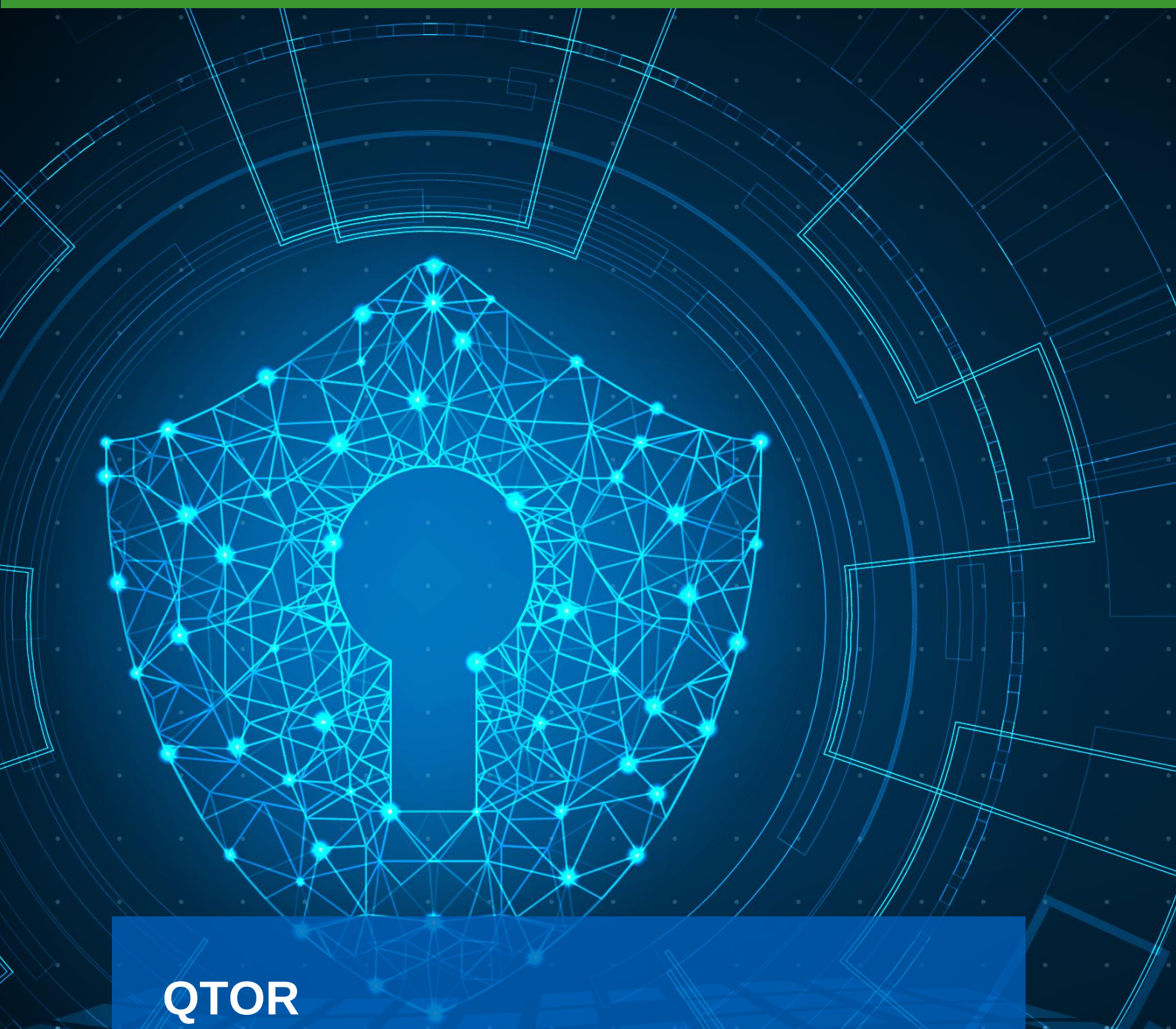


QTOR
FOR IBM SECURITY QRADAR SIEM

ADMIN GUIDE

Table of Contents

Overview

TOR Monitor App for IBM Security QRadar SIEM (hereinafter “QTOR” application), is a QRadar extension that allow users to easily monitor inbound and outbound connection to the DarkNet via TOR relay and exit nodes.

