ZSCALER AND SECLYTICS DEPLOYMENT GUIDE

JULY 2023, VERSION 1.0

BUSINESS DEVELOPMENT GUIDE

Contents

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)
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
SOC	Security Operations Center
SSL	Secure Socket Layer (RFC6101)
TIP	Threat Intelligence Platform
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
XFF	X-Forwarded-For (RFC7239)
ZCP	Zscaler Cloud Protection (Zscaler)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

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. For more information, see Zscaler's website.

SecLytics Overview

SecLytics uses advanced behavioral profiling and machine learning to power the only prevention, detection, and response (PDR) mechanism on the market.

The SecLytics Augur engine hunts adversaries in the wild during the setup stage, generating attack predictions on average 51+ days before they strike. Those predictions have been proven to be over 97% accurate and generate fewer than 0.01% false positives. Augur's patent-pending technology can tell an organization who specifically targets them in under 72 hours.

With partners and customers in North America, EMEA, and Japan, SecLytics plays a vital role in your overall cybersecurity strategy, improving your security posture, streamlining threat response, reducing SOC costs and keeping your networks safe from bad actors. To learn more, refer to the SecLytics 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
- SecLytics Resources
- Appendix A: Requesting Zscaler Support

Software Versions

This document was authored using the latest version of the 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 SecLytics Introduction

Overviews of the Zscaler and SecLytics 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 it as a secure internet on-ramp—all you do is 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 the 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 system (IPS), Sandboxing, data loss prevention (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.

SecLytics Augur Overview

SecLytics Augur is a predictive, detection, and response (PDR) platform that aligns and streamlines SOC workflow and hardens your perimeter. Augur's predictive intelligence gives you visibility on threats, and the platform also provides smart automation and orchestration to help you beat alert overload and take back control of your SOC.

Augur can replace your TIP, SIEM, and SOAR without the need to hire new analysts. Augur can slot into your existing infrastructure to improve coverage and streamline operations. SecLytics Augur provides the following benefits:

- Predicts Attacks Before They Happen. Augur identifies threat infrastructure using behavioral profiling and machine learning to predict attacks on average 51 days before launch.
- Blocks Attacks Automatically. TIPs and SIEMs produce alerts your team must evaluate and act on. Augur integrates directly with most major security platforms and automatically blocks attacks from identified threat actors.
- Streamlines SOC Operations. Augur blocks Level 1 threats automatically. It also curates and provides enrichment for Level 2 and 3 alerts. Analysts can act on enforcement across your security perimeter directly from Augur.

SecLytics Resources

The following table contains links to SecLytics support resources.

Name	Definition
SecLytics log in page	SecLytics customer log in page.

Integration

The SecLytics integration provides Zscaler with automated, highly accurate and actionable, attack predictions. These indicators are fed into Zscaler via API.

