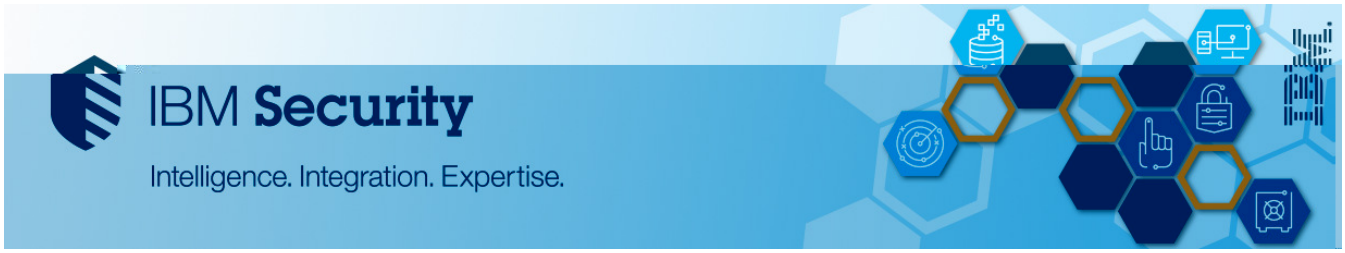


IBM® SECURITY PRIVILEGED IDENTITY MANAGER V2.0.2

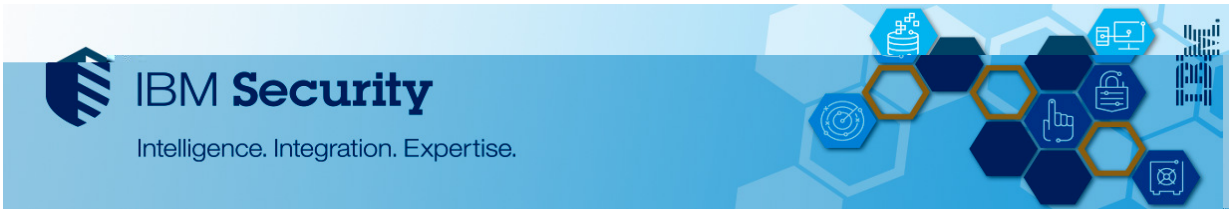
Integration with IBM QRadar Security Intelligence Platform

Configuration Cookbook

Low Chee Meng
Huang Qi (Victor)
LinLin Li
Haan-Ming Lim

Version 1.0

April 2016

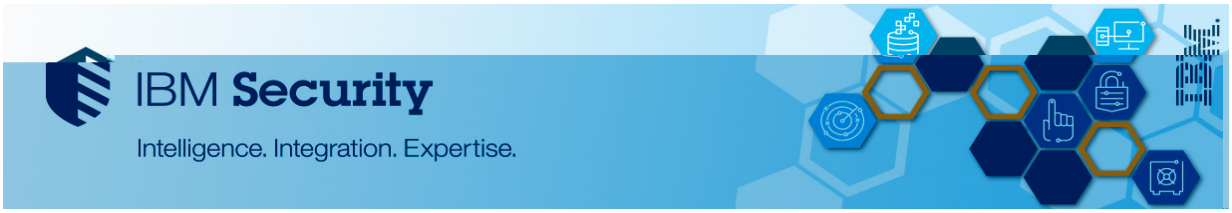


Contents

Document History

Version	Updates	Authors	Date
1.0	Created cookbook.	Chee Meng Low, Huang Qi (Victor), Linlin Li, Haan-Ming Lim	April 2016

For cookbook updates, contact one of the following authors:
Chee Meng (cheemeng.low@sg.ibm.com)
Victor (huangq@sg.ibm.com)
Linlin (linlin@sg.ibm.com)
Haan-Ming (haanming@sg.ibm.com)



1. Introduction

This cookbook describes the steps to integrate the IBM® Security Privileged Manager (ISPIM) with the IBM® QRadar Security Intelligence Platform (QRadar).

2. Requirements for IBM® QRadar Security Intelligence Platform

The IBM® Security Privileged Identity Manager (ISPIM) audit logs can be collected by the IBM® QRadar Security Intelligence Platform (QRadar) for monitoring, alerting, and co-relation with events from other QRadar event sources.

