Onapsis Security Platform

QRadar Integration Guide

Version 2.0.1

onapsis

Table of Contents

About this Guide

Overview of this Guide

This guide provides details on using the Onapsis Security Platform (OSP) to populate IBM® QRadar® with security events generated by the Vulnerability, Compliance and Detection capabilities of OSP. This integration reduced the time needed to carry out the analytical process, with all results and analysis from OSP available in the one QRadar console.

Audience

This guide is written for users responsible for keeping a company secure, including, but not limited to the following departments: Information Security, Compliance and Audit, and SAP Infrastructure and Governance.

If You Need Assistance

IBM Security QRadar products
See the *Links & Important Support Resources for IBM Security QRadar products* page available on the IBM Support site http://www-01.ibm.com/support/docview.wss?uid=swg21616144

Onapsis Security Platform
View the complete User Guide, available in the Onapsis Customer Portal (https://portal.onapsis.com)

Contact support by email at support@onapsis.com Monday-Friday 7am-7pm ET. Please include steps to reproduce the issue, screenshots, and indicate that you use OSP and list the version. Technical Support is unavailable during regional and major US holidays.

Manage QRadar Integration

Overview of QRadar Integration

You can alarm information in real-time to IBM QRadar to better analyze and gain visibility into vulnerabilities across your entire organization. The information from the alarms can be compared with information from your network (such as information flows or traffic, and data about ports and protocols), asset context, events from third-party devices, feeds, and other sources to provide your company with a comprehensive security posture assessment. With this integration, you extend your existing QRadar security processes and workflows to include security and compliance information from OSP, while retaining a single reporting tool for analyzing risk within your organization.

Pre-requisite for environments where the previous content pack is installed

If the *Onapsis Content Pack* is installed in your QRadar environment, it needs to be uninstalled for the new version to work properly. Pre-732, the old custom properties also need to be manually disabled or deleted (see instructions below).

Manually deleting a custom property

1. Click the Log Activity tab.
2. From the Search list box, select Edit Search.
3. Click Manage **Custom Properties**.
4. Select the **custom property** that you want to delete and click **Delete**

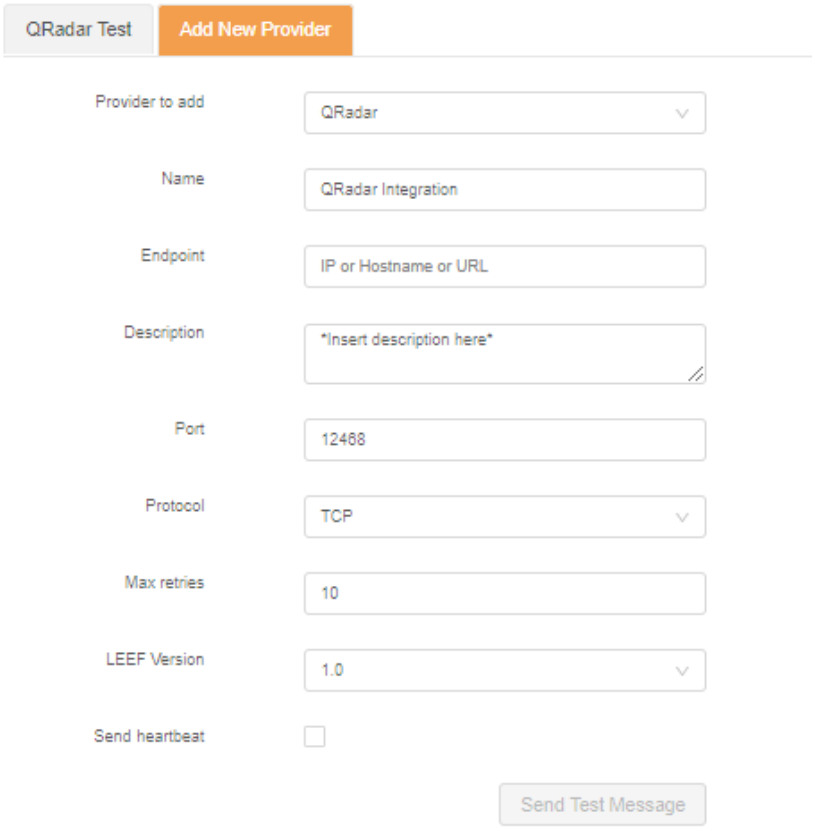
On the Onapsis QRadar App

The *Onapsis Security Platform for SAP* App does not currently work in conjunction with the new version of the Onapsis Content Pack.

