ZSCALER AND THREATCONNECT DEPLOYMENT GUIDE

JUNE 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
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**.

ThreatConnect Overview

ThreatConnect enables threat intelligence operations, security operations, and cyber risk management teams to work together for more effective, efficient, and collaborative cyber defense and protection. With ThreatConnect, organizations infuse ML and AI-powered threat intel and cyber risk quantification into their work, allowing them to orchestrate and automate processes to get the necessary insights and respond faster and more confidently than ever before. Over 200 enterprises and thousands of security professionals rely on ThreatConnect every day to protect their organizations' most critical assets. To learn more, refer to **ThreatConnect'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
- ThreatConnect 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 ThreatConnect Introduction

Overviews of the Zscaler and ThreatConnect 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.

ThreatConnect TI Ops Platform Overview

The ThreatConnect TI Ops Platform is more than a threat intelligence platform (TIP). It's an AI-powered platform that is a force multiplier for your cyber threat intel (CTI) team. The ThreatConnect Platform is the highly scalable and flexible solution required for implementing your cyber threat intelligence. It aggregates and enriches threat intel into a single location, allowing intel to be analyzed, prioritized, and actioned against the most relevant threats using AI and ML, automation, and robust interoperability across the tools in your enterprise. It also enables the organizations' cybersecurity teams to identify, investigate, and respond to threats more efficiently and accurately

ThreatConnect Resources

The following table contains links to ThreatConnect support resources.

Name	Definition
ThreatConnect Learning Portal	Online learning portal for ThreatConnect solutions.
ThreatConnect API Documentation	Online documentation for ThreatConnect API.
ThreatConnect App Documentation	Online documentation for the ThreatConnect App Framework.
ThreatConnect Customer Support	Support portal for ThreatConnect customers.

Zscaler ThreatConnect Integration

There are currently two apps that comprise the integration between the ThreatConnect Platform and Zscaler. The first is the Zscaler Job App, which selects certain URL and Host indicators and adds them to a Zscaler block list. The second is the Zscaler Playbook App that can perform several actions with the Zscaler platform, such as managing blocklists, retrieving details on DLP Dictionaries, submitting files to the Zscaler sandbox and much more.

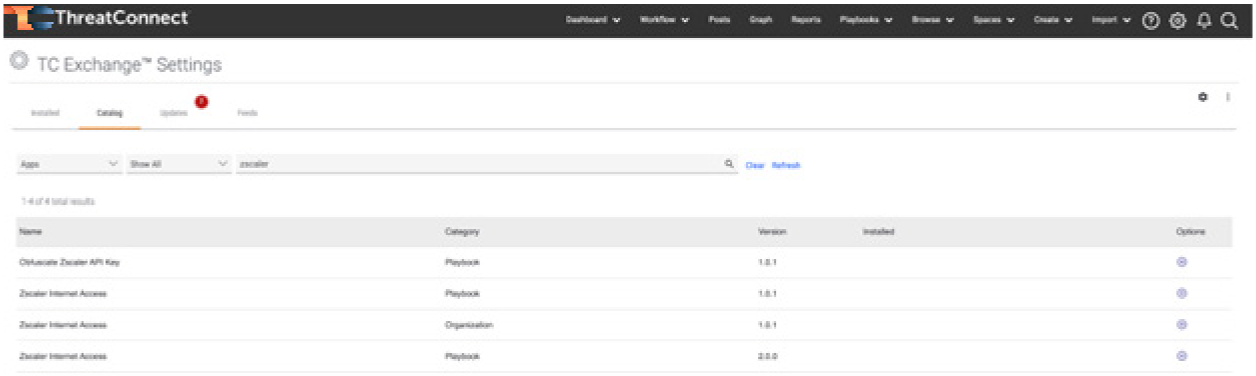
Refer to the following ThreatConnect technical documentation and release notes:

- Zscaler Internet Access: Playbook
- Zscaler Internet Access: Job

Installing the Zscaler Job App and Playbook App in the ThreatConnect Platform

To install the Zscaler Job app and Playbook app:

1. Go to the **App Catalog** on the **TcExchange** in the ThreatConnect Platform.
2. Click the **Catalog** tab and search for `Zscaler` in the search bar.
   a. The Zscaler Job App referred to in this guide is the Zscaler Internet Access entry of the Organization category.
   b. The Zscaler Playbook App referred to in this guide is the Zscaler Internet Access entry of the Playbook category. Check to always use the latest version if this is the first time the app is being installed. You can use older versions, but they tend not to have the latest features. Click the **Add** (**+**) icon to install the playbook app.

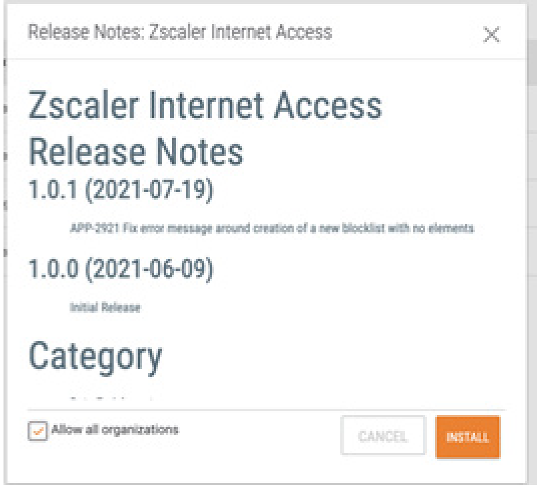


1-4 of 4 total results

Name	Category	Version	Installed	Options
Obfuscate Zscaler API Key	Playbook	1.0.1		⊕
Zscaler Internet Access	Playbook	1.0.1		⊕
Zscaler Internet Access	Organization	1.0.1		⊕
Zscaler Internet Access	Playbook	2.0.0		⊕

Figure 1. Catalog

3. Click **Install** to install the Job and Playbook app. For both, a new window appears and displays the release notes. Select Allow all organizations if all organizations on the ThreatConnect Platform need access to the Job App.



Release Notes: Zscaler Internet Access

Zscaler Internet Access Release Notes

1.0.1 (2021-07-19)

APP-2921 Fix error message around creation of a new blocklist with no elements

1.0.0 (2021-06-09)

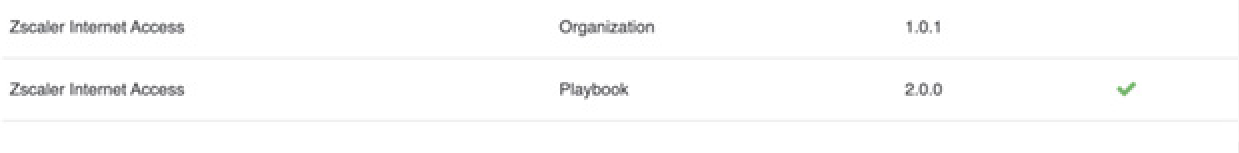
Initial Release

Category

☑ Allow all organizations

Figure 2. Release Notes

4. After an app is installed, a checkmark appears next to it when viewing the Catalog tab with the Zscaler search term populated.



Zscaler Internet Access	Organization	1.0.1	
Zscaler Internet Access	Playbook	2.0.0	✓

Figure 3. Installed apps

Zscaler Internet Access Playbook App Usage

In order to use the Zscaler Internet Access Playbook App, it must be added to a playbook. To create a playbook:

1. Go to the **Playbooks** tab and click **Create Playbook**.

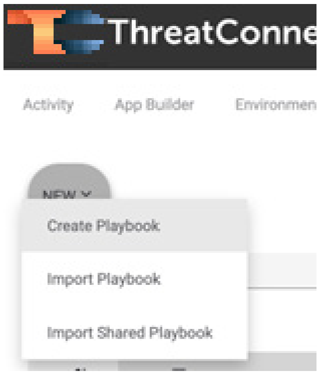
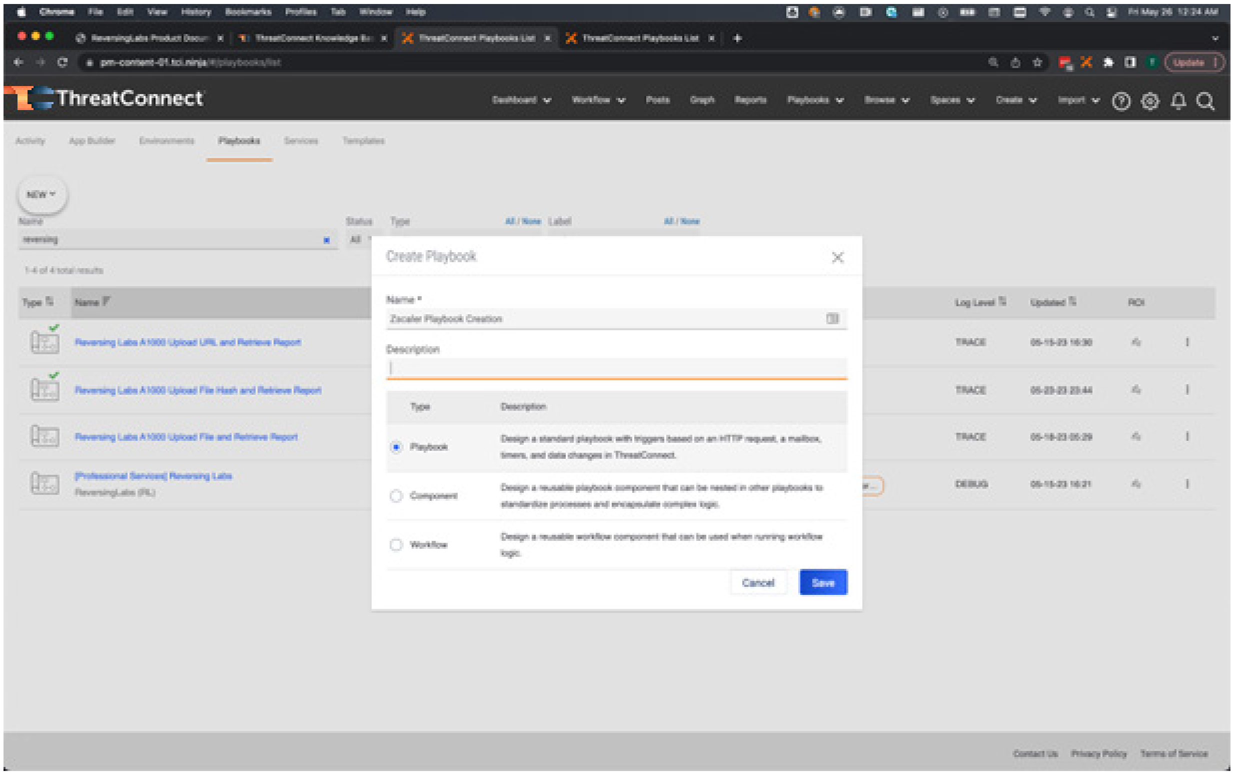


Figure 4. Create Playbook

2. In the window that displays, give a name to the playbook and select **Playbook** as the type. Optionally, provide a description.



