Hewlett Packard
Enterprise

HPE Security ArcSight User Behavior Analytics

Software Version: 5.0

Application Insight Packs Guide

July18, 2016

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

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

HPE Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Support

Contact Information

Phone	A list of phone numbers is available on the HPE Security ArcSight Technical Support Page: https://softwaresupport.hpe.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hpe.com
Protect 724 Community	https://www.protect724.hpe.com

Contents

Introduction

The HPE ArcSight UBA Application Insight Packs are extensions to the HPE Security ArcSight User Behavior Analytics products, and provide out-of-the-box application log collection and monitoring for the following applications:

- Amazon Web Services (AWS)
- Box
- Cerner
- Epic
- Google Apps

In this manual, you will find a brief description of each the Application Insight Packs, how to configure the application log collection, and the list of out-of-the-box content (policies, behavior profiles).

AWS Insight Pack

Description

Amazon Web Services (AWS) is a cloud computing platform provided by Amazon.com. AWS CloudTrail is a web service that records Amazon Web Services API calls for each account and provides the ability to retrieve theses logs. The log files include information such as the time of the API call, the identity and the source IP address of the API caller, the request parameters and the response elements returned by the AWS service. This log file information can be used for security analysis, resource change tracking, and compliance auditing.

For more information, go to the following URL: http://aws.amazon.com/cloudtrail/

The HPE ArcSight UBA AWS Insight Pack leverages the AWS CloudTrail web service to retrieve all the logs from AWS, provides visibility into activities performed in the AWS instance, and detects privilege abuse and abnormal behavior for users managing the AWS instances.

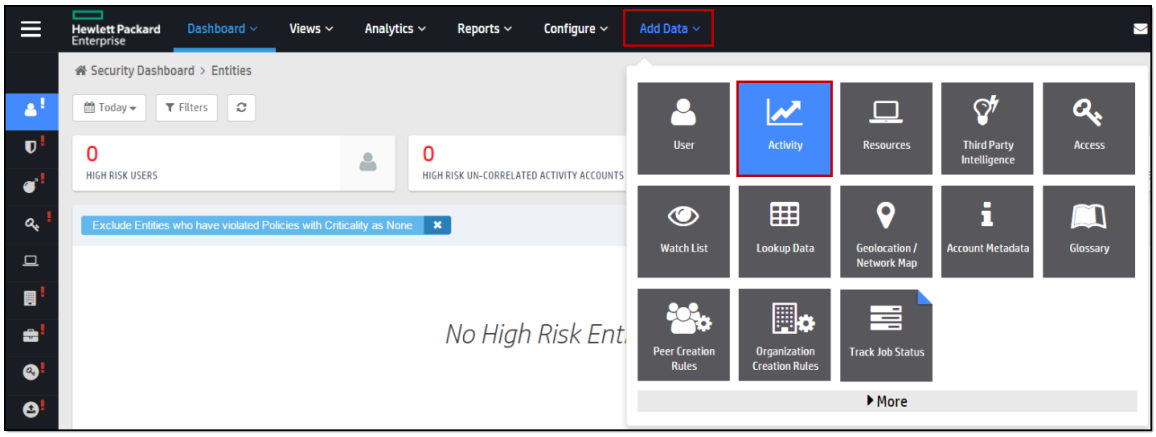
Creating the Data Source

HPE ArcSight UBA provides connection to AWS to pull in activity data. To connect to AWS, you will need following information:

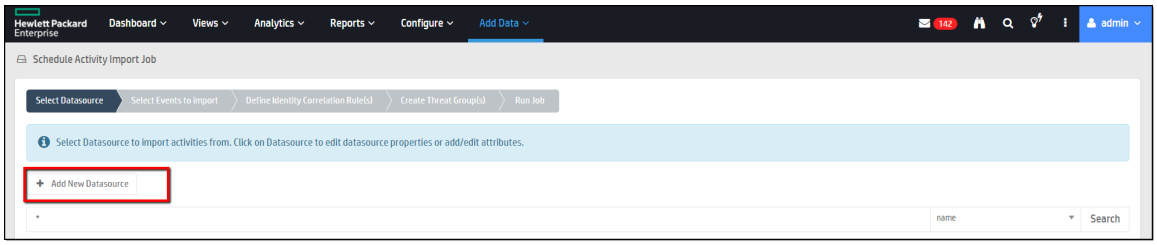
- AWS Access Key
- AWS Secret Key
- AWS Bucket

To create an AWS data source connection in HPE ArcSight UBA, use the following steps:

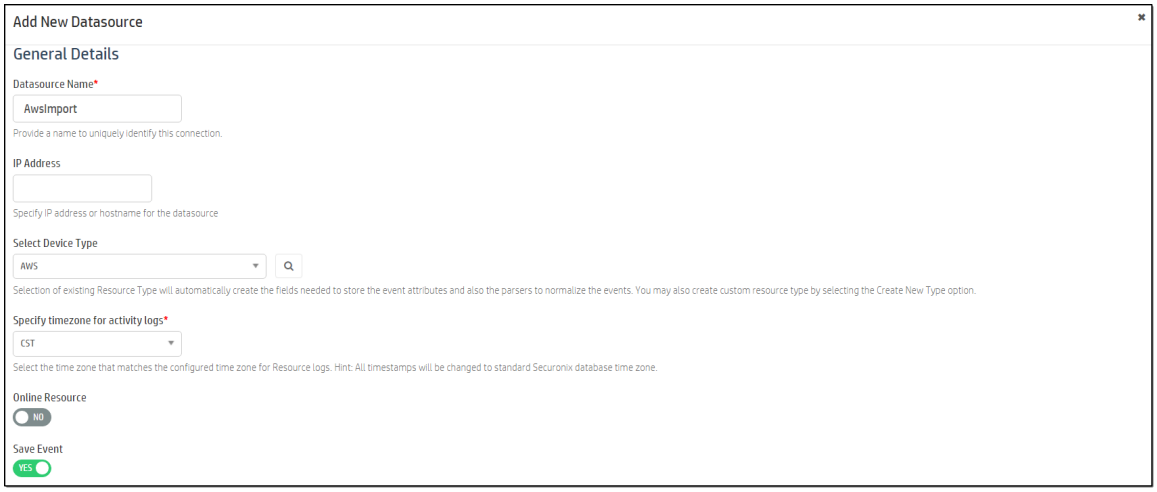
1. Navigate to **Add Data > Activity**.