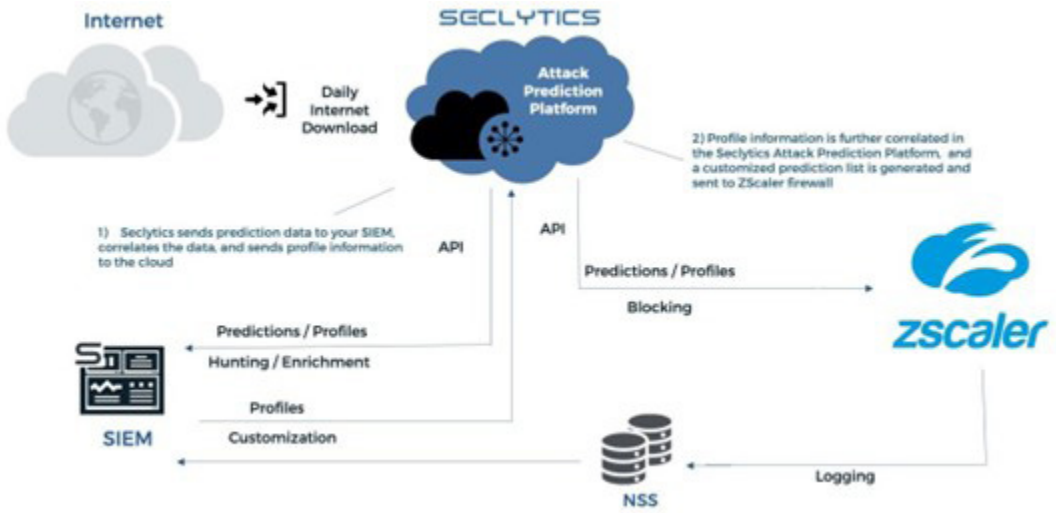

Figure 1. Zscaler and SecLytics integration architecture

The customized prediction information, in the form of URLs or IP addresses is pushed to Zscaler via APIs, protecting you against malicious traffic before there is any risk.

Requirements

Zscaler API access enabled. APIs are not enabled by default. Contact Zscaler Support to enable APIs.

Zscaler Configuration

After Zscaler API access has been enabled, you must create an:

- Administrator API role
- Administrator API user
- API key

Administrator API Role

From the ZIA Admin Portal, create an Administrator API role.

1. Go to **Administration** > **Role Management** > **Add Administrator Role**.
2. Fill in the following information. Turn off all controls not described next.
   a. **Name**: Enter a name. In this example, it is **SecLytics Integration**.
   b. **Policy Access**. Set to **Full**.

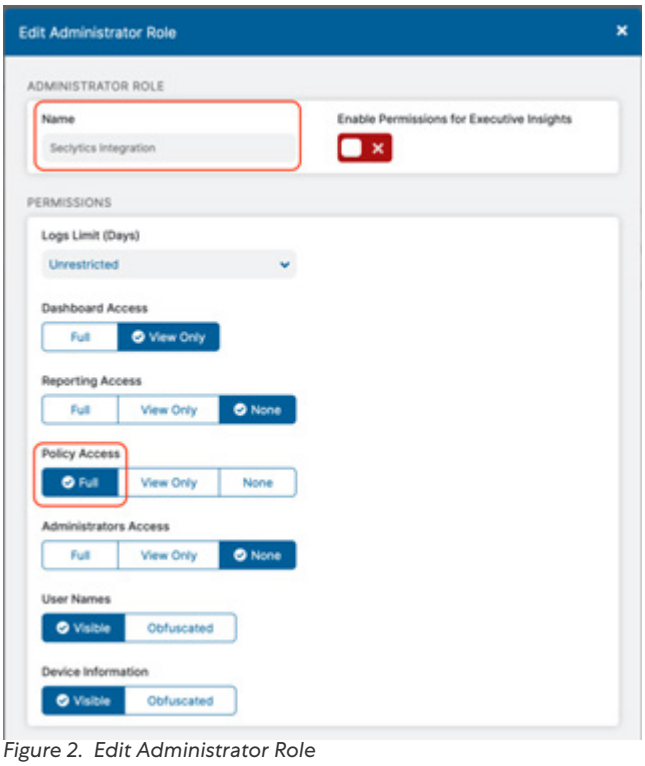

Figure 2. Edit Administrator Role

   c. **Functional Scope**. Enable **Firewall**, **DNAT**, **DNS**, **& IPS**.
   d. Enable **Access Control** and select **Policy and Resource Management**, **Custom URL Category Management**, and **Override Existing Categories**.

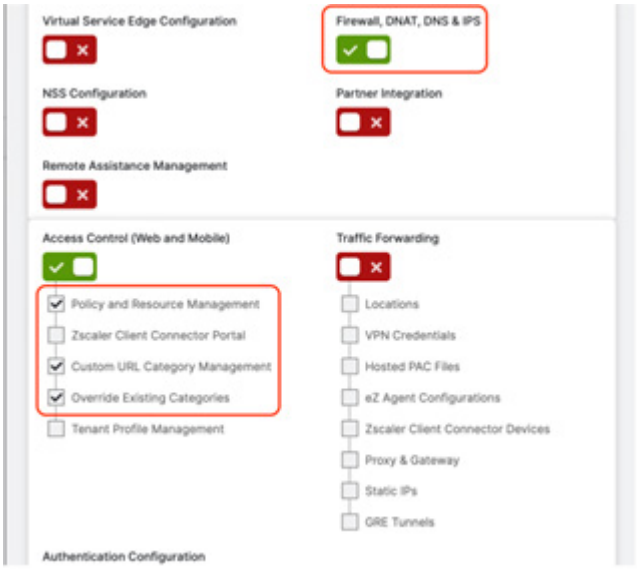

Figure 3. Administrator settings

3. Click **Save**.

Administrator API User

From the ZIA Admin Portal, create an Administrator API user.