Creating a QRadar Integration in OSP

Adding an Integration Provider

1. Navigate to **Integrations > Setup**
2. Select **Add New Provider**
3. From the Provider to add dropdown, select your integration type > **QRadar**
4. Fill in the other fields (see example below):
   4.1. Name – Displays when defining actions for an alarm
   4.2. Endpoint – IP or Hostname or URL of your QRadar console
   4.3. Port – Port number to connect to the service on the host – 12468 for TCP | 517 for UDP
   4.4. Protocol – TCP Highly Recommended
   4.5. Send heartbeat – Select to check if the OSP console is active (every 5 minutes)



5. Once QRadar is configured (see next section of this document), the integration can be tested by clicking on **Send Test Message**
6. Click **Add provider** at the bottom right of the screen

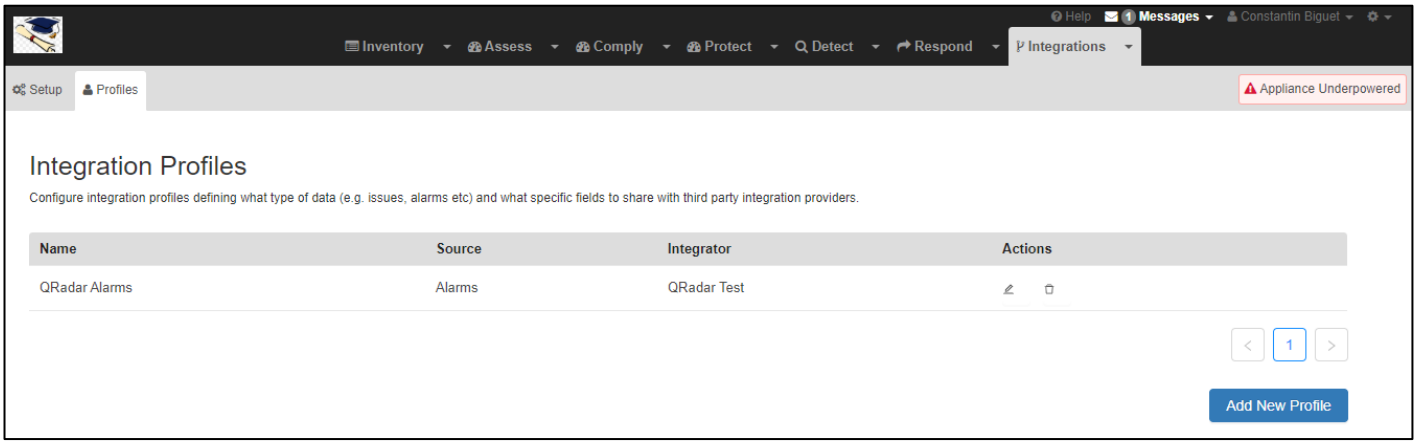
Setting up Integrations Profiles for your new Integration

Once you have created an integration, OSP can communicate with QRadar. Typically, you want to send information on alarms previously created in the Respond section of OSP (link to Creating Alarms here).

