SecurityScorecard App for QRadar v7.4.1 FP2+

App Specification Guide

Table of Contents

App functionality

Data Collection

QRadar admin/user can collect the information regarding Overall score, Factors, and Issues for the company from SecurityScorecard and ingest into QRadar as events by configuring the inputs from the SecurityScorecard tab.

QRadar console

Qradar admin/user can visualize the SecurityScorecard data on the QRadar console.

App Installation & Configuration

Prerequisites

Below is a list of requirements needed to run the app (v2.0.0) on QRadar:

- SecurityScorecard App For QRadar - QRadar 7.4.1 FP2+ (v2.0.0)
- QRadar version: 7.4.1 Fix Pack 2+

Upgrade

v.2.0.0

- *NOTE:* Users will be able to upgrade from v1.0.1 to v2.0.0 only if the app is installed on QRadar v7.4.1 FP2+ (app framework V2).
- Follow the same steps for Installation
- After installation, data collection will be stopped. To start it, users have to go to the configuration page and click on Process button.
- Clear the browser cache and refresh the QRadar page.

Installation

The application installation requires access to the QRadar console machine via a web interface. The web interface can be accessed via https://<<QRadarconsoleIP>>/. The installation process is as follows:

a. Login to QRadar console.

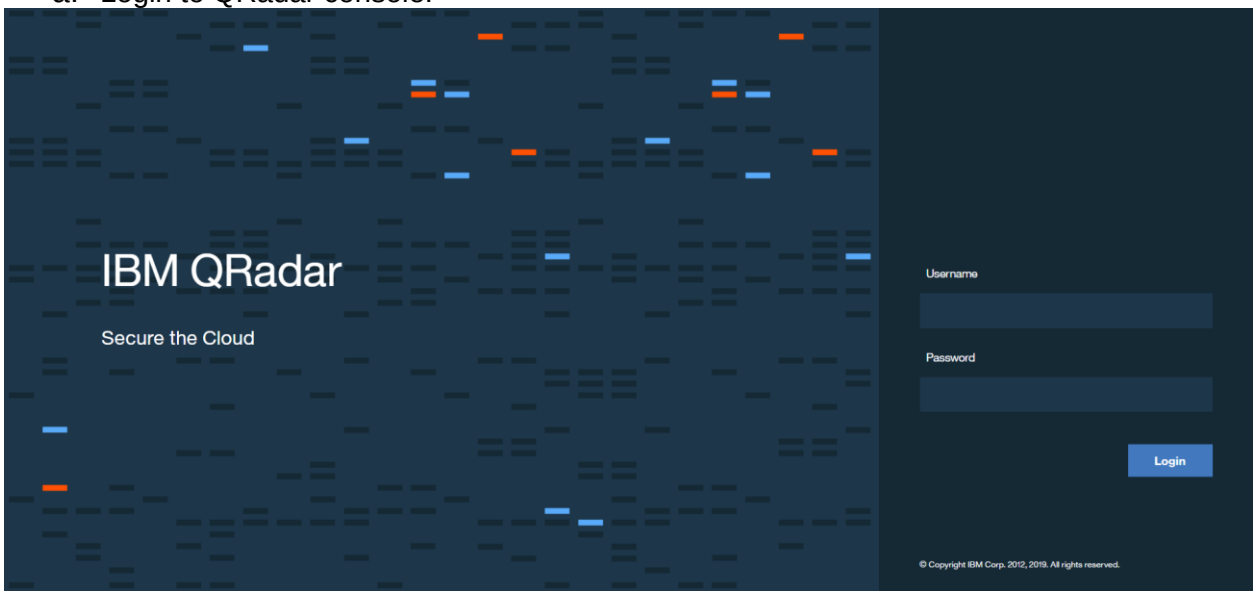


Figure 1: IBM QRadar login screen

b. Go to Admin → Extension Management.
c. Click on Add button then choose the downloaded zip file by clicking on **Browse** and then, click **Add**.

