

# ThreatQuotient



## **Symantec Management Center Connector Guide**

Version 1.0.0

Monday, February 8, 2021

### **ThreatQuotient**

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

### **Support**

Email: [support@threatq.com](mailto:support@threatq.com)

Web: [Support.threatq.com](http://Support.threatq.com)

Phone: 703.574.9893

---

# 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 © 2021 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.

# Contents

<b>Warning and Disclaimer .....</b>	<b>2</b>
<b>Contents .....</b>	<b>3</b>
<b>Versioning.....</b>	<b>4</b>
<b>Introduction .....</b>	<b>5</b>
Preface.....	5
Audience.....	5
<b>Prerequisites .....</b>	<b>6</b>
<b>Configure Symantec Management Center.....</b>	<b>7</b>
<b>Installation .....</b>	<b>9</b>
<b>Configuration .....</b>	<b>11</b>
<b>Usage.....</b>	<b>13</b>
Basic Usage .....	13
Command Line Arguments .....	13
<b>Change Log .....</b>	<b>14</b>

---

# Versioning

- Current integration version: 1.0.0
- Supported on ThreatQ versions: 4.40 or greater

---

# Introduction

The Symantec Management Center connector for ThreatQuotient allows a user to synchronize indicators of compromise from ThreatQ data collections with IP Address and URL lists in Management Center.

Once the indicators are synchronized, the lists can be used in security policies in Management Center.

The following is the mapping of indicators from ThreatQ to Management Center lists:

- IP Address -> IP Address List
- FQDN -> URL List
- URL – URL List

## Preface

This guide is to provide the information necessary to implement the Symantec Management Center connector for ThreatQuotient. This document is not specifically intended to form a site reference guide.

It is assumed that the implementation engineer has experience installing and commissioning ThreatQuotient Apps and integrations covered within the document, as well as experience necessary to troubleshoot at a basic level.

## Audience

This document is intended for use by the following parties:

1. ThreatQ and Security engineers.
2. ThreatQuotient Professional Services Project Team & Engineers.

---

# Prerequisites

Throughout this implementation document, there will be referrals to several files and directories, some of which will be symbolic, and others may change depend on specifics of the environmental setup.

Ensure all ThreatQ devices are set to the correct time, time zone and date, and using a clock source available to all.

To identify which time zone is closest to your present location, use the `timedatectl` command with the `list-timezones` command line option. For example, to list all available time zones in Europe, type:

## Time Zone List Example

```
timedatectl list-timezones | grep Europe
Europe/Amsterdam
Europe/Athens
Europe/Belgrade
Europe/Berlin
```

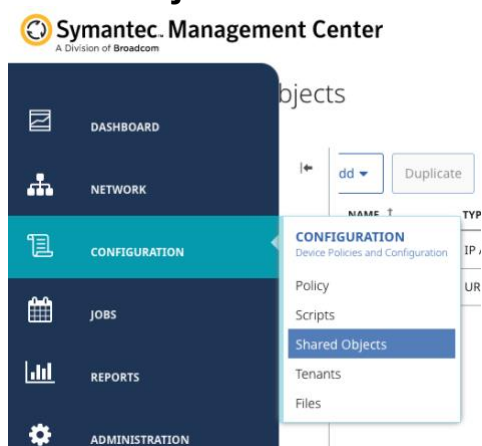
To change the time zone to UTC, type as root:

```
timedatectl set-timezone UTC
```

