HP User Behavior Analytics

HP UBA Version 1.1

Powered by SECURONIX

Application Insight Packs Guide

August 31, 2015

Table of Contents

Introduction

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

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

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, top n charts, behavior profiles).

Chapter 1: 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, and this information can be used for security analysis, resource change tracking and compliance auditing.

For more information: http://aws.amazon.com/cloudtrail/

The HP 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.

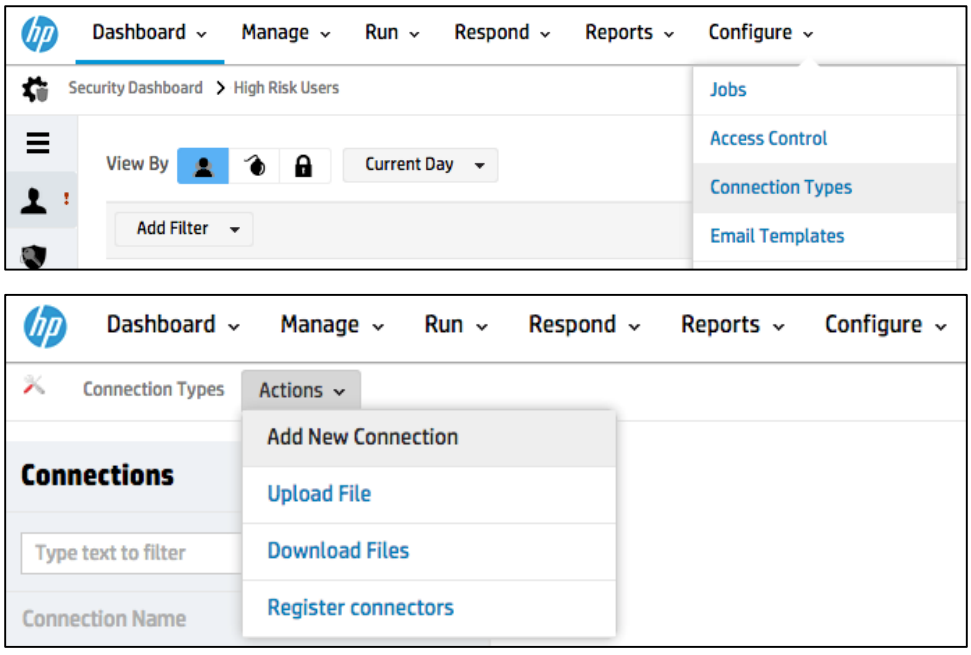
Connector

HP 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

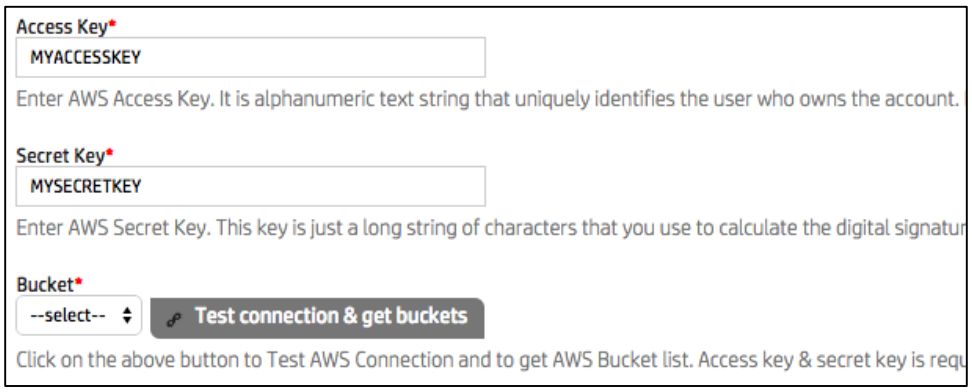
To create a connection in HP UBA, follow these steps:

1 Navigate to **Configure>Connection Types**, then to **Actions>Add New Connection**.

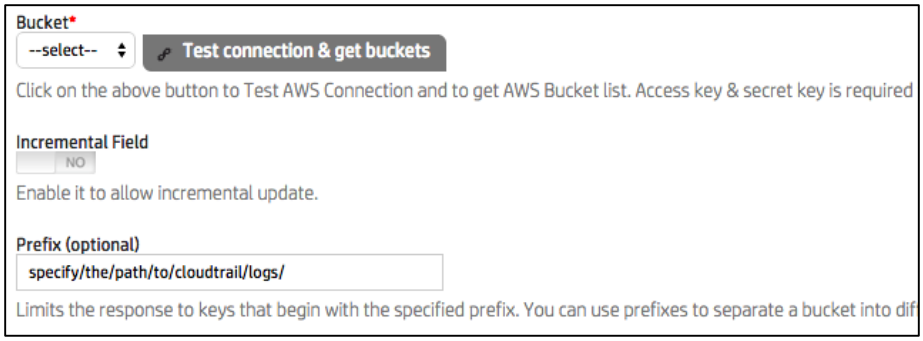


2 Provide a name for the connection, select **Resources** on the **Connection Type for** drop down menu, and select **AWS** from the **Connection Type** drop down:

3 Keep the default values for the various folder configurations, provide the Access Key and Secret Key, and then navigate to **Test connection & get buckets**.



4 If your connection is successful, you should see a list of buckets in the **Bucket** drop down. 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 Click **Save** to save the new connection.

6 Now that the connection is ready, you can set up the activity import by navigating to **Configure>Jobs**, then **Actions>Import>Activities**, and follow steps 1 through 5 to create a new activity import.

