	\${u_workphone!"Unknown"}
Event	\${u_title!"Unknown"}
Event	\${u_employeetype!"Unknown"}
Event	\${u_status!"Unknown"}
Event	\${u_uniquecode!"Unknown"}
Event	\${u_riskscore!"Unknown"}

Type	Attribute
Event	\$_customfield1!"Unknown"}
Event	\$_customfield2!"Unknown"}
Event	\$_customfield3!"Unknown"}
Event	\$_customfield4!"Unknown"}
Event	\$_customfield5!"Unknown"}
Event	\$_customfield6!"Unknown"}
Event	\$_customfield7!"Unknown"}
Event	\$_customfield8!"Unknown"}
Event	\$_customfield9!"Unknown"}
Event	\$_customfield10!"Unknown"}
Event	\$_customfield11!"Unknown"}
Event	\$_customfield12!"Unknown"}
Event	\$_customfield13!"Unknown"}
Event	\$_customfield14!"Unknown"}
Event	\$_customfield15!"Unknown"}
Event	\$_customfield16!"Unknown"}
Event	\$_customfield17!"Unknown"}
Event	\$_customfield18!"Unknown"}
Event	\$_customfield19!"Unknown"}
Event	\$_customfield20!"Unknown"}
Event	\$_customfield21!"Unknown"}
Event	\$_customfield22!"Unknown"}
Event	\$_customfield23!"Unknown"}

Type	Attribute
Event	`\${u_customfield24}!Unknown`
Event	`\${u_customfield25}!Unknown`
Event	`\${u_customfield26}!Unknown`
Event	`\${u_customfield27}!Unknown`
Event	`\${u_customfield28}!Unknown`
Event	`\${u_customfield29}!Unknown`
Event	`\${u_customfield30}!Unknown`
Event	`\${u_promoted}!Unknown`
Event	`\${u_createdate}!Unknown`
Event	`\${u_usergroup}!Unknown`
Event	`\${u_street}!Unknown`
Event	`\${u_city}!Unknown`
Event	`\${u_province}!Unknown`
Event	`\${u_zipcode}!Unknown`
Event	`\${u_userstate}!Unknown`
Event	`\${u_region}!Unknown`
Event	`\${u_country}!Unknown`
Event	`\${u_approveremployeeid}!Unknown`
Event	`\${u_delegateemployeeid}!Unknown`
Event	`\${u_technicalapproverid}!Unknown`
Event	`\${u_extension}!Unknown`
Event	`\${u_fax}!Unknown`
Event	`\${u_mobile}!Unknown`

Type	Attribute
Event	`\${u_pager! "Unknown"}`
Event	`\${u_jobcode! "Unknown"}`
Event	`\${u_comments! "Unknown"}`
Event	`\${u_createdby! "Unknown"}`
Event	`\${u_costcentername! "Unknown"}`
Event	`\${u_costcentercode! "Unknown"}`
Event	`\${u_enabledate! "Unknown"}`
Event	`\${u_disabledate! "Unknown"}`
Event	`\${u_deletedate! "Unknown"}`
Event	`\${u_updatedate! "Unknown"}`
Event	`\${u_sunrisedate! "Unknown"}`
Event	`\${u_sunsetdate! "Unknown"}`
Event	`\${u_criticality! "Unknown"}`
Event	`\${u_domintlin! "Unknown"}`
Event	`\${u_nameprefix! "Unknown"}`
Event	`\${u_namesuffix! "Unknown"}`
Event	`\${u_preferredname! "Unknown"}`
Event	`\${u_secondaryphone! "Unknown"}`
Event	`\${u_statusdescription! "Unknown"}`
Event	`\${u_vacationstart! "Unknown"}`
Event	`\${u_vacationend! "Unknown"}`
Event	`\${u_networkid! "Unknown"}`
Event	`\${u_workpager! "Unknown"}`

Type	Attribute
Event	`\${u_workextensionnumber}!Unknown`
Event	`\${u_workfax}!Unknown`
Event	`\${u_employeestatuscode}!Unknown`
Event	`\${u_locationcode}!Unknown`
Event	`\${u_locationname}!Unknown`
Event	`\${u_mailcode}!Unknown`
Event	`\${u_hiredate}!Unknown`
Event	`\${u_rehiredate}!Unknown`
Event	`\${u_recenthiredate}!Unknown`
Event	`\${u_terminationdate}!Unknown`
Event	`\${u_lastdayworked}!Unknown`
Event	`\${u_contractstartdate}!Unknown`
Event	`\${u_contractenddate}!Unknown`
Event	`\${u_employeetypedescription}!Unknown`
Event	`\${u_regtempin}!Unknown`
Event	`\${u_fulltimeparttimein}!Unknown`
Event	`\${u_managerfirstname}!Unknown`
Event	`\${u_managerlastname}!Unknown`
Event	`\${u_managemiddlename}!Unknown`
Event	`\${u_orgunitnumber}!Unknown`
Event	`\${u_companycode}!Unknown`
Event	`\${u_companynumber}!Unknown`
Event	`\${u_hierarchy}!Unknown`

Type	Attribute
Event	`\${u_lastperformancereviewdate! "Unknown"}`
Event	`\${u_lastperformancereviewresult! "Unknown"}`
Event	`\${u_standardhours! "Unknown"}`
Event	`\${u_shiftcode! "Unknown"}`
Event	`\${u_shiftname! "Unknown"}`
Event	`\${u_lanid! "Unknown"}`
Event	`\${u_userid! "Unknown"}`
Event	`\${u_transferreddate! "Unknown"}`
Event	`\${u_datasourceid! "Unknown"}`
Event	`\${u_timezoneoffset! "Unknown"}`
Event	`\${u_encrypted! "Unknown"}`
Event	`\${u_encryptedfields! "Unknown"}`
Event	`\${u_maskedfields! "Unknown"}`
Event	`\${u_masked! "Unknown"}`
Event	`\${u_lastsynctime! "Unknown"}`
Event	`\${u_mergeuniquecode! "Unknown"}`
Event	`\${u_skipencryption! "Unknown"}`
Resource Group	`\${rg_id! "Unknown"}`
Resource Group	`\${rg_name! "Unknown"}`
Resource Group	`\${rg_type! "Unknown"}`
Resource Group	`\${rg_vendor! "Unknown"}`
Resource Group	`\${rg_functionality! "Unknown"}`
Resource Group	`\${rg_ownerid! "Unknown"}`

Type	Attribute
Resource Group	`\${rg_riskscore! "Unknown"}`
Resource Group	`\${rg_criticality! "Unknown"}`
Resource Group	`\${rg_deviceid! "Unknown"}`
Resource Group	`\${rg_timezoneoffset! "Unknown"}`
Resource Group	`\${rg_aggregatelevel! "Unknown"}`
Resource Group	`\${rg_resourcetypeid! "Unknown"}`
Resource Group	`\${rg_clusterid! "Unknown"}`
Resource Group	`\${rg_ipaddress! "Unknown"}`
Resource Group	`\${rg_category! "Unknown"}`
Resource Group	`\${rg_amountroundupvalue! "Unknown"}`
Resource Group	`\${rg_syslogenabled! "Unknown"}`
Resource Group	`\${rg_syslogport! "Unknown"}`
Resource Group	`\${rg_customerid! "Unknown"}`
Resource Group	`\${rg_parentstatus! "Unknown"}`
Resource Group	`\${rg_parentid! "Unknown"}`
Resource Group	`\${rg_retainedaccessentitlements! "Unknown"}`
Mapped	`\${resourcename! "Unknown"}`
Mapped	`\${resourcetype! "Unknown"}`
Mapped	`\${ipaddress! "Unknown"}`
Mapped	`\${others! "Unknown"}`
Mapped	`\${eventcount! "Unknown"}`
Mapped	`\${siemid! "Unknown"}`
Mapped	`\${flowsiemid! "Unknown"}`

Type	Attribute
Mapped	\${alertid!"Unknown"}
Mapped	\${applicationprotocol!"Unknown"}
Mapped	\${destinationhostname!"Unknown"}
Mapped	\${destinationprocessid!"Unknown"}
Mapped	\${destinationmacaddress!"Unknown"}
Mapped	\${destinationntdomain!"Unknown"}
Mapped	\${destinationuserprivileges!"Unknown"}
Mapped	\${destinationprocessname!"Unknown"}
Mapped	\${destinationport!"Unknown"}
Mapped	\${destinationaddress!"Unknown"}
Mapped	\${destinationuserid!"Unknown"}
Mapped	\${destinationusername!"Unknown"}
Mapped	\${deviceaction!"Unknown"}
Mapped	\${deviceeventcategory!"Unknown"}
Mapped	\${deviceaddress!"Unknown"}
Mapped	\${devicehostname!"Unknown"}
Mapped	\${deviceprocessid!"Unknown"}
Mapped	\${filename!"Unknown"}
Mapped	\${filesize!"Unknown"}
Mapped	\${bytesin!"Unknown"}
Mapped	\${bytesout!"Unknown"}
Mapped	\${message!"Unknown"}
Mapped	\${eventoutcome!"Unknown"}

Type	Attribute
Mapped	\${transportprotocol!"Unknown"}
Mapped	\${requesturl!"Unknown"}
Mapped	\${sourcehostname!"Unknown"}
Mapped	\${sourcemacaddress!"Unknown"}
Mapped	\${sourcentdomain!"Unknown"}
Mapped	\${sourceprocessid!"Unknown"}
Mapped	\${sourceprocessname!"Unknown"}
Mapped	\${sourceport!"Unknown"}
Mapped	\${sourceuserprivileges!"Unknown"}
Mapped	\${sourceaddress!"Unknown"}
Mapped	\${transactionstring1!"Unknown"}
Mapped	\${transactionstring2!"Unknown"}
Mapped	\${transactionstring3!"Unknown"}
Mapped	\${transactionstring4!"Unknown"}
Mapped	\${transactionstring5!"Unknown"}
Mapped	\${transactionstring6!"Unknown"}
Mapped	\${categoryobject!"Unknown"}
Mapped	\${categorybehavior!"Unknown"}
Mapped	\${categorizedtime!"Unknown"}
Mapped	\${transactionnumber1!"Unknown"}
Mapped	\${transactionnumber2!"Unknown"}
Mapped	\${transactionnumber3!"Unknown"}
Mapped	\${transactionnumber4!"Unknown"}

Type	Attribute
Mapped	\${transactionnumber5!"Unknown"}
Mapped	\${baseeventid!"Unknown"}
Mapped	\${baseeventcount!"Unknown"}
Mapped	\${destinationdnsdomain!"Unknown"}
Mapped	\${deviceinboundinterface!"Unknown"}
Mapped	\${deviceoutboundinterface!"Unknown"}
Mapped	\${deviceprocessname!"Unknown"}
Mapped	\${deviceseverity!"Unknown"}
Mapped	\${emailsubject!"Unknown"}
Mapped	\${emailsender!"Unknown"}
Mapped	\${emailsenderdomain!"Unknown"}
Mapped	\${emailrecipient!"Unknown"}
Mapped	\${emailrecipientdomain!"Unknown"}
Mapped	\${emailrecipienttype!"Unknown"}
Mapped	\${filecreatetime!"Unknown"}
Mapped	\${filemodificationtime!"Unknown"}
Mapped	\${filepath!"Unknown"}
Mapped	\${filetype!"Unknown"}
Mapped	\${oldfilename!"Unknown"}
Mapped	\${oldfilepath!"Unknown"}
Mapped	\${oldfilesize!"Unknown"}
Mapped	\${oldfiletype!"Unknown"}
Mapped	\${requestclientapplication!"Unknown"}

Type	Attribute
Mapped	\${requestcontext!"Unknown"}
Mapped	\${requestmethod!"Unknown"}
Mapped	\${translatedipaddress!"Unknown"}
Mapped	\${translatedport!"Unknown"}
Mapped	\${sessionid!"Unknown"}
Mapped	\${customstring1!"Unknown"}
Mapped	\${customstring2!"Unknown"}
Mapped	\${customstring3!"Unknown"}
Mapped	\${customnumber1!"Unknown"}
Mapped	\${customnumber2!"Unknown"}
Mapped	\${customnumber3!"Unknown"}
Mapped	\${resourcecomments!"Unknown"}
Mapped	\${resourcecustomfield1!"Unknown"}
Mapped	\${resourcecustomfield2!"Unknown"}
Mapped	\${resourcecustomfield3!"Unknown"}
Mapped	\${resourcecustomfield4!"Unknown"}
Mapped	\${resourcecustomfield5!"Unknown"}
Mapped	\${resourcecustomfield6!"Unknown"}
Mapped	\${resourcecustomfield7!"Unknown"}
Mapped	\${resourcecustomfield8!"Unknown"}
Mapped	\${resourcehierarchy!"Unknown"}
Mapped	\${resourcehierarchyname!"Unknown"}
Mapped	\${resourcestatus!"Unknown"}

Type	Attribute
Mapped	\${resourcehostname!"Unknown"}
Mapped	\${zone!"Unknown"}
Mapped	\${classification!"Unknown"}
Geolocation for mapped IP address	\${eventcountry!"Unknown"}
Geolocation for mapped IP address	\${eventregion!"Unknown"}
Geolocation for mapped IP address	\${eventcity!"Unknown"}
Geolocation for mapped IP address	\${eventlatitude!"Unknown"}
Geolocation for mapped IP address	\${eventlongitude!"Unknown"}
Geolocation for mapped IP address	\${postalcode!"Unknown"}
Geolocation for source hostname	\${sourcehostnameecountry!"Unknown"}
Geolocation for source hostname	\${sourcehostnameregion!"Unknown"}
Geolocation for source hostname	\${sourcehostnameecity!"Unknown"}
Geolocation for source hostname	\${sourcehostnamelatititude!"Unknown"}
Geolocation for source hostname	\${sourcehostnamelongitude!"Unknown"}
Geolocation for source hostname	\${sourcehostnameepostalcode!"Unknown"}
Geolocation for destination hostname	\${destinationhostnameecountry!"Unknown"}
Geolocation for destination hostname	\${destinationhostnameregion!"Unknown"}
Geolocation for destination hostname	\${destinationhostnameecity!"Unknown"}
Geolocation for destination hostname	\${destinationhostnamelatititude!"Unknown"}
Geolocation for destination hostname	\${destinationhostnamelongitude!"Unknown"}
Geolocation for destination hostname	\${destinationhostnameepostalcode!"Unknown"}
Geolocation for resource hostname	\${resourcehostnameecountry!"Unknown"}
Geolocation for resource hostname	\${resourcehostnameregion!"Unknown"}

Type	Attribute
Geolocation for resource hostname	\${resourcehostnameecity!"Unknown"}
Geolocation for resource hostname	\${resourcehostnamelatititude!"Unknown"}
Geolocation for resource hostname	\${resourcehostnamelongitude!"Unknown"}
Geolocation for resource hostname	\${resourcehostnamepostalcode!"Unknown"}
Geolocation for device hostname	\${devicehostnameecountry!"Unknown"}
Geolocation for device hostname	\${devicehostnameregion!"Unknown"}
Geolocation for device hostname	\${devicehostnameecity!"Unknown"}
Geolocation for device hostname	\${devicehostnamelatititude!"Unknown"}
Geolocation for device hostname	\${devicehostnamelongitude!"Unknown"}
Geolocation for device hostname	\${devicehostnamepostalcode!"Unknown"}
Geolocation for device hostname	
Geolocation for device hostname	
TPI	\${tpi_addr!"Unknown"}
TPI	\${tpi_domain!"Unknown"}
TPI	\${tpi_type!"Unknown"}
TPI	\${tpi_src!"Unknown"}
TPI	\${tpi_date!"Unknown"}
TPI	\${tpi_text!"Unknown"}
TPI	\${tpi_category!"Unknown"}
TPI	\${tpi_reason!"Unknown"}
TPI	\${tpi_description!"Unknown"}
TPI	\${tpi_filename!"Unknown"}
TPI	\${tpi_action!"Unknown"}

Type	Attribute
TPI	\${tpi_criticality!"Unknown"}
TPI	\${tpi_version!"Unknown"}
TPI	\${tpi_malware!"Unknown"}
TPI	\${tpi_risk!"Unknown"}
TPI	\${tpi_recommendation!"Unknown"}
TPI	\${tpi_resolution!"Unknown"}
TPI	\${tpi_indicators!"Unknown"}
Account	\${accountcriticality!"Unknown"}
Account	\${accounttype!"Unknown"}
Account	\${accountcreateddate!"Unknown"}
Account	\${accountdisableddate!"Unknown"}
Account	\${accountwhitelisted!"Unknown"}
Account	\${accountblacklisted!"Unknown"}
Account	\${accountencrypted!"Unknown"}
Account	\${accountowner!"Unknown"}
Account	\${accountstatus!"Unknown"}
Account	\${devicecustomipv6address1!"Unknown"}
Account	\${devicecustomipv6address2!"Unknown"}
Account	\${devicecustomipv6address3!"Unknown"}
Account	\${devicecustomipv6address4!"Unknown"}
Account	\${devicecustomfloatingpoint1!"Unknown"}
Account	\${devicecustomfloatingpoint2!"Unknown"}
Account	\${devicecustomfloatingpoint3!"Unknown"}

Type	Attribute
Account	\${devicecustomfloatingpoint4!"Unknown"}
Account	\${devicecustomfloatingpoint1label!"Unknown"}
Account	\${devicecustomfloatingpoint2label2!"Unknown"}
Account	\${devicecustomfloatingpoint3label3!"Unknown"}
Account	\${devicecustomfloatingpoint4label4!"Unknown"}
Account	\${devicecustomstring1!"Unknown"}
Account	\${devicecustomstring2!"Unknown"}
Account	\${devicecustomstring3!"Unknown"}
Account	\${devicecustomstring4!"Unknown"}
Account	\${devicecustomstring5!"Unknown"}
Account	\${devicecustomstring6!"Unknown"}
Account	\${endtime!"Unknown"}
Account	\${starttime!"Unknown"}
Account	\${sourceuserid!"Unknown"}
Account	\${sourceusername!"Unknown"}
Account	\${destinationservername!"Unknown"}
Account	\${destinationtranslatedaddress!"Unknown"}
Account	\${destinationtranslatedport!"Unknown"}
Account	\${devicecustomdate1!"Unknown"}
Account	\${devicecustomdate2!"Unknown"}
Account	\${devicedirection!"Unknown"}
Account	\${devicednsdomain!"Unknown"}
Account	\${deviceexternalid!"Unknown"}

Type	Attribute
Account	\${devicefacility!"Unknown"}
Account	\${devicemacaddress!"Unknown"}
Account	\${devicentdomain!"Unknown"}
Account	\${filehash!"Unknown"}
Account	\${filepermission!"Unknown"}
Account	\${oldfilecreatetime!"Unknown"}
Account	\${oldfilehash!"Unknown"}
Account	\${oldfileid!"Unknown"}
Account	\${oldfilemodificationtime!"Unknown"}
Account	\${oldfilepermission!"Unknown"}
Account	\${sourcednsdomain!"Unknown"}
Account	\${sourceservicename!"Unknown"}

Appendix D: Access Privileges

In Access Control, you can grant specific access privileges to each user role. These areas include the following:

- Dashboard
- View
- Add Data
- Analytics
- Reports
- Configure
- Third Party Intelligence
- Other
- Application Status
- Geolocation
- Investigation Workbench

Privileges are grouped based on the module (i.e. dashboard, manage, detect, respond, reports, and configure). The complete list of privileges is displayed in the following table:

Category	URL	ID	Description
Add Data	/config/licenseSuccessSettings	369-7	Configuration-License Success Settings
Add Data	/users/showScheduleImportJob	185-6	Configure-Tasks-User Import[shows user import screen]
Add Data	/users/showUserJobStatusDetails	185-5	Configure-Tasks [shows details of user import job]
Add Data	/users/saveConfig	185-4	Configure-Tasks-Configure User Import[saves values for user import config received from user import config screen]
Add Data	/users/showImportConfig	185-3	Configure-Tasks-Configure User Import[shows user import config screen]
Add Data	/resource/updateActivityAttributeDisplayOrder	439-4	Resource-Update Activity Attribute Display Order
Add Data	/resource/showResourceGroupsForNode	439-3	Resource Groups For Node
Add Data	/resource/isAccessValueDuplicate	439-2	Resource-Check if Access Value is Duplicate

Category	URL	ID	Description
Add Data	/resource/saveConfigTemplate	439-1	Resource-Save Configuration Template
Add Data	/users/importUsers	185-7	Configure-Tasks-User Import[import users from specified datasource]
Add Data	/resource/getNitroWSDeviceList	439-0	Resource-Get Nitro WS Device List
Add Data	/watchList/listActivityTransactionNotInWatchlist	450-5	Watchlist-List of Activity Transactions Not in Watchlist
Add Data	/users	450-3	Users
Add Data	/resource/toggleSuspectchecksFlag	436-5	Resource-Toggle Suspectchecks Flag
Add Data	/resource/previewActivityCorrelationResults	442-0	Resource-Preview Activity Correlation Results
Add Data	/resource/updateAccountAttributes	441-8	Resource-Update Account Attributes
Add Data	/resource/showEditActivityUserFilter	441-7	Resource-Show Edit Activity User Filter

Category	URL	ID	Description
Add Data	/resource/showUncorrelatedAccountsWithAccessValue	441-6	Resource-Show Uncorrelated Accounts With Access Value
Add Data	/resource/showCorrelatedResults	441-5	Resource-Show Correlated Results
Add Data	/resource/showCorrelatedActivityAccountsUsage	438-9	Resource-Show Correlated Activity Accounts Usage
Add Data	/resource/saveActionFilters	441-4	Resource-Save Action Filter
Add Data	/peer/showCreationRules	186-8	Manage-Peers- Peer Creation Rules
Add Data	/peer/showJobForAssignmentRules	188-4	Manage-Peers- Peer Assignment Rules[shows list of peer assignment rules job]
Add Data	/resource/addReport	437-6	Resource-Add Report
Add Data	/resource/showBehaviorConfig	437-5	Resource-Show Behavior Con- figuration
Add Data	/resource/showAddResourceGlossary	437-4	Show Add Resource Gloss- ary
Add Data	/resource/updateGlossary	437-3	Resource-Update Glossary
Add Data	/resource/saveResourceGroupList	437-2	Save Resource Group List

Category	URL	ID	Description
Add Data	/resource/showJobsForAccess	437-1	Resource-Show Jobs For Access
Add Data	/resource/getDeviceList	437-0	Resource-Get Device List
Add Data	/resource/	436-9	Resource
Add Data	/peer/showJobForCreationRules	186-9	Manage-Peers-Peer Creation Rules[shows list of peer creation rules job]
Add Data	/resource/searchAJAX	436-8	Resource-Search using AJAX
Add Data	/resource/searchActivityAccountsAJAX	438-6	Resource-Search Activity Accounts using AJAX
Add Data	/users/showUserRiskDetails	444-2	Users-Show User Risk Details
Add Data	/resource/saveGlossaryImportConfig	192-0	Configure-Tasks-Configure Glossary Import[save values recieved from configure glossary import screen]
Add Data	/resource/isResourceAccessAttributeNameDuplicate	438-8	Check if Resource Access Attribute Name is Duplicate

Category	URL	ID	Description
Add Data	/resource/saveAccessImportConfig	191-8	Configure-Tasks-Configure Access Import[save values recieved from configure access import screen]
Add Data	/resource/resourceAccessConfig	191-7	Configure-Tasks-Configure Access Import[shows configure access import screen]
Add Data	/resource/saveConnType	191-6	Configure-Tasks-Configure Activity Import[save values recieved from configure activity import screen]
Add Data	/resource/resourceActivitiesConfig	191-5	Configure-Tasks-Configure Activity Import[shows configure activity import screen]
Add Data	/resource/showAccessCorrelationRulesList	436-7	Resource-Show Access Correlation Rules List
Add Data	/resource/listResourceGroupsForGlossaryImport	437-7	List Resource Groups For Glossary Import
Add Data	/resource/getDatasourceConnection	441-3	Resource-Get Datasource Connection
Add Data	/resource/importActivities	441-1	Resource-Import Activities

Category	URL	ID	Description
Add Data	/resource/resourceEvents	443-4	Resource-Resource Events
Add Data	/resource/showAppEvents	443-3	Resource-Show Application Events
Add Data	/resource/getResourceGroupGeneralDetails	443-2	Get General Details for Resource Group
Add Data	/resource/showBubbleChartByAccessValue	443-1	Resource-Show Bubble Chart By Access Value
Add Data	/resource/getSailpointDatasourceAttr	443-0	Resource-Get Sailpoint Datasource Attributes
Add Data	/resource/ipMappingEnabledChk	442-9	Resource-Check for IP Mapping Enabled
Add Data	/settings/updateLogLevels	196-6	Configure-Logging-Modules [update log level]
Add Data	/resource/isResourceAttributeNameDuplicate	442-7	Check if Resource Attribute Name is Duplicate
Add Data	/resource/updateResourceColor	443-5	Update Resource Color
Add Data	/resource/advancedSearchAddUser	442-6	Resource-Advanced Search Add User
Add Data	/resource/getFilterCondition	442-4	Resource-Get Filter Condition

