Mandiant

MANDIANT ADVANTAGE FOR IBM QRADAR

The Mandiant Advantage app for QRadar brings Mandiant's front-line intelligence to QRadar. It highlights indicators of compromise (IOCs) in your network and lets you identify and explore the ones that matter most.

Reduce alert fatigue by applying Mandiant's Indicator Confidence scoring to ensure you're only alerted when it matters. If you identify an active breach, the Mandiant Advantage app for QRadar provides one-click access to our Incident Response professionals. They are automatically provided with the relevant data to simplify and speed up the response process.

Pre-requisites

- QRadar version 7.4.x or 7.5.x
- Outbound network connectivity to Mandiant APIs using HTTPS on port 443

Get API Key ID and Secret

To obtain a **Service API Key** (which is tied to an organization rather than an individual user) for use with third-party security technologies such as a SIEM, contact **Support (https://www.mandiant.com/support)**.

To obtain an API Key ID and Secret for an individual user account, perform the following:

1. Navigate to the Mandiant Threat Intelligence web console.
2. Click **Account Settings**.
3. Select **API Access and Keys** from the navigation menu.
4. Click **Get Key ID and Secret**.
5. Copy and store the displayed values in a secure location.

New Install

1. Download the QRadar extension from the **IBM App Exchange (https://exchange.xforce.ibmcloud.com/hub/extension/3a996a7812c185dea2bf3731347b8226)**.
2. Log in to the QRadar console as an admin user.
3. Open the Admin page.
4. Click **Extensions Management**.
5. Click **Add**.
6. Browse to the location that the extension file was saved to upload the extension to your system.
7. Click **Add** to upload the extension.
8. Click **Install** to install the extension.

Upgrading from 1.0.0

In-place upgrades are supported: All previously defined settings for the Mandiant Advantage Account and Input are maintained after an upgrade.

1. Download the QRadar extension from the **IBM App Exchange (https://exchange.xforce.ibmcloud.com/hub/extension/3a996a7812c185dea2bf3731347b8226)**.
2. Log in to the QRadar console as an admin user.
3. Open the Admin page.
4. Click **Extensions Management.**
5. Click **Add**.

6. Browse to the location that the extension file was saved to upload the extension to your system.
7. Click **Add** to upload the extension.
8. Click **Install** to install the extension.
9. Leave the default option to **Replace existing items** selected to preserve the app settings.
10. Verify that your Mandiant Advantage account has been maintained.

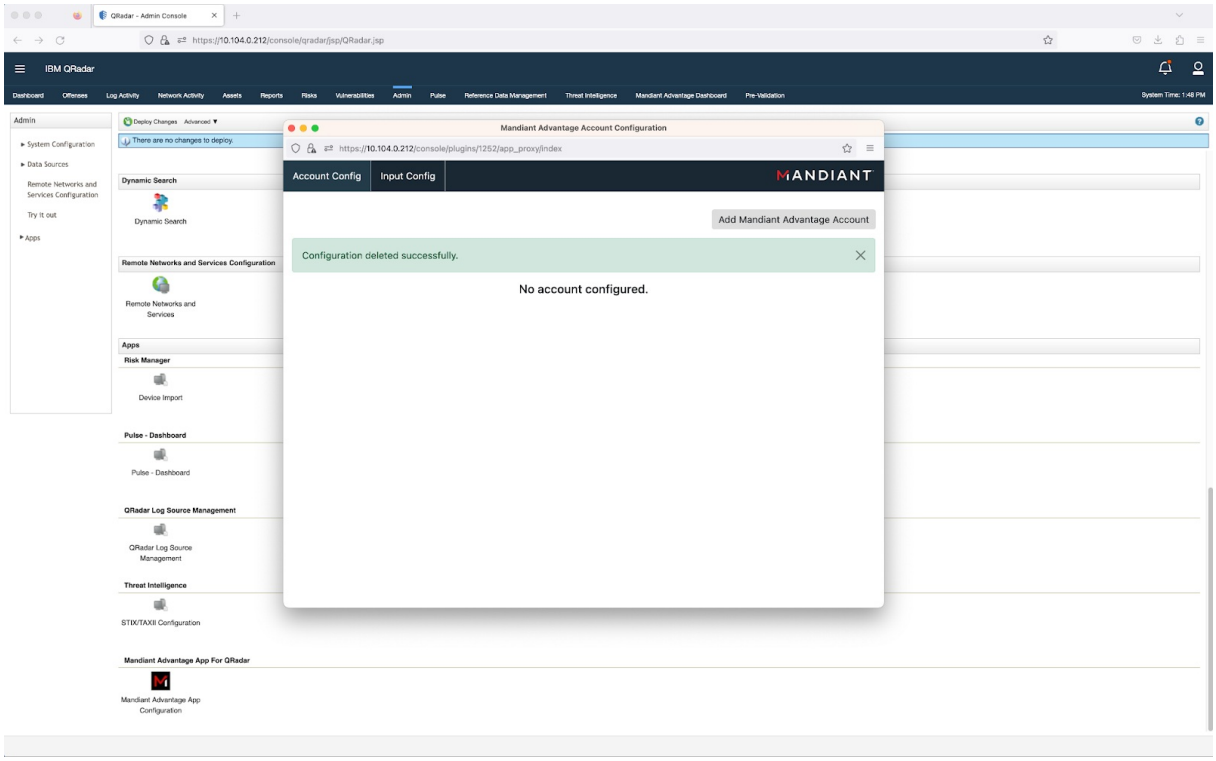
> Load the Input Configuration and define the Enable / Disable Offense Enrichment setting to the desired behavior. This is a new setting that needs to be defined before it can be used. Failure to do this will prevent Offense Enrichment from running.

