

ThreatQuotient



www.dan.me.uk Tor Node List CDF Guide

Version 2.0.0

February 07, 2022

ThreatQuotient

11400 Commerce Park Dr., Suite 200
Reston, VA 20191

 **ThreatQ Supported**

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

Support	4
Versioning.....	5
Introduction	6
Installation.....	7
Configuration	8
ThreatQ Mapping	9
www.dan.me.uk Tor Node List.....	9
Average Feed Run.....	10
Known Issues / Limitations	11
Change Log.....	12

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Copyright © 2022 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com

Support Web: <https://support.threatq.com>

Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.



ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Versioning

- Current integration version: 2.0.0
- Compatible with ThreatQ versions $\geq$ 4.20.0

Introduction

The www.dan.me.uk Tor Node List CDF for ThreatQ provides a full Tor node list (not more than one hour old) in script-readable format.

The integration provides the following feed:

- **www.dan.me.uk Tor Node List** - ingests indicators in a pipe-delimited format.

The integration ingests indicators and indicator attributes.

Important Notes:

- Nodes flagged **E** are those which allow exit from the Tor network.
- Nodes flagged **x** are those which allow exit from the Tor network, but do not publicly advertise that they do so.



The feed source (<https://www.dan.me.uk/tornodes>) can only be accessed once every 30 minutes. If accessed too often, your IP will be blocked.

Installation

Perform the following steps to install the integration:



The same steps can be used to upgrade the integration to a new version.

1. Log into <https://marketplace.threatq.com/>.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
 - Drag and drop the file into the dialog box
 - Select **Click to Browse** to locate the integration file on your local machine



ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.

6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to [configure and then enable the feed](#).

Configuration



ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **OSINT** option from the *Category* dropdown (optional).



If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration to open its details page.
4. Enter the following parameter under the **Configuration** tab:

PARAMETER

DESCRIPTION

Only Ingest Exit Nodes

If checked, the integration will only ingest nodes which allow exit from the Tor network. This parameter is unchecked by default, which results in ingesting all nodes.

Feed URL

This parameter is for UI display purposes only.

5. Review the **Settings** configuration, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

www.dan.me.uk Tor Node List

The feed ingests data using the following pipe-delimited format:

```
<ip>|<name>|<router-port>|<directory-port>|<flags>|<uptime>|<version>|<contactinfo>
```

Sample Response:

```
101.100.136.62|warduckcomingatya|9001|9030|RSDV|6699668|Tor 0.4.1.6|0xFFFFFFFF Warduck <warduck@gmail.com>
103.234.220.195|ASock|443|80|EFHRSDV|1918882|Tor 0.4.1.6|dobby_potter at aol.com or send hedwig
2605:6400:0030:f8f0:b055:151e:5dcf:7ae4|ULayerManning|443|80|FGRSDV|62|Tor 0.4.1.6|noc [AT] ulayer.net
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
ip	indicator.type	IP Address/IPv6 Address	N/A	The indicator type is derived from the value of ip
ip	indicator.value	N/A	101.100.136.62	
name	indicator.attribute	TOR Name	warduckcomingatya	
router-port	indicator.attribute	Router Port	9001	
directory-port	indicator.attribute	Directory Port	9030	
flags	indicator.attribute	Flags	RSDV	If the configuration parameter <code>Only Ingest Exist Nodes</code> is checked and <code>flags</code> contains neither E nor X, the indicator is not ingested.
uptime	indicator.attribute	Uptime	6699668	
version	indicator.attribute	Version	Tor 0.4.1.6	
contactinfo	indicator.attribute	Contact	0xFFFFFFFF Warduck <warduck@gmail.com>	

Average Feed Run

METRIC	RESULT
Run Time	12 min
Indicators	8660
Indicator Attributes	60238



Object counts and Feed runtime are supplied as generalities only - Feed runtime may vary based on system resources and load.

Known Issues / Limitations

The feed source (<https://www.dan.me.uk/tornodes>) can only be accessed once every 30 minutes. If accessed too often, your IP will be blocked.

Change Log

- Version 2.0.0
 - Initial release