QTOR requires Internet access to reach https://onionoo.torproject.org website which is used to gather information about active relay and exit TOR nodes.

QTOR package contains following new security content:

- QRadar application to poll TOR nodes
- Two custom rules for inbound and outbound TOR connections monitoring (works for both events and flows)

QTOR App is a free tool and available under Apache 2 license. Full text of the license is available on the official website: https://www.apache.org/licenses/LICENSE-2.0

Supported Versions

Supported QRadar versions are:

- 7.2.8 Patch 8 and higher

NOTE: QTOR App is developed by ScienceSoft Inc. and is not supported by IBM. You can request your own custom QRadar app to be developed or to get support for this particular app via the following email address: **qlean@scnsoft.com**.

QTOR Installation

QTOR App is distributed as a QRadar extension.

In order to install QTOR App please follow the steps below.

Downloading QTOR

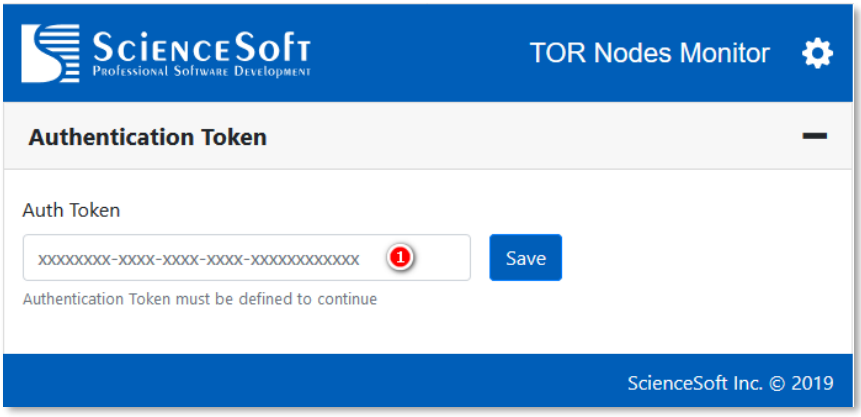
- Go to https://exchange.xforce.ibmcloud.com/hub
- Login using your IBMid
- Filter by Type: Application
- Select **QTOR** extension
- Click **Download** button at the top right corner
- Save the extension zip file

Installing QTOR

- Login to QRadar UI
- Go to **Admin** tab
- Open **Extensions Management**
- Click **Add** button
- Select **Install immediately** checkbox, click **Browse** button, locate the extension file downloaded from IBM App Exchange and click **Add** button
- Confirm on all steps and wait for installation to finish. This may take a while.
- Close **Extensions Management** window, press **Ctrl+F5** to fully reload QRadar UI. New **QTOR** icon will be added to QRadar **Admin** tab.
- **Deploy changes** if asked by QRadar

Configuring QTOR

- Login to QRadar UI
- Go to **Admin** tab
- Create new **Authorized Service**
- Open **QTOR** interface
- On the initial run you'll be presented with a configuration field to enter Authorization Token
- Enter **Authorization Token** generated on previous step (1)
- Press **Save** button to save configuration
- Proceed with next chapter to configure application (same window)