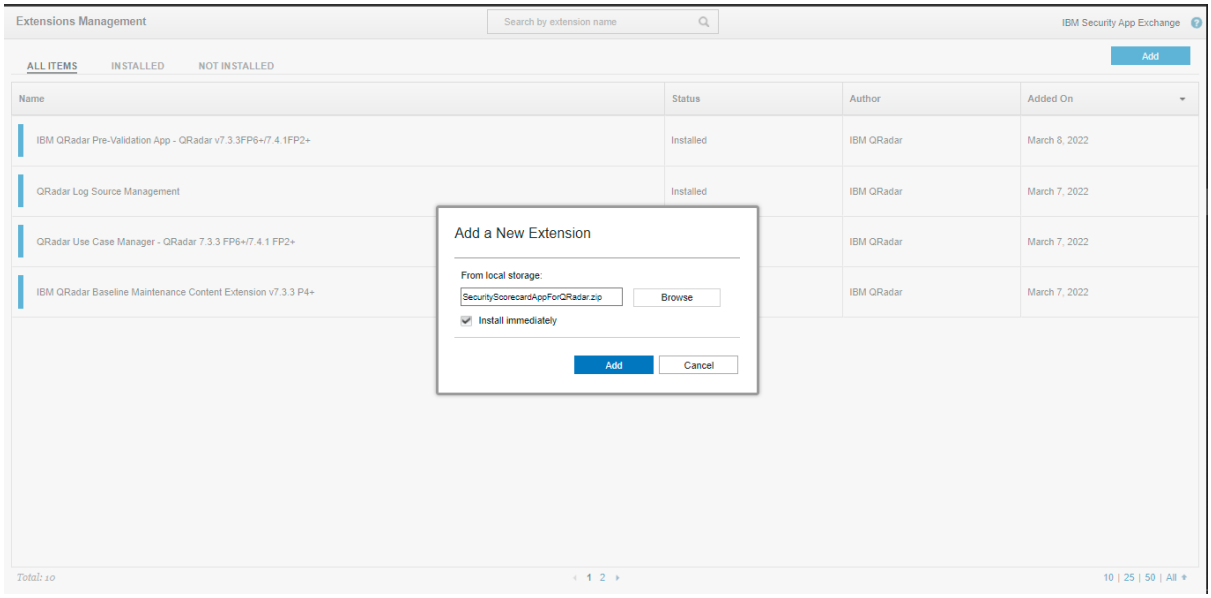


Figure 2: Add SecurityScorecard App For QRadar extension

d. QRadar will prompt a list of changes being made by the app. Click on the install button and do not uncheck the “Start a default instance of each app”.

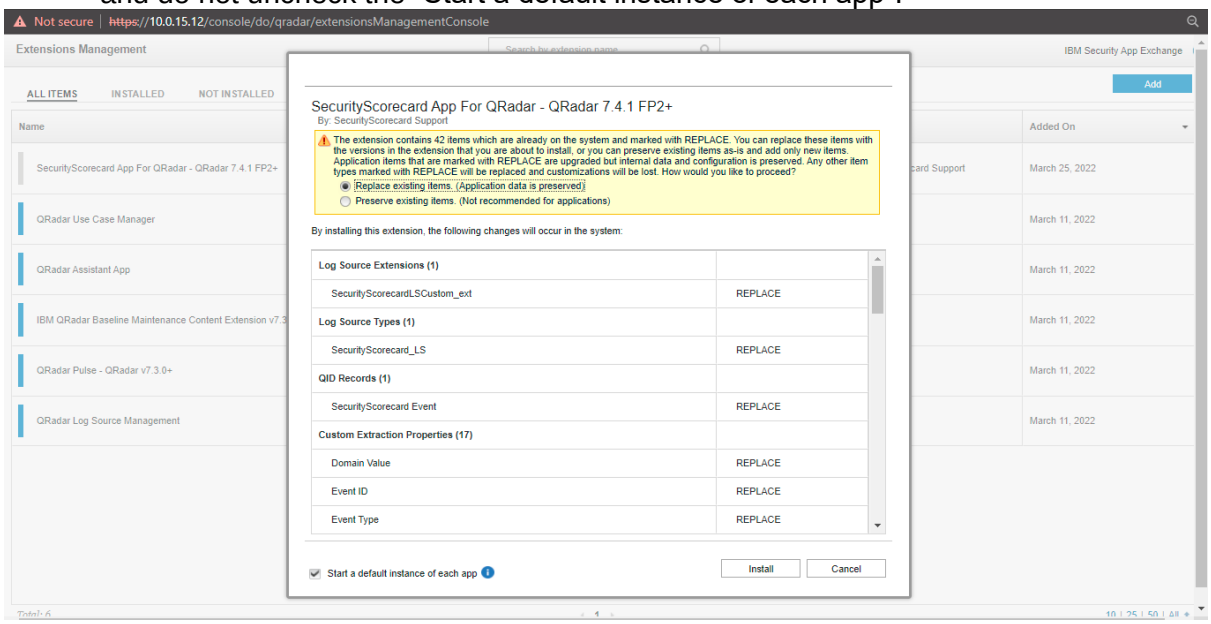


Figure 3: Install SecurityScorecard App For QRadar

e. Thereafter, it will show a window that the App is installed successfully along with lists of different components of the App.
f. Clear cache and refresh the browser window.
g. Navigate to Extensions Management via the Admin panel. After successful installation, it will show “Installed” status against “SecurityScorecard App For QRadar - QRadar 7.4.1 FP2+”.

