

ZSCALER AND PORTAL26 DEPLOYMENT GUIDE

Contents

Terms and Acronyms	3
About This Document	5
Zscaler Overview	5
Portal26 Overview	5
Audience	5
Software Versions	5
Request for Comments	5
Zscaler and Portal26 Introduction	6
ZIA Overview	6
ZPA Overview	6
Portal26 GenAI Overview	7
Portal26 Resources	7
Portal26 and Zscaler AI TRiSM Integration	8
Portal26 Extends Your Zscaler Deployment	8
Onboarding Zscaler	9
Adding Incident Receiver	10
Configuring DLP Policy Rules with Content Inspection	11
Defining DLP Inline Policy Rules with Content Inspection	12
Defining DLP Inline Policy Rules Without Content Inspection	14
Appendix A: Requesting Zscaler Support	16

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)
GRE	Generic Routing Encapsulation (RFC2890)
ICAP	Internet Content Adaptation Protocol
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IKE	Internet Key Exchange (RFC2409)
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
VM	Virtual Machine
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](#).

Portal26 Overview

Portal26 is the platform to help you embrace and accelerate the competitive promise of Generative AI (GenAI) throughout the enterprise. Portal26 is the AI TRISM platform to help you embrace and accelerate the competitive promise of GenAI throughout the enterprise. To learn more, refer to [Portal26.ai](#).

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](#)
- [Portal26 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 Portal26 Introduction

Overviews of the Zscaler and Portal26 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.

ZPA Overview

ZPA is a cloud service that provides secure remote access to internal applications running on a 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, 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.

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.

Portal26 GenAI Overview

Portal26 GenAI is Portal26's Governance Platform that lets you manage enterprise-wide GenAI Risks by gaining visibility into GenAI usage, implementing security and privacy guardrails, enforcing GenAI policy, and enabling GenAI monitoring and forensics. Portal26 GenAI includes a dashboard that provides visibility into GenAI usage and its risks.

Portal26 Resources

The following table contains links to Portal26 support resources.

Name	Definition
Portal26 Documentation	Online documentation for Portal26 GenAI.
Portal26 Zscaler Onboarding	Online documentation specific to Zscaler onboarding

Portal26 and Zscaler AI TRiSM Integration

The Portal26 and Zscaler integration enables trust, security, and risk management for AI usage within the enterprise. Portal26 is featured in Gartner's most recent 2023 Market Guide for AI TRiSM (which stands for AI Trust Security, and Risk Management).

Portal26 Extends Your Zscaler Deployment

Portal26 builds on top of Zscaler's industry leading platform and enables enterprises to fearlessly adopt GenAI by adding the following:

- AI usage analytics with tracking and historical trending
- Prompt monitoring and analytics with prompt audit/forensics
- GenAI policy distribution and tracking
- AI risk measurement and mitigation
- Strong second line of defense for GenAI DLP with real-time analysis of DLP performance
- AI-driven data exfiltration detection and related forensics on historical usage
- Departmental level reporting for actionable insights
- Employee education triggered by AI usage and behavior patterns
- Compliance, audit, and forensics for GenAI-based activity
- AI-driven prompt intelligence
- AI-driven data security and exfiltration analysis
- Executive reporting and dashboards

The following diagram shows a conceptualization of the integration.