Content

Policies		
Name	**Criticality**	**Description**
Activity by Terminated account - AWS	High	Inactive user performing activities
Non AWS Approved user using AWS Services	Low	Non-approved users using AWS services

Top N Charts	
Chart Name	**Description**
Top Users by Event Count	Top N users with highest number of events
Top Accounts by Event Count	Top N accounts with highest number of events
Top Event Name	Top N event names with highest number of events

Behavior Profiles		
Name	**Type**	**Attribute List**
BP_Login	Peak	Event Name

Activity Outliers		
Name	**Type**	**Criticality**
Abnormal activities compared to peer group	Peer Activity Outlier	Medium

Chapter 2: 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: https://www.box.com/

The HP 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

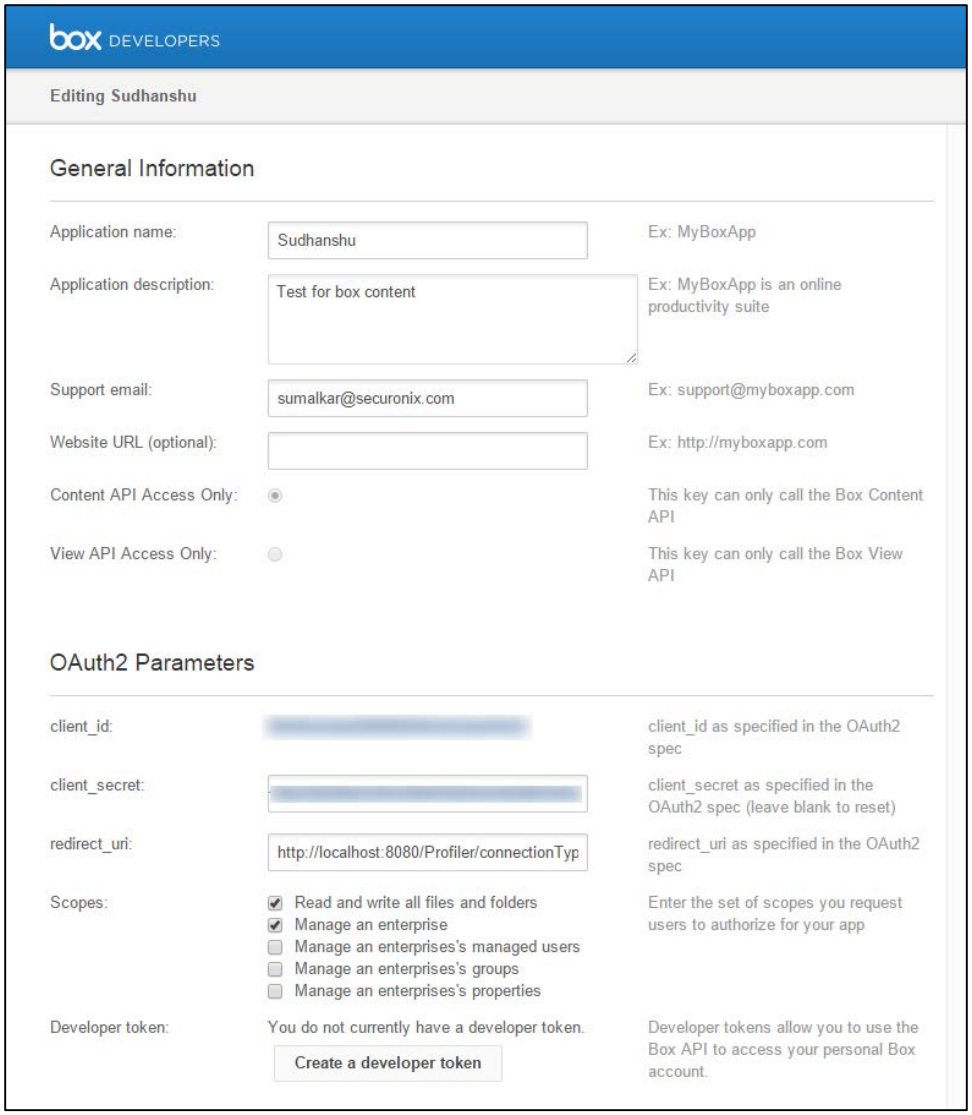
HP UBA provides connection to Box to pull in activity data. In order to get the activity data from Box, you will need an admin account on Box.com for the application from which you intend to import data into HP UBA.

1 Edit the application on Box.com and give it:

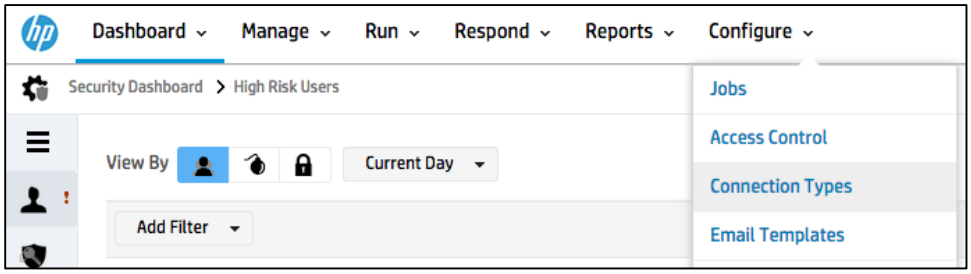
- Client_ID
- Client_Secret
- Redirect_URL

