Carbon Black Cloud QRadar App Product Guide V1.0

Table of Contents

Configure Carbon Black Cloud

To allow QRadar to receive data from Carbon Black Cloud, you must configure one or more policies in Carbon Black Cloud, configure a SIEM and API key, and associate the SIEM key with a policy that generates notifications. See Configure the Carbon Black Cloud App & DSM for IBM QRadar for more information.

QRadar Integration

The Carbon Black Cloud App for IBM QRadar allows administrators to leverage the industry's leading cloud-based, next-generation, anti-virus solution to prevent malware and non-malware attacks. This gives administrators access to the alerts and events exposed through the SIEM notifications API for Carbon Black Cloud, as well as device, process, and event information through optional use of the other Carbon Black Cloud APIs.

Overview

The Carbon Black Cloud app for QRadar contains two components:

- Carbon Black Cloud DSM – Normalizes the Carbon Black Cloud data into a format that QRadar can index. The Carbon Black Cloud DSM must be installed to take full advantage of the capabilities offered by the Carbon Black Cloud App for QRadar.
- Carbon Black Cloud App for IBM QRadar – The app allows you to configure the connection to the Carbon Black Cloud as well as monitor the Carbon Black Cloud sensors from within QRadar

For more information, see "Install Carbon Black Cloud App & DSM for IBM QRadar" below.

Install Carbon Black Cloud App & DSM for IBM QRadar

Install the Carbon Black Cloud app for IBM QRadar via the IBM X-Force Security App Exchange. This app allows administrators to leverage Carbon Black Cloud to view and detect suspicious endpoint activity from directly within the QRadar console.

Once installed, the app allows administrators to benefit from the sophisticated threat indicators and endpoint activity events produced by Carbon Black Cloud.

Refer to IBM documentation for instructions on how to install this app. Once the Carbon Black Cloud app and DSM for IBM QRadar are installed, continue with the following sections to configure and use the app.

Requirements

The Carbon Black Cloud app for IBM QRadar requires the following:

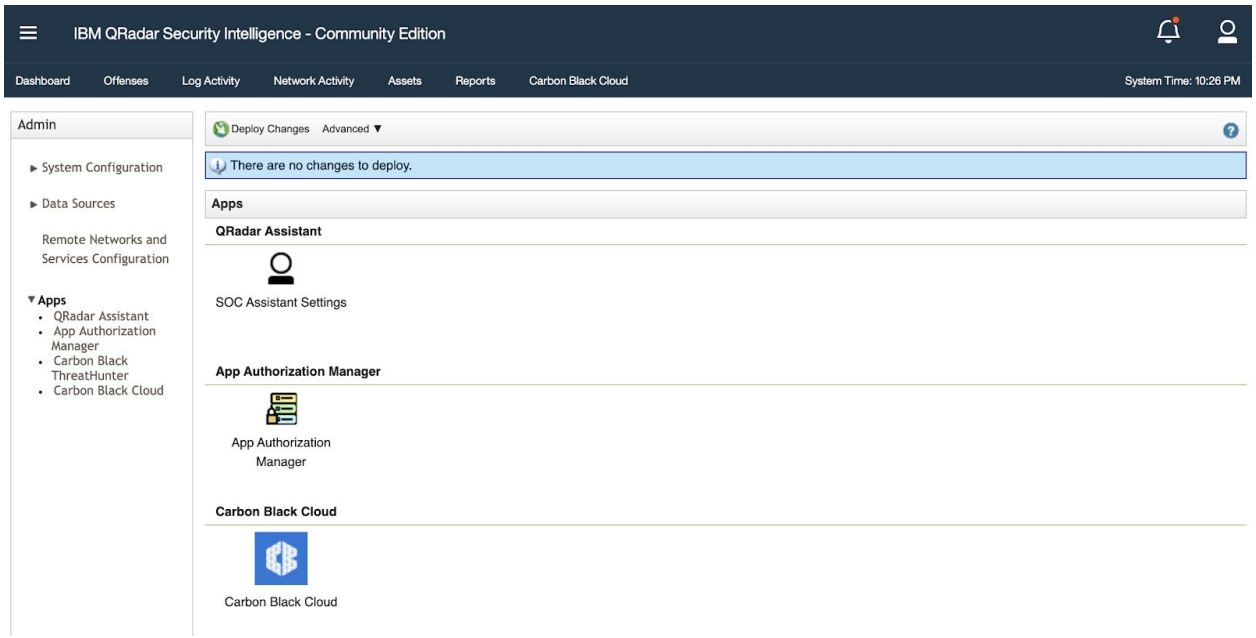
- Access to Carbon Black Cloud.
- IBM QRadar version 7.2.8 or later
- No additional hardware requirements are required to run the app above the standard requirements for Carbon Black Cloud and QRadar.