Category	URL	ID	Description
Add Data	/resource/fetchUiConfig	442-3	Resource-Fetch UI Config
Add Data	/users/save	445-5	Users-Save
Add Data	/users/updateCriticality	445-7	Users-Update Criticality
Add Data	/users/getUserActivityAccounts	450-2	Users-Get User Activity Accounts
Add Data	/users/showUserQuickInfo	448-1	Show User Quick Info
Add Data	/users/showManagerDetails	448-3	Users-Show Manager Details
Add Data	/users/getLastImportDateForResource	448-4	Users-Get Last Import Date for Resource
Add Data	/resource/showImportResourceMetadata	442-5	Show Import Resource Metadata
Add Data	/resource/showResourceGlossary	441-2	Show Resource Glossary
Add Data	/resource/saveNitroFieldFilter	443-6	Resource-Save Nitro Field Filter
Add Data	/resource/showActivityJobStatusDetails	443-8	Resource-Activity Job Status Details
Add Data	/users/getUsageTransactionsListForUser	444-4	Get Usage Transactions List for User
Add Data	/users/getMonths	444-5	Users-Get Months

Category	URL	ID	Description
Add Data	/users/getUpdatedToken	444-6	Users-Get Updated Token
Add Data	/users/advancedSearch	444-7	Users-Advanced Search
Add Data	/users/getDefaultQuery	444-8	Users-Get Default Query
Add Data	/users/verifyUserImportConfig	444-9	Users-Verify User Import Config
Add Data	/users/saveStatusDescriptionRules	445-0	Users-Save Status Description Rules
Add Data	/users/getPeerBaselines	445-1	Users-Get Peer Baselines
Add Data	/resource/listOwners	443-7	Resource-Owners List
Add Data	/users/showSearch	445-2	Users-Show Search
Add Data	/users/emailTemplates	445-4	Users-Email Templates
Add Data	/resource/showGlossaryImportConfig	441-9	Resource-Show Glossary Import Configuration
Add Data	/resource/searchResourceTypeAJAX	442-1	Search Resource Type using AJAX
Add Data	/users/decryptSelectedUsers	445-6	Users-Decrypt Selected Users
Add Data	/resource/showVennChartByAccessValue	442-2	Resource-Show Venn Chart By Access Value

Category	URL	ID	Description
Add Data	/resource/editFieldFilter	444-0	Resource-Edit Field Filter
Add Data	/resource/previewAccessImportConfig	443-9	Resource-Preview Access Import Configuration
Add Data	/users/isEmployeeIdDuplicate	444-3	Users-Check if Employee Id is Duplicate
Add Data	/users/showDLPAAlerts	445-3	Users-Show DLP Alerts
Add Data	/users/showAccessLevel3	448-5	Users-Access Level3
Add Data	/resource/saveLineFilters	437-8	Resource-Save Line Filters
Add Data	/resource/showAccessValuesByPeer	438-0	Resource-Show Access Values By Peer
Add Data	/config/showPreviewTEMP	369-9	Configuration-Show Pre-viewTEMP
Add Data	/config/isWorkflowDuplicate	369-8	Configuration-Check if Workflow is Duplicate
Add Data	/config/showSamlSettings	369-6	Configuration-Show SAML Settings
Add Data	/config/isFileExist	369-5	Configuration-Check if File Exists

Category	URL	ID	Description
Add Data	/config/maskUnmaskData	369-4	Configuration-Mask or Unmask Data
Add Data	/config/showConfigureResourceRiskLevels	369-3	Configuration-Show Configure Resource Risk Levels
Add Data	/config/getEncryptionKeyCount	369-2	Configuration-Get Key Count for Encryption
Add Data	/peer/getPeerActivityDates	422-5	Get Peer Activity Dates
Add Data	/config/updateJob	370-0	Configuration-Update Job
Add Data	/uf/saveRgUfConfig	302-6	Configure-Universal Forwarder-Save/Update Resource Group Configuration
Add Data	/resource/deleteAccessValue	440-6	Resource-Delete Access Value
Add Data	/resource/listFormatForActivity	440-3	Resource-List Format For Activity
Add Data	/resource/scheduleActivityCorrelationJob	440-2	Resource-Schedule Activity Correlation Job
Add Data	/resource/verifyAccessImportDatasourceConfig	440-1	Resource-Verify Access Import Datasource Configuration

Category	URL	ID	Description
Add Data	/resource/showAccessImportAttrMapping	440-0	Resource-Show Access Import Attribute Mapping
Add Data	/re-source/showActivityOutlierDetailsForResourceByJobId	439-9	Activity Outlier Details For Resource By Job Id
Add Data	/resource/showResourceActivitySummary	439-8	Show Resource Activity Summary
Add Data	/resource/showUnCorrelatedAccountDetails	439-7	Resource-UnCorrelated Account Details
Add Data	/peer/listSelectPeer	422-7	List Select Peer
Add Data	/resource/getPoliciesList	439-6	Resource-Get Policies List
Add Data	/config/deleteAttachment	370-1	Configuration-Delete Attachment
Add Data	/config/populatetpikb	370-2	Configuration-Populate PIKB
Add Data	/config/createGeoImportConfig	367-2	Configuration-Create Geolocation Import Configuration
Add Data	/config/manageEncryption	367-1	Configuration-Manage Encryption
Add Data	/config/saveMetaconnection	367-0	Configuration-Save Metadata Connection

Category	URL	ID	Description
Add Data	/config/showConfigurePeerRiskLevels	366-9	Configuration-Configure Peer Risk Levels
Add Data	/config/showDetails	366-8	Configuration-Show Details
Add Data	/config/refreshUploadLicense	368-8	Configuration-Refresh Upload License
Add Data	/config/isValidatePort	369-0	Configuration-Check if Port if Valid
Add Data	/config/showUploadLicense	371-4	Configuration-Show Upload License
Add Data	/config/checkConfig	369-1	Configuration-Check Configuration
Add Data	/config/getBeforeEncrypDecryptData	370-3	Configuration-Get Before Encryption or Decryption of Data
Add Data	/config/showAddWorkflowStatus	371-2	Configuration-Show Add Workflow Status
Add Data	/config/showSavedJobDetails	371-1	Configuration-Show Saved Job Details
Add Data	/config/getDistinctColValuesFromCRP	371-0	Configuration-Get Distinct Column Values From CRP

Category	URL	ID	Description
Add Data	/config/deleteConfig	370-8	Configuration-Delete Configuration
Add Data	/config	370-7	Configuration
Add Data	/config/decryptData	370-6	Configuration-Decrypt Data
Add Data	/config/selectJobsForChaining	370-5	Configuration-Select Jobs For Chaining
Add Data	/config/getSpecificBprofileconfigDetails	370-4	Configuration-Get Specific B Profile Configuration Details
Add Data	/config/saveButton	371-3	Configuration-Save Button
Add Data	/resource/saveActivityOutlierPolicy	437-9	Resource-Save Activity Outlier Policy
Add Data	/resource/showMonitorAccounts	439-5	Resource-Show Monitor Accounts
Add Data	/chainTransaction/searchTransactions	193-1	Manage-Resources-Activity Management [shows activity management screen]
Add Data	/watchList/auditLogs	451-6	Watchlist-Audit Logs

Category	URL	ID	Description
Add Data	/watchList/showWatchlistImportJob	451-7	Watchlist-Show Watchlist Import Job
Add Data	/watchList/listActivityAccountNotInWatchlist	451-8	Watchlist-List of Activity Accounts Not in Watchlist
Add Data	/watchList/showAddToWhitelist	451-9	Watchlist-Show Add to Whitelist
Add Data	/watchList/addSelectedMembers	452-1	Add Selected Members to Watchlist
Add Data	/watchList/	452-2	Show Watchlist
Add Data	/watchList/listUsersNotInWatchlist	452-3	Watchlist-List of Users Not in Watchlist
Add Data	/watchList/addToWL	452-4	Add to Watchlist
Add Data	/watchList/showWLImportConfig	451-5	Watchlist-Show Watchlist Import Configuration
Add Data	/resource/showCorrelationRulesList	440-9	Resource-Show Correlation Rules List
Add Data	/resource/selectResourceForActivitiesImport	192-1	Configure-Tasks-Activity Import [shows activity import screen]
Add Data	/watchList/getUpdatedToken	450-4	Watchlist-Get Updated Token

Category	URL	ID	Description
Add Data	/resource/searchActivityAccounts	438-7	Resource-Search Activity Accounts
Add Data	/resource/showAllTranForAccount	438-5	Resource-Show All Tran For Account
Add Data	/resource/previewTokens	438-4	Resource-Preview Tokens
Add Data	/resource/showResourceBehaviorSummary	438-3	Show Resource Behavior Summary
Add Data	/resource/selectedUsers	438-2	Resource-Selected Users
Add Data	/resource/showActivityOutliersJobStatus	438-1	Resource-Show Activity Outliers Job Status
Add Data	/resource/selectResourceForAccessImport	192-3	Configure-Tasks-Access Import [shows access import screen]
Add Data	/chainTransaction/list	193-2	Manage-Resources-Activity Management [shows list of activities on activity management screen]
Add Data	/resource/editArchSightLoggerFieldFilter	441-0	Resource-Edit ArchSight Logger Field Filter
Add Data	/watchList/memberlist	451-3	Watchlist-Show Memberlist

Category	URL	ID	Description
Add Data	/resource/scheduleGeolocationJob	193-0	Configure-Tasks-Populate Geolocation[schedule populate geolocation job]
Add Data	/resource/showGeolocationJob	192-9	Configure-Tasks-Activity Archival [show populate geolocation screen]
Add Data	/resource/scheduleActivityArchivalJob	192-8	Configure-Tasks-Activity Archival [schedule activity archival]
Add Data	/resource/previewGlossaryData	457-4	Preview glossary data while importing
Add Data	/resource/showScheduleActivityArchivalJob	192-7	Configure-Tasks-Activity Archival [shows activity archival screen]
Add Data	/resource/scheduleGlossaryJob	192-6	Configure-Tasks-Glossary Import [schedule glossary import job]
Add Data	/resource/selectResourceForGlossaryImport	192-5	Configure-Tasks-Glossary Import [shows glossary import screen]
Add Data	/resource/scheduleAccessJob	192-4	Configure-Tasks-Access Import [schedule access import job]

Category	URL	ID	Description
Add Data	/watchList/listAccessAccountNotInWatchlist	451-4	Watchlist-List of Access Accounts Not in Watchlist
Add Data	/resource/correlateToUser	440-5	Resource-Correlate to User
Add Data	/resource/scheduleActivityImportJob	192-2	Configure-Tasks-Activity Import [schedule activity import job]
Add Data	/resource/searchResourceGroupsAJAX	440-8	Search Resource Groups AJAX
Add Data	/watchList	450-6	Add Data-Show Watchlist
Add Data	/watchList/searchWLAJAX	450-7	Watchlist-Search Watchlist through AJAX
Add Data	/watchList/index	450-8	Watchlist
Add Data	/watchList/manageWatchListMembers	451-0	Watchlist-Manage WatchList Members
Add Data	/watchList/saveWlImportConfig	451-1	Watchlist-Save Watchlist Import Configuration
Add Data	/watchList/scheduleWLJob	451-2	Watchlist-Schedule Watchlist Job
Add Data	/resource/getFieldsForLineFilterRules	440-7	Resource-Get Fields For Line Filter Rules

Category	URL	ID	Description
Add Data	/users/showAccessLevel4	448-6	Users-Access Level4
Add Data	/users/previewData	448-7	Users-Preview Data
Add Data	/users/showDeleteAllUsersWarning	448-8	Users-Show Delete All Users Warning
Add Data	/peer	424-0	Peer
Add Data	/peer/showPeerCreationJobStatus	424-1	Show Peer Creation Job Status
Add Data	/resource/getResourceTypesList	424-2	Get Resource Types List
Add Data	/resource/showBehaviorActivityDetails	424-3	Resource-Show Behavior Activity Details
Add Data	/resource/saveResourceConfig	424-5	Save Resource Config
Add Data	/peer/showResourcesForPeerBehavior	423-6	Resources For Peer Behavior
Add Data	/resource/showActivityJobErrors	424-6	Resource-Show Activity Job Errors
Add Data	/resource/getDistinctColumnValue	424-7	Resource-Get Distinct Column Value
Add Data	/peer/advancedSearch	423-9	Peer-Advanced Search
Add Data	/resource/showLineFiltersList	424-8	Resource-Show Line Filters List

Category	URL	ID	Description
Add Data	/resource/uploadImportFile	425-0	Resource-Upload Import File
Add Data	/resource/showCreateResourceDialog	425-1	Show Create Resource Dialog
Add Data	/peer/showPeerUserAccessDetails	423-7	Peer User Access Details
Add Data	/peer/getUsageResourcesListForPeer	423-5	Get Usage Resources List for Peer
Add Data	/resource/verifyDatasourceConfig	427-2	Resource-Verify Datasource Config
Add Data	/resource/drillDownStackedChartByAccessValue	435-6	Resource-Filter Stacked Chart By Access Value
Add Data	/resource/assignSelectedUserToResource	436-2	Assign Selected User to Resource
Add Data	/resource/assignAppToUser	436-1	Resource-Assign App To User
Add Data	/resource/showVulnerabilities	424-9	Resource-Show Vulnerabilities
Add Data	/resource/showTranForAccount	436-0	Resource-Show Transaction for Account
Add Data	/peer/reloadAutoComplete	423-8	Peer-Reload Auto Complete
Add Data	/resource/updateResourceGroupAttributes	427-3	Update Resource Group Attributes
Add Data	/resource/loadsurereviewfilter	434-6	Resource-Load Sureview Filter

Category	URL	ID	Description
Add Data	/resource/getResourceActivityDates	430-5	Get Resource Activity Dates
Add Data	/resource/getDatasourceType	433-1	Resource-Get Datasource Type
Add Data	/resource/quickSearchAJAX	434-7	Resource-Quick Search using AJAX
Add Data	/resource/importAccess	434-8	Resource-Import Access
Add Data	/resource/showWhols	434-9	Resource-Show Who Is
Add Data	/resource/searchResourceGroup	435-0	Search Resource Group
Add Data	/resource/loadFields	435-1	Resource-Load Fields
Add Data	/resource/previewEventData	432-2	Resource-Preview Event Data
Add Data	/resource/addOwnerForAccessAttribute	435-2	Resource-Add Owner for Access Attribute
Add Data	/resource/isResourceNameDuplicate	435-4	Check if Resource Name is Duplicate
Add Data	/resource/showUncorrelatedResults	431-0	Resource-Show Uncorrelated Results
Add Data	/resource/updateAccountDescription	430-9	Resource-Update Account Description

Category	URL	ID	Description
Add Data	/resource/updateTransactionCriticality	430-8	Resource-Update Transaction Criticality
Add Data	/resource/showSelectOperatorAttributes	430-7	Resource-Show Select Operator Attributes
Add Data	/resource/renderResourceGroupEventTemplate	430-6	Render Resource Group Event Template
Add Data	/resource/selectedUsersEdit	432-7	Resource-Selected Users Edit
Add Data	/resource/updateAccessAccountAttributes	432-8	Resource-Update Access Account Attributes
Add Data	/resource/listAttributeValueForAccessAttribute	435-3	Resource-List Attribute Values for Access Attribute
Add Data	/resource/showTranListForAccount	434-4	Resource-Show Transaction List for Account
Add Data	/resource/toggleLineFilter	435-9	Resource-Toggle Line Filter
Add Data	/resource/getResourceAccessMetadataList	435-7	Get Resource Access Metadata List
Add Data	/resource/updateAccessValues	431-6	Resource-Update Access Values
Add Data	/resource/fillListVenn	425-5	Resource-Fill List Venn

Category	URL	ID	Description
Add Data	/resource/runBulkImportResources	426-6	Run Bulk Import Resources
Add Data	/resource/ipAddrConfig	431-7	Resource-IP Address Configuration
Add Data	/resource/saveResourceGlossary	431-9	Save Resource Glossary
Add Data	/resource/encryptDecryptAccessAttributeValue	426-2	Resource-Encrypt Decrypt Access Attribute Value
Add Data	/resource/savecefsettings	425-6	Resource-Save CEF Settings
Add Data	/resource/getSubTreeData	425-7	Resource-Get Sub Tree Data
Add Data	/resource/getParentResourceActivityAttributes	431-5	Get Parent Resource Activity Attributes
Add Data	/resource/getNodeResourceGroups	425-8	Get Node Resource Groups
Add Data	/resource/saveNitroLineFilters	426-0	Resource-Save Nitro Line Filters
Add Data	/resource/searchAccessAccountsAJAX	426-1	Resource-Search Access Accounts using AJAX
Add Data	/resource/editNitroFieldFilter	433-5	Resource-Edit Nitro Field Filter
Add Data	/resource/previewFieldFilters	426-3	Resource-Preview Field Filters

Category	URL	ID	Description
Add Data	/resource/saveFieldFilterTemplate	426-4	Resource-Save Field Filter Template
Add Data	/resource/attrCheck	426-5	Resource-Attribute Check
Add Data	/resource/checkAccountViolations	432-1	Resource-Check Account Violations
Add Data	/resource/showAddNewEntitlement	432-0	Resource-Add New Entitlement
Add Data	/resource/updateAccessAttribute	425-9	Resource-Update Access Attribute
Add Data	/resource/showFieldFilterRules	435-8	Resource-Show Field Filter Rules
Add Data	/resource/getNodesList	426-7	Resource-Get Nodes List
Add Data	/resource/saveArcsightloggerFieldFilter	432-4	Resource-Save Arcsight Logger Field Filter
Add Data	/peer/showAddParent	422-8	Peer-Show Add Parent
Add Data	/peer/	423-4	Peer Creation
Add Data	/resource/isScheduleJobNameDuplicate	435-5	Resource-Check if Schedule Job Name is Duplicate
Add Data	/peer/selectedOwnerEdit	422-9	Peer-Selected Owner Edit
Add Data	/peer/addUsersToPeer	423-0	Add Users To Peer

Category	URL	ID	Description
Add Data	/peer/isNameDuplicate	423-1	Peer-Check if Name is Duplicate
Add Data	/peer/showBehaviorByResource	423-2	Peer-Show Behavior By Resource
Add Data	/peer/showPeerAccessDetails	423-3	Peer Access Details
Add Data	/resource/showActivityOutliersJobWizard	432-3	Resource-Show Activity Outliers Job Wizard
Add Data	/resource/checkAccountViolationsForResource	425-2	Check Account Violations for Resource
Add Data	/resource/getUpdatedToken	425-4	Resource-Get Updated Token
Add Data	/resource/getThreatListParameter	431-8	Resource-Get Threat List Parameter
Add Data	/resource/showAccessImportConnType	427-1	Resource-Show Access Import Connection Type
Add Data	/resource/showResourcesForActivityOutliers	432-6	Show Resources for Activity Outliers
Add Data	/resource/showActivityOutliers	427-0	Resource-Show Activity Outliers
Add Data	/resource/filterResources	426-9	Filter Resources
Add Data	/resource/getTransactionsForResource	432-5	Get Transactions for Resource

Category	URL	ID	Description
Add Data	/resource/listResourceGroupsForAccessImport	426-8	List Resource Groups for Access Import
Add Data	/resource/assignToUserList	425-3	Resource-Assign to User List
Add Data	/resource/getSuspectChecksList	434-3	Resource-Get SuspectChecks List
Add Data	/resource/getChartsList	434-2	Resource-Get ChartsList
Add Data	/resource/showSearchUsers	434-1	Resource-Show Search Users
Add Data	/users/deleteAllUsers	446-4	Users-Delete All Users
Add Data	/users/getUserAccounts	446-5	Users-Get User Accounts
Add Data	/users/getUserActivityDates	446-6	Users-Get User Activity Dates
Add Data	/users/getDateTime	446-7	Users-Get Date and Time
Add Data	/users/validateDelimiters	446-8	Users-Validate Delimiters
Add Data	/users/getTransactionsForResource	446-9	Users-Get Transactions for Resource
Add Data	/users/showResourceAccountsForUserBehavior	447-0	Show Resource Accounts for User Behavior
Add Data	/users/getFilterCondition	447-1	Users-Get Filter Condition

Category	URL	ID	Description
Add Data	/users/showUserActivitySummary	446-3	Users-Show User Activity Summary
Add Data	/users/showUserImportJobErrors	447-2	Show User Import Job Errors
Add Data	/users/showTransactionSearchForUser	447-4	Show Transaction Search For User
Add Data	/users/beforeInterceptor	447-5	Users-Before Interceptor
Add Data	/users/getUserResources	447-6	Users-Get User Resources
Add Data	/users/showBehaviorByActivity	447-8	Users-Show Behavior By Activity
Add Data	/resource/scheduleImportResources	436-6	Schedule Import Resources
Add Data	/users/showAccessDetails	444-1	Users-Show Access Details
Add Data	/resource/verifyGlossaryImportDatasourceConfig	436-4	Resource-Verify Glossary Import Datasource Config
Add Data	/resource/showGlossaryJobStatusDetails	429-4	Resource-Show Glossary Job Status Details
Add Data	/users/validateIdentifiers	447-3	Users-Validate Identifiers
Add Data	/resource/loadDatasourceAttributes	428-8	Resource-Load Datasource Attributes
Add Data	/users/getTreeNodees	446-2	Users-Get Tree Nodes

Category	URL	ID	Description
Add Data	/users/getUsageResourcesListForUser	446-0	Get Usage Resources List for User
Add Data	/users/showAccessLevel1	448-9	Users-Access Level1
Add Data	/users/create	449-0	Users-Create
Add Data	/users/searchAJAX	449-1	Users-Search using AJAX
Add Data	/users/reloadAutoComplete	449-2	Users-Reload Auto Complete
Add Data	/users/getResourcesListForUser	449-3	Get Resources List for User
Add Data	/users/getTransactionsForAccount	449-4	Users-Get Transactions for Account
Add Data	/users/getDefaultOIADefaultQuery	449-5	Users-Get Default OIA Default Query
Add Data	/users/showBehaviorTimeWindowsSummary	449-6	Users-Show Behavior Time Windows Summary
Add Data	/users/showAccessLevel2	446-1	Users-Access Level2
Add Data	/users/quickSearchAJAX	449-7	Users-Quick Search using AJAX
Add Data	/users/showBehaviorWithSuspectForUser	449-9	Users-Behavior With Suspect for User

Category	URL	ID	Description
Add Data	/users/getTransactionsForResourceId	450-0	Users-Get Transactions For ResourceId
Add Data	/users/showBehaviorActivityDetails	450-1	Users-Behavior Activity Details
Add Data	/users/showDashboard	448-2	Users-Show Dashboard
Add Data	/users/showUserChangeHistory	448-0	Show User Change History
Add Data	/users/getUserAccountsByEmployeeId	445-8	Users-Get User Accounts By Employee Id
Add Data	/users/	447-9	Add Data-Enable User Import
Add Data	/users/showIPMappingForNetworkAddress	445-9	Users-Show IP Mapping for Network Address
Add Data	/users/showAttrMapping	449-8	Users-Attribute Mapping
Add Data	/resource/deleteReport	428-9	Resource-Delete Report
Add Data	/resource/getAccountData	429-0	Resource-Get Account Data
Add Data	/resource/getTransactionsForResourceId	429-1	Get Transactions for ResourceId
Add Data	/resource/previewAccessData	427-7	Resource-Preview Access Data
Add Data	/resource/saveArcsightLoggerLineFilters	427-6	Resource-Save Arcsight Logger Line Filters

Category	URL	ID	Description
Add Data	/resource/saveFieldFilterRules	427-5	Resource-Save Field Filter Rules
Add Data	/resource/searchTransactionsForResource	433-3	Search Transactions for Resource
Add Data	/resource/showUnCorrelatedActivityAccountsUsage	430-2	Resource-UnCorrelated Activity Accounts Usage
Add Data	/resource/getSolrFilterCondition	430-3	Resource-Get Solr Filter Condition
Add Data	/resource/showResourceEvents	430-4	Show Resource Events
Add Data	/resource/showCreateAttribute	434-5	Resource-Show Create Attribute
Add Data	/resource/reloadAutoComplete	427-8	Resource-Reload Auto Complete
Add Data	/resource/showCorrelationResults	433-6	Resource-CorrelationResults
Add Data	/resource/saveAccessConfigTemplate	433-8	Resource-Save Access Config Template
Add Data	/resource	431-4	Add Data-Resource
Add Data	/resource/showBehaviorTimeWindowsSummary	431-3	Resource-Show Behavior Time Windows Summary
Add Data	/resource/removeResourceGlossary	431-2	Remove Resource Glossary