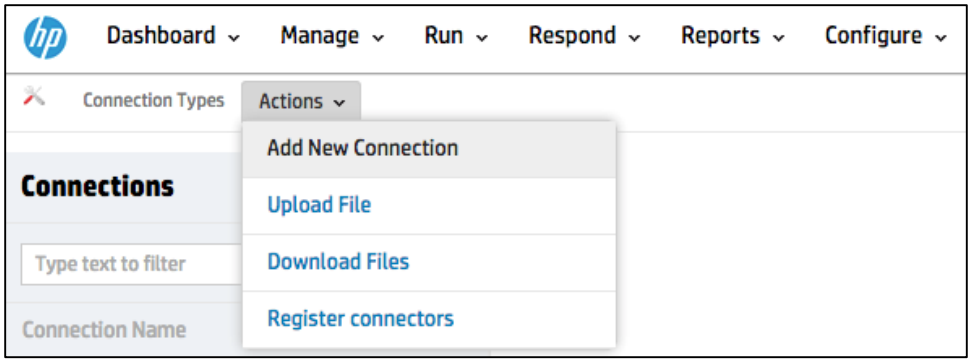
Example of **Redirect URL**: http://localhost:8080/Profiler/connectionType/generateOauthCode

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.

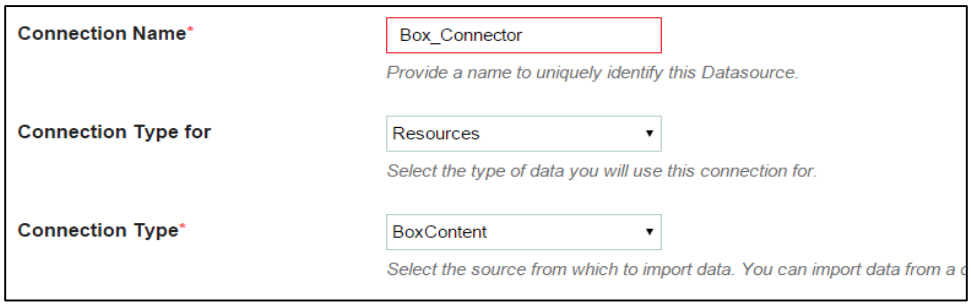


2 To make a connection in Securonix, navigate to **Configure>Connection Types,** then to **Actions>Add New Connection.**

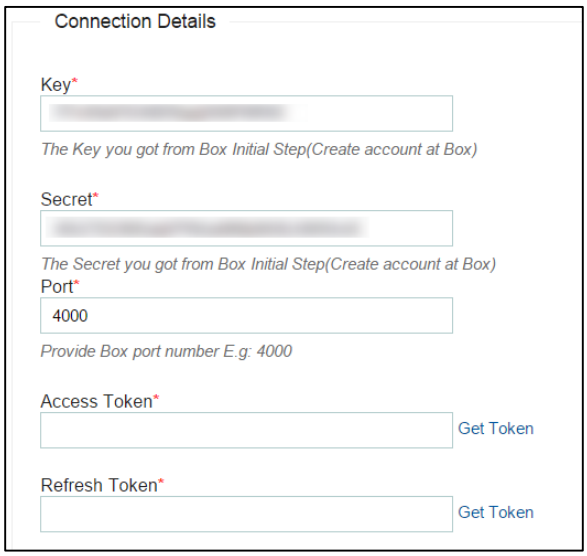




3 Provide an appropriate name to the connection, select **Resource** from the **Connection Type for** drop down and select **BoxContent** from the Connection Type drop down.



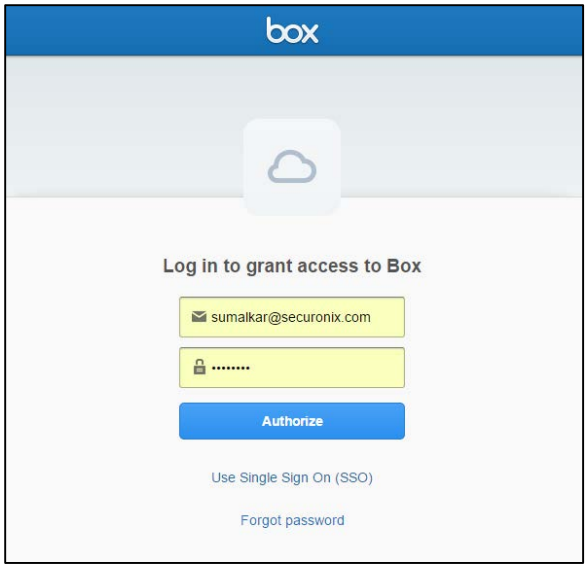
4 Provide the connection details as below:



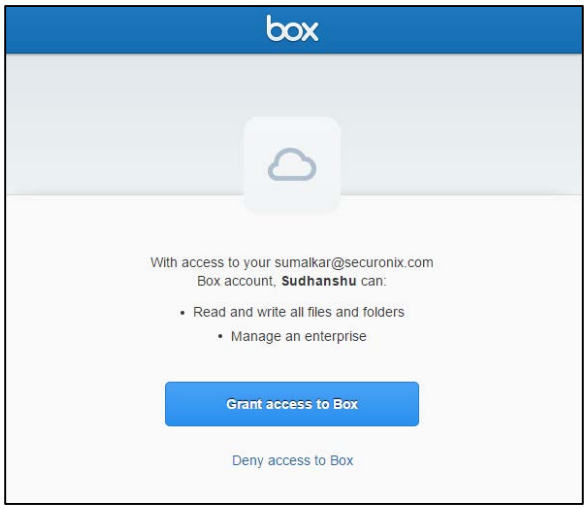
5 Provide the Client_ID and Client_Secret from the Box connection in the **Key** and **Secret** fields respectively.

