observe IT
a proofpoint company

IBM QRadar Integration Guide

observe IT
a proofpoint company

Table of Contents

observe IT
a proofpoint company

Overview

This document describes the integration of ObserveIT with IBM QRadar software.

FEATURES

The ObserveIT App for IBM QRadar does the following:

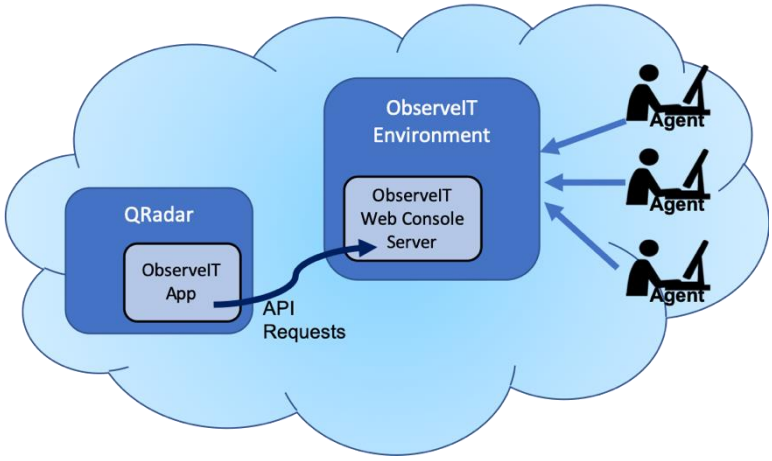
- Event Collection: Functions as a custom protocol to connect QRadar to the ObserveIT RESTful API and continuously pull the latest events. ObserveIT App pulls data from ObserveIT into QRadar as follows:
    - Subscribes to User Interface Activity, User Command Activity, and Alert events
    - Polls events from multiple ObserveIT instances
- Sample Dashboard: Provides a sample dashboard to highlight insights from your ObserveIT data and includes.
    - Summary of the most active endpoints and most visited sites
    - Charts to highlight the riskiest users and top alert categories
    - Customizable to suit your needs
- Sample Rules: Includes some custom rules to get you started such as:
    - Mapping the ObserveIT Severity to a corresponding numeric QRadar Severity
    - Creating offenses from High and Critical Severity Alerts

PREREQUISITES

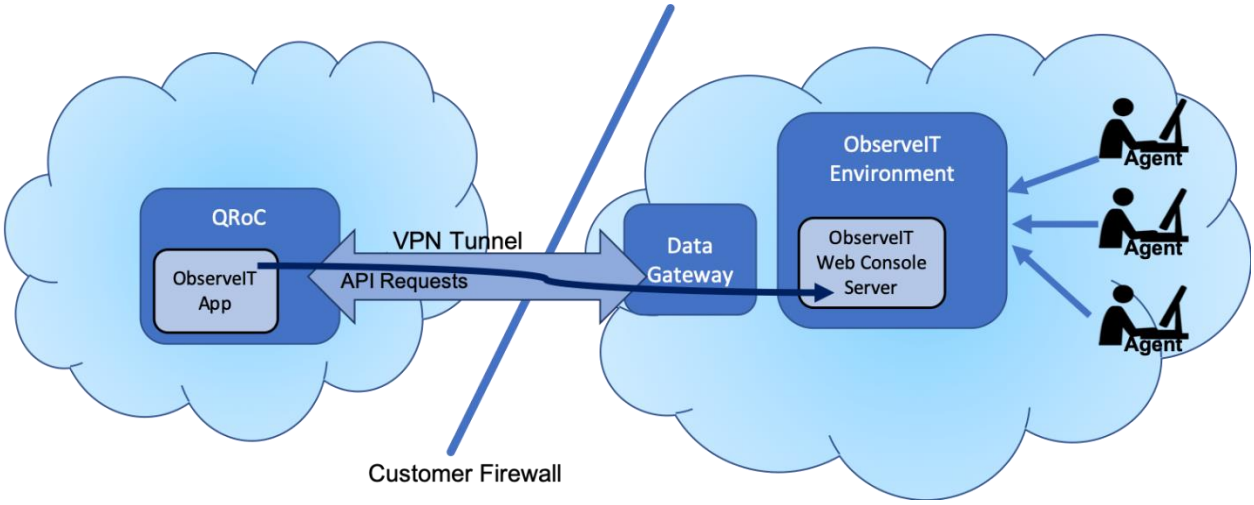
- Downloaded and install ObserveIT App from the IBM X-Force Exchange
- ObserveIT App communicates with your ObserveIT API directly, typically on port 443.
- ObserveIT (Minimum supported version 7.5.1)
- IBM QRadar (Minimum supported version 7.3.1)

DELPOYMENT ARCHITECTURE

The diagram shows how ObserveIT integrates into an on-prem IBM QRadar.



This shows an integration with QRadar On Cloud (QRoC).



Configuration

You configure ObserveIT App to reach the ObserveIT REST API and retrieve report data.