Category	URL	ID	Description
Add Data	/resource/loadResourceGroupEvents	431-1	Load Resource Group Events
Add Data	/resource/getActivityAttributesForResourceGroup	433-2	Get Activity Attributes for Resource Group
Add Data	/resource/searchResources	433-9	Search Resources
Add Data	/resource/getUsageTransactionsListForResource	434-0	Get Usage Transactions List For Resource
Add Data	/resource/showUserDetailsForActivityOutliers	433-7	Resource-Show User Details for Activity Outliers
Add Data	/config/saveCriticality	197-0	Configure-Criticality[schedule criticality job]
Add Data	/resource/saveActivityOutliers	428-0	Resource-Save Activity Outliers
Add Data	/resource/showEventsSummary	436-3	Resource-Show Events Summary
Add Data	/resource/showJobsForActivities	429-2	Resource-Show Jobs for Activities
Add Data	/resource/showAccessValueDetails	429-3	Resource-Show Access Value Details
Add Data	/resource/beforeInterceptor	429-5	Resource-Before Interceptor
Add Data	/resource/showResourceGroupsForNode_DELETE	427-4	Resource Groups For Node_DELETE

Category	URL	ID	Description
Add Data	/resource/showCreateResourceGroupList	429-6	Create Resource Group List
Add Data	/resource/checkViolationsForResource	429-7	Check Violations for Resource
Add Data	/resource/list	429-8	Resource-List
Add Data	/resource/getMappedActivityAttributesList	429-9	Resource-Get Mapped Activity Attributes List
Add Data	/resource/showEditUserFilter	430-0	Resource-Edit User Filter
Add Data	/resource/toggleAnalysisTpiState	430-1	Resource-Toggle Analysis Third Party Intelligence State
Add Data	/resource/showStackedChartByAccessValue	428-7	Resource-Show Stacked Chart By Access Value
Add Data	/resource/getExistingTemplateDetails	428-6	Resource-Get Existing Template Details
Add Data	/config/showConfigureCriticality	196-9	Configure-Criticality[shows schedule criticality job screen]
Add Data	/resource/showResourceMetadata	428-4	Show Resource Metadata
Add Data	/resource/showActivityJobStatusDetailsInProgress	428-3	Resource-Show Activity Job Status Details In Process

Category	URL	ID	Description
Add Data	/resource/maskUnmaskAccessAttributeValue	428-2	Resource-Masked Unmasked Access Attribute Value
Add Data	/resource/showCorrelatedAccountsWithAccessValue	433-0	Resource-Correlated Accounts With Access Value
Add Data	/resource/showReconciliationDetails	432-9	Resource-Show Reconciliation Details
Add Data	/resource/showActivityOutliersByJob	428-1	Resource-Show Activity Outliers By Job
Add Data	/config/writeToXML	367-3	Configuration-Write To XML
Add Data	/config/saveLookupConfig	367-4	Configuration-Save Lookup Configuration
Add Data	/resource/glossaryAccessConfig	191-9	Configure-Tasks-Configure Glossary Import[shows configure glossary import screen]
Add Data	/config/saveJobDetails	367-6	Configuration-Save Job Details
Add Data	/organization/addChildOrganizations	418-0	Add Child Organizations
Add Data	/organization/beforeInterceptor	417-6	Add Data-Organization Before Interceptor

Category	URL	ID	Description
Add Data	/organization/createOrganizationCreationRule	417-3	Organization Creation Rule
Add Data	/organization/getUpdatedToken	417-1	Add Data-Organization Get Updated Token
Add Data	/organization/deleteJob	417-0	Organization-Delete Job
Add Data	/organization/addApplicationsToOrg	416-8	Add Applications to Organization
Add Data	/peer/showPeerJobStatusDetailsChart	420-0	Peer Job Status Details Chart
Add Data	/peer/getAccessAttributesByResourceGroup	420-2	Peer-Get Access Attributes By Resource Group
Add Data	/peer/savePeerCreationRules	418-6	Save Peer Creation Rules
Add Data	/organization/loadCreationRule	416-6	Organization-Load Creation Rule
Add Data	/peer/showDashboard	422-3	Peer-Show Dashboard
Add Data	/peer/getPBMonths	422-2	Peer-Get PB Months
Add Data	/peer/show	422-1	Peer-Show
Add Data	/peer/quickSearchAJAX	422-0	Quick Search using AJAX
Add Data	/peer/checkHasOutliers	421-9	Peer-Check Has Outliers

Category	URL	ID	Description
Add Data	/peer/getUpdatedToken	421-8	Peer-Get Updated Token
Add Data	/peer/getTransactionsForPeer	421-7	Get Transactions for Peer
Add Data	/peer/showPeerJobStatusDetails	421-6	Show Peer Job Status Details
Add Data	/peer/getResourcesListForPeer	421-4	Get Resources List for Peer
Add Data	/peer/beforeInterceptor	421-5	Peer-Before Interceptor
Add Data	/peer/runRule	418-7	Peer-Run Rule
Add Data	/peer/listUsersForOwner	420-1	Peer-List Users For Owner
Add Data	/riskModeler/updateModelAttributes	308-1	Configure-Threat Model-Set Threat Model Live
Add Data	/riskModeler/saveThreatModel	308-2	Configure-Threat Model-Save Threat Model
Add Data	/org/assignResourceToOrg	314-4	Dashboard-Organization-Assign Resource To Organization
Add Data	/org/assignResourceToOrgHierarchy	314-5	Dashboard-Organization-Assign Resource To Organization Hierarchy

Category	URL	ID	Description
Add Data	/chainTransaction	410-5	Chain Transaction
Add Data	/chainTransaction/showUsersForTransaction	410-6	Show Users for Transaction
Add Data	/chainTransaction/showTransactions	410-7	Show Transactions
Add Data	/peer/showBehaviorActivityDetails	419-0	Peer-Show Behavior Activity Details
Add Data	/peer/getUsageTransactionsListForPeer	418-8	Get Usage Transactions List for Peer
Add Data	/peer/showScheduleCreationRule	419-9	Peer-Show Schedule Creation Rule
Add Data	/peer/showSearch	419-7	Peer-Show Search
Add Data	/peer/selectedOwner	419-6	Peer-Selected Owner
Add Data	/peer/listAddParent	419-5	Peer-List Add Parent
Add Data	/peer/showAccessOutliersByPeerChart	419-4	Show Access Outliers By Peer Chart
Add Data	/peer/listPeerTypes	419-3	List Peer Types
Add Data	/peer/selectPeerList	419-2	Select Peer List
Add Data	/peer/getRuleConditions	419-1	Peer-Get Rule Conditions

Category	URL	ID	Description
Add Data	/peer/showRiskyUsersForAccessValue	418-9	Peer-Show Risky Users for Access Value
Add Data	/peer/advancedSearchAddUser	419-8	Peer-Advanced Search Add User
Add Data	/riskModeler/showThreatModel	308-0	Configure-Threat Model-Show/Edit Threat Model
Add Data	/peer/showAddOwner	421-3	Peer-Show Add Owner
Add Data	/peer/listPeersForResourceGroup	421-2	List Peers for Resource Group
Add Data	/manageData/showProfileResourceAccessLevel1	413-3	Manage Data-Show Profile Resource Access Level1
Add Data	/config/showRiskModeler	202-8	Configure-Risk Modeler
Add Data	/endpoint/saveEndPointConfig	411-6	Save EndPoint Configuration
Add Data	/endpoint/beforeInterceptor	411-5	Endpoint-Before Interceptor
Add Data	/endpoint/getUpdatedToken	411-4	Endpoint-Get Updated Token
Add Data	/endpoint/showScheduleEndPointImportJob	411-3	Show Schedule EndPoint Import Job
Add Data	/endpoint/	411-2	Endpoint

Category	URL	ID	Description
Add Data	/endpoint	411-1	Show Endpoint
Add Data	/config/scheduleIpMappingJob	200-2	Configure-Tasks-IP Mapping[schedule ip mapping job]
Add Data	/endpoint/scheduleEndPointImport	411-0	Schedule EndPoint Import
Add Data	/manageData/addUsersToProfile	413-2	Manage Data-Add Users to Profile
Add Data	/manageData/	413-4	Enable Add Data
Add Data	/organization/advancedSearchAddUser	416-2	Organization-Advanced Search Add User
Add Data	/organization/createRule	414-6	Organization-Create Rule
Add Data	/organization/pauseJob	415-9	Organization-Pause Job
Add Data	/organization/deleteOrganizations	415-8	Delete Organizations
Add Data	/organization/showCreationRules	415-7	Organization-Show Creation Rules
Add Data	/organization/addResourcegroupsToOrg	415-6	Organization-Add Resource Groups to Organization
Add Data	/chainTransaction/update	410-9	Chain Transaction-Update

Category	URL	ID	Description
Add Data	/peer/searchAJAX	420-3	Peer-Search using AJAX
Add Data	/config/interruptJob	200-0	Configure-Tasks [interrupt job]
Add Data	/config/pauseJob	199-8	Configure-Tasks [pause job]
Add Data	/peer/showEventsSummary	421-1	Peer-Show Events Summary
Add Data	/peer/runPeerCreationRule	421-0	Run Peer Creation Rule
Add Data	/peer/showPeerAccessResourcesList	420-9	Peer Access Resources List
Add Data	/peer/listUsersNotInPeer	420-8	List Users Not In Peer
Add Data	/peer/searchPeerOwnerAJAX	420-7	Search Peer Owner using AJAX
Add Data	/peer/showBehavior	420-6	Peer-Show Behavior
Add Data	/peer/showBehaviorByActivity	420-5	Peer-Show Behavior by Activity
Add Data	/peer/create	420-4	Peer-Create
Add Data	/config/resumeJob	199-9	Configure-Tasks [resume job]
Add Data	/organization/addResourcesToOrg	416-7	Add Resources to Organization

Category	URL	ID	Description
Add Data	/chainTransaction/updateTranFlags	410-8	Chain Trans- action-Update Transaction Flags
Add Data	/config/showIpMappingJob	200-1	Configure-Tasks- IP Mapping[shows create ip mapping job screen]
Add Data	/manageData/removeUsersFromProfile	413-1	Manage Data- Remove Users from Profile
Add Data	/manageData/showAddOwnerProfile	413-0	Manage Data- Show Add Owner Profile
Add Data	/manageData/isResourceGroupIpDuplicate	412-9	Manage Data- Check if Resource Group Ip is Duplic- ate
Add Data	/manageData/showAddUsersToProfileDialog	412-8	Manage Data- Show Dialog for Add Users to Pro- file
Add Data	/config/cancelJob	199-6	Add Data-Tasks [cancel job]
Add Data	/config/reRunJob	199-7	Add Data-Tasks [re-run job]
Add Data	/organization/showJobForCreationRules	416-5	Organization- Show Job for Creation Rules

Category	URL	ID	Description
Add Data	/uf/addJobToUf	302-5	Configure-Universal Forwarder-Save/Update job of UF
Add Data	/uf/showUFResourceGroupConfig	302-4	Configure-Universal Forwarder-Shows Resource Group Configuration
Add Data	/uf/listUFJobList	302-3	Configure-Universal Forwarder-Shows list of jobs in UF
Add Data	/application/addResourcesToApp	408-2	Application-Add Resources to App
Add Data	/application/isNameDuplicate	408-3	Application-Check if Name is Duplicate
Add Data	/chainTransaction/getFilterCondition	409-5	Chain Transaction-Get Filter Condition
Add Data	/chainTransaction/edit	410-4	Chain Transaction-Edit
Add Data	/chainTransaction/create	410-3	Chain Transaction-Create
Add Data	/chainTransaction/delete	410-2	Chain Transaction-Delete
Add Data	/chainTransaction/getUpdatedToken	410-1	Chain Transaction-Get Updated Token

Category	URL	ID	Description
Add Data	/chainTransaction/beforeInterceptor	410-0	Chain Transaction-Before Interceptor
Add Data	/application/list	408-1	Application-List
Add Data	/chainTransaction/updateTransactionAttributes	409-9	Chain Transaction-UpdateTransactionAttributes
Add Data	/chainTransaction/show	409-7	Chain Transaction-Show
Add Data	/chainTransaction/showUncorrelatedAccountsForTransaction	409-6	Chain Transaction-Show Uncorrelated Accounts for Transaction
Add Data	/chainTransaction/save	409-4	Chain Transaction-Save
Add Data	/application/showCreateAppDialog	408-4	Show Create App Dialog
Add Data	/chainTransaction/	409-3	Show Chain Transaction
Add Data	/chainTransaction/showCreateTransactionDialog	409-2	Show Create Transaction Dialog
Add Data	/chainTransaction/showTransactionDetails	409-1	Show Transaction Details
Add Data	/application/getUpdatedToken	409-0	Application-Get Updated Token

Category	URL	ID	Description
Add Data	/chainTransaction/getUniqueTransactionsForResourceId	409-8	Chain Transaction-Get Unique Transactions for ResourceId
Add Data	/application/removeResourcesFromApp	408-9	Application-Remove Resources From App
Add Data	/resource/deleteLineFilter	204-7	Configure-Tasks-Activity Import Config-Line Filter [shows delete line filter screen]
Add Data	/resource/showLineFilters	204-5	Configure-Tasks-Activity Import Config-Line Filter [shows create line filter screen]
Add Data	/application/update	408-0	Application-Update
Add Data	/application/showAddResourcesDialog	407-9	Application-Show Add Resources Dialog
Add Data	/application/edit	407-8	Application-Edit
Add Data	/application/searchAJAX	407-7	Application-Search using AJAX
Add Data	/application/showAppDetails	407-6	Show Application Details

Category	URL	ID	Description
Add Data	/application/listResourcesNotApplications	407-5	List Resources Not Applications
Add Data	/application	407-4	Enable Application View
Add Data	/config/showPrivacySettings	203-3	Configure-Privacy Settings
Add Data	/resource/editLineFilter	204-6	Configure-Tasks-Activity Import Config-Line Filter [shows edit line filter screen]
Add Data	/config/showExportAccessJob	203-4	Configure-Tasks-Export-Access Entitlements
Add Data	/resource/showAccessImportConfig	203-7	Configure-Tasks-Import-Access-Edit/Setup Configuration
Add Data	/config/scheduleExportAccessJob	203-8	Configure-Tasks-Export-Access Entitlements [Schedule Access Entitlements Job]
Add Data	/resource/saveAccessCorrelationRules	203-9	Configure-Tasks-Access Import Config-Correlation Rule[saves Correlation rule]

Category	URL	ID	Description
Add Data	/resource/editAccessCorrelationRules	204-0	Configure-Tasks-Access Import Config-Correlation Rules[Update Correlation Rule]
Add Data	/resource/saveAccessUserFilter	204-1	Configure-Tasks-Access Import Config [save advanced settings]
Add Data	/resource/showEditAccessCorrelationRule	204-2	Configure-Tasks-Access Import Config-Correlation Rule [shows edit access import correlation rule]
Add Data	/resource/deleteAccessCorrelationRule	204-3	Configure-Tasks-Access Import Config-Correlation Rule[delete access import correlation rule]
Add Data	/resource/createAccessCorrelationRule	204-4	Configure-Tasks-Access Import Config-Correlation Rule [shows create access import correlation rule screen]
Add Data	/resource/showResourceActivitiesConfig	203-6	Configure-Tasks-Import-Activities-Edit/Setup Configuration

Category	URL	ID	Description
Add Data	/application/	408-8	Application
Add Data	/application/showResourcesforApp	408-7	Application-Show Resources for App
Add Data	/application/beforeInterceptor	408-6	Application-Before Interceptor
Add Data	/config/scheduleSavedJob	377-0	Configuration-Schedule Saved Job
Add Data	/config/showOwnersList	376-9	Configuration-Show Owners List
Add Data	/metadata/show	324-7	Metadata-Show
Add Data	/config/showDecryptDataDialog	317-4	Configure-Access Control[Show decrypted/Unmask data]
Add Data	/config/searchSavedJobAJAX	367-5	Configuration-Search Saved Job through AJAX
Add Data	/uf/registerUF	302-0	Configure-Universal Forwarder-Save/update UF
Add Data	/resource/editCorrelationRules	205-2	Configure-Tasks-Activity Import Config-Correlation Rule [update Correlation Rule]

Category	URL	ID	Description
Add Data	/resource/saveActivityUserFilter	205-3	Configure-Tasks-Activity Import Config-Advanced Settings [save advanced settings]
Add Data	/config/showPolicyScannerJob	377-1	Configuration-Show Policy Scanner Job
Add Data	/tpi/showScheduleTpiImportJob	205-6	Configure-Tasks-TPI Import[shows tpi import screen]
Add Data	/config/saveRiskModel	205-9	Configure-RiskModeler [update modeler]
Add Data	/config/showCreateNode	206-0	Configure-Clustering [Clustering Modification]
Add Data	housekeepingJobs	301-3	Configure-Settings-House Keeping Jobs
Add Data	smtpSettings	301-7	Configure-Settings-SMTP Server Settings
Add Data	/uf/deleteUF	301-9	Configure-Universal Forwarder-Delete UF
Add Data	/uf/showAddJobToUF	302-1	Configure-Universal Forwarder-Add/edit UF Job

Category	URL	ID	Description
Add Data	/org/confirmAssignmentOfResourceToOrgHierarchy	314-6	Dashboard-Organization-Confirm-Assign Resource To Organization Hierarchy
Add Data	/uf/removeUfJob	302-2	Configure-Universal Forwarder-Remove Job from UF
Add Data	/resource/showResourceConfig	205-7	Configure-Show Resource Configuration
Add Data	/config/isduplicatenode	377-2	Configuration-Check if Node is Duplicate
Add Data	/config/attachFile	377-3	Configuration-Attach File
Add Data	/config/completeDeleteJob	377-4	Configuration-Complete Delete Job
Add Data	/application/save	408-5	Application-Save
Add Data	/resource/showCorrelationRules	204-8	Configure-Tasks-Activity Import Config-Correlation Rule [shows create Correlation Rule screen]

Category	URL	ID	Description
Add Data	/resource/showEditCorrelationRule	204-9	Configure-Tasks-Activity Import Config-Correlation Rule [shows edit Correlation Rule screen]
Add Data	/resource/deleteActivityCorrelationRule	205-0	Configure-Tasks-Activity Import Config-Correlation Rule [shows delete Correlation Rule]
Add Data	/uf/index	386-4	Add Data-Universal Forwarder Job
Add Data	/metadata/save	324-8	Metadata-Save
Add Data	/metadata	324-9	Show Metadata
Add Data	/metadata/create	325-0	Metadata-Create
Add Data	/metadata/	325-1	Metadata
Add Data	/uf/	386-9	Universal Forwarder
Add Data	/uf/beforeInterceptor	386-8	Universal Forwarder-Before Interceptor
Add Data	/uf/controlUf	386-7	Control Universal Forwarder

Category	URL	ID	Description
Add Data	/uf/togglePolicyscratch	386-6	Universal Forwarder-Toggle Policy Scratch
Add Data	/uf/getUpdatedToken	386-5	Universal Forwarder-Get Updated Token
Add Data	/uf/showPolicies	386-3	Universal Forwarder-Show Policies
Add Data	/metadata/index	324-6	Metadata-index
Add Data	/uf/toggleJobStatus	386-2	Universal Forwarder-Toggle Job Status
Add Data	/uf	386-1	Add Data-Universal Forwarder
Add Data	/tpi/showTpiExport	384-5	Show Third Party Intelligence Export
Add Data	/organization/interruptJob	415-4	Organization-Interrupt Job
Add Data	/organization/addUsersToOrg	415-3	Add Users to Organization
Add Data	/resource/saveCorrelationRules	205-1	Configure-Tasks-Activity Import Config-Correlation Rule [save Correlation Rule]
Add Data	/organization/cancelJob	414-8	Organization-Cancel Job

Category	URL	ID	Description
Add Data	/config/registerUser	366-5	Configuration-Register User
Add Data	/config/showEmailTemplateNotificationSettings	366-6	Configuration-Show Email Template Notification Settings
Add Data	/config/showAuditDetails	372-8	Configuration-Show Audit Details
Add Data	/config/rac	373-8	Configuration-Rac
Add Data	/config/_setAdvancedSearchObject	373-6	Configuration-Set Advanced Search Object
Add Data	/config/testNitroConnection	373-5	Configuration-Test Nitro Connection
Add Data	/config/downloadFiles	373-4	Configuration-Download Files
Add Data	/config/showGroupOwnersList	373-3	Configuration-Show Group Owners List
Add Data	/config/saveSystemAction	366-4	Configuration-Save System Action
Add Data	/config/getFieldsFromSQL	373-2	Configuration-Get Fields From SQL
Add Data	/config/continueWithEncryption	373-0	Configuration-Continue With Encryption

Category	URL	ID	Description
Add Data	/config/testSureViewConnection	372-9	Configuration-Test Sure View Connection
Add Data	/config/getColumnNames	372-7	Configuration-Get Column Names
Add Data	/config/beforeMaskingUnmasking	374-0	Configuration-Before Masking or Unmasking
Add Data	/config/httpListnerAction	372-6	Configuration-HTTP Listner Action
Add Data	/config/saveEncryptionSetting	372-5	Configuration-Save Encryption Setting
Add Data	/config/showManageLicense	372-4	Configuration-Show Manage License
Add Data	/config/updateAssociatedAccountFlag	372-3	Configuration-Update Associated Account Flag
Add Data	/config/showNitroDevicesList	373-1	Configuration-Show Nitro Devices List
Add Data	/config/searchAJAXConnType	372-2	Configuration-Search using AJAX by Connection Type

Category	URL	ID	Description
Add Data	/config/isScheduleJobNameDuplicate	359-2	Configuration-Check if Scheduled Job Name is Duplicate
Add Data	/config/isDatasourceNameDuplicate	359-4	Configuration-Check if Data-source Name is Dupliacte
Add Data	/config/showConfigureActivityrRiskLevels	360-2	Configure Activity Risk Levels
Add Data	/config/getSpecificPolicyDetails	361-1	Configuration-Get Specific Policy Details
Add Data	/config/isValidEmail	361-0	Configuration-Check if Email is Valid
Add Data	/config/getDatasourceAttributes	360-9	Configuration-Get Datasource Attributes
Add Data	/config/showIndexActivityTransactions	360-8	Configuration-Show Index Activity Transactions
Add Data	/config/scheduleHostnameLookupJob	360-7	Configuration-Schedule Host-name Lookup Job
Add Data	/config/saveScreen	360-6	Configuration-Save Screen
Add Data	/config/compareAuditXML	360-5	Configuration-Compare Audit XML

Category	URL	ID	Description
Add Data	/config/showSelectUsers	359-3	vSelect Users
Add Data	/config/generateKey	360-4	Configuration-Generate Key
Add Data	/config/advancedSearch	360-1	Configuration-Advance Search
Add Data	/config/checkDataToMask	359-1	Configuration-Check Data for Masking
Add Data	/config/showScheduleIndexingService	360-0	Configuration-Schedule Indexing Service
Add Data	/config/getBoxToken	359-9	Configuration-Get Box Token
Add Data	/config/deleteSavedJob	359-8	Configuration-Delete Saved Job
Add Data	/config/showSelectResources	359-7	Configuration-Select Resources
Add Data	/config/showCreateJsecUser	359-6	Configuration-Create Jsec User
Add Data	/config/showDatasourceList	359-5	Configuration-Show List of Data-sources
Add Data	/config/beforeKeyGeneration	360-3	Configuration-Key Generation
Add Data	/config/saveWorkflow	372-1	Configuration-Save Workflow
Add Data	/config/showSystemWorkflowDetails	372-0	Configuration-Show System Workflow Details

Category	URL	ID	Description
Add Data	/config/getAvailablePrivateKeys	371-9	Configuration-Get Available Private Keys
Add Data	/config/attachFileToCase	374-5	Configuration-Attach File To Case
Add Data	/config/saveStatus	374-4	Configuration-Save Status
Add Data	/config/scheduleIndexActTrans	371-7	Configuration-Schedule Index for Activity Transaction
Add Data	/config/showAuditXML	371-5	Configuration-Show Audit XML
Add Data	/config/	366-7	Show Configuration
Add Data	/config/testAwsConnection	367-8	Configuration-Test AWS Connection
Add Data	/config/config	368-7	Add Data-Show Configuration
Add Data	/config/schedulePolicyScanner	368-6	Configuration-Schedule Policy Scanner
Add Data	/config/removeSystemActions	374-7	Configuration-Remove System Actions
Add Data	/config/getDateFormats	368-5	Configuration-Get Date Formats