For IBM Security Privileged Identity Manager Version 2.0 and later, you need to install and configure these 3 QRadar Device Support Modules (DSM):

Requirement	Step	Additional
	Device Support Module for IBM® Security Privileged Identity Manager	This module collects (through Java Database Connectivity (JDBC) lookup) and parses audit logs from the Privileged Credential Manager (PCM) database of ISPIM. Events that are collected include Check-in-Check-out (CICO) events, Credential resetting password events and Credential Management events.
	Device Support Module for IBM® Security Access Manager for Enterprise Single Sign-On	This module collects (through Syslog output from ISPIM virtual appliance) and parses audit logs from the Enterprise Single Sign-On (ESSO) database of ISPIM. Events that are collected include Check-in-Check-out (CICO) events initiated from the ESSO agent. This module is not necessary if you do not deploy ESSO Agents in your ISPIM deployment.
	Device Support Module for IBM® Privileged Session Recorder	This module collects (through JDBC lookup) and parses audit logs from the Privileged Session Recorder (PSDR) database of ISPIM. Events that are collected include Command Logs of SSH sessions recorded by Enterprise Single Sign-On (ESSO)/PSR Agent. This module is not necessary if you do not enable Session Recording feature in your ISPIM deployment.

3. Install and configure QRadar Device Support Modules

Each QRadar Device Support Module (DSM) has its own specific installation and configuration instructions. You can refer to the following sections to install and configure the DSMs.

3.1. IBM® Security Privileged Identity Manager (Privileged Credential Manager) Device Support Module Configuration

The IBM® Security QRadar Device Support Module (QRadar DSM) for IBM® Security Privileged Identity Manager (ISPIM) collects events from ISPIM devices.

Things to note	Step	Additional
	This configuration includes a requirement to configure a database view V_PIM_AUDIT_EVENT into the Privileged Credential Manager (PCM) database.	The DSM consumes events from this view.

3.1.1. IBM® Security Privileged Identity Manager Device Support Module Specifications

The following table identifies the specifications for the IBM® Security Privileged Identity Manager Device Support Module (ISPIM DSM).

Specification	Value
Manufacturer	IBM
DSM name	IBM Security Privileged Identity Manager
RPM file name	DSM-IBMSecurityPrivilegedIdentityManager-Qradar_version-build_number.noarch.rpm
Supported versions	V2.0
Protocol	JDBC
Recorded event types	Audit Authentication System
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	IBM Security Privileged Identity Manager website (http://www-03.ibm.com/software/products/en/pim/)

3.1.2. Collect events from IBM® Security Privileged Identity Manager

To collect events from IBM® Security Privileged Identity Manager (ISPIM), complete the following steps:

Step	Additional
If automatic updates are not enabled, download and install the most recent version of the following Red Hat Package Managers (RPMs) on your QRadar Console:	• JDBC Protocol RPM • ISPIM Device Support Module RPM
Collect information from the ISPIM web user interface.	
Add an ISPIM log source on the QRadar Console.	See 3.1.2.1 IBM® Security Privileged Identity Manager log source parameters.

3.1.2.1. IBM® Security Privileged Identity Manager log source parameters

The following table describes the parameters that require specific values for IBM® Security Privileged Identity Manager (ISPIM) event collection:

Parameter	Value
Log Source Type	IBM® Security Privileged Identity Manager
Protocol Configuration	JDBC
Log Source Identifier	<DATABASE@HOSTNAME>
Database Type	DB2
Database Name	Must match the value in the **Database name** field in the IBM® Security Privileged Identity Manager.
IP or Hostname	Must match the value in the **Hostname** field in the IBM® Security Privileged Identity Manager.
Port	Must match the value in the **Port** field in the IBM® Security Privileged Identity Manager.
Username	Must match the value in the **Database administrator ID** field in the IBM® Security Privileged Identity Manager.
Predefined Query	None
Table Name	*DB2ADMIN*.V_PIM_AUDIT_EVENT Replace *DB2ADMIN* with the actual database schema name as identified in the Database Administrator ID parameter in the IBM® Security Privileged Identity Manager.
Select List	*
Compare Field	TIMESTAMP
Use Prepared Statements	Select this check box.
Start Date and Time	Initial date/time for the JDBC retrieval.
Polling Interval	10

EPS Throttle	20000

3.1.3. Configuring IBM® Security Privileged Identity Manager

To configure a log source in IBM® Security QRadar, you must record some information from IBM® Security Privileged Identity Manager (ISPIM).

Before you begin, make sure that for the ISPIM DB2 database, incoming TCP connections are enabled to communicate with QRadar.