In order to tell OSP what it must send, you need to create integration profiles linked to your QRadar integration. The steps to complete are detailed below:

1. Navigate to **Integrations > Profiles**
2. Select **Add New Profile**
3. Choose a Profile Name, and select your QRadar integration
4. Select a Source
5. For Notification Cadence, it is recommended to select **Send All Alarms** from the dropdown menu
6. For Data, check all boxes
7. Review profile and click **Save**

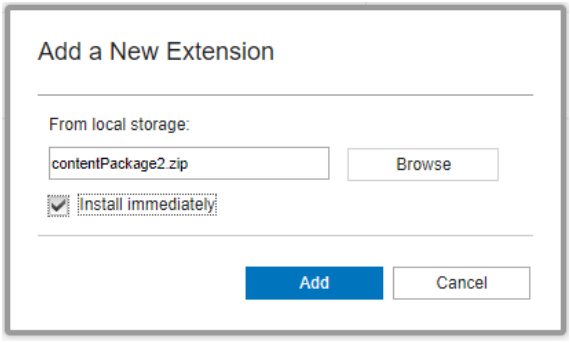
Assuming that you want QRadar to receive Alarms, your integration profiles page should look something like this:



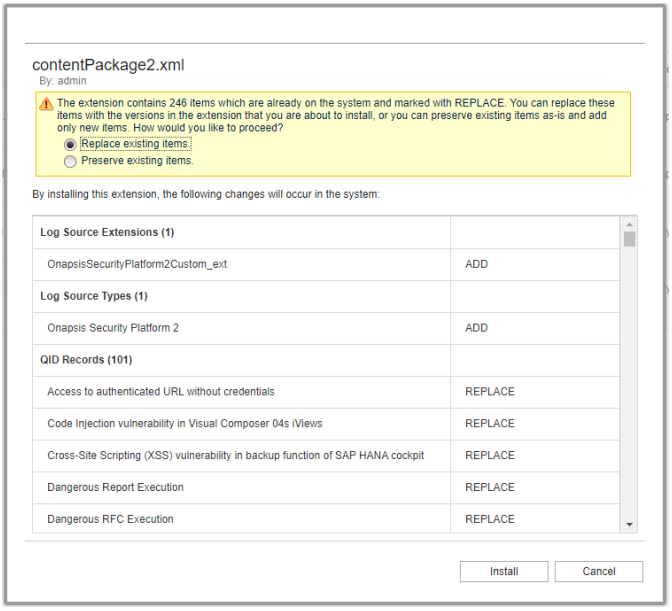
Configuring QRadar to receive and recognize OSP events

Installing the OSP package in QRadar

1. Go to the **Admin** tab, and click on **Extensions Management**
2. Click on the **Add** button
3. Select the Onapsis Package (zip file) from your local storage
4. Check the **Install immediately** box, and click on **Add**



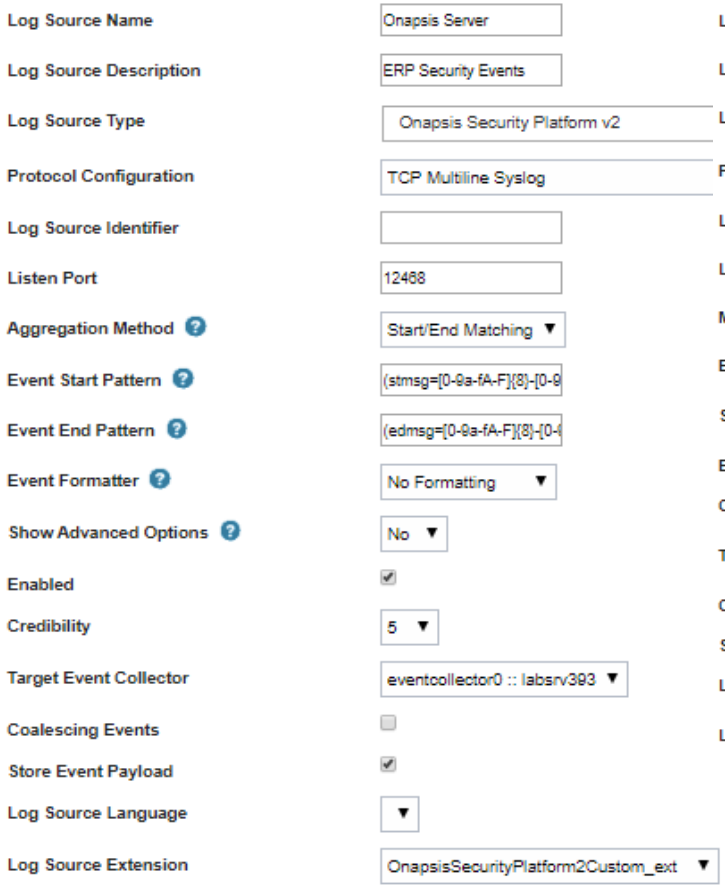
5. If the extension contains items already in your system, select **Replace existing items** and hit **Install**

