



VMware
Carbon Black™

ZSCALER AND VMWARE CARBON BLACK DEPLOYMENT GUIDE

Contents

Terms and Acronyms	4
About This Document	5
Zscaler Overview	5
VMware Overview	5
Audience	5
Software Versions	5
Request for Comments	5
Zscaler and VMware Carbon Black Introduction	6
ZIA Overview	6
ZPA Overview	6
Zscaler Resources	6
VMware Carbon Black Overview	7
VMware Carbon Black Resources	7
Zscaler Integrations with Carbon Black	8
Zscaler Sandbox Connector	8
ZPA Posture Check	9
Use Case 1: Zscaler Sandbox Connector for Carbon Black Cloud	10
Overview	10
Requirements	10
License	10
Support	10

Installation	10
Configuration	11
Carbon Black Configuration	11
Zscaler Configuration	12
Running the Script	13
Examples	13
Use Case 2: ZPA Posture Check	14
Use Case 2: Overview	14
Appendix A: Requesting Zscaler Support	15

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)
CBC	Carbon Black Cloud (VMware)
CSV	Comma-Separated Values
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
IKE	Internet Key Exchange (RFC2409)
IPSec	Internet Protocol Security (RFC2411)
PFS	Perfect Forward Secrecy
PSK	Pre-Share Key
SSL	Secure Socket Layer (RFC6101)
XFF	X-Forwarded-For (RFC7239)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

About This Document

The following sections describe the organizations and requirements detailed in this 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. For more information, see [Zscaler's website](#) or follow Zscaler on Twitter [@zscaler](#).

VMware Overview

VMware (Nasdaq: [VMW](#)) is a leader in cloud-native endpoint protection dedicated to keeping the world safe from cyberattacks. The VMware Carbon Black Cloud consolidates endpoint protection and IT operations into an endpoint protection platform (EPP) that prevents advanced threats, provides actionable insight, and enables businesses of all sizes to simplify operations. By analyzing billions of security events per day across the globe, VMware Carbon Black has key insights into attacker's behaviors, enabling customers to detect, respond to and stop emerging attacks.

With Carbon Black, customers benefit from better protection, better performance, and immediate time-to-value delivered by the cloud-native platform.

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](#)
- [VMware Carbon Black Resources](#)
- [Appendix A: Requesting Zscaler Support](#)

Software Versions

This document was authored using ZIA and Carbon Black Agent version 3.5.0.1756 on Windows 10.

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 VMware Carbon Black Introduction

The following sections describe overviews of the Zscaler and VMware Carbon Black applications.



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, please 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, Intrusion Prevention Systems (IPS), Sandboxing, Data Loss Prevention (DLP), and Browser Isolation, allowing you to start with the services you need now and activate others as your needs grow.

ZPA Overview

ZPA is a cloud service that provides secure remote access to internal applications running on cloud or data center using a zero trust framework. With ZPA, applications are never exposed to the internet, making them completely invisible to unauthorized users. The service enables the applications to connect to users via inside-out connectivity rather than extending the network to them.

ZPA provides a simple, secure, and effective way to access internal applications. Access is based on policies created by the IT administrator within the ZPA Admin Portal and hosted within the Zscaler cloud. On each user device, a piece of software called Zscaler Client Connector is installed. Zscaler Client Connector ensures the user's device posture and extends a secure microtunnel out to the Zscaler cloud when a user attempts to access an internal application.

Zscaler Resources

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

Name	Definition
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
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.
ZIA Test Page	Checks to see name and status of your Zscaler cloud.

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

Name	Definition
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
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.
ZIA Test Page	Checks to see name and status of your Zscaler cloud.

VMware Carbon Black Overview

[VMware Carbon Black Cloud™ Endpoint Standard](#) is a next-generation antivirus (NGAV) and endpoint detection and response (EDR) solution that protects against the full spectrum of modern cyberattacks. Using the VMware Carbon Black Cloud™ universal agent and console, the solution applies behavioral analytics to endpoint events to streamline detection, prevention, and response to cyberattacks.

The VMware Carbon Black platform provides:

- Protection from known and emerging attacks and in-product alerts on the latest threats
- Prioritized alerts, attack chain visualizations, and in-product response capabilities
- Flexible security policies
- A single agent and cloud-native platform
- An active and engaged user community of internal security experts and peers

VMware Carbon Black Resources

The following table contains links to VMware Carbon Black support resources.

