ZSCALER AND VMWARE CARBON BLACK DEPLOYMENT GUIDE

APRIL 2022, VERSION 1.1

BUSINESS DEVELOPMENT GUIDE

Contents

©2022 Zscaler, Inc. All rights reserved.

©2022 Zscaler, Inc. All rights reserved.

Terms and Acronyms

Acronym	Definition
CA	Central Authority (Zscaler)
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)
ZEN	Zscaler Enforcement Node (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

About This Document

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 on Zscaler, visit www.zscaler.com 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, please refer to:

- Appendix A: Requesting Zscaler Support
- Zscaler Resources
- VMware Carbon Black Resources

©2022 Zscaler, Inc. All rights reserved.

Software Versions

This document was authored using Zscaler Internet Access and Carbon Black Agent version 3.5.0.1756 on Windows 7 and Windows 10.

Request for Comments

- **For Prospects and Customers**: We value reader opinions and experiences. Please contact us at 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

Zscaler Overview

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

Zscaler Internet Access (ZIA) Overview

Zscaler Internet Access (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, CASB, and Browser 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.
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.

©2022 Zscaler, Inc. All rights reserved.

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	What URLs are used to access the APIs?
Network Containment/Quarantine	What happens when a Device is placed in Quarantine?
Carbon Black Blog	VMware Carbon Black security blog.
Carbon Black Zscaler Connector Page	GitHub repository for the Zscaler 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.

©2022 Zscaler, Inc. All rights reserved.

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).

Use Case 1: 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 we find more information about files that landed on the end host prior to CB 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, it checks all the unique hashes against a database of pre-screened files. If the file is not known, a request is sent 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.

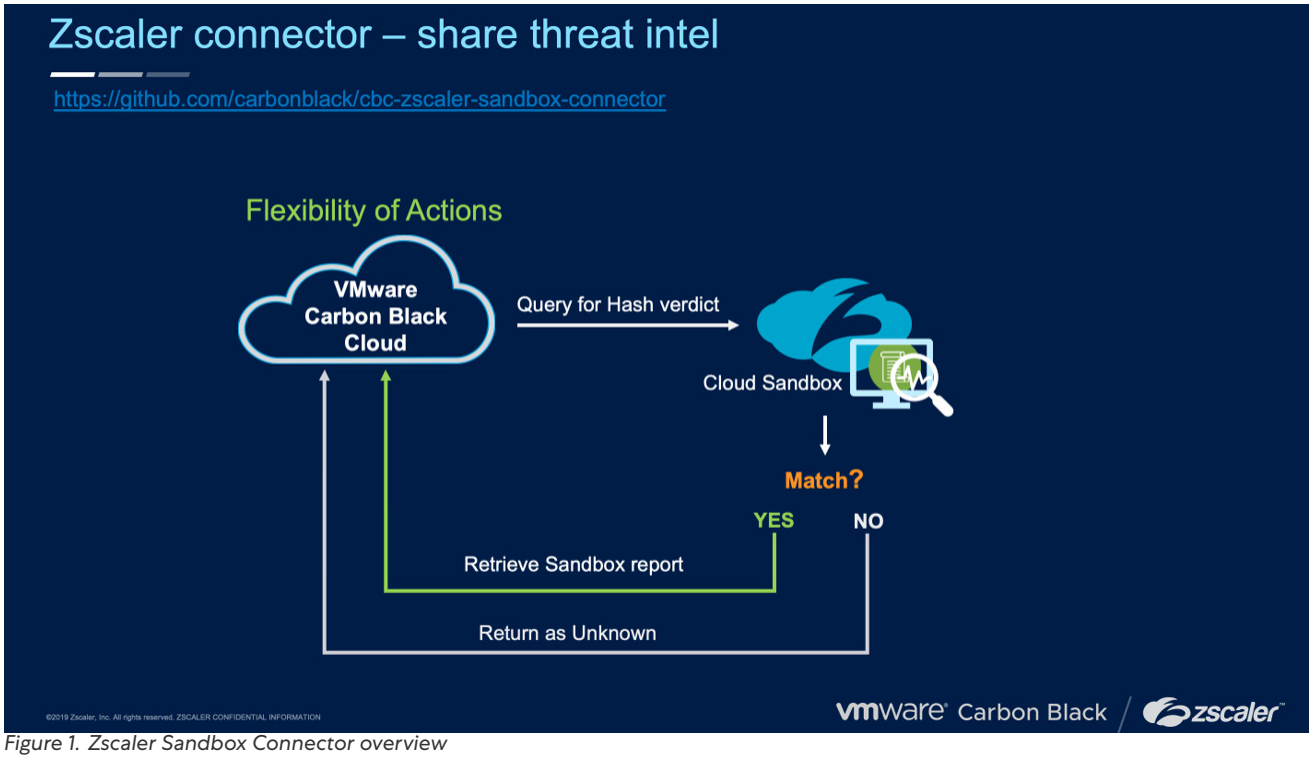

Figure 1. Zscaler Sandbox Connector overview

©2022 Zscaler, Inc. All rights reserved.