Category	URL	ID	Description
Add Data	/config/beforeEncryptDecrypt	368-3	Configuration-Before Encryption Decryption
Add Data	/config/runSavedJob	368-2	Configuration-Run Saved Job
Add Data	/config/checkLogTampering	368-1	Configuration-Check Log Tampering
Add Data	/config/beforeInterceptor	368-0	Configuration-Before Interceptor
Add Data	/config/updateCaseOwner	367-9	Configuration-Update Case Owner
Add Data	/config/getJobGroups	367-7	Configuration-Get Job Groups
Add Data	/config/encryptDecryptText	368-9	Configuration-Encryption and Decryption Text
Add Data	/config/showImports	199-3	Configure-Tasks
Add Data	/config/showSelectPeers	368-4	Configuration-Select Peers
Add Data	/config/previewPeerRiskLevels	374-8	Configuration-Preview Peer Risk Levels
Add Data	/config/scheduleGenerateCasesJob	374-9	Configuration-Schedule Generate Cases Job

Category	URL	ID	Description
Add Data	/config/deleteCaseAttachment	375-0	Configuration-Delete Case Attachment
Add Data	/config/showHelp	371-8	Configuration-Show Help
Add Data	/config/showDefaultConfig	373-9	Configuration-Show Default Configuration
Add Data	/config/listResourceGroupsForIndex	374-2	Configuration-List Resource Groups for Indexing
Add Data	/config/licenseSuccess	371-6	Configuration-License Install Success
Add Data	/config/showScheduleImportJob	375-5	Configuration-Show Schedule Import Job
Add Data	/config/emailTemplate	376-4	Configuration-Email Template
Add Data	/config/updateDecryptFlag	376-3	Configuration-Update Decryption Flag
Add Data	/config/checkForEncryptedDataBeforeMasking	376-2	Configuration-Check For Encrypted Data Before Masking
Add Data	/config/checkSecDB	376-1	Configuration-Check SecDB
Add Data	/config/analyzeLineFilters	376-0	Configuration-Analyze Line Filters

Category	URL	ID	Description
Add Data	/config/isduplicatenodeurl	375-9	Configuration-Check if Node Url is Duplicate
Add Data	/config/createSamlDetails	375-8	Configuration-Create SAML Details
Add Data	/config/getBeforeMaskUnmaskData	375-7	Configuration-Get Before Masking Unmasking of Data
Add Data	/config/showImportConfig	375-6	Configuration-Show Import Configuration
Add Data	/config/importDevicesFromNitro	375-4	Configuration-Import Devices From Nitro
Add Data	/config/showAddAction	374-3	Configuration-Show Add Action
Add Data	/config/removeActions	375-3	Configuration-Remove Actions
Add Data	/config/getRemoteDatasources	375-2	Configuration-Get Remote Data-sources
Add Data	/config/showDesignScreen	375-1	Configuration-Show Design Screen
Add Data	/config/getEncryptionKeys	361-2	Configuration-Get Encryption keys
Add Data	/config/searchJobAJAX	359-0	Configuration-Search Job through AJAX

Category	URL	ID	Description
Add Data	/config/updateHelpPref	376-7	Configuration-Update Help Preferences
Add Data	/config/showEncryptionJobDetails	356-8	Configuration-Show Encryption Job Details
Add Data	/config/showForms	363-0	Configuration-Show Forms
Add Data	/config/getJobId	362-9	Configuration-Get Job Id
Add Data	/config/showGenerateCases	362-8	Configuration-Generate Cases
Add Data	/config/showMetadataConfig	362-7	Configuration-Show Metadata Configuration
Add Data	/config/showLookupImportJob	362-6	Configuration-Show Job for Lookup Import
Add Data	/config/getDatasourceByType	362-5	Configuration-Get Datasources by Type
Add Data	/config/getJobFields	362-4	Configuration-Get Job Fields
Add Data	/config/testCEFSyslogConnection	362-3	Configuration-Test Syslog Connection for CEF
Add Data	/config/importJiraCase	363-1	Configuration-Import JIRA Case
Add Data	/config/afterInterceptor	362-2	Configuration-After Interceptor

Category	URL	ID	Description
Add Data	/config/getJobStatusList	362-0	Configuration-Get List of Job Status
Add Data	/config/isValidConfiguation	361-9	Configuration-Check if Configuration is Valid
Add Data	/config/saveSamlDetails	361-8	Configuration-Save SAML Details
Add Data	/config/showSystemAddAction	361-7	Configuration-Show System Add Action
Add Data	/config/saveMetdataConfig	361-6	Configuration-Save Metadata Configuration
Add Data	/config/isDirectoryValid	363-7	Configuration-Check if Directory is Valid
Add Data	/config/checkPrivacyMasterRole	363-8	Configuration-Check Role in Privacy Master
Add Data	/config/checkMaskingConfig	363-9	Configuration-Check Masking Configuration
Add Data	/config/changeLineFilterOrder	362-1	Configuration-Change Order of Line Filter
Add Data	/config/uploadFile	365-3	Configuration-Upload File
Add Data	/config/previewResourceRiskLevels	363-2	Configuration-Preview Risk Levels for Resources

Category	URL	ID	Description
Add Data	/config/scheduleLookupImport	363-5	Configuration-Schedule Lookup Import
Add Data	/config/adminaccess	358-8	Configuration-Show Administrative Access
Add Data	/config/showAllJobs	199-4	Configure-Tasks [shows list of all jobs]
Add Data	/config/deleteJob	199-5	Configure-Tasks [delete job]
Add Data	/manageData/beforeInterceptor	413-5	Manage Data-Before Interceptor
Add Data	/manageData/listAddUsersToProfile	414-4	Manage Data-List Add Users To Profile
Add Data	/manageData	414-3	Manage Data
Add Data	/manageData/showProfileResourceAccessLevel2	414-2	Manage Data-Show Profile Resource Access Level2
Add Data	/manageData/afterInterceptor	414-1	Manage Data-After Interceptor
Add Data	/config/scheduleMetadataImport	363-3	Configuration-Schedule Metadata Import
Add Data	/manageData/isResourceGroupNameDuplicate	414-0	Manage Data-Check if Resource Group Name is Duplicate

Category	URL	ID	Description
Add Data	/manageData/searchProfilesAJAX	413-8	Manage Data-Search Profiles using AJAX
Add Data	/manageData/getUpdatedToken	413-7	Manage Data-Get Updated Token
Add Data	/manageData/isNameDuplicate	413-6	Manage Data-Check if Name is Duplicate
Add Data	/config/savejsecUser	376-8	Configuration-Save Jsec User
Add Data	/config/resetSystemWorkflow	376-6	Configuration-Reset System Workflow
Add Data	/peer/showUsersWithoutAccessForOutliers	422-6	Peer-Show Users Without Access For Outliers
Add Data	/config/getPolicyMasterForSelectedType	376-5	Configuration-Get Policy Master For Selected Type
Add Data	/config/testDbConnection	363-6	Configuration-Test DB Connection
Add Data	/manageData/showProfileResourceAccessLevel3	413-9	Manage Data-Show Profile Resource Access Level3
Add Data	/config/saveAction	366-3	Configuration-Save Action
Add Data	/config/controlNode	363-4	Configuration-Control Node

Category	URL	ID	Description
Add Data	/config/saveSystemWorkflow	366-1	Configuration-Save System Workflow
Add Data	/config/getUpdatedToken	358-6	Configuration-Get Updated Token
Add Data	/config/getDecryptedUserValues	358-5	Configuration-Get Decrypted Values for Users
Add Data	/config/setAudit	358-4	Configuration-Set Audit
Add Data	/config/saveDownloadFiles	358-3	Configuration-Save Downloaded Files
Add Data	/config/deleteData	358-2	Configuration-Delete Data
Add Data	/config/checkDataToDecrypt	358-1	Configuration-Check Data to Decrypt
Add Data	/config/previewUserRiskLevels	358-0	Configuration-Preview User Risk Levels
Add Data	/config/scheduleGenerateUserCasesJob	357-7	Configuration-Schedule Generate User Cases Job
Add Data	/config/getSchedules	358-7	Configuration-Get Schedules
Add Data	/config/showScheduleHostnameLookup	358-9	Configuration-Schedule Hostname Lookup

Category	URL	ID	Description
Add Data	/config/getEncryptedUserValues	357-5	Configuration-Get Values for Encrypted User
Add Data	/config/uploadLicense	357-4	Configuration-Upload License
Add Data	/config/showSavedJobs	357-3	Configuration-Show Saved Jobs
Add Data	/config/getFileName	357-2	Configuration-Get File Name
Add Data	/config/testLdapConnection	357-1	Configuration-Test LDAP Connection
Add Data	/config/updateIDPMetadata	366-2	Configuration-Update IDP Metadata
Add Data	/config/showWorkflowDetails	356-9	Configuration-Show Workflow Details
Add Data	/config/showGenerateUserCases	357-0	Configuration-Show Generate User Cases
Add Data	/config/downloadAttachment	357-6	Configuration-Download Attachment
Add Data	/config/encryptData	357-8	Configuration-Encrypt Data
Add Data	/config/activateKey	357-9	Configuration-Activate Key

Category	URL	ID	Description
Add Data	/config/showGeolImportConfig	361-4	Configuration-Show Configuration for Geolocation Import
Add Data	/config/getMetadataAsString	365-9	Configuration-Get Metadata as String
Add Data	/config/deleteStatus	365-7	Configuration-Delete Status
Add Data	/config/showMaskingJobDetails	361-3	Configuration-Show Job Details for Masking
Add Data	/config/jsecUsers	366-0	Configuration-Jsec Users
Add Data	/config/isEmailTemplateNameDuplicate	365-6	Configuration-Check if Email Template Name is Duplicate
Add Data	/config/testRemoteConnection	365-5	Configuration-Test Remote Connection
Add Data	/config/showRegisterUser	365-4	Configuration-View Register user
Add Data	/config/scheduleIdxServiceJob	365-2	Configuration-Schedule Indexing Service Job

Category	URL	ID	Description
Add Data	/config/saveNetworkClassificationImportConfig	365-1	Configuration-Save Import Configuration for Network Classification
Add Data	/config/deleteWorkflowIns	365-0	Configuration-Delete Workflow Lines
Add Data	/config/showScheduleNetClassificationImportJob	364-0	Configuration-Show Schedule Import Job for Network Classification
Add Data	/config/previewActivityRiskLevels	364-2	Configuration-Preview Activity Risk Levels
Add Data	/config/userSearchAjax	364-8	Configuration-Search User through AJAX
Add Data	/config/isduplicatenodehttpurl	364-6	Configuration-Check if Node HTTP-URL is Duplicate
Add Data	/config/showMetadataImportJob	364-5	Configuration-Show Metadata Import Job
Add Data	/config/checkForEncryptedData	364-3	Configuration-Check for Encrypted Data
Add Data	/config/saveMaskingSetting	364-9	Configuration-Save Settings for Masking

Category	URL	ID	Description
Add Data	/config/scheduleNetworkClassificationImport	364-1	Configuration-Schedule Import Job for Network Classification
Add Data	/config/showJobDetails	361-5	Configuration-Show Job Details
Analytics	/suspectActivities/loadPGOutliersAttrs	347-4	Suspect Activities-Load PG Outliers Attributes
Analytics	/suspectActivities/showUsersWithoutAccessByJobId	349-7	Suspect Activities-Show Users Without Access By Job-Id
Analytics	/suspectActivities/showResourcesForBehaviorBasedOutliers	347-3	Suspect Activities-Show Resources For Behavior Based Outliers
Analytics	/suspectActivities/showSuspect	347-2	Suspect Activities-Show Suspect
Analytics	/suspectActivities/showConfigModes	346-9	Suspect Activities-Show Config Modes
Analytics	/suspectActivities/showPolicyManagement	347-0	Suspect Activities-Show Policy Management
Analytics	/suspectActivities/showConfigureAccessOutlierJob	348-1	Suspect Activities-Show Configure Access Outlier Job
Analytics	/suspectActivities/runPolicy	347-5	Suspect Activities-Run Policy

Category	URL	ID	Description
Analytics	/suspectActivities/showConfigureActivityOutlierJob	347-1	Suspect Activities-Show Configure Activity Outlier Job
Analytics	/suspectActivities/showMessageDetails	347-6	Suspect Activities-Show Message Details
Analytics	/suspectActivities/beforeInterceptor	349-6	Suspect Activities-Before Interceptor
Analytics	/suspectActivities/saveChildPolicy	347-8	Suspect Activities-Save Child Policy
Analytics	/suspectActivities/isPolicyDuplicate	347-9	Suspect Activities-Check if Policy is Duplicate
Analytics	/suspectActivities/searchVariableOnGroupAJAX	340-2	Suspect Activities-Search Variable on Group AJAX
Analytics	/suspectActivities/showResourcesForActivityOutliers	348-0	Suspect Activities-Show Resources For Activity Outliers
Analytics	/suspectActivities/deletePolicyViolations	348-2	Suspect Activities-Delete Policy Violations
Analytics	/suspectActivities/showAddChecksDialog	348-3	Suspect Activities-Show Add Checks Dialog
Analytics	/suspectActivities/updateIncludeInAnalysisForActivityAttributes	348-4	Suspect Activities-Update Include In Analysis For Activity Attributes
Analytics	/suspectActivities/showWIList	349-8	Suspect Activities-Show WI List

Category	URL	ID	Description
Analytics	/suspectActivities/checkvaliddirective	348-5	Suspect Activities-Check Valid Directive
Analytics	/suspectActivities/showManageSuspectActivities	348-6	Suspect Activities-Show Manage Suspect Activities
Analytics	/suspectActivities/loadSuspectActivitiesQueueChart	347-7	Suspect Activities-Load Suspect Activities Queue Chart
Analytics	/suspectActivities/showFunctionConfig	349-9	Suspect Activities-Show Function Config
Analytics	/resource/showEntityDetailsForActivityOutliers	458-3	Show resource entity details for activity outliers
Analytics	/suspectActivities/showRunPolicy	194-5	Detect-Policy Violations[show run policy screen]
Analytics	/suspectActivities/savePolicyCategory	348-7	Suspect Activities-Save Policy Category
Analytics	/suspectActivities/showEditHqlPolicy	350-4	Suspect Activities-Show Edit HQL Policy
Analytics	/suspectActivities/addCustomCheck	350-5	Suspect Activities-Add Custom Check
Analytics	/suspectActivities/showAddOwnerRemediator	340-1	Suspect Activities-Show Add Owner Remediator

Category	URL	ID	Description
Analytics	/suspectActivities/resourceGroupBasedPolicies	459-3	Display resource group based policies for suspect activities
Analytics	/resource/showEntitiesWithActivityByJobId	458-4	Show resource entities with activity by job id
Analytics	/resource/showEntitiesWithoutActivityByJobId	458-2	Show resource entities with activity by job id
Analytics	/activityIP/showEntitiesWithoutActivityByJobId	458-1	Show activity ip entities without activity by job id
Analytics	/activityIP/showEntityDetailsForActivityOutliers	458-0	Show activity ip entity details for activity outliers
Analytics	/activityIP/showEntitiesWithActivityByJobId	457-9	Show activity ip entities with activity by job id
Analytics	/suspectActivities/searchPolicyJobAJAX	340-0	Suspect Activities-Search Policy Job through AJAX
Analytics	/suspectActivities/getAllColumns	457-2	Show all columns for Suspect activities
Analytics	/suspectActivities/showAccessOutlierJobs	193-3	Analytics-Access Outliers Jobs
Analytics	/suspectActivities/showResourcesForAccessOutliers	193-5	Detect-Access Outliers[shows resources for access outliers]

Category	URL	ID	Description
Analytics	/suspectActivities/scheduleAnomalyDetectionJob	193-6	Detect-Access Outliers-Schedule Access Outliers Job[shows create access outlier job screen]
Analytics	/suspectActivities/runAccessOutlierJob	193-7	Detect-Access Outliers-Schedule Access Outliers Job[schedule access outlier job]
Analytics	/suspectActivities/detectSuspect	193-8	Detect-Activity Outliers-Schedule Activity Outliers Job[shows create activity outlier job screen]
Analytics	/suspectActivities/runActivityOutlierJob	193-9	Detect-Activity Outliers-Schedule Activity Outliers Job[schedule activity outlier job]
Analytics	/suspectActivities/showSavedPolicies	194-0	Detect-Policy Violations[shows list policies]
Analytics	/suspectActivities/showCreatePolicy	194-1	Detect-Policy Violations-Create Policy [shows create policy screen]

Category	URL	ID	Description
Analytics	/suspectActivities/showCreateHQLPolicy	194-2	Detect-Policy Violations-Create Policy With Direct HQL[shows create policy Direct HQL screen]
Analytics	/suspectActivities/savePolicy	194-3	Detect-Policy Violations[save values for policy recieved from create policy screen]
Analytics	/suspectActivities/showEditPolicy	194-4	Detect-Policy Violations[shows edit policy screen]
Analytics	/suspectActivities/showCasesPanel	194-6	Respond-Incidents-Assigned To Me/Assigned To Group[shows casses assigned]
Analytics	/suspectActivities/showPeerGroupBasedJobWizard	348-8	Suspect Activities-Show Peer Group Based Job Wizard
Analytics	/analytics/showTrasactionLevels	320-6	Analytics-Show Trasaction Levels
Analytics	/suspectActivities/showEditCompositePolicy	349-0	Suspect Activities-Show Edit Composite Policy
Analytics	/analytics/saveBehDefaultConfig	318-6	Analytics-Save Behavior Default Configuration
Analytics	/analytics/showUserDetails	318-5	Analytics-Show User Details

Category	URL	ID	Description
Analytics	/analytics/listUsers	318-4	Analytics-Show Users
Analytics	/analytics/showConfig	318-3	Analytics-Show Configuration
Analytics	/analytics/showBehaviorProfileConfig	318-2	Analytics-Show Behavior Profile Configuration
Analytics	/analytics/searchActivityTransactionAJAX	318-1	Analytics-Search Activity Transaction
Analytics	/reviews/showReviews	316-4	Respond-Activity Review-[Shows List of Activity Review Jobs with filters]
Analytics	/analytics/listUsersWithProfiles	320-0	Analytics-List all Users with Profiles
Analytics	/analytics/getResources	320-1	Analytics-Get Resources
Analytics	/analytics/showDashboard	320-2	Analytics-Show Dashboard
Analytics	/suspectActivities/saveAccessOutliers	336-9	Suspect Activities-Save Access Outliers
Analytics	/certifications/showAccessReviewJobs	321-8	Certifications-Show Access Review Jobs
Analytics	/analytics/scheduleBehaviorProfileJob	320-7	Analytics-Schedule Behavior Profile Job

Category	URL	ID	Description
Analytics	/analytics/showUserSuspect	320-8	Analytics-Show User Suspect Analysis
Analytics	/analytics/behaviorProfileJobs	320-9	Analytics-Show Behavior Profile Jobs
Analytics	/analytics/selectedUsers	321-0	Analytics-Show Selected Users
Analytics	/analytics/showAccountSelectionDialog	321-1	Analytics-Show Account Selection Dialog
Analytics	/analytics/showJobStatus	321-2	Analytics-Show Job Status
Analytics	/analytics/	321-3	Analytics
Analytics	/analytics/updateIncludeInAnalysisForActivityAttributes	321-4	Analytics-Update Include In Analysis For Activity Attributes
Analytics	/analytics/manageProfiles	321-5	Analytics-Manage Profiles
Analytics	/analytics/showManageSuspectActivities	321-6	Analytics-Show and Manage Suspect Activities
Analytics	/suspectActivities/showManageUserBehavior	350-3	Suspect Activities-Show Manage User Behavior
Analytics	/suspectActivities/reloadAutoComplete	336-8	Suspect Activities-Reload Auto Complete

Category	URL	ID	Description
Analytics	/suspectActivities/showMultiEditPolicy	336-7	Suspect Activities-Show Multi Edit Policy
Analytics	/suspectActivities/showUserDetailsForActivityOutliers	336-6	Suspect Activities-Show User Details For Activity Outliers
Analytics	/suspectActivities/showLevelChecks	349-1	Suspect Activities-Show Level Checks
Analytics	/suspectActivities/searchVariableAJAX	349-2	Suspect Activities-Search Variable through AJAX
Analytics	/suspectActivities/showUserRiskDetails	349-3	Suspect Activities-Show User Risk Details
Analytics	/suspectActivities/showUserSuspect	349-4	Suspect Activities-Show User Suspect
Analytics	/suspectActivities/saveTier2Policy	349-5	Suspect Activities-SaveTier2 Policy
Analytics	/suspectActivities/saveOutlierPoliciesAsDefaultPolicyTemplate	345-7	Suspect Activities-Save Outlier Policies As Default Policy Template
Analytics	/suspectActivities/showVariableSelection	337-5	Suspect Activities-Show Variable Selection
Analytics	/suspectActivities/getSysData	337-1	Suspect Activities-Get System Data

Category	URL	ID	Description
Analytics	/monitor/showAccessReviewJobs	304-6	Detect-Access Reviews
Analytics	/analytics	319-9	Enable Analytics View
Analytics	/analytics/getBehaviorNames	319-8	Analytics-Get Behavior Names
Analytics	/analytics/getUpdatedToken	319-7	Analytics-Get Updated Token
Analytics	/analytics/showResourceProfileAndWindows	319-6	Analytics-Show Resource Profile and Windows
Analytics	/analytics/saveBPConfig	319-4	Analytics-Save Behavior Profile Config
Analytics	/analytics/showActivityAttributes	319-3	Analytics-Show Activity Attributes
Analytics	/analytics/updateIncludeInAnalysisForTransactionLevels	319-2	Analytics-Update Include in Analysis For Transaction Levels
Analytics	/analytics/beforeInterceptor	319-1	Analytics-Call Before Interceptor
Analytics	/analytics/getDateTime	319-0	Analytics-Get Date and Time
Analytics	/analytics/showAddUsersDialog	318-9	Analytics-Show Add User Dialog
Analytics	/analytics/showAnalytics	318-8	Analytics-Show Analytics

Category	URL	ID	Description
Analytics	/analytics/showManageUserBehavior	318-7	Analytics-Show Manage User Behavior
Analytics	/suspectActivities/searchAttributeValue	336-4	Suspect Activities-Search Attribute Value
Analytics	/suspectActivities/getPolicyFunctions	336-5	Suspect Activities-Get All Policy Functions
Analytics	/suspectActivities/saveCompositePolicy	348-9	Suspect Activities-Save Composite Policy
Analytics	/suspectActivities/saveThreatIndicator	350-2	Suspect Activities-Save Threat Indicator
Analytics	/suspectActivities/detectAnomalies	340-5	Suspect Activities-Detect Anomalies
Analytics	/suspectActivities/showSuspectEvents	350-0	Suspect Activities-Show Suspect Events
Analytics	/suspectActivities/showSuspectChecks	339-3	Suspect Activities-Show Suspect Checks Activities
Analytics	/suspectActivities/saveSuspectPolicy	337-2	Suspect Activities-Save Suspect Policy
Analytics	/suspectActivities/listUsers	339-4	Suspect Activities-List all Users
Analytics	/suspectActivities/createCompositePolicy	339-5	Suspect Activities-Create Composite Policy

Category	URL	ID	Description
Analytics	/monitor/showBehaviorProfileJobs	194-9	Detect-Behavior
Analytics	/suspectActivities/getEntitiesList	339-7	Suspect Activities-Get Entities List
Analytics	/suspectActivities/getUpdatedToken	339-8	Suspect Activities-Get Updated Token
Analytics	/monitor/showPolicyManagement	195-0	Detect-Policy Violations
Analytics	/suspectActivities/showAccessOutliers	193-4	Detect-Access Outliers[shows access outliers]
Analytics	/monitor/showActivityOutlierJobs	194-8	Detect-Activity Outliers
Analytics	/suspectActivities/showDirectiveDetails	339-2	Suspect Activities-Show Directive Details
Analytics	/suspectActivities/savePgBasedOutlierPolicy	346-6	Suspect Activities-Save Pg-Based Outlier Policy
Analytics	/suspectActivities/showUserDetailsForAccessOutliers	341-3	Suspect Activities-Show User Details For Access Outliers
Analytics	/suspectActivities/updatePolicies	341-2	Suspect Activities-Update Policies
Analytics	/suspectActivities/showAllPolicyJobs	341-1	Suspect Activities-Show All Policy Jobs

Category	URL	ID	Description
Analytics	/suspectActivities/updatePolicyAttributes	341-0	Suspect Activities-Update Policy Attributes
Analytics	/suspectActivities/showAssignToUsers	344-7	Suspect Activities-Show Assign to Users
Analytics	/suspectActivities/searchPoliciesAJAX	344-8	Suspect Activities-Search Policies AJAX
Analytics	/suspectActivities/showSuspectPoliciesList	344-9	Suspect Activities-Show Suspect Policies List
Analytics	/suspectActivities/chkForSqlClauses	345-0	Suspect Activities-Check For SQL Clauses
Analytics	/suspectActivities/showSuspectExclusionRules	345-1	Suspect Activities-Show Suspect Exclusion Rules
Analytics	/suspectActivities/getNonCompositePolicies	345-2	Suspect Activities-Get Non Composite Policies
Analytics	/suspectActivities/displayAllAttributeValues	341-4	Suspect Activities-Display All Attribute Values
Analytics	/suspectActivities/saveThreatIndicatorGeneric	345-3	Suspect Activities-Save Threat Indicator Generic
Analytics	/suspectActivities/showDatasourceList	339-1	Suspect Activities-Show Data-sources List