2. On the Schedule Activity Import Job tab, click **Add New Datasource**.

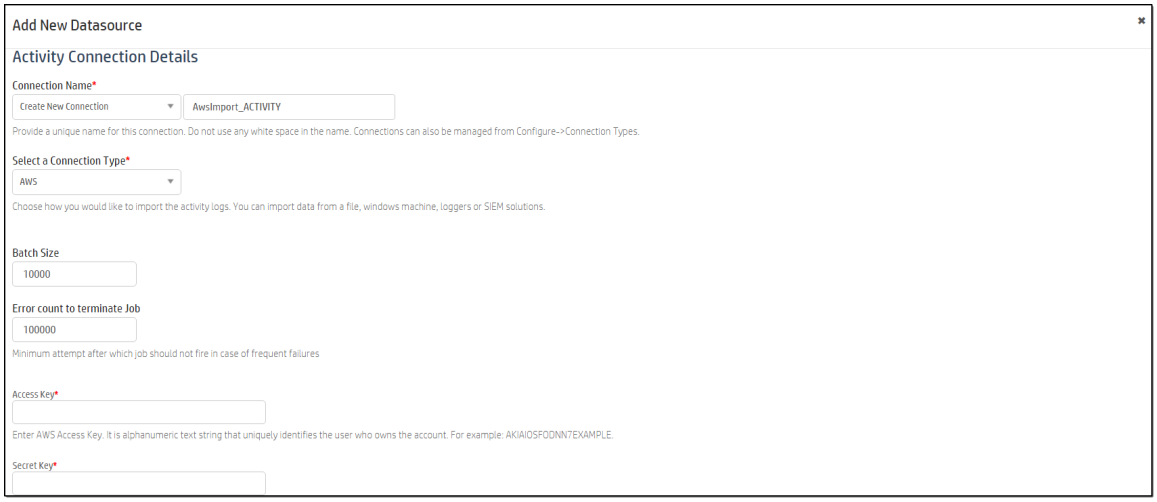


3. In the General Details section, provide the following information:

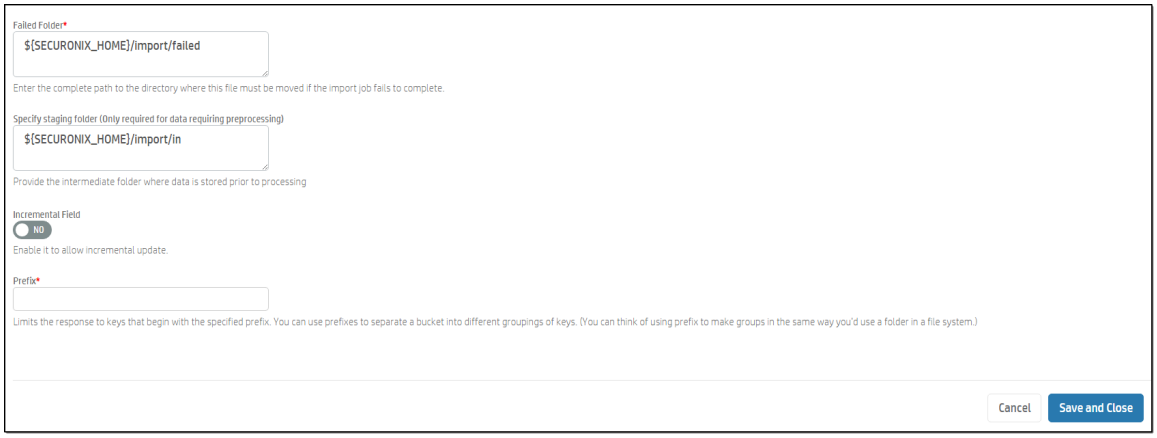


   a. Specify a **Datasource Name**.
   b. (Optional) Specify the **IP Address** or hostname for the datasource.
   c. From the **Select Device Type** drop-down list, choose **AWS** or create a new device type if AWS does not exist.
   d. From the **Specify timezone for activity logs** drop-down list, select a timezone.

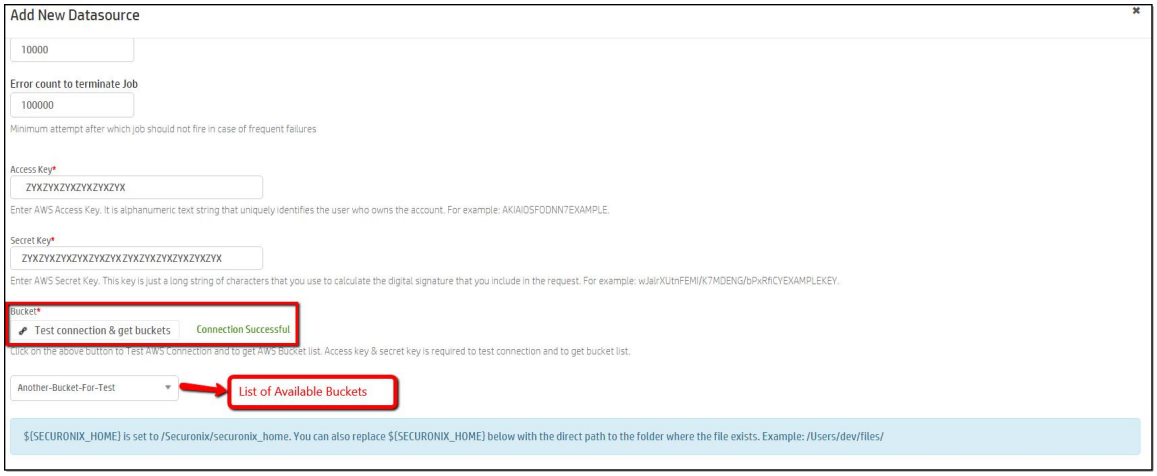
4. In the Activity Connection Details section, provide the following information:



   a. Provide a unique **Connection Name**, or use the default.
   b. From the **Select a Connection Type** drop-down, choose **AWS**.
   c. Provide the **Batch Size** and **Error count to terminate job**.
   d. Enter the **Access Key** and **Secret Key**.
   e. If your connection is successful, you should see a list of buckets in the **Bucket** drop-down list. Select the bucket you would like to use and add a **Prefix** (optional) if you would like to limit the response to keys that begin with the specific prefix.



5. To save the new connection, click **Save and Close**.
   The following image shows an example of a successful connection:



6. Click **Save and Next**, and then, to finish setting up the AWS activity import, proceed with steps 2 through 5 of the Add Activity Data section in the *HPE ArcSight UBA Administration Guide*.

Content

Policies				
Signature ID	**Policy Name**	**Policy Description**	**Policy Type**	**Criticality**
1000038	Activity by Terminated account – AWS	Inactive user performing activities.	Rule-based	High
1000044	Non AWS Approved user using AWS Services	User that is not on the approved list of users for AWS is performing AWS activities.	Rule-based	Low

Box Insight Pack

Description

Box is an online file sharing and personal cloud content management service for businesses providing a cloud-based enterprise content collaboration platform that enables organizations of various sizes to access, store, share and manage their content and information.

For more information, go to the following URL: https://www.box.com/

The HPE ArcSight UBA Box Insight Pack imports file sharing and administrative events from Box, provides visibility into activities performed on the Box platform and analyzes the log data for data snooping, data theft, and account abuse.

Connector

HPE ArcSight UBA provides a connection to Box to pull in activity data. In order to get the activity data from Box, you will need an admin account on Box.com for the application from which you intend to import data into HPE ArcSight UBA.

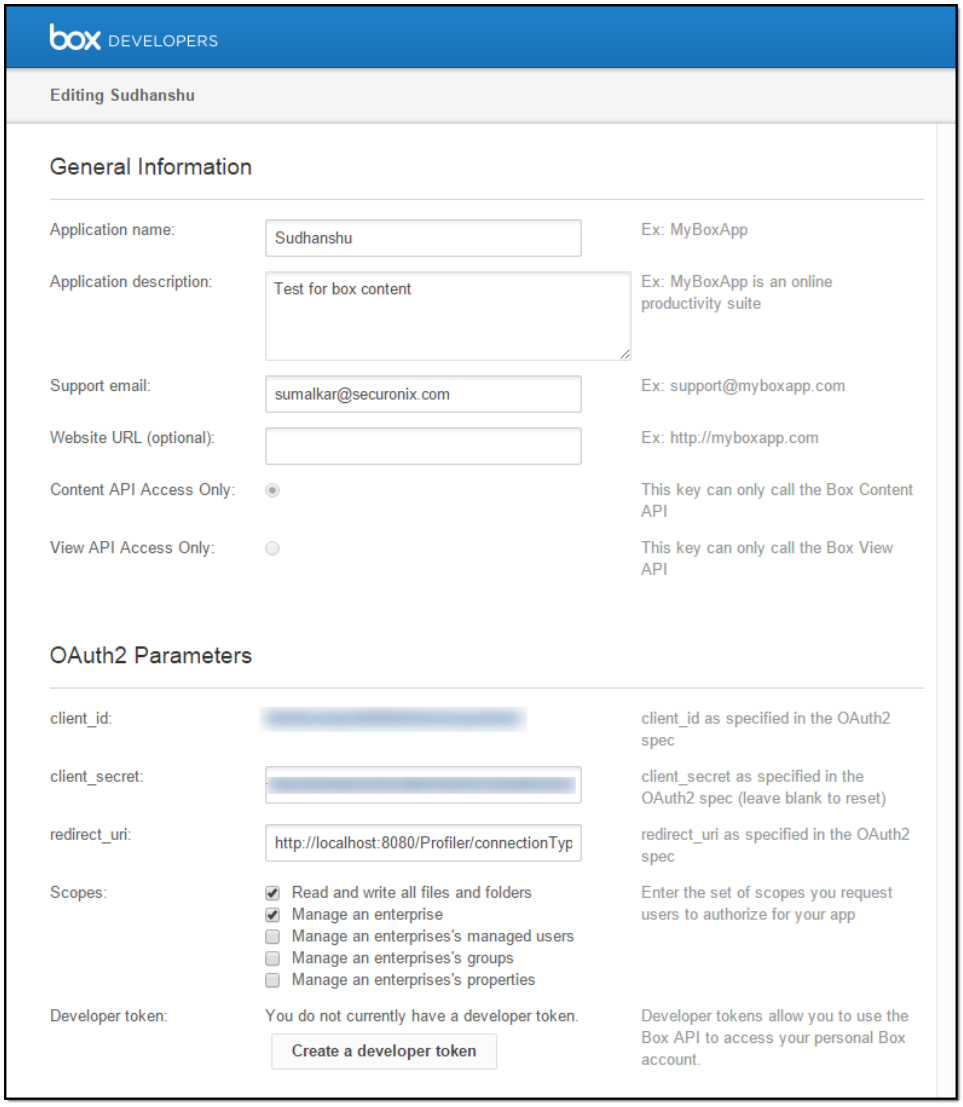
1. Edit the application on Box.com and provide the following information:

   - Client_ID
   - Client_Secret
   - Redirect_URL

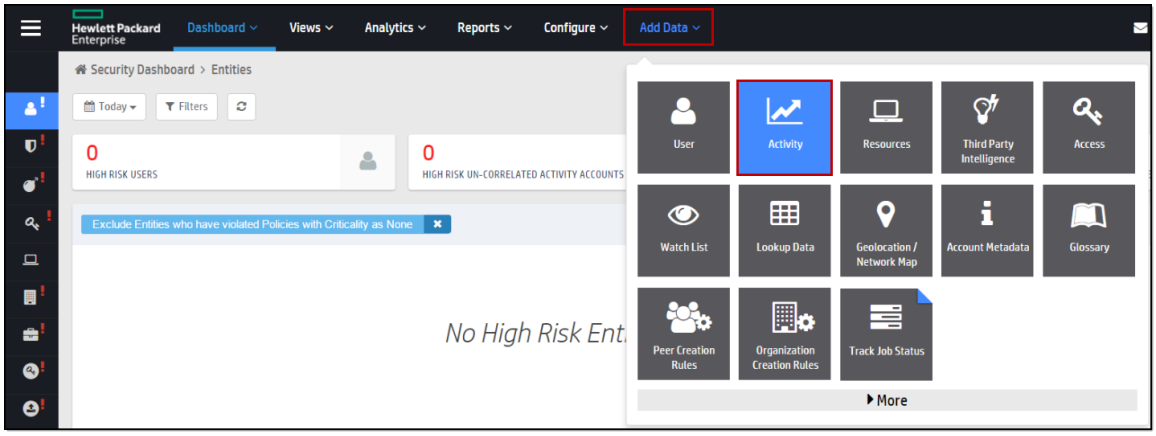
     Example of **Redirect URL**:

     "http://localhost:8080/Profiler/connectionType/generateOauthCode"

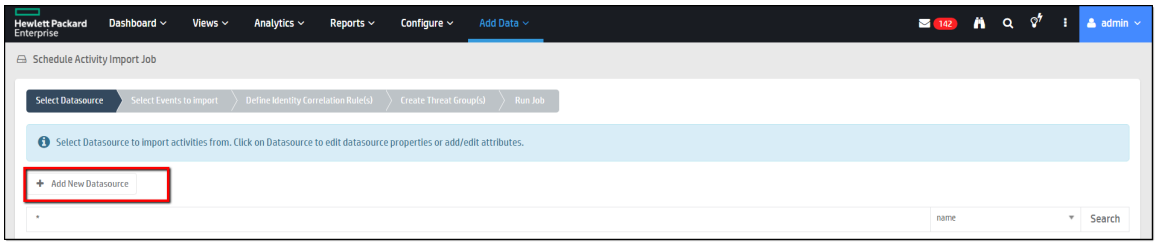
     Please provide your application's URL instead of "localhost:8080". This redirect URL will be used for creating an Access Token later while creating connections.


box DEVELOPERS
Editing Sudhanshu
General Information
Application name:
Sudhanshu
Ex: MyBoxApp
Application description:
Test for box content
Ex: MyBoxApp is an online productivity suite
Support email:
sumalkar@securonix.com
Ex: support@myboxapp.com
Website URL (optional):
Ex: http://myboxapp.com
Content API Access Only:
This key can only call the Box Content API
View API Access Only:
This key can only call the Box View API
OAuth2 Parameters
client_id:
client_id as specified in the OAuth2 spec
client_secret:
client_secret as specified in the OAuth2 spec (leave blank to reset)
redirect_uri:
http://localhost:8080/Profiler/connectionTyp
redirect_uri as specified in the OAuth2 spec
Scopes:
Read and write all files and folders
Manage an enterprise
Manage an enterprises's managed users
Manage an enterprises's groups
Manage an enterprises's properties
Enter the set of scopes you request users to authorize for your app
Developer token:
You do not currently have a developer token.
Create a developer token
Developer tokens allow you to use the Box API to access your personal Box account.

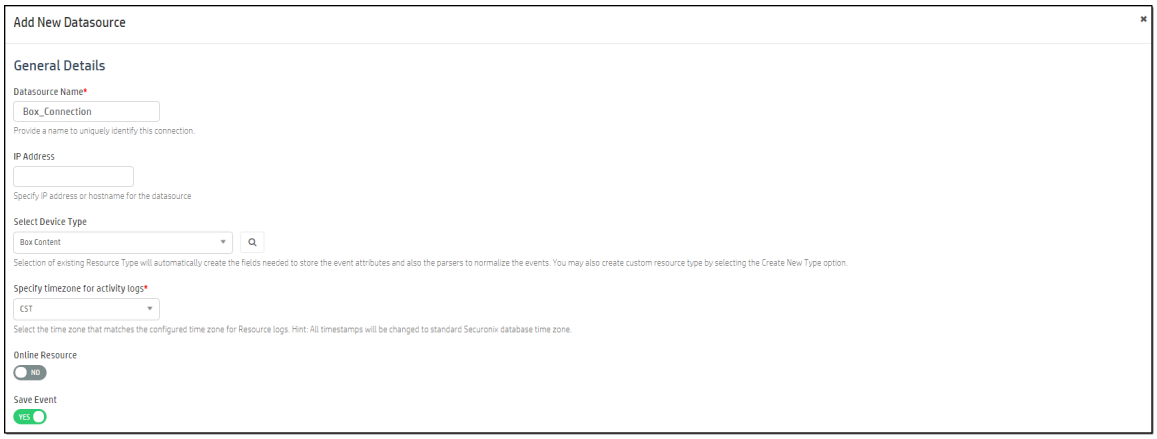
2. To make a connection, navigate to **Add Data > Activity**.