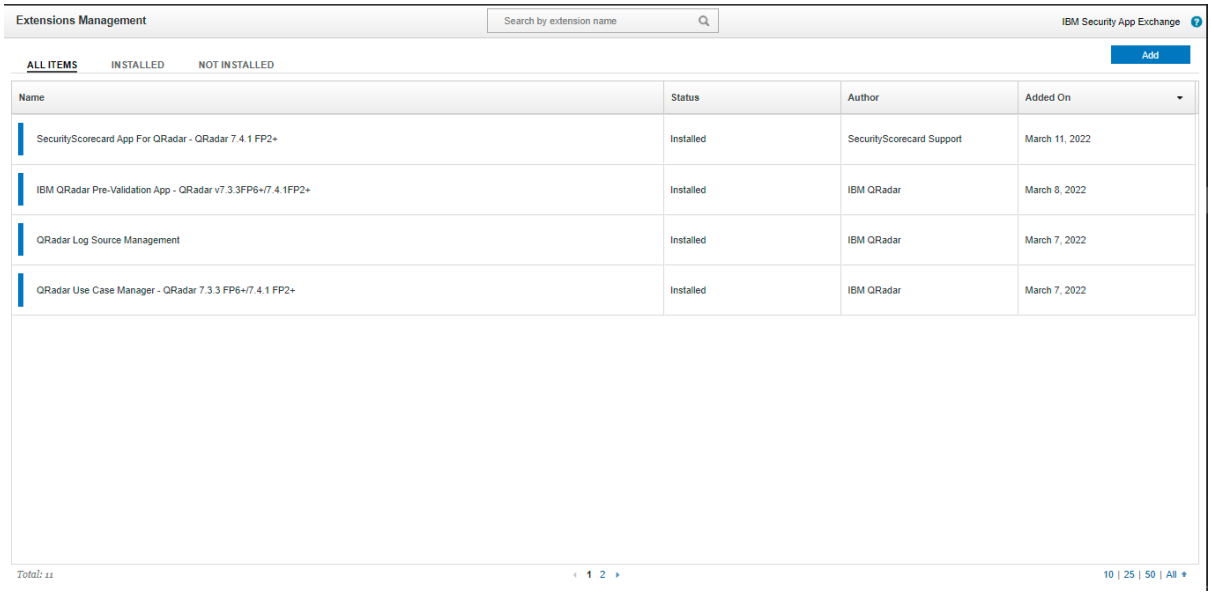


Figure 4: Installation successful

App Configuration

After completing the installation, users must have to save the configuration to use app functionality.

The setup process for configuring the app is as follows:

- Go to the SecurityScorecard tab.

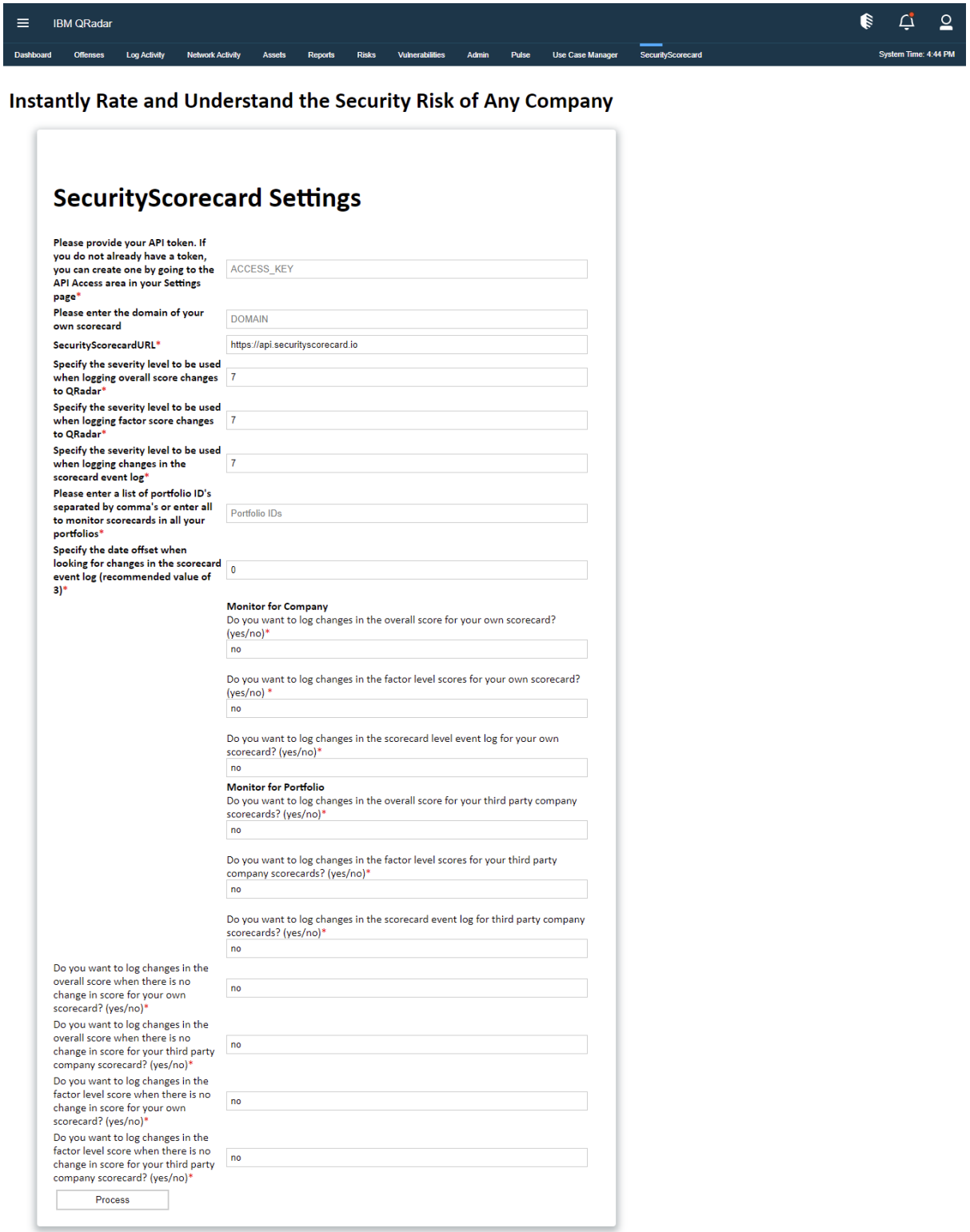


Figure 5: Config page

- Config page would have fields as below:

Data Input fields	Description	Mandatory	Default Value
Please provide your API token. If you do not already have a token, you can create one by going to the API Access area in your Settings page	API Key to access the endpoint of SecurityScorecard.	Yes	No value set as default. Need to give during adding inputs.
Please enter the domain of your own scorecard	This field takes domain names.	No	No Default value
SecurityScorecardURL	This field takes a SecurityScorecard URL. Ex. https://api.securityscorecard.io	Yes	https://api.securityscorecard.io
Please enter a list of portfolio IDs separated by commas or enter all to monitor scorecards in all your portfolios	It takes portfolio Ids. For all we need to give as “All” or for specific portfolios we need to give a comma separated portfolio Ids. Ex. “portfolioId1,portfolioId2, portfolioId3”.	Yes	No Default value
Specify the severity level to be used when logging factor score changes to QRadar	It sets the severity level of the factor. It should be valued between 1 to 10. Ex. 8.	Yes	7
Specify the severity level to be used when logging overall score changes to QRadar	It sets the severity level of Overall. It should be valued between 1 to 10. Ex. 8.	Yes	7
Specify the severity level to be used when logging changes in the scorecard event log	It sets the severity level of a new issue. It should be valued between 1 to 10. Ex. 8.	Yes	7
Specify the date offset when looking for changes in the scorecard event log	This takes the integer value of days, like how many days before the current date data you want to	Yes	0

(recommended value of 3)	get. Ex. 4. So the date will be set like 4 days before the current date.		
Do you want to log changes in the overall score for your own scorecard? (yes/no)	In this field, We need to give yes/no value to get data for the overall score for self or not.	Yes	no
Do you want to log changes in the overall score for your third-party company scorecards? (yes/no)	In this field, We need to give yes/no value to get data for an overall score for portfolios or not.	Yes	no
Do you want to log changes in the factor level scores for your own scorecard? (yes/no)	In this field, We need to give yes/no value according to get data for factor level score for self or not.	Yes	no
Do you want to log changes in the factor level scores for your third party company scorecards? (yes/no)	In this field, We need to give yes/no value to get data for factor level scores for portfolios or not.	Yes	no
Do you want to log changes in the scorecard level event log for your own scorecard? (yes/no)	In this field, We need to give yes/no value according to whether or not we get data for the issue-level score for self or not.	Yes	no
Do you want to log changes in the scorecard event log for third-party company scorecards? (yes/no)	In this field, We need to give yes/no value to get data for issue level scores for portfolios or not.	Yes	no
Do you want to log changes in the overall score when there is no change in score for your own scorecard? (yes/no)	In this field, We need to give yes/no value if you want to log changes in the overall score when there is no change in score for your own scorecard	Yes	no
Do you want to log changes in the overall score when	In this field, We need to give yes/no value if you want to log	Yes	no

there is no change in score for your third party company scorecard? (yes/no)	changes in the overall score when there is no change in score for your third party company scorecard		
Do you want to log changes in the factor level score when there is no change in score for your own scorecard? (yes/no)	In this field, We need to give yes/no value if you want to log changes in the factor level score when there is no change in score for your own scorecard	Yes	no
Do you want to log changes in the factor level score when there is no change in score for your third party company scorecard? (yes/no)	In this field, We need to give yes/no value if you want to log changes in the factor level score when there is no change in score for your third-party company scorecard.	Yes	no

- After successful configuration of the configuration page, the background process will start fetching data from the SecurityScorecard and will ingest in the Log activity.

Uninstalling the Application

To uninstall the application, the user needs to perform the following steps.

1. Go to the Admin Page.
2. Open Extension Management.
3. Select SecurityScorecard App For QRadar - QRadar 7.4.1 FP2+ application.
4. Click on Uninstall.

NOTE:

- On uninstalling the app, all the Custom Event Properties, and configuration page will be removed.
- On uninstalling the app, only the log sources which are provided in the bundle will get uninstalled (i.e. SECURITYSCORECARD Log Source).
- On uninstalling the app, removal of Log source type, Log source extension, DSM event mappings (including QIDs) is not supported by QRadar yet.
- To remove SecurityScorecard App for QRadar's event mappings, navigate to Admin -> DSM Editor -> Select the "SecurityScorecard_LS" log source type and click the "Select" button -> "Event Mappings" tab -> Select each event mapping and click the delete icon.
- To remove SecurityScorecard App for QRadar's log source type, navigate to Admin -> DSM Editor -> Select the log source type to be deleted in the pop-up menu in this case "SecurityScorecard_LS", and click on the delete icon.

Steps to check application logs

Users can go inside the application docker container. In the docker container user can see logs.

- Follow steps for accessing the docker container of the SecurityScorecard App. "Access application docker"
- cd /opt/app-root/store/log (For navigating to log directory)
- ls (For getting list of all logs files)

File	Description
app.log	Contains logs of the configuration page and data collection

Access application docker

A user can go inside the application docker container. In the docker container, the user can see logs and configure some parameters.
Perform the below command on your QRadar instance via SSH.

- Run **/opt/qradar/support/recon ps**
- Above command will list all the applications installed in QRadar, then find the app with the name “SecurityScorecard App For QRadar” and copy the App-ID of that.
- Now run **/opt/qradar/support/recon connect App-ID***(That is copied in the above step)*

Now the user is in the docker container.