Name	Definition
Carbon Black Threat Hunter API Documentation	A list of Threat Hunter actions available in the Enterprise EDR console programmatically via APIs.
Carbon Black Defense API Documentation	A list of Defense actions available in the Enterprise EDR console programmatically via APIs.
Carbon Black Support Portal	Tap into the knowledge of thousands of security professionals around the globe.
Identify Cloud Service Hostname	List the URLs used to access the APIs.
Network Containment/Quarantine	What happens when a device is placed in Quarantine.
Carbon Black Blog	VMware security blog.
Carbon Black Zscaler Connector Page	GitHub repository for the Zscaler Sandbox Connector.
Carbon Black GitHub Page	GitHub repository for VMware Carbon Black.
Carbon Black Community page	A VMware Carbon Black user exchange for sharing best practices and threat intelligence.

Zscaler Integrations with Carbon Black

Integrating the Zscaler and VMware Carbon Black solutions enables cross-platform workflows that reduce dwell time and mean-time-to-remediate (MTTR).

Zscaler Sandbox Connector

Zscaler scans all files before they reach the endpoint if they come through the network, but what happens when a file comes in via other connections? How do you find more information about files that landed on the end host prior to Carbon Black sensor installation?

The Zscaler connector scans for any CBC Enterprise Standard (formerly CB Defense) events or CBC Enterprise EDR (formerly CB Threat Hunter) processes. After pulling the processes, the Zscaler connector checks all the unique hashes against a database of pre-screened files. If the file is not known, the connector sends a request to Zscaler's ZIA Sandbox to see if it has any information on it. Action is taken if it does, or if the file is known to be bad from the local database.

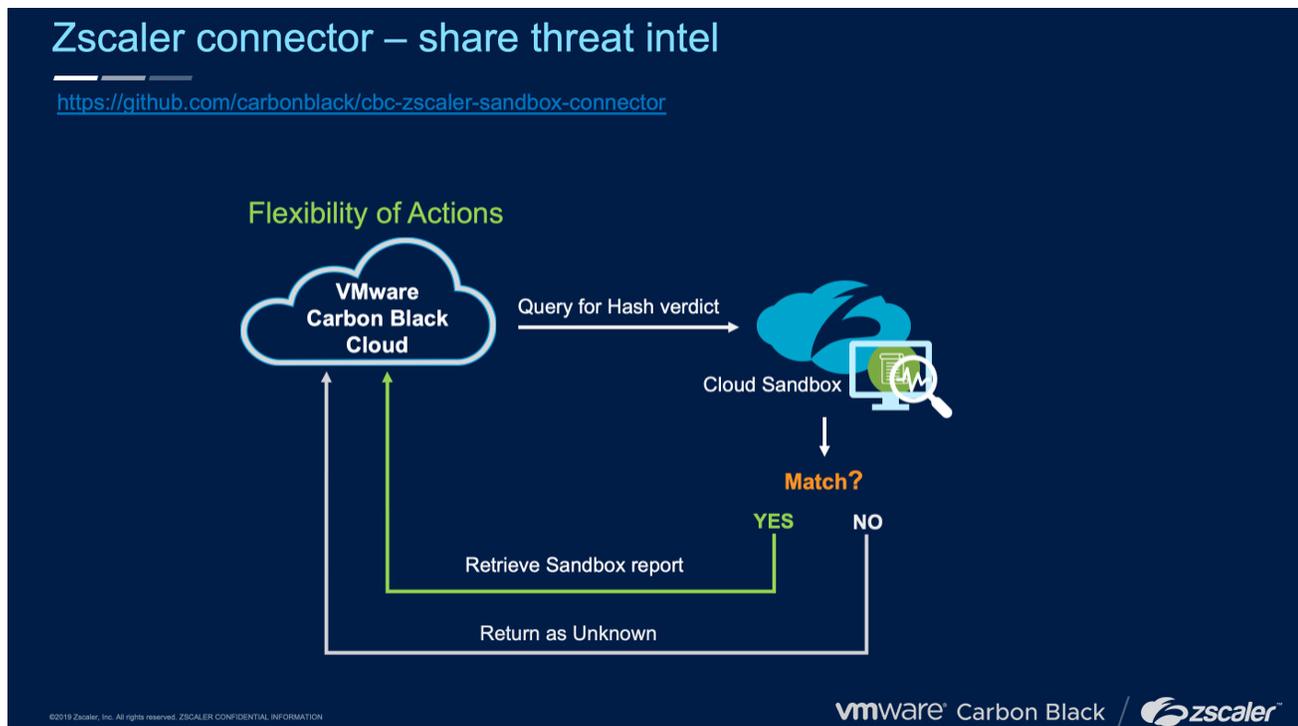


Figure 1. Zscaler Sandbox Connector overview

ZPA Posture Check

A device's "posture profile" is a set of criteria that the device must meet to access applications using ZPA. You can select a device posture profile when configuring [access policies](#) (government agencies, see [access policies](#)) in the ZPA Admin Portal. However, you must [configure these device posture profiles](#) (government agencies, see [configure these device posture profiles](#)) in the Zscaler Client Connector.