Name: reversing
Status: All
Type: All / None
Label: All / None

1-4 of 4 total results

Type	Name	Log Level	Updated	ROI
	Reversing Labs A1000 Upload URL and Retrieve Report	TRACE	05-15-23 16:30	
	Reversing Labs A1000 Upload File Hash and Retrieve Report	TRACE	05-23-23 23:44	
	Reversing Labs A1000 Upload File and Retrieve Report	TRACE	05-18-23 05:29	
	[Professional Services] Reversing Labs ReversingLabs (RL)	DEBUG	05-15-23 16:21	

Create Playbook

Name *: Zscaler Playbook Creation

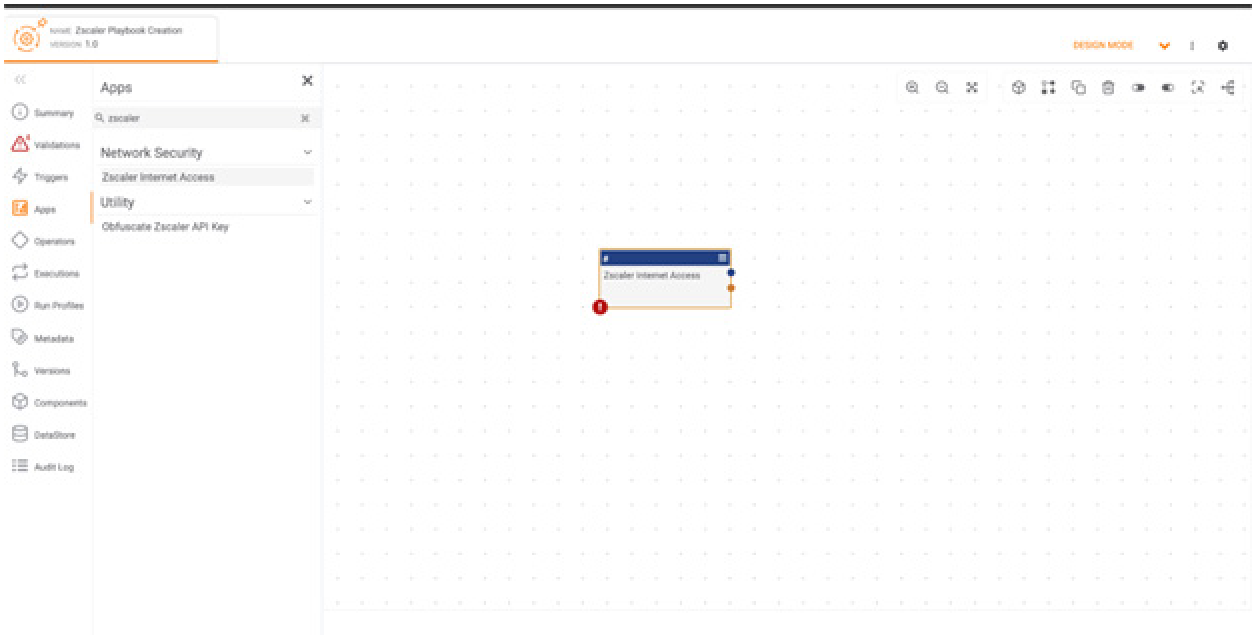
Description:

Type	Description
● Playbook	Design a standard playbook with triggers based on an HTTP request, a mailbox, timers, and data changes in ThreatConnect.
○ Component	Design a reusable playbook component that can be nested in other playbooks to standardize processes and encapsulate complex logic.
○ Workflow	Design a reusable workflow component that can be used when running workflow logic.

Cancel Save

Figure 5. Playbook name

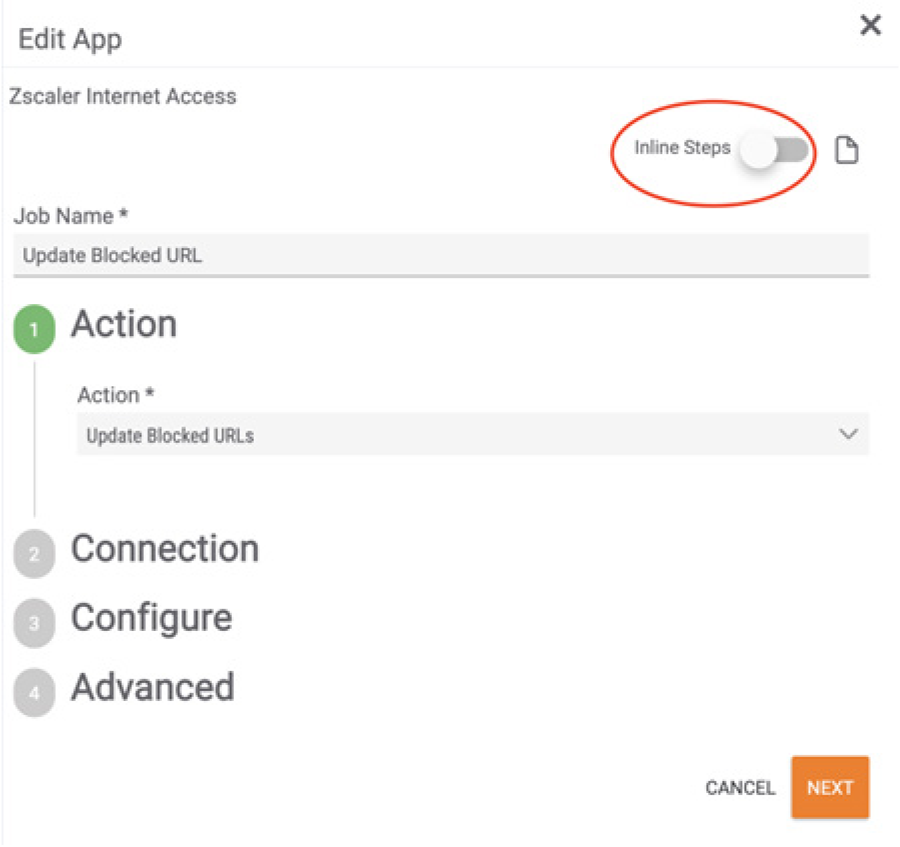
3. After the playbook is created, click the **Apps** section and enter `Zscaler` as the search term in the search bar. Click the **Zscaler Internet Access** app and it appears in the playbook canvas.



zscaler

Figure 6. Zscaler Internet Access App

4. Double clicking the app opens the **Edit App** interface. Zscaler recommends toggling **Inline Steps** so that you can completely see the configuration.

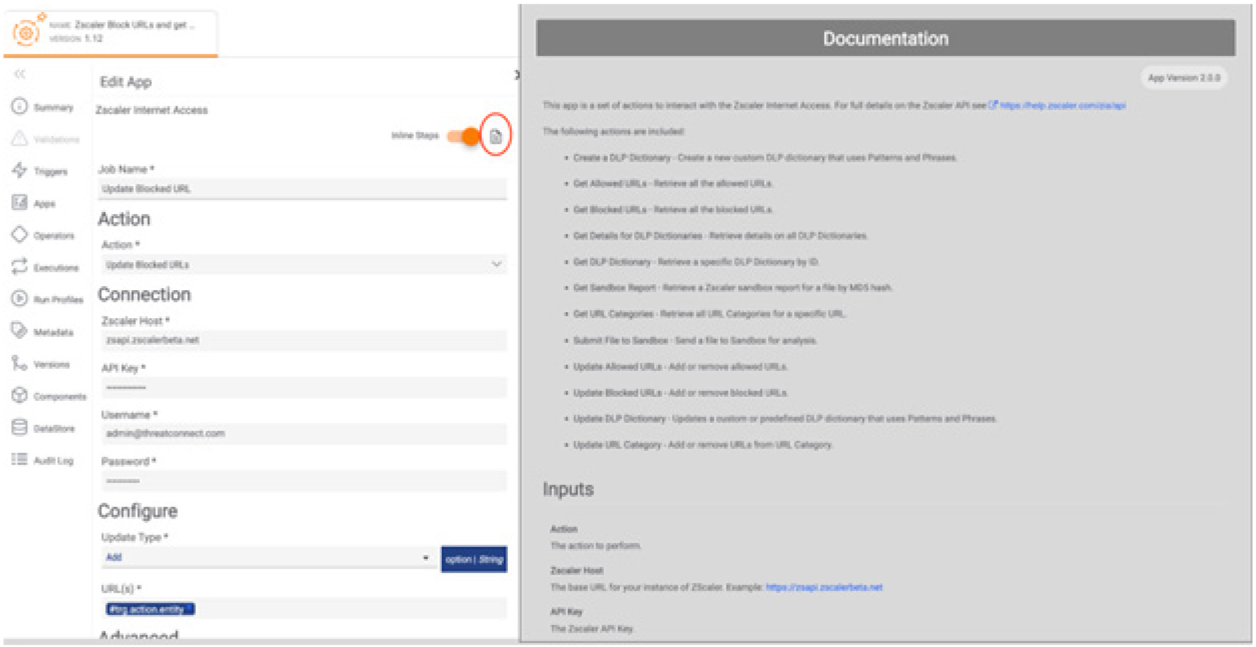


Job Name *
Update Blocked URL

Action *
Update Blocked URLs

Figure 7. Edit app

5. Click the **Document** icon next to the inline steps to display the **Documentation** for the app.



Edit App

Zscaler Internet Access

Job Name *
Update Blocked URL

Action

Action *
Update Blocked URLs

Connection

Zscaler Host *
zsapi.zscalerbeta.net

API Key *
****

Username *
admin@threatconnect.com

Password *
****

Configure

Update Type *
Add

URL(s) *
#trg.action.entity

Advanced

Documentation

App Version 2.0.0

This app is a set of actions to interact with the Zscaler Internet Access. For full details on the Zscaler API see https://help.zscaler.com/zia/api

The following actions are included:

- Create a DLP Dictionary - Create a new custom DLP dictionary that uses Patterns and Phrases.
- Get Allowed URLs - Retrieve all the allowed URLs.
- Get Blocked URLs - Retrieve all the blocked URLs.
- Get Details for DLP Dictionaries - Retrieve details on all DLP Dictionaries.
- Get DLP Dictionary - Retrieve a specific DLP Dictionary by ID.
- Get Sandbox Report - Retrieve a Zscaler sandbox report for a file by MD5 hash.
- Get URL Categories - Retrieve all URL Categories for a specific URL.
- Submit File to Sandbox - Send a file to Sandbox for analysis.
- Update Allowed URLs - Add or remove allowed URLs.
- Update Blocked URLs - Add or remove blocked URLs.
- Update DLP Dictionary - Updates a custom or predefined DLP dictionary that uses Patterns and Phrases.
- Update URL Category - Add or remove URLs from URL Category.