CREATING APPLICATION IN OBSERVEIT

To integrate ObserveIT with IBM QRadar using RESTful API, you register the application to authenticate access. Oauth2 is the method of authenticating access to the ObserveIT RESTful API.

This procedure describes how to generate a token that you use when you configure ObserveIT TA for QRadar.

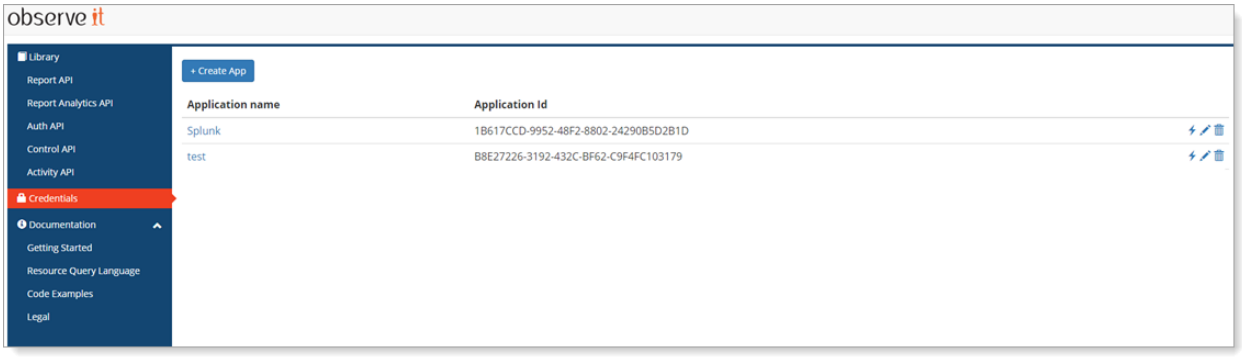
1. From the ObserveIT Web Console, click the ❓ in the upper-right corner and select **Developer Portal** from the menu.

   Notes:

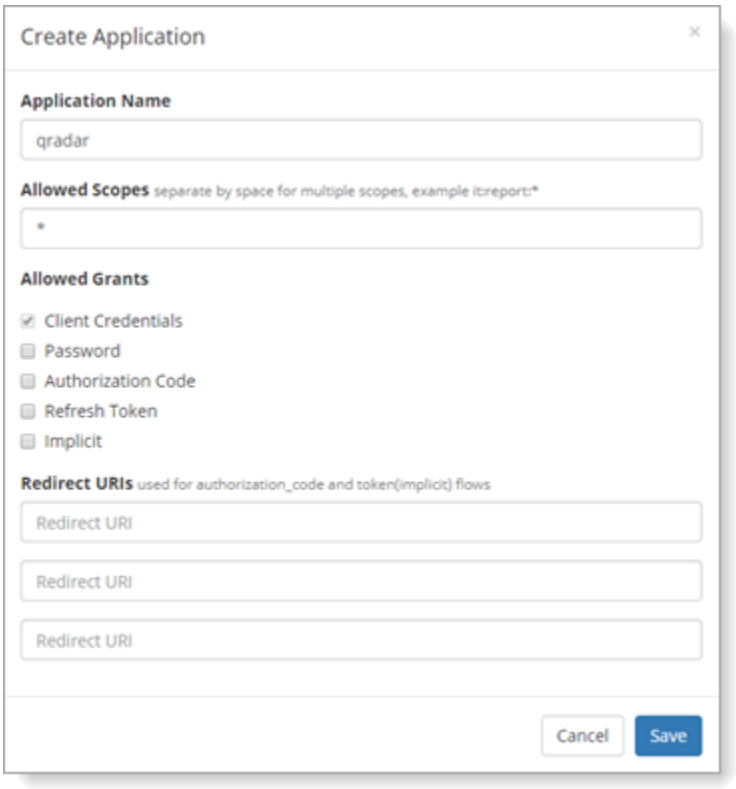
   If the **Developer Portal** is not installed by default, you will be prompted to install it.

   If the **Developer Portal** fails to properly load, log out of the ObserveIT console and log back in with a local system account rather than an LDAP account.

2. From the **Developer Portal**, select **Credentials** and then click the **Create App** button.



The **Create Application** dialog box displays. This is where you register the application.