11. Optional: Uninstall version 1.0.0 to clean up the system.

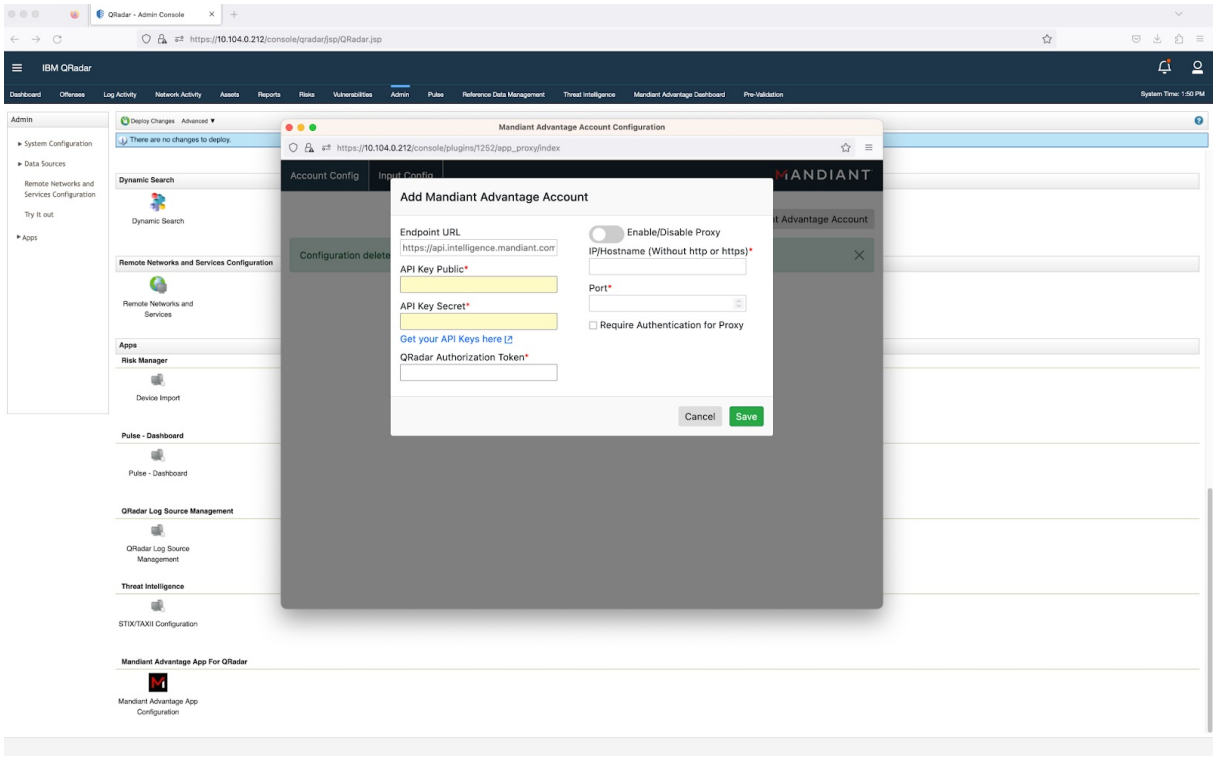
Configuration

Add a Mandiant Account

1. Log in to the QRadar console as an admin user.
2. Open the Admin page.
3. Scroll to the Apps section.
4. Click **Mandiant Advantage App Configuration** to open the following modal:



