ZSCALER AND RECORDED FUTURE DEPLOYMENT GUIDE

OCTOBER 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
SCF	Security Controls Framework
SSL	Secure Socket Layer (RFC6101)
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)

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 or follow Zscaler on Twitter @zscaler.

Recorded Future Overview

Recorded Future is the world's largest intelligence company. Recorded Future's Intelligence Cloud provides complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,600 businesses and government organizations across more than 70 countries. To learn more, refer to Recorded Future'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
- Recorded Future 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 Recorded Future Introduction

Overviews of the Zscaler and Recorded Future 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, 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, IPS, Sandboxing, DLP, 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.
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.

Recorded Future Intelligence Cloud Overview

The Recorded Future Intelligence Cloud combines persistent data collection, large-scale graph analysis, and the analytical acumen of our global research team to provide complete coverage of intelligence across adversaries, their infrastructure, and the organizations they target, empowering business and security leaders to act with speed and confidence.

Recorded Future Resources

The following table contains links to Recorded Future support resources.

Name	Definition
Recorded Future Support	Support for Recorded Future products.
Recorded Future University	Training for Recorded Future products.

Application Functionality

Recorded Future for Zscaler functionality is underpinned by the Recorded Future API, which is the repository from which risklists are fetched. The app fetches risklists and pushes them to Zscaler via the Zscaler API. This makes the risklists available for use in URL Filtering Policies and Firewall Filtering Policies.

Introduction

Recorded Future delivers security intelligence to amplify the effectiveness of security and IT teams by informing decisions in real time with contextual, actionable intelligence. Offering a singular view of digital, brand, and third-party risk that is ready for integration, Recorded Future analyzes data from open, closed, proprietary, and aggregated sources.

The Recorded Future and Zscaler integration works by updating the blocklists on a Zscaler customer account. This happens through web APIs that connect the two platforms together. The integration is a Python script that can run on a server anywhere that has connectivity between the Recorded Future and Zscaler clouds.

The Integration has been developed and tested by Recorded Future. It is a python script that pulls threat feeds from the Recorded Future platform and calls Zscaler APIs to update blocklists.

Figure 1. Zscaler and Recorded Future integration architecture

This integration was developed using the Recorded Future Connect API and v1 of the Zscaler Cloud API.

Prerequisites

- Zscaler account enabled with API access: Zscaler API Key, Username, and Password.
- Minimum Zscaler Internet Access Essentials License.
- Recorded Future Connect API Token.
- Python 3.6 or higher.

Zscaler Configuration

Configuration on the Zscaler side is needed to create a restricted account for API access. The following sections walk through the steps.

Enable Zscaler API Access

Request API Access by raising a support ticket. After Zscaler Support enables API access, move to the next steps in this guide.

Create Zscaler API Key

The Recorded Future integration requires a Zscaler API Key to operate. Perform the following steps to obtain the key:

1. Go to **Administration** > **Cloud Service API Security**.

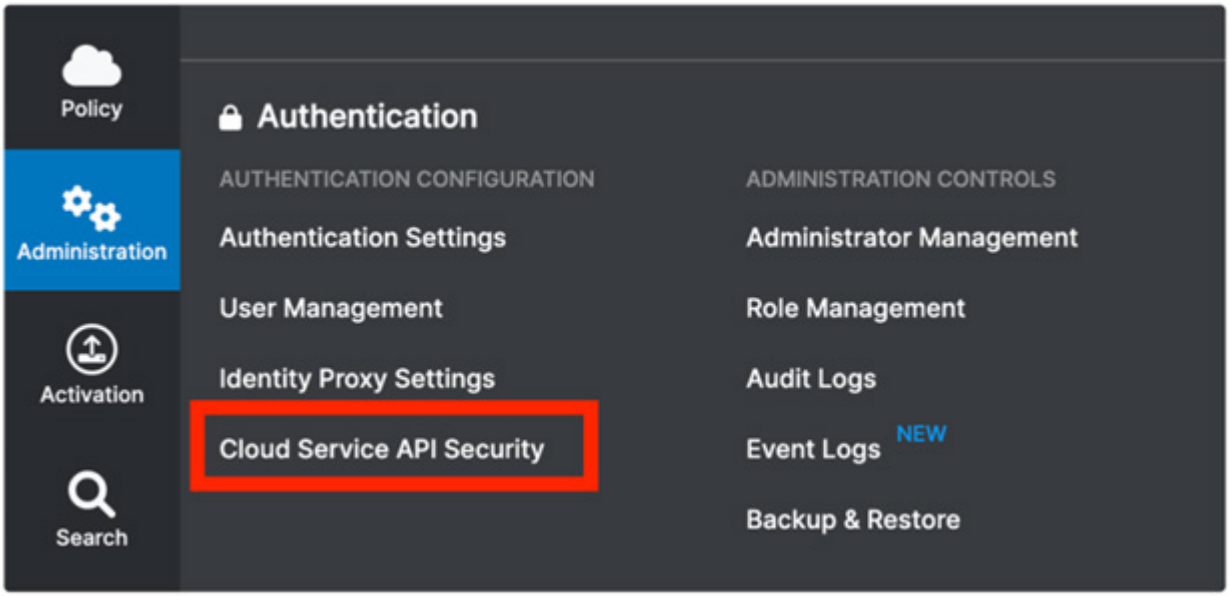

Figure 2. Cloud Service API Security

2. Click **Add API Key**.
3. Click **Save**.
4. Take note of the Base URI and the generated API Key

To learn more about Zscaler API Key management, see Managing Cloud Service API Key (government agencies, see Managing Cloud Service API Key).

Create an Administrative Role

The purpose of the role is to limit the integration user access to only a set of allowed actions:

- Create and manage Custom URL Categories.
- Create and manage IP & FQDN Groups.

To create an administrator role:

1. Click on the **Administration** tab.
2. Click **Role Management**.
3. Click **Add Administrator Role**.
4. Set permissions as shown next.

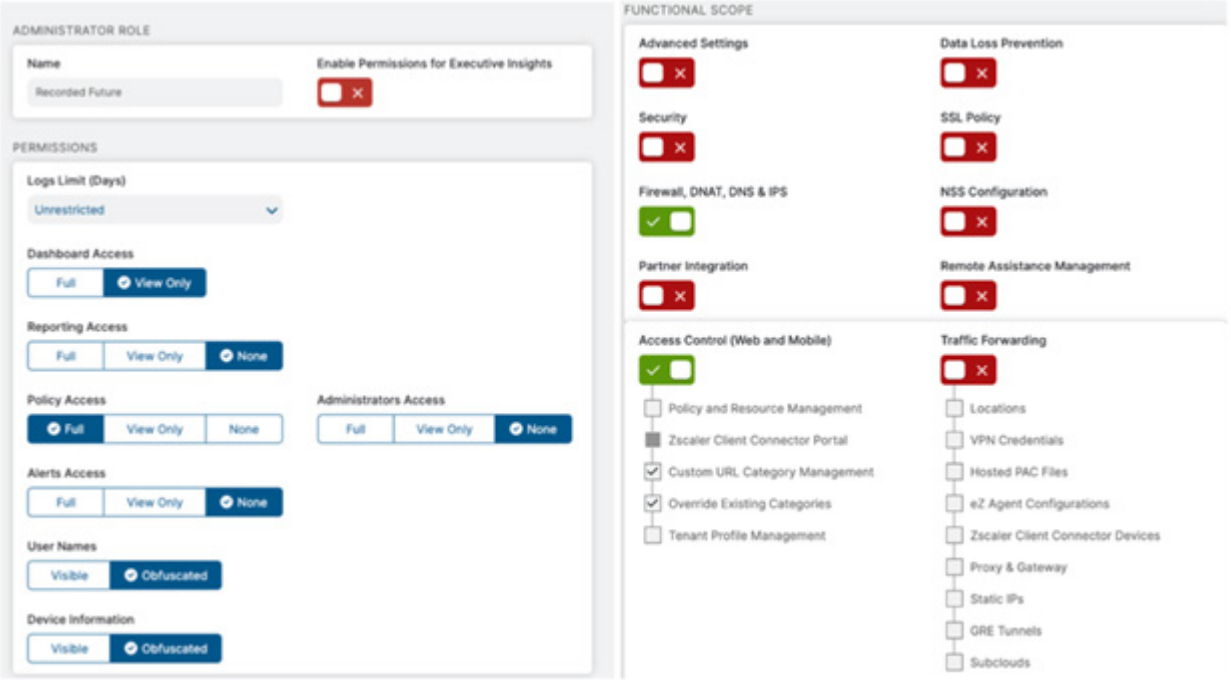

Figure 3. Add Administrator Role

5. Click **Save**.

Add an Administrative Account

After the Administrative role is created, you can create an administrative account for the integration.