1. Go to **Administrator** > **Administrator Management** > **Add Administrator**.
2. Enter an **Email** and **Name**.
3. In the **Role** field, choose the role created in the previous step.

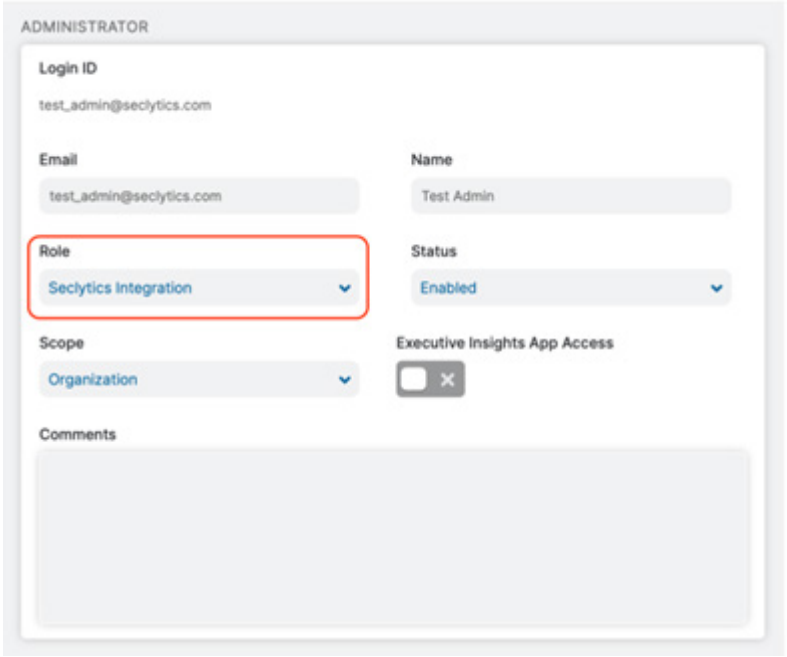

Figure 4. Administrator API User

API Key Creation

From the ZIA Admin Portal, create an API key.