3. Click **Add New Datasource**.



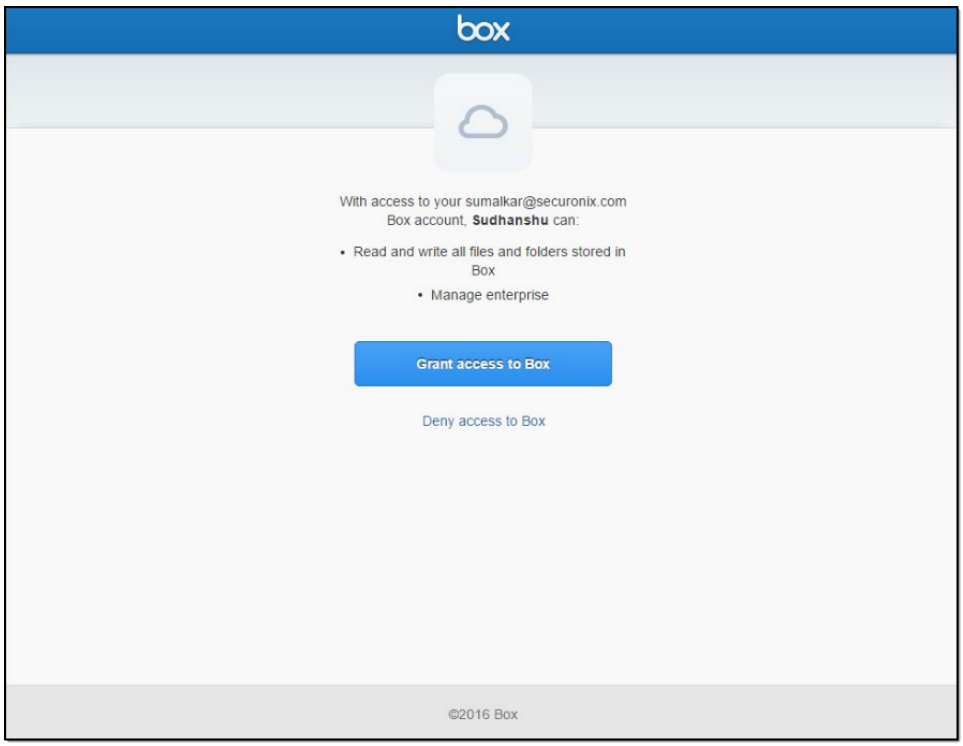
4. In the General Details section, provide the following information:



   a. Specify a **Datasource Name**.
   b. (Optional) Specify the **IP Address** or hostname for the datasource.
   c. From the **Select Device Type** drop-down list, choose **Box Content** or create a new device type if Box Content does not exist.
   d. From the **Specify timezone for activity logs** drop-down list, select a timezone.

5. In the Activity Connection Details section, provide the following information:

a. Provide a unique **Connection Name**, or use the default.
b. From the **Select a Connection Type** drop-down list, choose **Box Content**.
c. Provide the **Batch Size** and **Error count to terminate job**.
d. In the **Key** field, enter the key you received from Box during the initial account creation.
e. In the **Secret** field, enter the secret you received from Box during the initial account creation.
f. Click Generate Tokens, and then grant access to Box.



6. After the access and refresh tokens have been generated, click **Populate Tokens** in the HPE ArcSight UBA application.

7. The Access Tokens and Refresh Tokens are populated:

8. Click **Save and Close**.
9. You can now select the new data source and click **Preview** to see the data.

10. Click **Save and Next**, and then, to finish setting up the Box activity import, proceed with steps 2 through 5 of the Add Activity Data section in the *HPE ArcSight UBA Administration Guide*.

Content

Policies				
Signature ID	**Policy Name**	**Policy Description**	**Policy Type**	**Criticality**
1000069	Activity by Terminated account	Inactive users performing activities.	Rule-based	High

Cerner Insight Pack

Description

Health IT company Cerner is one of the largest suppliers of electronic health record systems in the country. Cerner EMR systems are used within some of the largest health systems in the country. Cerner created EMR to allow healthcare professionals to store, capture, and access patient health information electronically in both acute and ambulatory care settings. By digitizing electronic health-care records and centralizing their access, the Cerner application provides tremendous efficiencies to healthcare workers. However, the healthcare records and financial records of customers must be protected within the Cerner application.

For more information, go to the following URL: http://www.cerner.com

The HPE ArcSight UBA Cerner Insight Pack imports data from Cerner and provides real time monitoring and threat detection against data snooping (family, neighbor, friend, VIP), inappropriate and suspicious access to healthcare records, break the glass event auditing and deceased patient record snooping.

Connector

Understanding Cerner Event Logs

How do Cerner Audit Logs work?

Cerner EMR uses a messaging queue system to handle logging of its auditable events.

1. As messages are put on the queue, Cerner EMR will send that data to the HPE ArcSight UBA application (HTTP protocol) as an audit event message.
2. The HPE ArcSight UBA application receives a message from Cerner EMR, writes this message to a log file, and then responds to Cerner EMR with a message containing the number of records received.
3. This log file is then imported into the HPE ArcSight UBA application.

Define Which Events to Audit

The Cerner Millennium tool, **ppraudteventmanager.exe** is used to select the audit events that are sent to HPE ArcSight UBA. This application can be found in the "C:\Program Files\Cerner" directory on a Citrix server hosting the front-end applications for the environment being audited.

Use the following steps to select and enable events:

1. Log in to the **ppraudite ventmanager.exe** tool with DBA rights.
2. Select the events your organization would like to audit or import a list of pre-selected events provided by your Cerner consultant.
3. After the events have been selected, save your selections and exit the tool.
4. If auditing is turned on, after five minutes, Server 30 will have recognized your selected events and will start sending those events.

Test Connectivity

In order to configure the Cerner Millennium back end for auditing, you must have DBA access to the system.

1. Configure ports:
   - The default configuration is: Primary: 8081 Secondary: 8181
   - If the default settings need to be modified, simply make the changes by navigating to **Configure > Connection Types**. Select the **CernerListener** connection type and change the port.
2. Test Server Connectivity:
   - From Cerner Audit Servers, test the IP and port number to make sure all servers can connect and there are no firewall issues. TCP ports 8081 and 8181 may need to be opened on any intermediary network firewalls.
   - Connectivity verification to port level can be tested using a Telnet client as follows:

     ```
     telnet <SECURONIX_APPLIANCE_IP> 8081 [enter]
     GET / HTTP/1.0 [enter] [enter]
     ```
   - A successful response to these commands should include the line:

     ```
     HTTP/1.1 200 OK
     ```

     If you do not receive this message and have verified that the HPE ArcSight UBA application is configured and ready to accept Cerner auditing traffic, a network or firewall issue is the likely cause.

Configure Destination for Audit Events

1. Log in to the back-end application node and enter the registry for Cerner (lregview).
2. Update the registry key.
3. If you do not have auditing turned on, add the key.
4. If you do have auditing turned on, modify the key:

```
Enter lregview
CD to \\environment\<domain>\node\<node name>
```

```
MD VisualGold
CD VisualGold
```

5. Configure where the audit messages will be sent:

```
setp . url http://<SECURONIX_IP_or_DNS_NAME>:8081/Iguazu-Rts/
CernerListener
setp . alt_url http://<SECURONIX_IP_or_DNS_NAME>:8181/Iguazu-Rts/
CernerListener
Configure Authorization
setp . auth cerner:<password>
setp . alt_auth cerner:<password>
exit lregview
```

6. Update the system to recognize the changes (Start Cerner 500).

```
$cer_mgr_exe/start_cerner_500 -env common,<environment name> -
noinst -verbose newgrp - d_<domain>
```

7. Turn on Security (this should already be on):

   - Start Server 32: Security Master if it's not started already.

Configure Destination for Audit Events

1. Turn on Auditing.
2. If server 70 and 71 are not configured to run:

```
cycle server 30
enterscp
modify 70 –inst 1
start 70
```

   Check to make sure running "server – entry 70"

```
modify 71 -prop callvg=y
modify 71 -inst 1
start server 71
exit scp
```

3. If server 70 and 71 are already running, then cycle both servers across the domain.

Note: In order to start seeing data in the queue, there must be activity on the system. After the servers have been reconfigured and started, you will start to see messages in the queue within a few minutes. These messages will then leave the queue and be received by the HPE ArcSight UBA application.

Configure Cerner Listener on HPE ArcSight UBA

1. Create a new connection type for receiving events:
    a. Enter a port number.
    b. Make sure that the device firewall is configured to receive events on this port.
    c. At this stage, both servers should be connected and sending data back-and-forth to each other.
    d. Review the data on the HPE ArcSight UBA application by navigating to the folder set up for storing events.
2. Import Events:
    a. Create a new resource group for the Cerner instance.
    b. Select resource type as **Cerner Millennium**.
    c. Create Correlation rules.
    d. Schedule import job.