Inputs

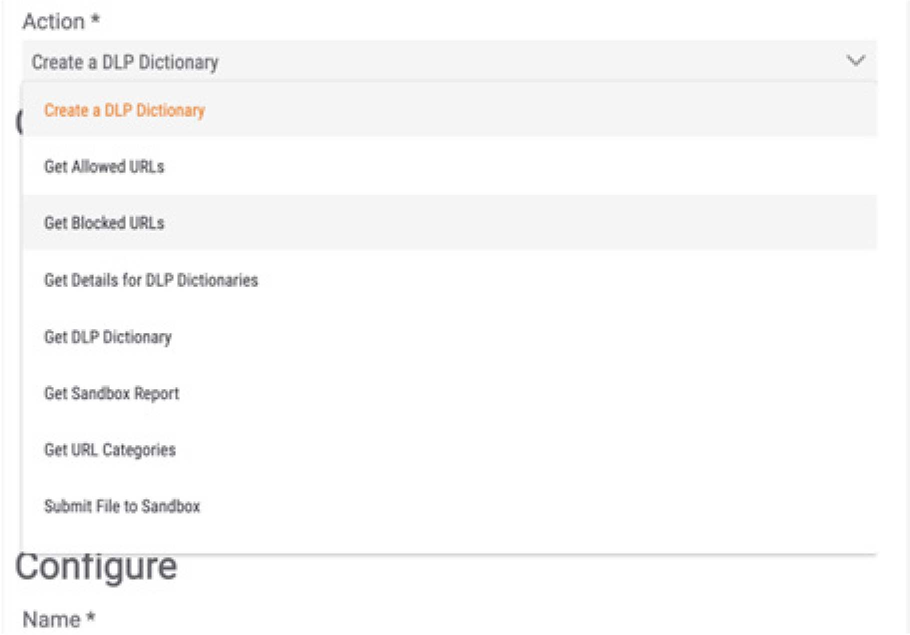
Action
The action to perform.

Zscaler Host
The base URL for your instance of ZScaler. Example: https://zsapi.zscalerbeta.net

API Key
The Zscaler API Key.

Figure 8. Documentation

6. To use the app, edit the app to give it a name representing its function in the playbook. Under **Action**, select the mode of operation for the app as this is a multifunction app. Note that the fields under the **Configure** section change based on the action selected.



Action *

Create a DLP Dictionary

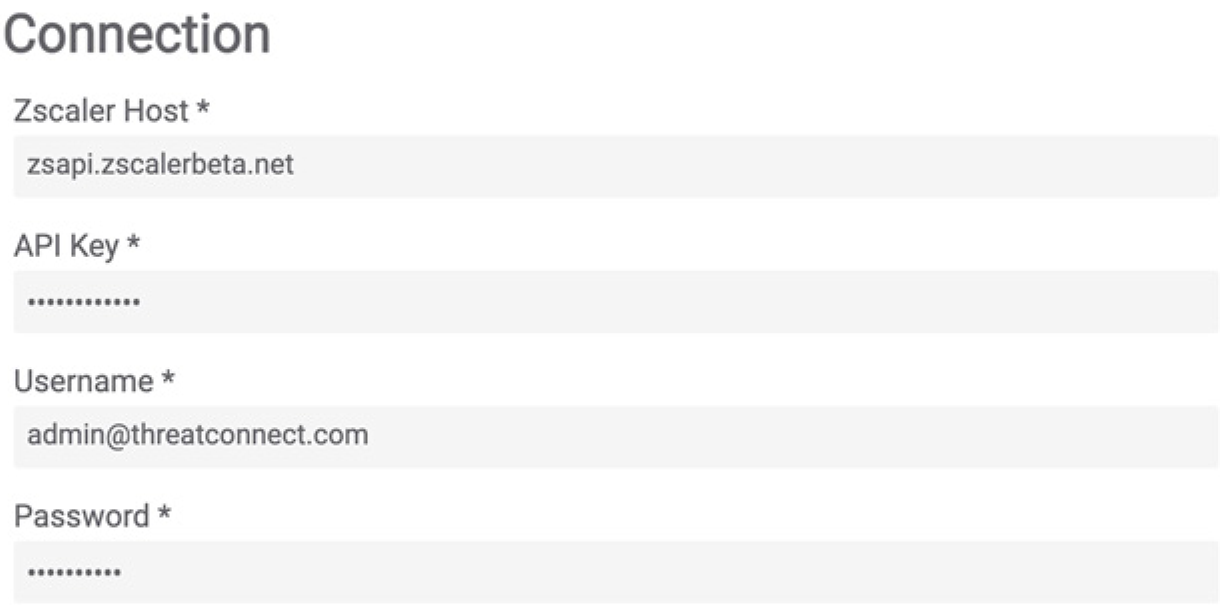
- Create a DLP Dictionary
- Get Allowed URLs
- Get Blocked URLs
- Get Details for DLP Dictionaries
- Get DLP Dictionary
- Get Sandbox Report
- Get URL Categories
- Submit File to Sandbox

Configure

Name *

Figure 9. Actions

7. Under **Connection**, enter the **Zscaler Host** address, Zscaler **API Key**, the Zscaler login **Username** and **Password**.



Connection

Zscaler Host *
zsapi.zscalerbeta.net

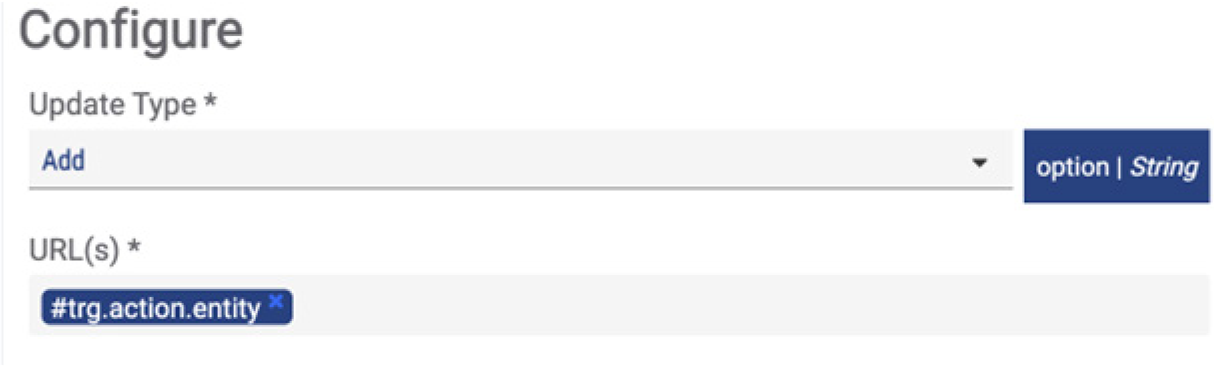
API Key *
••••••••••••

Username *
admin@threatconnect.com

Password *
••••••••••

Figure 10. Connection

8. In this example, the **Configure** section consists of the options for the **Update Blocked URLs** action. For each action type, these configuration options differ.



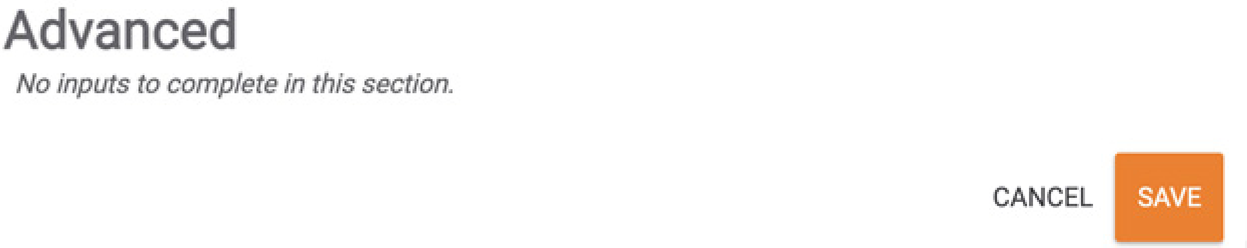
Configure

Update Type *
Add

URL(s) *
#trg.action.entity

Figure 11. Configure

9. Certain actions contain an **Advanced** section, but depending on the previous configuration, they might not need to be configured. Click **Save**.