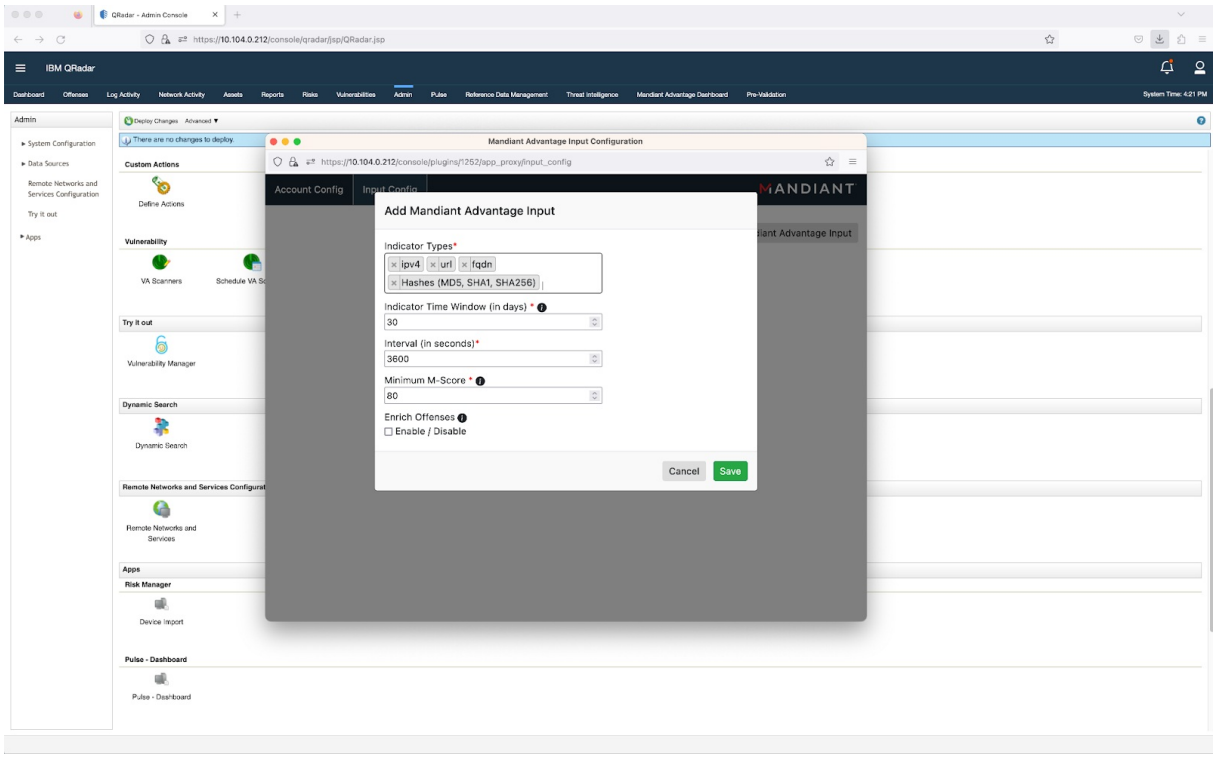
5. Click **Add Mandiant Advantage Account** to open the following modal:



6. Complete the form and click **Save**.

Add an Input

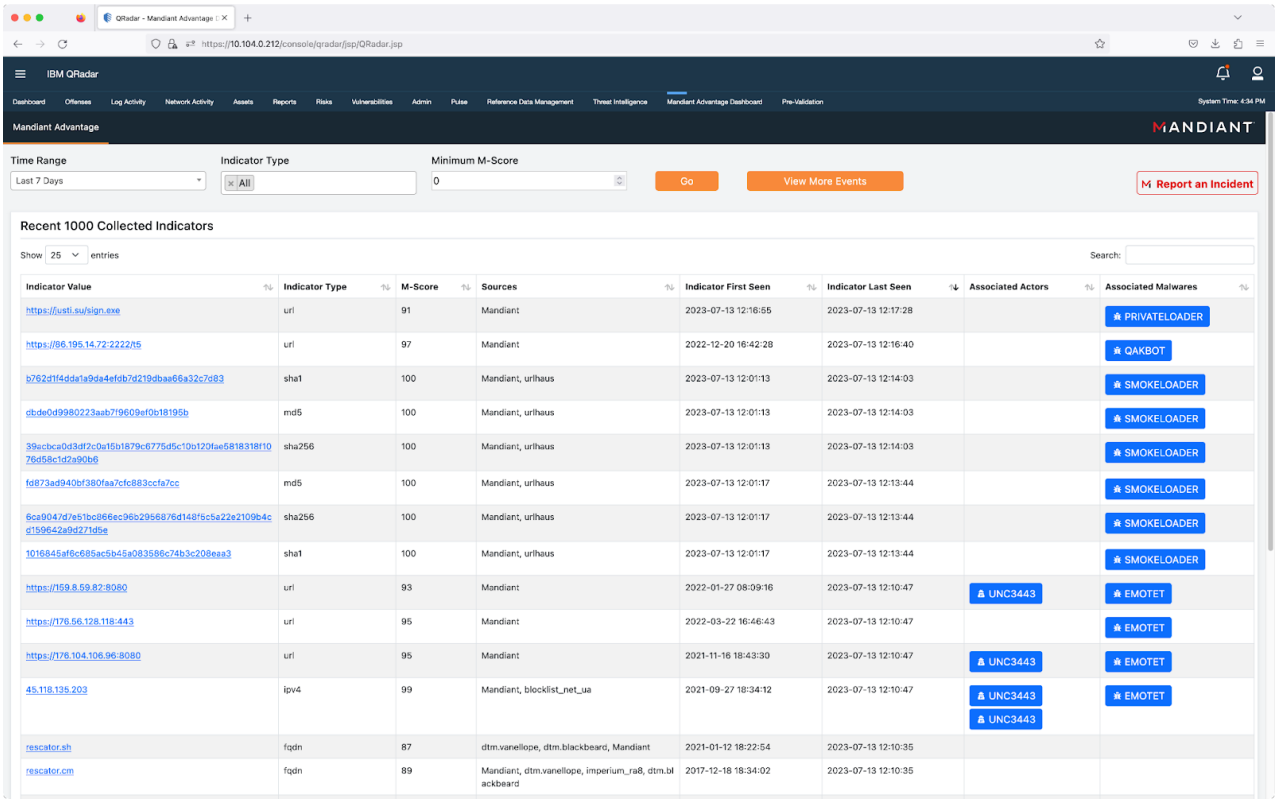
1. While logged in to the QRadar console as an admin user with the Mandiant Advantage App Configuration modal open, click **Input Config**.
2. Click **Add Mandiant Advantage Input** to display the Add Mandiant Advantage Input modal.
3. Complete the form with the desired options and click **Save**.



The Indicator Collection and and Offense Enrichment processes will start to function.

Dashboard

The **Mandiant Advantage Dashboard** is accessed from the main navigation menu of the QRadar Console. It displays a list of indicators ingested into the system. Filters are provided to help you locate indicators of interest.