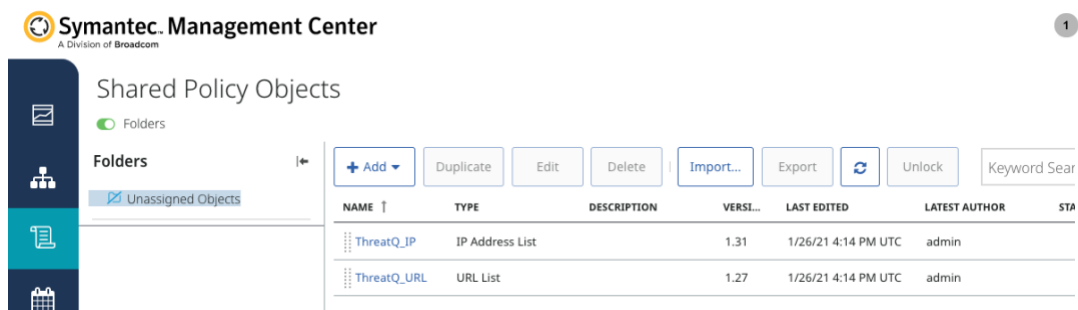
# Configure Symantec Management Center

In order for Management Center to accept the indicators from ThreatQ, a user needs to create IP Address and URL lists in Management Center. Once configured, the lists will be automatically synchronized with dedicated data collections in ThreatQ. Any indicators added to, or removed from, collections will also be added or removed from the lists in Management Center.

1. In order to create lists in Management Center, navigate to **Configuration** -> **Shared Objects**.

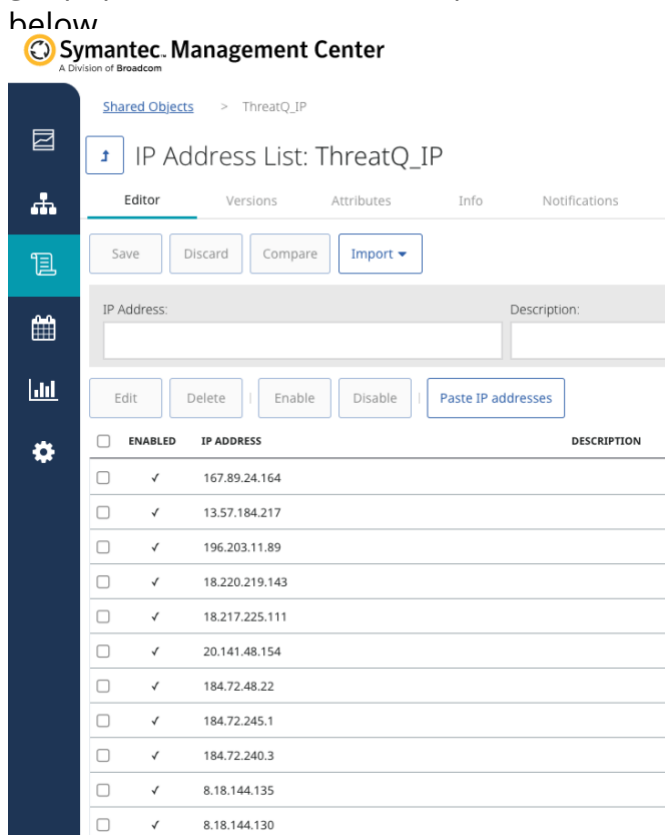


2. Next, click on **Add**, and select **Add Object** from the dropdown menu. From the dropdown on the next window select either **IP Address List** or **URL List**, and follow the next steps to configure the list.



- Copy the name of the list and paste in the appropriate field in the custom connector UI configuration in ThreatQ and execute the integration from the command line. At that point the appropriate list in Management Center will get populated, and when completed it will look similar to the snapshot

below



**Symantec Management Center**  
A Division of Broadcom

Shared Objects > ThreatQ\_IP

IP Address List: ThreatQ\_IP

Editor Versions Attributes Info Notifications

Save Discard Compare Import

IP Address: Description:

Edit Delete Enable Disable Paste IP addresses

ENABLED	IP ADDRESS	DESCRIPTION
<input type="checkbox"/>	✓ 167.89.24.164	
<input type="checkbox"/>	✓ 13.57.184.217	
<input type="checkbox"/>	✓ 196.203.11.89	
<input type="checkbox"/>	✓ 18.220.219.143	
<input type="checkbox"/>	✓ 18.217.225.111	
<input type="checkbox"/>	✓ 20.141.48.154	
<input type="checkbox"/>	✓ 184.72.48.22	
<input type="checkbox"/>	✓ 184.72.245.1	
<input type="checkbox"/>	✓ 184.72.240.3	
<input type="checkbox"/>	✓ 8.18.144.135	
<input type="checkbox"/>	✓ 8.18.144.130	



# Installation

The Management Center connector for ThreatQ is installed from the ThreatQ repository with YUM credentials.

1. Install the connector for ThreatQ by using the following command:

```
sudo pip install tq-conn-symantec-mc
```

Upon successful execution of the pip install, a driver called `tq-conn-symantec-mc` is installed.