Step	User Interface
Log in to ISPIM.	
Click the **Configure Privileged Identity Manager** tab.	
In the **Manage External Entities** pane, select **Database Server Configuration**.	
Double-click the **Identity data store** row in the **Database Server Configuration** column.	
Record the values for the following parameters:	▪ Hostname ▪ Port ▪ Database name ▪ Database Administrator ID

To create a view in ISPIM DB2 database in the same schema as identified in the Database Administrator ID parameter, run the following SQL statement:	`CREATE view V_PIM_AUDIT_EVENT`
	`AS`
	`SELECT`
	`ae.ID, ae.itim_event_category as event_category, ae.ENTITY_NAME, service.NAME service_name,`
	`ae.ENTITY_DN, ae.ENTITY_TYPE,`
	`ae.ACTION, ae.INITIATOR_NAME, ae.INITIATOR_DN, ae.CONTAINER_NAME, ae.CONTAINER_DN,`
	`ae.RESULT_SUMMARY, ae.TIMESTAMP,`
	`lease.POOL_NAME, lease.LEASE_DN, lease.LEASE_EXPIRATION_TIME, lease.JUSTIFICATION,`
	`ae.COMMENTS, ae.TIMESTAMP2, ae.WORKFLOW_PROCESS_ID`
	`FROM AUDIT_EVENT ae`
	`LEFT OUTER JOIN AUDIT_MGMT_LEASE lease ON (ae.id = lease.event_id)`
	`LEFT OUTER JOIN SA_EVALUATION_CREDENTIAL cred ON (LOWER(ae.entity_dn) = LOWER(cred.DN))`
	`LEFT OUTER JOIN V_SA_EVALUATION_SERVICE service ON (LOWER(cred.service_dn) = LOWER(service.dn));`

3.1.4. Adding a log source

If a log source is not automatically discovered, you can manually add a log source to receive events from your network devices or appliances.

Step	User Interface
Click the **Admin** tab.	
Click the **Log Sources** icon.	
Click **Add**.	
Configure the common parameters for your log source.	
Configure the protocol-specific parameters for your log source.	
Click **Save**.	
On the **Admin** tab, click **Deploy Changes**.	

3.1.4.1. Generic log source parameters

The following table describes the common log source parameters for all log source types:

Parameter	Description
Log Source Identifier	The IPv4 address or host name that identifies the log source. If your network contains multiple devices that are attached to a single management console, specify the IP address of the individual device that created the event. A unique identifier for each, such as an IP address, prevents event searches from identifying the management console as the source for all the events.
Enabled	When this option is not enabled, the log source does not collect events and the log source is not counted in the license limit.
Credibility	Credibility is a representation of the integrity or validity of events that are created by a log source. The credibility value that is assigned to a log source can increase or decrease based on incoming events or adjusted as a response to user-created event rules. The credibility of events from log sources contributes to the calculation of the offense magnitude and can increase or decrease the magnitude value of an offense.
Target Event Collector	Specifies the QRadar Event Collector that polls the remote log source. Use this parameter in a distributed deployment to improve Console system performance by moving the polling task to an Event Collector.
Coalescing Events	Increases the event count when the same event occurs multiple times within a short interval. Coalesced events provide a way to view and determine the frequency with which a single event type occurs on the **Log Activity** tab. When this check box is clear, events are viewed individually and events are not bundled. New and automatically discovered log sources inherit the value of this check box from the **System Settings**

	configuration on the **Admin** tab. You can use this check box to override the default behavior of the system settings for an individual log source.

3.2. IBM® Security Access Manager (Enterprise Single Sign-On) Device Support Module Configuration

You can use the IBM® Security Access Manager for Enterprise Single Sign-On Device Support Module (ESSO DSM) for IBM® Security QRadar (QRadar) to receive events that are forwarded by using syslog.

Things to note	Step	Additional
	QRadar can collect events from ISAMESSO versions 8.1/8.2.	
	Events that are forwarded by the ISAMESSO include audit, system, and authentication events.	
	Events are read from the following database tables and forwarded by using syslog:	▪ IMSLOGUserService ▪ IMSLOGUserAdminActivity ▪ IMSLOGUserActivity
	All events that are forwarded to QRadar from ISAMESSO use ### as a syslog field-separator.	
	ISAMESSO forwards events to QRadar by using UDP on port 514.	