Category	URL	ID	Description
Analytics	/suspectActivities/saveWatchList	338-9	Suspect Activities-Save Watch List
Analytics	/analytics/loadSearchBar	320-5	Analytics-Load Analytics Search Bar
Analytics	/suspectActivities/saveSCBasedOutlierPolicy	337-3	Suspect Activities-Save SC Based Outlier Policy
Analytics	/reviews/showActivityReviewWizard	195-6	Respond-Activity Reviews[shows list of activity review table]
Analytics	/reviews/activityReviewsList	195-5	Respond-Activity Reviews[shows list of activity review]
Analytics	/analytics/generateProfiles	195-2	Detect-Behavior-Schedule Behavior Profile Job [shows schedule behavior profile screen]
Analytics	/analytics/showJobsForBehaviorProfiles	195-1	Detect-Behavior [shows list of behavior job]
Analytics	/incidents/showCaseManagement	195-3	Respond-Incidents
Analytics	/suspectActivities/showActivityOutliersJobs	339-6	Suspect Activities-Show Activity Outliers Jobs

Category	URL	ID	Description
Analytics	/reviews/createActivityReview	195-7	Respond-Activity Reviews[shows create activity review screen]
Analytics	/suspectActivities/getDateTime	338-7	Suspect Activities-Get Date and Time
Analytics	/suspectActivities/assignToUserList	339-0	Suspect Activities-Assign to Users List
Analytics	/suspectActivities/saveQuickAlertPolicy	337-6	Suspect Activities-Save Quick Alert Policy
Analytics	/suspectActivities/listUsersForOwnerRemediator	337-8	Suspect Activities-List Users For Owner Remediator
Analytics	/suspectActivities/showPreviewPolicyResults	337-9	Suspect Activities-Show Preview Policy Results
Analytics	/suspectActivities/showEditTier2Policy	338-0	Suspect Activities-Show Edit Tier 2 Policy
Analytics	/suspectActivities/showSuspectCheckDetails	338-1	Suspect Activities-Show Suspect Check Details
Analytics	/suspectActivities/showBehaviorBasedOutliersJobStatus	338-2	Suspect Activities-Show Behavior Based Outliers Job Status

Category	URL	ID	Description
Analytics	/suspectActivities/saveRiskTypeGeneric	338-3	Suspect Activities-Save Risk Type Generic Activities
Analytics	/suspectActivities/getChildPolicies	338-5	Suspect Activities-Get Policies on Child Nodes
Analytics	/suspectActivities/showUsersWithoutActivityByJobId	338-6	Suspect Activities-Show Users Without Activity By JobId
Analytics	/suspectActivities/getSolrObjectattrsForPolicy	338-8	Suspect Activities-Get Solr Object Attributes For Policy
Analytics	/suspectActivities/saveDirectiveDetails	339-9	Suspect Activities-Save Directive Details
Analytics	/suspectActivities/showAddThreatIndicator	337-7	Suspect Activities-Show Add Threat Indicator
Analytics	/suspectActivities/getWatchlistEntitiesList	345-4	Suspect Activities-Get Watchlist Entities List
Analytics	/suspectActivities/showActivityOutlierDetailsForUserByJobId	345-5	Suspect Activities-Show Activity Outlier Details For User By Job-Id
Analytics	/suspectActivities/showEditQuickAlertPolicy	345-6	Suspect Activities-Show Edit Quick Alert Policy

Category	URL	ID	Description
Analytics	/suspectActivities/showDashboard	342-9	Suspect Activities-Show Dashboard
Analytics	/suspectActivities/showActivityOutliers	343-0	Suspect Activities-Show Activity Outliers
Analytics	/suspectActivities/saveAsDefaultPolicyTemplate	343-1	Suspect Activities-Save As Default Policy Template
Analytics	/suspectActivities/addChecksFromLevel	343-3	Suspect Activities-Add Checks From Level
Analytics	/suspectActivities/getDeviationFieldsForPolicy	341-7	Suspect Activities-Get Deviation Fields For Policy
Analytics	/suspectActivities/showActivityOutliersJobStatus	343-4	Suspect Activities-Show Activity Outliers Job-Status
Analytics	/suspectActivities/getColumns	343-5	Suspect Activities-Get Columns
Analytics	/suspectActivities/updateCase	343-6	Suspect Activities-Update Case
Analytics	/suspectActivities/showAccessOutliersJobStatus	343-7	Suspect Activities-Show Access Outliers Job-Status
Analytics	/suspectActivities/showOutputFieldMapping	343-8	Suspect Activities-Show Output Field Mapping
Analytics	/suspectActivities/showAddRiskType	342-8	Suspect Activities-Show Add Risk Type

Category	URL	ID	Description
Analytics	/suspectActivities/advancedSearchAddUser	343-9	Suspect Activities-Advanced Search Add User
Analytics	/suspectActivities/showEditChildPolicy	344-1	Suspect Activities-Show Edit Child Policy
Analytics	/suspectActivities/saveCaseCustomValues	344-2	Suspect Activities-Save Case Custom Values
Analytics	/suspectActivities/assignToUser	341-8	Suspect Activities-Assign to User
Analytics	/suspectActivities	344-3	Suspect Activities
Analytics	/suspectActivities/showUsersWithAccessByJobId	344-4	Suspect Activities-Show Users With Access By Job-Id
Analytics	/suspectActivities/getResources	344-5	Suspect Activities-Get Resources
Analytics	/suspectActivities/saveActivityOutliers	346-5	Suspect Activities-Save Activity Outliers
Analytics	/suspectActivities/showPolicyJobStatus	346-7	Suspect Activities-Show Policy Job-Status
Analytics	/monitor/showAccessOutlierJobs	194-7	Detect-Access Outliers
Analytics	/suspectActivities/showOutlierDetailsForUserByJobId	346-8	Suspect Activities-Show Outlier Details For User By Job-Id

Category	URL	ID	Description
Analytics	/suspectActivities/saveAccessOutlierConfig	344-0	Suspect Activities-Save Access Outlier Config
Analytics	/suspectActivities/deletePolicy	342-7	Suspect Activities-Delete Policy
Analytics	/suspectActivities/showAddUsersDialog	342-6	Suspect Activities-Show Add Users Dialog
Analytics	/suspectActivities/showPolicyJobDetails	342-5	Suspect Activities-Show Policy Job Details
Analytics	/suspectActivities/showGraph	340-9	Suspect Activities-Show Graph
Analytics	/suspectActivities/showSuspectChecksBasedJobWizard	345-8	Suspect Activities-Show Suspect Checks Based Job Wizard
Analytics	/suspectActivities/showQuickAlertPolicy	345-9	Suspect Activities-Show Quick Alert Policy
Analytics	/suspectActivities/showUsersWithActivityByJobId	340-8	Suspect Activities-Show Users With Activity By JobId
Analytics	/suspectActivities/showClosedCaseDetails	340-7	Suspect Activities-Show Closed Case Details
Analytics	/suspectActivities/showActivityOutliersByJob	340-6	Suspect Activities-Show Activity Outliers By Job

Category	URL	ID	Description
Analytics	/suspectActivities/getResourceAttributes	346-0	Suspect Activities-Get Resource Attributes
Analytics	/suspectActivities/getFunctionParams	346-1	Suspect Activities-Get Function Params
Analytics	/suspectActivities/selectedUsers	346-2	Suspect Activities-Selected Users
Analytics	/suspectActivities/getSubTreeItems	340-4	Suspect Activities-Get Sub Tree Items
Analytics	/suspectActivities/previewPolicyResults	340-3	Suspect Activities-Preview Policy Results
Analytics	/suspectActivities/saveHQLPolicy	346-3	Suspect Activities-Save HQL Policy
Analytics	/suspectActivities/updateTaskStatus	346-4	Suspect Activities-Update Task Status
Analytics	/suspectActivities/searchPolicyJob	341-5	Suspect Activities-Search Policy Job
Analytics	/suspectActivities/showAllJobsForPolicy	341-6	Suspect Activities-Show All Jobs For Policy
Analytics	/suspectActivities/showCreateTier2Policy	344-6	Suspect Activities-Show Create Tier 2 Policy
Analytics	/suspectActivities/showBehaviorBasedOutliers	343-2	Suspect Activities-Show Behavior Based Outliers

Category	URL	ID	Description
Analytics	/suspectActivities/showAllJobsOfPolicy	342-2	Suspect Activities-Show All Jobs of Policy
Analytics	/suspectActivities/showConfig	342-1	Suspect Activities-Show Configuration
Analytics	/suspectActivities/	342-3	Show Suspect Activities
Analytics	/suspectActivities/getSuspectChecksList	342-0	Suspect Activities-Get Suspect Checks List
Analytics	/suspectActivities/saveActivityOutlierConfig	341-9	Suspect Activities-Save Activity Outlier Configuration
Analytics	/suspectActivities/showAccessOutliersByJob	342-4	Suspect Activities-Show Access Outliers By Job
Analytics	/suspectActivities/createCompositeChildPolicy	350-1	Suspect Activities-Create Composite Child Policy
Analytics	/suspectActivities/removeChecksFromLevel	338-4	Suspect Activities-Remove Checks From Level
Analytics	/analytics/reloadAutoComplete	320-3	Analytics-Reload Auto Complete
Analytics	/monitor/beforeInterceptor	325-2	Monitor-Before Interceptor
Analytics	/activityIP/list	406-3	Activity IP-Show List

Category	URL	ID	Description
Analytics	/activityIP/showBehaviorActivityDetails	406-4	Activity IP-Show Behavior Activity Details
Analytics	/activityIP/showBehavior	406-5	Activity IP-Show Behavior
Analytics	/activityIP/saveActivityOutlierPolicy	406-6	Activity IP-Save Activity Outlier Policy
Analytics	/activityIP/showActivityOutlierDetailsForActivityIPByJobId	406-7	Activity IP-Show Activity Outlier Details For Activity IP By Job-Id
Analytics	/activityIP/	406-8	Show Activity IP
Analytics	/activityIP/showActivityOutliers	406-2	Activity IP-Show Activity Outliers
Analytics	/activityIP/getActivityIPList	407-0	Activity IP-Get Activity IP List
Analytics	/activityIP/showActivityOutliersByJob	407-2	Activity IP-Show Activity Outliers By Job
Analytics	/suspectActivities/showOpenCaseDetails	337-0	Suspect Activities-Show Open Case Details
Analytics	/activityIP/showResourcesForActivityOutliers	405-5	Activity IP-Show Resources For Activity Outliers
Analytics	/activityIP/showResourceBehaviorSummary	405-8	Activity IP-Show Resource Behavior Summary

Category	URL	ID	Description
Analytics	/suspectActivities/getObjectAttributesForPolicy	337-4	Suspect Activities-Get Object Attributes For Policy
Analytics	/analytics/isScheduleJobNameDuplicate	320-4	Analytics-Check for Duplicate Schedule Names
Analytics	/activityIP/showActivityOutliersJobStatus	407-1	Activity IP-Show Activity Outliers Job-Status
Analytics	/activityIP/listActivityIPClassifications	406-1	Activity IP-List of Activity IP Classifications
Analytics	/activityIP	407-3	Enable Activity IP View
Analytics	/activityIP/showBehaviorConfig	405-9	Activity IP-Show Behavior Configuration
Analytics	/activityIP/searchAJAX	406-0	Activity IP-Search through AJAX
Analytics	/monitor	325-4	Enable Analytics
Analytics	/monitor/	325-5	Monitor
Analytics	/reviews/beforeInterceptor	334-5	Reviews-Before Interceptor
Analytics	/reviews	334-6	Analytics-Reviews
Analytics	/reviews/getUpdatedToken	334-7	Reviews-Get Updated Token

Category	URL	ID	Description
Analytics	/reviews/showActivityReviews	334-8	Reviews-Show Activity Reviews
Analytics	/monitor/afterInterceptor	325-3	Monitor-After Interceptor
Analytics	/reviews/	335-0	Reviews
Analytics	/riskModeler/showRiskModeler	307-9	Configure-Threat Model-Show Threat Model List
Analytics	/reviews/showDashboard	334-9	Reviews-showDashboard
Analytics	/analytics/advancedSearchAddUser	319-5	Analytics-Advance User Add Search
Analytics	/activityIP/saveActivityOutliers	406-9	Activity IP-Save Activity Outliers
Analytics	/activityIP/showUserDetailsForActivityOutliers	405-4	Activity IP-Show User Details For Activity Outliers
Analytics	/activityIP/showActivityOutliersJobWizard	405-6	Activity IP-Show Activity Outliers Job Wizard
Analytics	/activityIP/getUpdatedToken	405-7	Activity IP-Get Updated Token
Application Statistics	/stats/terminateQuery	384-1	Application Statistics-Terminate Query
Application Statistics	/stats/applicationStatistics	384-0	Show Application Statistics

Category	URL	ID	Description
Application Statistics	/stats	384-3	Application Statistics
Application Statistics	/stats/	384-2	Show Statistics View
Configure	/settings/addHolidays	382-9	Settings-Add Holidays
Configure	/clustering	356-4	Enable Clustering View
Configure	/settings/uninstallLicense	382-7	Settings-Uninstall License
Configure	/settings/installLicense	383-3	Settings-Install License
Configure	/settings/showHouseKeeping	383-2	Settings-Show HouseKeeping
Configure	/settings/holidays	383-5	Settings-Holidays
Configure	/settings/showSyslogSettings	383-1	Settings-Show Syslog Settings
Configure	/settings/saveSafeDomains	383-0	Settings-Save Safe Domains
Configure	/settings/showAddHolidaysDialog	382-8	Settings-Add Holidays Dialog
Configure	/connectionType/editConnector	378-7	Connection Type-Edit Connector
Configure	/settings/showModuleList	196-5	Configure-Logging-Modules [shows list of modules]

Category	URL	ID	Description
Configure	/config/showCreateWorkflow	365-8	Configuration-Show Create Workflow
Configure	/connectionType/deleteClientSecret	378-2	Connection Type-Delete Client Secret
Configure	/connectionType/testSplunkConnection	378-8	Connection Type-Test Splunk Connection
Configure	/connectionType/showConnectionProperties	378-6	Connection Type-Show Connection Properties
Configure	/connectionType	378-5	Configure Connection Type
Configure	/connectionType/uploadSecret	378-4	Connection Type-Upload Secret
Configure	/connectionType/displayConnectors	378-3	Connection Type-Display Connectors
Configure	/settings/showHouseKeepingJobs	383-6	Settings-Show HouseKeeping Jobs
Configure	/settings/removeHolidaysFromYear	380-9	Settings-Remove Holidays From Year
Configure	/settings/	383-7	Enable Settings View
Configure	/settings/syslogConf	382-2	Settings-Syslog Configuration

Category	URL	ID	Description
Configure	/settings/saveUserPreferencesOfMenus	383-9	Settings-Save User Preferences Of Menus
Configure	/settings/saveArchiveSettings	381-7	Settings-Save Archive Settings
Configure	/settings/showLdapAuthenSettings	382-3	Settings-Show LDAP Authentication Settings
Configure	/connectionType/index	378-1	Show Connection Type
Configure	/settings/index	382-1	Display Settings
Configure	/settings/saveLdapAuthenSettings	382-0	Settings-Save LDAP Authentication Settings
Configure	/settings/scheduleHouseKeepingJob	381-9	Settings-Schedule HouseKeeping Job
Configure	/settings/showEncryptDecryptText	381-8	Settings-Show Encryption Decryption Text
Configure	/settings/saveproductdescription	381-6	Settings-Save Product Description
Configure	/settings/saveSyslogProperties	382-5	Settings-Save Syslog Properties
Configure	/settings/controlSyslog	383-8	Settings-Control Syslog
Configure	/settings/beforeInterceptor	381-5	Settings-Before Interceptor

Category	URL	ID	Description
Configure	/settings/getUpdatedToken	381-3	Settings-Get Updated Token
Configure	/settings/saveDNSServers	381-2	Settings-Save DNS Servers
Configure	/settings/showArchival	381-1	Settings-Show Archival Settings
Configure	/settings/showLicDetails	381-0	Settings-Show Installed License Details
Configure	/settings/deleteSmtp	382-4	Settings-Delete SMTP
Configure	/settings/removeYearFromHolidaySettings	382-6	Settings-Remove Year From Holiday Settings
Configure	/settings/testSmtpServer	380-8	Settings-Test SMTP Server
Configure	/settings	383-4	Show Settings
Configure	/settings/saveSystemConfiguration	196-3	Configure-System [saves system configuration]
Configure	/settings/saveAppSettings	381-4	Settings-Save Application Settings
Configure	/connectionType/	379-0	Connection Type
Configure	/email/queuedMailsList	379-7	Email Template-Queued Mails List
Configure	/connectionType/getOauthTokens	377-9	Connection Type-Get Oauth Tokens

Category	URL	ID	Description
Configure	/certifications	323-0	Certifications
Configure	/connectionType/authenticateApi	459-4	Allow api authentication for connection types
Configure	/certifications/getResourcesForCertification	321-7	Certifications-Get Resources For Certification
Configure	/certifications/saveManualCertOutliers	321-9	Certifications-Save Manual Cert Outliers
Configure	/certifications/runCertificationJob	322-0	Certifications-Run Certification Job
Configure	/certifications/scheduleCertificationJob	322-1	Certifications-Schedule Certification Job
Configure	/certifications/showCertJobStatus	322-2	Certifications-Show Certifications Job Status
Configure	/certifications/showManualCertUsersByJob	322-3	Certifications-Show Manual Certification Users By Job
Configure	/certifications/showResourcesForManualCert	322-4	Certifications-Show Resources For Manual Certifications
Configure	/settings/testWS	459-6	Settings-Test web-socket

Category	URL	ID	Description
Configure	/certifications/	322-5	Enable Certifications View
Configure	/certifications/showCertConfiguration	322-7	Certifications-Show Certifications Configuration
Configure	/certifications/getUpdatedToken	322-8	Certifications-Get Updated Token
Configure	/certifications/showManualCertByJob	322-9	Certifications-Show Manual Certifications By Job
Configure	/config/showConfigureRiskLevels	196-7	Configure-Criticality
Configure	/connectionType/getGeneratedTokens	459-5	Allow token generation for connection types
Configure	/resource/getXMLDataController	455-9	Show XML data for resource group
Configure	/clustering/	356-7	Clustering
Configure	/clustering/autoUpdate	356-6	Clustering-Auto Update
Configure	/clustering/isNodeUpByPolicy	356-5	Clustering-Check by Policy of the Node is Up
Configure	/certifications/saveCertConfig	322-6	Certifications-Save Certifications Config

Category	URL	ID	Description
Configure	/connectionType/checkDBConnection	378-0	Connection Type- Check Database Connection
Configure	/email/getUpdatedToken	380-1	Email Template- Get Updated Token
Configure	/email/showEmailTemplateVariables	379-3	Email Template- Show Email Tem- plate Variables
Configure	/connectionType/generateOauthCode	377-8	Connection Type- Generate Oauth Code
Configure	/connectionType/getSplunkSavedSearches	377-7	Connection Type- Get Saved Searches from Splunk
Configure	/config/showWorkflowList	373-7	Configuration- ShowWork- flowList
Configure	/connectionType/beforeInterceptor	377-6	Connection Type- Before Interceptor
Configure	/connectionType/getUpdatedToken	379-1	Connection Type- Get Updated Token
Configure	/settings/showEncryptionMasking	380-7	Settings-Show Encryption Mask- ing Settings
Configure	/email/showEmailTemplatesList	197-2	Configure-Email Templates[shows list of email tem- plates]

Category	URL	ID	Description
Configure	/settings/showWeekEndDialog	380-6	Settings-Show Week End Settings Dialog
Configure	/settings/updateHolidayList	380-5	Settings-Update Holiday List
Configure	/settings/showSystemConfiguration	196-2	Configure-System
Configure	/email	380-4	Configure Email Template
Configure	/email/index	380-3	Show Email Template
Configure	/email/updateEmailQueue	380-2	Email Template-Update Email Queue
Configure	/email/beforeInterceptor	380-0	Email Template-Before Interceptor
Configure	/connectionType/filterConnections	379-2	Connection Type-Filter Connections
Configure	/email/deleteEmails	379-9	Email Template-Delete Emails
Configure	/email/	379-8	Enable Email
Configure	/clustering/manualSync	356-3	Clustering-Sync Nodes Manually
Configure	/email/editEmailTemplate	379-5	Email Template-Edit Email Template
Configure	/email/fetchMailBody	379-4	Email Template-Fetch Mail Body

Category	URL	ID	Description
Configure	/config/showThreatLibrary	370-9	Configuration-Show Threat Library
Configure	/clustering/beforeInterceptor	355-7	Clustering-Before Interceptor
Configure	/connectionType/regConnector	378-9	Connection Type-Register Connector
Configure	/accessControl/showEditUser	198-4	Configure-Access Control[show edit user screen]
Configure	/clustering/isNodeUpOnly	354-0	Clustering-Only Check if the Node is Up
Configure	/clustering/showEditNode	356-0	Clustering-Show Edit Node
Configure	/clustering/syncDatasource	355-9	Clustering-Sync Datasources
Configure	/clustering/authnticateNode	355-8	Clustering-Authenticate Node
Configure	/connectionType/getPolicyOutputConnections	377-5	Connection Type-Get Policy Output Connections
Configure	/clustering/forceHealthCheck	355-6	Clustering-Force Health Check
Configure	/clustering/showNodesWithStatus	355-5	Clustering-Show All Nodes with Status

Category	URL	ID	Description
Configure	/clustering/getNodeThreadConfig	355-4	Clustering-Get Configuration of Node Thread
Configure	/clustering/mergeDeleteNodeData	355-3	Clustering-Merge Data from Deleted Node
Configure	/clustering/removeResourcesFromNode	353-9	Clustering-Remove Selected Resources from the Node
Configure	/clustering/getUpdatedToken	355-2	Clustering-Get Updated Token
Configure	/clustering/showDatasourcesForNode	355-0	Clustering-Show List of Data-sources for Node
Configure	/clustering/showResourcesForNode	354-9	Clustering-Show List of Resources for Node
Configure	/clustering/deleteNode	354-8	Clustering-Delete Node
Configure	/clustering/showCreateNode	354-7	Clustering-Create Node
Configure	/clustering/isNodeUpByRg	354-6	Clustering-Check by Resource Group if the Node Status is Up
Configure	/accessControl/showUsersOfRole	352-7	Access Control-Show Users for Different Roles
Configure	/clustering/clusterNodeList	354-5	Clustering-View Cluster Nodes List

Category	URL	ID	Description
Configure	/clustering/toggleClustering	354-4	Clustering-Toggle Clustering On or Off
Configure	/clustering/showClusterNodeDetails	354-3	Clustering-Show Cluster Node Details
Configure	/clustering/showAddResourcesToNodeDialog	355-1	Clustering-Dialog for Add Resources to Node
Configure	/clustering/testNodeDbConnectionWithMaster	354-2	Clustering-Test Database Connection of Selected Node with Master
Configure	/uf/listUF	302-7	Configure-Universal Forwarder-Shows list of UF
Configure	/clustering/saveNodeThreadConfig	353-8	Clustering-Save the Thread Configuration of Node
Configure	/connectionType/addUpdateConnectionType	197-8	Configure-Connection Types [shows create/edit connection type screen]
Configure	/clustering/saveNode	356-1	Clustering-Save Node
Configure	/clustering/isNodeUp	353-2	Clustering-Identify if the Node is Running or not

Category	URL	ID	Description
Configure	/clustering/isNodeUpByName	353-6	Clustering-Check by Name if the Node is Up
Configure	/email/showEmailTemplates	197-1	Configure-Email Templates
Configure	/email/deleteEmailTemplate	197-3	Configure-Email Templates [deletes email template]
Configure	/email/createEmailTemplate	197-4	Configure-Email Templates[shows create email template screen]
Configure	/accessControl	352-9	Access Control
Configure	/email/saveEmailTemplate	197-5	Configure-Email Templates[save values for email template recieved from create/edit email template screen]
Configure	/clustering/manualSyncNode	353-7	Clustering-Sync the Node Manually
Configure	/accessControl/showAddUsersSearch	353-0	Access Control-Show Add Users Search

Category	URL	ID	Description
Configure	/accessControl/changePassword	198-3	Configure-Access Control[update password recieved from change password screen]
Configure	/connectionType/showConnectionTypes	197-6	Configure-Connection Types
Configure	/accessControl/showChangePassword	198-2	Configure-Access Control[shows change password screen]
Configure	/connectionType/saveConnectionTypes	197-9	Configure-Connection Types [save/update values of connection type recieved from create/edit screen]
Configure	/clustering/toggleNode	353-3	Clustering-Turn On or Turn Off the Node
Configure	/clustering/testNodeDbConnection	353-4	Clustering-Test the Connection of the Node Database
Configure	/connectionType/showConnectionList	197-7	Configure-Connection Types [shows list of connections]
Configure	/clustering/getNodeName	353-5	Clustering-Get Node Name