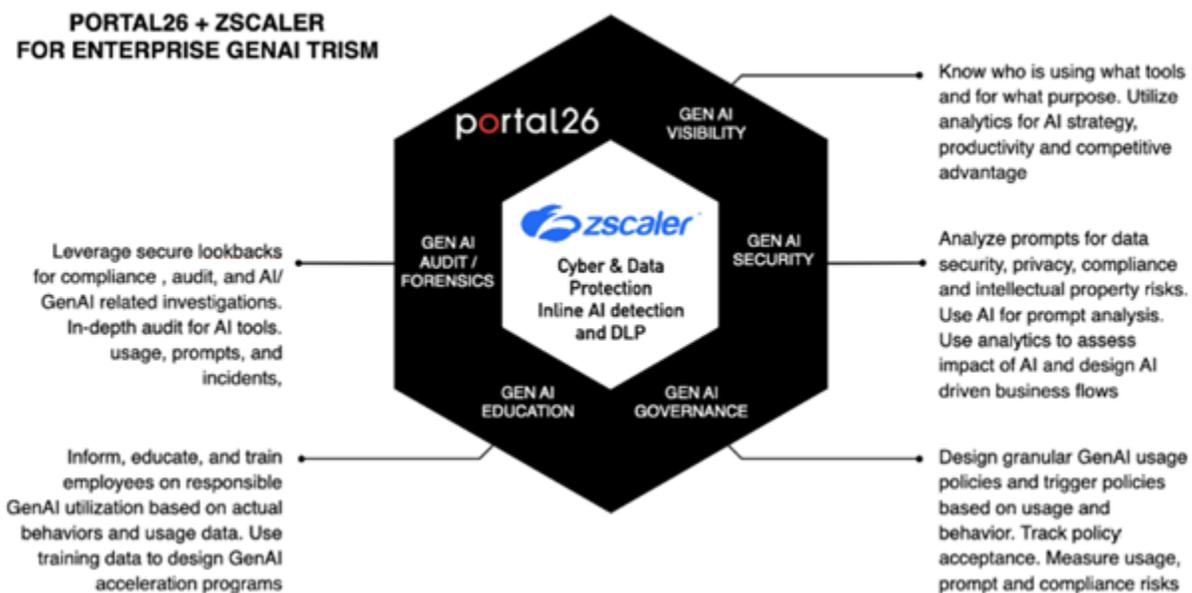


Figure 1. Portal26 and Zscaler integration

Onboarding Zscaler

As a tool specializing in providing insights into the usage patterns of GenAI tools such as ChatGPT and Google Gemini, Portal26's primary focus is on understanding and analyzing the interactions of employees with these tools. The objective lies in offering valuable observations related to user engagement and behavior.

To achieve this goal, Portal26 facilitates user data acquisition through approaches tailored to prevalent network security solutions. For organizations using Zscaler, Portal26 enables the seamless transmission of prompt data through ZIA to an incident receiver hosted by Portal26. This process ensures a secure and streamlined transfer of data, allowing Portal26 to delve into user interactions effectively.

In the following example, one tenant uses Azure AD and the other uses Okta as identity providers. The third user is registered directly at the GenAI web site (not using SSO).