3.2.1. IBM® Security Access Manager (Enterprise Single Sign-On) Device Support Module Requirements

Requirements	Step	Additional

	You must be an administrator, or your user account must include credentials to access the IMS Configuration Utility to configure syslog forwarding for events.	
	Any firewalls that are configured between your ISAMESSO and QRadar are ideally configured to allow UDP communication on port 514.	This configuration requires you to restart your ISAMESSO appliance.
	This configuration includes a requirement to enable and direct syslog output of ESSO audit logs from the IBM® Security Privileged Identity Manager virtual appliance (ISPIM VA) to the QRadar through the “update_syslog” command of the ISPIM VA command line interface.	

3.2.2. Configuring syslog forwarding

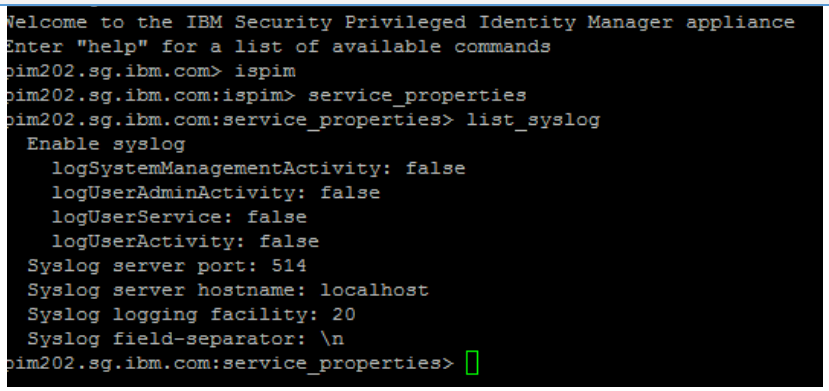
To forward events to QRadar, you must configure a syslog destination on your IBM® Security Access Manager for Enterprise Single Sign-On (ISAM ESSO) appliance.

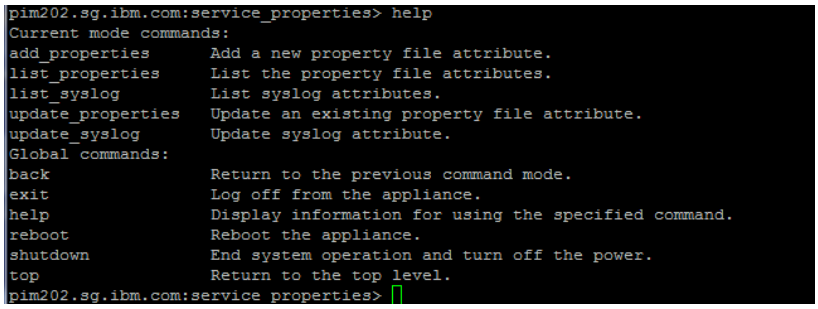
<table>
<tr><th>Step</th><th>Additional</th></tr>
<tr><td>Log on to the ISPIM virtual appliance command line interface.</td><td></td></tr>
<tr><td>Type the following commands:

>ispim

>service_properties

>list_syslog

>update_syslog</td><td>




</td></tr>
<tr><td>Configure the following options:

ISAMESSO: Syslog parameters</td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Enable syslog</td><td>From the Available Tables list, you must select the following tables, and click Add.

• logUserService
• logUserActivity
• logUserAdminActivity</td></tr>
<tr><td>Syslog server port</td><td>Type 514 as the port number used for forwarding events to QRadar.</td></tr>
</table>
</td></tr>
</table>

	Syslog server hostname — Type the IP address or host name of your QRadar Console or Event Collector. **Syslog logging facility** — Type an integer value to specify the facility of the events that re forwarded to QRadar. The default value is 20. **Syslog field-separator** — Type ### as the characters used to separate name-value pair entries in the syslog payload.
Click **Update** to save the configuration.	
Restart your ISAMESSO appliance.	The syslog configuration is complete. The log source is added to QRadar as ISAMESSO syslog events are automatically discovered. Events that are forwarded to QRadar are displayed on the **Log Activity** tab.

3.2.3. Configuring a log source in IBM® Security QRadar

QRadar automatically discovers and creates a log source for syslog events from IBM® Security Access Manager for Enterprise Single Sign-On (ISAM ESSO).

Take note that the following procedure is **optional**.

Step	Additional
Click the **Admin** tab.	
Click the **Log Sources** icon.	
Click **Add**.	
In the **Log Source Name** field, type a name for your log source.	
From the **Log Source Type** list, select **IBM Security Access Manager for Enterprise Single Sign-On**.	
Using the **Protocol Configuration** list, select **Syslog**.	