Configure the Carbon Black Cloud App & DSM for IBM QRadar

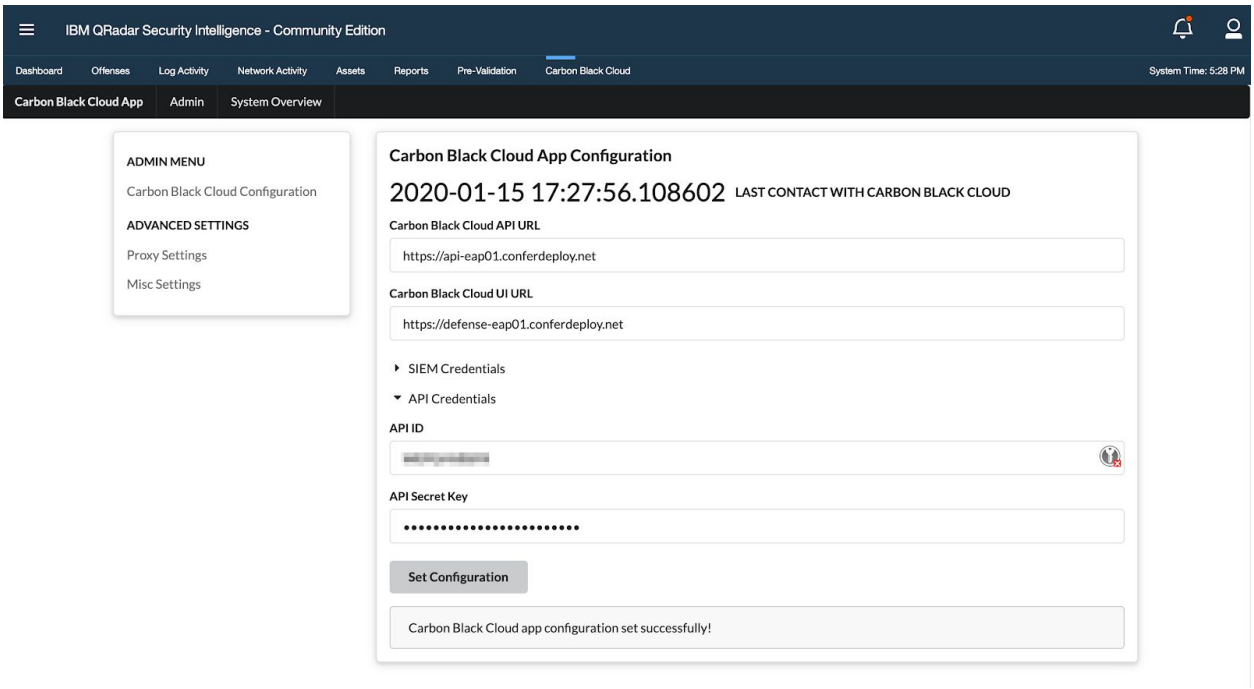
Once the Carbon Black Cloud app for IBM QRadar is installed, then you must configure it to connect to your Carbon Black Cloud server.

To configure the Carbon Black Cloud app for IBM QRadar to connect to your Carbon Black Cloud server:

- Navigate to the Carbon Black Cloud tab of your Qradar server dashboard or From the ADMIN tab select the 'Carbon Black Cloud' plugin.



- Next, you must access the Carbon Black Cloud server to retrieve the API IDs and API keys for the user you will use for this integration:
- Log into the Carbon Black Cloud server with the appropriate account.
    - In the menu bar of the Carbon Black Cloud console select the Gear shaped settings icon and then '**API Keys**' and "**Add API Key**".
    - Configure a new **SIEM** type connector and note the **SIEM API SECRET KEY** and **SIEM API ID**.
    - See the Carbon Black Cloud User's guide for instructions on how to do so.
    - In the menu bar of the Carbon Black Cloud console select the Gear shaped settings icon and then '**API Keys**' and "**Add API Key**".
    - Configure a new **API** type connector and note the **API SECRET KEY** and **API ID**.
    - See the Carbon Black Cloud User's guide for instructions on how to do so.
    - Configure a policy on Carbon Black Cloud if one is not already created.
    - In the menu bar of the Carbon Black Cloud console, select the Gear-shaped settings icon. From there, select '**Notifications**' followed by '**Add Notification**'.
    - Configure the notification settings to the desired policy and the **SIEM** connector created above.
- Return to the Carbon Black Cloud app for IBM QRadar **Admin** page and do the following:
    - Paste the SIEM API key into the **Carbon Black Cloud SIEM API Key** field.
    - Paste the API key into the **Carbon Black Cloud API Key** field.
    - Paste the API ID for the API type token into the **Carbon Black Cloud API API ID** field.
    - Paste the API ID for the API type token into the **Carbon Black Cloud SIEM API API ID** field.
- Enter the API URL for your CB Defense server instance in the **Carbon Black Cloud API URL** field. For example, enter: https://api-url.conferdeploy.net
- Enter the UI URL for your CB Defense server instance in the **Carbon Black Cloud UI URL** field. For example, enter: https://defense-url.conferdeploy.net
- **NOTE: Do not place a trailing slash (/) on this URL.**