Category	URL	ID	Description
Configure	/accessControl/manageUsers	198-0	Configure-Access Control
Configure	/accessControl/assignUserToRole	353-1	Access Control-Assign Users to Role
Configure	/clustering/addResourcesToNode	354-1	Clustering-Add Selected Resources to the Node
Configure	/accessControl/list	198-1	Configure-Access Control[shows list of users]
Configure	/accessControl/showSearch	351-4	Access Control-Show Search
Configure	/accessControl/showUserCreate	198-6	Configure-Access Control[shows create user screen]
Configure	/accessControl/userUpdateDelete	198-5	Configure-Access Control[update values of user recied from user edit screen]
Configure	/accessControl/showManageGroup	352-4	Access Control-Manage Groups
Configure	/accessControl/updateRole	352-3	Access Control-Update Role
Configure	/accessControl/savePasswordProperties	352-2	Access Control-Save Password Properties
Configure	/accessControl/searchGroupAJAX	352-1	Access Control-Search Group

Category	URL	ID	Description
Configure	/accessControl/groupList	352-0	Access Control-List of Groups
Configure	/accessControl/userSave	351-9	Access Control-Save User
Configure	/accessControl/updatedCheckboxField	351-8	Access Control-Show Updated Checkbox Field
Configure	/accessControl/showRoleCreate	198-7	Configure-Access Control-Manage Roles[shows create role screen]
Configure	/accessControl/addUserList	351-7	Access Control-Add User List
Configure	/accessControl/getUpdatedToken	351-5	Access Control-Get Updated Token
Configure	/accessControl/index	351-2	Access Control-Index
Configure	/accessControl/showSearchGroup	351-1	Access Control-Show Search Group
Configure	/accessControl/searchAJAX	351-0	Access Control-Search
Configure	/accessControl/showOrgDetails	350-9	Access Control-Show Organization Details
Configure	/accessControl/quickSaveGroup	350-8	Access Control-Quick Save Group

Category	URL	ID	Description
Configure	/accessControl/checkUserNameDuplication	350-6	Access Control-Check Duplicates for User Names
Configure	/accessControl/	352-8	Enable Access Control
Configure	/accessControl/checkRoleNameDuplication	350-7	Access Control-Check Duplicates for Role Names
Configure	/accessControl/deleteGroup	351-6	Access Control-Delete Group
Configure	/accessControl/saveRole	198-8	Configure-Access Control-Manage Roles[save values of role recieved from create role screen]
Configure	/accessControl/saveGroup	351-3	Access Control-Save Group
Configure	/clustering/showClustering	305-7	Configure-Clustering
Configure	/settings/showApplicationSettings	300-9	Configure-Settings-Application Settings
Configure	/accessControl/showSearchRole	198-9	Configure-Access Control-Manage Roles[show search role screen]
Configure	/config/showWorkflows	305-1	Configure-Workflows

Category	URL	ID	Description
Configure	/accessControl/validatePassword	352-6	Access Control-Validate Password
Configure	/accessControl/roleList	199-0	Configure-Access Control-Manage Roles[shows list of roles]
Configure	/accessControl/roleDelete	199-2	Configure-Access Control-Manage Roles[deletes role]
Configure	/config/showCriticalityJobs	196-8	Configure-Criticality[shows list criticality job]
Configure	/clustering/listResources	356-2	Clustering-List All Resources
Configure	/accessControl/showPasswordControlProperties	206-3	Configure-Access Control-Password Control
Configure	/uf/showUF	206-5	Configure-Universal Forwarder
Configure	/accessControl/showRoleUpdate	199-1	Configure-Access Control-Manage Roles[update values of role recieved from edit role screen]
Configure	/settings/customizeMenu	301-0	Configure-Settings-Customize Menu
Configure	/accessControl/beforeInterceptor	352-5	Access Control-Before Interceptor

Category	URL	ID	Description
Configure	/email/queuedEmails	306-0	Configure-Queued emails
Configure	/settings/showDNSServers	301-1	Configure-Settings-DNS Servers
Configure	/settings/holidayMetaList	301-2	Configure-Settings- Holidays
Configure	/settings/showAddLicense	301-4	Configure-Settings- Install License
Configure	/uf/showRegisterUF	301-8	Configure-Universal Forwarder- Create/edit UF screen
Configure	/settings/showAppLogs	300-8	Configure-Settings-Application Logs
Configure	/settings/showLogging	301-5	Configure-Settings- Logging
Configure	/settings/showSafeDomainList	301-6	Configure-Settings-Safe Domains
Dash-board	/highRiskUsers/showHighRiskUsersChart	403-1	HighRisk Users Chart
Dash-board	policy_category:FRAUD	462-2	Dashboard-Security Dashbaord-FRAUD
Dash-board	policy_category:SECURITY POLICY VIOLATION	462-3	Dashboard-Security Dashbaord-SECURITY POLICY VIOLATION

Category	URL	ID	Description
Dash-board	policy_category:ACCOUNT MISUSE	462-4	Dashboard-Security Dashbaord-ACCOUNT MISUSE
Dash-board	policy_category:EXPLOIT	462-5	Dashboard-Security Dashbaord-EXPLOIT
Dash-board	policy_category:MALWARE	462-6	Dashboard-Security Dashbaord-MALWARE
Dash-board	/highRiskUsers/showHighRiskAccessAccountCount	402-6	HighRisk Access Account Count
Dash-board	/incidents/getCaseCount	404-5	Incidents-Get Case Count
Dash-board	/incidents/getCaseHistory	404-3	Incidents-Get Case History
Dash-board	/highRiskUsers/showEntityCounts	402-8	High Risk Users-Entity Counts
Dash-board	/highRiskUsers/showRiskScoreTrend	402-9	High Risk Users-Show Risk Score Trend
Dash-board	policy_category:IDENTITY ISSUE	462-1	Dashboard-Security Dashbaord-IDENTITY ISSUE
Dash-board	/highRiskUsers/showHighRiskUsersList	403-0	HighRisk Users List
Dash-board	/incidents/showCaseComments	404-6	Incidents-Show Case Comments

Category	URL	ID	Description
Dash-board	policy_category:TRAFFIC ANOMALY	462-0	Dashboard-Security Dashbaord-TRAFFIC ANOMALY
Dash-board	/highRiskUsers/getUpdatedToken	402-7	High Risk Users-Get Updated Token
Dash-board	policy_category:INSIDER THREAT	461-8	Dashboard-Security Dashbaord-INSIDER THREAT
Dash-board	/dashboard/updateTaskAssistantPref	400-1	Dashboard-Update Task Assistant Preferences
Dash-board	/highRiskUsers	403-2	High Risk Users
Dash-board	/dashboard/showHistogramForAccessScanner	400-0	Dashboard-Histogram For Access Scanner
Dash-board	/dashboard/showHighRiskResourcesChart	400-2	HighRisk Resources Chart
Dash-board	/dashboard/showAccessPoliciesForUser	400-3	Dashboard-Access Policies For User
Dash-board	/dashboard/saveUserPreferences	400-4	Dashboard-Save User Preferences
Dash-board	/executiveDashboard/showCaseStatusChart	400-6	Executive Dashboard-Show Case Status Chart
Dash-board	/dashboard/showHighRiskUsersByCategory	398-9	HighRisk Users By Category

Category	URL	ID	Description
Dash-board	/highRiskUsers/followEntity	402-5	High Risk Users-Follow Entity
Dash-board	/incidents/	404-7	Incidents
Dash-board	/incidents/searchJira	404-8	Incidents-Search JIRA
Dash-board	/highRiskUsers/getPoliciesByType	458-5	Show high risk users policies by type
Dash-board	/highRiskUsers/getCriticality	458-6	Show high risk users criticality
Dash-board	/export/getViolators	458-8	Show export violators
Dash-board	/highRiskUsers/returnTypes	459-7	Show high risk users return types
Dash-board	policy_category:CONFIGURATION ERROR	461-9	Dashboard-Security Dashbaord-CONFIGURATION ERROR
Dash-board	/incidents/getUpdatedToken	403-3	Incidents-Get Updated Token
Dash-board	/dashboard/showRiskyUsersForPeer	394-0	Dashboard-Risky Users For Peer
Dash-board	/incidents/getIncidentListByCategory	403-5	Incidents-Get Incident List By Category
Dash-board	/dashboard/showUserHRASCDetails	394-2	Dashboard-Show User HR ASC Details

Category	URL	ID	Description
Dash-board	/dashboard/showPolicyTree	394-3	Dashboard-Show Policy Tree
Dash-board	/dashboard/showResourceThreatsList	394-4	Dashboard-Show Resource Threats List
Dash-board	/dashboard/createCase	394-5	Create Case
Dash-board	/dashboard/removeFromWhitelist	394-6	Dashboard-Remove From Whitelist
Dash-board	/dashboard/fetchVisualData	394-7	Dashboard-Fetch Visual Data
Dash-board	/dashboard/showHistogram	394-1	Dashboard-Show Histogram
Dash-board	/dashboard/drillDowncorrelationResults	393-2	Dashboard-Filter Correlation Results
Dash-board	/dashboard/showEventScannerWidget	393-1	Dashboard-Show Event Scanner Widget
Dash-board	/dashboard/loadSecurityControlCenter	392-9	Dashboard-Load Security Control Center
Dash-board	/dashboard/showResourceStatisticsDetails	391-4	Dashboard-Resource Statistics Details
Dash-board	/dashboard/showPeerStatisticsDetails	391-5	Dashboard-Peer Statistics Details
Dash-board	/dashboard/showPoliciesWidget	399-9	Dashboard-Policies Widget

Category	URL	ID	Description
Dash-board	/dashboard/showCorrelationResults	391-6	Dashboard-Correlation Results
Dash-board	/dashboard/showRiskyUsersForResource	394-8	Dashboard-Show Risky Users For Resource
Dash-board	/dashboard/getOtherPoliciesList	393-9	Get Other Policies List
Dash-board	/dashboard/listSelectOrganization	393-8	List Organizations
Dash-board	/dashboard/loadAccessReviewProgressByTypeChart	393-7	Dashboard-Load Access Review Progress By Type Chart
Dash-board	/incidents/showCaseCommentsByScreenId	403-6	Incidents-Show Case Comments By Screen Id
Dash-board	/incidents/showJiraSearch	403-7	Incidents-Show Jira Search
Dash-board	/incidents/sendCaseNotification	403-8	Incidents-Send Case Notification
Dash-board	/incidents/showJiraCaseComments	403-9	Incidents-Show Jira Case Comments
Dash-board	/incidents/showIncidentsWidget	404-0	Incidents Widget
Dash-board	/incidents/showIncidentsByUserGroupChart	404-1	Show Incidents By User Group Chart
Dash-board	/incidents/showCaseDetails	404-2	Incidents-Show Case Details

Category	URL	ID	Description
Dash-board	/incidents	404-4	Show Incidents Widget
Dash-board	/dashboard/showAccessReviewsWidget	391-2	Dashboard-Access Reviews Widget
Dash-board	/dashboard/showThreatPolicyCounts	398-8	Dashboard-Threat Policy Counts
Dash-board	/dashboard/showUserHRASCChart	398-6	Dashboard-User HRASC Chart
Dash-board	/dashboard/getCasesForEntity	393-3	Dashboard-Get Cases For Entity
Dash-board	/dashboard/certifyHighRiskAccessActivity	393-4	Certify HighRisk Access Activity
Dash-board	/dashboard	393-5	Grant Dashboard Access
Dash-board	/dashboard/	393-6	Dashboard
Dash-board	/incidents/showIncidentsTrendChart	403-4	Incidents Trend Chart
Dash-board	/dashboard/showHighRiskResourceDetails	399-8	HighRisk Resource Details
Dash-board	/adminDashboard/setEventColor	387-3	Administrative Dashboard-Set Event Color for Status
Dash-board	/dashboard/loadPoliciesList	399-6	Dashboard-Load Policies List

Category	URL	ID	Description
Dash-board	/dashboard/loadActivityImportHistoryChartByResource	390-9	Dashboard-Load Activity Import History Chart By Resource
Dash-board	/adminDashboard/loadActivityAccountSummary	390-0	Administrative Dashboard-Load Activity Account Summary
Dash-board	/adminDashboard/	389-0	Enable Administrative Dashboard
Dash-board	/adminDashboard/loadPeerGroupSummary	388-3	Administrative Dashboard-Load Peer Group Summary
Dash-board	/adminDashboard/beforeInterceptor	388-8	Administrative Dashboard-Before Interceptor
Dash-board	/adminDashboard/loadPercentageAdminSummary	387-0	Administrative Dashboard-Load Percentage Change in Imports Summary
Dash-board	/adminDashboard/loadJobDurationChart	390-8	Administrative Dashboard-View Job Duration Trend
Dash-board	/adminDashboard/loadUserEntSummary	387-1	Administrative Dashboard-Load User Entity Summary

Category	URL	ID	Description
Dash-board	/adminDashboard	387-4	Show Administrative Dashboard
Dash-board	/adminDashboard/loadActivityImportHistoryLineChart	387-5	Administrative Dashboard-Load Activity Import History Line Chart
Dash-board	/adminDashboard/loadActivityTransSummary	387-6	Administrative Dashboard-Load Activity Transaction Summary
Dash-board	/adminDashboard/index	387-7	View Administrative Dashboard
Dash-board	/adminDashboard/loadLicInfoDetails	387-8	Administrative Dashboard-View Details of Installed Licenses
Dash-board	/email/emailQueueCount	379-6	Email Template-Email Queue Count
Dash-board	/adminDashboard/loadResourceActivityAccountCount	387-2	Administrative Dashboard-Load Resource Activity Account Count
Dash-board	/dashboard/sendReminder	391-0	Dashboard-Enable Send Reminder
Dash-board	/adminDashboard/wrapTitle	390-7	Administrative Dashboard-Title

Category	URL	ID	Description
Dash-board	/adminDashboard/loadPeerCountChart	389-1	Administrative Dashboard-View Peer Creation Count Trends
Dash-board	/dashboard/showPolicyDetailsForUserByResource	391-7	Dashboard-Policy Details For User By Resource
Dash-board	/adminDashboard/loadJobSummary_Backup	389-8	Administrative Dashboard-Display Jobs Summary
Dash-board	/adminDashboard/getJobType	389-2	Administrative Dashboard-Get Job Type
Dash-board	/adminDashboard/loadAccessAccountSummary	389-3	Administrative Dashboard-Load Access Account Summary
Dash-board	/adminDashboard/loadResourceAcsEntCount	389-4	Administrative Dashboard-Load Resource Access Entity Count
Dash-board	/adminDashboard/loadJobAdminSummary	389-5	Administrative Dashboard-View Administrative Job Summary
Dash-board	/adminDashboard/loadCorrelatedAccountChart	390-6	Administrative Dashboard-Load Correlated Account Chart

Category	URL	ID	Description
Dash-board	/adminDashboard/loadEvents	389-6	Administrative Dashboard-Load Events
Dash-board	/adminDashboard/assignSelectedUserToResource	389-9	Administrative Dashboard-Assign Selected User to Resource
Dash-board	/adminDashboard/loadIpAddrSummary	390-5	Administrative Dashboard-View IP Address Summary
Dash-board	/adminDashboard/loadJobGroupCountSummaryByDate	390-1	Administrative Dashboard-View Import Count Summary for Job Groups By Date
Dash-board	/adminDashboard/loadJobSummary	390-2	Administrative Dashboard-View Jobs Summary
Dash-board	/adminDashboard/loadResourceActTransCount	390-3	Administrative Dashboard-Load Resource Account Transaction Count
Dash-board	/adminDashboard/getJobDetails	390-4	Administrative Dashboard-Get Job Details
Dash-board	/adminDashboard/loadResourceAccessAccountCount	389-7	Administrative Dashboard-Load Resource Access Account Count

Category	URL	ID	Description
Dash-board	/adminDashboard/getUpdatedToken	387-9	Administrative Dashboard-Get Updated Token
Dash-board	/adminDashboard/loadResourceSummary	388-0	Administrative Dashboard-Load Resource Summary
Dash-board	/adminDashboard/loadPolicyexCountChart	388-1	Administrative Dashboard-View Policy Ex Chart
Dash-board	/highRiskUsers/	401-9	Show High Risk Users
Dash-board	/highRiskUsers/showHighRiskActivityAccountCount	402-0	HighRisk Activity Account Count
Dash-board	/highRiskUsers/showThreatPolicyCounts	402-1	High Risk Users-Threat Policy Counts
Dash-board	/highRiskUsers/showRiskyUserPolicies	402-2	High Risk Users-Risky User Policies
Dash-board	/executiveDashboard/getUpdatedToken	400-8	Executive Dashboard-Get Updated Token
Dash-board	/highRiskUsers/showHighRiskActivityIPCount	402-4	HighRisk Activity IP Count
Dash-board	/highRiskUsers/beforeInterceptor	401-8	High Risk Users-Before Interceptor
Dash-board	/executiveDashboard/showCasesByGroupChart	400-7	Executive Dashboard-Show Cases By Group Chart

Category	URL	ID	Description
Dash-board	/dashboard/showRiskyUsersForGroupOwner	399-0	Dashboard-Show Risky Users For Group Owner
Dash-board	/dashboard/showViolatorsByPolicyCategories	399-1	Dashboard-Show Violators By Policy Categories
Dash-board	/dashboard/loadTaskAssistantList	399-2	Dashboard-Load Task Assistant List
Dash-board	/dashboard/showUserStatisticsDetails	399-3	Dashboard-User Statistics Details
Dash-board	/dashboard/showViolationAdditionalDetails	399-4	Dashboard-Show Violation Additional Details
Dash-board	/dashboard/loadResourceConfigPoliciesDetails	399-5	Dashboard-Load Resource Configuration Policies Details
Dash-board	/executiveDashboard/showHighRiskSuspectChecksChart	400-5	Executive Dashboard-HighRisk Suspect Checks Chart
Dash-board	/highRiskUsers/showHighRiskUsersCount	401-7	High Risk Users Count
Dash-board	/highRiskUsers/showHistogram	401-6	High Risk Users-ShowHistogram
Dash-board	/executiveDashboard/	401-5	Executive Dashboard
Dash-board	/adminDashboard/loadEventSummary	388-2	Administrative Dashboard-View Events Summary

Category	URL	ID	Description
Dash-board	/adminDashboard/loadUserSummary	388-4	Administrative Dashboard-Load Users Summary
Dash-board	/adminDashboard/loadGraphTrendDetails	388-5	Administrative Dashboard-View Details of Trend Graphs
Dash-board	/adminDashboard/loadResourceEventCount	388-6	Administrative Dashboard-Load Resource Event Count
Dash-board	/adminDashboard/loadAccessImportHistoryLineChart	388-7	Administrative Dashboard-Load Access Import History Line Chart
Dash-board	/adminDashboard/loadSecAppDetails	388-9	Administrative Dashboard-View Securonix Application Details
Dash-board	/dashboard/showAccessScannerWidget	391-1	Dashboard-Access Scanner Widget
Dash-board	/dashboard/getUserForPeers	398-4	Dashboard-Get User for Peers
Dash-board	/dashboard/updateHighRiskObject	391-3	Dashboard-Update HighRisk Object
Dash-board	/executiveDashboard/beforeInterceptor	400-9	Executive Dashboard-Before Interceptor

Category	URL	ID	Description
Dash-board	/executiveDashboard/highRiskAggregateResources	401-0	Executive Dash-board-HighRisk Aggregate Resources
Dash-board	/executiveDashboard	401-1	Executive Dash-board- Enable View
Dash-board	/executiveDashboard/showHighRiskThreatChart	401-2	Executive Dash-board-HighRisk Threat Chart
Dash-board	/executiveDashboard/showPoliciesByVioltionCount	401-3	Executive Dash-board-Policies By Violaion Count
Dash-board	/executiveDashboard/highRiskAggregateUsers	401-4	Executive Dash-board-HighRisk Aggregate Users
Dash-board	/dashboard/showRiskyUsersForAccessValue	399-7	Risky Users For Access Value
Dash-board	/dashboard/showJobEventDetails	391-8	Dashboard-Job Event Details
Dash-board	/highRiskUsers/showHighRiskUsersWidget	402-3	HighRiskUsers Widget
Dash-board	/dashboard/loadResourceOutlierAccessDetails	392-0	Dashboard-Load Resource Outlier Access Details
Dash-board	/riskModeler/showRunThreatModel	335-5	Risk Modeler-Show Run Threat Model

Category	URL	ID	Description
Dash-board	DEFAULTWORKFLOW:CLAIM	316-1	Dashboard-Security Dashbaord-Bulk Action:CLAIM
Dash-board	DEFAULTWORKFLOW:CLOSE AS FIXED	316-0	Dashboard-Security Dashbaord-Bulk Action:CLOSE AS FIXED
Dash-board	DEFAULTWORKFLOW:ASSIGN TO ANALYST	315-9	Dashboard-Security Dashbaord-Bulk Action:ASSIGN TO ANALYST
Dash-board	/dashboard/showThreatDetails	315-7	Dashboard-Security Dashbaord-Threats-Shows Threat Details
Dash-board	/riskModeler/showThreatModelList	335-4	Risk Modeler-Show Threat Model List
Dash-board	/dashboard/deletePolicyViolation	316-8	Dashboard-Security Dashboard-Delete Violations
Dash-board	/dashboard/showHighRiskOutlierActivityUserList	315-5	Dashboard-Security Dashbaord-Threats-High Risk Outlier Lis
Dash-board	/dash-board/showHighRiskActivitiesSuspectChecksChart	315-3	Dashboard-Security Dashbaord-Threats-Threats By Suspect Checks Chart

Category	URL	ID	Description
Dash-board	/dashboard/showHighRiskActivitiesByThreatChart	315-2	Dashboard-Security Dashbaord-Threats-Threats By Criticality Chart
Dash-board	/dashboard/showHighRiskActivitiesByResourceChart	315-1	Dashboard-Security Dashbaord-Threats-Threats By Resource Chart
Dash-board	/riskModeler/saveRiskModel	336-3	Risk Modeler-Save Risk Model
Dash-board	/dashboard/showAccessValuesForHighRiskAccess	300-1	Dashboard-Security Dashboard-High Risk Access [shows high risk access by Access Value list]
Dash-board	/dashboard/showHighRiskAccessByGroupOwnerChart	300-2	Dashboard-Security Dashboard-High Risk Access [shows high risk access by Group Owner graph]
Dash-board	/dashboard/showHighRiskActivitiesByThreatCategoryChart	315-4	Dashboard-Security Dashbaord-Threats-Threats By Category Chart
Dash-board	about_license	207-3	Dashboard-Administrative Dashboard-About License

Category	URL	ID	Description
Dash-board	POLICYVIOLATIONSWORKFLOW:Mark As Concern	316-9	Dashboard-Security Dashbaord-Policy Violations:Mark As Concern
Dash-board	/dashboard/showActivityOutliersWidget	317-1	Dashboard-Security Dashboard-Peer Based Activities
Dash-board	/export/exportObjectsToRtf	324-1	Export-Export Objects to RTF
Dash-board	policy_category:ALERT	312-4	Dashboard-Security Dashbaord-ALERT
Dash-board	policy_category:DATA EXFILTRATION	312-5	Dashboard-Security Dashbaord-DATA EXFILTRATION
Dash-board	/adminDashboard/loadAccessImportHistory	312-9	Dashboard-Administrative Dashboard-Access Import History
Dash-board	/riskModeler	336-1	Risk Modeler Widget
Dash-board	/riskModeler/getUpdatedToken	336-0	Risk Modeler-Get Updated Token
Dash-board	POLICYVIOLATIONSWORKFLOW:Mark As Non-Concern	317-0	Dashboard-Security Dashbaord-Policy Violations:Mark As Non-Concern

Category	URL	ID	Description
Dash-board	/riskModeler/showJobOutput	335-9	Risk Modeler-Show Job Output
Dash-board	/riskModeler/searchJobAJAX	335-7	Risk Modeler-Search Job AJAX
Dash-board	/incidents/showReviews	195-4	Respond-Activity Reviews
Dash-board	/riskModeler/searchRiskModelJobs	335-6	Risk Modeler-Search Risk Model Jobs
Dash-board	/executiveDashboard/loadExecutiveDashboard	317-6	Dashboard-Executive Dashboard
Dash-board	/geolocation/showGeolocation	317-3	Dashboard-Geolocation Map
Dash-board	/incidents/showSendCaseNotification	317-2	Dashboard-Security Dashboard-Incidents [Send Case Notification Email]
Dash-board	/riskModeler/runThreatModel	335-8	Risk Modeler-Run Threat Model
Dash-board	/adminDashboard/loadActivityImportHistory	182-4	Dashboard-Administrative Dashboard-Activity Import History [shows activity import history details]