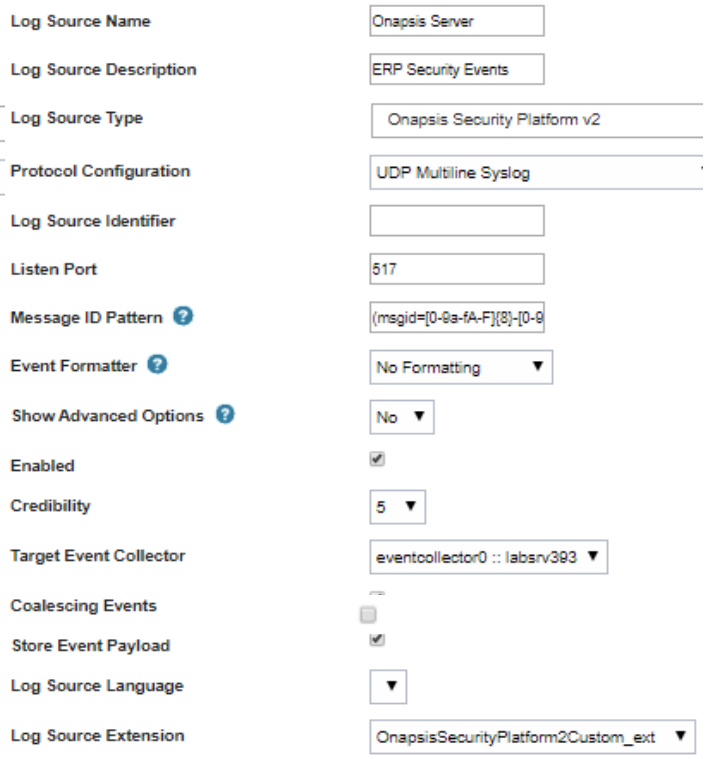


Creating an OSP log source in QRadar

1. Go to the **Admin** tab, and click on **Log Sources**
2. Click on **Add**
3. Fill in the fields as shown in the image below
   3.1. Enter the IP address of your OSP console in **Log Source Identifier**
   3.2. Choose your preferred **Target Event Collector** from the dropdown menu
   3.3. Copy the regex in the table below and paste them in the appropriate fields
   3.4. For **Advanced Options**, select only "Flatten Multiline Events into a single line" for TCP, and nothing for UDP
4. Click on **Save**
5. In the Admin tab, click on **Deploy Changes**

Integration using TCP protocol (Recommended)	Integration using UDP protocol





Event Start Pattern	(stmsg=[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12})	Message ID Pattern	(msgid=[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12})
Event Start Pattern	(edmsg=[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12})		

User Activity Event Mappings

As of 2.2020.32, Onapsis offers a set of pre-packaged alarms including the User Activity Alarms that are the most important to monitor in your SIEM. These will be automatically recognized by the Onapsis DSM. If you create any custom user activity alarms, you will have to add them by following the instructions below.