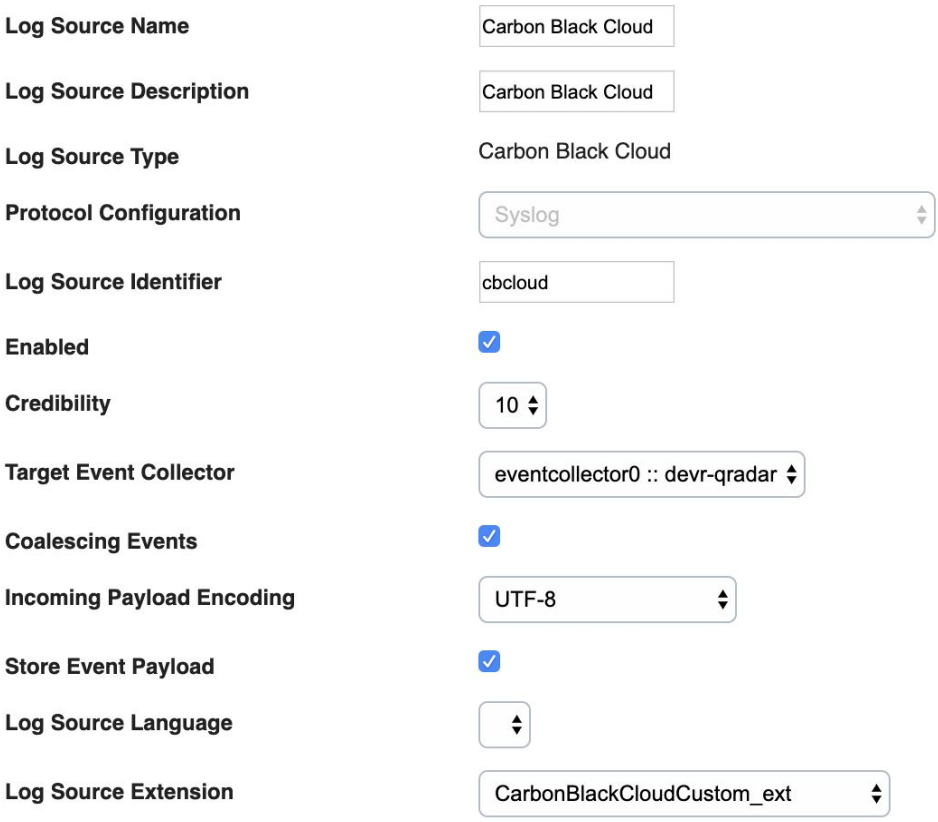


To test the configuration of the Carbon Black Cloud app for IBM QRadar after setting the URL and API key:

- After the correct parameters are entered, click **Set Configuration** to save the new configuration. A grey status bar will appear that reads “Carbon Black Cloud Configuration Set Successfully”.
- Once configured, you should also see the last time the server has been polled for notifications (the poller runs every five minutes by default this can be adjusted in **Misc Settings**).

For QRadar to pick up the Carbon Black Cloud logs automatically you may need to manually add the Log Source:

- The IBM knowledge base has information on adding a log source
- Below is the required configuration