Configure the following values:

Syslog parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your ISAMESSO appliance.
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	Select the **Credibility** of the log source. The range is 0 – 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	Select the **Event Collector** to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for

		each log source.
	Incoming Event Payload	From the **Incoming Event Payload** list, select the incoming payload encoder for parsing and storing the logs.
	Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Click **Save**.		
On the **Admin** tab, click **Deploy Changes**.		

3.3. IBM® Privileged Session Recorder Device Support Module Configuration

The IBM® Security QRadar Device Support Module (QRadar DSM) for IBM® Privileged Session Recorder (PSR) can collect event logs from your PSR device.

3.3.1. IBM® Privileged Session Recorder Device Support Module Specification

The following table lists the specification for the IBM® Privileged Session Recorder Device Support Module (PSR DSM).

Specification	Value
Manufacturer	IBM
DSM name	Privileged Session Recorder
RPM filename	DSM-IBMPrivilegedSessionRecorder
Protocol	JDBC
QRadar recorded event types	Command Execution Audit Events
Automatically discovered?	No
Includes Identity?	No
More information	IBM website (http://www.ibm.com/)

3.3.2. Collect IBM® Privileged Session Recorder events

To collect IBM® Privileged Session Recorder (PSR) events, see the following steps:

<table>
<tr><th>Step</th><th>Additional</th></tr>
<tr><td>If automatic updates are not enabled, download and install the following RPMs on your QRadar Console:</td><td>▪ Protocol-JDBC RPM
▪ IBM Privileged Session Recorder DSM RPM</td></tr>
<tr><td>On the IBM® Security Privileged Identity Manager (ISPIM) dashboard, obtain the database information for the PSR data store and configure your PSR DB2 database to allow incoming TCP connections.</td><td></td></tr>
<tr><td>For each instance of PSR, create a PSR log source on the QRadar Console.

Use the table PSR log source to define the parameters.</td><td>
<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Log Source Type</td><td>IBM Privileged Session Recorder</td></tr>
<tr><td>Protocol Configuration</td><td>JDBC</td></tr>
<tr><td>Log Source Identifier</td><td>DATABASE@HOSTNAME</td></tr>
<tr><td>Database Type</td><td>DB2</td></tr>
<tr><td>Database Name</td><td>The Session Recorder data store name that you configured on the IBM Privileged Identity Manager dashboard.</td></tr>
<tr><td>IP or Hostname</td><td>The Session Recorder database server address.</td></tr>
<tr><td>Port</td><td>The port that is specified on IBM Privileged Identity Manager dashboard.</td></tr>
</table>
</td></tr>
</table>

Username	The DB2 database user name
Password	The DB2 database password
Predefined Query	IBM Privileged Session Recorder
Use Prepared Statements	This option must be selected.
Start Date and Time	The initial date and time for the JDBC retrieval.

3.3.3. Configuring IBM® Privileged Session Recorder to communicate with QRadar

Things to note	Step
	Before you can configure a log source in IBM® Privileged Session Recorder (PSR) for IBM® Security QRadar (QRadar), obtain the database information for the PSR data store.
	You must also configure your PSR DB2 database to allow incoming TCP connections from QRadar.
	PSR is a component of IBM® Security Privileged Identity Manager (ISPIM).

Step	Additional
Log in to the ISPIM web user interface.	
Select the **Configure Privileged Identity Manager** tab.	
Select **Database Server Configuration** in the **Manage External Entities** section.	
In the table, double-click the **Session Recording data store** row in the **Database Server Configuration** column.	
Record the following parameters to use when you configure a log source in QRadar:	

IBM Privileged Session Recorder Field	QRadar Log Source Field
Hostname	IP or Hostname
Port	Port
Database name	Database Name
Database administrator ID	Username

3.4. Download and install Security Content Packages (QRadar RPM Packages)

The Device Support Modules (DSM) mentioned in the previous topic only extract standard event properties (time of event, user ID, event name) from the IBM® Security Privileged Identity Manager (ISPIM) events. ISPIM-specific event attributes (target resource, lease expiry, client IP) remain embedded in a generic "payload" attribute of the event captured by QRadar. To extract ISPIM-specific attributes, you can download and install more QRadar (rpm) packages, called Security Content Packages.

The Security Content Packages extract the ISPIM-specific event attributes as "custom properties" that can be displayed in its own column in the QRadar console, and, which can be directly referenced in QRadar rules.