6 Provide **Port** number. Default is 4000.

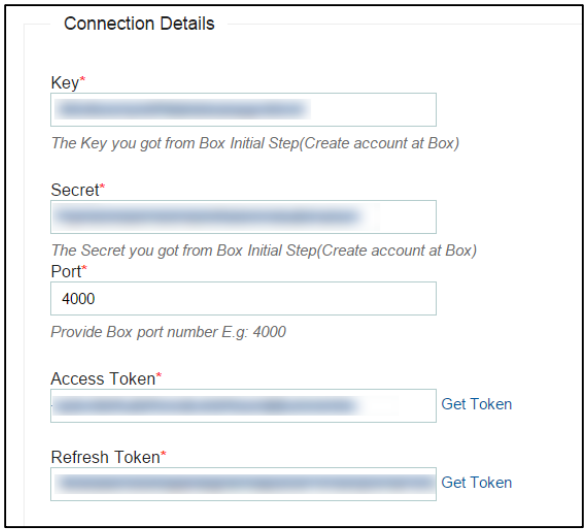
7 Click the **Get Token** link for receiving the **Access Token**. This will open up a new window in your browser.



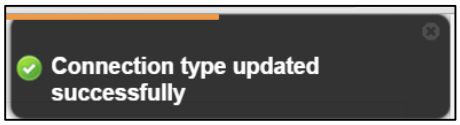
8 Login to the Box website with the admin account and navigate to **Grant Access to Box.**



9 When you click **Grant access to Box** with the help of initial **Redirect_URL** given in the Box application, the **Access Token** and **Refresh Token** information will be directly passed to the connection that we are trying to establish in Securonix.



10 Click **Save**. You will see following message.



Content

Policies		
Name	**Criticality**	**Description**
Activity by Terminated account	High	Inactive users performing activities

Top N Charts	
Chart Name	**Description**
Top IP Addresses	Top N users with highest number of events
Top Event Type	Top N event types with highest number of events
Top End Resource	Top N end resource with highest number of events
Top SourceUserName	Top N source username with highest number of events

Behavior Profiles		
Name	**Type**	**Attribute List**
BP_Download	Peak	Event Type

Activity Outliers		
Name	**Type**	**Criticality**
Suspicious activity - Abnormal admin activities compared to peer group	Peer Activity Outlier	Medium
Suspicious Activity – High number of files downloaded	Suspect Activity Outlier	High

Chapter 3: 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 healthcare 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: http://www.cerner.com

The HP 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

Understand Cerner Event Logs

How do Cerner Audit Logs work?

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

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

Define Which Events to Audit

The Cerner Millennium tool **ppraudteventmanager.exe** is used to select the audit events that are sent to HP 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.

These are the 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. Once 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 needs to be modified, simply make the changes by navigating to the **Configure>Connection Types**. Select the **CernerListerner** 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 HP UBA appliance is configured and ready to accept Cerner auditing traffic, a network/firewall issue is the likely cause.

Configure Destination for Audit Events

1. Log into 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 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. Once 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 HP UBA appliance.