User Interface

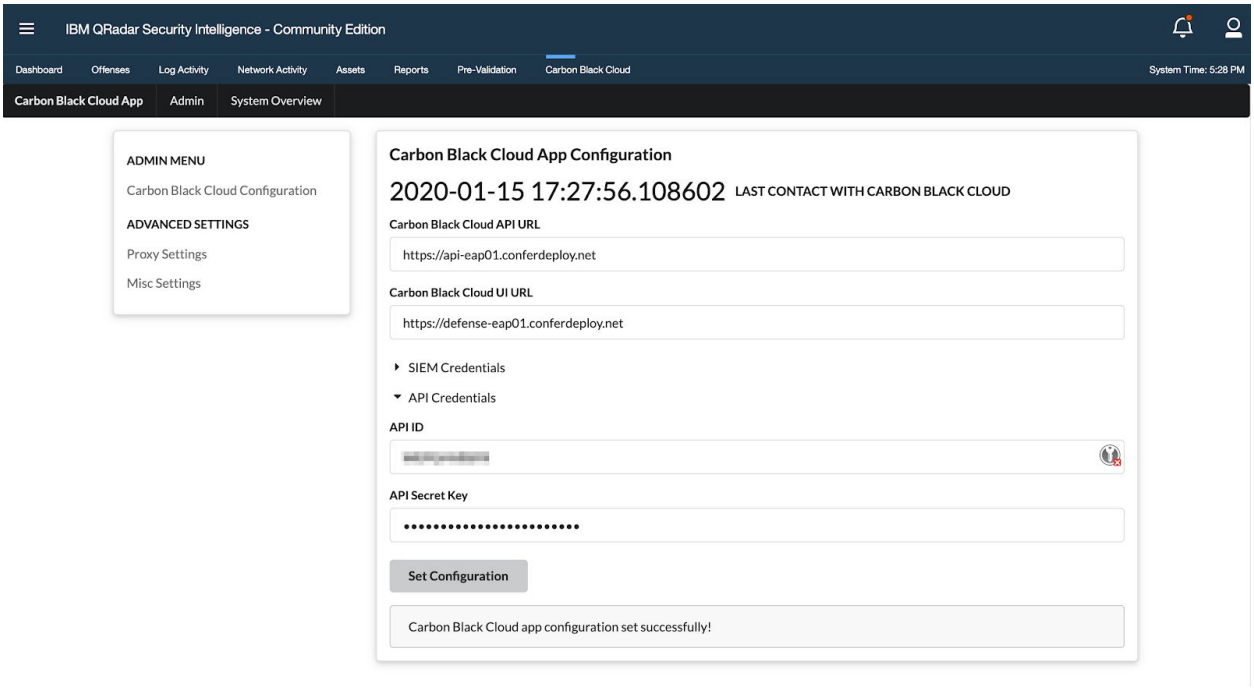
The Carbon Black Cloud app for IBM QRadar contains two major user interface components: **Carbon Black Cloud Admin** and **Overview tabs**.

Admin Sub-Tab

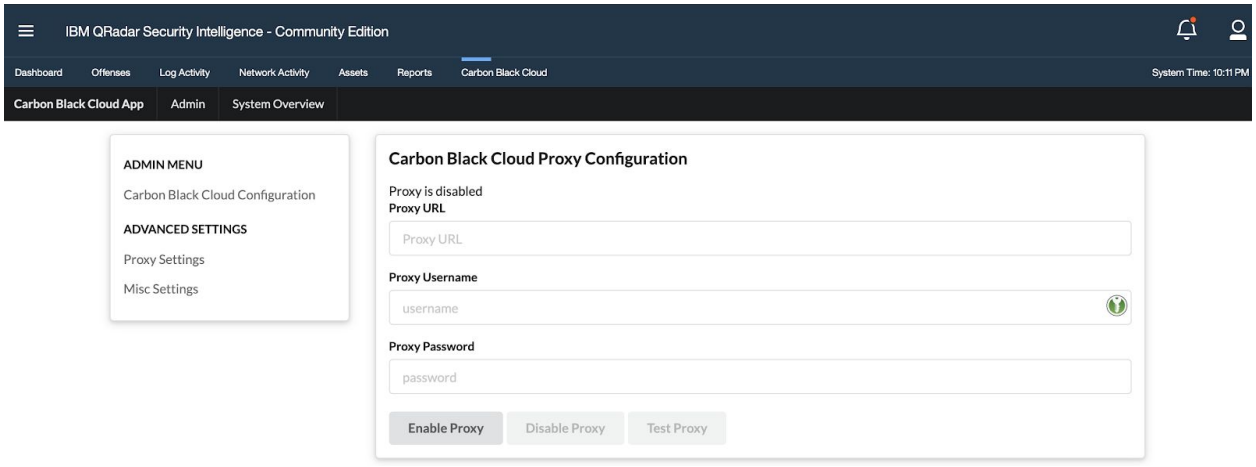
The **Admin** sub-tab allows you to configure the app. Only QRadar users with “Admin” privileges can access or change settings in this tab.