Category	URL	ID	Description
Dash-board	/adminDashboard/showCorrelationResultsDetails	182-3	Dashboard-Administrative Dashboard-Correlation Results [shows correlation results deatails]
Dash-board	/dashboard/accessRequest	200-5	Access Request
Dash-board	/adminDashboard/loadGlossaryImportHistoryChart	182-5	Dashboard-Administrative Dashboard-Glossary Import History [shows glossary import history details]
Dash-board	/dashboard/showHighRiskAccessByAccessValueChart	300-0	Dashboard-Security Dashboard-High Risk Access [shows high risk access by Access Value graph]
Dash-board	/riskModeler/	336-2	Risk Modeler
Dash-board	/export/index	323-1	Export-index
Dash-board	about_application	207-2	Dashboard-Administrative Dashboard-About Application

Category	URL	ID	Description
Dash-board	/dashboard/showHighRiskResourcesList	206-6	Dashboard-Security Dashboard-High Risk Resources [shows high risk resources]
Dash-board	/dashboard/showHighRiskUsersChart	180-5	Dashboard-Security Dashboard-High Risk Users [shows high risk users graph]
Dash-board	/export/exportObjectsToCsv	323-4	Export-Export Objects to CSV
Dash-board	/adminDashboard/loadSummary	206-2	Dashboard-Administrative Dashboard-Summary
Dash-board	/users/showInvestigationWorkbench	205-8	Dashboard-Launch Investigation Workbench
Dash-board	/dashboard/loadScheduledJobsCalendar	205-4	Dashboard-JobCalendar [shows job calendar]
Dash-board	/dashboard/loadExecutiveDashboard	203-2	Dashboard-Load Executive Dashboard
Dash-board	/export/exportToPdf	323-2	Export-Export to PDF

Category	URL	ID	Description
Dash-board	/dashboard/showUsersWithAccessForOutliers	391-9	Dashboard-Users With Access Outliers
Dash-board	/export/exportToXML	323-3	Export-Export to XML
Dash-board	/dashboard/showHighRiskUsersList	180-6	Dashboard-Security Dashboard-High Risk Users [shows list of high risk users]
Dash-board	/dashboard/showHighRiskAccessUsersChart	180-7	Dashboard-Security Dashboard-High Risk Access [shows high risk access users graph]
Dash-board	/dashboard/showHighRiskAccessUserList	180-8	Dashboard-Security Dashboard-High Risk Access [shows list of high risk access users]
Dash-board	/dashboard/getAccessListByResource	200-4	Access Request-[shows access list by resource]
Dash-board	/dashboard/submitAccessRequest	200-3	Access Request-[submit access request]
Dash-board	/adminDashboard/loadCorrelationChart	182-2	Dashboard-Administrative Dashboard-Correlation Results [shows correlation results graph]

Category	URL	ID	Description
Dash-board	/adminDashboard/showUserImportHistoryDetails	182-1	Dashboard-Administrative Dashboard-User Import History [shows user import history details]
Dash-board	/adminDashboard/loadUserImportHistoryChart	182-0	Dashboard-Administrative Dashboard-User Import History [shows user import history graph]
Dash-board	/dashboard/showPolicyDetails	181-8	Dashboard-Security Dashboard-User Defined Policies[shows details of user defined policies]
Dash-board	/dashboard/showDOSAccounts	181-7	Dashboard-Security Dashboard-Possible DOS Attack[shows possible dos accounts list]
Dash-board	/dashboard/showIncidentsProgress	181-6	Dashboard-Security Dashboard-Incidents [shows incident progress]
Dash-board	/incidents/showIncidentsList	181-5	Dashboard-Security Dashboard-Incidents[shows list of incidents]

Category	URL	ID	Description
Dash-board	/incidents/showIncidentsChart	181-4	Dashboard-Security Dashboard-Incidents [shows incidents graph]
Dash-board	/dashboard/highRiskAccountsFromMultipleIP	181-3	Dashboard-Security Dashboard-High Risk Accounts[shows list of high risk accounts]
Dash-board	/dashboard/showDLPPeersList	181-2	Dashboard-Security Dashboard-DLP Alerts[shows list of DLP alerts]
Dash-board	/dashboard/showDLPPeersListGraph	181-1	Dashboard-Security Dashboard-DLP Alerts [shows DLP alerts graph]
Dash-board	/dashboard/showHighRiskActivitiesList	181-0	Dashboard-Security Dashboard-High Risk Activities[shows list of high risk activities]
Dash-board	/dashboard/showHighRiskActivitiesChart	180-9	Dashboard-Security Dashboard-High Risk Activities [shows high risk activities graph]

Category	URL	ID	Description
Dash-board	/dashboard/showGroupOwnersForHighRiskAccess	300-3	Dashboard-Security Dashboard-High Risk Access [shows high risk access by Group Owner list]
Dash-board	/dashboard/showHighRiskAccessPeerChart	300-4	Dashboard-Security Dashboard-High Risk Access [shows high risk access by Peer graph]
Dash-board	/adminDashboard/loadAdministrativeDashboard	181-9	Dashboard-Administrative Dashboard
Dash-board	/dashboard/showHighRiskAccessByResourceChart	300-6	Dashboard-Security Dashboard-High Risk Access [shows high risk access by Resource graph]
Dash-board	/dashboard/updateCase	397-8	Update Case
Dash-board	/dashboard/showEntityCounts	397-9	Dashboard-Entity Counts
Dash-board	/dashboard/loadResourceAccessPoliciesDetails	398-0	Dashboard-Load Resource Access Policies Details
Dash-board	/dashboard/showViolationsChartData	398-1	Dashboard-Violations Chart Data

Category	URL	ID	Description
Dash-board	/dashboard/loadResourceAlertsPoliciesDetails	398-2	Dashboard-Load Resource Alerts Policies Details
Dash-board	/dashboard/searchUserImportJobAJAX	398-3	Dashboard-Search User Import Job using AJAX
Dash-board	/dashboard/showRiskyUserAccounts	397-7	Dashboard-Risky User Accounts
Dash-board	policy_category:ROGUE ACCESS PRIVILEGES	462-7	Dashboard-Security Dashbaord-ROGUE ACCESS PRIVILEGES
Dash-board	/dashboard/showCreateCase	392-1	Enable Create Case
Dash-board	/dashboard/showHighRiskOutlierActivitiesChart	395-0	HighRisk Outlier Activities Chart
Dash-board	/dashboard/addToWhiteList	396-9	Dashboard-Add To WhiteList
Dash-board	/dashboard/showSearchOrg	396-7	Dashboard-Show Search Organization
Dash-board	/dashboard/showUsersWithoutAccessForOutliers	395-2	Dashboard-Show Users Without Access Outliers
Dash-board	/dashboard/showCalendarEventList	395-3	Dashboard-Show Calendar Events List
Dash-board	/dashboard/showUsersWithActivity	398-5	Dashboard-Users With Activity

Category	URL	ID	Description
Dash-board	/dashboard/showSendReminder	397-6	Dashboard-Show Send Reminder
Dash-board	/dashboard/showHighRiskThreatsListByCategory	397-5	HighRisk Threats List By Category
Dash-board	/dashboard/appCorrelationChart	397-4	Dashboard-App Correlation Chart
Dash-board	/dashboard/showPeersListForHighRiskAccess	300-5	Dashboard-Security Dashboard-High Risk Access [shows high risk access by Peer list]
Dash-board	/dashboard/showHighRiskResourcesWidget	392-2	HighRisk Resources Widget
Dash-board	/dashboard/rejectCert	392-3	Dashboard-Rejection Cert
Dash-board	/dashboard/loadActivityImportHistoryChartByJob	392-4	Dashboard-Load Activity Import History Chart By Job
Dash-board	/dashboard/showHighRiskAccessWidget	392-5	HighRisk Access Widget
Dash-board	/dashboard/createAccessCertCases	392-6	Dashboard-Create Access Certification Cases
Dash-board	/dashboard/showAccessScannerUsersList	392-7	Dashboard-Show Access Scanner Users List
Dash-board	/dashboard/loadDatasourceFilter	392-8	Dashboard-Load Datasource Filter

Category	URL	ID	Description
Dash-board	/dashboard/showUsersWithoutActivity	393-0	Dashboard-Show Users Without Activity
Dash-board	/dashboard/showUserDetailsForActivityOutliers	398-7	Dashboard-User Details For Activity Outliers
Dash-board	/dashboard/assignCertToUser	394-9	Dashboard-Assign Certificate to User
Dash-board	/dashboard/loadSecurityDashboard	395-1	Load Security Dashboard
Dash-board	/dashboard/loadActivityImportHistoryChart	397-1	Dashboard-Load Activity Import History Chart
Dash-board	/dashboard/showPolicyTrend	397-2	Dashboard-Show Policy Trend
Dash-board	/dashboard/showSuspectEventAdditionalDetails	397-3	Dashboard-Show Suspect Event Additional Details
Dash-board	/dashboard/beforeInterceptor	395-4	Dashboard-Before Interceptor
Dash-board	/dashboard/loadActivityDashboard	395-5	Dashboard-Load Activity Dashboard
Dash-board	/dashboard/loadResourceActivityPoliciesDetails	397-0	Dashboard-Load Resource Activity Policies Details
Dash-board	/dashboard/showAddToWhitelist	395-7	Dashboard-Show Add To Whitelist

Category	URL	ID	Description
Dash-board	/export/	324-5	Dashboard-Show Export
Dash-board	/dashboard/showWhitelistSearch	304-5	Dashboard-Whitelist
Dash-board	/dashboard/showHighRiskAccess	302-9	Dashboard-Security Dashboard - High Risk Access
Dash-board	/dashboard/showCerts	302-8	Dashboard-Security Dashboard - Show Certifications on Dashboard
Dash-board	/export/beforeInterceptor	324-4	Export-Before Interceptor
Dash-board	/dashboard/getUpdatedToken	395-6	Dashboard-Get Updated Token
Dash-board	/riskModeler/showThreatModelJobs	335-3	Risk Modeler-Show Threat Model Jobs
Dash-board	/export/getMaskingParams	324-2	Export-Get Masking Params
Dash-board	/export/exportObjectsToPdf	324-0	Export-Export Objects to PDF
Dash-board	/export/exportToRtf	323-9	Export-Export to RTF
Dash-board	/export/getReportName	323-8	Export-Get Report Name
Dash-board	/export	323-7	Dashboard-Enable Export

Category	URL	ID	Description
Dash-board	/export/exportObjectsToXML	323-6	Export-Export Objects to XML
Dash-board	/export/columnCheck	323-5	Export-Column Check
Dash-board	/dashboard/showResourcesForHighRiskAccess	300-7	Dashboard-Security Dashboard-High Risk Access [shows high risk access by Resource list]
Dash-board	/dashboard/showAccessScannerSummary	304-9	Dashboard-Access Scanner
Dash-board	/dashboard/getTaskAssistantList	305-0	Dashboard-Task Assistant
Dash-board	/export/exportToCsv	324-3	Export-Export to CSV
Dash-board	/riskModeler/configureRiskModel	335-2	Risk Modeler-Configure Risk Model
Dash-board	/riskModeler/deleteThreatModel	335-1	Risk Modeler-Delete Threat Model
Dash-board	/dashboard/showHighRiskAccessUserDetails	395-9	Show HighRisk Access User Details
Dash-board	/dashboard/showAccessScannerDataSummary	396-0	Show Access Scanner Data Summary
Dash-board	/dashboard/listViolationActions	396-1	Dashboard-List Violation Actions

Category	URL	ID	Description
Dash-board	/dashboard/loadResourceOutlierActivitiesDetails	396-2	Dashboard-Load Details of Resource Outlier Activities
Dash-board	/dashboard/showDateOfUserImportJob	396-3	Dashboard-Show Date of User Import Job
Dash-board	/dashboard/showUserDetailsForAccessOutliers	396-4	Dashboard-Show User Details For Access Outliers
Dash-board	/dash-board/showPoliciesListForViolatorByPolicyCategory	395-8	Dashboard-Show Policies List For Violator By Policy Category
Dash-board	/dashboard/showHighRiskAccessCertProgress	396-6	Show HighRisk Access Certification Progress
Dash-board	/dashboard/switchCorrelationGraph	396-8	Dashboard-Switch Correlation Graph
Dash-board	/dashboard/loadDashboard	180-4	Dashboard-Security Dashboard
Dash-board	policy_category:Suspicious Activity	462-8	Dashboard-Security Dashbaord-Suspicious Activity
Dash-board	/dashboard/showHighRiskActivitiesTrendChart	315-6	Dashboard-Security Dashbaord-Threats-Threats By Trend Chart
Dash-board	/dashboard/showPolicyCategoriesWidet	305-9	Dashboard-Policy Categories Widget

Category	URL	ID	Description
Dash-board	/dashboard/showWhitelistDetails	396-5	Dashboard-Show Whitelist Details
Geoloca-tion	/geolocation/getFilters	453-0	Geolocation-Get Filters
Geoloca-tion	/geolocation/listDatasources	452-8	Geolocation-List Datasources
Geoloca-tion	/geolocation	452-9	Show Geolocation
Geoloca-tion	/workbench/basicGeoLoc	454-1	Geolocation-Show Basic Geolocation [Top right quick link]
Geoloca-tion	/geolocation/getUpdatedToken	453-3	Geolocation-Get Updated Token
Geoloca-tion	/geolocation/geoLocationData	453-1	Geolocation-Geolocation Data
Geoloca-tion	/geolocation/	453-2	Geolocation
Invest-igation Work-bench	/workbench/nodelinkdata	461-6	Show node link data
Invest-igation Work-bench	/workbench/getlocation	461-7	Allow getting loc-ation
Invest-igation Work-bench	/workbench/showPolicyViolators	455-2	Investigation Work-bench-Show Policy Violators

Category	URL	ID	Description
Investigation Workbench	/workbench/geoLocation	455-8	Investigation Workbench-Show GeoLocation
Investigation Workbench	/workbench/	455-7	Investigation Workbench
Investigation Workbench	/workbench/getChildAccessLevels	455-6	Investigation Workbench-Show Access Levels for Child Node
Investigation Workbench	/workbench	455-5	Enable Investigation Workbench
Investigation Workbench	/workbench/investigatePeerComparison	455-4	Investigation Workbench-Peer Comparison Investigation
Investigation Workbench	/workbench/getUpdatedToken	455-3	Investigation Workbench-Get Updated Token
Investigation Workbench	/workbench/listAccessValues	455-1	Investigation Workbench-List Access Values
Investigation Workbench	/workbench/showNewInvestigationWorkbench	454-0	Investigation Workbench-Show New Workbench

Category	URL	ID	Description
Investigation Workbench	/workbench/investigateObject	454-6	Investigation Workbench-Object Investigation
Investigation Workbench	/workbench/networkgeoloc	455-0	Investigation Workbench-Show Network Geolocations
Investigation Workbench	/workbench/initWorkbenchSearch	453-9	Investigation Workbench-Search Initialization
Investigation Workbench	/workbench/displayScreenshot	454-4	Investigation Workbench-View/Display Screenshot
Investigation Workbench	/workbench/showInvestigationWorkbench	454-2	Show Investigation Workbench
Investigation Workbench	/workbench/searchObjects	453-8	Investigation Workbench-Search Objects
Investigation Workbench	/workbench/sourceDestinationPlot	454-9	Investigation Workbench-Show Sources of Destination Plot
Investigation Workbench	/workbench/getAssociatedObjects	454-5	Investigation Workbench-Get Associated Objects

Category	URL	ID	Description
Investigation Workbench	/workbench/showPolicyViolatorsForPeer	454-8	Investigation Workbench-Show Policy Violator Accounts for Peer
Investigation Workbench	/workbench/searchAJAX	454-3	Investigation Workbench-Search
Other	SELFAUDITWORKFLOW:Decline	318-0	This is when user decline the activity.
Other	SELFAUDITWORKFLOW:Confirm	317-9	This is when user confirms the activity.
Other	/solr/**	317-7	/solr/**
Reports	/reports/deleteCategory	312-2	Reports-Delete Category
Reports	/reports/showActivityOrphanAccountsByResourceReport	328-7	Reports-Show Activity Orphan Accounts By Resource Report
Reports	/reports/showResourceGroupList	328-8	Reports-Show Resource-Group List
Reports	/reports/editCategory	312-3	Reports-Edit Category
Reports	/reports/addCategory	312-1	Reports-Add Category

Category	URL	ID	Description
Reports	/export/exportReport	311-6	Reports-Save And Generate Adhoc Reports
Reports	/reports/deleteReport	311-9	Reports-Delete Reports
Reports	/reports/showReportScheduler	311-8	Reports-Schedule Reports
Reports	/reports/editReport	311-7	Reports-Edit Reports
Reports	/reports/showRedundantNonUserAccountsReport	328-6	Reports-Show Redundant Non User Accounts Report
Reports	/reports/createReport	312-0	Reports-Create Reports
Reports	/reports/loadColumns	328-5	Reports-Load Columns
Reports	/config/showAuditList	364-7	Configuration-Show Audit List
Reports	/reports/getReportParameters	326-1	Reports-Get Report Parameters
Reports	/reports/showDormantAccountsReport	326-2	Reports-Show Dormant Accounts Report
Reports	/reports/showUserAccessByResourceReport	326-3	Reports-Show User Access By Resource Report
Reports	/reports/createAdhocReport	311-3	Reports-Create Adhoc Reports

Category	URL	ID	Description
Reports	/reports/deleteAdHocReport	311-5	Reports-Delete Adhoc Reports
Reports	/reports/uploadJrxmlFile	334-3	Reports-Upload JRXML File
Reports	/reports/showRacfOutlierAnalysisReport	329-4	Reports-Show Racf Outlier Analysis Report
Reports	/reports/showUserDetailsReport	332-6	Reports-Show User Details Report
Reports	/reports/showOutlierAnalysisReportByApplicationPermission	332-7	Reports-Show Outlier Analysis Report By Application Permission
Reports	/reports/showResourceReport	332-8	Reports-Show Resource Report
Reports	/reports/showResourceActivityReportbyUser	332-9	Reports-Show Resource Activity Report by User
Reports	/reports/showHighRiskAccessReport	333-0	Reports-Show High Risk Access Report
Reports	/reports/saveNewCategory	333-1	Reports-Save New Category
Reports	/reports/showAdOutlierAnalysisReport	326-0	Reports-Show AdOutlier Analysis Report
Reports	/reports/showPeerAssignmentRulesReport	326-4	Reports-Show Peer Assignment Rules Report

Category	URL	ID	Description
Reports	/reports/selectPeerList	327-6	Reports-Select Peer List
Reports	/reports/showUserActivityReport	328-4	Reports-Show User Activity Report
Reports	/reports/saveUserReport	325-9	Reports-Save User Report
Reports	/reports/paginateReports	328-9	Reports-Paginate Reports
Reports	/reports/showReportParameters	329-1	Reports-Show Report Parameters
Reports	/reports/showResourceList	329-2	Reports-Show Resources List
Reports	/reports/	329-0	Enable Reports View
Reports	/reports/showAnomalyDetectionRulesbyUser	325-7	Reports-Show Anomaly Detection Rules by User
Reports	/reports/selectResourceGroupList	325-6	Reports-Select Resource Group List
Reports	/reports/showPeerList	325-8	Reports-Show Peer List
Reports	/reports/listParameters	327-3	Reports-List Parameters
Reports	/reports/exportSavedReport	311-4	Reports-Run Adhoc Reports
Reports	/reports/getUpdatedToken	326-7	Reports-Get Updated Token

Category	URL	ID	Description
Reports	/reports/showPeerActivityReport	326-8	Reports-Show Peer Activity Report
Reports	/reports/beforeInterceptor	326-5	Reports-Before Interceptor
Reports	/reports/runSubReport	328-3	Reports-Run Sub Report
Reports	/reports/showUserPeerReport	327-0	Reports-Show User Peer Report
Reports	/reports/showPeerSuspiciousActivityReport	327-1	Reports-Show Peer Suspicious Activity Report
Reports	/reports/showAdhocReportList	327-2	Reports-Show Adhoc Report List
Reports	/reports/selectResourceList	326-6	Reports-Select Resources List
Reports	/reports/showUserActivityReportbyDate	328-2	Reports-Show User Activity Report by Date
Reports	/reports/runTopNReport	328-0	Reports-Run Top N Report
Reports	/reports/scheduledReportList	327-9	Reports-Scheduled Report List
Reports	/reports/showUserBehaviorProfileReport	327-8	Reports-Show User Behavior Profile Report
Reports	/reports/showSelectUsersDialog	333-2	Reports-Show Select Users Dialog

Category	URL	ID	Description
Reports	/reports/showUserAccesAccountReport	327-5	Reports-Show User Acces Account Report
Reports	/reports/showUserSuspiciousActivityReport	327-4	Reports-Show User Suspicious Activity Report
Reports	/reports/showTopHighestActivityUsersReport	328-1	Reports-Show Highest User Activ-ity Report
Reports	/reports/showTopNReportsList	326-9	Reports-Show Top N Reports List
Reports	/reports/showOutlierReports	207-1	Outlier Reports
Reports	/reports/saveTopNReport	327-7	Reports-SaveTop N Report
Reports	/reports/showResourceReports	206-9	Resource Reports
Reports	/reports/showHqlQuery	305-6	Reports-Ad-Hoc Reports
Reports	/reports/showReportList	329-9	Reports-Show Reports List
Reports	/reports/showAccessOutlierReport	330-0	Reports-Show Access Outlier Report
Reports	/reports/showGroupOwnerByResourceGroupReport	330-1	Reports-Show Group Owner By Resource Group Report

Category	URL	ID	Description
Reports	/reports/showAnomalyActivitybyUser	330-2	Reports-Show Anomaly Activity by User
Reports	/reports/getResourceGroups	330-3	Reports-Get Resource Groups
Reports	/reports/showResourceActivityReportbyIP	330-4	Reports-Show Resource Activity Report by IP
Reports	/reports/showSharedLoginActivityReport	330-5	Reports-Show Shared Login Activity Report
Reports	/reports/showPeerBehaviorProfileReport	329-5	Reports-Show Peer Behavior Profile Report
Reports	/reports/testExportReport	330-7	Reports-Test Export Report
Reports	/reports/showhighRiskAccessByPeer	331-8	Reports-Show High Risk Access By Peer
Reports	/reports/searchParameterValue	331-7	Reports-Search Parameter Value
Reports	/reports/runReport	305-5	Reports-Run Report
Reports	/reports/showHighRiskAccessByResourceReport	331-6	Reports-Show High Risk Access By Resource Report
Reports	/reports/showGenerateReport	331-9	Reports-Show Generate Report

Category	URL	ID	Description
Reports	/reports/showJRMAAnalysisReport	332-0	Reports-Show JRM Analysis Report
Reports	/reports/showresourceActivityReportbyDate	331-4	Reports-Show Resource Activity Report by Date
Reports	/reports/listUsers	331-3	Reports-List All Users
Reports	/reports/showTerminatedUsersAccountsReport	331-2	Reports-Show Terminated Users Accounts Report
Reports	/reports/getFilterCondition	331-1	Reports-Get Filter Condition
Reports	/reports/saveSubReport	331-0	Reports-Save Sub Report
Reports	/reports/showresourceActivityReport	330-9	Reports-Show Resource Activity Report
Reports	/reports/showUncorrelatedAccessAccountReport	330-8	Reports-Show Uncorrelated Access Account Report
Reports	/reports/downloadReport	332-1	Reports-Download Report
Reports	/reports/showHighRiskUsersReport	330-6	Reports-Show High Risk Users Report
Reports	/reports/showScheduledReports	207-0	Schedule Reports

Category	URL	ID	Description
Reports	/reports/showUserHighRiskAccessReport	331-5	Reports-Show User High Risk Access Report
Reports	/reports/saveReport	305-4	Reports-Save Report
Reports	/reports/dashboard	304-8	Reports-By Categories
Reports	/reports/generateHQL	329-8	Reports-generateHQL
Reports	/reports/showPeerGroupReports	206-8	Peer Reports
Reports	/reports/showUserReports	206-7	User Reports
Reports	/reports	333-3	Reports
Reports	/reports/showUserReport	333-4	Reports-Show User Report
Reports	/reports/showTopNReports	206-4	Reports-Show Top N Reports
Reports	/reports/showPeerGroupAnalysisReport	333-5	Reports-Show Peer Group Analysis Report
Reports	/reports/searchParameterList	333-6	Reports-Search Parameter List
Reports	/config/searchAJAXAudit	374-6	Configuration-Search AJAX Audit
Reports	/reports/impalaTest	459-2	Test impala reports