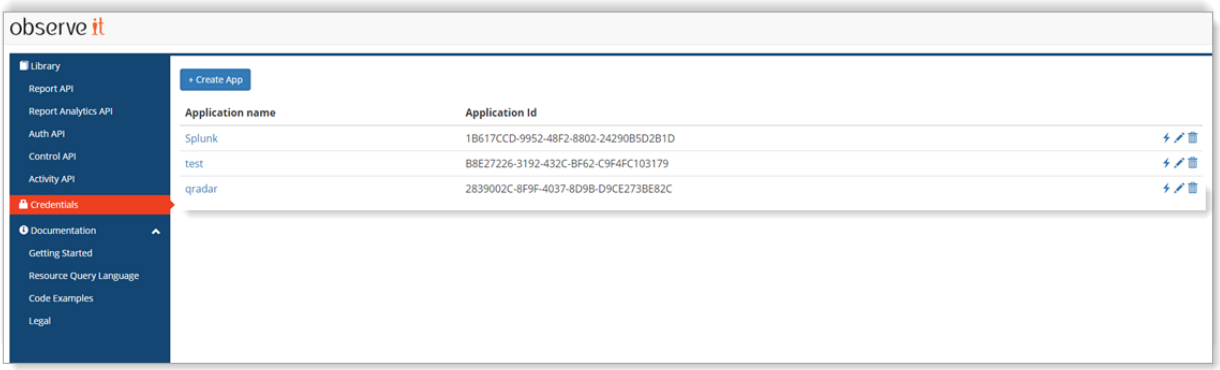


3. Do the following:

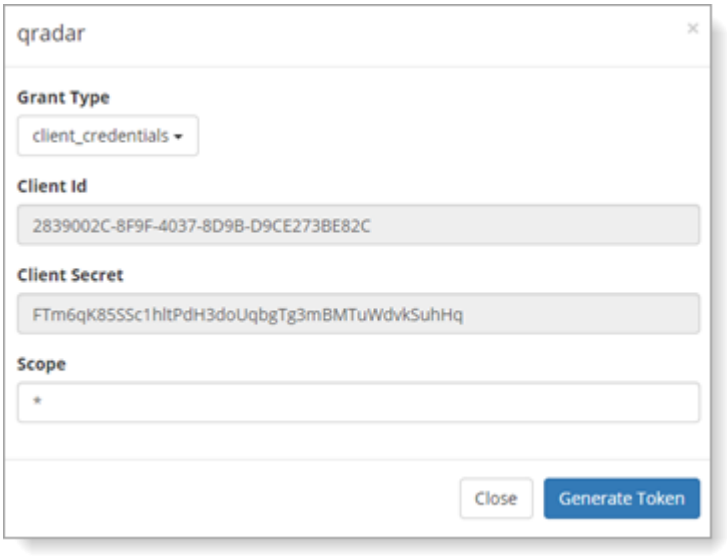
    a. In the **Application Name** field, enter a name. It is recommended that you choose a name you can recognize, such as **QRadar**, **QRadar1** etc.

    b. In **Allowed Grants**, check **Client Credentials**.

    c. Click **Save** and the application is added to the list.



4. Click the application you just created. The dialog box for generating a token displays.



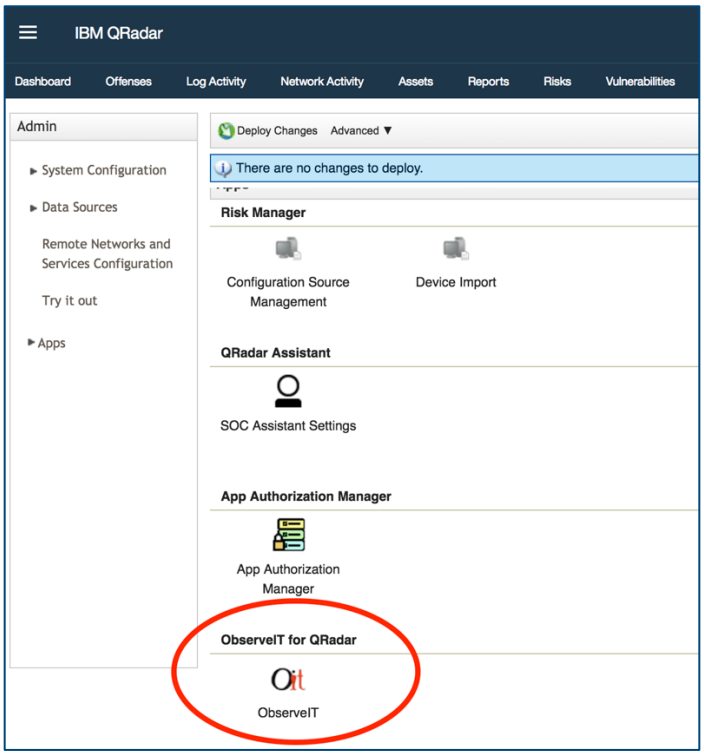
Note the **Client Id** and **Client Secret** values. You will enter them into the configuration screen of the **QRadar add-on**. (See: Configuring ObserveIT App for QRadar.)

CONFIGURING OBSERVEIT APP FOR QRADAR

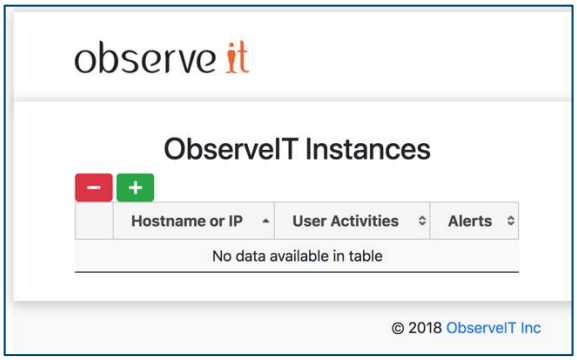
This procedure describes the registration process in QRadar.

