

IBM QRadar Integration Guide

Table of Contents

OVERVIEW	3
FEATURES	3
PREREQUISITES	4
DELPOYMENT ARCHITECTURE	4
APP CONTENTS.....	4
CONFIGURATION	6
CREATING APPLICATION IN OBSERVEIT	6
CONFIGURING OBSERVEIT APP FOR QRADAR	8
USAGE	11
APPLICATION TUNING	11
VIEWING EVENTS	11
DASHBOARD.....	14
CONFIGURING THE DASHBOARD	14
SUPPORT	15
RELEASE NOTES	16

Overview

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

FEATURES

The ObserveIT App for IBM QRadar does the following:

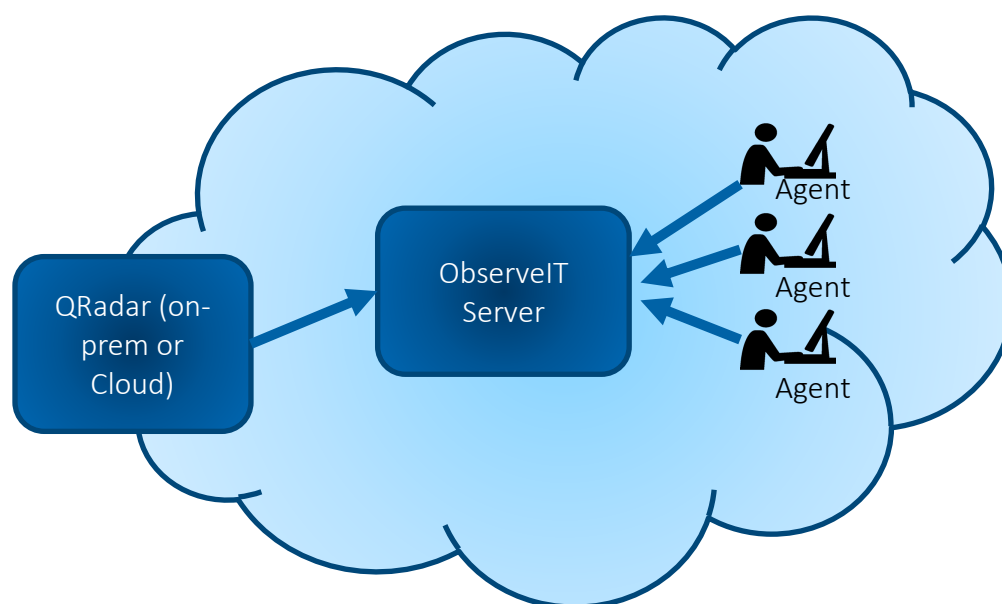
- **Event Collection:** Functions as a custom protocol to connect QRadar to the ObserveIT RESTful API and continuously pull the latest events. ObserveIT App pulls data from ObserveIT into QRadar as follows:
 - Subscribes to User Interface Activity, User Command Activity, and Alert events
 - Polls events 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 7.6.2)
- IBM QRadar (Minimum supported version 7.3.1)

DELPOYMENT ARCHITECTURE

The diagram shows how ObserveIT integrates into IBM QRadar.



APP CONTENTS

The ObserveIT App for QRadar includes the following contents.

- 1 Dashboard with 5 associated searches
 - ObserveIT Dashboard
 - ObserveIT Top Alert Categories
 - ObserveIT Endpoint Activity
 - ObserveIT Visited Sites
 - ObserveIT Top Risky Users
 - ObserveIT Most Used Applications
- 1 Custom Application