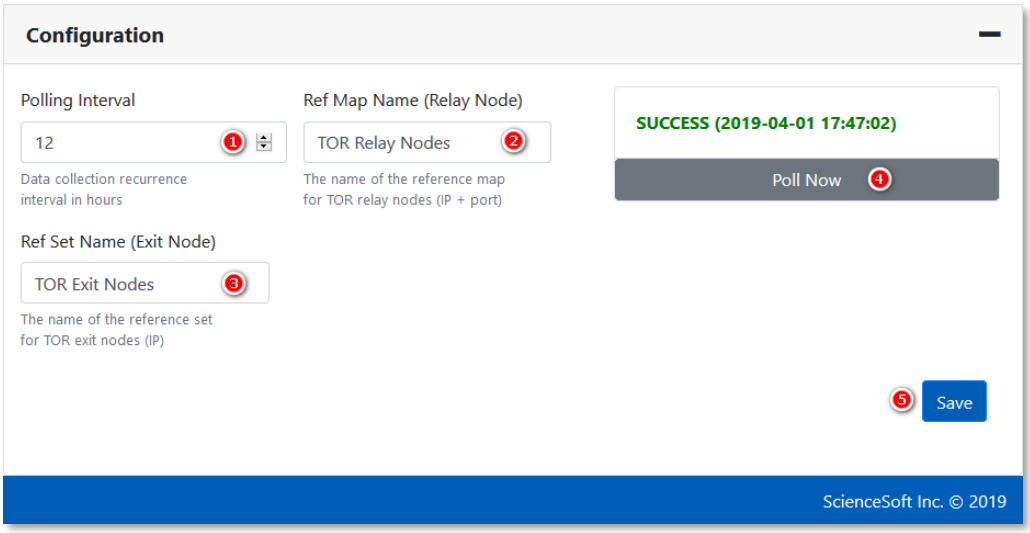


Configuration

Configuring Application

Follow steps below to configure application:

- In QRadar UI, navigate to **Admin** tab
- Open **QTOR**

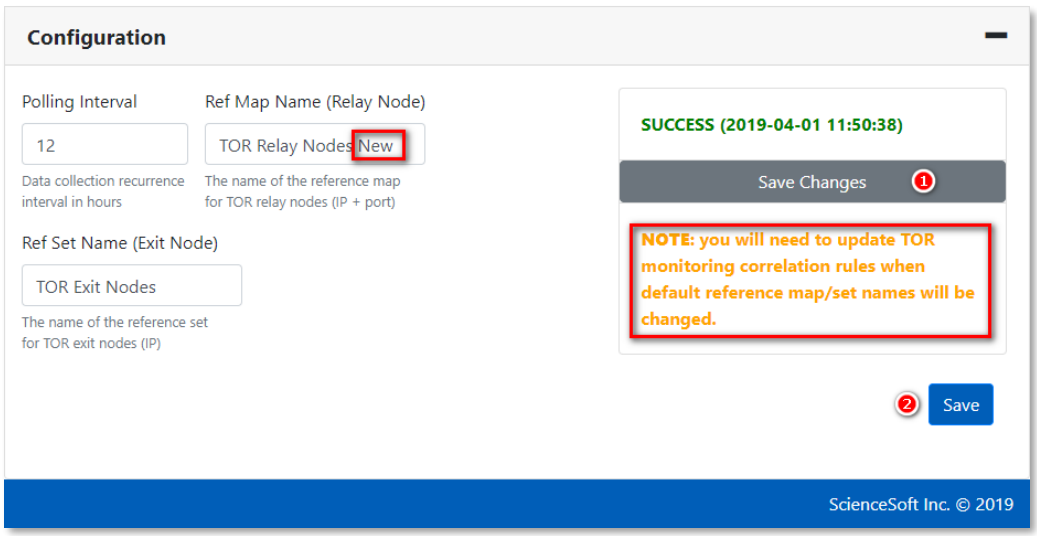


Following configuration options are available for modification:

1. **Polling Interval** (in hours) – defines frequency of TOR node polling from Internet.
2. **Ref Map Name** – the name of the reference map to store TOR relay nodes information (IP addresses and ports).
3. **Ref Set** – the name of the reference set to store TOR exit nodes information (IP addresses).
4. **Poll Now** – allows to perform TOR node polling immediately.

Press **Save** (5) button to save configuration.

NOTE: you will need to update TOR monitoring correlation rules when default reference map/set names will be changed. Press (1) or (2) to save new name(s) and then update the rules.



Usage

Custom Rules

QTOR App is shipped with two rules for inbound and outbound TOR connections monitoring:

- TOR Nodes: Incoming TOR Traffic Detected
- TOR Nodes: Outgoing TOR Traffic Detected

Those rules are configured to generate offenses when at least 5 connection to the TOR network are detected within 10 hours timeframe.