1. Go to **Administrator** > **Cloud Service API Key**.

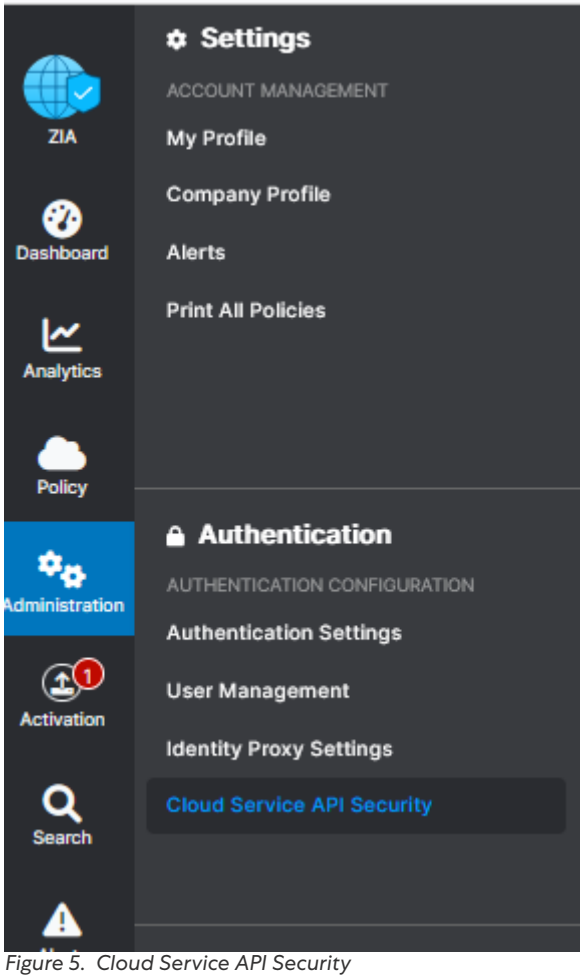

Figure 5. Cloud Service API Security

2. If an API key is present, copy the API key. The API key is used when configuring SecLytics.
3. Also copy your base URL for the API key.

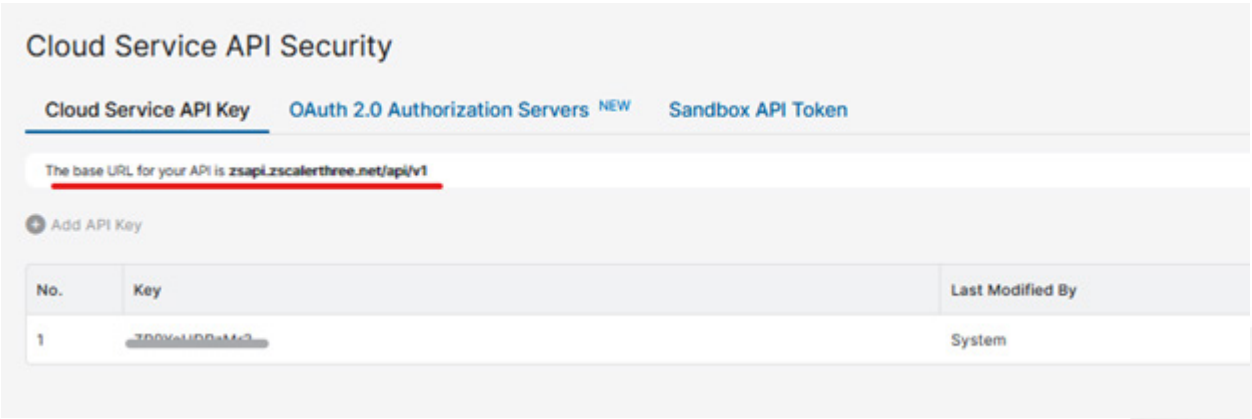

Figure 6. API Key base URL

Activating Changes

If the ZIA Admin Portal shows the **Activation** icon with a number indicator, activate the changes by clicking **Activation** and clicking **Activate**.

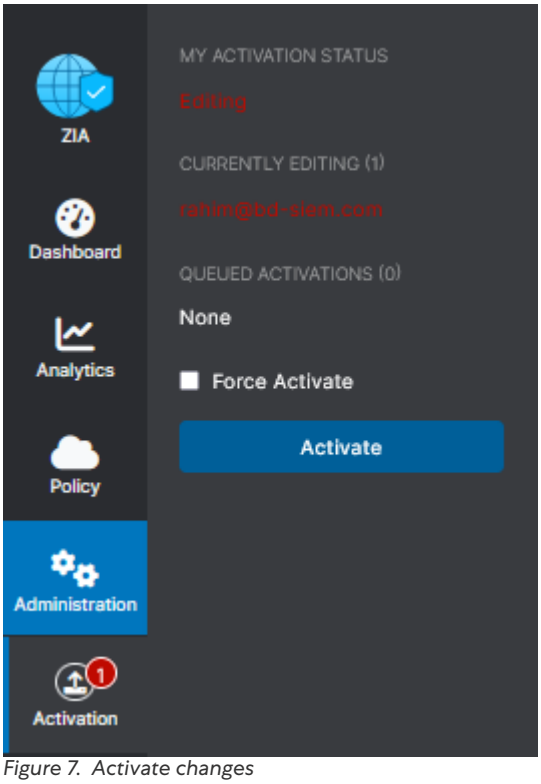

Figure 7. Activate changes

SecLytics Configuration

An administrator is required to make the following configurations.