ZPA can have Zscaler Client Connector confirm the presence of a running Carbon Black agent and allow access to sensitive applications only if this posture check passes.

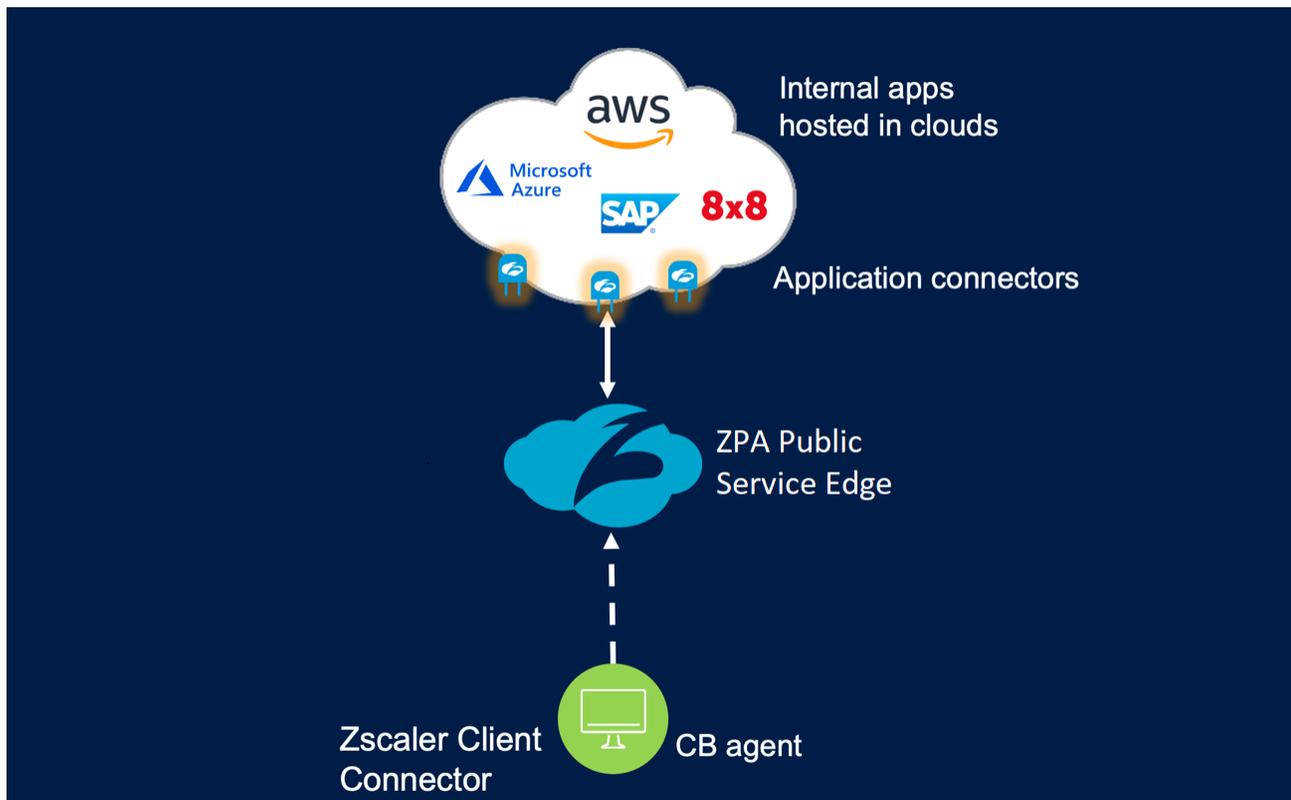


Figure 2. ZPA posture check overview

Use Case 1: Zscaler Sandbox Connector for Carbon Black Cloud

This integration between Zscaler's ZIA Sandbox, VMware CBC Endpoint Standard, and CBC Enterprise EDR lets Zscaler scan all files before they reach the endpoint even if the files don't come through the network or prior to sensor installation.