Configure Cerner Listener on HP UBA

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

Audit Exception

Cerner AUDIT.EXCEPTION Queue

Reprocessing Queues: In the event that messages are not sent to the HP UBA appliance, they will start to queue on the Cerner side into the AUDIT.EXCEPTION queue. When that happens, it is possible to resend those messages to the HP UBA appliance. 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>
```

Content

Policies		
Name	**Criticality**	**Description**
Accessing PHR of discharged patient	Medium	Policy checks if the event has Discharge Date of the patient in past. So checking if discharge date starts with either 1 or 2 as in for example 1999-02-01 or 2010-12-01
Activity by Terminated account	High	Inactive users performing activities
VIP PHR accessed	Medium	Checking if the VIP flag is set to Y

Top N Charts	
Chart Name	**Description**
Top Transactions by Event Count	Top N transactions by highest number of events
Top message	Top N event messages by highest number of events
Top IP Addresses	Top N IP addresses by highest number of events
Top Users by Event Count	Top N Users by highest number of events

Behavior Profiles		
Name	**Type**	**Attribute List**
_Peak_Behavior	peak	event_name
BP_Run_Reports	peak	event_name
BP_VIP	peak	event_name

Activity Outliers		
Name	**Type**	**Criticality**
Suspicious Activity – High volume of VIP PHR accessed	Suspect Activity Outlier	High
Suspicious – High Volume PHR accessed	Suspect Activity Outlier	High
Suspicious Activity – Activity performing activity never conducted before	Suspect Check Real Time	High

Chapter 4: CyberArk Insight Pack

Description

CyberArk is an information security company focused on privileged account security. CyberArk is delivering a new category of targeted security solutions that help leaders stop reacting to cyber threats and get ahead of them, preventing attack escalation before irreparable business harm is done.

For more information: http://www.cyberark.com/

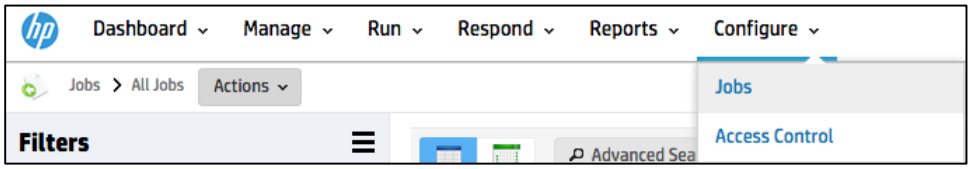
The HP UBA CyberArk Insight Pack connects to CyberArk to download detailed Password Vault data and session data and conducts behavior-based analytics on individual user commands for use in identifying the misuse or compromise of privileged credentials and the replacement of manual auditing requirements.

Connector

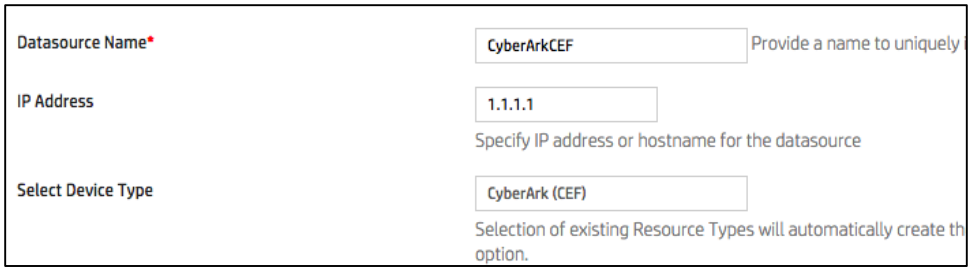
HP UBA provides different ways to pull data from CyberArk:

We will take “CyberArk (CEF)” as an example to show how to import activity data in HP UBA:

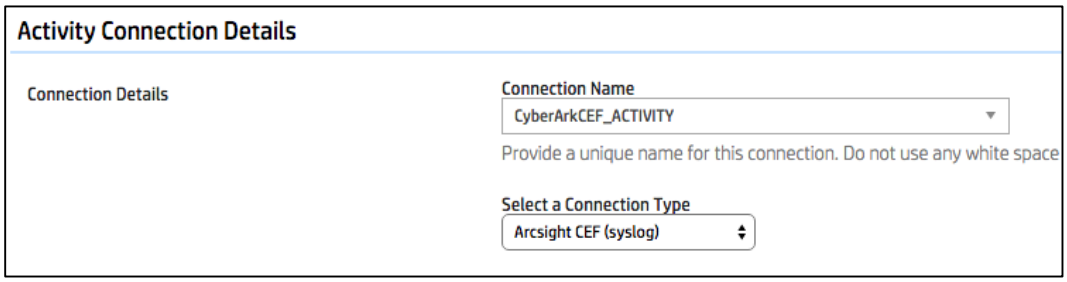
1 Navigate to **Configure>Jobs**, then **Actions>Import>Activities**.

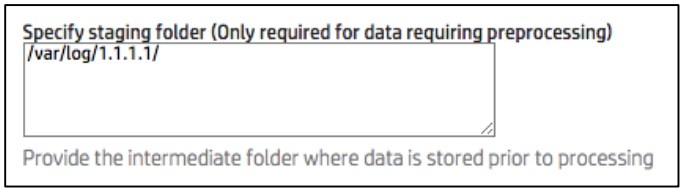


2 Click **Add New Datasource**, provide a name for the datasource, its IP address and select **CyberArk (CEF)** from the **Select Device Type** drop down menu:



3 In the **Activity Connection Details** section, select **Arcsight CEF (syslog)** as the **Connection Type**, then provide the file name as well as the location of the staging folder for the file (e.g.; /var/log/1.1.1.1/ if you are using syslog and the datasource IP address is 1.1.1.1):





4 Save the new data source, select it from the list, and then proceed with Steps 2 through 5 to finish setting up the CyberArk CEF activity import.

Content

Policies		
Name	**Criticality**	**Description**
Activity by Terminated account – CyberArk	High	Inactive users performing activities