The **Admin** interface provides access for the following:

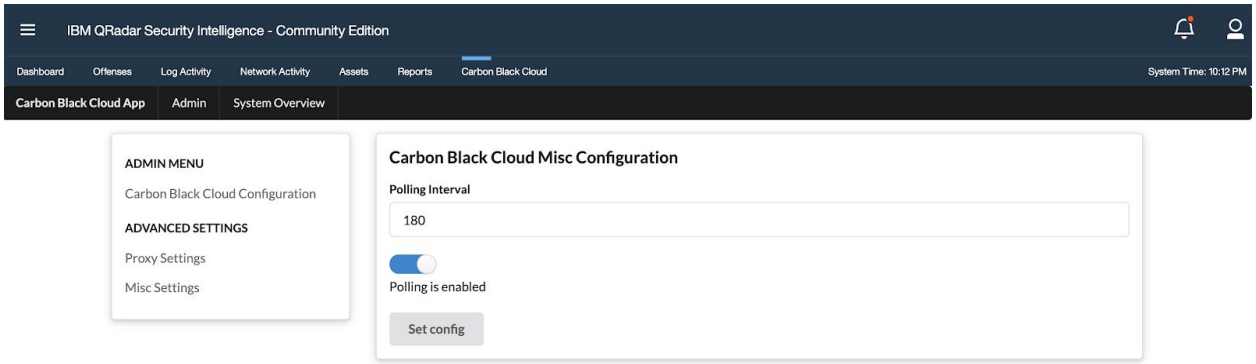
- **Carbon Black Cloud Configuration** - Allows you to adjust the URLs and API keys associated with your Carbon Black Cloud server or cluster. These are all the configuration options required for most deployments.



- **Proxy Settings**- Allows setting of optional proxy configuration, using an HTTP CONNECT PROXY with username/password authentication. When configured, the proxy will be used for all communication with Carbon Black Cloud.
    - The Proxy URL format is as follows [http/https]://[hostname]:[port]



- **Misc Settings** - Allows adjustment of additional configuration options. Here the user can control the polling interval for the Carbon Black Cloud notifications poller - in seconds, which defaults to 180 or 3 minutes. Polling can also be disabled/enabled. Use the **Set Configuration** button to apply your configuration changes.



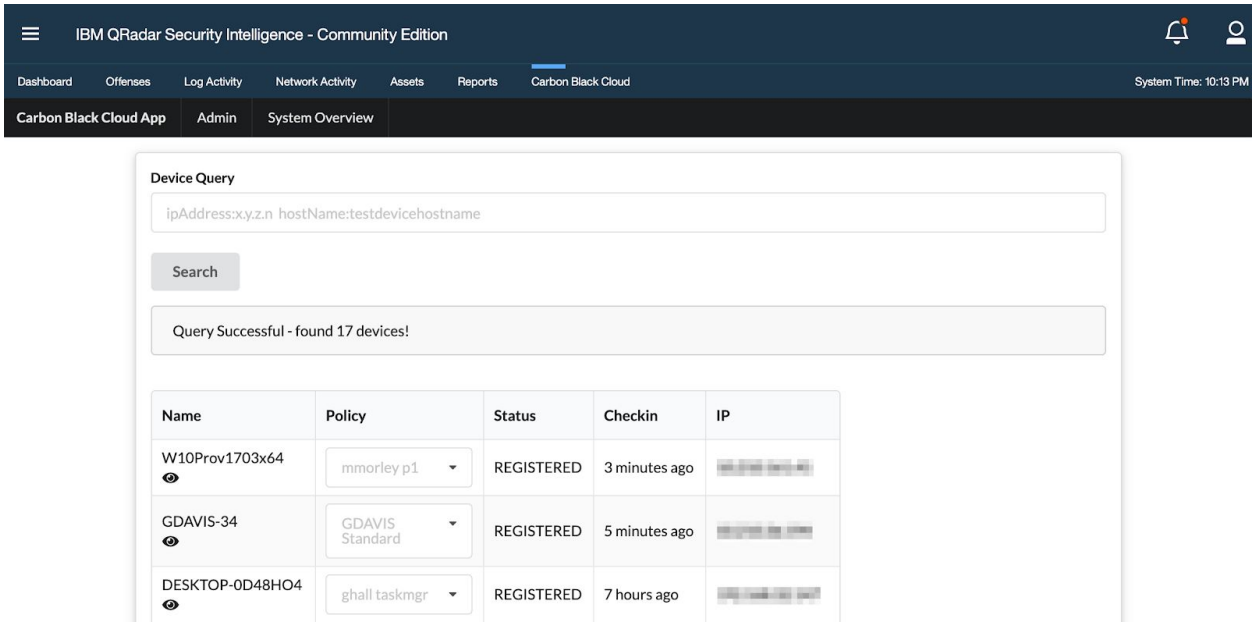
Overview Sub-Tab

The **Overview** sub-tab allows you to view the status of your sensors and change their assigned security policies.