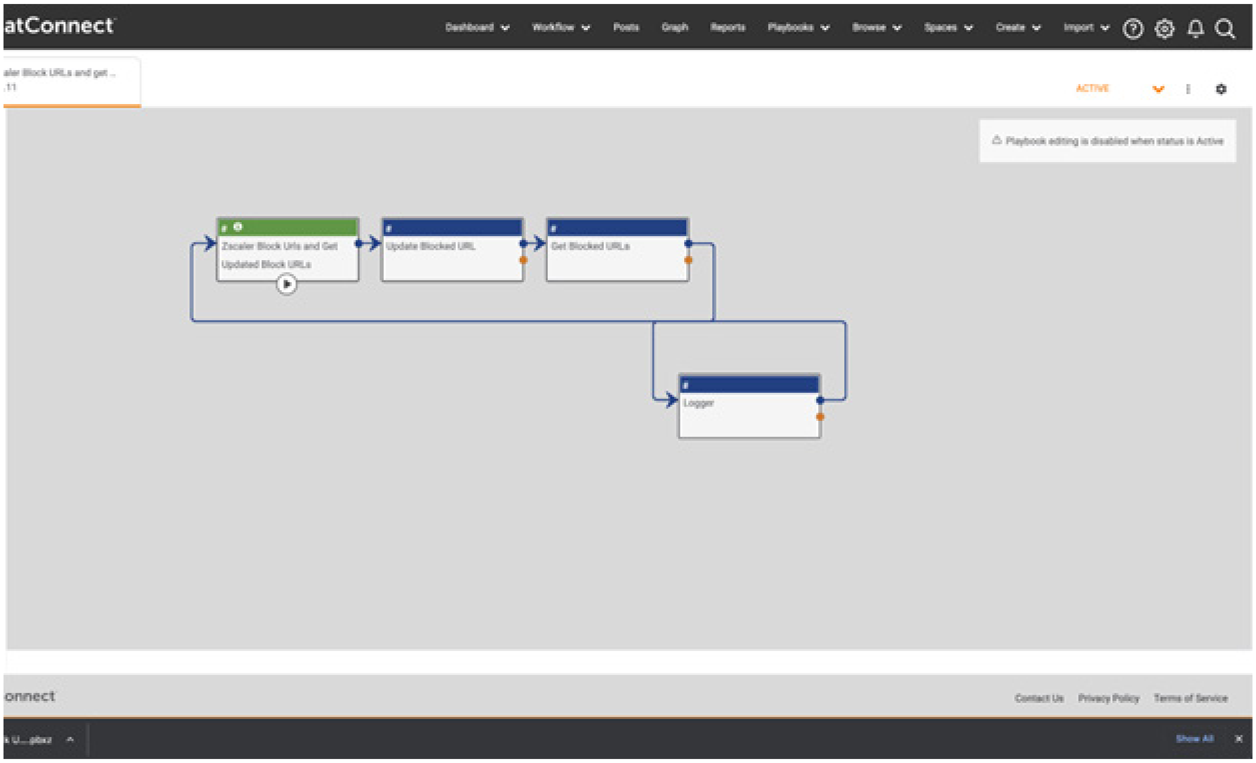


Advanced

No inputs to complete in this section.

Figure 12. Advanced

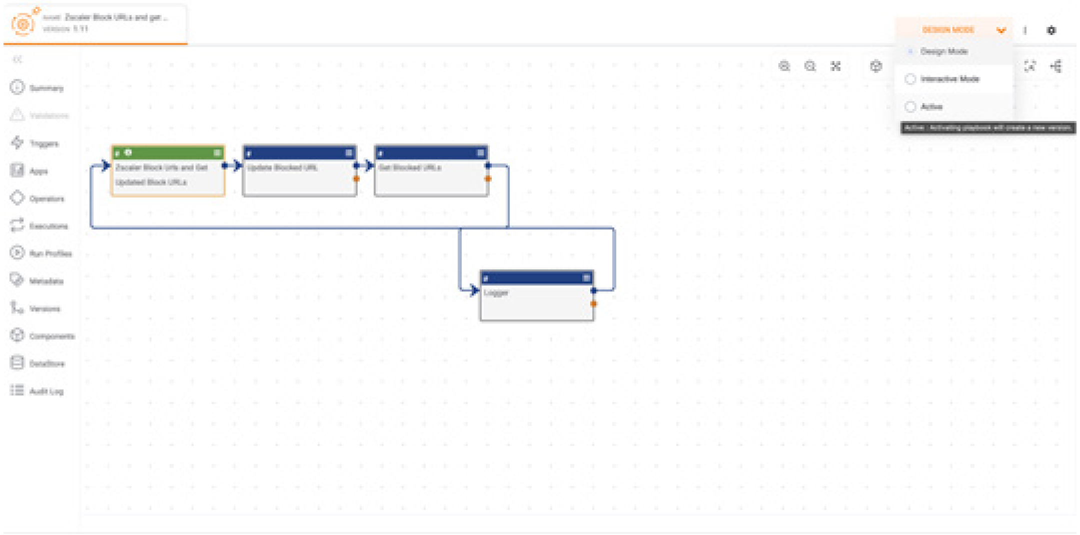
10. After saving the edits with no validation errors, the app is ready to use and can be used in a playbook. You can use multiple Zscaler Internet Access Playbook Apps with different actions in a single playbook.



⚠ Playbook editing is disabled when status is Active

Figure 13. Playbook apps

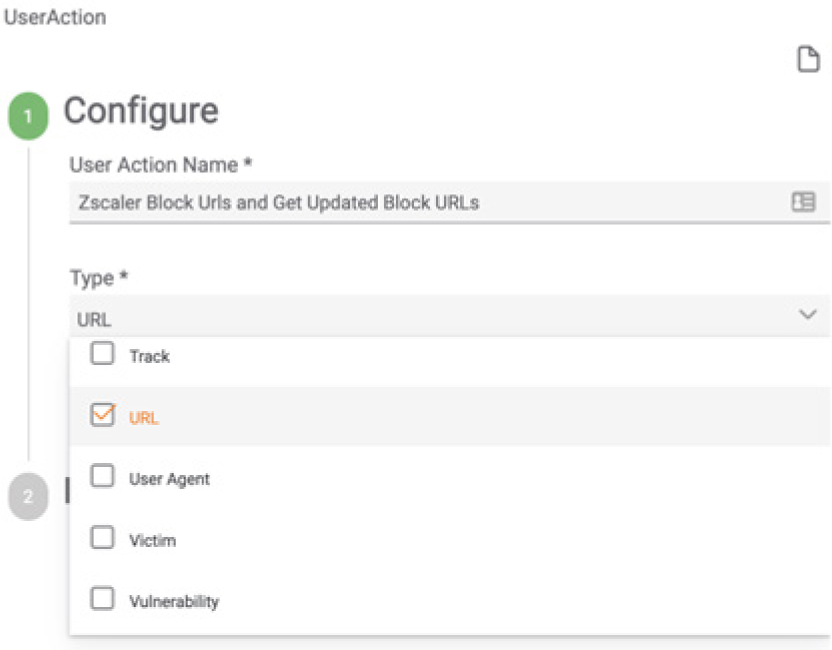
11. After a playbook is ready for use, select **Active** in the top right-hand corner.



Active : Activating playbook will create a new version.

Figure 14. Activate playbook

The playbook is triggered based on the type of trigger selected. In this example, a user action trigger was selected as well as the indicator type of URL. This playbook activates on a URL indicator.



UserAction

1 Configure

User Action Name *

Zscaler Block Urls and Get Updated Block URLs

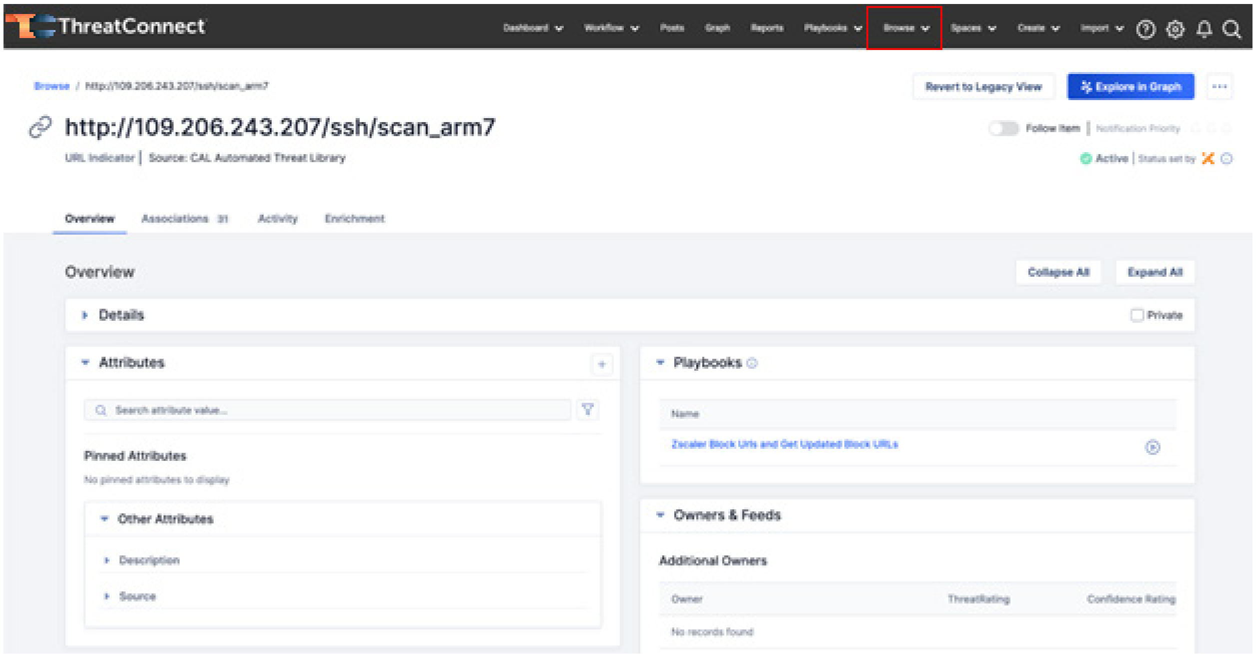
Type *

URL

- □ Track
- ☑ URL
- □ User Agent
- □ Victim
- □ Vulnerability

Figure 15. Trigger action

12. Navigate to the Browse tab and select a URL indicator to activate the playbook.



Browse / http://109.206.243.207/ssh/scan_arm7

http://109.206.243.207/ssh/scan_arm7

URL Indicator | Source: CAL Automated Threat Library

Follow Item | Notification Priority

Active | Status set by

Overview

Details □ Private

Attributes

Search attribute value...