Attempted use of password change Command – CyberArk	High	Detect any password changes that are performed from a CyberArk Session based on the keystroke logs
Attempted use of the telnet utility – CyberArk	High	User attempted use of telnet utility.
Changed access permissions of system objects – CyberArk	Medium	User changed access permissions of system objects.
Circumventing monitoring tool via xterm	High	User circumvented monitoring tool via xterm.
Local Account Modification – CyberArk	High	Local Account Modification
Password snooping – CyberArk	Medium	Password snooping
Potential Monitoring Tools / Logs Tampering – CyberArk	Medium	Potential monitoring tools / logs tampering
Security Configuration Changes – CyberArk	Medium	Security configuration changes
Use of insecure file transfer method – CyberArk	Medium	Use of insecure file transfer method
User sending emails from server	High	User sending emails from server

Top N Charts	
Chart Name	**Description**
Top Users by Event Count	Top N users by highest number of events
Top Accounts by Event Count	Top N accounts by highest number of events
Top Transactions by Event Count	Top N transactions by highest number of events
Top IP Addresses	Top N IP addresses by highest number of events

Chapter 5: 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.

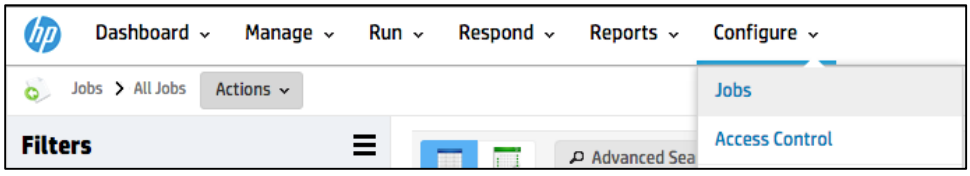
For more information: http://www.epic.com/

The HP 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.

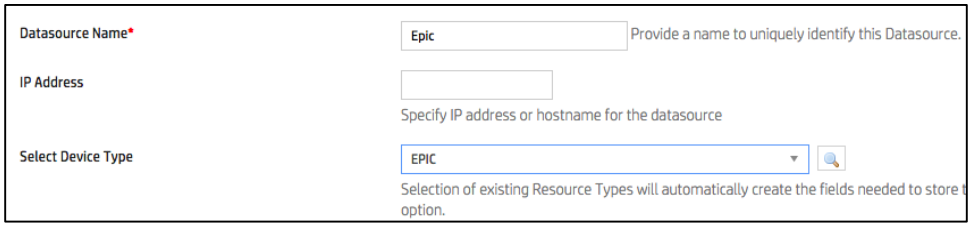
Connector

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

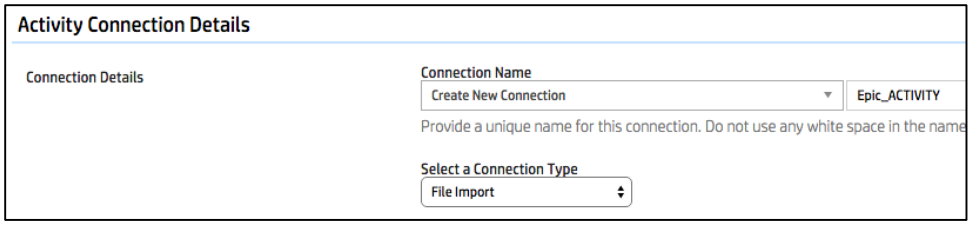
1 Navigate to **Configure>Jobs**, then to **Actions>Import>Activities**

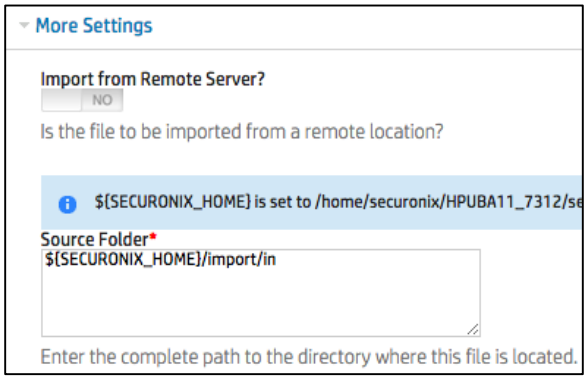


2 Click **Add New Datasource**, provide a name and IP address for the datasource and select **Epic** from the **Select Device Type** drop down menu.



3 In the **Activity Connection Details** section, select **File Import** as the **Connection Type**, then provide the name of the file (Clarity file) and its location (default: ${SECURONIX_HOME}/import/in).





4 Save the new data source, select it from the list and proceed with Steps 2 through 5 to finish setting up the Epic activity import.

Content

Policies		
Name	**Criticality**	**Description**
Activity by Terminated account - EPIC	High	Inactive users performing activities
EPIC Break the Glass	Low	Any activity with ACCESS_LOG_METRIC.METRIC_NAME = Break The Glass
EPIC Break the Glass for accessing VIP PHR	Medium	Any activity with ACCESS_LOG_METRIC.METRIC_NAME = Break The Glass for VIP patient
EPIC co-worker PHR accessed	Medium	EPIC.PATIENT_EMPLOYER Starts With “HOSPITAL NAME”. Need to change the hospital name according to requirement in the policy.
EPIC Deceased PHR accessed	Low	Checking the Records of a Deceased patient
EPIC Family Member PHR accessed	Medium	Checking the records of family members
EPIC Self PHR accessed	Medium	Same Person examining himself
EPIC VIP PHR accessed	Medium	Policy to check if the VIP flag is set to Y in the event

Top N Charts	
Chart Name	**Description**
Top Users by Event Count	Top N users by highest number of events
Top IP Addresses	Top N IP addresses by highest number of events
Top Accounts by Event Count	Top N accounts by highest number of events
Top Transactions by Event Count	Top N transactions by highest number of events

Behavior Profiles		
Name	**Type**	**Attribute List**
BP_EPIC	peak	ZC_ACCESS_LOG_TYPE.NAME

Activity Outliers		
Name	**Type**	**Criticality**
Suspicious Activity – High number of PHR accessed	Suspect Activity Outlier	High