Your ObserveIT instance(s) needs to be registered in the ObserveIT QRadar app. The access token (with the **Client ID** and **Client Secret)** you generated in the ObserveIT **Developer Portal** will be used to authenticate with the API.

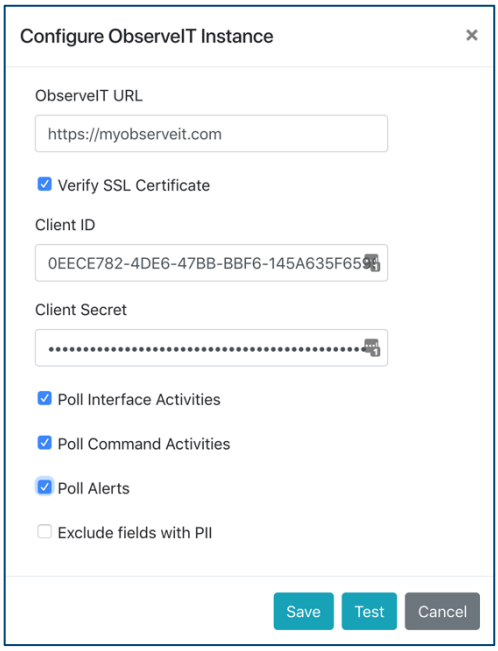
1. Open the QRadar Admin screen and scroll down to the bottom. Click the **ObserveIT** icon.



The list of ObserveIT instances displays.



2. Click the **+** button to add your ObserveIT instance.



3. Complete the **Configure ObserveIT Instance** dialog box.
   a) Enter the **Client ID** and **Client Secret** values that you copied previously. (See: Creating Application in ObserveIT.)
   b) **Verify SSL Certificate**: If your ObserveIT instance is using a self-signed certificate and you are unable to assign it a trusted one, then uncheck the **Verify SSL Certificate** box. Note that this is a less secure option

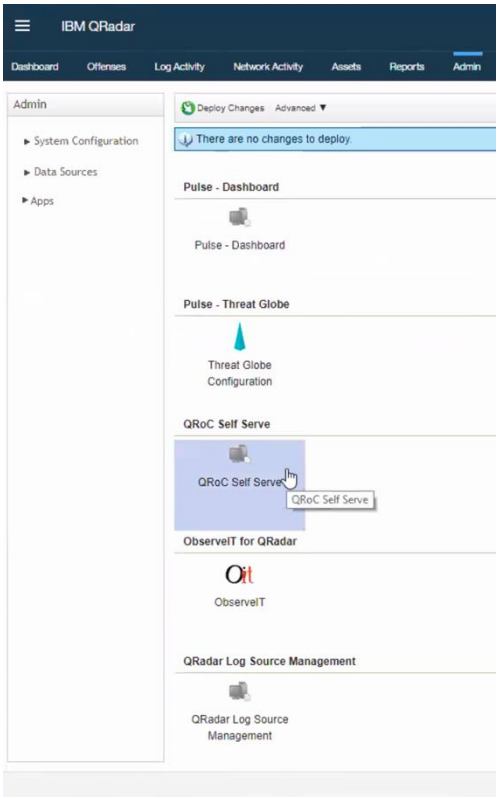
c) **Exclude fields with PII:** If checked, then any fields that might contain **Personally Identifiable Information** are not be loaded into QRadar.
Note: The following fields will be excluded from the user activity and alert data: loginName, secondaryLoginName, endpointName, remoteHostName, windowTitle, accessedUrl, domainName, secondaryDomainName, remoteAddress, sqlUserName

4. Click Test before saving to verify the connection between QRadar and ObserveIT.

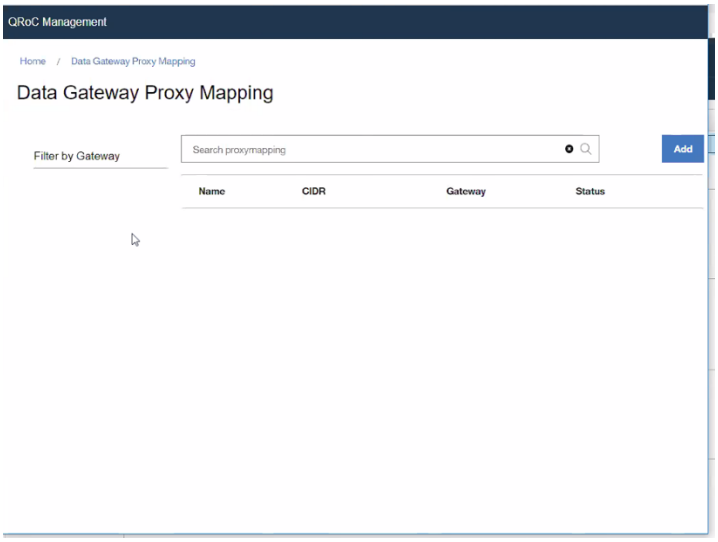
QRADAR ON CLOUD

This section describes the requirements for configuring the ObserveIT app for QRadar in a QRoC environment. A Data Gateway must be installed on your local network to allow the HTTP(S) API requests from the ObserveIT QRadar app to connect to the ObserveIT web console.