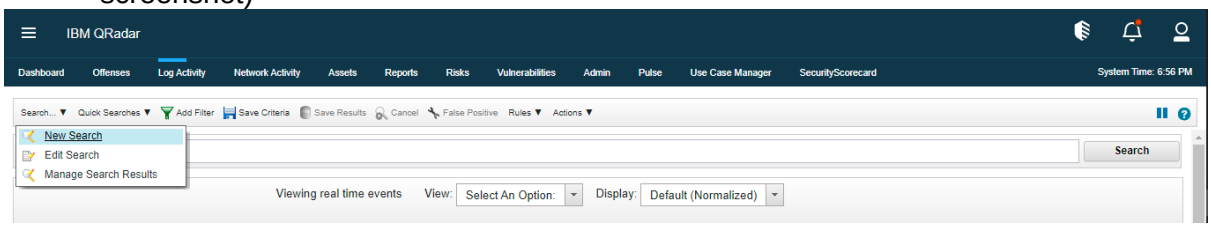
Dashboard

QRadar Dashboard/Console

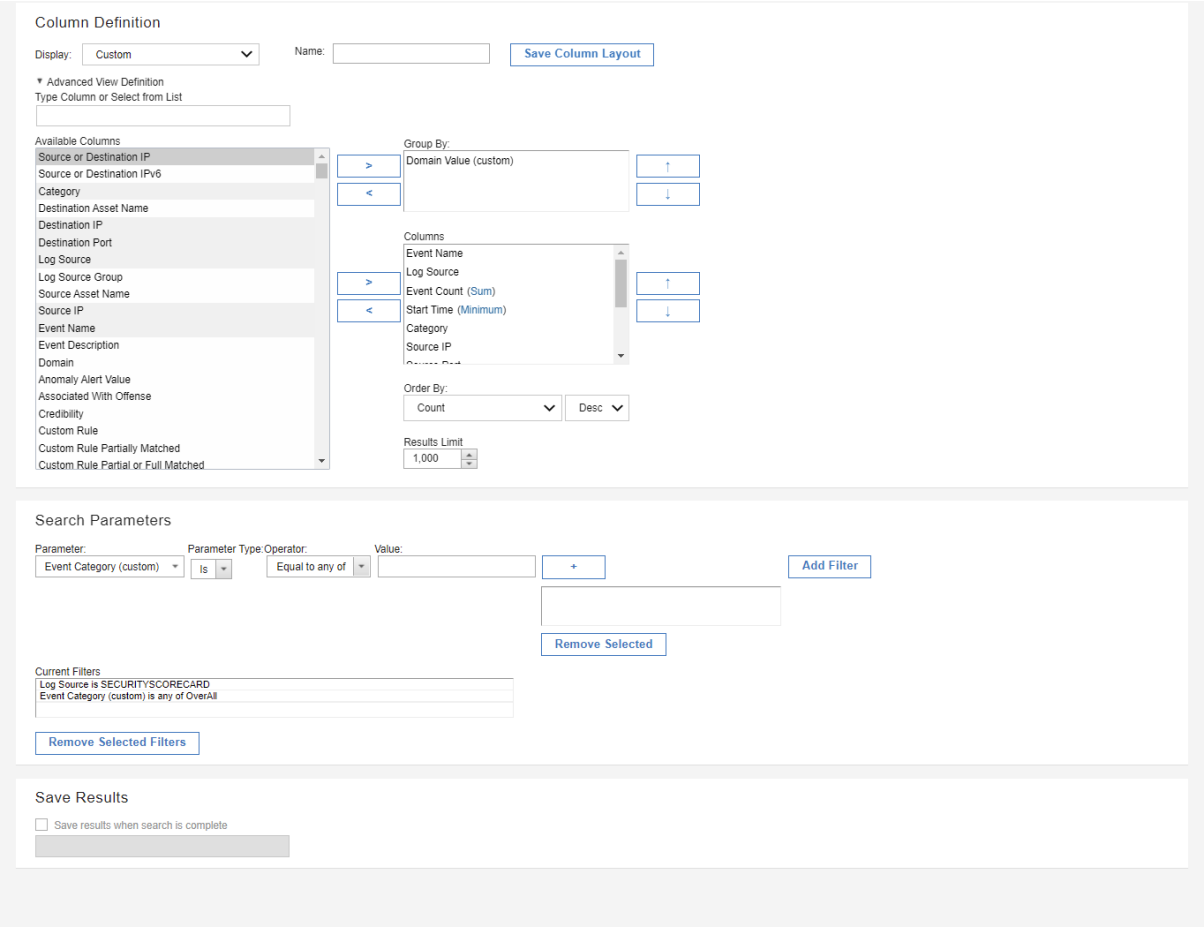
Users can view the events by creating different panels in the QRadar Dashboard.

To create a dashboard panel:

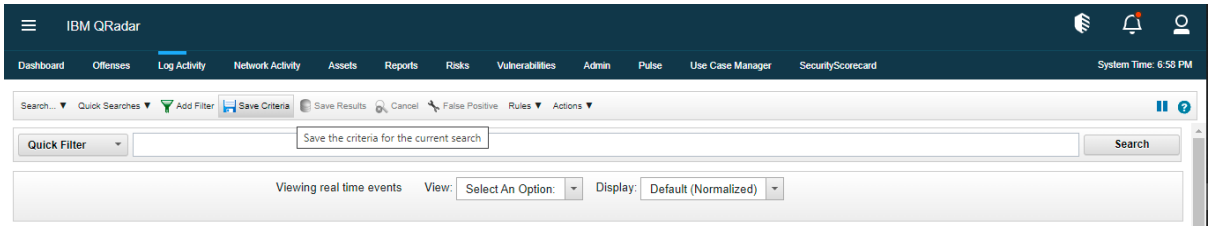
- Create a search by clicking on Log Activity -> Search -> New Search (Refer to below screenshot)