Audit Exception

Cerner AUDIT.EXCEPTION Queue

Reprocessing Queues: In the event that messages are not sent to the HPE ArcSight UBA application, they will start to queue on the Cerner side into the AUDIT.EXCEPTION queue. If this happens, it is possible to resend those messages to the HPE ArcSight UBA application. The following command enables you to resend those missed messages:

In QCP:

```
requeue -all CPMSRVAUDITBATCH -src AUDIT.EXCEPTION
```

Sample Cerner Feed

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<srvhandle><audit_list>
<audit_version>1</audit_version>
<event_dt_tm>2008-07-30 14:04:15.00</event_dt_tm>
<outcome_ind>0</outcome_ind>
<user_name></user_name>
<prsnl_id> 0</prsnl_id>
<prsnl_name></prsnl_name>
<role></role>
<role_cd> 0</role_cd>
<enterprise_site>HNAM</enterprise_site>
<audit_source>CERT</audit_source>
<audit_source_type>1</audit_source_type>
<network_acc_type>1</network_acc_type>
```

```
<network_acc_id>CERCERTCITRIX</network_acc_id>
<context><![CDATA[]]></context>
<application></application>
<task></task>
<request></request>
<appl_ctx></appl_ctx>
<perform_cnt></perform_cnt>
<event_list>
<event_name>Logon Attempt</event_name>
Cerner Response
<?xml version=\"1.0\"?>
<securelog>
<status>
<result>OK</result>
<COUNT>4</COUNT>
</status>
</securelog>
```

Cerner Response