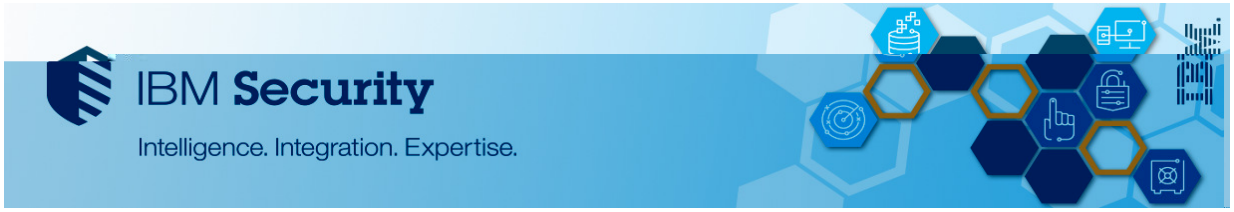
The following are links to the Security Content Packages for ISPIM:

Resource	Step	Additional
	IBM® Security Privileged Identity Manager (Privileged Credential Manager) Security Content Package	http://www.ibm.com/support/docview.wss?uid=swg21961191
	IBM® Security Access Manager (Enterprise Single Sign-On) Security Content Package	http://www.ibm.com/support/docview.wss?uid=swg21963370
	IBM® Privileged Session Recorder Security Content Package	http://www.ibm.com/support/docview.wss?uid=swg21961386

Things to note	Step	User Interface
	You can download the QRadar RPM Packages from Fix Central.	
	Log on to the QRadar admin command line interface to install the RPM packages.	Type the command: rpm -Uvh <rpm name>

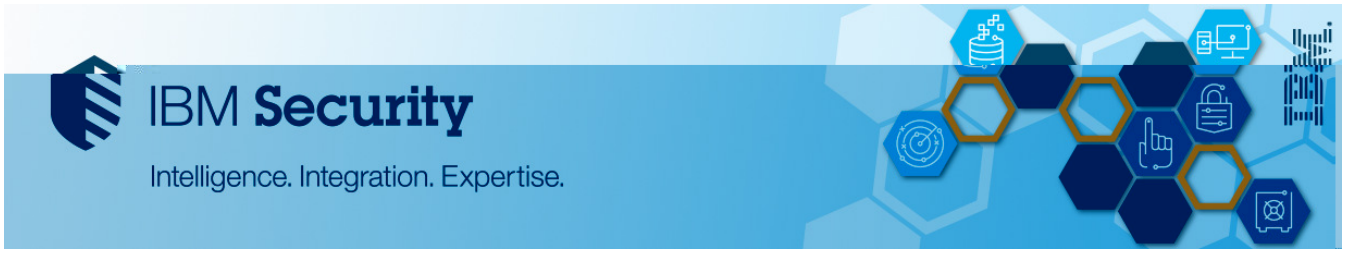
3.4.1. Configure QRadar to display ISPIM events with ISPIM-specific properties

With the Security Event Packages installed and configured, you can configure QRadar to display IBM® Security Privileged Identity Manager (ISPIM) events with ISPIM-specific properties.



Event Name	Log Source	Start Time ▼	Username	Credential ID (custom)	Resource Name (custom)	Action Result (custom)	Lease Expiry Time (custom)	Lease DN (custom)
CredentialLeaseManagement Checkin SU…	PIM@207	Apr 18, 2016, 2:3…	james	operator2	IAM_DOMAIN	SUBMITTED	N/A	28737935419145…
CredentialLeaseManagement Checkin SU…	PIM@207	Apr 18, 2016, 2:3…	james	operator1	IAM_DOMAIN	SUBMITTED	N/A	28735789394966…
CredentialLeaseManagement Checkin SU…	PIM@207	Apr 18, 2016, 2:3…	james	finsysadm	FINDB	SUBMITTED	N/A	28735432055429…
CredentialLeaseManagement GetPasswo…	PIM@207	Apr 18, 2016, 1:4…	james	finsysadm	null	SUCCESS	N/A	N/A
CredentialLeaseManagement Checkout S…	PIM@207	Apr 18, 2016, 1:4…	james	operator2	IAM_DOMAIN	SUCCESS	2016-04-18 13:3…	28737935419145…
CredentialLeaseManagement Checkout S…	PIM@207	Apr 18, 2016, 1:4…	james	operator1	IAM_DOMAIN	SUCCESS	2016-04-18 07:3…	28735789394966…
CredentialLeaseManagement GetPasswo…	PIM@207	Apr 18, 2016, 1:4…	james	operator1	null	SUCCESS	N/A	N/A
CredentialLeaseManagement Checkout S…	PIM@207	Apr 18, 2016, 1:4…	james	finsysadm	FINDB	SUCCESS	2016-04-18 13:3…	28735432055429…

Figure 1 Events with IBM Security Privileged Identity Manager properties.