1. Go to **Administration** > **Administrator Management**.
2. Click **Add Administrator**.

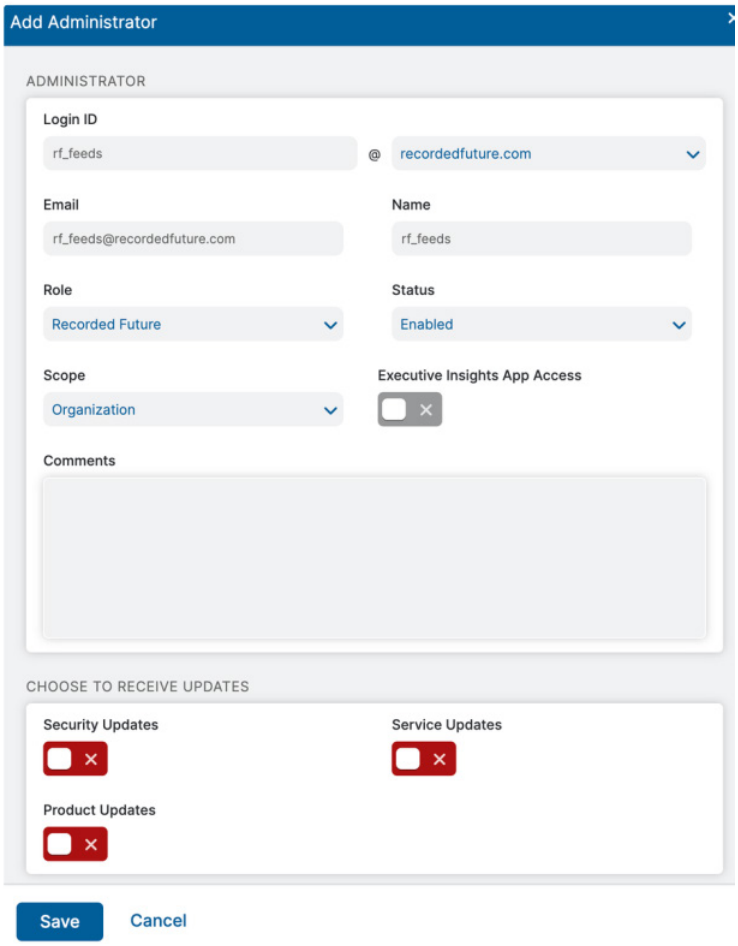

Figure 4. Administrator Settings

3. Click **Save**.

Activating the Changes

Activate the changes:

1. Click the **Activation** tab.
2. Click **Activate**.

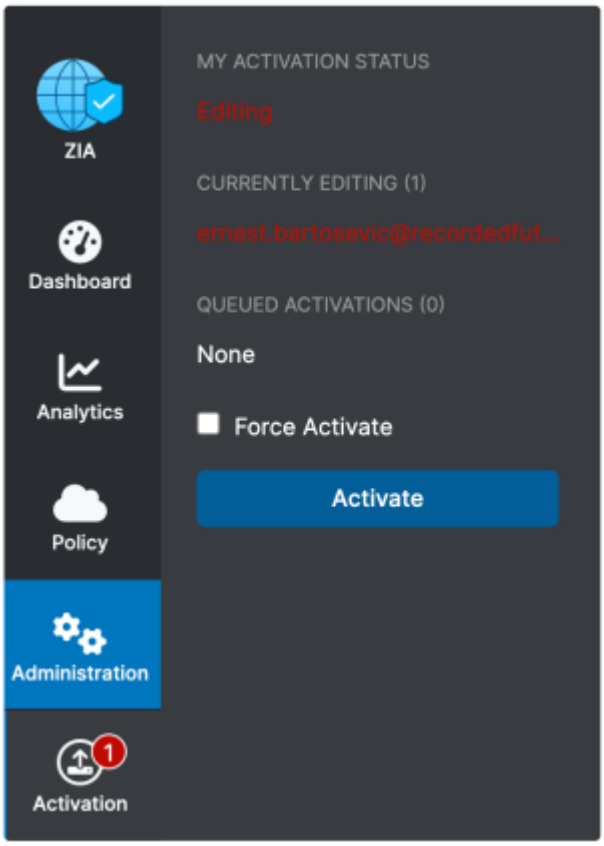

Figure 5. Activate changes

Integration Script Deployment

The following sections describe how to deploy the Recorded Future script.

Set Environmental Variables

Setting of these environmental variables is optional, however, setting them makes it straightforward to maintain and run the script.

```
export RF_API_KEY=<RF Connect API Token>

export ZS_API_KEY=<Zscaler API Key>

export ZS_API_USERNAME=<Zscaler Username>

export ZS_API_PASSWORD=<Zscaler Password>
```

Script Installation

To install the script:

1. Extract `zscaler_<version>.tar.gz` . For example: zscaler_3.0.0-05.tar.gz
2. Go to the zscaler_<version> directory.

   ```
   cd zscaler_<version>
   ```

3. Create a virtual environment.

   ```
   python3 -m venv
   ```

   OR

   ```
   virtualenv venv
   ```

4. Activate the virtual environment.

   ```
   source venv/bin/activate
   ```

5. Install Python dependencies.

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


Script Configuration

Configure the integration in `config/settings.ini`:

```
##################################################

# base_uri - ZScaler Base API URI

# max_domains - Max number of domains to be loaded into a custom URL category

# max_ips - Max number of IPs to be loaded into a Destination IPv4 Group

##################################################

[zscaler]

base_uri = CHANGE_ME

max_domains = 25000

max_ips = 8000

##################################################

# entity_type - Specifies the entity type. Options: [ip/domain/url]

# enabled - Specifies whether the risklist is enabled. Options [True/False]

# fusion_file - Specifies a path to a fusion file (Optional)

# category_name - Name for the Custom URL Category / Destination IPv4 Group

# category-description - Description for the Custom URL Category / Destination IPv4
Group

##################################################

[risklist_weaponized_domains]

entity_type = domain

enabled = true

fusion_file = public/prevent/weaponized_domains.json

category_name = Recorded Future SCF - Prevent Domains

category_description = Malicious IoCs from Recorded Future Security Control Feed:
Weaponized Domains and URLs -

[risklist_c2_communicating_ips]

entity_type = ip

enabled = true

fusion_file = public/prevent/c2_communicating_ips.json

category_name = Recorded Future SCF - Prevent C2C IPs
```



```
category_description = Malicious IoCs from Recorded Future Security Control Feed:
Command and Control IPs [Prev

################################################

# proxy_enabled - Specifies whether RF API requests should be routed via a proxy.
Options: [true/false]

# proxy_servers - Specifies proxy servers.

# verify_ssl - Specifies whether the certificate the site holds should be validated.
Options: [true/false]

################################################

[rfapi]

proxy_enabled = false

proxy_servers = ["https://localhost:8080"]

verify_ssl = true
```

Adding More risklists

The integration supports an arbitrary number of risk lists. In order to add an additional IP risklist, add a new risklist stanza and ensure its name starts with the word risklist_ , for example:

```
[risklist_example_ips]

entity_type = ip

enabled = true

fusion_file = public/example/path/to/another/risklist.json

category_name = Recorded Future SCF Example risklist config name

category_description = Example description
```


Supported risklist Format

By default, the integration fetches JSON formatted SCFs, but also supports single column CSV risklists. See the following example of a single column CSV configuration:

Example CSV IP risklist content:

```
104.250.170.27

104.250.170.28

104.250.170.29

109.230.238.142

109.230.238.140

109.230.238.143
```