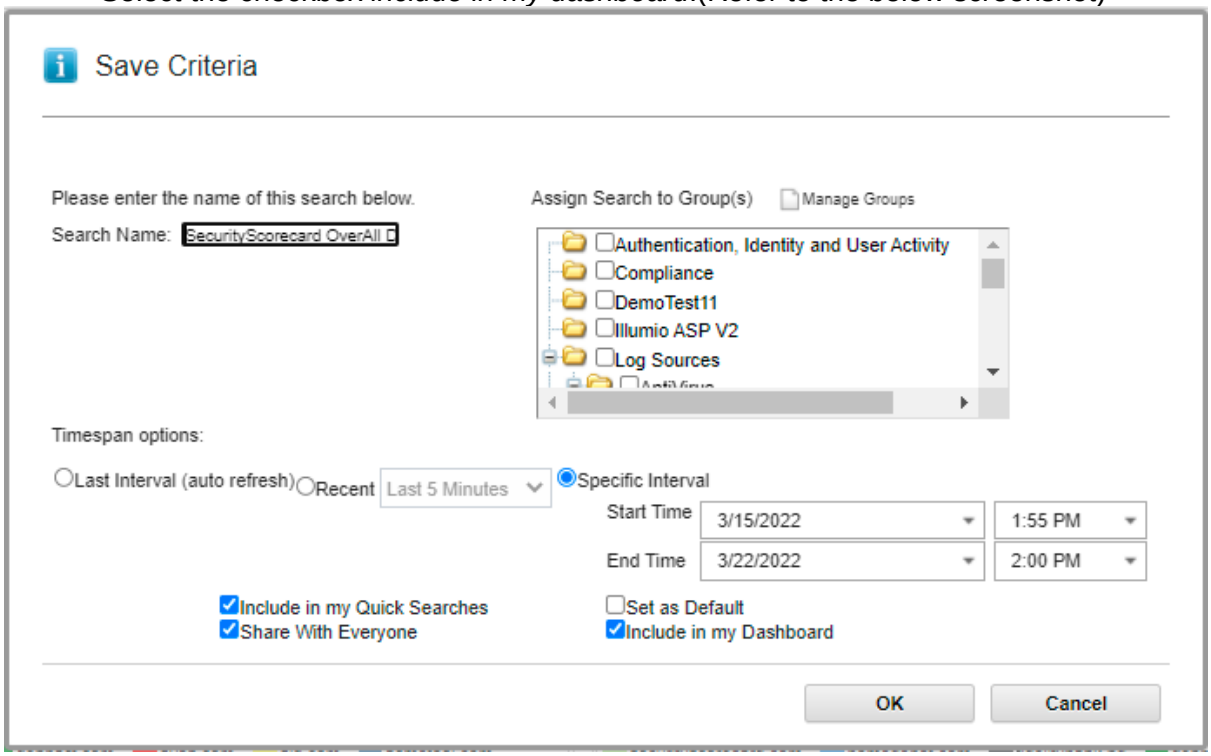
- Provide the log source as SECURITYSCORECARD and Event Category as one of the following values: OverAll, Factor, or Issue in the Search Parameter section.
- Apply Group By in any of the fields to visualize it in the dashboard, without applying group by, it won't be visible on the dashboard.(Refer to the below screenshot)



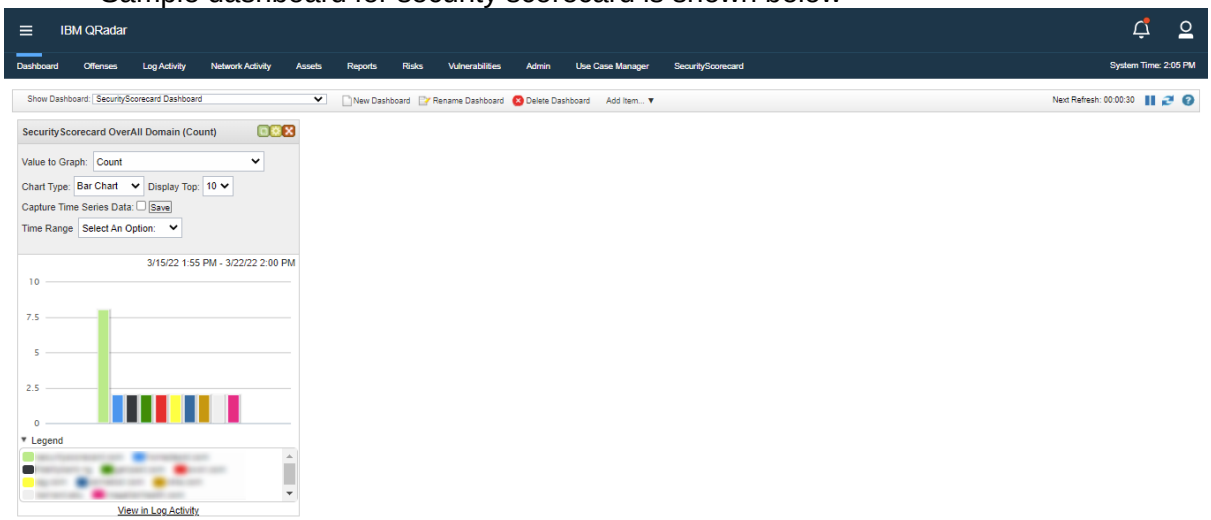
- After applying the search, click on the save criteria to save the search. (Refer to the below screenshot)



