ZSCALER AND ECLECTICIQ DEPLOYMENT GUIDE

JUNE 2025, 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
CTI	Cyber Threat Intelligence
DLP	Data Loss Prevention
DNS	Domain Name Service
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
PFS	Perfect Forward Secrecy
PSK	Pre-Share Key
SOC	Security Operations Center
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

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.

EclecticIQ Overview

EclecticIQ is a global provider of threat intelligence technology and services that empower customers to neutralize critical cyber threats to their business. Guided by our values—being curious, bold, accountable, and collaborative—we help security teams make smarter, faster decisions with dynamic solutions that reduce complexity and streamline threat detection and response. To learn more, refer to EcleticIQ'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
- EclecticIQ 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 EclecticIQ Introduction

Overviews of the Zscaler and EclecticIQ 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.

EclecticIQ Intelligence Center Overview

Intelligence Center is an AI-embedded threat intelligence platform (TIP) that empowers security leaders and teams to better safeguard their business against the threats that are most critical to them. How? By providing contextual insights and cutting through data overload. Designed for CTI and SOC teams in large enterprises and government agencies, it centralizes security tools and intelligence feeds, automating data collection and transforming it into real-time intelligence tailored to the organization's unique business needs

EclecticIQ Resources

The following table contains links to EclecticIQ support resources.

Name	Definition
EclecticIQ Intelligence Center Documentation	Guidance for installation, extensions, public API, and security issues.

Introduction

This article describes how to configure outgoing feeds for a particular feed source. To see how to configure outgoing feeds in general, refer to the **EclecticIQ documentation**.

- Transport type: Zscaler Outgoing Feed
- Content type: Zscaler JSON model
- Published data: The Zscaler Outgoing Feed publishes supported observables to a URL category on ZIA, to which you can then apply URL filtering rules.

Requirements

The following are required for this integration:

- Zscaler username
- Zscaler password
- Zscaler base URI
- Zscaler API key
- (Optional) URL category ID

To learn more about your Zscaler username, password, base URI, and API key, see **Getting Started** (government agencies, see **Getting Started**).

Configure the Outgoing Feed

To configure the outgoing feed:

1. Log in to the ZIA Admin Portal.
2. In the left-hand navigation, go to **Data configuration** > **Outgoing Feeds**.
3. Click the **Add (+)** icon.
4. Under **Transport and Content**, fill out the following fields:
   a. **Transport type**: Select **Zscaler Outgoing Feed** from the drop-down menu.
   b. **Content type**: Select **Zscaler JSON model** from the drop-down menu.
   c. **Datasets**: Select one or more existing datasets from the drop-down menu. The menu displays only datasets that contain observables supported by the **Transport** type you've selected.
   d. **Update strategy**: Select an update strategy. The supported update strategy is **Append**.
   e. **API URL**: Retrieve your base URI from the ZIA Admin Portal. To learn more, see **Getting Started** (government agencies, see **Getting Started**).
   f. **Username**: Enter your Zscaler user name.
   g. **Password**: Enter your Zscaler password.
   h. **API Key**: Enter your Zscaler API key. Retrieve your API key from the ZIA Admin Portal. To learn more, see **Getting Started** (government agencies, see **Getting Started**).
   i. **URL Category ID**: Set to **Non_Categorizable** by default.
5. Store your changes by selecting **Save**.

URL Category ID

By default, this outgoing feed sends supported observables to the Non_Categorizable predefined URL category.

To change this, change the value of the URL Category ID field for this outgoing feed. You can have the outgoing feed send observables to:

- One of the predefined URL categories.
- An existing custom URL category.

You must know the category ID of the URL category that you want to send observables to.

For a CSV list of predefined URL categories and their category IDs, see **About URL Categories** (government agencies, see **About URL Categories**).

You can find the respective category IDs for predefined URL categories in the **URL Category Enum Value (Cloud API) column of the CSV file**.

To find the category ID of a custom URL category, access the **Configuring URL Categories Using API** or consult Zscaler Support.

Supported Observable Types

This outgoing feed supports the following observable types:

- URI
- Domain
- IPv4

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**.

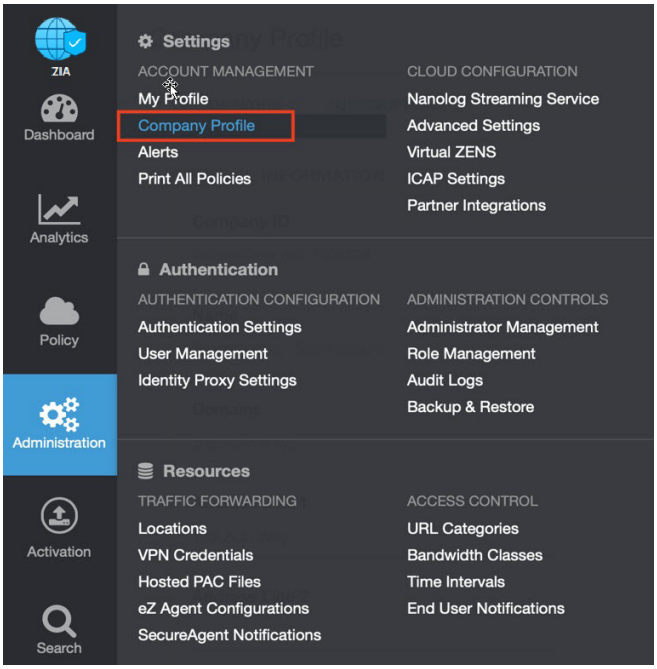

Figure 1. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.