Overview

The connector scans for any CBC Enterprise Standard events or CBC Enterprise EDR processes. After pulling the processes, the connector checks all the unique hashes against a database of files that have been checked in the past. If the file is not known, the connector requests if Zscaler's ZIA Sandbox has any information on it. If it does, or if the file is known bad from the local database, action is taken.

Action options consist of:

- Adding to a CBC Enterprise EDR Watchlist Feed
- Passing the event and sandbox report to a webhook
- Running a script
- Isolating the endpoint
- Moving the endpoint into a policy

Requirements

- Python 3.x with sqlite3
- VMware CBC Endpoint Standard or Enterprise EDR
- Zscaler ZIA with licensed Sandbox

License

Use of the Carbon Black API is governed by the license found in the [GitHub LICENSE](#) section.

Support

1. View all API and integration offerings on the Developer Network along with reference documentation, video tutorials, and how-to guides.
2. Use the [Developer Community Forum](#) to discuss issues and get answers from other API developers in the Carbon Black Community.
3. Create a GitHub issue for bugs and change requests.

Installation

Clone the repository into a local folder:

```
git clone git@github.com:carbonblack/cbc-zscaler-sandbox-connector.git
```

Install the requirements:

```
pip install -r requirements.txt
```

Edit the **config.conf** file and update with your configuration.

Configuration

You can find all the configurable settings for the integration in [config.conf](#).

Carbon Black Configuration

Create one API access level and three API keys.

Custom Access Level Permissions

Category	Permission Name	.Notation Name	Create	Read	Update	Delete	Execute
Custom Detections	Feeds	org.feeds	X	X	X		
Device	General Information	device		X			
Device	Policy assignment	device.policy			X		
Search	Events	org.search.events	X	X			
Unified Binary Store	SHA-256	ubs.org.sha256		X			

Access Levels (API key type)

1. API
2. Custom [Select your Custom Access Level]
3. Live Response (optional, used in action.py)

Find the Organization Key in the upper-left of the **Settings > API Keys** page.

Carbon Black	Configure Carbon Black Cloud
url	URL of CBC instance
org_key	Org Key
api_id	API ID
api_key	API Secret Key
custom_api_id	Custom API ID
custom_api_key	Custom API Secret Key
lr_api_id	LiveResponse API ID
lr_api_key	LiveResponse API Secret Key
cbd_enabled	Enable CBC Endpoint Standard? [true/false]
cbth_enabled	Enable CBC Enterprise EDR? [true/false]
cbd_timespan	Specify how far back to pull CBC Endpoint Standard events [3h, 1d, 1w, 2w, 1m, all]
reputation_filter	Filter CBC Enterprise EDR processes by reputation. Default is NOT_LISTED

Zscaler Configuration

Find the API key in **Administration > API Key Management**.

Zscaler	Configure ZIA
url	URL for Zscaler ZIA
api_key	API Key
username	Login Username
password	Login Password
bad_types	Bad Types in Sandbox Reports [MALICIOUS,SUSPICIOUS, BENIGN]

Python 3.x ships with SQLite. If you don't have SQLite, you must install it.

```
pip install sqlite3).
```

Sqlite3	Configure sqlite3
Filename	Filename of the sqlite3 database.

When a file is detected that matches the types defined in the **Zscaler > bad_types** configuration, actions are triggered. By default, all actions are disabled.

watchlist

When this field is populated, a Threat Feed is either created or updated with a report of the detected file. The report contains a short description, some tags, and the severity from the Zscaler Sandbox report. If indicators already exist, they are not duplicated.

webhook

When this field is populated, a POST request is made to the HTTP endpoint provided in the value of the configuration. The body of the POST request is an array of the Carbon Black event or process and the Zscaler report ([cb_event, zs_report]). Duplication might occur on this action.

script

Populating this field executes a script at the path and with the parameters provided in the value of the configuration. There are three find/replace that occur ({device_id}, {command}, {argument}).

Populating this field executes a script at the path and with the parameters provided in the value of the configuration. Find/replace occurs for: ({device_id}, {command}, {argument}).

The [config.conf](#) file includes an example that executes a provided [action.py](#). The action.py kills the triggered process.

isolate

When this field is populated with "true," the device is isolated.

policy

When this field is populated, the device is moved to the policy named with the configuration value. This is not the policy ID.

