



ZSCALER AND THREATQUOTIENT DEPLOYMENT GUIDE

Contents

Terms and Acronyms	3
About This Document	5
Zscaler Overview	5
ThreatQuotient Overview	5
Audience	5
Software Versions	5
Request for Comments	5
Zscaler and ThreatQuotient Introduction	6
ZIA Overview	6
ThreatQuotient ThreatQ Platform Overview	7
ThreatQuotient Resources	7
Introduction	8
Prerequisites	8
Integration Dependencies	9
Create Zscaler URL Category	10
Installation	11
Creating a Python 3.6 Virtual Environment	11
Installing the Connector	11
Example Output	12
Configuration	13
Usage	15
Command Line Arguments	15
CRON	15
Limitations	16
Change Log	16
Appendix A: Requesting Zscaler Support	17

Terms and Acronyms

The following table defines acronyms used in this deployment guide. When applicable, a Request for Change (RFC) is included in the Definition column for your reference.

Acronym	Definition
CA	Central Authority (Zscaler)
CSV	Comma-Separated Values
DLP	Data Loss Prevention
DNS	Domain Name Service
DPD	Dead Peer Detection (RFC 3706)
FQDN	Fully Qualified Domain Name
GRE	Generic Routing Encapsulation (RFC2890)
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IKE	Internet Key Exchange (RFC2409)
IoC	Indicators of Compromise
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SaaS	Software as a Service
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
XFF	X-Forwarded-For (RFC7239)
ZPC	Zscaler Posture Control (Zscaler)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

Trademark Notice

© 2024 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

About This Document

The following sections describe the organizations and requirements of this deployment guide.

Zscaler Overview

Zscaler (NASDAQ: [ZS](#)) enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) services create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler delivers its services 100% in the cloud and offers the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions can't match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss. To learn more, see [Zscaler's website](#).

ThreatQuotient Overview

ThreatQuotient improves security operations by fusing together data sources, tools, and teams to accelerate threat detection and response. ThreatQuotient's data-driven security operations platform helps teams prioritize, automate, and collaborate on security incidents. It enables more focused decision making and maximizes limited resources by integrating existing processes and technologies into a unified workspace. To learn more, refer to [ThreatQuotient's website](#).

Audience

This guide is for network administrators, endpoint and IT administrators, and security analysts responsible for deploying, monitoring, and managing enterprise security systems. For additional product and company resources, see:

- [Zscaler Resources](#)
- [ThreatQuotient Resources](#)
- [Appendix A: Requesting Zscaler Support](#)

Software Versions

This document was authored using the latest version of Zscaler software.

Request for Comments

- **For prospects and customers:** Zscaler values reader opinions and experiences. Contact partner-doc-support@zscaler.com to offer feedback or corrections for this guide.
- **For Zscaler employees:** Contact z-bd-sa@zscaler.com to reach the team that validated and authored the integrations in this document.

Zscaler and ThreatQuotient Introduction

Overviews of the Zscaler and ThreatQuotient applications are described in this section.



If you are using this guide to implement a solution at a government agency, some of the content might be different for your deployment. Efforts are made throughout the guide to note where government agencies might need different parameters or input. If you have questions, contact your Zscaler Account team.

ZIA Overview

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of ZIA as a secure internet on-ramp—just make Zscaler your next hop to the internet via one of the following methods:

- Setting up a tunnel (GRE or IPSec) to the closest Zscaler data center (for offices).
- Forwarding traffic via our lightweight Zscaler Client Connector or PAC file (for mobile employees).

No matter where users connect—a coffee shop in Milan, a hotel in Hong Kong, or a VDI instance in South Korea—they get identical protection. ZIA sits between your users and the internet and inspects every transaction inline across multiple security techniques (even within SSL).

You get full protection from web and internet threats. The Zscaler cloud platform supports Cloud Firewall, IPS, Sandboxing, DLP, and Isolation, allowing you to start with the services you need now and activate others as your needs grow.

Zscaler Resources

The following table contains links to Zscaler resources based on general topic areas.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

The following table contains links to Zscaler resources for government agencies.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

ThreatQuotient ThreatQ Platform Overview

The ThreatQ Platform improves the efficiency and effectiveness of existing security operations by fusing together disparate data sources, tools, and teams to accelerate threat detection, investigation, and response. The platform gets data in different formats and languages from different vendors and systems to work together. From there, it focuses on getting the right data to the right systems and teams at the right time to make security operations more data-driven, efficient, and effective.

ThreatQuotient Resources

The following table contains links to ThreatQuotient support resources.