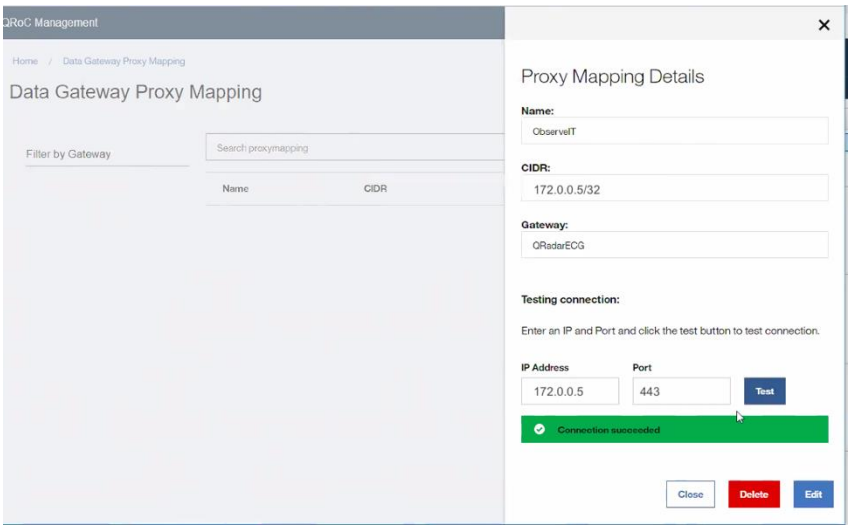
1. In the QRoC Admin Console, select "QRoC Self Service".



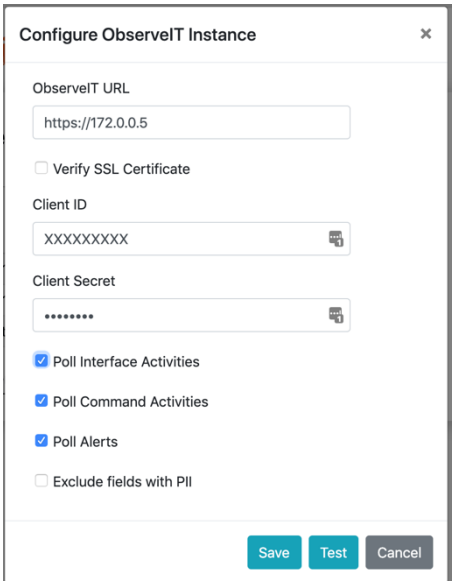
2. Click Add to add a new proxy mapping.



3. Configure a proxy mapping to the ObserveIT Web Console and test the connection.



4. Configure the ObserveIT app, using the IP address as the hostname in the URL. Unless your ObserveIT certificate has the IP address specifically included as a valid subject alt name, you will need to uncheck the Verify SSL Certificate option.



For more details, please visit the IBM Knowledge Center.
https://www.ibm.com/support/knowledgecenter/en/SSKMKU/com.ibm.qradar.doc_cloud/c_qross_proxy_mapping.html

Usage

APPLICATION TUNING

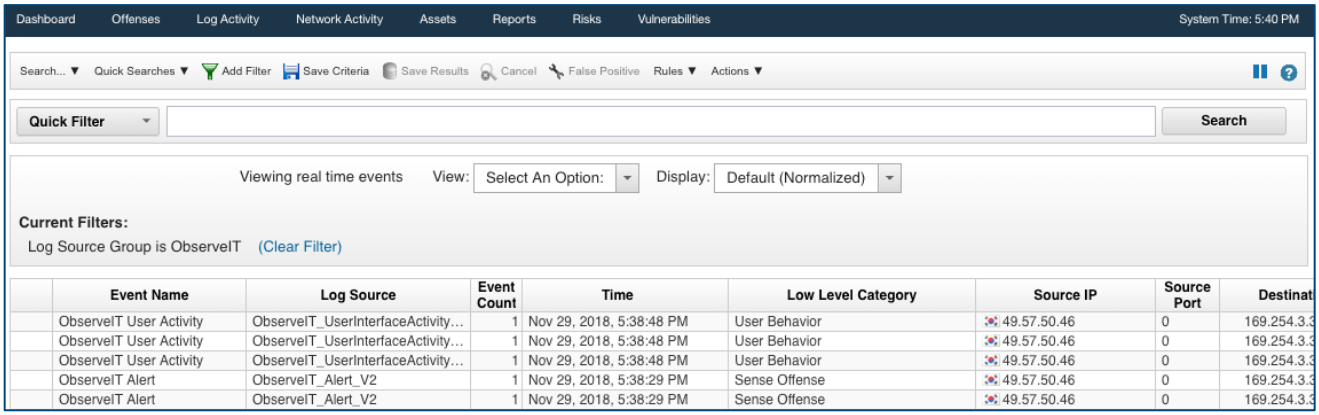
ObserveIT custom properties: Enable indexing and update the pre-parse settings according to the searches and reports you need.