Example configuration to ingest the example CSV IP risklist:

```
[risklist_custom_ips]

entity_type = ip

enabled = true

fusion_file = home/custom_ips.csv

category_name = Recorded Future Custom IPs

category_description = Custom Malicious IoCs
```

Crontab

Schedule the script to run on a recurring basis, for example: run every hour.

```
crontab -e

0 * * * * <path_to_venv_python> run_feed.py > /dev/null 2>&1
```

Running the Integration Script

To execute the integration script, run the following command.

```
> python3 run_feed.py
```

Example with credentials passed via the command line arguments:

```
> python3 run_feed.py -k <rf_api_key> -zu <zscaler_username> -zp <zscaler_password>
-zk <zscaler_api_key>
```

For example, when the env variables are set up, run:

```
> python3 run_feed.py
```


Command Line Arguments

```
usage: run_feed.py [-h] [-s SETTINGS] [-k RF_TOKEN] [-zk ZS_API_KEY] [-zu ZS_API_
USERNAME] [-zp ZS_API_PASSWORD] [--log-level {DEBUG,INFO,WARNING,ERROR,CRITICAL}]
```

Recorded Future for Zscaler

```
optional arguments:

-h, --help show this help message and exit

-s SETTINGS, --settings

Settings file path

-k RF_TOKEN, --key RF_TOKEN
```

Recorded Future API key

```
-zk ZS_API_KEY, --zkey ZS_API_KEY

Zscaler API key

-zu ZS_API_USERNAME, --zuser ZS_API_USERNAME
```

Zscaler API Username

```
-zp ZS_API_PASSWORD, --zpassword ZS_API_PASSWORD
```

Zscaler API Password

```
--log-level {DEBUG,INFO,WARNING,ERROR,CRITICAL}

Logging level
```


Verifying the Integration Results

After the integration script is executed with the default risk lists risklist_weaponized_domains and risklist_c2_communicating_ips, the following is created and visible in the ZIA Admin Portal:

- Custom URL Category: Recorded Future SCF - Prevent Domains:
  - To verify the results, go to **Administration** > **URL Categories** > **Recorded Future SCF - Prevent Domains**.
  - Review the **Last Updated** time in the **Description** to verify when the URL Category was last updated.

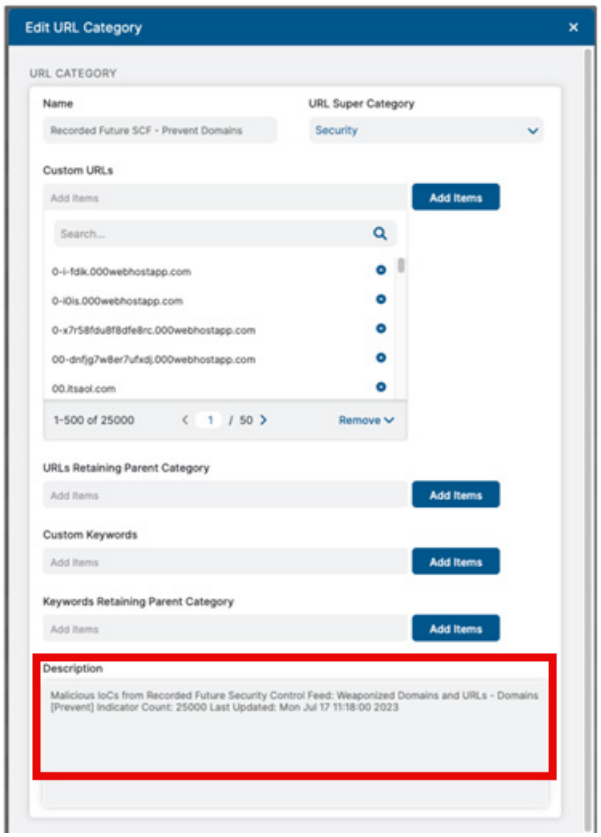

Figure 6. Edit URL Category

- Destination IPv4 Group: Recorded Future SCF - Prevent C2C Ips:
  - To verify the results, go to **Administration** > **IP & FQDN Groups** > **Destination IPv4 Groups** > **Recorded Future SCF - Prevent C2C Ips**.
  - Review the **Last Updated** time in the **Description** to verify when the Destination IPv4 Group was last updated.