Category	URL	ID	Description
Reports	/reports/loadCategoryList	459-1	Show report category list
Reports	/reports/setSubreportConnection	329-6	Reports-Set Subreport Connection
Reports	/reports/reportsAjaxSearch	458-9	Allow reports search
Reports	/reports/showAnomalyReports	196-1	Reports-Anomaly Reports[shows anomaly reports screen]
Reports	/reports/showReports	332-5	Reports-Show Reports
Reports	/reports/runTopNReportSolr	459-0	Run TopNReport using Solr
Reports	/reports/showSelectUser	334-2	Reports-Show Select User
Reports	/reports/displayReports	334-1	Reports-Display Reports
Reports	/reports/generateResponse	334-0	Reports-Generate Response
Reports	/reports/showUserActivityReportbyIP	333-9	Reports-Show User Activity Report by IP
Reports	/reports/showAccessOrphanAccountsByResourceReport	333-8	Reports-Show Access Orphan Accounts By Resource Report
Reports	/reports/showScheduledReport	333-7	Reports-Show Scheduled Report

Category	URL	ID	Description
Reports	/reports/afterInterceptor	334-4	Reports-After Interceptor
Reports	/reports/showTerminatedUsersAccountsActivityReport	332-4	Reports-Show Terminated Users Accounts Activity Report
Reports	/config/showAuditing	202-7	Configure-Auditing
Reports	/reports/showTopHighestRiskUsers	332-2	Reports-Show Top Highest Risk Users
Reports	/reports/loadCategories	329-3	Reports-Load Categories
Reports	/reports/showAnomalyActivitybyResource	332-3	Reports-Show Anomaly Activity by Resource
Reports	/reports/scheduleReport	329-7	Reports-Schedule Report
Third Party Intelligence	/tpi/showCreateNewCore	385-0	Third Party Intelligence-Show Create New Core
Third Party Intelligence	/tpi/searchTpi	384-9	Search Third Party Intelligence
Third Party Intelligence	/tpi	384-8	Enable Third Party Intelligence
Third Party Intelligence	/tpi/showTpiSearch	304-7	Dashboard-Third Party Intelligence

Category	URL	ID	Description
Third Party Intel- ligence	/tpi/saveTPICore	384-6	Save Third Party Intelligence Core
Third Party Intel- ligence	/tpi/scheduleTpiExport	384-4	Schedule Third Party Intelligence Export
Third Party Intel- ligence	/tpi/searchTpiKB	384-7	Search Third Party Intelligence KB
Third Party Intel- ligence	/tpi/getUpdatedToken	385-1	Third Party Intel- ligence-Get Updated Token
Third Party Intel- ligence	/tpi/showTpiResultsOfSearchValue	385-9	Show Third Party Intelligence Res- ults of Search Value
Third Party Intel- ligence	/tpi/saveTPIRecords	385-8	Save Third Party Intelligence Records
Third Party Intel- ligence	/tpi/index	385-2	ShowThird Party Intelligence
Third Party Intel- ligence	/tpi/showTPIKBSearch	385-7	Show Third Party IntelligenceKB Search
Third Party Intel- ligence	/tpi/	385-6	Show Third Party Intelligence
Third Party Intel- ligence	/tpi/scheduleTpiImport	385-3	Schedule Third Party Intelligence Import

Category	URL	ID	Description
Third Party Intel- ligence	/tpi/showTpiExtraParams	385-5	Show Third Party Intelligence Extra Parameters
Third Party Intel- ligence	/tpi/showCreateNewTPIEntry	385-4	Show Create New Third Party Intel- ligence Entry
Third Party Intel- ligence	/tpi/beforeInterceptor	386-0	Third Party Intel- ligence-Before Interceptor
Views	/organization/showSearchOrg	417-2	Show Search Organization
Views	/peer/showPeerAccess	303-4	Manage-Peers [shows Peer Access Details]
Views	/peer/showPeerBehaviorPanel	303-5	Manage-Peers [shows Peer Behavior]
Views	/organization/edit	303-6	Manage-Organ- izations[shows edit organization screen]
Views	/organization/showChildOrganizations	304-0	Manage-Organ- izations[shows Child-Organ- ization]
Views	/resource/editAccessAttribute	308-8	Manage- Resources[Edit Access Attribute]

Category	URL	ID	Description
Views	/organization/showApplicationsforOrg	303-8	Manage-Organizations[shows Applications of Organization]
Views	/peer/showPeerActivities	303-3	Manage-Peers [shows Peer Activities]
Views	/resource/showResourceActivities	304-1	Manage-Resources[shows Resource Activities]
Views	/organization/showUsersforOrg	303-7	Manage-Organizations[shows Users of Organization]
Views	/users/showUserBehaviorPanel	303-2	Manage-Users [shows User Behavior]
Views	/resource/showAddActivityAttributesDialog	308-4	Manage-Resources[Add Activity Attributes]
Views	/users/showUserOrgs	303-0	Manage-Users [shows Organizations of User]
Views	/resource/deleteRGData	308-3	Manage-Resources[Delete Resource Group Data]
Views	/resource/showMonitorAccess	304-2	Manage-Resources[shows Resource Access details]

Category	URL	ID	Description
Views	/resource/removeActivityAttributes	308-5	Manage-Resources [Remove Activity Attributes]
Views	/resource/showAddAccessAttributesDialog	308-6	Manage-Resources[Add Access Attributes]
Views	/resource/removeAccessAttributes	308-7	Manage-Resources [Remove Access Attributes]
Views	/org/showHighRiskOrgApplicationsAggregateList	313-9	Dashboard-Organization-Show High Risk Organization Aggregate Applications
Views	/org/showHighRiskOrgUsersAggregateList	314-1	Dashboard-Organization-Show High Risk Organization Aggregate Users
Views	/org/showHighRiskUsersForOrgByCategory	315-0	Dashboard-Organization-Show High Risk Users In Organization By Category
Views	/org/listHighRiskOrgs	314-2	Dashboard-Organization-Show High Risk Organizations
Views	/organization/save	416-4	Organization-Save

Category	URL	ID	Description
Views	/organization/listOrganizations	416-9	Organization-List Organizations
Views	/users/showUserActivities	303-1	Manage-Users [shows User Activities]
Views	/resource/showResourceBehaviorPanel	304-3	Manage-Resources[shows Resource Behavior]
Views	/resource/delete	307-6	Manage-Resources[Delete Resource]
Views	/resource/deleteResourceGroup	307-8	Manage-Resources[Delete Resource Group]
Views	/organization/showAddResourcegroupToOrg	310-6	Manage-Organizations[Add Resource Groups to Organization]
Views	/organization/removeResourcegroupsFromOrg	310-7	Manage-Organizations[Remove Resource Groups from Organization]
Views	/watchList/showCreateEditWatchlist	310-8	Manage-Watchlist [Show Create Watchlist]
Views	/watchList/deleteWL	310-9	Manage-Watchlist [Remove Watchlist]

Category	URL	ID	Description
Views	/watchList/addMembers	311-0	Manage-Watchlist [Add Members to Watchlist]
Views	/watchList/removeWLMembers	311-1	Manage-Watchlist [Remove Members from Watchlist]
Views	/resource/reCorrelateAccounts	311-2	Manage-Resource [Show Resource:Re-corelate Accounts]
Views	/org/showHighRiskOrgsWidget	313-1	Dashboard-Organization-Show High Risk Orgnization Widget
Views	/org/showOrgHierarchy	313-2	Dashboard-Organization-Show Organization Hierarchy
Views	/org/showOrgLevel2	313-3	Dashboard-Organization-Show Organization Level 2
Views	/org/showOrgLevel3	313-4	Dashboard-Organization-Show Organization Level 3
Views	/org/showHighRiskOrgTrendingChart	313-5	Dashboard-Organization-Show Organization Trending Chart

Category	URL	ID	Description
Views	/org/showHighRiskOrgResourcesList	313-6	Dashboard-Organization-Show High Risk Organization Resources
Views	/org/showHighRiskOrgResourcesAggregateList	313-7	Dashboard-Organization-Show High Risk Organization Aggregate Resources
Views	/org/showHighRiskOrgApplicationsList	313-8	Dashboard-Organization-Show High Risk Organization Applications
Views	/resource/edit	309-1	Manage-Resources[Edit Resource]
Views	/resource/deleteResourceData	309-0	Manage-Resources[Delete Resource Data]
Views	/resource/editActivityAttribute	308-9	Manage-Resources[Edit Activity Attribute]
Views	/organization/showResourcesforOrg	303-9	Manage-Organizations[shows Resources of Organization]
Views	/organization/showAddUsersDialog	307-1	Manage-Organization[Add Users to Organization]

Category	URL	ID	Description
Views	/organization/removeUsersFromOrg	307-2	Manage-Organizations[Remove Users From Organization]
Views	/peer/deletePeerType	307-3	Manage-Peers [Delete Peer Type]
Views	/peer/showAddUsersDialog	307-4	Manage-Peers [Add Users to Peer]
Views	/peer/removeUsersFromPeer	307-5	Manage-Peers [Remove Users From Peer]
Views	/users/delete	307-7	Manage-Users [Delete User]
Views	/reports/runTopNReports	304-4	Manage-Resources[Top N Charts]
Views	/organization/showJobForAssignmentRules	417-4	Organization-Show Job for Assignment Rules
Views	/manageData/showOrgSearch	203-0	Manage-Organizations
Views	/organization/isNameDuplicate	417-7	Organization-Check if Name is Duplicate
Views	/resource/showResourceGroupDetails	203-5	Manage-Resource-Resource name link [shows resource details]

Category	URL	ID	Description
Views	/org/	405-1	Show Organization View
Views	/org	405-2	Enable Organization View
Views	/org/showOrgRiskHistoryChart	405-3	Organization-Show Organization Risk History Chart
Views	/org/showHighRiskOrgs	203-1	Dashboard-Security Dashboard-High Risk Organizations
Views	/organization/showCreateOrgDialog	310-5	Manage-Organizations[Show Create Organization]
Views	/manageData/showAppSearch	202-9	Manage-Applications
Views	/lookupTable/deleteLookupTableEntry	411-7	Delete Lookup Table Entry
Views	/resource/importResources	200-6	Manage-Resources[shows import resource screen]
Views	/lookupTable/autocompleteSearch	411-8	LookupTable-Autocomplete Search
Views	/lookupTable/getMaxRows	412-0	LookupTable-Get Max Rows
Views	/organization/listSelectOrganization	415-5	List Select Organization

Category	URL	ID	Description
Views	/lookupTable/index	412-1	View Look-upTable
Views	/lookupTable/listLookupTableData	412-2	List Lookup Table Data
Views	/lookupTable/filterLookupTables	412-3	Filter Lookup Tables
Views	/lookupTable/	412-4	Show Look-upTable
Views	/lookupTable/createLookuptable	412-5	Create Lookup Table
Views	/lookupTable/listLookupTables	412-6	ListLookupTables
Views	/lookupTable	412-7	Enable Look-upTable View
Views	/organization/addChildOrganizationsList	414-5	Add Child Organizations List
Views	/organization/showAssignmentRules	414-7	Organization-Show Assignment Rules
Views	/organization/resumeJob	414-9	Organization-Resume Job
Views	/organization/loadCAssociationRule	415-0	Organization-Show Association Rule
Views	/organization/showAddOrg	415-1	Show Add Organization
Views	/organization/showSchedulePeerAssignmentRule	415-2	Organization-Show Schedule Peer Assignment Rule

Category	URL	ID	Description
Views	/org/getUpdatedToken	405-0	Organization-Get Updated Token
Views	/org/beforeInterceptor	404-9	Organization-Before Interceptor
Views	/org/updateOrgRiskScores	314-3	Dashboard-Organization-Update Organization Risk Score
Views	/lookupTable/updateRowValues	411-9	LookupTable-Update Row Values
Views	/organization/	417-8	Views-Show Organization
Views	/organization/reRunJob	417-9	Organization-reRun Job
Views	/organization/treeView	418-1	Organization-Tree View
Views	/organization	418-2	View-Enable Organization View
Views	/organization/listUsersNotInOrg	418-3	List Users Not In Organization
Views	/organization/showOrgResourceGroups	418-4	Show Organization Resource Groups
Views	/organization/list	418-5	Organization-List
Views	/peer/peerSearchAjax	422-4	Peer Search Ajax

Category	URL	ID	Description
Views	/resource/quickSearchResourceGroupAJAX	424-4	Quick Search Resource Group using AJAX
Views	/resource/getAccessLastRunData	427-9	Resource-Get Access Last Run Data
Views	/resource/listResourceTypes	428-5	List Resource Types
Views	/resource/loadResourcesGroups	433-4	Load Resources Groups
Views	/organization/searchAJAX	417-5	Organization-Search usingAJAX
Views	/resource/getActivityLastRunData	440-4	Resource-Get Activity Last Run Data
Views	/users/userSearchAjax	447-7	Users-Search Users
Views	/watchList/listWatchList	450-9	Watchlist-List of WatchLists
Views	/watchList/saveWatchList	452-0	Watchlist-Save WatchList
Views	/manageData/manageWatchlist	305-8	Manage-Watch-lists
Views	/whiteList/	452-6	Views-Enable Whitelist
Views	/whiteList/showWhitelist	452-7	Views-Show Whitelist

Category	URL	ID	Description
Views	/org/showPendingAssignments	314-7	Dashboard-Organization-Show Pending Assignments
Views	/org/showPendingAssignmentsList	314-8	Dashboard-Organization-Show Pending Assignments List View
Views	/org/showHighRiskOrgsByCategory	314-9	Dashboard-Organization-Show High Risk Organization By Category
Views	/organization/searchTreeElement	416-3	Organization-Search Tree Element
Views	/organization/listApplicationNotInOrganisation	416-1	List Application Not In Organisation
Views	/organization/showOrgDetails	416-0	Show Organization Details
Views	/resource/getResourcesForGroup	442-8	Get Resources For Group
Views	/organization/removeChildOrganizations	310-4	Manage-Organizations[Remove Child Organizations from Organization]
Views	/peer/pauseCreationJob	188-0	Manage-Peers-Peer Creation Rules[pause peer creation rule job]

Category	URL	ID	Description
Views	/organization/removeResourcesFromOrg	310-2	Manage-Organizations[Remove Resources from Organization]
Views	/resource/addResourcePeers	457-6	Add resource peers
Views	/resource/removePeersFromResources	457-7	Remove peers from resources
Views	/resource/getResourcesPeerList	457-8	View resources peer list
Views	/spotter/loadDashboard	458-7	Spotter [NLP Search Engine]
Views	/peer/showSchedulePeerAssignmentRule	188-5	Manage-Peers-Peer Assignment Rules[shows peer assignment rule job screen]
Views	/resource/getActivityIPPaginatedList	460-8	Display activity IP paginated list
Views	/resource/profileTypeMapping	460-7	Allow profile type mapping for resource
Views	/resource/getAccountsPaginatedList	460-6	Display paginated list for resources
Views	/resource/showBehavior	191-4	Manage-Resources-Behavior profile[shows resource behavior]

Category	URL	ID	Description
Views	/resource/showDataManagement	191-3	Manage-Resources-Access Management[shows access management screen]
Views	/resource/resourceAccessAccounts	191-2	Manage-Resources-Access Accounts [shows list of access accounts]
Views	/peer/createRule	188-6	Manage-Peers-Peer Assignment Rules[runs peer creation job]
Views	/peer/resumeCreationJob	188-1	Manage-Peers-Peer Creation Rules[resume peer creation rule job]
Views	/peer/removeResourcesFromPeer	459-8	Allow to remove resources from peer
Views	/peer/listResourcesNotInPeer	460-4	Display resources to add in peers
Views	/manageData/showProfileDetails	183-0	Manage-Profiles [shows profile details]
Views	/manageData/showEditProfile	183-1	Manage-Profiles [shows edit profile screen]

Category	URL	ID	Description
Views	/manageData/showUsersforProfile	183-2	Manage-Profiles [shows list of users of profile]
Views	/manageData/showResourcesForProfile	183-3	Manage-Profiles [shows list of resources of profile]
Views	/manageData/updateProfile	183-4	Manage-Profiles [update values for profiles received from edit profile screen]
Views	/manageData/showCreateProfile	183-5	Manage-Profiles [shows create profile screen]
Views	/manageData/saveProfile	183-6	Manage-Profiles [saves values for profiles received from create profile screen]
Views	/manageData/showResourceSearch	183-7	Manage-Resources[shows list of Resources with sub menu]
Views	/users/list	183-8	Manage-Users [shows list of users]
Views	/peer/searchResourcePeerAJAX	460-1	Allow resource peer search
Views	/resource/showResourcesPeer	457-5	Show resource peer view

Category	URL	ID	Description
Views	/peer/loadSearchBar	460-2	Display peer search bar
Views	/peer/listResourcePeers	457-3	View resource peers
Views	/resource/getProfileTypesForName	461-1	Display profile types for name in resource
Views	/resource/listActivityAttributes	190-4	Manage-Resources-Activity Attributes [shows list of activity attributes]
Views	/resource/update	190-3	Manage-Resources [update value for resource received from edit resource screen]
Views	/resource/showResource	190-1	Manage-Resources[shows resource values]
Views	/users/showCreateUserDialog	183-9	Manage-Users [shows create new user screen]
Views	/resource/addAccessAttribute	189-3	Manage-Resources[save values for access attribute received from create access attribute screen]

Category	URL	ID	Description
Views	/resource/showResourceUsage	190-0	Manage-Resources[shows resource usage]
Views	/resource/showResourceDetails	189-9	Manage-Resources[shows resource details with tabs]
Views	/resource/save	189-8	Manage-Resources-Create Resource[save values for resource recieved from create resource screen]
Views	/resource/create	189-7	Manage-Resources-Create Resource[shows create resource screen]
Views	/resource/saveResourceGroup	189-6	Manage-Resources[save values for resource group recieved from create resource group screen]
Views	/resource/showCreateResourceGroupDialog	189-5	Manage-Resources-Create Resource Group [shows create resource group screen]

Category	URL	ID	Description
Views	/resource/updateActivityAttribute	190-9	Manage-Resources-Activity Attributes [update value for activity attribute received from edit activity attribute screen]
Views	/resource/listAccessAttributes	189-1	Manage-Resources[shows list of access attributes]
Views	/resource/updateResourceGroup	189-0	Manage-Resources [update value for resource group received from edit resource group screen]
Views	/resource/editResourceGroup	188-9	Manage-Resources[shows edit resource group screen]
Views	/resource/listResourcesForResourceGroup	188-8	Manage-Resources[shows list of resources]
Views	/resource/listResourceGroups	188-7	Manage-Resources[shows list of resource groups]

Category	URL	ID	Description
Views	/resource/addActivityAttribute	190-6	Manage-Resources-Activity Attributes[save values for activity attribute recieved from create activity attribute screen]
Views	/resource/accountTypeMapping	460-9	Allow account type mapping for resource
Views	/resource/resourceAccounts	191-0	Manage-Resources-Accounts[shows accounts]
Views	/resource/showResourceAccounts	191-1	Manage-Resources-Accounts[shows list of accounts]
Views	/watchList/listResourcesNotInWatchlist	461-5	Show resources not in watchlist
Views	/watchList/listIPAddressNotInWatchlist	461-4	Show IP address for watchlist
Views	/users/getAccountsPaginatedList	461-3	Show users accounts paginated list
Views	/resource/getResourcePaginatedList	461-2	Show resource paginated list
Views	/resource/loadBehaviorProfileDisplay	461-0	Show behavior profile display for resource

Category	URL	ID	Description
Views	/organization/showAddChildOrganizationDialog	310-3	Manage-Organizations[Add Child Organizations to Organization]
Views	/peer/getPaginateResourcesForPeer	460-3	Paginate resources for peer
Views	/peer/showAssignmentRules	188-3	Manage-Peers-Peer Assignment Rules
Views	/peer/addResourcesToPeer	459-9	Allow adding of resources to peer
Views	/peer/showAddResourcesDialog	460-0	Display add resource dialog
Views	/lookupTable/showLookupTableData	316-3	Manage-Lookup Table-[Shows List of Lookup Tables with filters]
Views	/peer/showCreatePeerDialog	186-6	Manage-Peers-Create Peer Manually[shows create peer screen]
Views	/peer/showUsersforPeer	186-5	Manage-Peers [shows list of users in the peer]
Views	/peer/showPeerBehavior	186-4	Manage-Peers Behavior[shows peer behavior]
Views	/peer/delete	186-3	Manage-Peers [delete peer]

Category	URL	ID	Description
Views	/peer/update	186-2	Manage-Peers [update value for peer received from edit peer screen]
Views	/peer/edit	186-1	Manage-Peers [shows edit peer screen]
Views	/peer/showPeerDetails	186-0	Manage-Peers [shows peer details]
Views	/peer/list	185-9	Manage-Peers [shows list of peers]
Views	/peer/save	186-7	Manage-Peers [saves values for peer received from create peer screen]
Views	/organization/update	307-0	Manage-Organizations[Update organization]
Views	/watchList/manageWatchlist	316-2	Manage-Watchlist-[Shows List of watchlists with filters]
Views	/org/showHighRiskOrgUsersList	314-0	Dashboard-Organization-Show High Risk Organization Users

Category	URL	ID	Description
Views	/users/addOrgs	309-2	Manage-Users [Add Organizations]
Views	/users/removeOrgsFromUser	309-3	Manage-Users [Remove Organizations]
Views	/users/addPeers	309-4	Manage-Users [Add Peers]
Views	/users/removePeersFromUser	309-5	Manage-Users [Remove Peers]
Views	/peer/editPeerType	309-6	Manage-Peers [Show Edit Peer]
Views	/peer/updateCriticality	309-7	Manage-Peers [Update Criticality]
Views	/resource/updateResourceAttributes	309-8	Manage-Resources [Update Resource Attributes]
Views	/organization/showAddApplicationDialog	309-9	Manage-Organizations [Add Applications to Organization]
Views	/organization/removeApplicationsFromOrg	310-0	Manage-Organizations [Remove Applications from Organization]
Views	/organization/showAddResourcesToOrgDialog	310-1	Manage-Organizations [Add Resources to Organization]

Category	URL	ID	Description
Views	/peer/createPeerCreationRule	187-0	Manage-Peers-Peer Creation Rules[shows peer creation rule job screen]
Views	/resource/searchAJAXForResources	460-5	Allow resources search
Views	/peer/deleteJob	187-1	Manage-Peers-Peer Assignment Rules[delete peer assignment rule job]
Views	/peer/reRunJob	187-3	Manage-Peers-Peer Assignment Rules[rerun peer assignment rule job]
Views	/users/update	185-2	Manage-Users [update values for User received from edit user screen]
Views	/users/edit	185-1	Manage-Users [shows edit user screen]
Views	/users/showBehavior	185-0	Manage-Users [shows behavior profile]
Views	/users/showUserProfiles	184-9	Manage-Users [shows users profiles]

Category	URL	ID	Description
Views	/users/showUserAccessAccounts	184-8	Manage-Users [shows access accounts of user]
Views	/users/showUserAccess	184-7	Manage-Users [shows user access]
Views	/users/showUserPeers	184-6	Manage-Users [shows peer groups of user]
Views	/users/show	184-5	Manage-Users [shows general details of user]
Views	/users/showRiskyUserAccounts	184-4	Manage-Users [shows high risk accounts for user]
Views	/users/showUserRiskScorecard	184-3	Manage-Users [shows riskscore-card for user]
Views	/users/showUserBehavior	184-2	Manage-Users [shows behavior profile for user]
Views	/users/showEventsSummary	184-1	Manage-Users [shows monitor activites for user]
Views	/manageData/listProfiles	182-9	Manage-Profiles [shows list of profiles]
Views	/manageData/showManageProfiles	182-8	Manage-Profiles [shows list of profiles with sub menu]

Category	URL	ID	Description
Views	/manageData/showPeerSearch	182-7	Manage-Peers [shows list of parent and child peers with sun menu]
Views	/peer/listParents	185-8	Manage-Peers [shows list of parent peers]
Views	/peer/interruptCreationJob	188-2	Manage-Peers-Peer Creation Rules[interrupt peer creation rule job]
Views	/users/showUserDetails	184-0	Manage-Users [shows users details with tabs]
Views	/manageData/showUserSearch	182-6	Manage-Users [shows list of users with sub menu]
Views	/peer/reRunCreationJob	187-9	Manage-Peers-Peer Creation Rules[rerun peer creation rule job]
Views	/peer/cancelCreationJob	187-8	Manage-Peers-Peer Creation Rules[cancel peer creation rule job]
Views	/peer/deleteCreationJob	187-7	Manage-Peers-Peer Creation Rules[delete peer creation rule job]

Category	URL	ID	Description
Views	/peer/interruptJob	187-6	Manage-Peers-Peer Assignment Rules[interrupt peer assignment rule job]
Views	/peer/resumeJob	187-5	Manage-Peers-Peer Assignment Rules[resume peer assignment rule job]
Views	/peer/pauseJob	187-4	Manage-Peers-Peer Assignment Rules[pause peer assignment rule job]
Views	/peer/cancelJob	187-2	Manage-Peers-Peer Assignment Rules[cancel peer assignment rule job]
Views	/whiteList	452-5	Views-Whitelist

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 (Micro Focus ArcSight 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 arst-techpubs@hpe.com.

We appreciate your feedback!