- 5 Custom Rules
- 3 Syslog Log Sources
 - ObserveIT_Alert_V2
 - ObserveIT_UserCommandActivity_V2
 - ObserveIT_UserInterfaceActivity_V2
- 2 Log Source Types
 - ObserveIT Alerts
 - ObserveIT User Activities
- 33 Custom Properties
 - Observeit Severity
 - Rule Category Name
 - Secondary Login Name
 - Domain Name
 - Session Url
 - Observed At
 - Collector ID
 - Secondary Domain Name
 - Command Params
 - Process Executable
 - Endpoint ID
 - Accessed Site Name
 - Endpoint Name
 - ID
 - Remote Address
 - Remote Hostname
 - Timezone Offset
 - Login Name
 - Accessed Url
 - Collector Url
 - Created At
 - Rising Value
 - Playback Url
 - ObserveIT Application Name
 - SQL User Name
 - User Activity Observed At
 - User Activity Event ID
 - Event Playback Url
 - Details
 - Details Url
 - SQL Command
 - Rule Description
 - ObserveIT Rule Name


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.

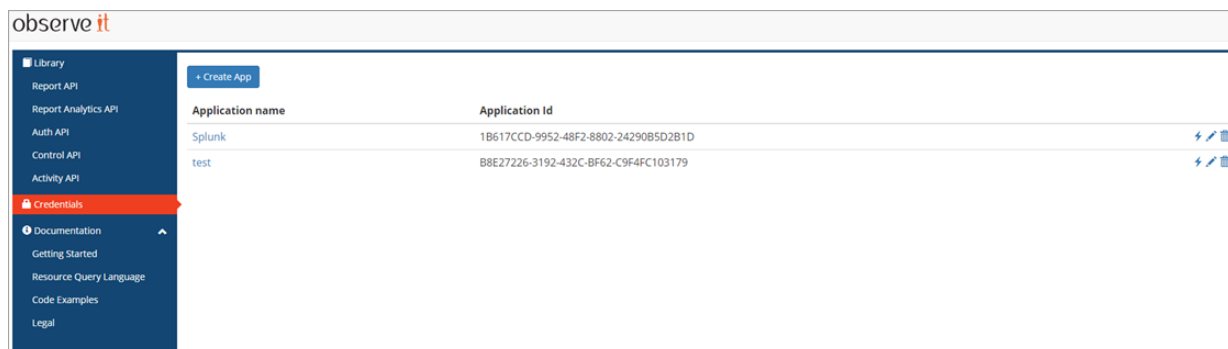
1. From the ObserveIT Web Console, click the  in the upper-right corner and select **Developer Portal** from the menu.

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.

Create Application [X]