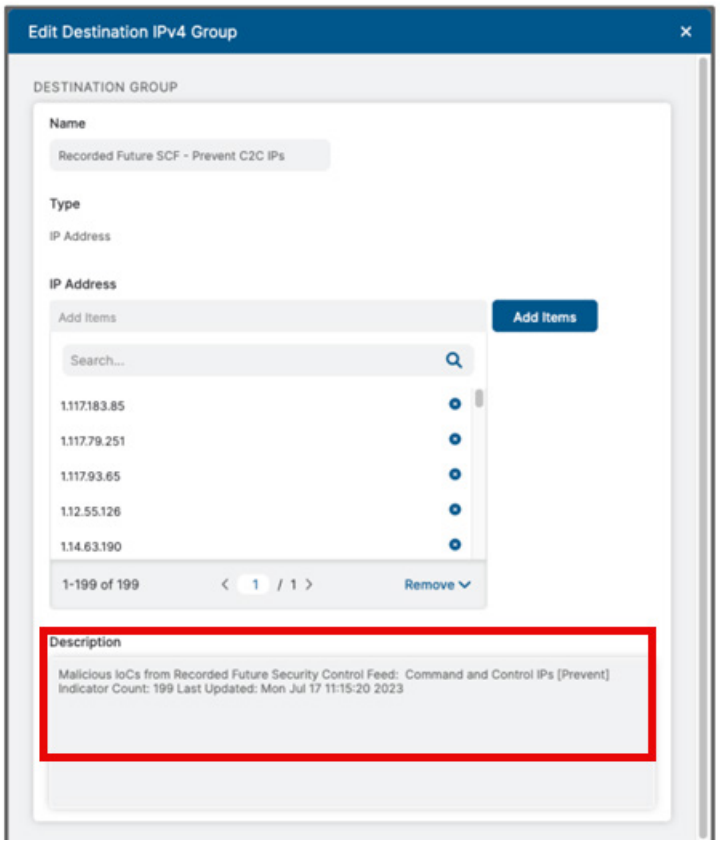

Figure 7. Edit Destination IPv4 Group

Troubleshooting

The integration uses a rotating file handler to create logs in the logs/ directory. Up to 5 files are kept. Log file entries are timestamped, contain the log level, the script name, and the line number from the script for each log entry.

Logging Level

Adjust the logging level by specifying the --log-level argument.

For example, to enable DEBUG logging:

```
python run_feed.py --log-level DEBUG
```

Check When risklist Was Updated

See Verifying the Integration Results.

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**.