Name	Definition
ThreatQuotient Support	Support Guide

Introduction

This document describes how a ThreatQ admin can export FQDNs and URLs from a Threat Collection to Zscaler's URL blacklist via the Zscaler Blacklist Export integration.

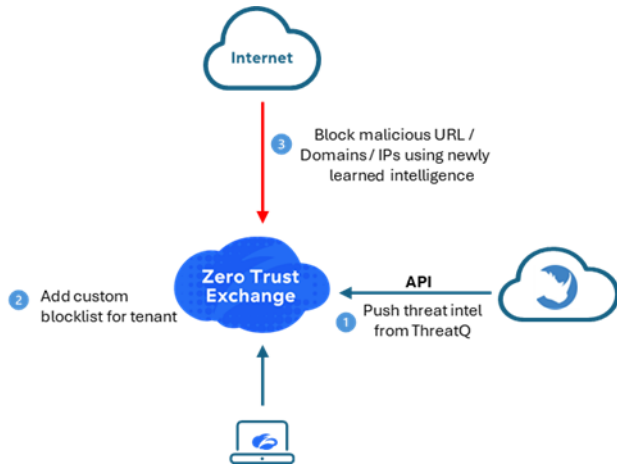


Figure 1. Zscaler and ThreatQuotient integration

ZIA maintains a global database of malicious IPs, Domains, or URLs (i.e., IoCs) and blocks these threats inline in all ZIA customer tenants if pertinent security engines are enabled by ZIA admins. ZIA also maintains per-tenant custom URL lists. You can bring in your own custom threat feeds and populate these URL lists. You can then reference these custom URL lists in ZIA URL policies for granularly controlling end-user access within that ZIA tenant.

ThreatQ expands your defenses with real-time access to global IoCs delivered by ThreatQ. An existing ThreatQ intelligence and ZIA customer can set up this integration to continually push high value threats from the ThreatQ Platform into their ZIA tenant.

Prerequisites

TimeZone

- You should ensure all ThreatQ devices are set to the correct time, time zone, and date (UTC is recommended), 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, enter the following command to list all available time zones in Europe:

```
timedatectl list-timezones | grep Europe
```

```
Europe/Amsterdam
```

```
Europe/Athens
```

```
Europe/Belgrade
```

```
Europe/Berlin
```

Enter the following command, as root, to change the time zone to UTC:

```
timedatectl set-timezone UTC
```


Integration Dependencies



You must install the integration in a Python 3.6 environment.

The following is a list of required dependencies for the integration. These dependencies are downloaded and installed during the installation process. If you are an Air Gapped Data Sync (AGDS) user, or run an instance that cannot connect to network services outside of your infrastructure, you must download and install these dependencies separately as the integration will not download them during the install process.



The items listed in bold are pinned to a specific version. In these cases, you should download the version specified to ensure proper function of the integration.

Dependency	Version	Notes
threatqsdk	>=1.8.2	N/A
threatqcc	>=1.4.1	N/A
python-dateutil	N/A	N/A

Create Zscaler URL Category

To create a Zscaler URL category:

1. Log in to your ZIA Admin Portal.
2. Go to **Administration > URL-Categories**.
3. Add a new URL category with the name `ThreatQ`.
4. In the URL Super Category drop-down menu, select **User-Defined**.
5. Click **Save**.

The screenshot shows the 'Add URL Category' dialog box. It has a title bar 'Add URL Category' with a close button. The main content area is titled 'URL CATEGORY'. It contains the following fields and controls:

- Name:** A text input field containing 'ThreatQ'.
- URL Super Category:** A dropdown menu showing 'User-Defined'.
- Administrator Operational Scope:** A section header.
- Scope Type:** A dropdown menu showing 'Any'.
- Custom URLs:** A section with an 'Add Items' button, a search bar with 'Search...' and a magnifying glass icon, a list item 'gambling.com' with a plus icon, and a pagination bar showing '1-1 of 1' with navigation arrows and a 'Remove' button.
- URLs Retaining Parent Category:** A section with an 'Add Items' button.
- Custom Keywords:** A section with an 'Add Items' button.
- Keywords Retaining Parent Category:** A section with an 'Add Items' button.
- Description:** A text area at the bottom.

At the bottom of the dialog are two buttons: 'Save' and 'Cancel'.

Figure 2. Add URL Category

To learn more, see the ZIA API key in the [ZIA Cloud Service API Developers Guide](#) (government agencies, see [ZIA Cloud Service API Developers Guide](#)).

Installation

The following provides you with steps on installing a Python 3 Virtual Environment and installing the connector.