Application Name
qradar

Allowed Scopes separate by space for multiple scopes, example it:report:*
*

Allowed Grants

- Client Credentials
- Password
- Authorization Code
- Refresh Token
- Implicit

Redirect URIs used for authorization_code and token(implicit) flows

Redirect URI

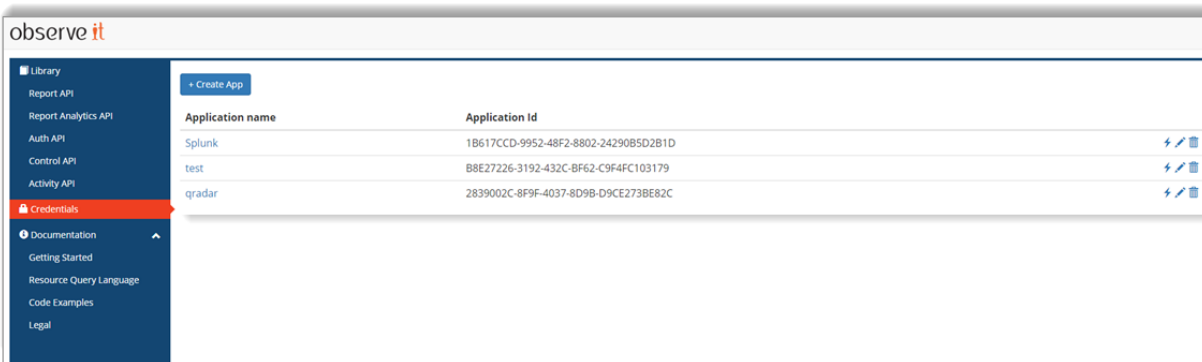
Redirect URI

Redirect URI

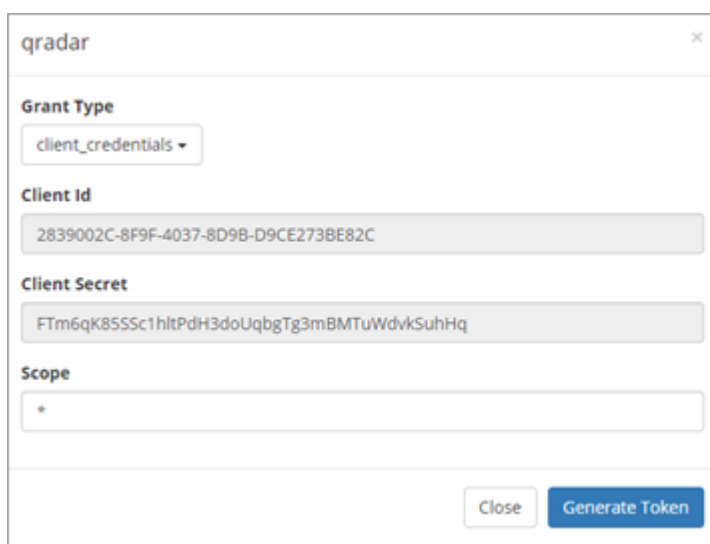
Cancel Save

3. Do the following:

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



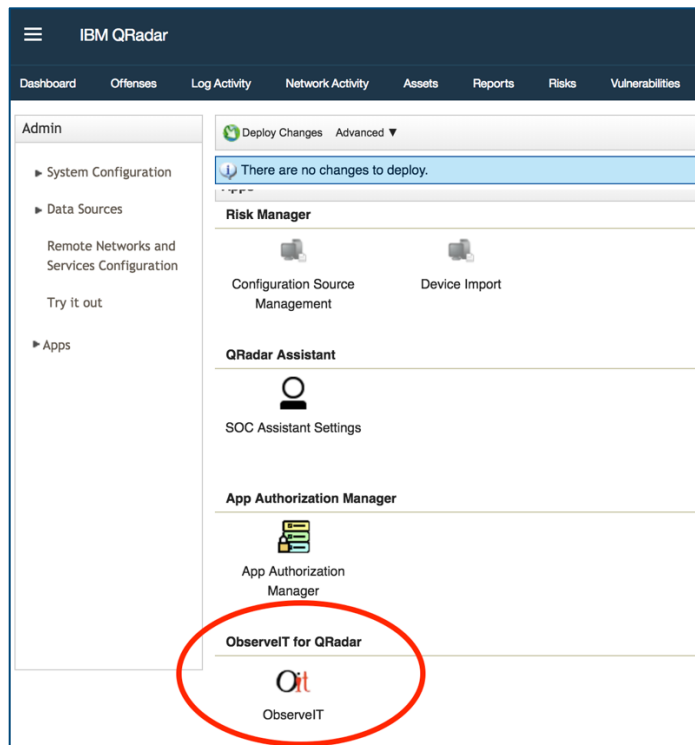
Note the **Client Id** and **Client Secret** values. You will enter them into the configuration screen of the QRadar add-on. (See: [Configuring ObserveIT App for QRadar.](#))

CONFIGURING OBSERVEIT APP FOR QRADAR

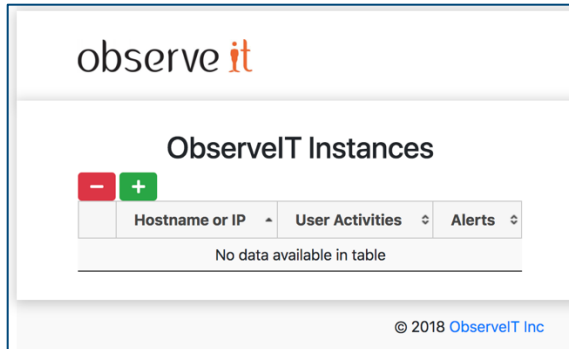
This procedure describes the registration process in QRadar.