1. Log in to the SecLytics dashboard.
2. Click **Integrations** and select **New Integration**.
3. Select **Proxy**. Find the Zscaler tile and click **Install**.

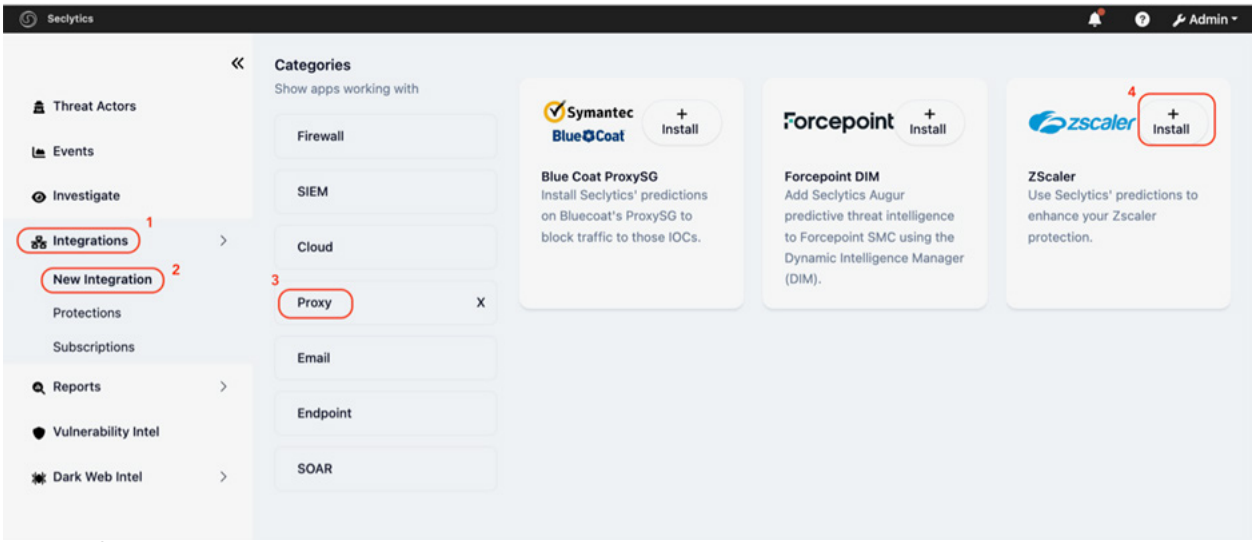

Figure 8. SecLytics new integration

4. Fill in the Zscaler credentials created earlier, and click **Save**.