Creating a Python 3.6 Virtual Environment

Run the following commands to create the virtual environment:

```
mkdir /opt/tqvenv/

sudo yum install -y python36 python36-libs python36-devel python36-pip

python3.6 -m venv /opt/tqvenv/<environment_name>

source /opt/tqvenv/<environment_name>/bin/activate

pip install --upgrade pip

pip install threatqsdk threatqcc

pip install setuptools==59.6.0
```

Installing the Connector



When upgrading users, review the change log for updates to configuration parameters before updating. If there are changes to the configuration file (new/removed parameters), you must first delete the previous version's configuration file before proceeding with the following install steps listed. Failure to delete the previous configuration file results in the connector failing.

1. Go to the ThreatQ Marketplace and download the .whl file for the integration.
2. If not previously done, activate the virtual environment:

```
<> source /opt/tqvenv/<environment_name>/bin/activate
```

3. Transfer the .whl file to the /tmp directory on your ThreatQ instance.
4. Install the connector on your ThreatQ instance:

```
pip install /tmp/tq_conn_zscaler_blacklist_export-<version>-py3-none-any.whl
```

A driver called tq-conn-zscaler-blacklist-export is installed. After installing, a script stub appears in /opt/tqvenv/<environment_name>/bin/tqconn-zscaler-blacklist-export.

5. After you install the application, a directory structure must be created for all configurations, logs, and files using the mkdir -p command. Use the following commands to create the required directories:

```
mkdir -p /etc/tq_labs/

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

6. Perform an initial run using the following command:

```
/opt/tqvenv/<environment_name>/bin/tq-conn-zscaler-blacklistexport -ll /var/log/tq_labs/ -c /etc/tq_labs/ -v3
```

7. 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.
ThreatQ Client ID	This is the OAuth ID that can be found at Settings Gear > User Management > API details within the user's details.
ThreatQ Username	This is the Email Address of the user in the ThreatQ System for integrations.
ThreatQ Password	The password for the ThreatQ account.
Status	This is the default status for objects that are created by this Integration.

Example Output

```
/opt/tqvenv/<environment_name>/bin/tq-conn-zscaler-blacklist-export -ll /var/log/tq_labs/ -c /etc/tq_labs/ -v3
```

ThreatQ Host: <ThreatQ Host IP or Hostname>

ThreatQ Client ID: <ClientID>

ThreatQ Username: <EMAIL ADDRESS>

ThreatQ Password: <PASSWORD>

Status: Review

Connector configured. Set information in UI

You must configure and then enable the connector.

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. Go to your integrations management page in ThreatQ.
2. (Optional) Select the **Labs** option from the **Category** drop-down menu.

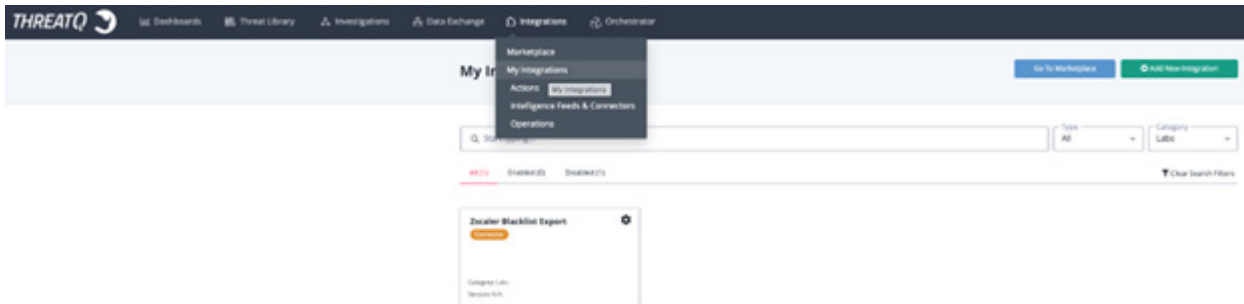



Figure 3. Category drop-down

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

Parameter	Description
API Hostname	The API hostname obtained from the ZIA Admin Portal. Note: You can find this by going to Administration > Cloud Service API Key Management.
Zscaler Username	Your Zscaler username.
Zscaler Password	The password associated with the username.
API Key	Your API Key provided by Zscaler. Note: You can find this by going to Administration > Cloud Service API Key Management.
Threat Library Data Collection Name	Enter the name of the data collection from ThreatQ that you would like to export to Zscaler. Important: The data collection selected should only include URLs and FQDNs.
Category Name	Enter a name for the category you want to export IoCs to.
Category Description	Enter a description for the category you want to export IoCs to.
Verify Host SSL	Enable or disable server certificate validation.



Disabled

Enabled

Additional Information

Integration Type: Connector

Configuration

API Hostname

Enter the API hostname obtained from the Zscaler admin console

Zscaler Username

Enter your Zscaler Cloud (ZIA) username to authenticate.

Zscaler Password

Enter your Zscaler Cloud (ZIA) password to authenticate.

API Key

Enter the API key provided in Zscaler (Administration -> Cloud Service API Security)

Threat Library Data Collection Name

Enter the name of the data collection from ThreatQ that you'd like to export to Zscaler.

Category Name

Enter a name for the category you want to export IOCs to.

Category Description

Enter a description for the category you want to export IOCs to.

☐ Automatically Activate Pending Changes

If enabled, the integration will automatically activate pending policy/category changes.

☒ Verify Host SSL

If checked, use SSL to connect

Save

Figure 4. Zscaler Blacklist Export

- Review any additional settings, make any changes if needed, and click **Save**.
- Click the **Enable** toggle switch located above the **Additional Information** section.

Usage

Use the following command to execute the driver:

```
/opt/tqvenv/<environment_name>/bin/tq-conn-zscaler-blacklistexport -v3 -ll /var/log/tq_labs/ -c /etc/tq_labs/
```

Command Line Arguments

This connector supports the following custom command line arguments.

Parameter	Description
-h, --help	Review all additional options and their descriptions.
-ll LOGLOCATION, --loglocation LOGLOCATION	Sets the logging location for the connector. The location should exist and be writable by the current user. A special value of stdout means to log to the console (this happens by default).
-c CONFIG, --config CONFIG	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 is used. This file is also where some information from each run of the connector might be put (last run time, private oauth, etc.)
-v {1,2,3}, --verbosity {1,2,3}	This is the logging verbosity level where 3 means everything.
-n, --name	(Optional) Name of the connector (this is used to allow users to configure multiple Intelligence Mailbox connector instances on the same TQ box).

CRON

Automatic CRON configuration was removed from this script. To run this script on a recurring basis, use CRON or some other job scheduler. The argument in the CRON script must specify the config and log locations.

Add an entry to your Linux crontab to execute the connector at a recurring interval. Depending on how quickly you need updates, you can run this multiple times a day (no more than once an hour) or a few times a week.

In the following example, the command executes the connector every two hours.

1. Log into your ThreatQ host via a CLI terminal session.
2. Enter the following command:

```
crontab -e
```

This enables the editing of the crontab, using vi. Depending on how often you want the cronjob to run, you must adjust the time to suit the environment.

3. Enter the following commands:

Every 2 Hours Example