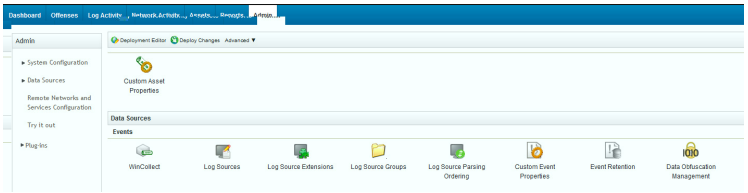
Things to note	Step	Additional
	The QRadar admin can configure custom rules in QRadar to co-relate ISPIM checkout events with native events from various managed hosts.	For example, the QRadar can associate certain abnormal activities that are detected from native logs, by hosts, with the ISPIM user that checked out the Privileged ID in question. It is also possible to customize the QRadar Console to support click-through from the ISPIM checkout log entry into the IBM® Privileged Session Recording (PSR) console to replay the recorded session.
	From ISPIM 2.0, Check-in-Check-out (CICO) events collected through the ISPIM (Privileged Credential Manager (PCM)) Device Support Module (DSM) will contain a “Lease DN” property that can be used as a common handle to easily match a Check-in (CI) event to its corresponding Check-out (CO) event.	This Lease DN is also included in the Description field of CICO events collected by the Enterprise Single Sign-On (ESSO) DSM.
	Login to the QRadar SIEM console as admin.	https://<IP Address>

See the list of useful PIM-specific custom properties. These properties can be selectively added when configuring a custom search on PIM events.

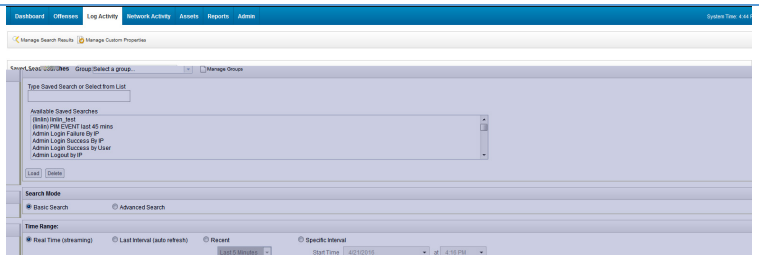
To generate the list of properties, navigate to **Admin** tab. Under **Data Sources** > **Events**, select **Custom Event Properties**.

Property Name	Log Source Type
Credential ID	IBM Security Access Manager for Enterprise Singl...
Credential Pool	IBM Security Access Manager for Enterprise Singl...
Resource Name	IBM Security Access Manager for Enterprise Singl...
Client Application	IBM Security Access Manager for Enterprise Singl...
Client Hostname	IBM Security Access Manager for Enterprise Singl...
Recording ID	IBM Security Access Manager for Enterprise Singl...
Action Result	IBM Security Access Manager for Enterprise Singl...
Lease DN	IBM Security Privileged Identity Manager
Credential ID	IBM Security Privileged Identity Manager
Action Result	IBM Security Privileged Identity Manager
Resource Name	IBM Security Privileged Identity Manager
Lease Expiry Time	IBM Security Privileged Identity Manager

Property Name	Log Source Type
Client Hostname	IBM Privileged Session Recorder
Local User ID	IBM Privileged Session Recorder
Executed Command	IBM Privileged Session Recorder
Resource Name	IBM Privileged Session Recorder
Recording ID	IBM Privileged Session Recorder
Application User ID	IBM Privileged Session Recorder
Client Application	IBM Privileged Session Recorder



To configure a custom search on PIM events, navigate to **Log Activity**.



For example:

For **Search Mode**, leave the default setting.

Under **Time Range**, select **Recent** and **Last 12 Hours** from the drop-down list.