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.

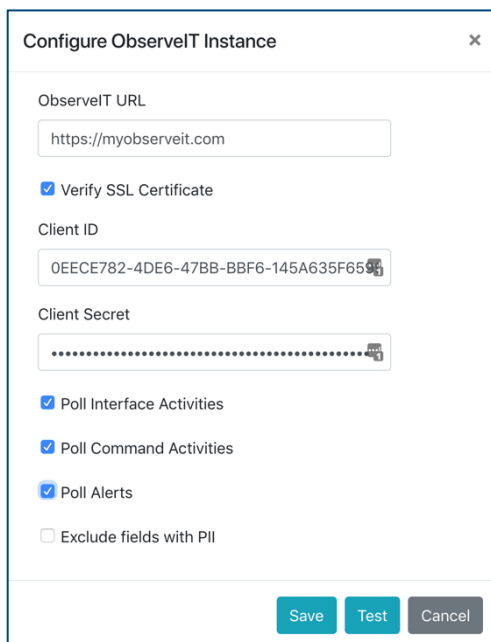
1. Open the QRadar Admin screen and scroll down to the bottom. Click the **ObserveIT** icon.



The list of ObserveIT instances displays.



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



3. Complete the **Configure ObservelT Instance** dialog box.
 - a) Enter the **Client ID** and **Client Secret** values that you copied previously. (See: Creating Application in ObservelT.)
 - b) **Verify SSL Certificate**: If your ObservelT 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 ObservelT.

Usage

APPLICATION TUNING

ObservelT 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 ObservelT data collection is configured and enabled.

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

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities System Time: 5:40 PM

Search... Quick Searches Add Filter Save Criteria Save Results Cancel False Positive Rules Actions

Quick Filter Search

Viewing real time events View: Select An Option: Display: Default (Normalized)

Current Filters:
Log Source Group is ObserveIT (Clear Filter)

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination
ObserveIT User Activity	ObserveIT_UserInterfaceActivity...	1	Nov 29, 2018, 5:38:48 PM	User Behavior	[Redacted]	0	[Redacted]
ObserveIT User Activity	ObserveIT_UserInterfaceActivity...	1	Nov 29, 2018, 5:38:48 PM	User Behavior	[Redacted]	0	[Redacted]
ObserveIT User Activity	ObserveIT_UserInterfaceActivity...	1	Nov 29, 2018, 5:38:48 PM	User Behavior	[Redacted]	0	[Redacted]
ObserveIT Alert	ObserveIT_Alert_V2	1	Nov 29, 2018, 5:38:29 PM	Sense Offense	[Redacted]	0	[Redacted]
ObserveIT Alert	ObserveIT_Alert_V2	1	Nov 29, 2018, 5:38:29 PM	Sense Offense	[Redacted]	0	[Redacted]

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.

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities

Return to Event List Offense Map Event False Positive Extract Property Previous Next Print Obfuscation View Playback