```
<?xml version=\"1.0\"?>
<securelog>
<status>
<result>OK</result>
<COUNT>4</COUNT>
</status>
</securelog>
```

Content

Cerner [Database]

Policies				
Signature ID	**Policy Name**	**Policy Description**	**Policy Type**	**Criticality**
649001	Employee Accessing Records of Deceased Patient [Cerner DB]	This policy detects users who perform activity on deceased patient's records. This indicates possible account misuse and data theft.	Rule-based	High
649002	Account Performing Cerner Activity Never Conducted Before [Cerner DB]	This is behavior-based, suspect-check-based policy detects when an account is performing activity that has never been performed before.	Behavior-based	High
649003	Activity by Terminated User [Cerner DB]	This policy detects terminated users who perform any activity. This indicates insider threat and possible data theft.	Rule-based	High
649004	Users with title PRN Performing Cerner Activities [Cerner DB]	This rule-based policy detects violation when employee with title 'PRN' is trying to access medical records.	Rule-based	High
649005	Snooping After Patient Discharge Date [Cerner DB]	This policy is rule based policy detects violation when Cerner employee accesses patient records after patient's discharge date. Indicates possible exfiltration of critical patient data.	Quick Alert	High
649006	Only Peer in Peer Group Performing Critical Activity [Cerner DB]	This behavior-based policy detects a user within a peer group who performs critical activity that has not been performed by other members of the same peer group.	Behavior-based	High

Policies				
649007	Employees accessing One's Own Records [Cerner DB]	Access to a record where both the Employee and Patient SSN are same.	Quick Alert	High
649008	Spike in Cerner Critical Events [Cerner DB]	This behavior-based policy detects violation when user performs critical cerner activity than his/her normal behavior of performing that activity.	Behavior-based	High
649009	User Created & Deleted in 24 Hours [Cerner DB]	This policy detects a user who has created and deleted the same user account within the past 24 hours, indicating Event Name=User Added||User Deleted. This indicates possible misuse of administrative privileges.	Quick Alert	High
649011	Co-Worker Snooping Activity [Cerner DB]	This policy detects if an employee is looking at patient records of a co-worker.	Rule-based	High

Cerner [HttpListener]

Policies				
Signature ID	**Policy Name**	**Policy Description**	**Policy Type**	**Criticality**
647001	Snooping After Patient Discharge Date [Cerner Listener]	This rule-based policy detects violation when Cerner employee accesses patient records after patient's discharge date. Indicates possible exfiltration of critical patient data.	Quick Alert	Medium
647002	Activity by Terminated User [Cerner Listener]	This policy detects terminated users who perform any activity. This indicates insider threat and possible data theft.	Rule-based	High

Policies				
647003	Spike in Cerner Critical Events [Cerner Listener]	This is behavior-based policy detects violation when user performs critical Cerner activity than his/her normal behavior of performing that activity.	Behavior-based	High
647004	Multiple Login Attempts/Multiple Accounts From Same Host [Cerner Listener]	This quick alert policy detects multiple login attempts from multiple accounts from same host. This indicates account misuse.	Quick Alert	Medium
647005	Login Attempt by Same Account From Multiple Hosts [Cerner Listener]	This directive-based, quick alert policy detects violation when login attempts by same account has been made from multiple hosts in specified time. Indicates possible compromised account.	Quick Alert	Medium
647006	Only Peer in Peer Group Performing Critical Activity [Cerner Listener]	This behavior-based policy detects a user within a peer group who performs critical activity that has not been performed by other members of the same peer group.	Behavior-based	High
647007	Users with Title PRN Performing Activities [Cerner Listener]	This rule-based policy detects violation when employee with title 'PRN' is trying to access medical records.	Rule-based	Low
647008	User Created & Deleted in 24 Hours [Cerner Listener]	This policy detects user who has created and deleted the same user account within the past 24 hours, indicating Event Name=User Added| |User Deleted. This indicates possible misuse of administrative privileges.	Quick Alert	High

Policies				
647009	Employees accessing One's Own Records [Cerner HttpListener]	Access to a record where both the Employee and Patient SSN are same.	Rule-based	Medium
647010	Employee Accessing Records of Deceased Patient [Cerner Listener]	This policy detects users who perform activity on deceased patient's records. This indicates possible account misuse and data theft.	Rule-based	Medium
649011	Account Performing Rare Cerner Activity [Cerner Listener]	This behavior-based policy detects abnormal activity when a rare Cerner activity is performed by user.	Behavior-based	High
649013	Co-Worker Snooping Activity [Cerner Listener]	This policy detects if an employee is looking at patient records of a co-worker.	Rule-based	High

Cerner Snooping [Database]

Policies				
Signature ID	**Policy Name**	**Policy Description**	**Policy Type**	**Criticality**
650001	Family Snooping Activity [Cerner Snooping DB]	This policy detects an employee looking at records of patient staying in same apartment with him/her and having same last name.	Rule-based	High
650002	Neighbor Snooping Activity [Cerner Snooping DB]	This policy detects if an employee is looking up patient records while employee and patient stay within distance of 1 mile.	Rule-based	High

Cerner Snooping [HttpListener]

Policies				
Signature ID	**Policy Name**	**Policy Description**	**Policy Type**	**Criticality**
650001	Family Snooping Activity [Cerner Snooping Listener]	This policy detects an employee looking at records of patient staying in same apartment with him/her and having same last name.	Rule-based	High
650002	Neighbor Snooping Activity [Cerner Snooping Listener]	This policy detects if an employee is looking up patient records while employee and patient stay within distance of 1 mile.	Rule-based	High

Epic Insight Pack

Description

Epic is a software company making software for mid-size hospitals and healthcare organizations. Epic offers a suite of healthcare software that supports functions related to patient care, clinical systems for doctors, nurses, emergency personnel and other care provides.