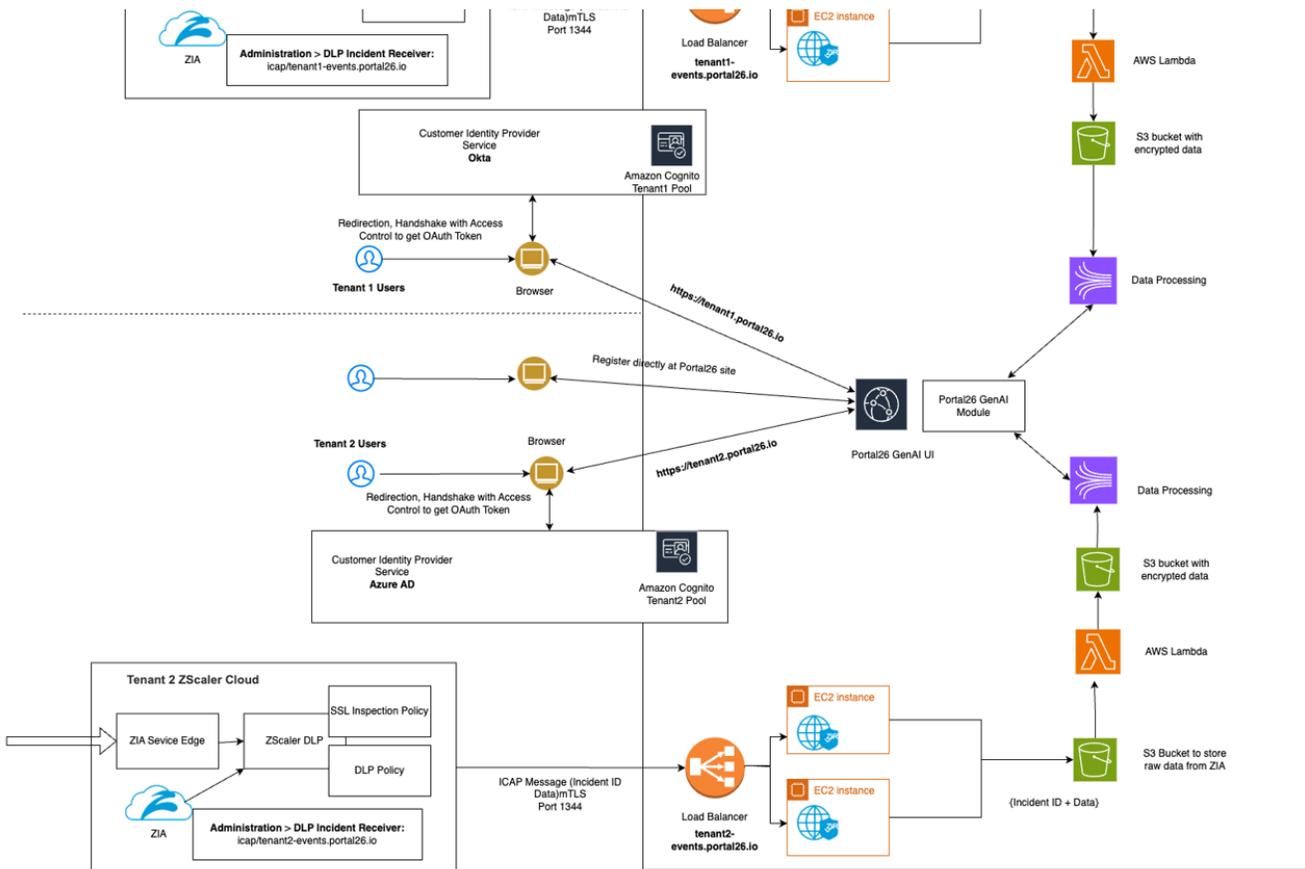


Figure 2. Zscaler and Portal26 GenAI architecture



Guidance in the Zscaler and Portal26 Deployment Guide assumes ZIA is deployed and configured for SSL inspection on the AI and ML Applications URL Categories.

Portal26 GenAI provides a managed solution where the incident receiver is deployed in the Portal26 cloud to provide data telemetry into Portal26 GenAI. The incident receiver will be deployed and managed by Portal26 the configuration and policy is the responsibility of the Customer.

The Zscaler Incident Receiver is a tool that allows you to receive information about DLP policy violations securely. It can run on an EC2 instance on Amazon Web Services (AWS), on an Azure VM, or on-premises. The Zscaler service sends information about policy violations via ICAP to the Incident Receiver. This tool sends the policy-violating content and a JSON file containing the metadata for the inline web and CASB DLP policy scan (e.g., the URL, Collaborators, DLP dictionaries, DLP engines, etc.).

The following steps are guidance for configuration and policy definition in ZIA for both incident receiver and DLP policy.

Adding Incident Receiver

In the ZIA Admin Portal, add an incident receiver:

1. Go to **Administration > DLP Incident Receiver**.
2. Click the **Zscaler Incident Receiver** tab.
3. Locate the **Zscaler Incident Receiver** in the table and click **Edit**. The **Edit Incident Receiver** window appears.
4. In the **Edit Incident Receiver** window:
 - a. Change the **Incident Receiver Name**.
 - b. Change the **Status** to **Enabled** or **Disabled**.
 - c. For **IP Address**, change the incident receiver URI. If you change the URI, make sure you update the incident receiver VM. To learn more, see [Configuring the Zscaler Incident Receiver](#) (government agencies, see [Configuring the Zscaler Incident Receiver](#)).
 - d. Download or regenerate the Certificate. If you regenerate the certificate, make sure you update the incident receiver VM with the new file. To learn more, see [Configuring the Zscaler Incident Receiver](#) (government agencies, see [Configuring the Zscaler Incident Receiver](#)).
 - e. If you want to remove the incident receiver, click **Delete**.
5. Click **Save** and activate the change.