- Select the checkbox *include in my dashboard*.(Refer to the below screenshot)



- Go to the dashboard.
- Click on add items and select the name of the search that you saved from the list.
- Sample dashboard for security scorecard is shown below



Release notes

v2.0.0

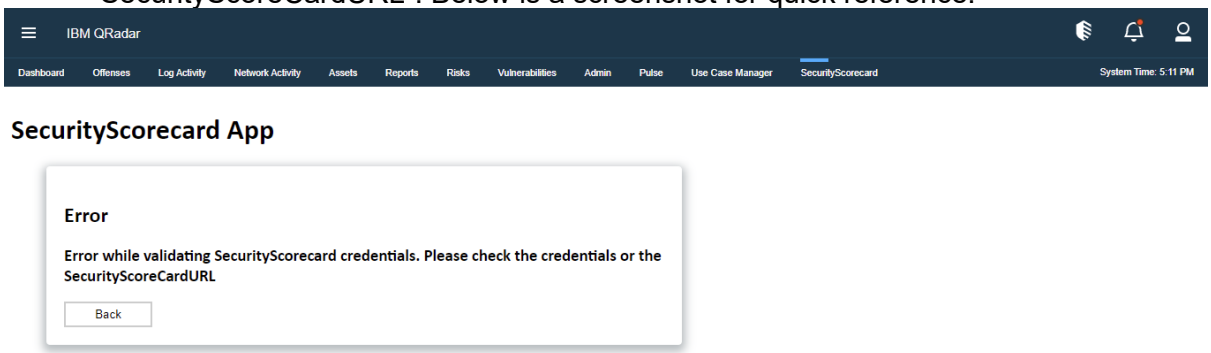
- Migrated from python2 to python3.
- Minor bug fix.

Troubleshooting

This section describes the common issues that might happen during the deployment or the running of the app and the steps to resolve the issues.

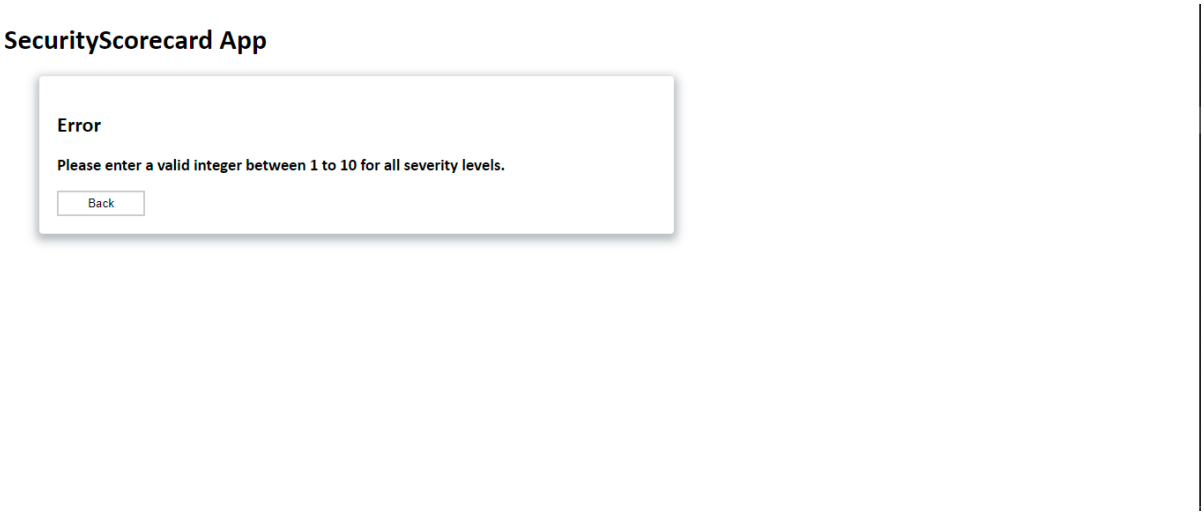
Case #1 – App configuration fails with various error messages

- **Problem:** New configuration fails with error message “Error while validating SecurityScorecard credentials. Please check the credentials or the SecurityScoreCardURL”. Below is a screenshot for quick reference.



Troubleshooting Steps: This happens when there is an issue with the validation of the access key, so authentication fails while saving the configuration. Users are recommended to provide a valid access token and valid SecurityScorecardURL. For checking logs “Steps to check logs”.

- **Problem:** New configuration fails with error message “Please enter a valid integer between 1 to 10 for all severity levels.”. Below is a screenshot for quick reference.



Troubleshooting Steps: This happens when a user has entered either non-integer values in any of the severity levels or has entered a value besides 1 to 10. Users are recommended to enter values between 1 to 10 in severity levels. For checking logs "Steps to check logs"

Case #2 – UI-related issues in the app

- **Problem:** Configuration page shows error or unintended behavior.

Troubleshooting Steps: Clear the browser cache and reload the webpage.