Pinned Attributes

No pinned attributes to display

Other Attributes

- Description
- Source

Playbooks

Name
Zscaler Block Urls and Get Updated Block URLs

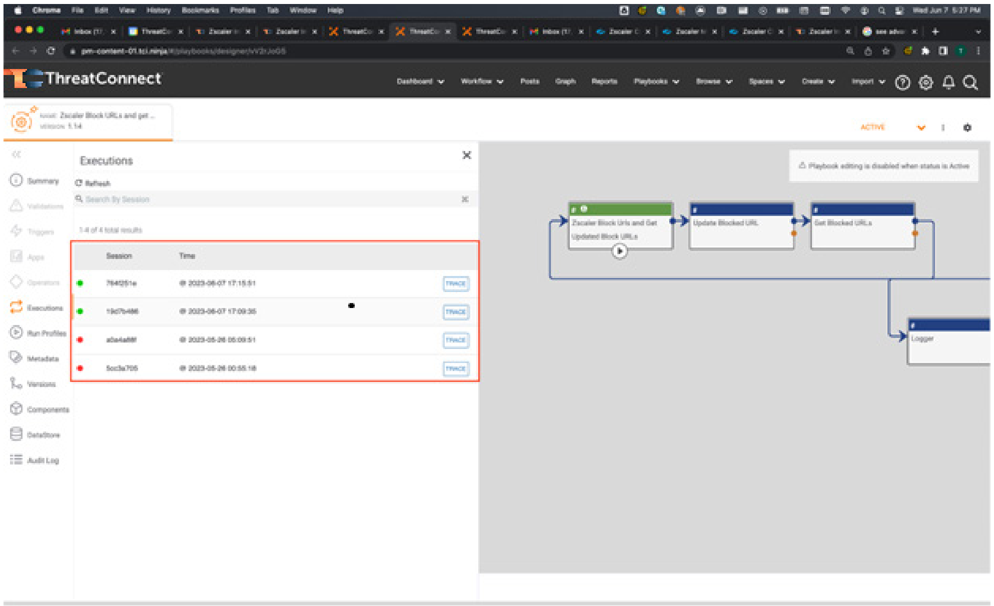
Owners & Feeds

Additional Owners

Owner	ThreatRating	Confidence Rating
No records found		

Figure 16. Browse tab

13. You can see each playbook execution in the **Executions** section of the playbook. Executions marked with a red icon mean that there was an error with the playbook. Executions marked with a green icon mean that the playbook completed successfully.



Executions

1-4 of 4 total results

	Session	Time	
🟢	7641251e	⊕ 2023-06-07 17:15:51	TRACE
🟢	19c7b486	⊕ 2023-06-07 17:09:35	TRACE
🔴	a0a4a88f	⊕ 2023-05-26 05:09:51	TRACE
🔴	5cc3a705	⊕ 2023-05-26 00:55:18	TRACE

Figure 17. Playbook execution

14. After a playbook has successfully completed, you can check the effects of the playbook on the ZIA Admin Portal. For example, you can see the effects of **Update Blocked URLs** action by going to **Policy** > **Security** > **Advanced Threat Protection**.

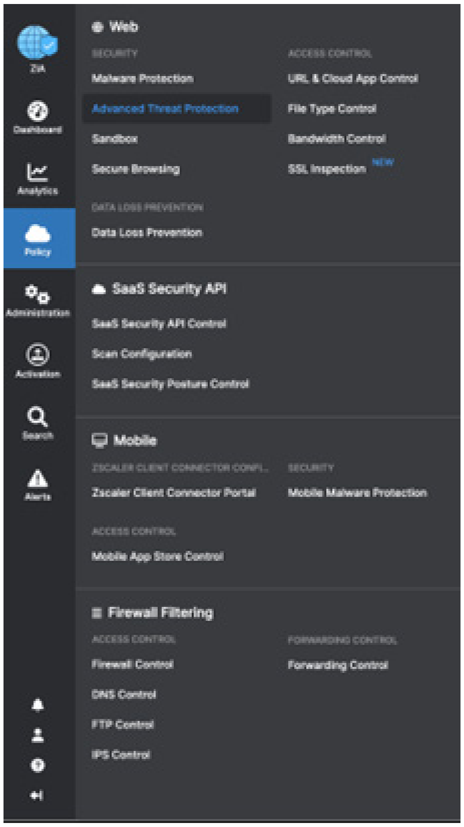
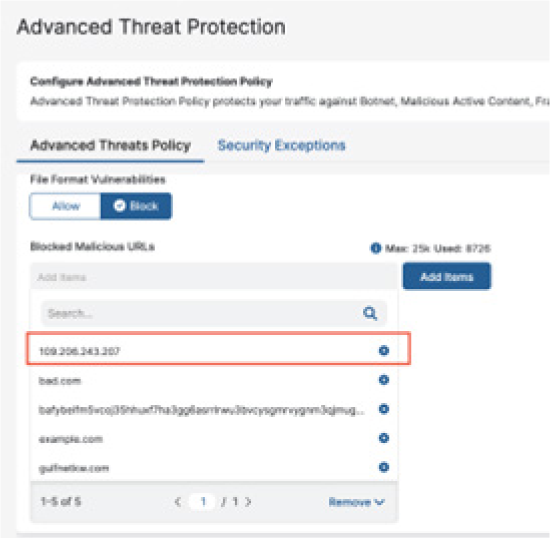


Figure 18. Update Blocked URLs

15. Scroll down to the **Blocked Malicious URLs** section to see that the indicator the playbook ran on was added.



Advanced Threat Protection

Configure Advanced Threat Protection Policy

Advanced Threat Protection Policy protects your traffic against Botnet, Malicious Active Content, Fr

File Format Vulnerabilities: Allow / Block (selected)

Blocked Malicious URLs

Max: 25k Used: 8726

109.206.243.207

bad.com

bafybeifm5vcoj35hhuxf7ha3gg6asrrirwu3bvcysgmrvygnm3qjmug...

example.com

gulfnetkw.com

1-5 of 5

Figure 19. Advanced Threat Protection

ZIA Job App Usage

To use the ZIA Job App:

1. Go to the **Org Settings** section of the **ThreatConnect Platform** using the gear menu.

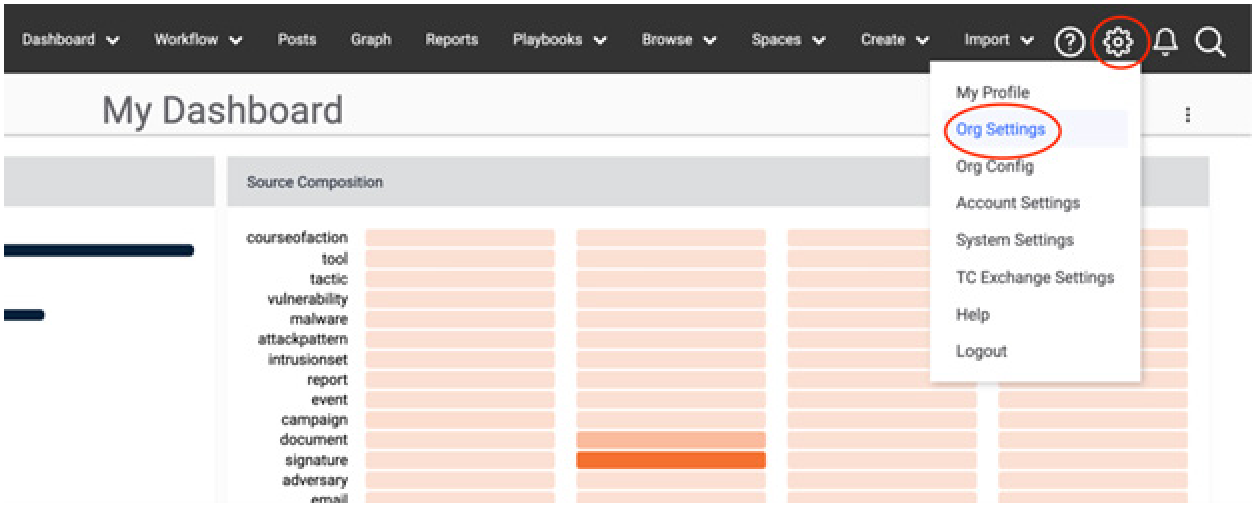
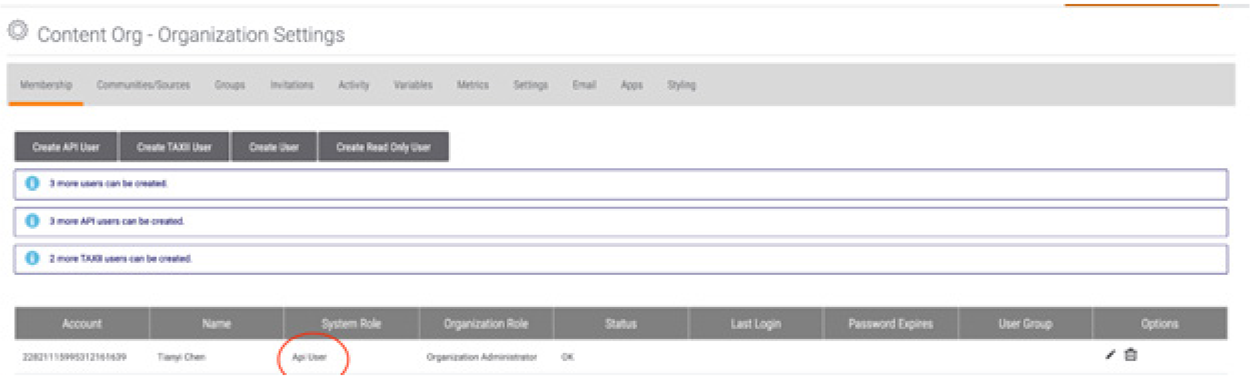


Figure 20. Organization Settings

2. Check that there is an API user in your organization under the **Membership** tab.



3 more users can be created.

3 more API users can be created.

2 more TAXII users can be created.