Figure 3. Zscaler Incident Receiver configuration

Configuring DLP Policy Rules with Content Inspection

You can use Zscaler's DLP engines to detect data, allow, or block transactions, and notify your organization's auditor when a user's transaction triggers a DLP rule. For the Zscaler and Portal26 deployment, your organization forwards information about transactions that trigger DLP policy to Portal26 via secure ICAP. However, Zscaler does not take ICAP responses from Portal26.

Zscaler only monitors or blocks content according to the policy you configure, then forwards information about transactions so that your organization can take necessary remediation steps.



The Zscaler DLP engines support files up to 400 MB and can scan the first 100 MB of the extracted text. The maximum size also applies to files extracted from archive files.

To configure a DLP policy rule with content inspection make sure you have completed the steps for DLP Dictionaries and DLP engines:

- [Defining DLP Dictionaries](#) (government agencies, see [Defining DLP Dictionaries](#)).
- [Defining DLP Engines](#) (government agencies, see [Defining DLP Engines](#)).

Defining DLP Inline Policy Rules with Content Inspection

In the ZIA Admin Portal, enter the following DLP Rule attributes:

1. Go to **Policy > Data Loss Prevention**.
2. Click **Add**.
3. In the **Add DLP Rule** window, enter the following DLP Rule attributes:
 - a. **Rule Order:** Policy rules are evaluated in ascending numerical order (Rule 1 before Rule 2, etc.), and the Rule Order reflects this rule's place in the order. You can change the value, but if you've enabled Admin Ranking, then the assigned Admin Rank determines the Rule Order values you can select.
 - b. **Admin Rank:** Enter a value from 0–7 (0 is the highest rank). Your assigned admin rank determines the values you can select. You cannot select a rank that is higher than your own. The rule's Admin Rank determines the value you can select in Rule Order, so that a rule with a higher Admin Rank always precedes a rule with a lower Admin Rank
 - c. **Rule Name:** Enter a unique name for the DLP rule or use the default name.
 - d. **Rule Status:** An enabled rule is actively enforced. A disabled rule is not actively enforced, but does not lose its place in the Rule Order, the service skips it and moves to the next rule.
 - e. **Rule Label:** Select a rule label to associate it with the rule.
 - f. **Content Matching:** Select **DLP Engines**.
 - g. **DLP Engines:** Select the applicable DLP Engine.
 - h. **URL Categories:** Select **AI and ML Applications**.

The screenshot shows the 'Add DLP Rule' configuration window. The 'DLP RULE' section includes fields for Rule Order (2), Severity (Information), Rule Name (GEN AI DLP), Rule Status (Enabled), and Rule Label (---). The 'CRITERIA' section includes Content Matching (Select DLP Engines), DLP Engines (Bard Engine), URL Categories (AI and ML Applications), Cloud Applications (Any), ZPA Application Segment (Any), File Type (Any), Minimum Data Size (KB) (0), Users (Any), Groups (Any), Departments (Any), User Risk Profile (Any), Locations (Any), and Location Groups (Any). At the bottom, there are 'Save' and 'Cancel' buttons.

Figure 4. DLP Inline with Content Inspection Policy



You can choose up to four DLP Engines per inline policy.

If you do not select an auditor and notification template, a notification is not required for this rule.

OCR: Enable this option to allow Zscaler's DLP engines to scan images in files. This option is not currently supported by Portal26.

4. For **DLP Incident Receiver**, select the incident receiver created in the previous steps.
5. Select the **Action** for the rule. You can **Allow** or **Block** transactions that match the rule. If you select Allow, the service allows and logs the transaction. If you select Block, the service blocks and logs the transaction.
6. (Optional) Configure the **Client Connector Notification**. You can **Enable** or **Disable** Client Connector notifications for the rule when violations occur. The field is only available if you enable the **Web DLP Violations** option for your organization on the **End User Notifications** page in the ZIA Admin Portal, and you select the **Action** as **Block** for the rule. To learn more, see [Configuring End User Notifications](#) (government agencies, see [Configuring End User Notifications](#)).
7. Click **Save** and [activate the change](#).