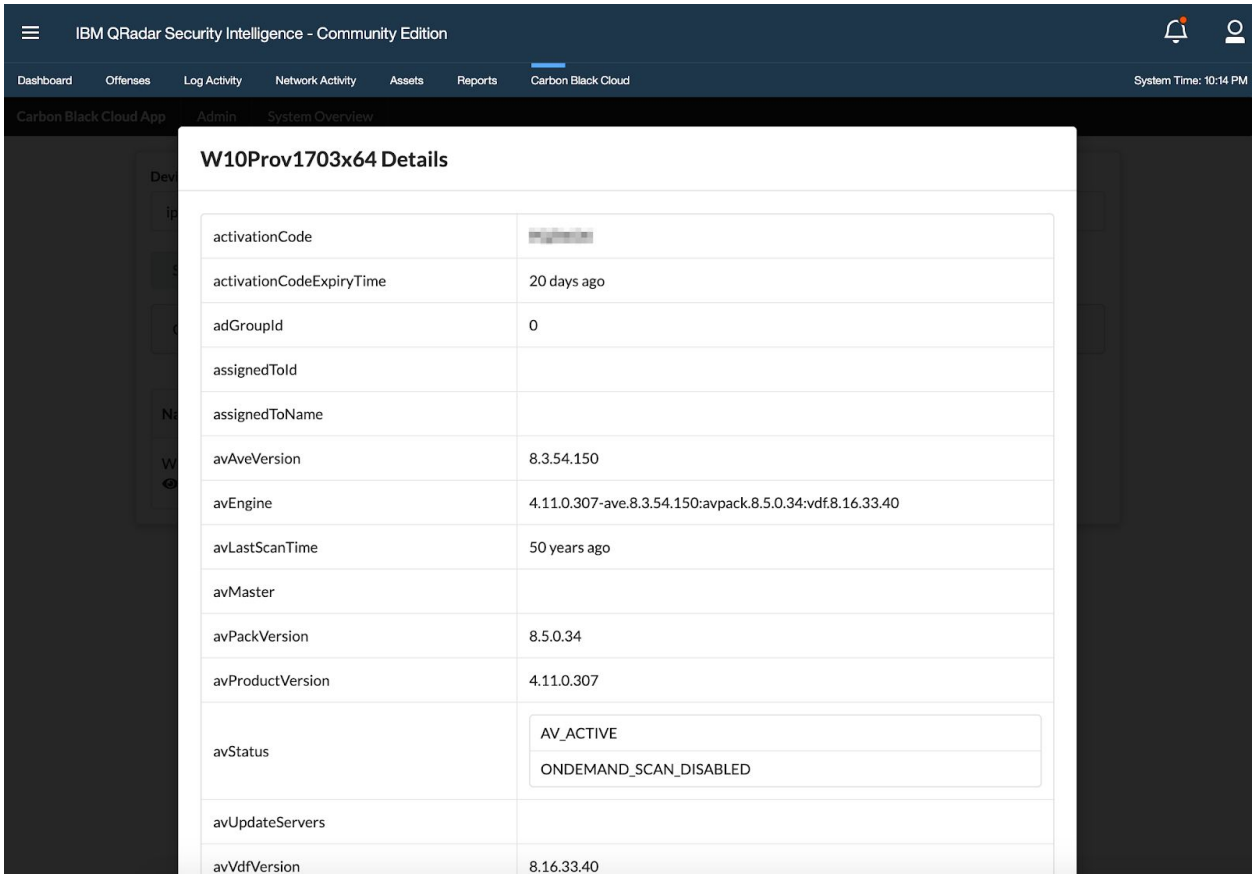
The **Overview** interface provides access to a Sensor Query field where the user can query by ipAddress, hostName, hostNameExact, ownerName or ownerNameExact. Multiple queries are implicitly, logically ANDED.

From this view, you can access details about each sensor's configuration by selecting the 'eyeball' icon below each Sensor Name.