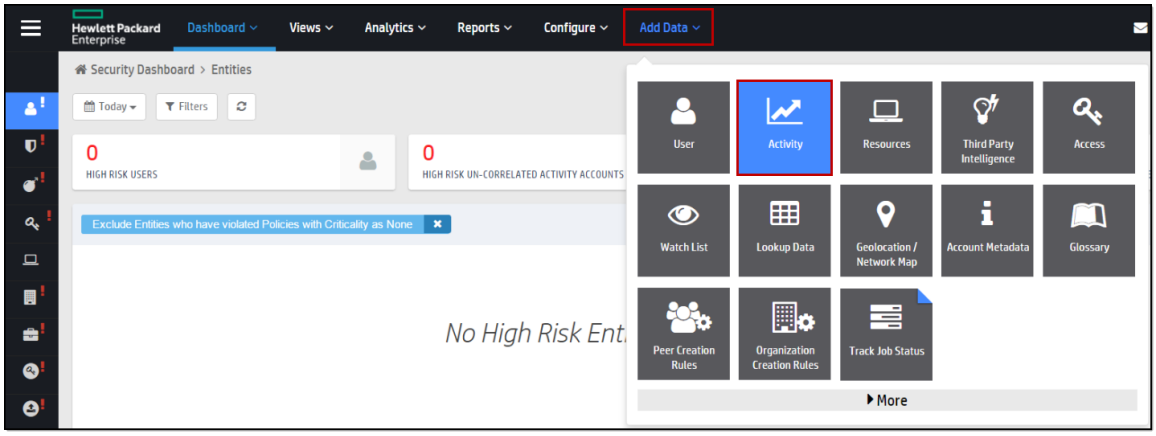
For more information, go to the following URL: http://www.epic.com/

The HPE ArcSight UBA Epic Insight Pack imports detailed logs from Epic for the identification of high risk user behavior using out-of-the-box behaviors and threat models specific to Epic and healthcare environments such as data snooping, VIP snooping and break-the-glass privileged user sessions.

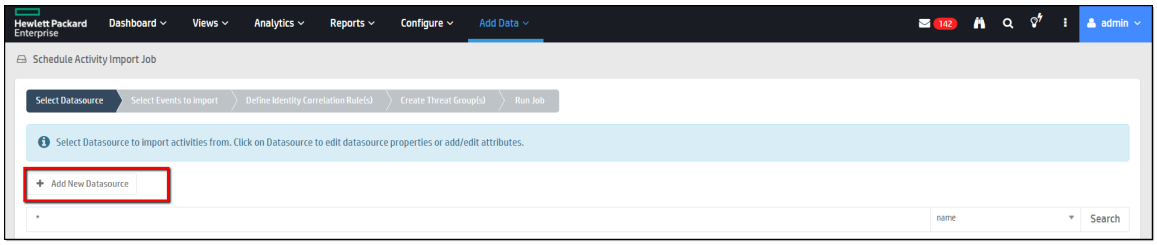
Connector

HPE ArcSight UBA imports activity data from Epic using a clarity file (a pipe-delimited file generated by executing a query on Epic's native database). When the clarity file is available, it can be imported into HPE ArcSight UBA as a file import.

1. Navigate to **Add Data > Activity**.



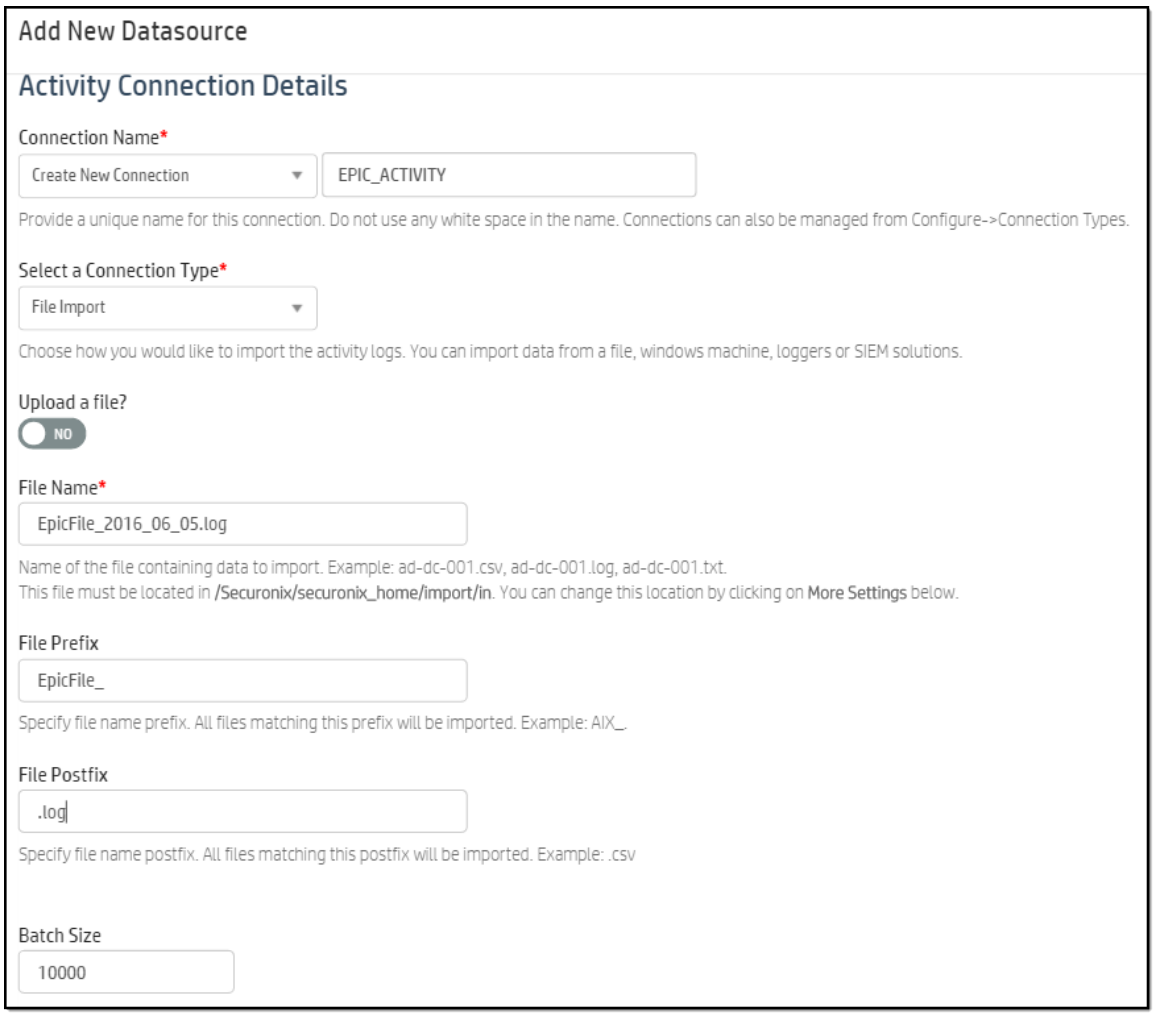
2. Click **Add New Datasource**.



3. In the General Details section, provide the following information:

   a. Specify a **Datasource Name**.
   b. (Optional) Specify the **IP Address** or hostname for the datasource.
   c. From the **Select Device Type** drop-down list, choose **EPIC** or create a new device type if EPIC does not exist.
   d. From the **Specify timezone for activity logs** drop-down list, select a timezone.

4. In the Activity Connection Details section, provide the following information:



   a. Provide a unique **Connection Name**, or use the default.
   b. From the **Select a Connection Type** drop-down list, choose **File Import**.
   c. Enter a **File Name**, **File Prefix**, and **File Postfix**.
   d. Provide the **Batch Size** and **Error count to terminate job**.

5. Click **Save and Close**.
6. You can now select the new data source and click **Preview** to see the data.
7. Click **Save and Next**, and then , to finish setting up the Epic activity import, proceed with steps 2 through 5 of the Add Activity Data section in the *HPE ArcSight UBA Administration Guide*.

Content

Epic [Database]

Policies				
Signature ID	**Policy Name**	**Policy Description**	**Policy Type**	**Criticality**
657001	Activity by Terminated User []	This policy detects terminated users who perform any activity. This indicates possible account misuse and data theft.	Rule-based	High
657002	Activity after Discharge date []	This policy detects users who perform any activity on a patient after his/her discharge. This indicates possible account misuse and data theft.	Quick Alert	Low
657003	Activity on Specific Patient(s) []	This policy detects users who perform any activity on specific patients. This indicates possible account misuse and data theft.	Quick Alert	Low
657004	Break the Glass Activity []	This policy detects users who perform any 'Break the Glass' activity. This indicates possible account misuse and data theft.	Quick Alert	Low
657005	Activity on Deceased Patient's Record []	This policy detects users who perform activity on deceased patient's records. This indicates possible account misuse and data theft.	Quick Alert	Low
657006	Activity on Family Member's Record []	This policy detects users who perform activity on patient's records who are their family. This indicates possible account misuse and data theft.	Rule-based	Low

Policies				
657007	Activity by a User from Multiple IPs []	This policy detects a user who logs into Epic multiple times from multiple IP addresses within a 1-hour period. This indicates possible account misuse.	Quick Alert	High
657008	Self Examination Activity []	This policy detects users who perform any activity on their own records. This indicates possible account misuse and data theft.	Rule-based	Low
657009	VIP Activity []	This policy detects users who perform any activity on a patient classified as a VIP. This indicates possible account misuse and data theft.	Quick Alert	Low
657010	Type 7 Activity Performed []	This policy detects users who perform 'Type 7' type of activity on their own records. This indicates possible account misuse and data theft.	Quick Alert	High
657011	Excessive # of Break The Glass []	This policy detects users who perform excessive number of 'Break the Glass' activity. This indicates possible account misuse and data theft.	Behavior-based	High
657012	Activity by an Employee on Co-Worker []	This policy detects if an employee is performing any activity on the patient records of a co-worker. This indicates possible account misuse.	Rule-based	High
657013	Activity by an Employee on Relative []	This policy detects an activity performed by an employee on patient records of his/her family member. This indicates account misuse.	Rule-based	High

Epic Snooping [Database]

Policies				
Signature ID	**Policy Name**	**Policy Description**	**Policy Type**	**Criticality**
658001	Activity by Employee on Neighbor []	This policy detects if an employee is looking up patient records while employee and patient stay within distance of 1 mile.	Rule-based	High
658002	Employee Performing Activity on Family Members []	This policy detects an employee looking at records of patient staying in same apartment with him/her and having same last name.	Rule-based	High

Google Apps Insight Pack

Description

Google Apps is a set of web application by Google such as Google Email, Google Calendar, and Google Drive. All these web applications offer an online alternative to traditional office suite software.

For more information, go to the following URL: https://developers.google.com/google-apps/

The HPE ArcSight UBA Google Apps Insight Pack imports Google Admins, Drive, Google Token and Login related events (such as files created or edited, logon activity, account creation/deletion), and detects account misuse related to access of confidential files or conducting privileged activity.

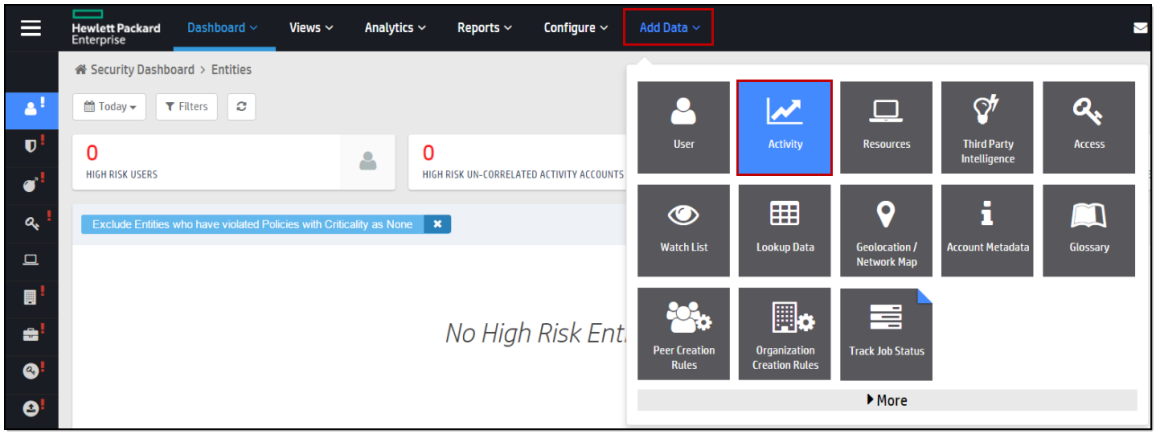
Connector

To connect to Google apps, you need the following information:

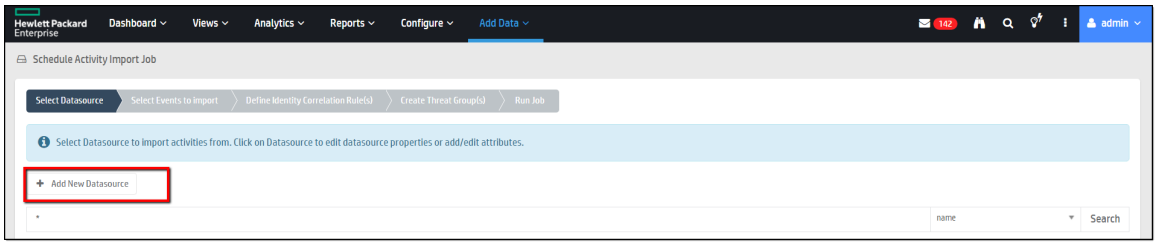
- Project
- Service Account Email
- Admin User Email
- Private Key File (.p12 file)

To connect to an application under Google Apps, you must create individual connections and activity imports for each application. The main steps are similar for importing activity data from the various Google Apps, we will use “Google Drive” as an example:

1. Navigate to **Add Data > Activity**.



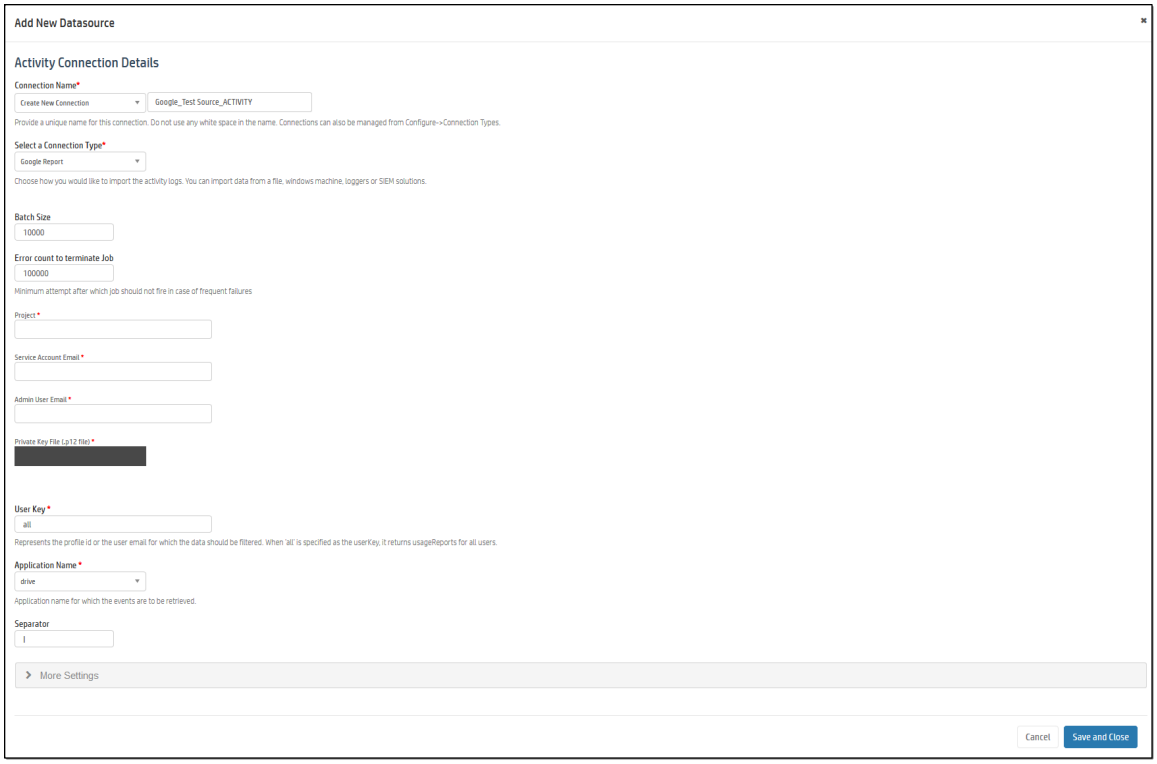
2. On the Schedule Activity Import Job tab, click **Add New Datasource**.