Defining DLP Inline Policy Rules Without Content Inspection

When you configure a Rule Without Content Inspection policy, you do not use Zscaler DLP engines to detect data. Instead, Zscaler detects content based on criteria you specify, then sends information about that content to Portal26. This rule type enables visibility and forwarding of user-initiated AI prompts to the Portal26 hosted incident receiver.

1. Go to **Policy > Data Loss Prevention**.
2. Click **Add**.
3. In the **Add DLP Rule** window, enter the following DLP Rule attributes:
 - a. **Rule Order:** Policy rules are evaluated in ascending numerical order (Rule 1 before Rule 2, etc.), and the Rule Order reflects this rule's place in the order. You can change the value, but if you've enabled Admin Ranking, then the assigned Admin Rank determines the Rule Order values you can select.
 - b. **Admin Rank:** Enter a value from 0–7 (0 is the highest rank). Your assigned admin rank determines the values you can select. You cannot select a rank that is higher than your own. The rule's Admin Rank determines the value you can select in Rule Order, so that a rule with a higher Admin Rank always precedes a rule with a rule with a lower Admin Rank.
 - c. **Rule Name:** Enter a unique name for the DLP rule or use the default name.
 - d. **Rule Status:** An enabled rule is actively enforced. A disabled rule is not actively enforced but does not lose its place in the Rule Order, the service skips it and moves to the next rule.
 - e. **Rule Label:** Select a rule label to associate it with the rule.
 - f. **Content Matching:** Select **None**.
 - g. **URL Categories:** Select **AI and ML Applications**.
 - h. **Outbound Data:** ALL.

The screenshot shows the 'Add DLP Rule' configuration window. The window is titled 'Add DLP Rule' and contains two main sections: 'DLP RULE' and 'CRITERIA'.

DLP RULE

- Rule Order: 1
- Severity: Information
- Rule Name: Portal 26
- Rule Status: Enabled
- Rule Label: ---

CRITERIA

- Content Matching: Select DLP Engines (None selected)
- URL Categories: AI and ML Applications
- Cloud Applications: Any
- ZPA Application Segment: Any
- Outbound Data: Select File Types (All selected)
- Data Size (KB): 0
- Users: Any
- Groups: Any
- Departments: Any
- User Risk Profile: Any
- Locations: Any

Figure 5. DLP Inline without Content Inspection Policy



If you do not select an auditor and notification template, a notification is not required for this rule.

4. For **DLP Incident Receiver**, select the incident receiver created in the previous steps.
5. Select the **Action** for the rule to **Allow**.
6. Click **Save** and [activate the change](#).

ZIA DLP Policy and Incident Receiver configuration is now complete. To validate the configuration is working properly confirm incident receiver's data flows into Portal26 by verifying in the Portal26 GenAI portal. To learn more, go to [Portal26.ai](#).

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**.

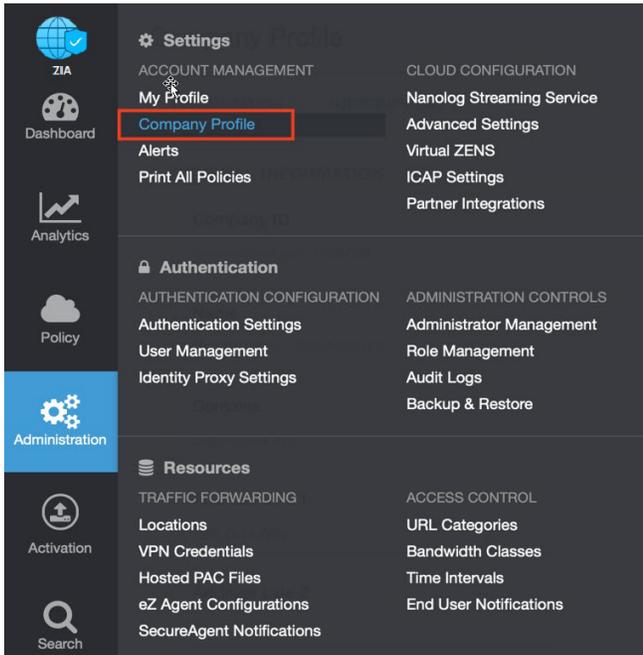


Figure 6. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.