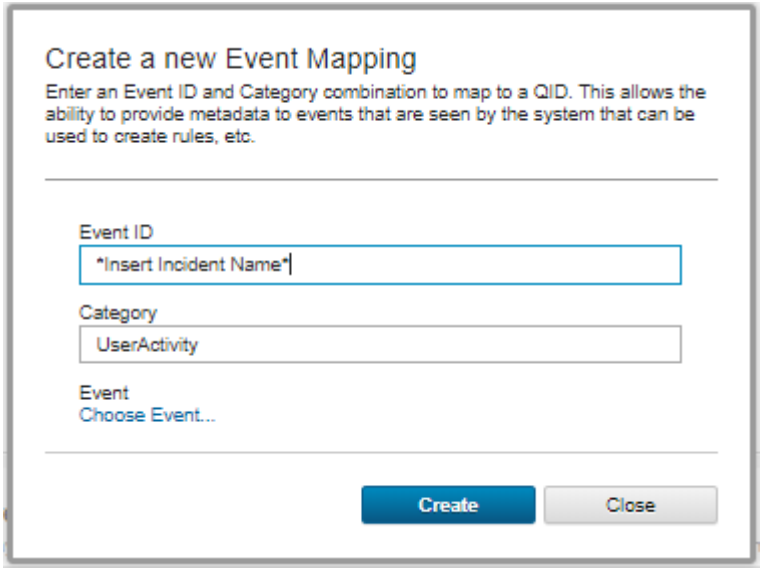
Adding Custom User Activity Alarms

When creating a User Activity Alarm in OSP, make sure to accurately describe the actions that should be taken when that incident occurs. Those descriptions are used to define the corresponding Events in QRadar. Precise descriptions will ensure your SOC team take the correct steps to fix the issue.
There are two options to add these events to the DSM: doing it manually using the GUI or using a python script (provided to you on demand) to create a User Activity package. Both options are described below.

Using the GUI

Adding an event mapping:

1. In the Admin tab, click on **DSM Editor**
2. When prompted, choose **Onapsis Security Platform 2** as a log source type
3. Go to the **Event Mappings** tab, and click on the **+** button
4. Fill in the fields as shown below



5. Click on **Choose Event…**
6. Click on **Create New QID Record**
7. Give the event a name, description, high- and low-level category, severity
8. In the search results, select the QID you created and hit **Ok**
9. Click on **Create**

Using the provided script

1. Export OSP alarms to CSV
   1.1. Navigate to Respond > Alarm Profiles
   1.2. Click on Export Report > Alarm profiles CSV
   1.3. Wait for the report to load, and click on Alarm profiles CSV again
2. Identify the ID of the Onapsis DSM
   2.1. SSH into your QRadar environment
   2.2. Execute the following command: $ sudo /opt/qradar/bin/contentManagement.pl -a search -c sensordevicetype -r "OnapsisSecurityPlatform2"
   2.3. Record the returned ID
3. Generate the OSP UserActivity Package
   3.1. Put the CSV report and python script into a common folder
   3.2. Execute qradar_useractivity_package.py to transform the report into the adequate XML file (you will be asked to input the CSV file's name and the Onapsis DSM ID)
   3.3. Zip OSP_UserActivity_Package.xml
4. To install the package, follow the same procedure as in the "Install the OSP package in QRadar" section of this document

Onapsis QRadar Integration Technical Overview

NOTE: Prior to installing version 2.0 customers need to uninstall all previous versions of the Onapsis Content Pack and Onapsis Security Platform for SAP QRadar

This document is intended to give an overview of how the integration between Onapsis Security Platform and QRadar functions. The Onapsis QRadar Technical Integration consists of two principal components.

- **QRadar Connector** - The connector defines the transport mechanism from the Onapsis Security Platform (OSP) to the QRadar platform, plus the mapping of application fields in OSP to fields in QRadar

The QRadar connector and app are intended to support two principal use cases

- **Detection and Response** - The analyst views information about OSP alarms within the QRadar console.
- **Vulnerability and Compliance** - The analyst views results of OSP scans within the QRadar console (not currently supported)

The QRadar connector uses syslog to communicate with the QRadar system. By default, QRadar uses port 517 for UDP Multiline Syslog and 12468 for TCP Multiline Syslog. The Syslog Redirect protocol is designed to better support the use of syslog forwarders. More information can be found in the Syslog Redirect protocol overview.

QRadar Connector

The QRadar Connector uses UDP or TCP to send log information from OSP to QRadar. Information on how to configure this connector can be found in OSP QRadar Integration Guide.

QRadar supports the LEEF format for collecting and parsing logs from third party products. More information about this standard can be found here. LEEF also supports the use of custom fields as well as those explicitly defined in the standard.