EPIC – Activity never conducted before by an account	Suspect Check Real Time	Medium

Chapter 6: 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: https://developers.google.com/google-apps/

The HP 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.

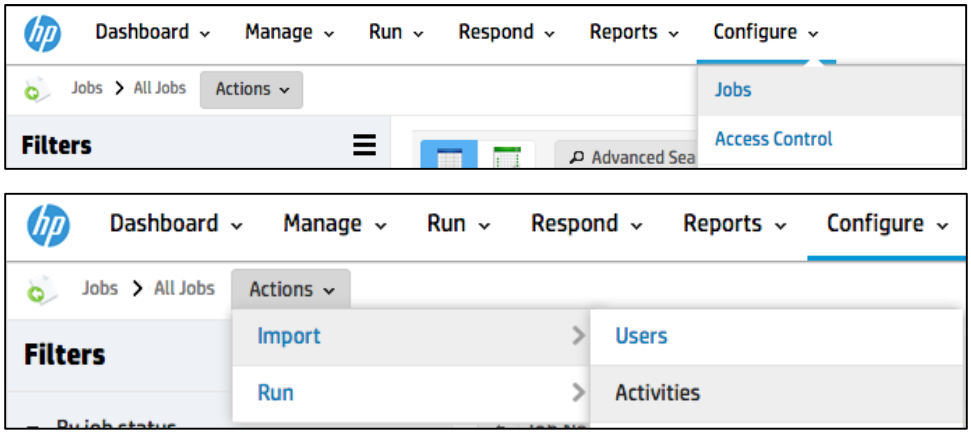
Connector

To connect to Google apps, you need following information:

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

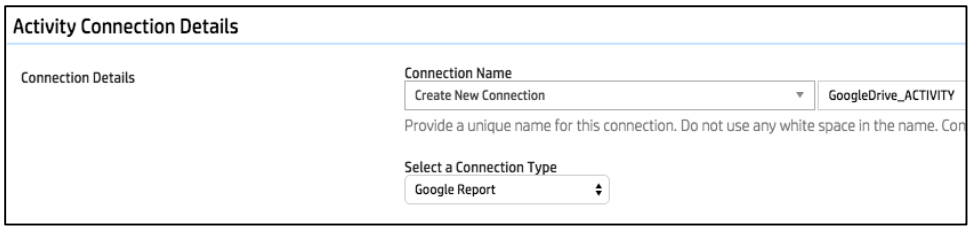
To connect to different application under Google Apps, you need to create individual connections and activity imports per application. The main steps are similar for importing activity data from the various Google Apps, we will take “Google Drive” as an example:

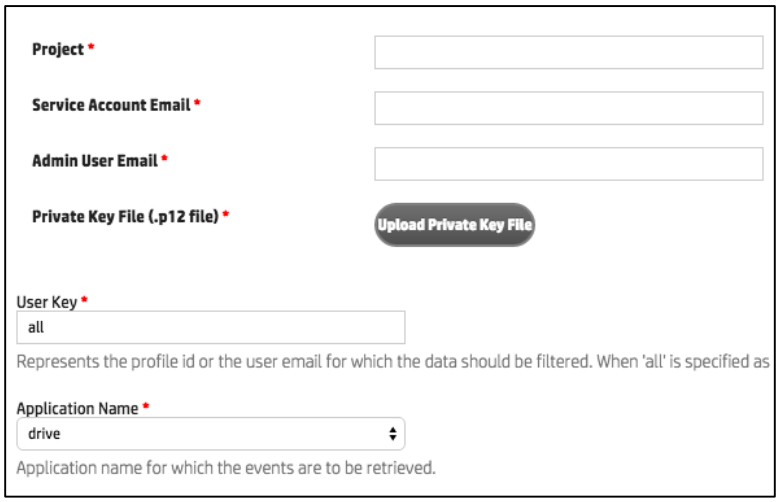
1 Navigate to **Configure>Jobs**, then to **Actions>Import>Activities.**



2 Click **Add New Datasource**, provide a name for the datasource and select **Google Drive** from the **Select Device Type** drop down menu.

3 In the **Activity Connection Details** section, select **GoogleReport** as the **Connection Type**, provide the Project, Service Account Email, Admin User Email, upload the Private Key File and select **drive** from the **Application Name** drop down menu.





4 Save the new data source, select it from the list, and then proceed with Steps 2 through 5 to finish setting up the Google Drive activity import.

Content

Policies			
Connection Type	**Name**	**Criticality**	**Description**
Google Drive	Activity by a non-MyCompany User on Google Drive	Medium	Activity on Google Drive by users not part of my company. Policy needs to be updated with the company's domain.
Google Drive	Activity by Terminated Account – Google Drive	High	Inactive users performing activities
Google Drive	Activity on sensitive files	Medium	Activity on files with .exe, .jar, .lic file extensions.
Google Drive	Activity to non-MyCompany Domain	Medium	Activity to a domain that is not part of my company. Policy needs to be updated with the company's domain.
Google Admin	Activity by Terminated account - – Google Apps Admin	High	Inactive users performing activities

Policies			
Connection Type	**Name**	**Criticality**	**Description**
Google Tokens	Activity by Terminated account - – Google Apps token	High	Inactive users performing activitiesMISSING
Google Login	Multiple failed logins followed by a successful login	Medium	Multiple failed logins followed by a successful loginMISSING
Google Login	Multiple logon from different IP address within a given span of time	Low	Multiple logon from different IP address within a given span of time
Google Login	Successful Login by Terminated UserTerminated users having successful logon event.	High	Terminated users having successful logon event.MISSING

Top N Charts	
Chart Name	**Description**
Google Drive – Top Level 1 Tran by Event count	Top N level 1 transaction by highest number of events
Google Drive – Top IP Addresses	Top N IP addresses by highest number of events
Google Drive – Top Accounts by Event Count	Top N accounts by highest number of events
Google Admin – Top Users by Event Count	Top N users by highest number of events
Google Admin – Top IP Addresses	Top N IP addresses by highest number of events
Google Admin – Top Transactions by Event Count	Top N transactions by highest number of events
Google Tokens – Top Users by Event Count	Top N users by highest number of events
Google Tokens – Top IP Addresses	Top N IP addresses by highest number of events