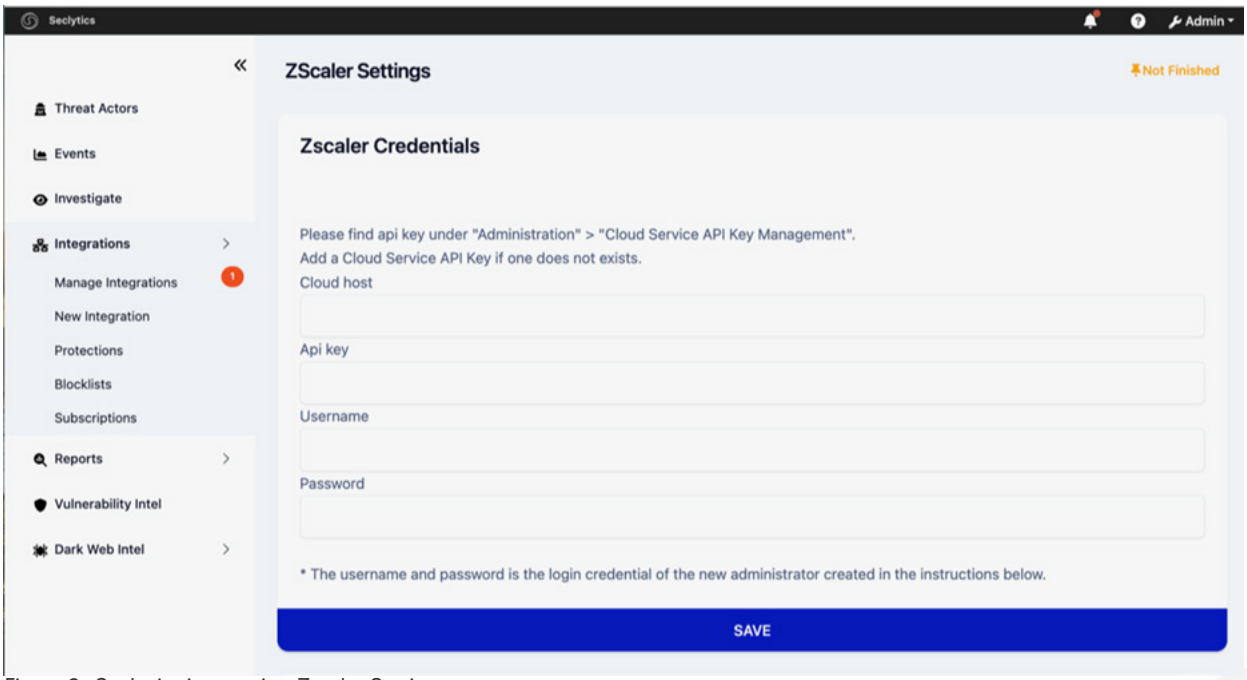

Figure 9. SecLytics integration Zscaler Settings

5. Click **Manage Integrations**. This displays a Zscaler tile with the Active flag.

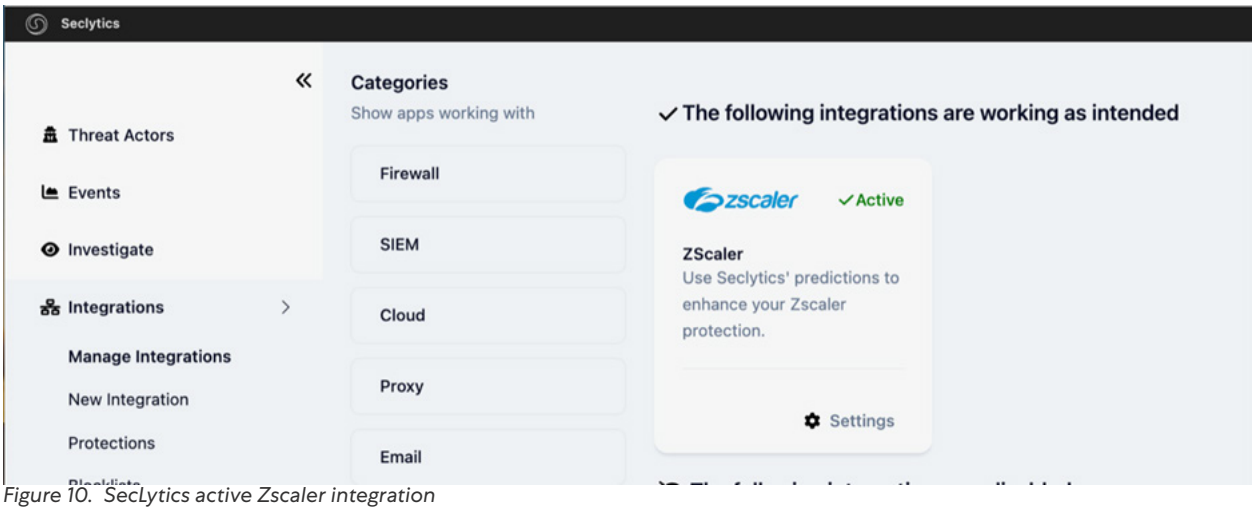

Figure 10. SecLytics active Zscaler integration