OSP sends the following fields to QRadar

Detection and Response Event

Name	Description	Type
Alarm Profile	The name of the alarm profile that triggered the alarm	Custom
Asset Name	System ID of the asset where the alarm was triggered	Custom
Client	The SAP client triggering the alarm	Custom
Created At	The time at which OSP detected the issue	Custom
Detected Compliance	A boolean flag that marks if the assessment returned findings	Custom

Dev Time	Time the alarm was triggered	LEEF
Dev Time Format	Time format of the previous field	LEEF
Erp Event Source	The log source within the ERP system that causes the trigger e.g. SAL	Custom
Erp Host	The IP address of the ERP system triggering the alarm	Custom
Erp Time	The time on the ERP system when the alarm was triggered	Custom
Event ID	The type of alarm – Exploitation, Zero Day, Sensitive Access, Vulnerable Access, User Activity	LEEF
Event Type	The type of event on the ERP system	Custom
FQDN	Domain name that specifies the OSP location in the DNS tree hierarchy	Custom
Incident Name	Name of the incident that triggered the alarm	Custom
Incident Detail	Detail of the incident that triggered the alarm	Custom
Job Name	Name of the assessment scan or compliance audit that detected the issue (compliance or assessment alarm only)	Custom
Logline	The ERP event that triggered the alarm	Custom
Matching Rule	Hash of the rule that matched with our event to generate the incident	Custom
Module Category	Category of the module that generated the issue. This field will only be completed if the alarm is of an Assessment type.	Custom
Module Description	Description of the module that generated the issue. This field will only be completed if the alarm is of an Assessment type.	Custom
Module Name	Name of the module that generated the issue. This field will only be completed if the alarm is of an Assessment type.	Custom
Modified	The ERP user modified by the action that triggered the alarm (when applicable)	Custom

Patch Applied	Boolean that tells whether the sap note related to the incident was patched or not	Custom
Policy	Policy name of the audit that triggered the alarm (If the alarm type is Compliance)	Custom
Policy ID	ID of the policy that triggered the alarm (If the alarm type is Compliance)	Custom
Reason	The reason why the SAP event occurred, usually a numerical value, sometimes a legend e.g. INVALID_PASSWORD, or VERIFY_FAILED	Custom
Sap Security Notes	Sap note related to the incident	Custom
Success	The result of the transaction that triggered the alarm, e.g. ABAP, Java	Custom
System Type	The type of ERP system that triggered the alarm	Custom
tcode	The tcode of the transaction that triggered the alarm	Custom
Terminal Source	The host name/IP address of the suspected attackers machine	Custom
Username	The username of the ERP user triggering the alarm	Custom
User Type	The type of ERP user e.g. DIALOG, SERVICE	Custom
Vulnerability Cvss	CVSS Score. Only valid for assessment alarms	Custom

Known Issues

There are several known issues with the current version of the QRadar integration.

- It is currently not possible to map assessment and compliance data in QRadar, this will be fixed in a subsequent version.
- Heartbeat and Test Messages are not currently mapped either

Appendix I - Sample Alarm

```
msgid=2869012a-630b-4d66-952e-21092a369ab2LEEF:1.0|Onapsis Inc.|Onapsis Security
Platform|2.2020.21.0.0|Exploitation|assetName=T74 devTime=2020-10-22T21:38:00.879922+00:00
devTimeFormat=yyyy-MM-dd'T'HH:mm:ss.SSS sid=T74 detectedCompliance=None jobName=None
moduleCategory=None moduleDescription=None moduleName=None vulnerabilityCvss=None client=001
destinationPort=None dst=labsapsrv079_T74_00 erpEventSource=SAL erpHost=192.168.206.79
erpTime=2020-10-22T21:37:08+00:00 eventType=UserUnlocked incidentDetail=None
incidentName=Unlocking of User DDIC logline=User DDIC Unlocked
matchingRule=2b6f9ecd98824e3bbac2debb3abd98fb modified=DDIC patchApplied=None protocol=None
reason=None sapSecNotes=None sourcePort=None success=None systemType=ABAP
terminalSource=172.21.53.102 usrName=ZONAPSIS userType=None
alarmProfileMatches=[{"alarm_name": "exploitation alarm", "profile_id": 3}]
eventId=Exploitation
```