Offenses: By default, all user sessions with one or more High or Critical level alerts will generate an offense, using the session ID as the offense source. You can customize and configure the rules. You may choose to use the loginName or ruleCategory as the offense source depending on how you prefer to manage offenses and investigate alerts.

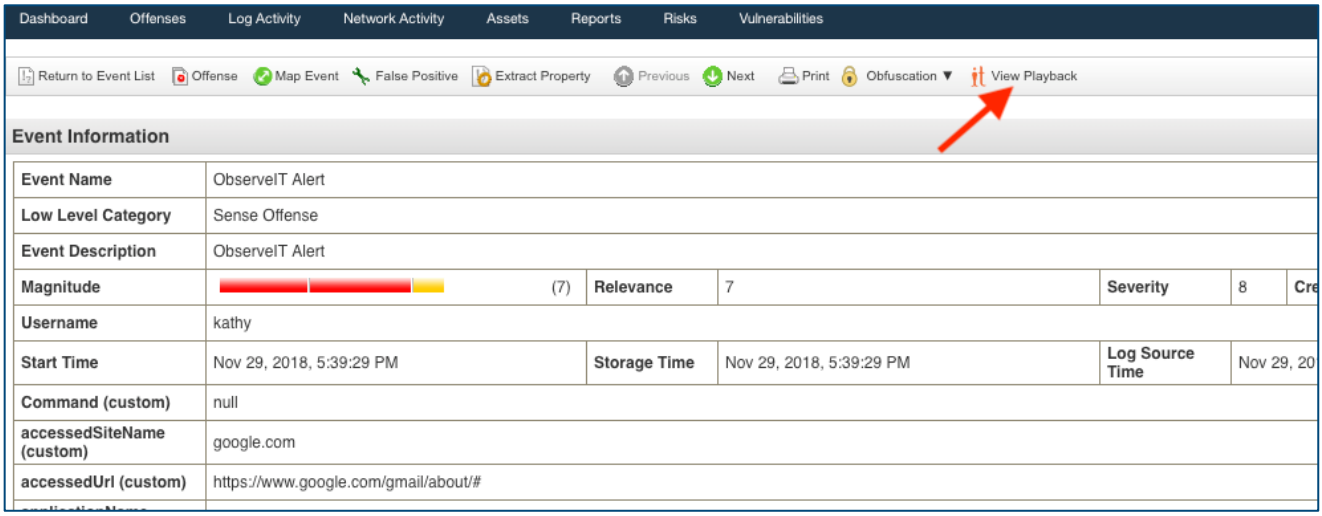
VIEWING EVENTS

You view events logged as soon as ObserveIT data collection is configured and enabled.

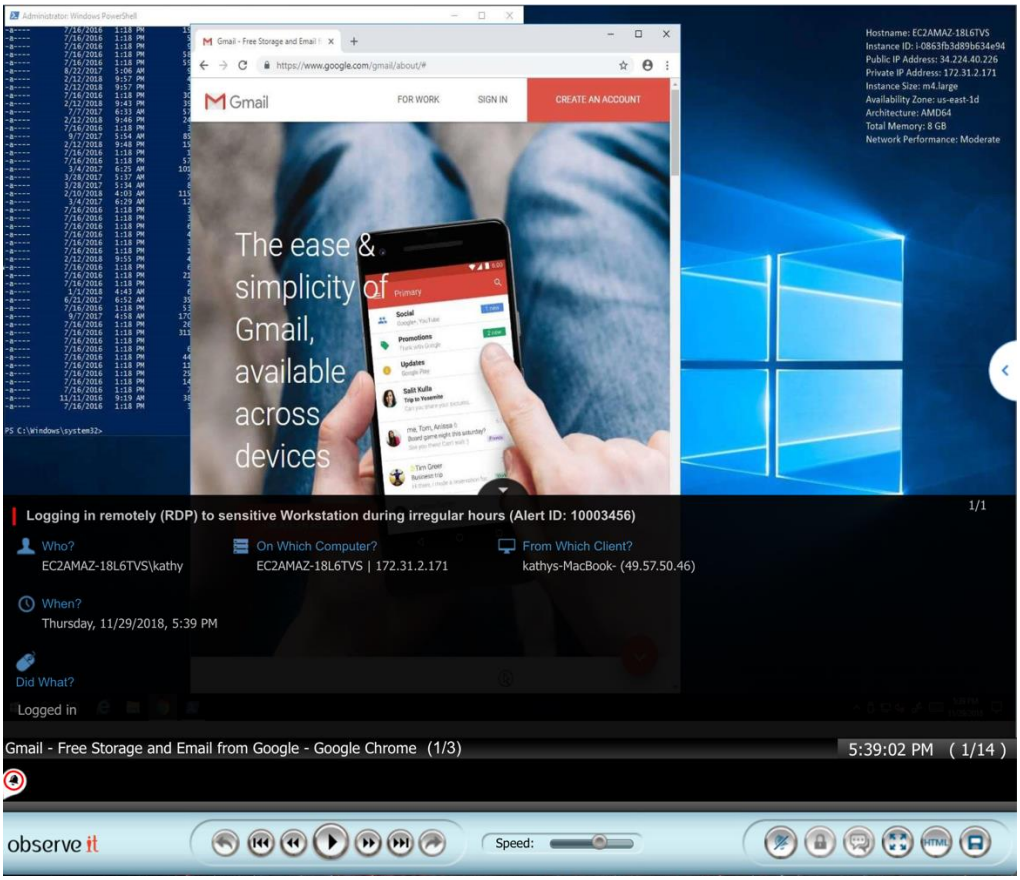
In the **Log Activity** screen, you see events coming in from the **ObserveIT Log Source Group**. All fields in the events are parsed into custom event properties.