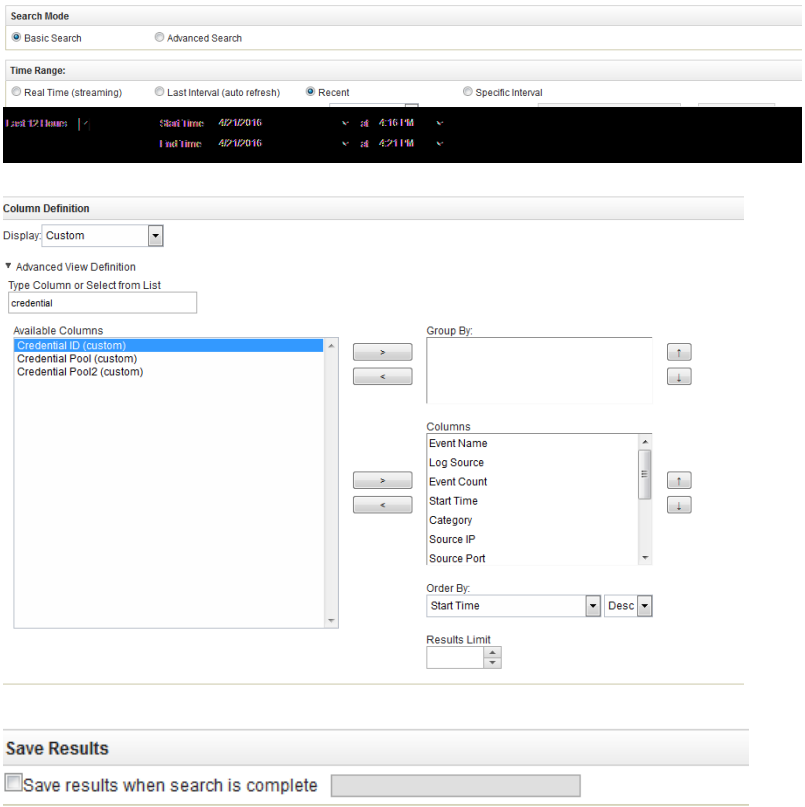
Under **Column Definition**, refer to the list of PIM-specific properties mentioned earlier and select a few from the **Available Columns**.

Select **Credential ID (custom).** Click "**>**" next to the **Columns** field.

Repeat the same for **Resource Name (custom)**, **Action Result (custom)**, **Lease Expiry (custom)**, **Lease DN (custom)**.

Click **Search**.

Select **Save Results** to save results of custom search.



Refer to figure 1 Events with ISPIM Properties above for the search results.

3.5. Configure QRadar console to add a URL link to ISPIM PSR console to review recording of checked-out ID

Step	Additional
You can select an IBM® Security Privileged Identity Manager (ISPIM) event that has an associated Session Recording ID, and navigate to the ISPIM Session Recorder console to replay the recording of that particular session.	This process requires customizing QRadar to add a right-click menu option to events that displays a Privileged Session Recorder Recording ID. Since single sign-on does not exist between QRadar and PSR consoles, you must log in to the Privileged Session Recording console if you are not already logged in.
To enhance the right-click menu for event and flow columns, go to	Enhance the right-click menu for event and flow columns

Set up the right-click menu from QRadar to Privileged Session Recording console by specifying the following parameters in the `/opt/qradar/conf/arielRightClick.properties` file:	`pluginActions=PSRSessionIdAction`
	`PSRSessionIdAction.arielProperty=Recording ID`
	`PSRSessionIdAction.text=View PIM Session Recording`
	`PSRSessionIdAction.url=https://<Session Recording Server IP or hostname>/recorder/ui/SessionRecordingContainer.html?recordingId=$Recording ID$`

3.6. Configure QRadar to invoke ISPIM API upon certain events

You can have QRadar invoke an ISPIM API in response to certain triggering events.

Step	Additional
QRadar can be configured to invoke specific Directory Integrator assembly lines upon certain triggering conditions.	You can also customize such an assembly line to issue calls to ISPIM APIs.
See the article on how the QTrigger framework can be used to have QRadar events trigger API calls to external systems (such as Guardium):	Guardium QTrigger framework
With IBM® Security Privileged Identity Manager v2.0.1, a number of ISPIM administrative functions was exposed as RESTful APIs. Therefore, it is conceivable for customers to configure QRadar such that certain offenses would trigger a call to ISPIM to perform remediation actions.	For example, if there is a QRadar offense suggesting a possible breach involving a shared ID, it is possible to use this mechanism to instruct ISPIM to temporarily suspend the user from further Check-outs from ISPIM.
See the YouTube video on a sample scenario involving integration between QRadar, Guardium and ISPIM:	https://www.youtube.com/watch?v=TedDkWnAArc