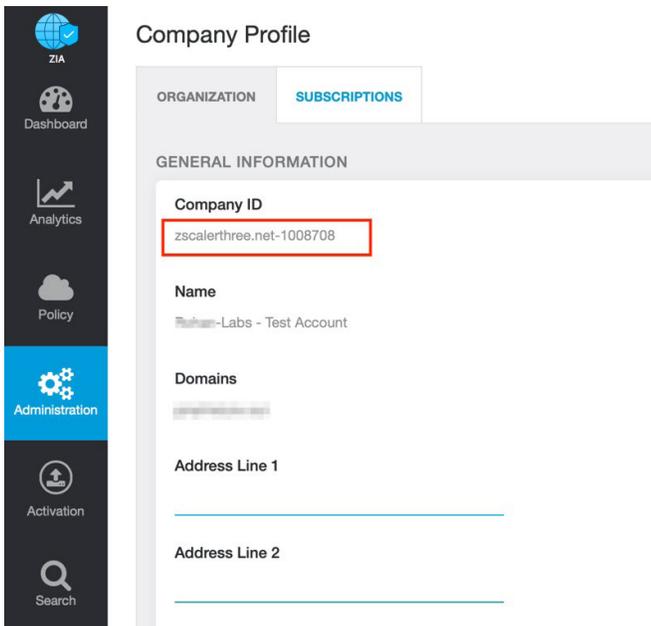


Figure 7. Company ID

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

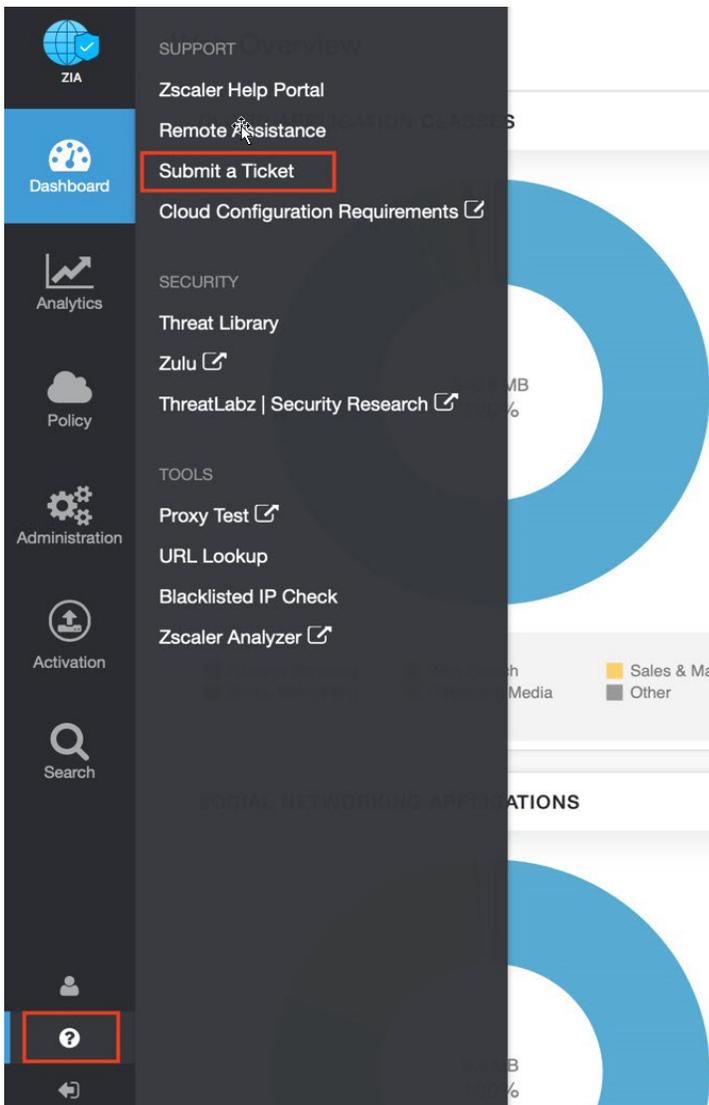


Figure 8. Submit a ticket