Case #3 – Error while initiating socket connection with IBM QRadar

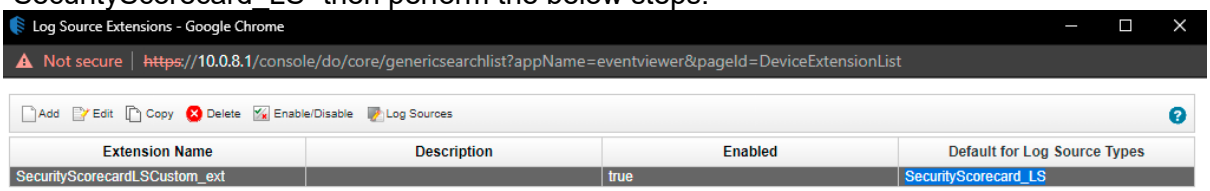
- **Problem:** "Error while initiating socket connection with IBM QRadar" observed in log files.

Troubleshooting Steps:
This issue might be observed in the QRadar v2 app framework (< v7.4.2 FP2). To resolve it, please refer to the following link: https://www.ibm.com/support/pages/node/6395080

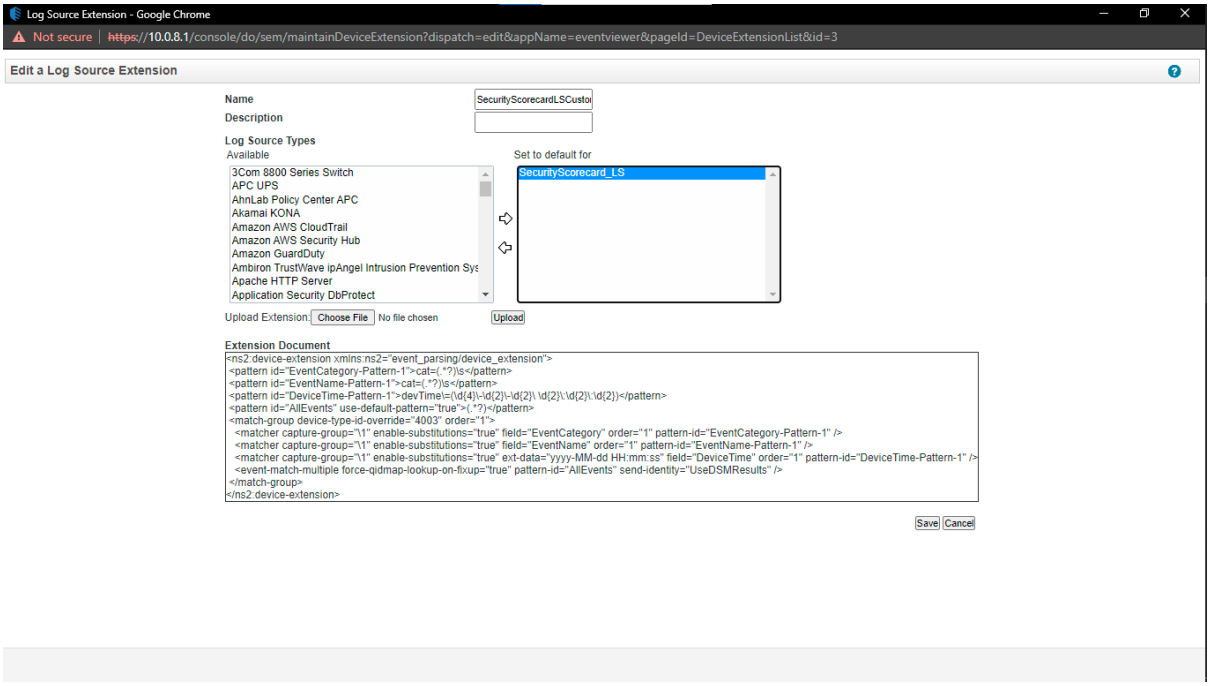
Case #4 – Events are parsed as Unknown or SecurityScorecard_LS Message

- **Problem:** SecurityScorecard events are parsed as "Unknown" or "SecurityScorecard_LS Message".

Troubleshooting Steps:
1. Go to the Log Source Extensions tab under the Admin section.
2. Confirm that "Default for Log Source Types" is "SecurityScorecard_LS". If it is not "SecurityScorecard_LS" then perform the below steps.



3. Click on SecurityScorecardLSCustom_ext which will download an XML file.
4. Log into QRadar console view SSH and execute the following command: /opt/qradar/bin/contentManagement.pl -a search -c 24 -r .*SecurityScorecard
5. Copy the ID corresponding to SECURITYSCORECARD. If the ID copied is **4003**, then in the XML file, change device-type-id-override="4001" to device-type-id-override="**4003**"
6. Click on Upload and select the modified XML file. Select default Log Source Type as “SecurityScorecard_LS”.
7. Click on Save.
8. After clicking on Save, confirm that the value of device-type-id-override is correct for all the extensions. Refer below screenshot:



Case #5 – All other issues which are not a part of the Document

- **Problem:** If the problem is not listed in the document, please follow below steps.

Troubleshooting Steps: Please follow below steps to generate log files:

1. Click on System and License Management in the Admin Panel.
2. Select the host on which the tab SecurityScorecard app for Qradar v7.4.1 FP2+ is installed.
3. Click on Actions in the top panel and select the option Collect Log Files.
4. A pop-up named Log File Collection will open.
5. Click on Advance Options.
6. Select the checkbox to Include Debug Logs, Application Extension Log, Setup Log (Current Version).
7. Click on Collect Log Files Button after selecting 5 days as data input.
8. Click on "Click here to download files".
9. This will download all the log files in a single zip on your local machine.