6. Click **Settings**. This displays the configured API credential. Click **Edit** to update it, if needed.

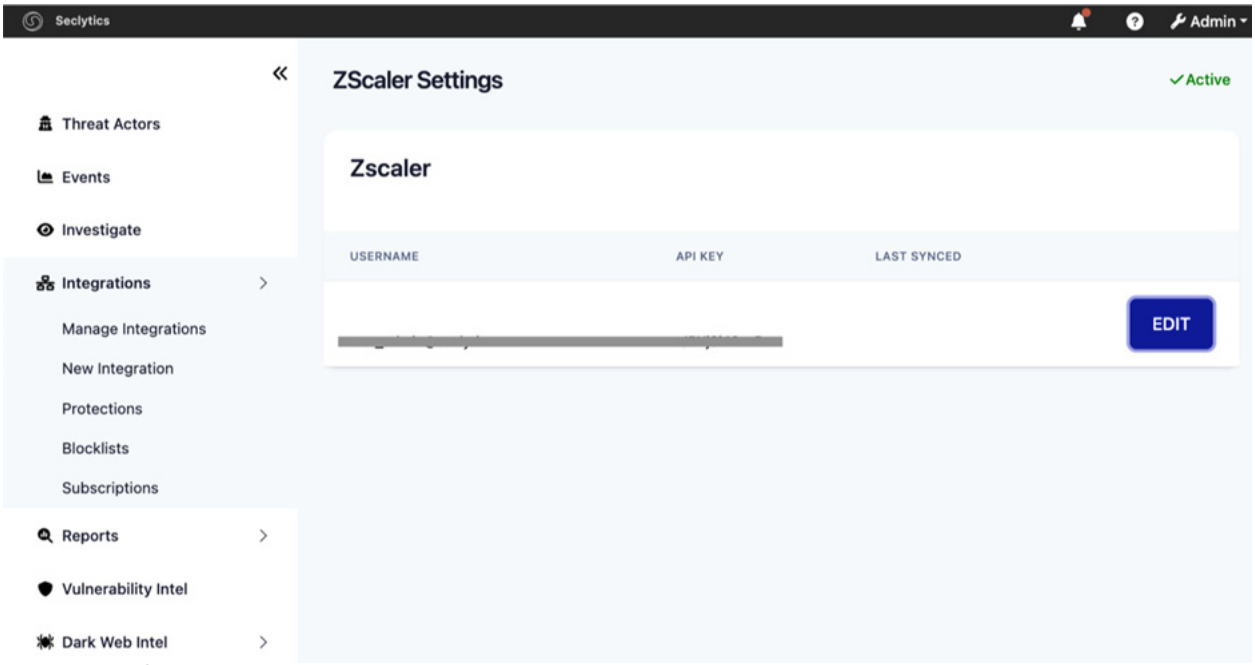

Figure 11. Edit SecLytics Zscaler integration

Appendix A: Requesting Zscaler Support

If you need Zscaler Support for provisioning 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**.