Use Case 2: ZPA Posture Check

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

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

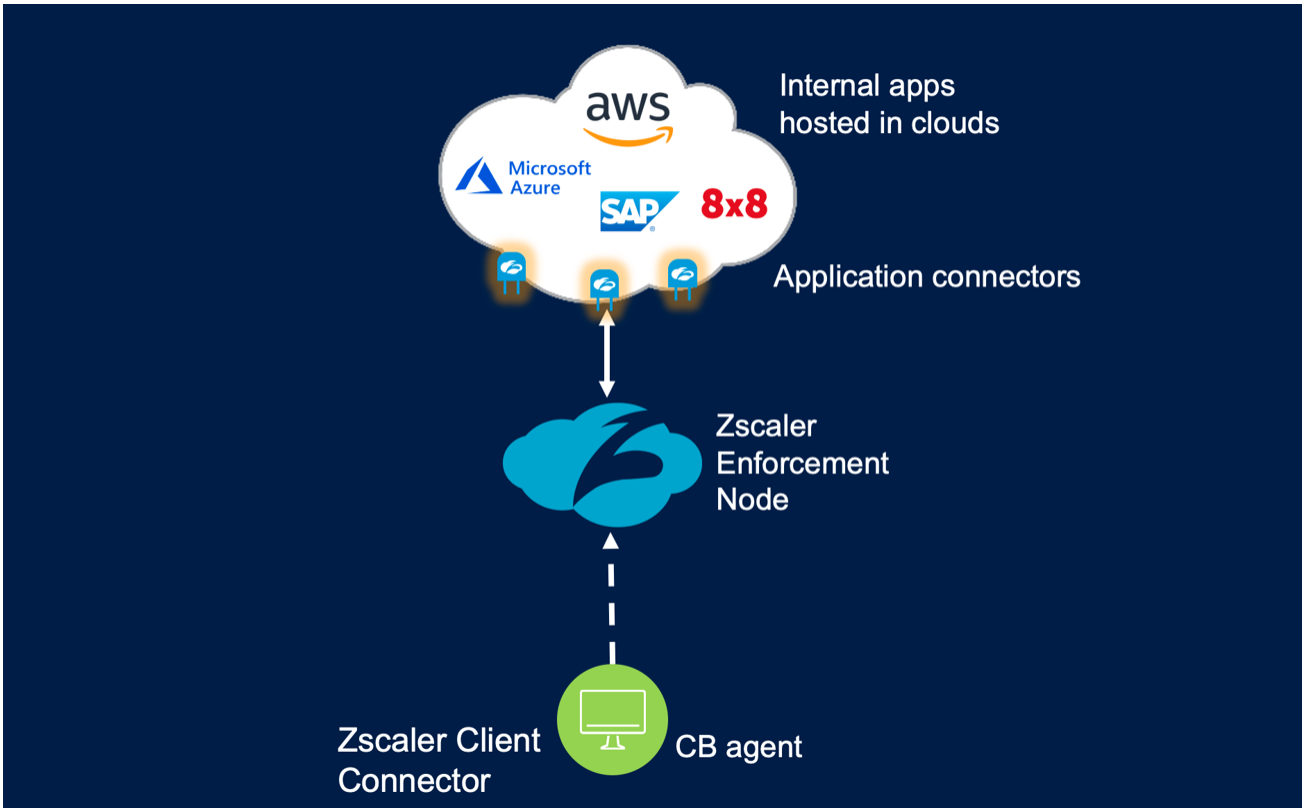

Figure 2. ZPA posture check overview

©2022 Zscaler, Inc. All rights reserved.

Use Case 1: Zscaler Sandbox Connector for Carbon Black Cloud

This integration between **Zscaler's ZIA Sandbox**, **VMware Carbon Black Cloud (CBC) Endpoint Standard (formerly CB Defense)**, and **CBC Enterprise EDR (formerly CB Threat Hunter)** lets Zscaler scan all files before they reach the endpoint even if they 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 it checks all the unique hashes against a database of files that have been checked in the past. If the file is not known, it 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 Carbon Black Cloud 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. Formal Carbon Black Support coming with v1.0.