2. Once the application has been installed, a directory structure must be created for all configuration, logs and files, using the `mkdir -p` command. See example below:

Creating Integration Directories Example

```
mkdir -p /etc/tq_labs/  
mkdir -p /var/log/tq_labs/
```

3. Perform an initial run using the following command:

```
tq-conn-symantec-mc -c /etc/tq_tabs/ -ll /var/log/tq_labs/ -v3
```

Enter the following parameters when prompted:

Parameter	Description
ThreatQ Host	This is the host of the ThreatQ instance, either the IP Address or Hostname as resolvable by ThreatQ.
Client ID	This is the OAuth id that can be found at Settings Gear → User Management → API details within the user's details.
Email Address	This is the User in the ThreatQ System for integrations.
Password	The password for the above ThreatQ account.
Status	This is the default status for IoCs that are created by this Integration. It is common to set this to "Review", but Organization SOPs should be respected when setting this.

---

**Example Output:**

```
tq-conn-symantec-mc -c /etc/tq_labs/ -ll /var/log/tq_labs/ -v3
ThreatQ Host: <ThreatQ Host IP or Hostname >
Client ID: <ClientID>
E-Mail Address: <EMAIL ADDRESS>
Password: <PASSWORD>
Status: Active
Connector configured. Set information in UI
```

The driver will run once, where it will connect to the ThreatQ instance and install the UI component of the Connector. The feed will be added to the **Labs** category on the integrations management page. You will still need to [configure and enable the connector](#).

# Configuration

**Note:** 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 connector:

1. Navigate to your main ThreatQ page.
2. Select Integrations -> Feeds and Connectors and search for the Symantec Management Center connector

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

3. Enter the following configuration parameter:

Parameter	Description
IP / Hostname	Hostname or IP address of Symantec Management Center
Port (default is 8082)	Port for communicating with the Management Center instance (default is 8082)
Username	Username for logging to Management Center
Password	Password for logging to Management Center
ThreatQ indicator types to send to Management Center	Select the type of ThreatQ indicators to send to Management Center. This is a multiselect field that allows users to select IP, FQDN and URL
Data collection with indicators of compromise send to Management Center	The name of the data collection in the ThreatQ instance with IOCs to send to Management Center. Multiple data collection names should be comma-delimited
Management Center list with IP Addresses	The name of the IP Address list in Management Center to which indicators should be added

Parameter	Description
Management Center list with URLs and FQDNs	The name of the URL and FQDN list in Management Center to which the indicators should be added
Do you want to modify indicators of compromise that contain a port?	ProxySG cannot use indicators of compromise that contain a port. Please chose one of the methods above for modifying the port. Options are (1) Do not modify the indicators, (2) Keep only the portion of the indicators before the port, and (3) Keep the original indicator but remove the port. The default is "Do not modify the indicators"

4. Click on **Save**.
5. Click on the toggle switch, located above the *Additional Information* section, to enable it.

# Usage

This connector is used just like any other custom connector. However, it has one additional CLI argument that you can include for historical imports.

## Basic Usage

```
tq-conn-symantec-mc -c /etc/tq_labs/ -ll /var/log/tq_labs/ -v3
```

## Command Line Arguments

This connector supports the following custom command line arguments:

Argument	Description
<code>-h, --help</code>	Shows this help message and exits.
<code>-ll LOGLOCATION, --loglocation LOGLOCATION</code>	Sets the logging location for the connector. The location should exist and be writable by the current. A special value of 'stdout' means to log to the console (this happens by default).
<code>-c CONFIG, --config CONFIG</code>	This is the location of the configuration file for the connector. This location must be readable and writable by the current user. If no config file path is given, the current directory will be used. This file is also where some information from each run of the connector may be put (last run time, private oauth, etc.)
<code>-v {1,2,3}, --verbosity {1,2,3}</code>	This is the logging verbosity level. <b>Note:</b> 3 means everything.
<code>-hist, --historical</code>	Allows you to set a historical date to import context since <b>Example:</b> [-hist [YYY-MM-DD]]
<code>-n, --name</code>	Change the name of the connector.

---

# Change Log

Version	Details
1.0.0	Initial Release