From the **Event Details** screen for either User Activity or Alert events, you can click the **View Playback** button to go directly to the player in ObserveIT.



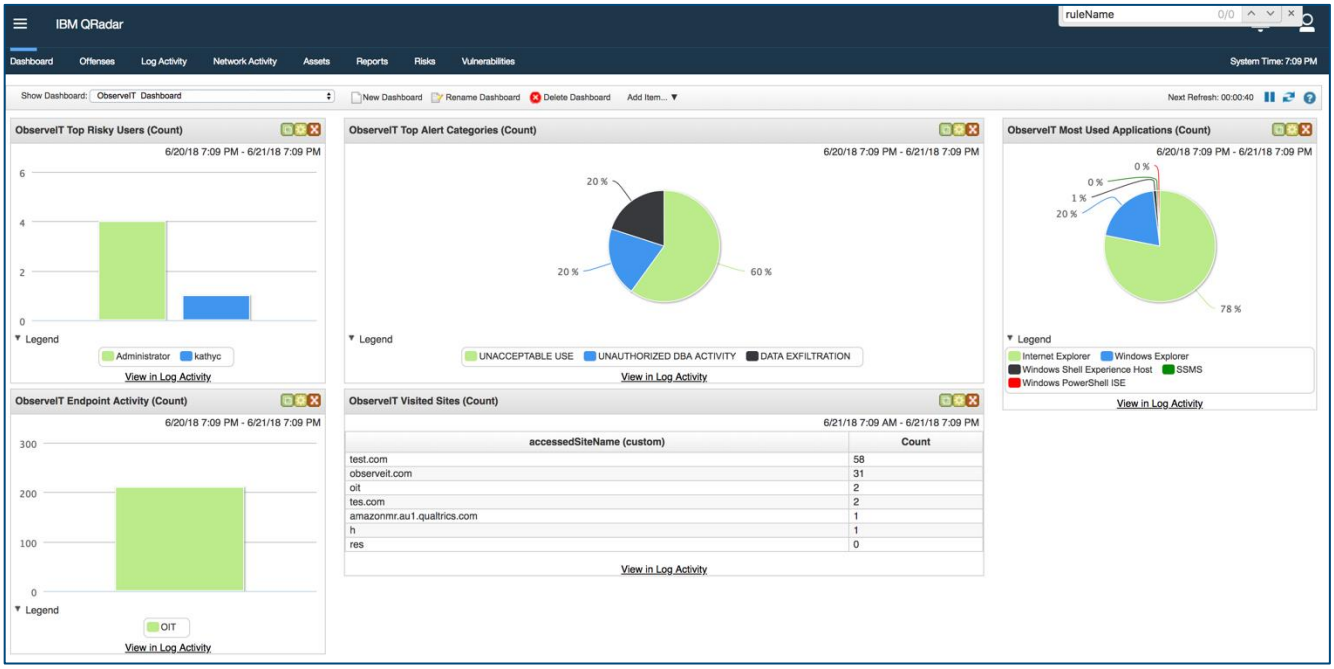
Example of player:


Hostname: EC2AMAZ-18L6TVS
Instance ID: i-0863fb3d89b634e94
Public IP Address: 34.224.40.226
Private IP Address: 172.31.2.171
Instance Size: m4.large
Availability Zone: us-east-1d
Architecture: AMD64
Total Memory: 8 GB
Network Performance: Moderate
Gmail
FOR WORK
SIGN IN
CREATE AN ACCOUNT
The ease & simplicity of Gmail, available across devices
1/1
Logging in remotely (RDP) to sensitive Workstation during irregular hours (Alert ID: 10003456)
Who?
EC2AMAZ-18L6TVS\kathy
On Which Computer?
EC2AMAZ-18L6TVS | 172.31.2.171
From Which Client?
kathys-MacBook- (49.57.50.46)
When?
Thursday, 11/29/2018, 5:39 PM
Did What?
Logged in
Gmail - Free Storage and Email from Google - Google Chrome (1/3)
5:39:02 PM (1/14)
observe it
Speed:

observe IT
a proofpoint company

DASHBOARD

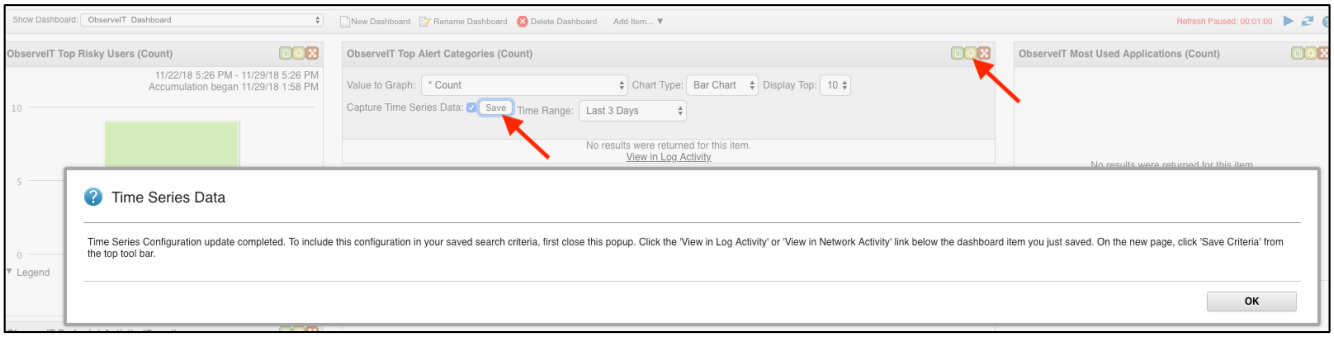
You can use the QRadar dashboard to review the ObserveIT data.



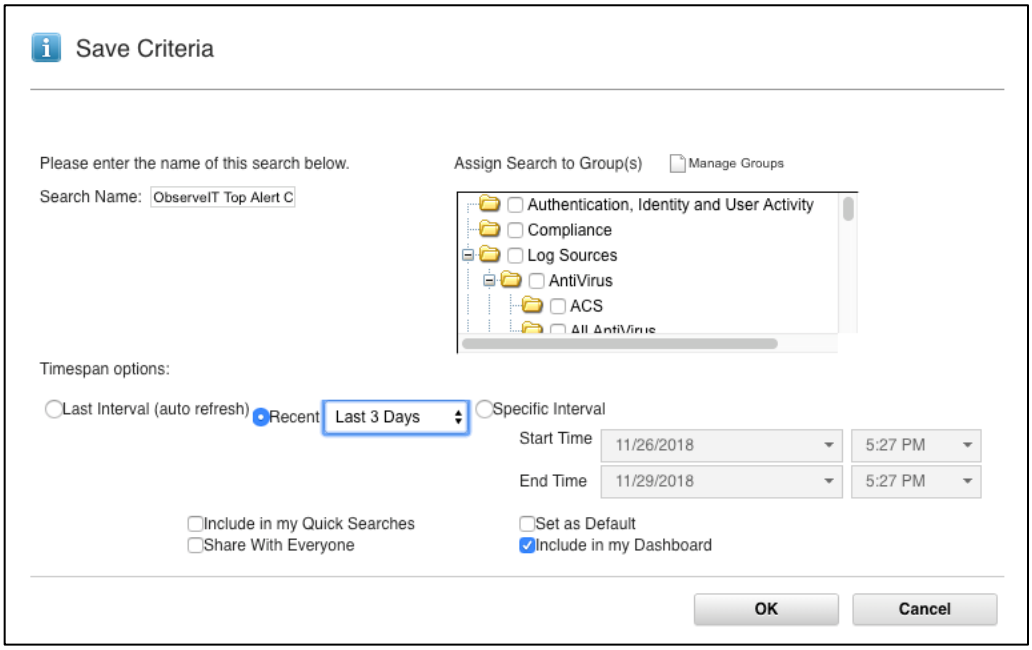
CONFIGURING THE DASHBOARD

To enable the dashboard, you need to configure the **Saved Searches**.

For each dashboard item, click on the **Settings** button, then check **Capture Time Series Data** and click **Save**.



From the prompt, click **View in Log Activity** link and the **Save Criteria** dialog box displays.



In the **Timespan** options, select **Recent** and click **OK**.

Support

For help using the ObserveIT platform or the ObserveIT App for IBM QRadar, please contact the ObserveIT support organization.
https://www.observeit.com/support/
You can also send an email to integrations@observeit.com with questions about this and other ObserveIT integrations.

Not a customer yet? Start your Free Trial of ObserveIT today!

Free Trial

Start your free trial with ObserveIT today. Detect and prevent insider threats in minutes. Reduce your risk, speed up investigations, and streamline compliance.

observe IT
a proofpoint company

Release notes

Version	Date	Notes

2.0.0	2018-11-29	• New:
		  ○ Example Dashboard and Rules
		• Improved:
		  ○ Use new V2 REST API to retrieve events

	2019-05-15	• New: ○ QRoC supported