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.

©2022 Zscaler, Inc. All rights reserved.

Configuration

All the configurable settings for the integration can be found in **config.conf**.

Carbon Black Configuration

You need to 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)

The Organization Key can be found 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	How far back to pull CB Defense events? [3h, 1d, 1w, 2w,1m, all]
reputation_filter	Filter CB ThreatHunter processes by reputation. Default is NOT_LISTED

©2022 Zscaler, Inc. All rights reserved.

Zscaler Configuration

The API key can be found 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. [MALICOUS,SUSPICIOUS, BENIGN]

Python 3.x ships with sqlite. If for some reason you don't have sqlite, you need to 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. Indicators are not duplicated if they already exist.

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 may 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}).

An example is provided in the **config.conf**. This executes the provided example **action.py**, which 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

©2022 Zscaler, Inc. All rights reserved.

Running the Script

The script has 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 overwrites the **last_pull** value stored in the database and pulls all of the Cloud EDR processes since that time.

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
```

©2022 Zscaler, Inc. All rights reserved.

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** in the ZPA Admin Portal. However, you must configure **device posture profiles** in the Zscaler Client Connector.

Use Case 2: Overview

This is an integration between Zscaler Private Access (ZPA) platform and Carbon Black.

Within ZPA, **policies** can be setup 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** that can be tied to access policies.

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

This 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.

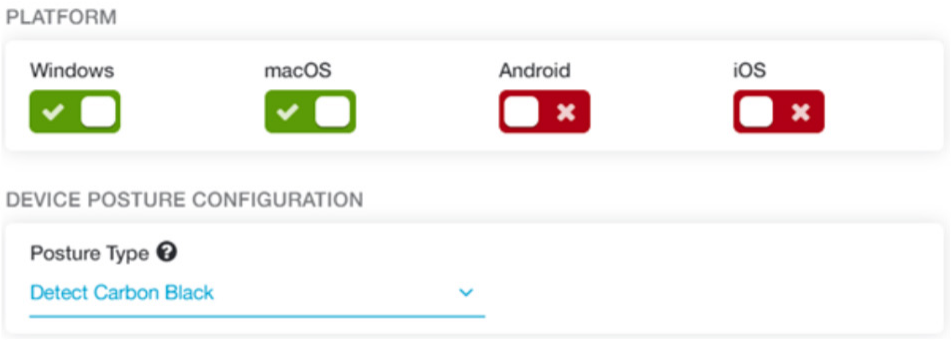

Figure 3. Device posture configuration

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

Client Connector 3.5 and above	Client Connector 3.4 and below
4d66d506976bde36ae01ab3335d501bec9fb9837	4d66d506976bde36ae01ab3335d501bec9fb9837
f855a4a29ecefdd9ad04384ae3a099aff61d717f	
9033309926659b4346c496d44407d39e0487868c	
d9665dc3abce52eaf263dad3412c7cedb9e79b9d	

©2022 Zscaler, Inc. All rights reserved.

Appendix A: Requesting Zscaler Support

Gather Support Information

You might need Zscaler support for provisioning certain services, or to help troubleshoot configuration and service issues. Zscaler support is available 24/7 hours a day, year-round. To contact Zscaler support, select **Administration** > **Settings** > **Company profile**.

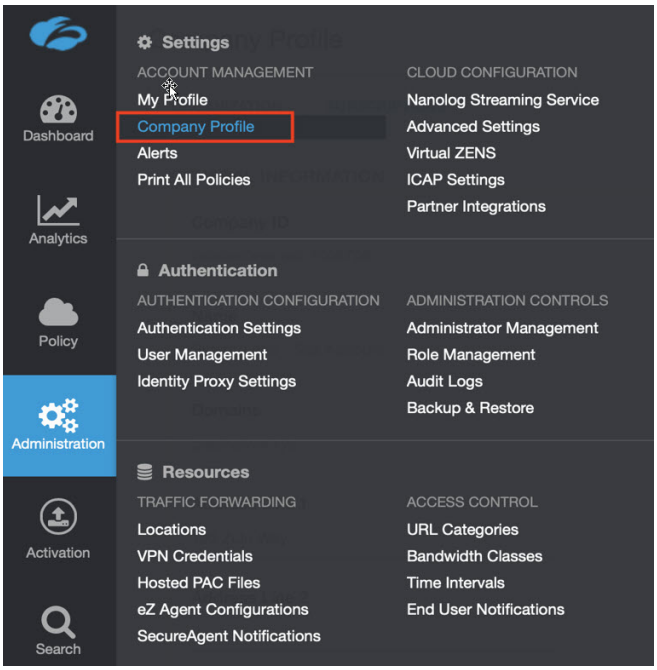

Figure 4. Collecting details to open support case with Zscaler TAC

Save Company ID

Copy your Company ID.

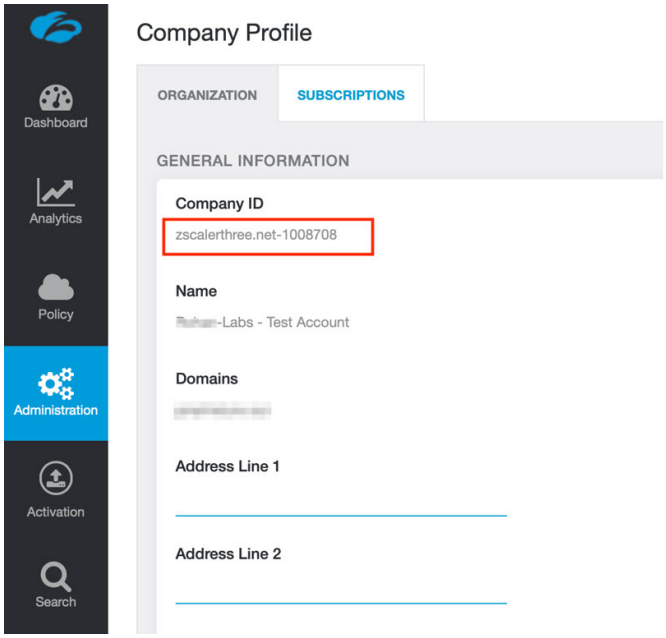

Figure 5. Company ID

©2022 Zscaler, Inc. All rights reserved.

Enter Support Section

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

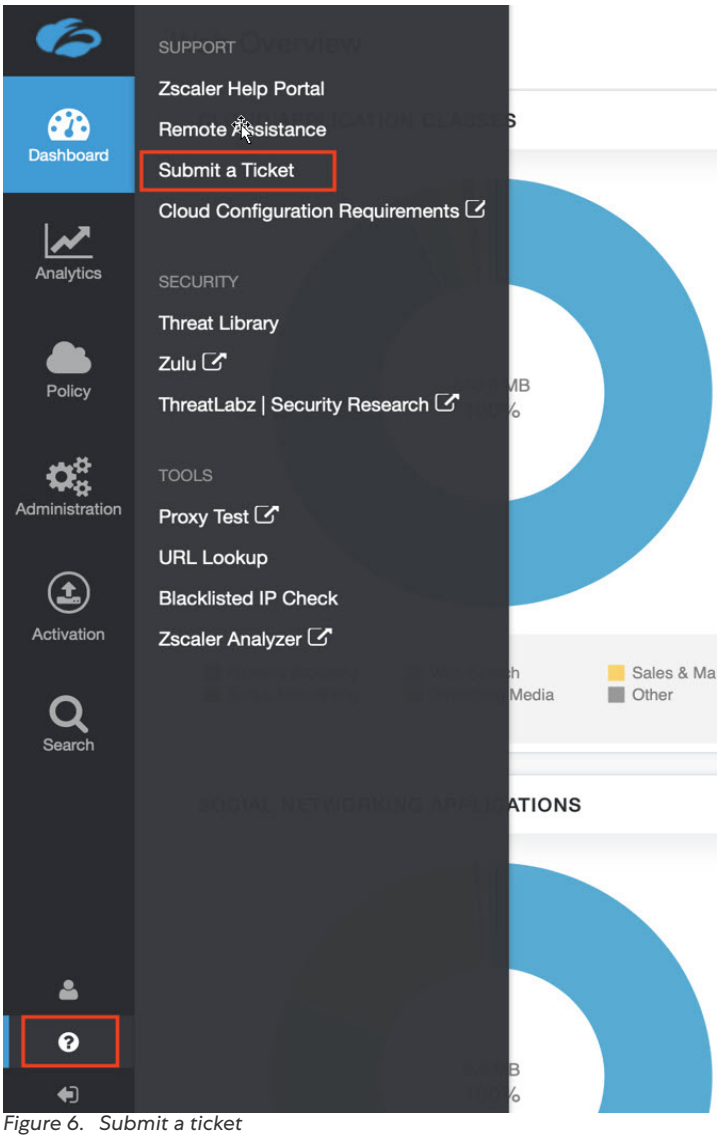

Figure 6. Submit a ticket

©2022 Zscaler, Inc. All rights reserved.