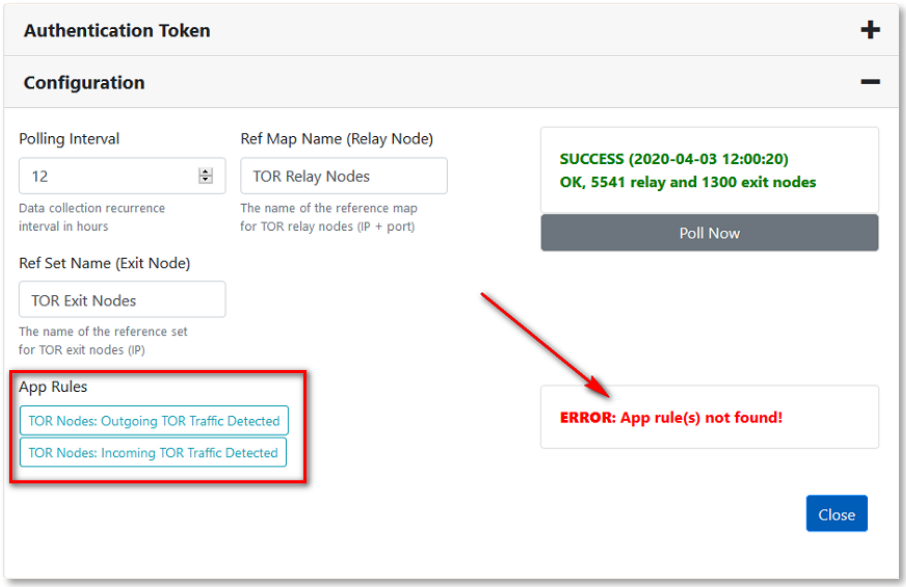
Please modify the rule logic of you want to change alerting or response behavior.

NOTE: you will need to update TOR monitoring correlation rules when reference map/set names are changed from their defaults.

Authorization Token Privileges and Rules

When authorization token is not granted with full admin privileges, you may experience “App rule(s) not found” error in QTOR user interface. However, this does not mean that rules are not installed with app.

Insufficient privileges are only affecting ability to open rules details directly from QTOR interface (see the screenshot below). Application functionality is not affected.

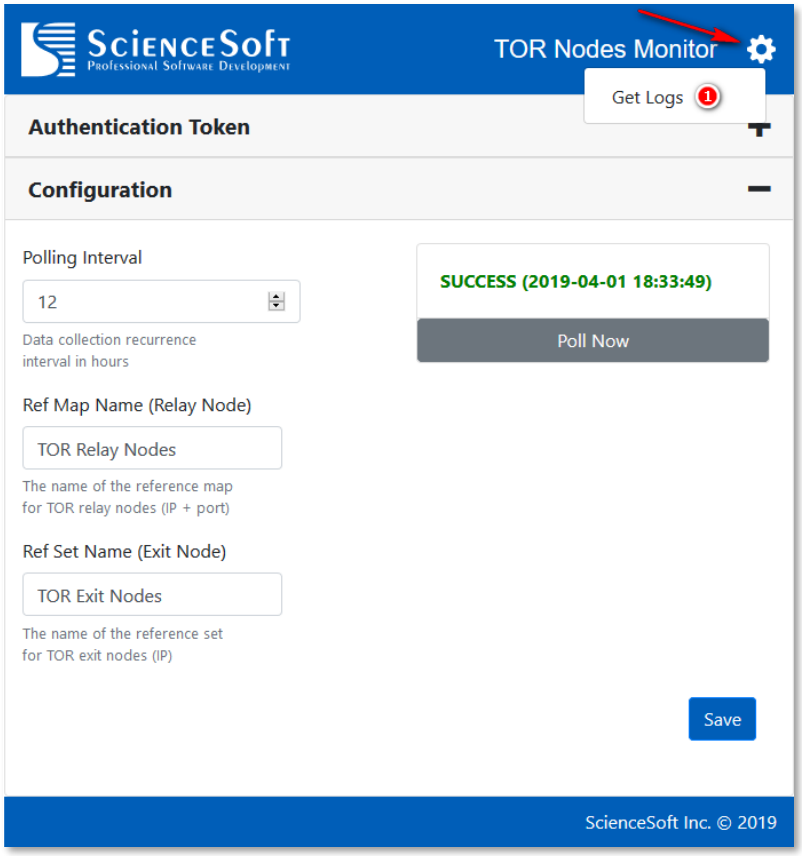


Troubleshooting

Getting Application Logs

If have any other problems with QTOR App please download the application log archive and forward it to the following address for investigation: **qlean@scnsoft.com**

To download the log archive open configuration page and press **Gear** button, then select **Get Logs** item (1):



Appendix A: Release notes

1.0.0

Initial version