Event Information

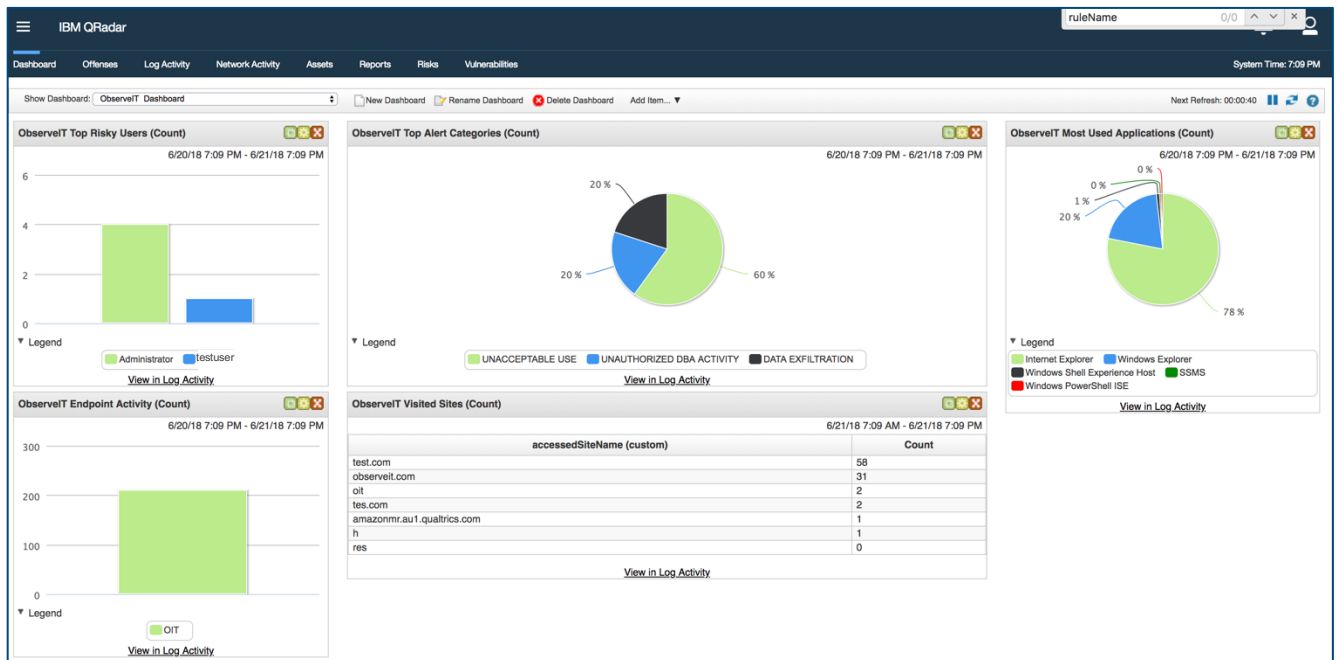
Event Name	ObserveIT Alert						
Low Level Category	Sense Offense						
Event Description	ObserveIT Alert						
Magnitude	[Progress Bar]		(7)	Relevance	7	Severity	8
Username	testuser						
Start Time	Nov 29, 2018, 5:39:29 PM		Storage Time	Nov 29, 2018, 5:39:29 PM		Log Source Time	Nov 29, 2018, 5:39:29 PM
Command (custom)	null						
accessedSiteName (custom)	google.com						
accessedUrl (custom)	https://www.google.com/gmail/about/#						

Example of player:

The screenshot displays a remote desktop session of a Windows workstation. On the left, a Windows PowerShell terminal window shows a list of system events with timestamps ranging from 7/16/2016 to 11/21/2018. The main desktop area features a Google Chrome browser window displaying the Gmail 'About' page. The page content includes the text: "The ease & simplicity of Gmail, available across devices" and a mobile phone displaying the Gmail interface. To the right of the browser window, a system information panel lists details such as Hostname, Instance ID, Public IP Address (172.31.2.171), Private IP Address, Instance Size (m4.large), Availability Zone (us-east-1d), Architecture (AMD64), Total Memory (8 GB), and Network Performance (Moderate). Below the desktop content, a notification bar reads: "Logging in remotely (RDP) to sensitive Workstation during irregular hours (Alert ID: 10003456)". Below this, a metadata section provides details: "Who?" (redacted), "On Which Computer?" (172.31.2.171), "From Which Client?" (-MacBook- (49.57.50.46)), "When?" (Thursday, 11/29/2018, 5:39 PM), and "Did What?" (Logged in). At the bottom of the screen, a taskbar shows the "observe it" logo, navigation controls, and a "Speed:" slider.