Account	Name	System Role	Organization Role	Status	Last Login	Password Expires	User Group	Options
22821115995312161639	Tianyi Chen	Api User	Organization Administrator	OK				

Figure 21. Membership tab

3. If there is no user created for the API User, click **Create API User**.

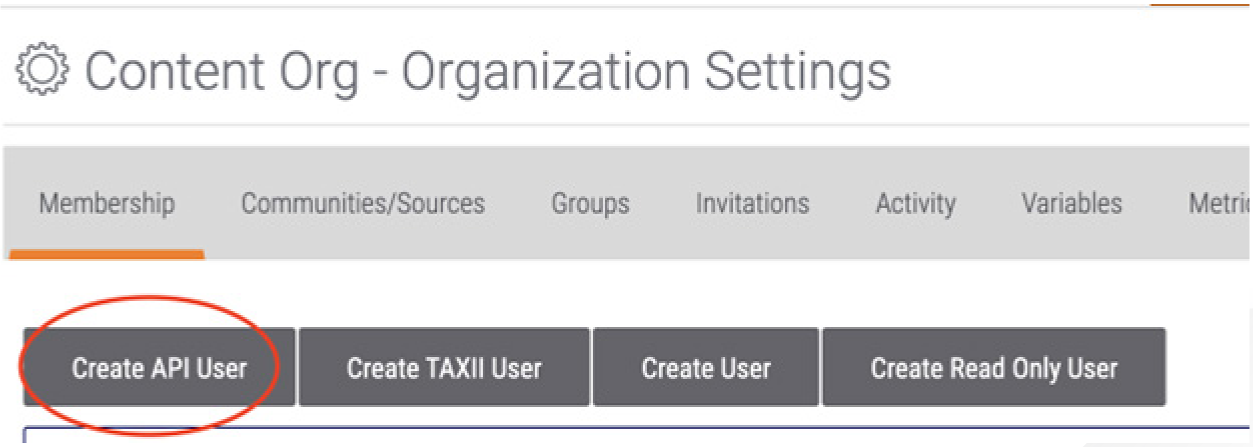
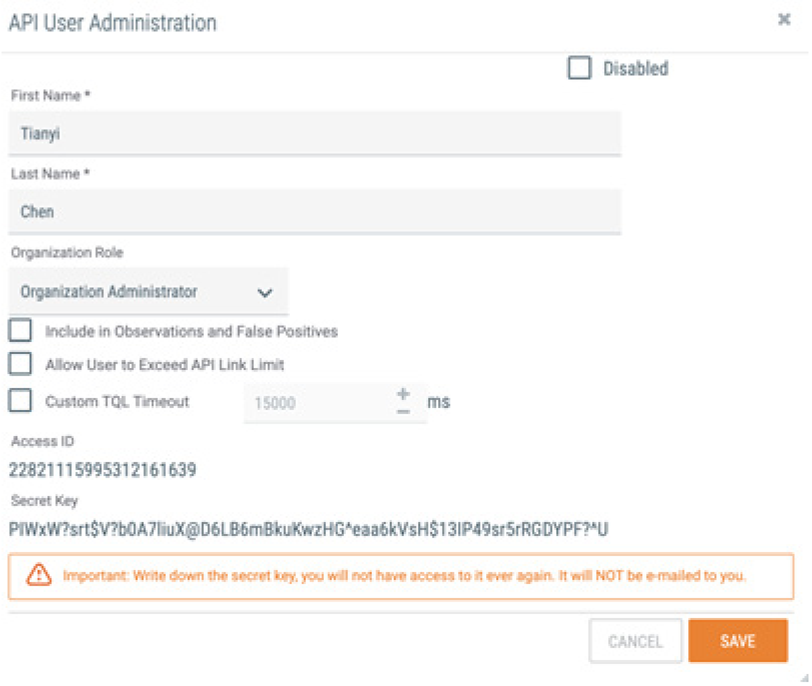


Figure 22. Create API User

4. Select **Organization Administrator** as the **Organization Role**. Note the Secret Key as it is only shown once.
5. Click **Save**.



API User Administration

☐ Disabled

First Name *

Tianyi

Last Name *

Chen

Organization Role

Organization Administrator

☐ Include in Observations and False Positives

☐ Allow User to Exceed API Link Limit

☐ Custom TQL Timeout 15000 ms

Access ID

22821115995312161639

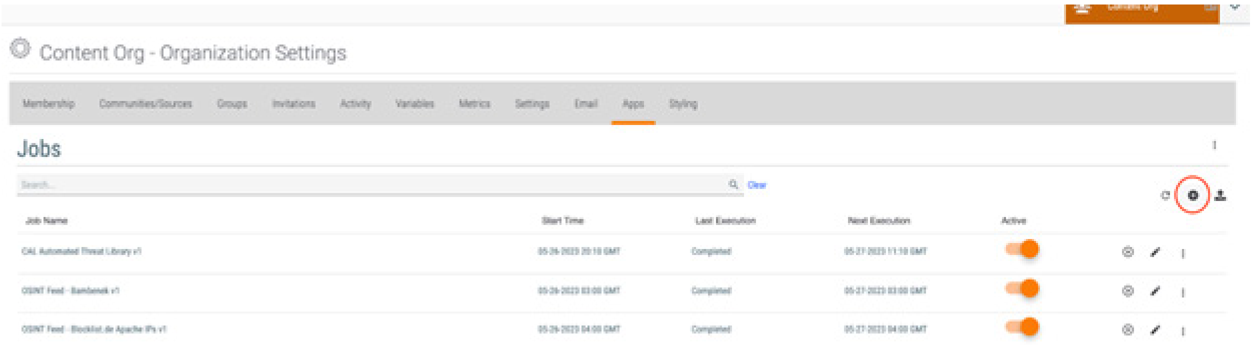
Secret Key

PIWxW?srt$V?b0A7liuX@D6LB6mBkuKwzHG^eaa6kVsH$13IP49sr5rRGDYPF?^U

Important: Write down the secret key, you will not have access to it ever again. It will NOT be e-mailed to you.

Figure 23. API User Administration

6. Select the **Apps** tab under **Organization Settings**, and click **Add** (**+**) on the **Jobs** page to create a Job.



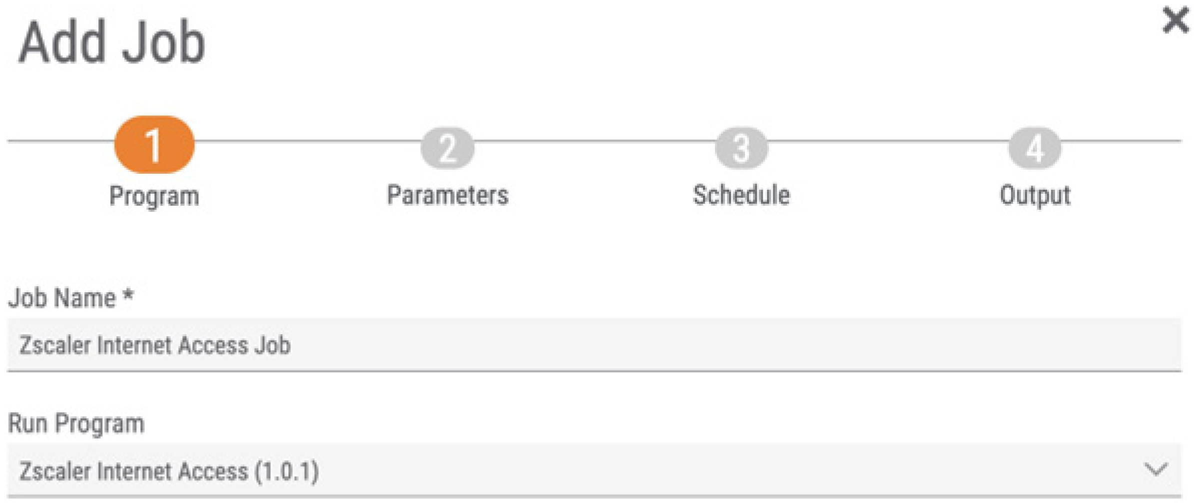
Content Org - Organization Settings

Jobs

Job Name	Start Time	Last Execution	Next Execution	Active
CAL Automated Threat Library v1	05-26-2023 20:10 GMT	Completed	05-27-2023 11:10 GMT	
OSINT Feed - Bambenek v1	05-26-2023 03:00 GMT	Completed	05-27-2023 03:00 GMT	
OSINT Feed - Blocklist.de Apache IPs v1	05-26-2023 04:00 GMT	Completed	05-27-2023 04:00 GMT	

Figure 24. Add a job

7. Select a Job to create. Give the Job an appropriate name and select **Zscaler Internet Access** as the **Run Program**.
8. Click **Next**.



Job Name *

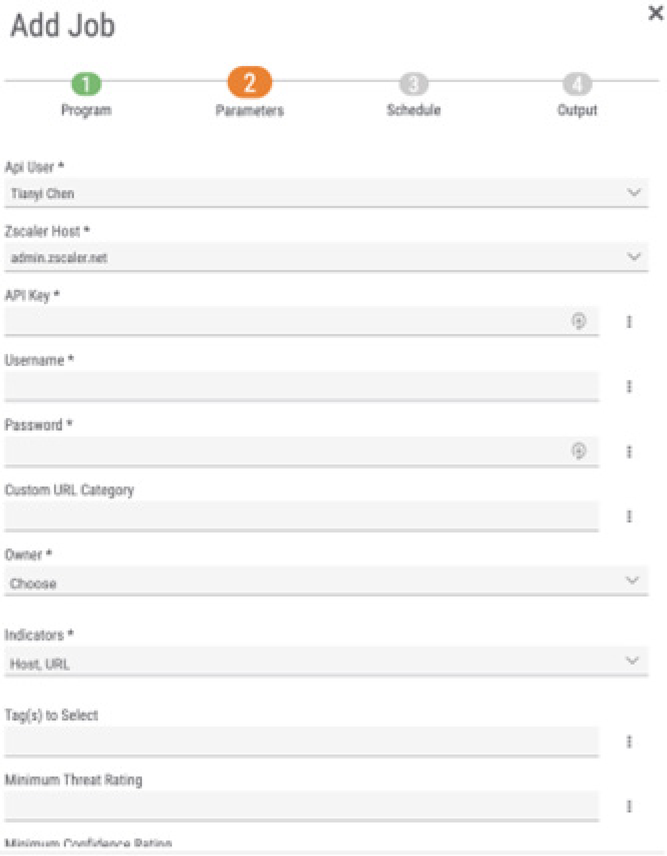
Zscaler Internet Access Job

Run Program

Zscaler Internet Access (1.0.1)

Figure 25. Job Name

9. Mandatory configuration parameters are marked with an asterisk (*) in the **Add Job** wizard. Each configuration parameter is explained next.
   a. For **API User**, select an API User to use from the drop-down menu.
   b. For **Zscaler Host**, select the appropriate Zscaler Host that matches your login URL for Zscaler.
   c. For **API Key**, enter the Zscaler API Key.
   d. For **Username**, enter the Zscaler username that is used to log in to the Zscaler host.
   e. For **Password**, enter the Zscaler password that is used to log in to the Zscaler host.
   f. (Optional) For **Custom URL Category**, select the Zscaler URL category that is added to the URL and Host indicators in the Zscaler host. This custom Category groups all of the indicators and host sent to Zscaler if set.
   g. For **Owner**, Choose the owner in the ThreatConnect platform to pull data from. Each owner represents a source containing Threat Intelligence.
   h. For **Indicators**, select either Host indicators or URL Indicators to send to the Zscaler host.
   i. (Optional) For **Tag(s) to Select**, enter tags by which to filter the data in the sources.
   j. (Optional) For **Minimum Threat Rating**, select the threshold cut off for URL and Host indicators.
   k. (Optional) For **Minimum Confidence Rating**, select the confidence rating cut off for URL and Host indicators.
   l. For **Logging Level**, select how verbose the logs for the job app are.