Google Tokens – Top Transactions by Event Count	Top N transactions by highest number of events
Google Login – Top IP Addresses	Top N IP addresses by highest number of events
Google Login – Top Users by Event Count	Top N users by highest number of events
Google Login – Top Accounts by Event Count	Top N accounts by highest number of events

Behavior Profiles		
Name	**Type**	**Attribute List**
Peak_GoogleDrive_Delete	peak	EventName
Peak_GoogleDrive_Download	peak	EventName
Peak_GoogleDrive_Print	peak	EventName
BP_Logon_Failures	peak	EventName

Activity Outliers			
Connection Type	**Name**	**Type**	**Criticality**
Google Drive	Google Drive Access from rare IP Address	Suspect Check Real Time	Low
Google Login	Suspicious high number of login failures	Suspect Activity Outlier	High

Chapter 7: Lieberman Insight Pack

Description

Lieberman is a privileged identity management (PIM) and security management company that provides software products that help customers isolate and contain data breaches that occur after attackers penetrate the network perimeter. Lieberman protects access to system with sensitive information from APTs (Advanced Persistent Threats) and malicious insiders with elevated privileges.

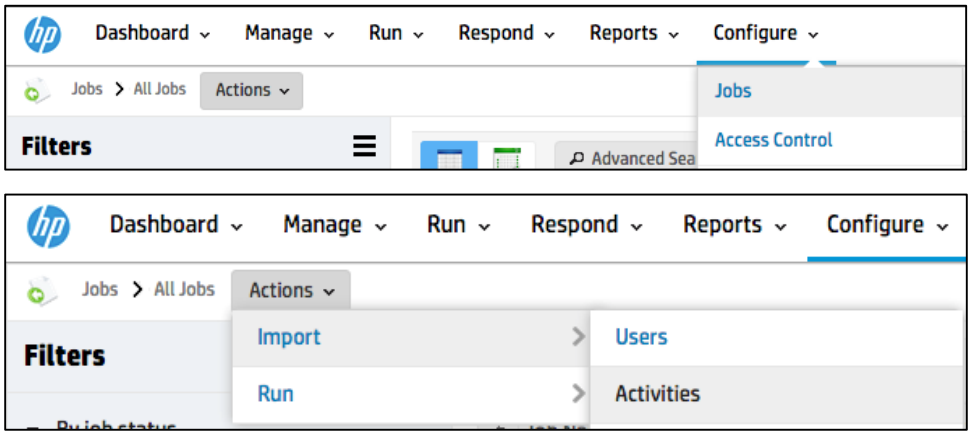
For more information: http://www.liebsoft.com

The HP UBA Lieberman Insight Pack imports log data from Lieberman and detects malicious activities such as users checking another user's password vault, user elevating their permissions, and abnormal activity behaviors.

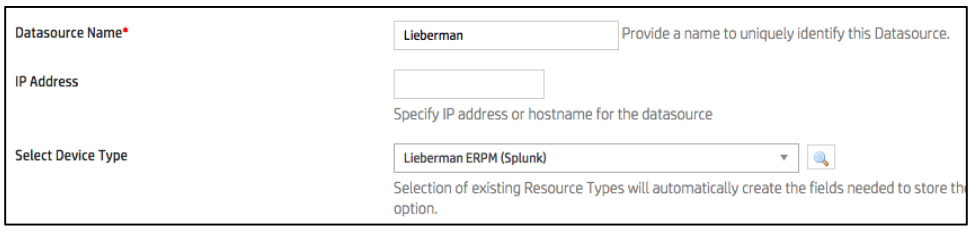
Connector

HP UBA imports activity data from Lieberman. To create a connection in HP UBA, follow these steps:

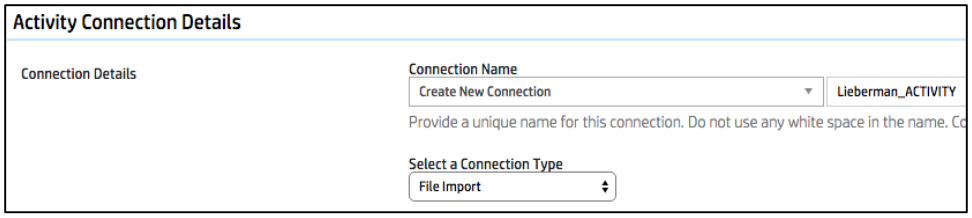
1 Navigate to **Configure>Jobs**, then to **Actions>Import>Activities.**

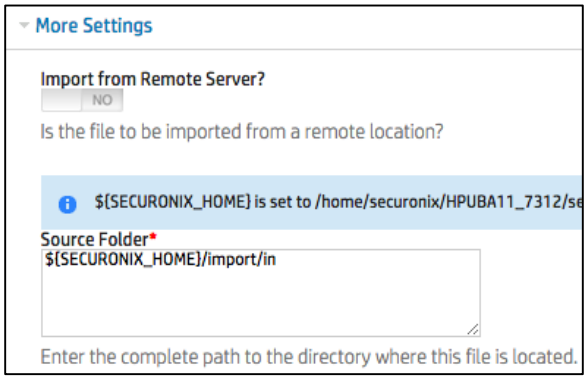


2 Click **Add New Datasource**, provide a name and IP address for the datasource and select **Lieberman ERPM (Splunk)** (if you are importing Lieberman data from Splunk) from the **Select Device Type** drop down menu.



3 In the **Activity Connection Details** section, select **File Import** as the **Connection Type**, provide the name of the file and its location (default: ${SECURONIX_HOME}/import/in):





4 Save the new data source, select it from the list, and then proceed with Steps 2 through 5 to finish setting up the Lieberman activity import.

Content

Policies			
Connection Type	**Name**	**Criticality**	**Description**
Query	Activity by Terminated account - Lieberman	High	Inactive users performing activities
Query	After Business hours password activity	High	Accounts performing PASSWORD_ACCESS_GRANTED PASSWORD_CHECKED_OUT PASSWORD_RETRIEVED activities after 7pm and before 6am
Query	User checking out another user's password vault	High	MISSING
Query	User elevating self permissionsself-permissions	High	User elevating self permissionsself-permissions, looking for transaction PASSWORD_ACCESS_GRANTED

Top N Charts	
Chart Name	**Description**
Top DHOST	Top destination hosts by highest number of events
Top Event	Top events by highest number of events

Behavior Profiles		
Name	**Type**	**Attribute List**
BP_PSWD_Checkout	peak	Event

Activity Outliers		
Name	**Type**	**Criticality**
Suspicious activity – Unusual number of activities within peer group	Peer Activity Outlier	Medium
Suspicious high number of password check outs	Suspect Activity Outlier	High
Event rarity on Lieberman ERPM	Suspect Check Real Time	Medium