```
0 */2 * * * /opt/tqvenv/<environment_name>/bin/tq-connzscaler- blacklist-export -c /etc/tq_labs/ -ll /var/log/tq_labs/ -v3
```

4. Save and exit CRON.

Limitations

Zscaler only allows up to 25,000 custom URLs to be stored in its platform, globally. The integration checks to ensure that the number of URLs in the category does not exceed 25,000.

Change Log

Version 1.1.0

- Resolved an issue where URLs would not be removed from a URL category.
- Added validation to ensure the custom URL quota is not exceeded.
- Resolved an issue where sensitive user fields were not masked.
- Added the ability to automatically activate pending policy changes.
- Added the following new configuration parameters: Category Name, Category Description, and Verify Host SSL.

Version 1.0.0

- Initial release

Appendix A: Requesting Zscaler Support

If you need Zscaler Support to provision certain services or to help troubleshoot configuration and service issues, it is available 24/7/365.

To contact Zscaler Support:

1. Go to **Administration > Settings > Company Profile**.

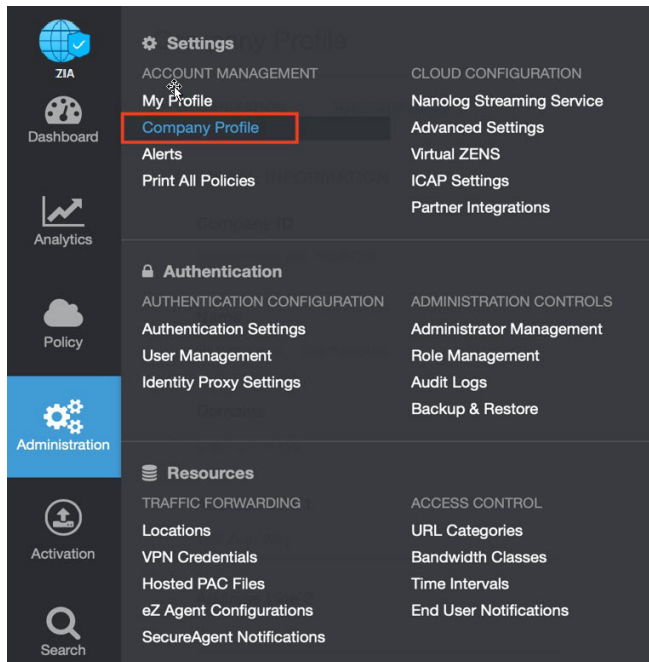


Figure 5. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.

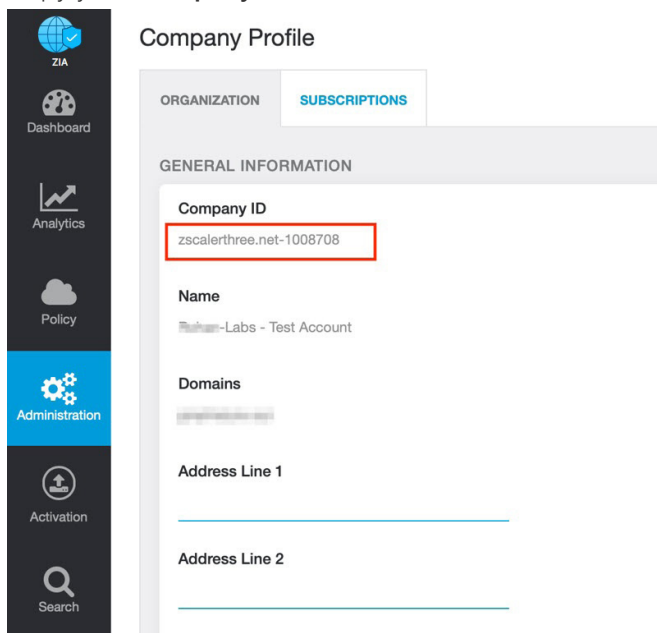


Figure 6. Company ID

3. With your company ID information, you can open a support ticket. Go to **Dashboard** > **Support** > **Submit a Ticket**.

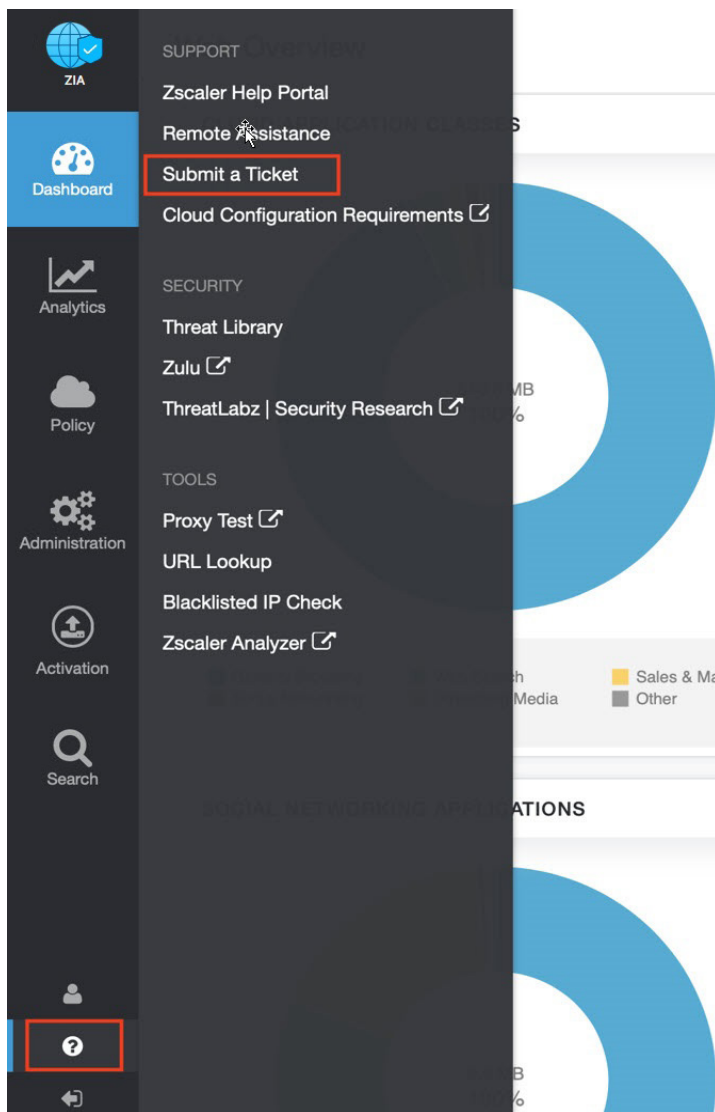


Figure 7. Submit a ticket