Api User *
Tianyi Chen

Zscaler Host *
admin.zscaler.net

API Key *

Username *

Password *

Custom URL Category

Owner *
Choose

Indicators *
Host, URL

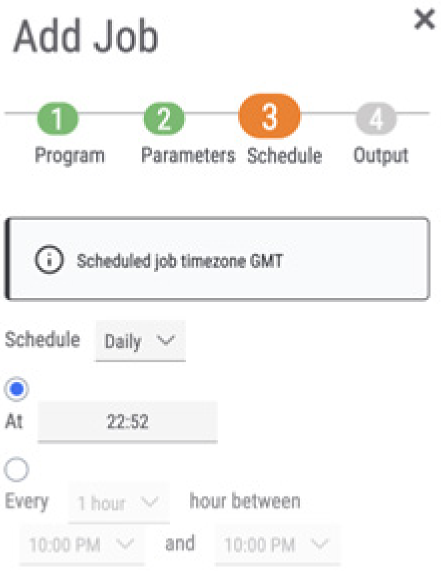
Tag(s) to Select

Minimum Threat Rating

Minimum Confidence Rating

Figure 26. Add job

10. Click **Next**.
11. Set the **Schedule** of the job app for either **Daily** or a set frequency.



Scheduled job timezone GMT

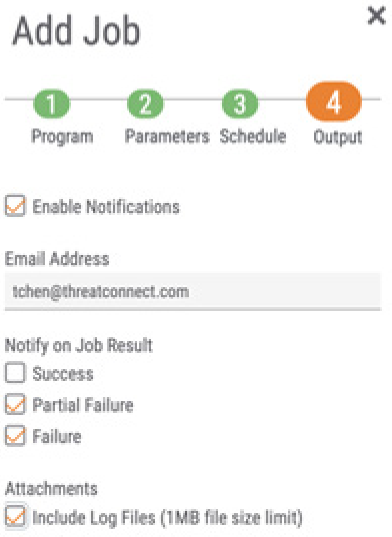
Schedule: Daily

● At 22:52

○ Every 1 hour hour between 10:00 PM and 10:00 PM

Figure 27. Schedule

12. Next, configure notifications for the Job app. Zscaler recommends you enable notifications for job failures.



☑ Enable Notifications

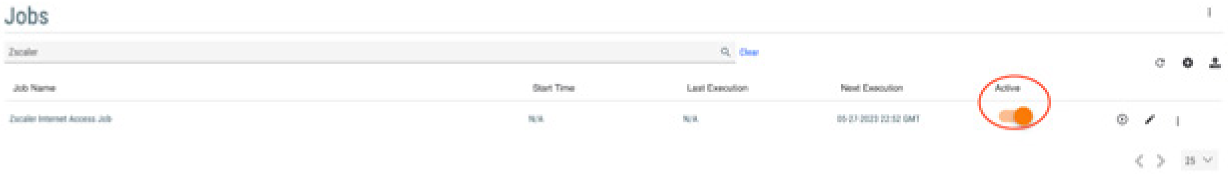
Email Address: tchen@threatconnect.com

Notify on Job Result
☐ Success
☑ Partial Failure
☑ Failure

Attachments
☑ Include Log Files (1MB file size limit)

Figure 28. Notifications

13. Click **Save** to finish configuring the job app.
14. Go to the created job and select **Active**.



Jobs

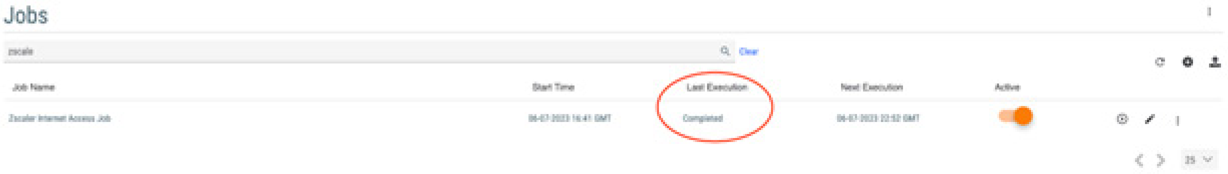
Zscaler

Job Name	Start Time	Last Execution	Next Execution	Active
Zscaler Internet Access Job	N/A	N/A	05-27-2023 22:52 GMT	●

Figure 29. Activate job

The Zscaler Internet Access job is active and runs as scheduled.

After the Job is run, the last execution field is the status of the run. If the status is **Error** or **Partial Error**, there was an issue with the run. Usually this is due to authentication issues, data mismatch, or API errors. If the last execution **Running**, then the job is currently running and shows **Completed** when it is complete.



Jobs

zscale

Job Name	Start Time	Last Execution	Next Execution	Active
Zscaler Internet Access Job	06-07-2023 16:41 GMT	Completed	06-07-2023 22:52 GMT	●

Figure 30. Job status

15. After the Job is finished, navigate to the ZIA Admin Portal to check the result of the job run. If no custom categories were set, the URL and Host indicators are automatically added to the Zscaler block list.
16. If a custom URL category was set, go to **Administration** > **Access Control** > **URL Categories** to view the result of the job run.

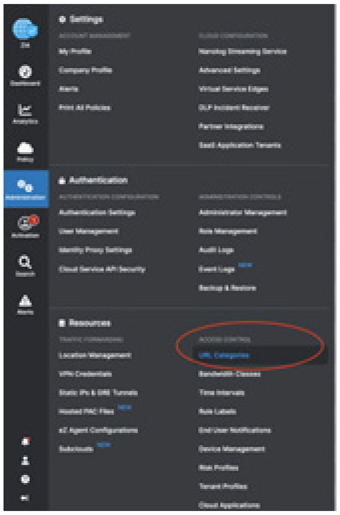
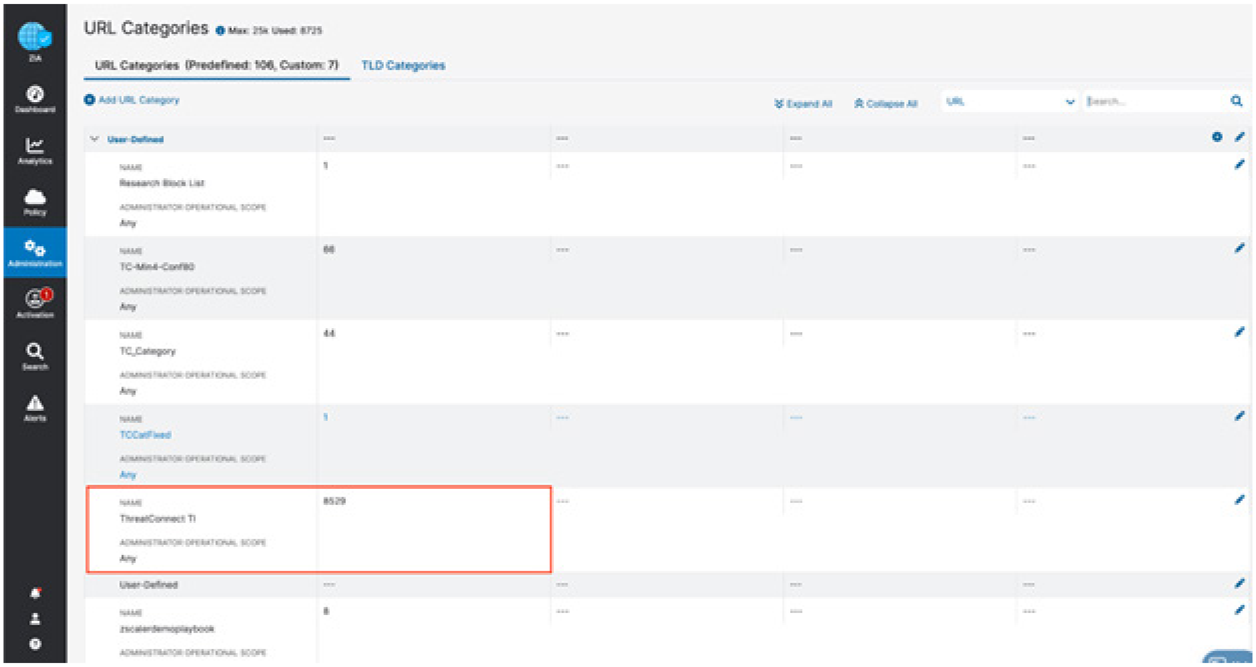


Figure 31. URL Categories

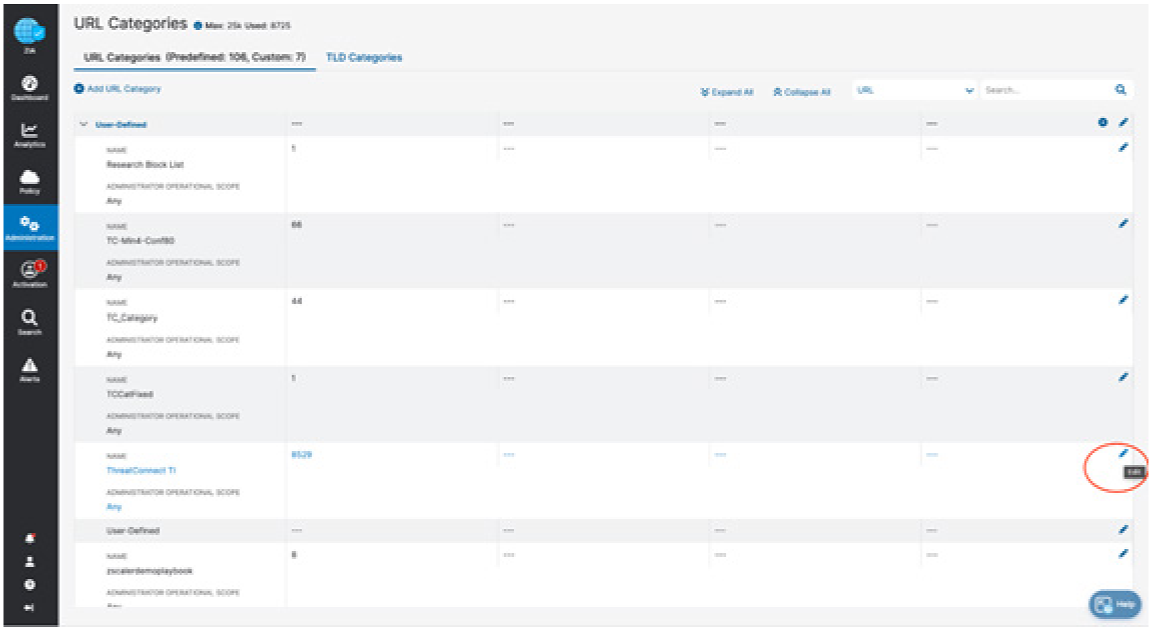
17. In the **URL Categories page**, click the **Custom URL** category section and the custom URL category set appears.