Actions	Configure Actions
watchlist	Name of watchlist to populate.
webhook	URL to POST a JSON object of the event and sandbox report.
script	A script to execute.
isolate	Isolate the endpoint.
Policy	Policy to move offending devices.

Running the Script

The script includes the following CLI options:

Arguments	Actions
-h, --help	Show this help message and exit.
--last_pull	Set the last pull time in ISO8601 format.
--cbd	Pull CBD events.
--cbth	Pull CBTH processes.

The **--last_pull** option pulls all Cloud EDR processes and then updates the **last_pull** value stored in the database with a new timestamp.

The **--cbd** and **--cbth** options pulls the NGAV events and Cloud EDR processes respectively, even if they are disabled in the configuration file.

Examples

Typical usage:

```
python app.py
```

Specify Cloud EDR start date:

```
python app.py --last_pull 2020-01-01T12:34:56.000Z
```

Use Case 2: ZPA Posture Check

The device posture profile is a set of criteria that a device must meet to access applications with ZPA. You can select a device posture profile when configuring [access policies](#) (government agencies, see [access policies](#)) in the ZPA Admin Portal. However, you must configure [device posture profiles](#) (government agencies, see [device posture profiles](#)) in the Zscaler Client Connector.

Use Case 2: Overview

This is an integration between ZPA platform and Carbon Black.

Within ZPA, [policies](#) (government agencies, see [policies](#)) is set up that control access to sensitive applications based on certain endpoint posture assessments.

In this case, the Zscaler Client Connector checks for the presence of a running Carbon Black agent on the endpoint. This constitutes the [posture check](#) (government agencies, see [posture check](#)) that is tied to access policies.

This posture check is supported for laptops and desktops running macOS or Windows.

The posture check is only applicable if you're using Zscaler Client Connector version 2.1.2 or later. If you choose Windows, macOS, or Linux, select **Detect Carbon Black** for the **Posture Type**. The user must have Carbon Black running on the device to pass the posture validation check.

The screenshot shows the 'DEVICE POSTURE CONFIGURATION' interface in ZPA. Under the 'PLATFORM' section, there are four toggle switches: 'Windows' (checked, green), 'macOS' (checked, green), 'Android' (unchecked, red with 'X'), and 'iOS' (unchecked, red with 'X'). Below this, the 'DEVICE POSTURE CONFIGURATION' section has a 'Posture Type' dropdown menu with a question mark icon, currently set to 'Detect Carbon Black'.

Figure 3. Device posture configuration in ZPA

The following signer certificate matching thumbprints are supported for the Carbon Black RepMgr.exe executable.

Client Connector 3.5 and later	Client Connector 3.4 and earlier
4d66d506976bde36ae01ab3335d501bec9fb9837	4d66d506976bde36ae01ab3335d501bec9fb9837
f855a4a29ecefdd9ad04384ae3a099aff61d717f	
9033309926659b4346c496d44407d39e0487868c	
d9665dc3abce52eaf263dad3412c7cedb9e79b9d	

Appendix A: Requesting Zscaler Support

You might need Zscaler Support for provisioning certain services, or to help troubleshoot configuration and service issues. Zscaler Support is available 24/7/365.

To contact Zscaler Support:

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

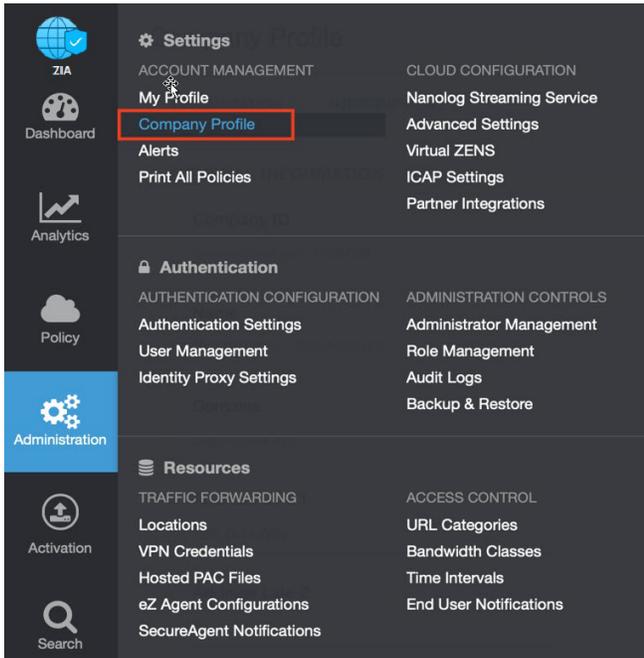


Figure 4. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.