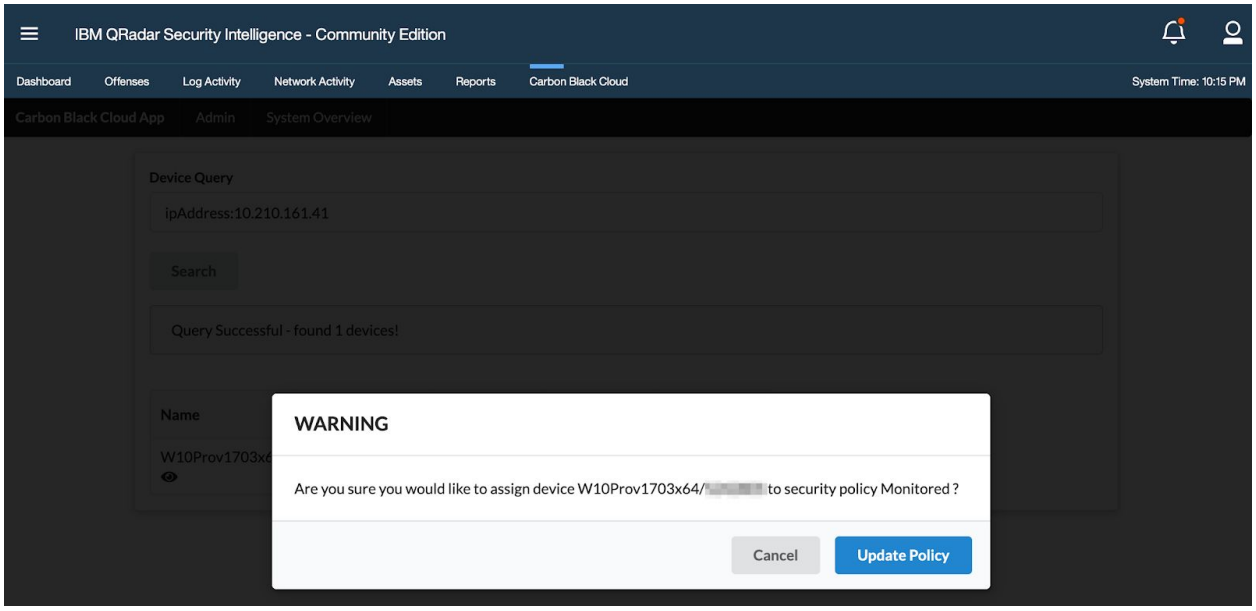
You can also select the Policy dropdown to change the assigned security policy.



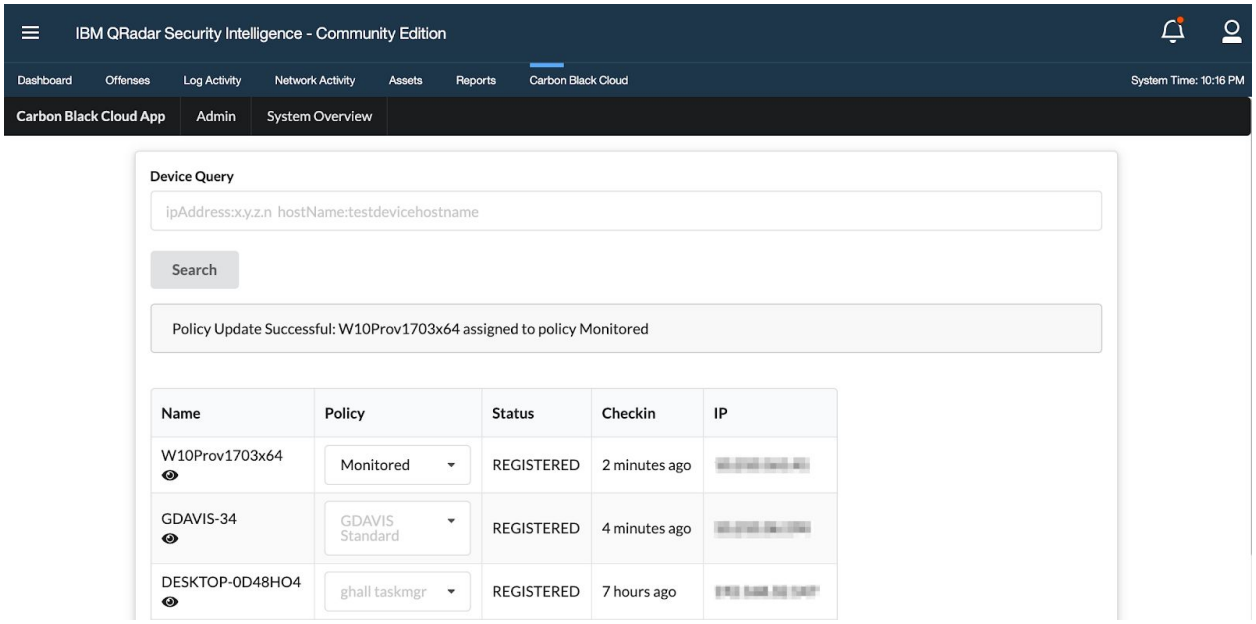
View of the modal with details about the sensor Sensor:



If you make a change to the Policy dropdown, you will receive a warning asking you to verify that you want to assign a new security policy. Select Update Policy to verify the change and return to the Overview Sub-Tab.