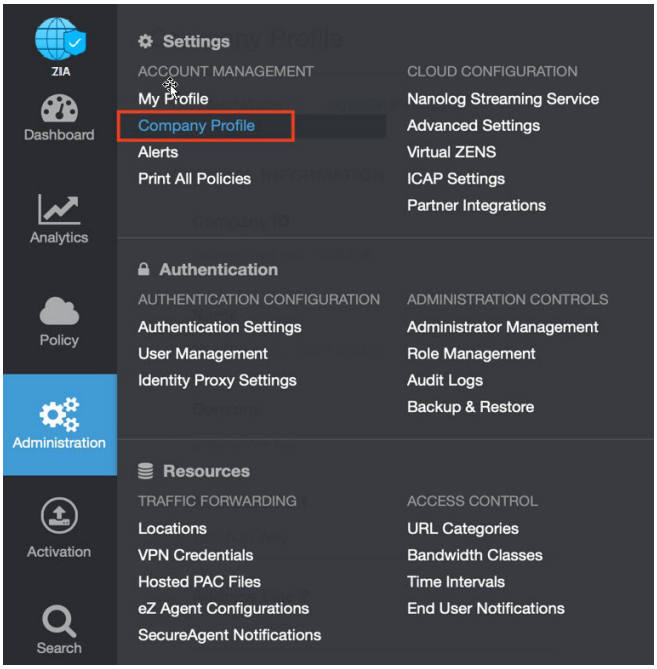

Figure 8. Collecting details to open support case with Zscaler TAC

2. Copy your Company ID.

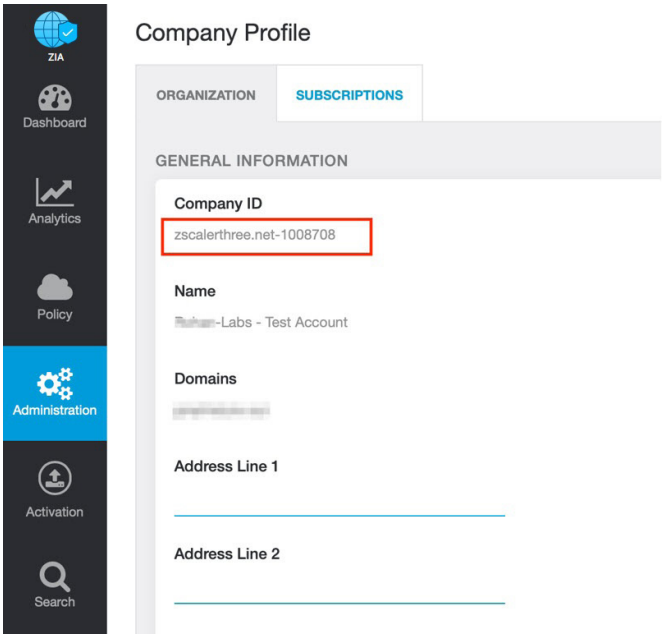

Figure 9. Company ID

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

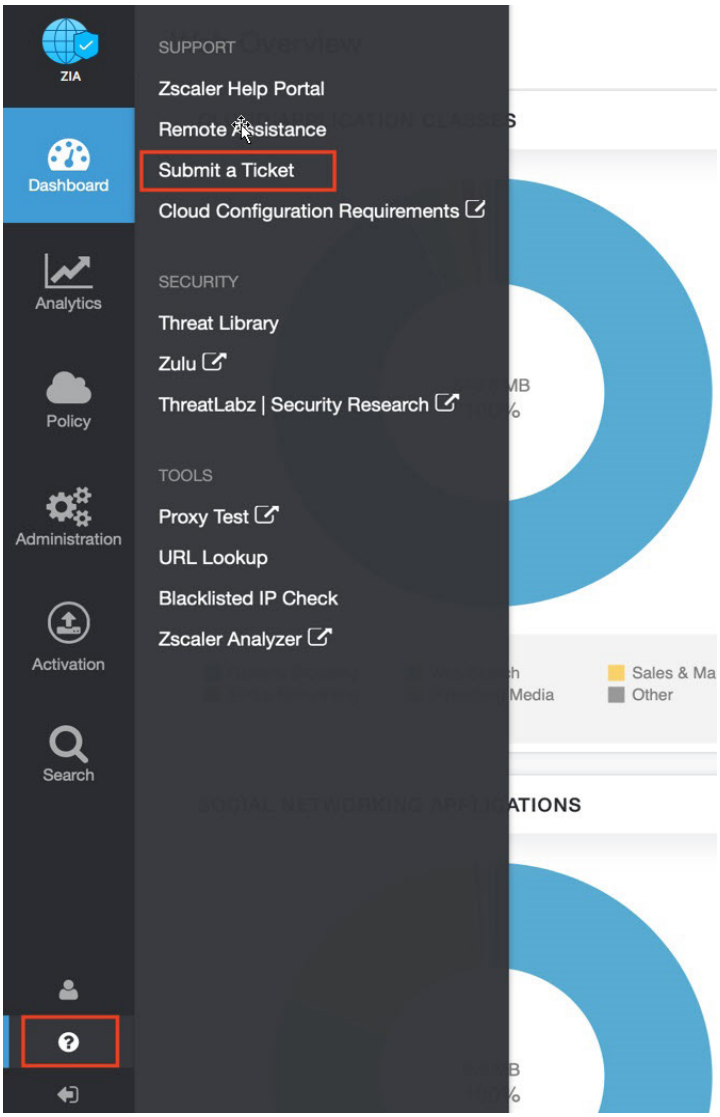

Figure 10. Submit a ticket