DASHBOARD

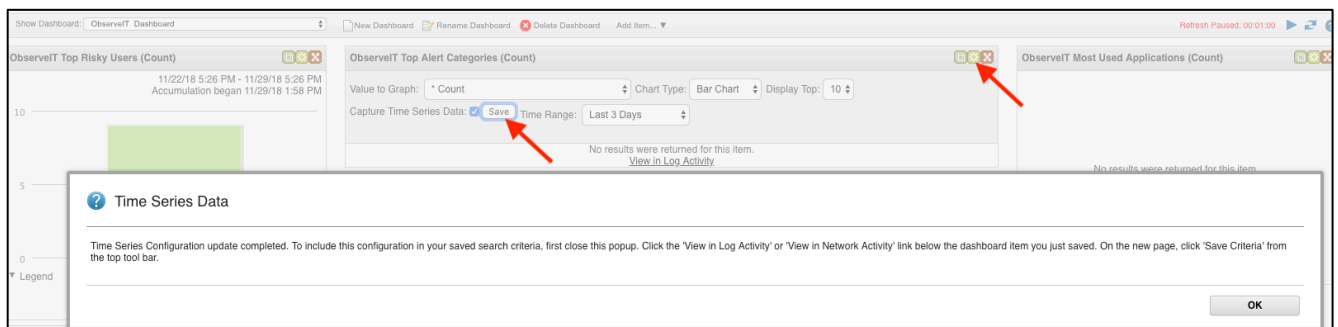
You can use the QRadar dashboard to review the ObserveIT data.



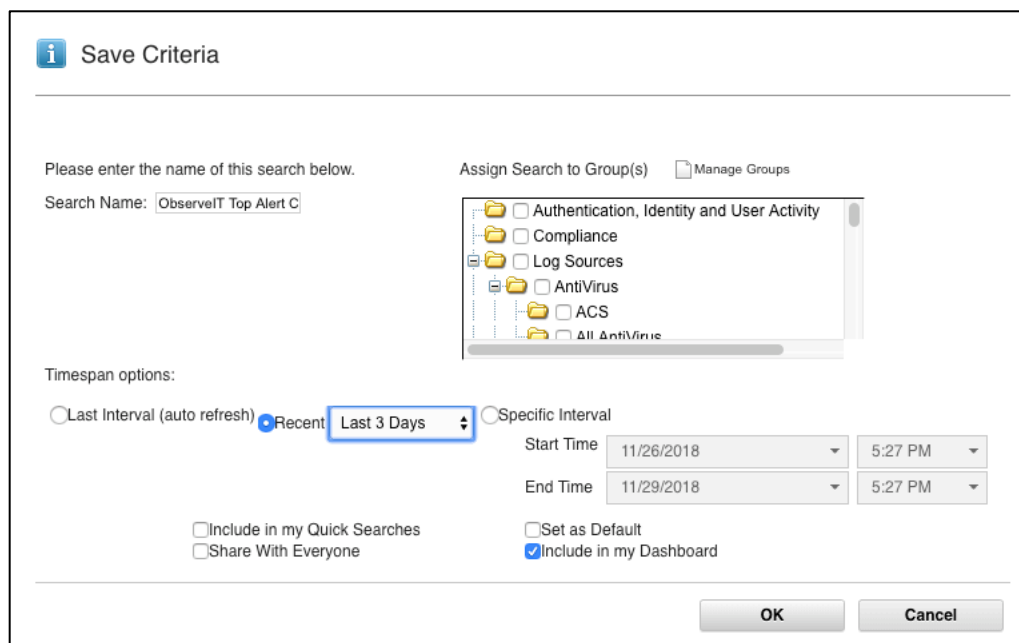
CONFIGURING THE DASHBOARD

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.

Release notes

Version	Date	Notes
2.0.0	2018-11-29	<ul style="list-style-type: none">• New:<ul style="list-style-type: none">○ Example Dashboard and Rules• Fixed:• Improved:<ul style="list-style-type: none">○ Use new V2 REST API to retrieve events