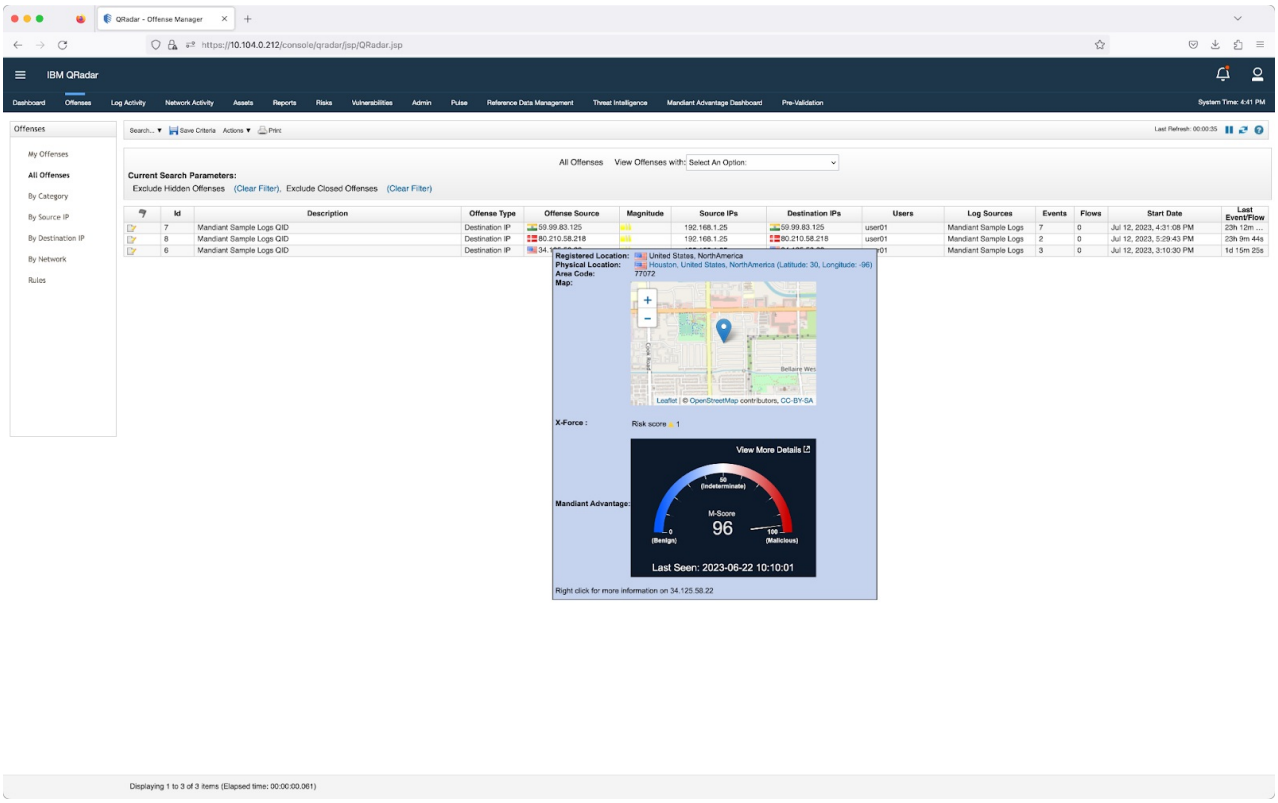


Hover Enrichment

Wherever one of the following data types are displayed in the QRadar console, Hover Enrichment is available for the value:

- IP Address
- Indicator Value
- URL
- SHA 256 Hash
- File Hash

On hover, the value is checked against the Mandiant API. If the value is known to Mandiant, the **IC Score**, **Last Seen** date, and a link to the indicator in the Mandiant Advantage platform is displayed.



Troubleshooting

Accessing the container to view logs

QRadar apps run as Docker containers on the QRadar host. To access a shell of the container running the app:

1. Run this command to find the installed apps:

```
psql -U qradar

select id, name from installed_application;
```

2. View what apps are running:

```
docker ps -a
```

3. Look for the ID of the Mandiant app and copy the Container ID.
4. Run this command to start a shell on the container:

```
docker container exec -it CONTAINER_ID /bin/bash
```

Log files are written to this directory: `opt/app-root/store/log`

Release Notes

- **v1.1.1**
  - **New Features**:
    - Added a setting to override the Syslog server for use when ingesting data.
    - Added a setting to **Enable/Disable** automated Offense enrichment.
    - Added a setting to **Include/Exclude** Open Source indicators.

> Default is **Exclude** to limit the number of indicators added to QRadar Reference Sets.

- The Mandiant Indicator QRadar Reference Sets are now recreated on every update to ensure they always contain the latest Threat Intelligence.
- Indicators that drop below the **Minimum IC Score** specified in the **Input** definition are now included in the QRadar index so the lifecycle of an indicator can be seen in QRadar.
- The app now uses the Mandiant API Base URL.

- **Bug Fixes**:
  - Fixed an issue where QRadar Offenses were enriched multiple times with the same information.
  - Fixed an issue where the app would fail to connect to QRadar through Syslog, causing data ingestion to fail.