3. In the General Details section, provide the following information:

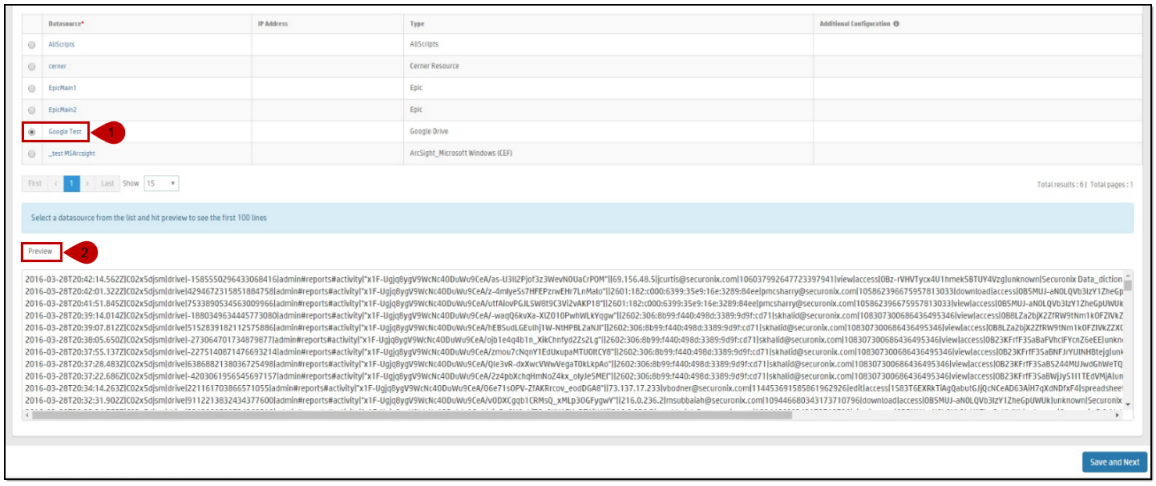
   a. Specify a **Datasource Name**.
   b. (Optional) Enter the IP Address or hostname for the data source.
   c. From the **Select Device Type** drop-down list, choose **Google Drive**.
   d. From the **Specify timezone for activity logs** drop-down list, select a timezone.

4. In the Activity Connection Details section, provide the following information:



a. From the **Select a Connection Type** drop-down, choose **Google Report**.
b. Enter the **Project**.
c. Provide a **Service Account Email** and an **Admin User Email**.
d. Upload the **Private Key File**.
e. From the **Application Name** drop-down list, select **drive**.

5. Select the data source and click **Preview** to see the data.



6. Save the new data source, select it from the list, and then, to finish setting up the Google activity import, proceed with steps 2 through 5 of the Add Activity Data section in the *HPE ArcSight UBA Administration Guide*

Content

Google Admin [API]

Policies				
Signature ID	**Policy Name**	**Policy Description**	**Policy Type**	**Criticality**
1000065	Activity by Terminated account - Google Apps Admin	Inactive users performing activities.	Rule-based	High

Google Drive [API]

Policies				
Signature ID	**Policy Name**	**Policy Description**	**Policy Type**	**Criticality**
785001	Drive Permissions to External Domain [G Drive]	This policy detects any activity performed by a non-company domain; for example, permissions for files sent from the drive, files accessed from the drive, etc. This indicates intellectual theft by a non-domain user.	Quick Alert	High
785002	Activity by Terminated User [G Drive]	This policy detects terminated users who perform activities on Google Drive. This indicates possible account misuse and data theft.	Rule-based	High
785003	Suspicious Activity From Malicious IP by Threat Intelligence [G Drive]	This policy detects suspicious activities from malicious IP addresses. This indicates the presence of malware.	Quick Alert	Medium
785004	Activity by Non-Corporate User [G Drive]	This policy detects any activity performed by a non-company user on Google Drive; for example, viewing documents, editing, etc. This indicates intellectual theft by a non-company user.	Quick Alert	High
785006	Drive Permission Set to Self [G Drive]	This policy detects a user who grants permissions to his or her own account allowing access to view, edit, download, etc., documents from their own Securonix domain to a non-Securonix domain email. This indicates possible data theft.	Rule-based	Medium

Policies				
785008	Activities by a User from Multiple IPs [G Drive]	This policy detects a user who performs activities on Google Drive from multiple IP addresses within a 1-hour period. This indicates possible account misuse.	Quick Alert	High
785009	Activities by a User from Multiple Locations [G Drive]	This policy detects a user who performs activities on Google Drive from multiple IP addresses within a 1-hour period. This indicates possible account misuse.	Quick Alert	High
785011	Publicly Shared Documents [G Drive]	This policy detects a user who shares a document on Google Drive with anyone on the Internet or anyone with a link from the Internet. This indicates possible data theft.	Quick Alert	High
785012	Permission to Competitors [G Drive]	This policy detects an activity where one user grants permissions to other users who have a competitor's domain address. This indicates possible intrusion, data theft, or intellectual property theft.	Rule-based	High
785013	Downloads from Same Account but Different IP Addresses [G Drive]	This policy detects files downloaded by the same account, using different IP addresses, within a 1-hour period. This indicates activities from multiple locations, and may indicate account misuse.	Quick Alert	Medium
785014	Activities on Sensitive Files [G Drive]	This policy detects any type of activity, such as viewing, downloading, etc., performed on sensitive files such as source code or licenses. This indicates theft of sensitive files.	Rule-based	Medium

Policies				
785014	Activities on Sensitive File Extensions [G Drive]	This policy detects any type of activity, such as viewing, downloading, etc., performed on sensitive files such as source code or licenses. This indicates theft of sensitive files.	Quick Alert	Medium
785016	Files Deleted from Manager's Account [G Drive]	This policy detects a user who deletes documents owned by their managers. This indicates possible data loss.	Rule-based	Low
785017	Excessive # of Documents Uploaded followed by Permission Change [G Drive]	This policy detects any user uploading excessive # of documents, followed by permission changes o the same documents by the same user and the same document being downloaded by another user. This indicates possible data theft.	Quick Alert	High
785018	Transactions not Performed by Peers [G Drive]	This policy detects protocols not frequently or normally used by members of a peer group. This indicates unusual activity by a user.	Behavior-based	Low
785019	Excessive # of Transactions Performed [G Drive]	This policy detects a high amount critical transactions like download, upload, print, change of permission, etc. performed on Google Drive by all users on the system. This indicates possible data theft.	Behavior-based	High

Google Login [API]

Policies				
Signature ID	**Policy Name**	**Policy Description**	**Policy Type**	**Criticality**
1000038	Successful Login by Terminated User	Terminated users having successful logon event.	Rule-based	High
1000039	Multiple failed logins followed by a successful login	Multiple failed logins followed by a successful login.	Rule-based	Medium
1000040	Multiple logon from different IP address within a given span of time	Multiple logon from different IP address within a given span of time.	Rule-based	Low

Google Tokens [API]

Policies				
Signature ID	**Policy Name**	**Policy Description**	**Policy Type**	**Criticality**
1000041	Activity by Terminated account - Google Apps token	Activity by Terminated account - Google Apps token	Rule-based	High

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Documentation (HPE Security ArcSight User Behavior Analytics 5.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arc-doc@hpe.com.

We appreciate your feedback!