User-Defined	---	---	---	---
NAME Research Block List ADMINISTRATOR OPERATIONAL SCOPE Any	1	---	---	---
NAME TC-Min4-Conf80 ADMINISTRATOR OPERATIONAL SCOPE Any	66	---	---	---
NAME TC_Category ADMINISTRATOR OPERATIONAL SCOPE Any	44	---	---	---
NAME TCCatFixed ADMINISTRATOR OPERATIONAL SCOPE Any	1	---	---	---
NAME ThreatConnect TI ADMINISTRATOR OPERATIONAL SCOPE Any	8529	---	---	---
User-Defined	---	---	---	---
NAME zscalerdemoplaybook ADMINISTRATOR OPERATIONAL SCOPE	8	---	---	---

Figure 32. Custom URL

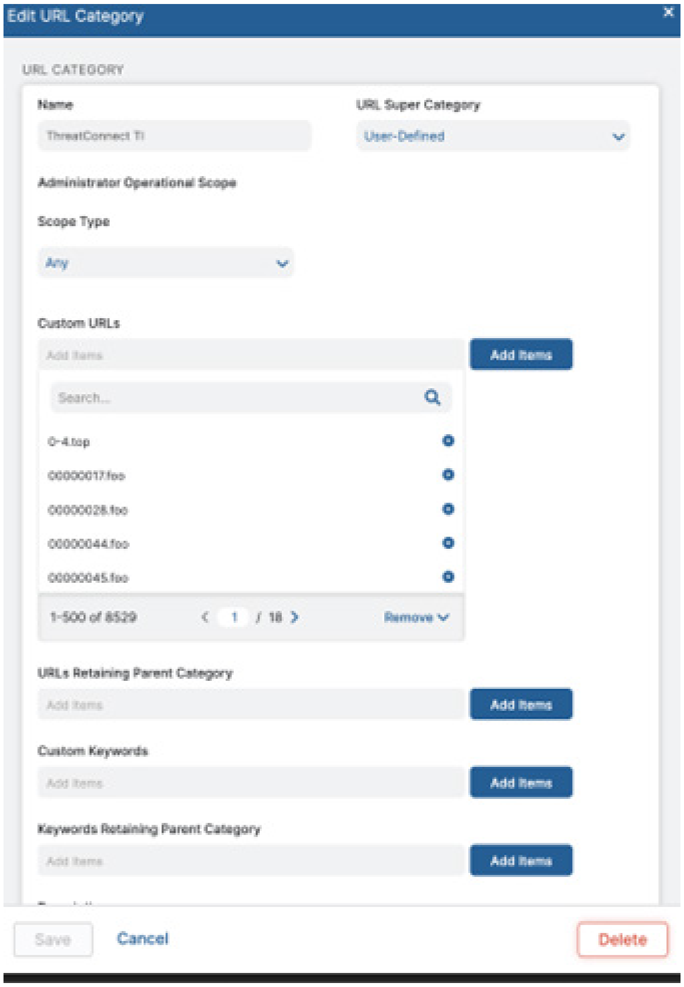
18. Click the **Edit** icon.



User-Defined	---	---	---	---
NAME Research Block List ADMINISTRATOR OPERATIONAL SCOPE Any	1	---	---	---
NAME TC-Min4-Conf80 ADMINISTRATOR OPERATIONAL SCOPE Any	66	---	---	---
NAME TC_Category ADMINISTRATOR OPERATIONAL SCOPE Any	44	---	---	---
NAME TCCatFixed ADMINISTRATOR OPERATIONAL SCOPE Any	1	---	---	---
NAME ThreatConnect TI ADMINISTRATOR OPERATIONAL SCOPE Any	8529	---	---	---
User-Defined	---	---	---	---
NAME zscalerdemoplaybook ADMINISTRATOR OPERATIONAL SCOPE Any	8	---	---	---

Figure 33. Edit URLs and Hosts

You can view the blocked URLs and Hosts.



Edit URL Category

URL CATEGORY

Name: ThreatConnect TI

URL Super Category: User-Defined

Administrator Operational Scope

Scope Type: Any

Custom URLs

- 0-4.top
- 00000017.foo
- 00000028.foo
- 00000044.foo
- 00000045.foo

1-500 of 8529 | 1 / 18

URLs Retaining Parent Category

Custom Keywords

Keywords Retaining Parent Category

Figure 34. Edit blocked URLs and Hosts

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**.

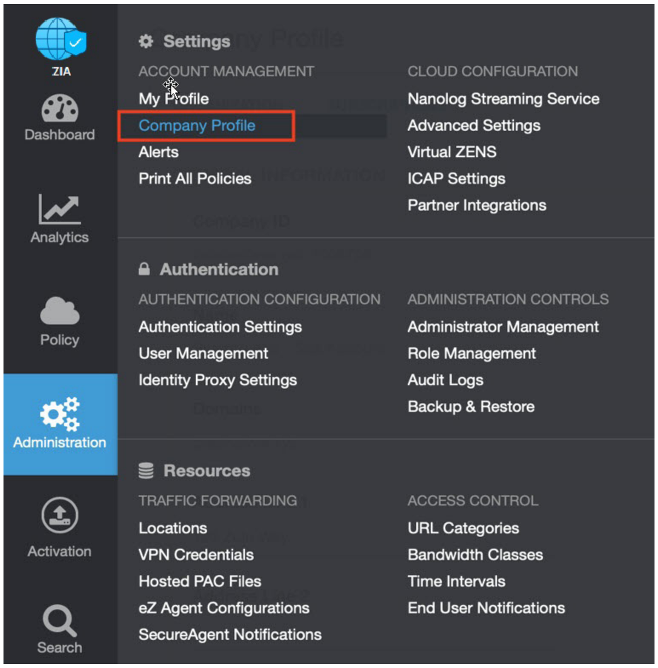
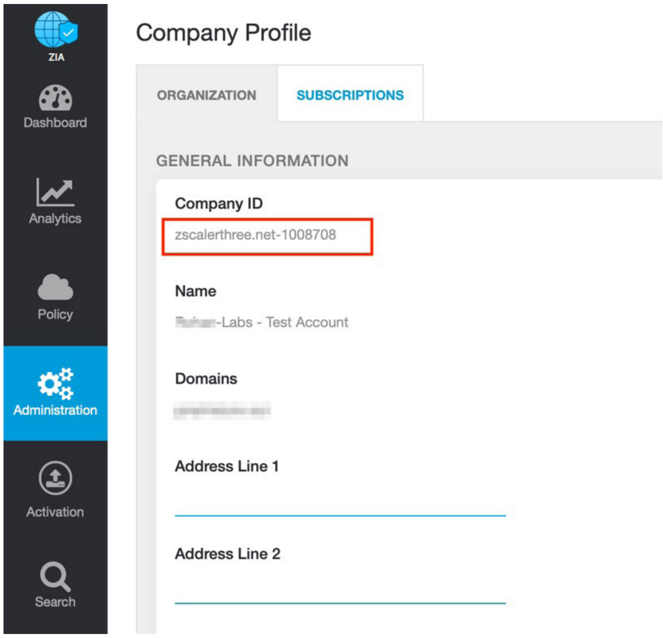


Figure 35. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.



Company Profile

GENERAL INFORMATION

Company ID
zscalerthree.net-1008708

Name
[redacted]-Labs - Test Account

Domains
[redacted]

Address Line 1

Address Line 2

Figure 36. Company ID

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

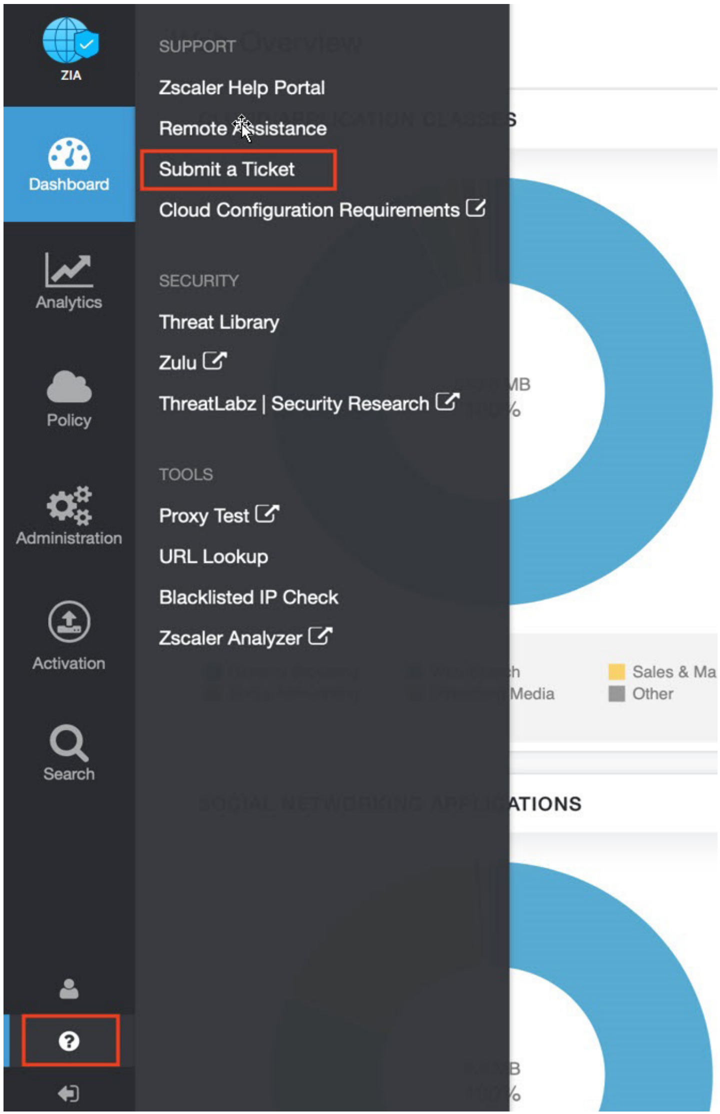


Figure 37. Submit a ticket