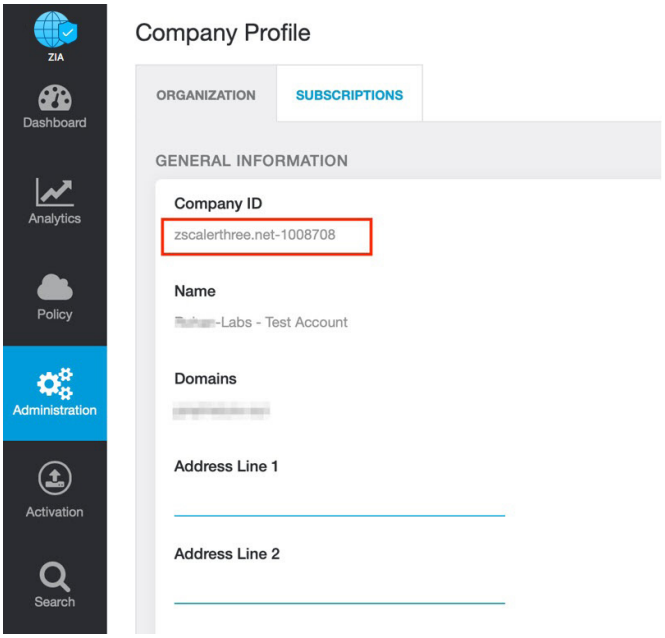

Figure 2. Company ID

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

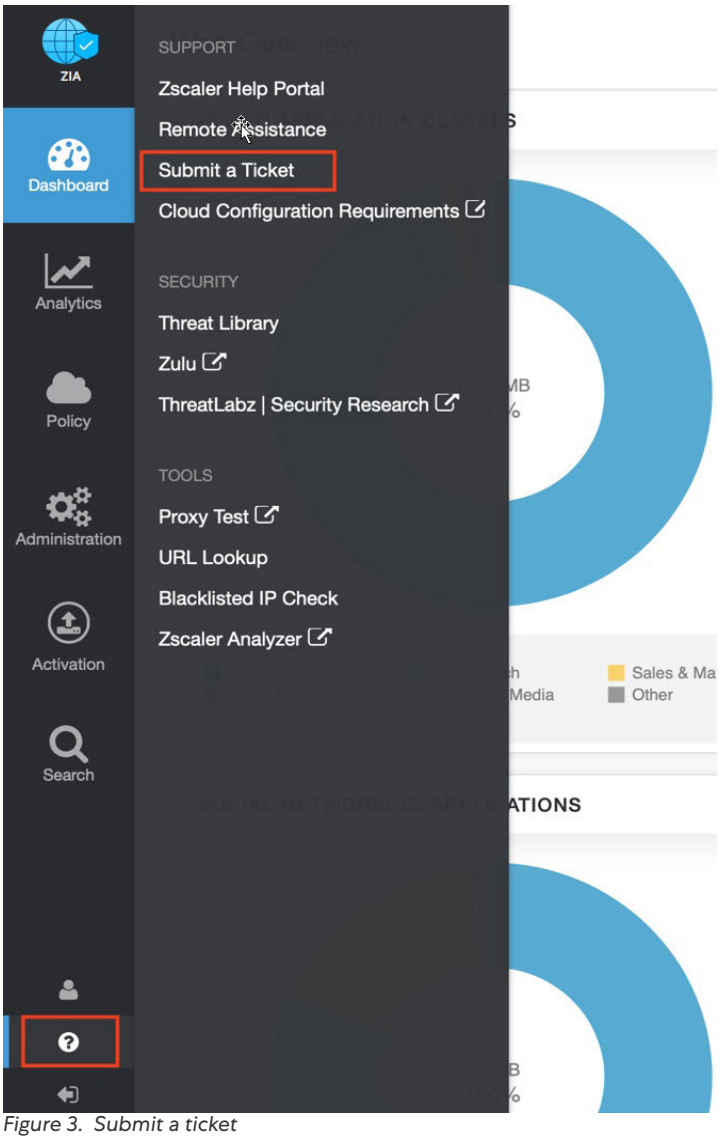

Figure 3. Submit a ticket