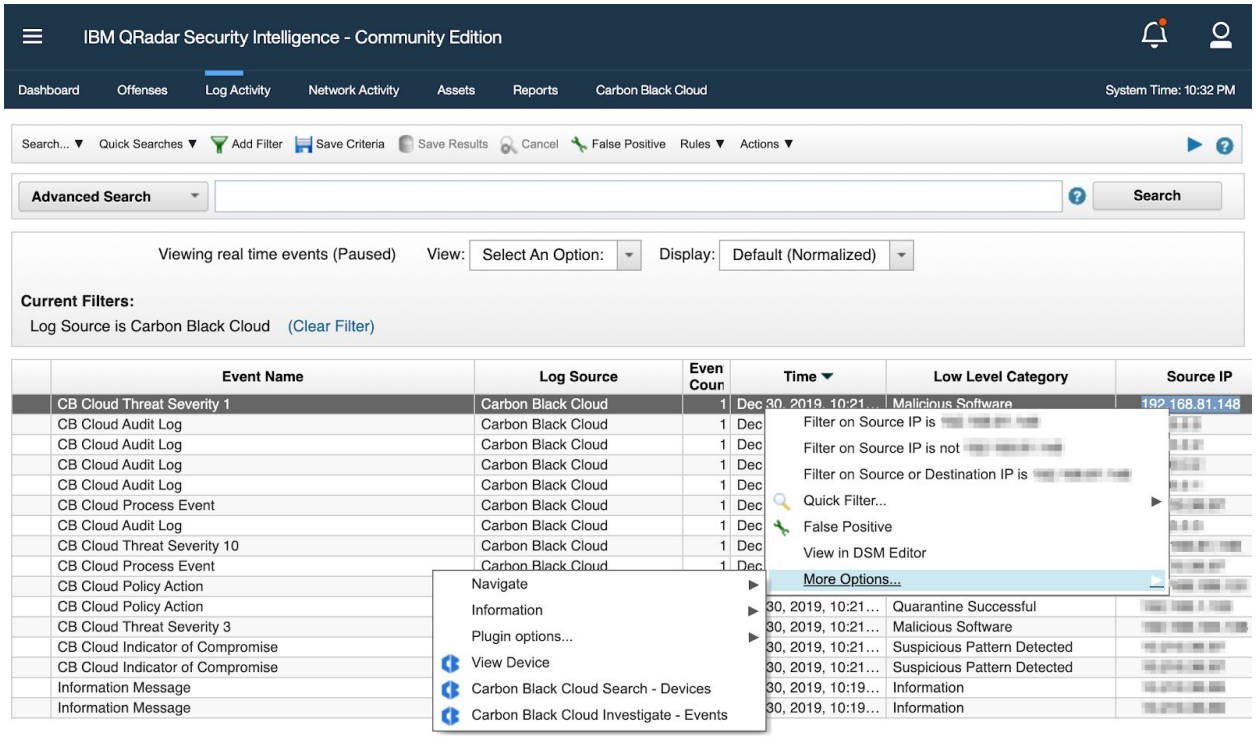


When you return to the Overview Sub-Tab, you will see the change reflected in the Policy dropdown.



Log Activity Tab

Log Activity Tab right-click menus:
Added various right-click context menus with support for right-clicking on ‘ip’ elements in various Qradar views and querying for devices and events within the Carbon Black Cloud UI as well as searching for devices in the QRadar UI where policies can be changed.



Troubleshooting

Carbon Black Cloud is not making contact

- API traffic is also supported on the UI url https://defense-<hostname>
- If the url change does not solve the problem, check the network on the QRadar host to confirm connectivity to Carbon Black Cloud

Carbon Black Cloud events are not appearing in log activity even though contact has been made

- Check that the API keys are of the correct key type
- Confirm that the SIEM key is assigned to one or more Notification Rules
- Check the notification rule history for notifications that have been sent

Proxy configuration is not saving to the app

- Enter the proxy configuration before enabling the proxy
- If the proxy is already enabled, disable then re-enable the proxy