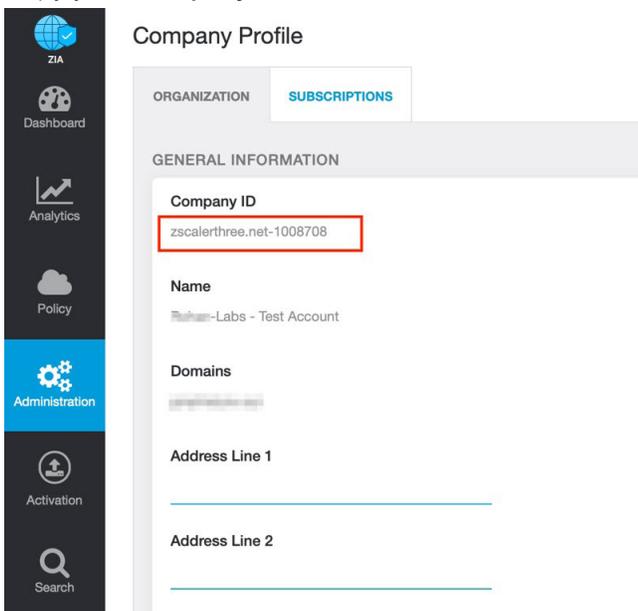


Figure 5. Company ID

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

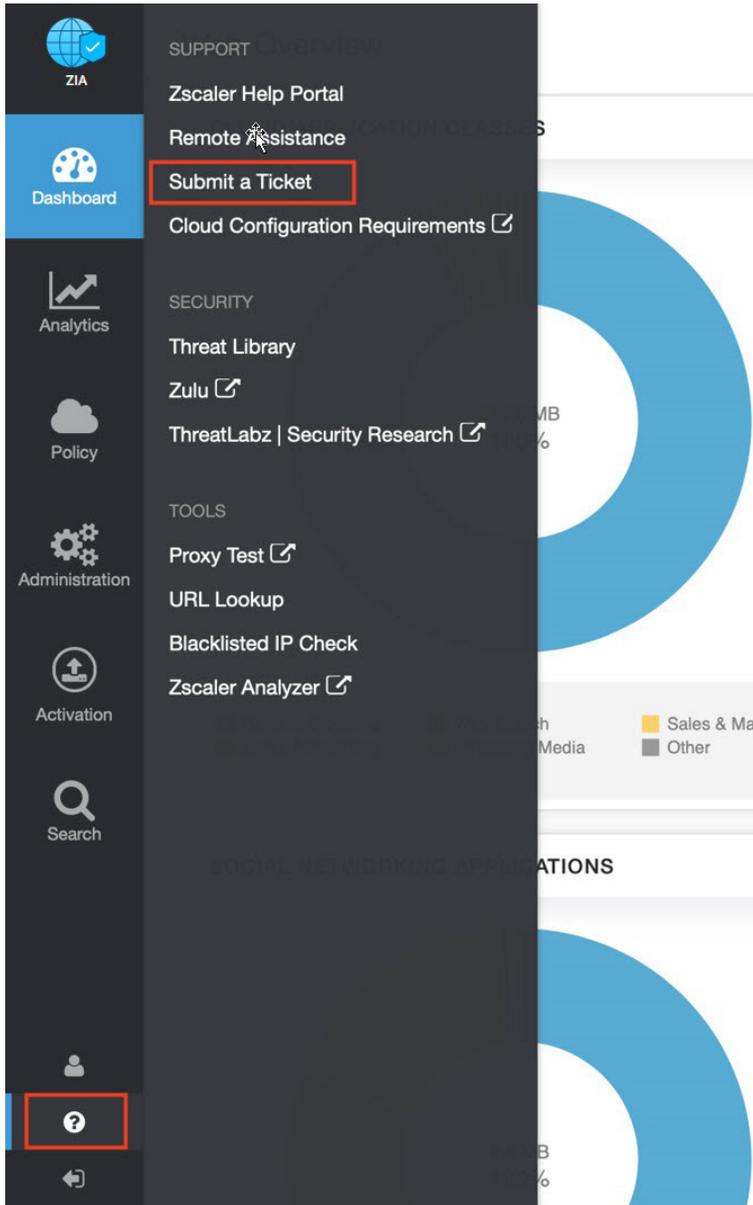


Figure 6. Submit a Ticket