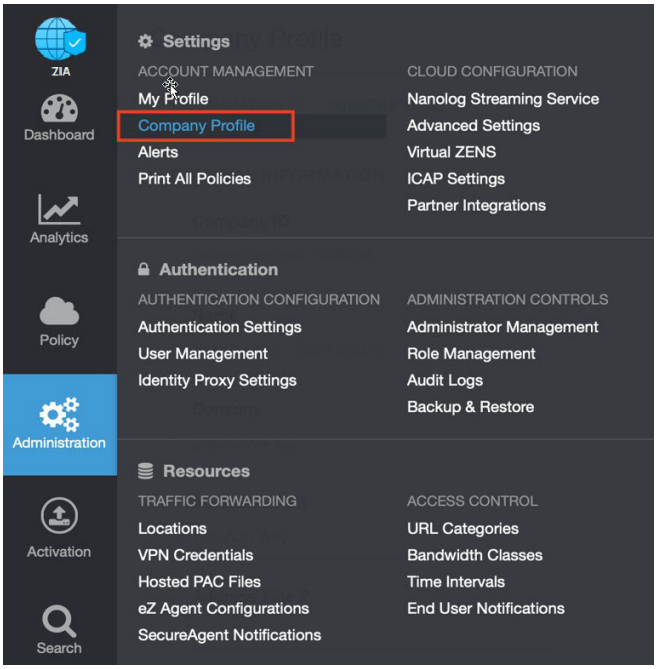

Figure 12. Collecting details to open support case with Zscaler TAC

2. Copy your Company ID.

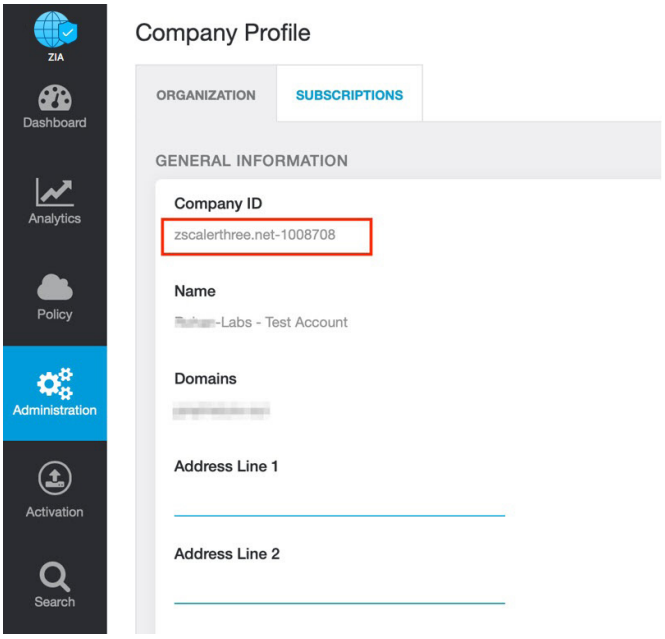

Figure 13. Company ID

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

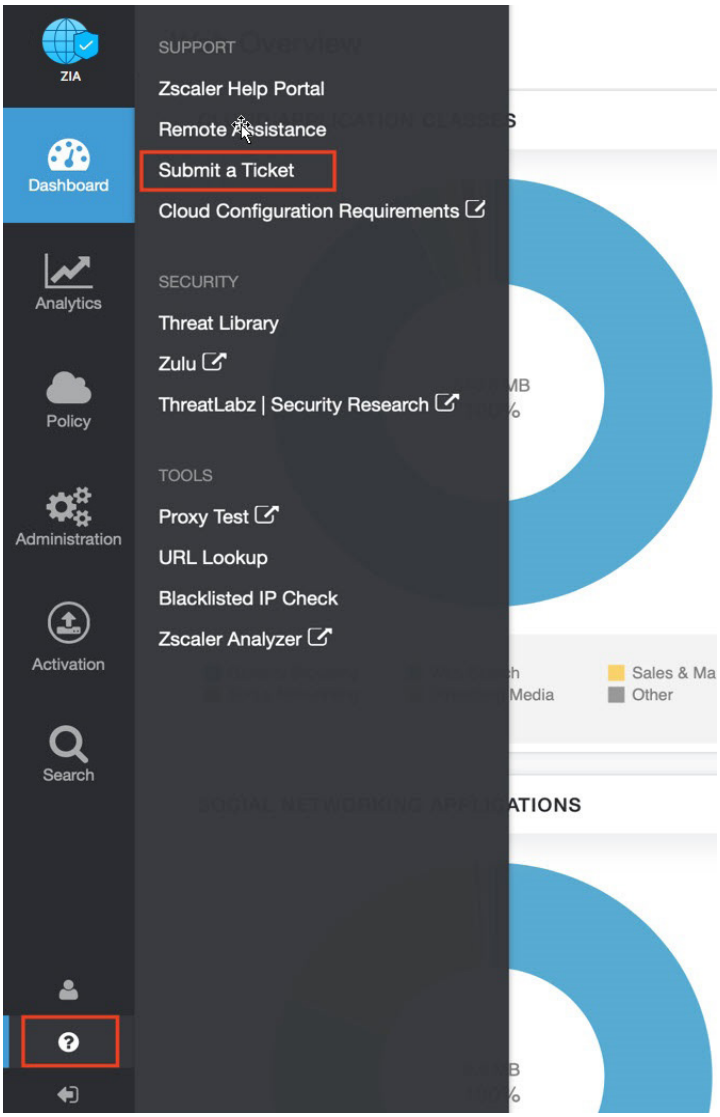

Figure 14. Submit a ticket

