



Zscaler™ Internet Access Integration

Software Version 1.0

User Guide

July 14, 2023

30074-02 EN Rev. A



©2023 ThreatConnect, Inc.

ThreatConnect® is a registered trademark, and TC Exchange™ is a trademark, of ThreatConnect, Inc.

Zscaler™ is a trademark of Zscaler, Inc.



Table of Contents

Overview	4
App Installation	4
Zscaler Internet Access Job App	7
Zscaler Internet Access Playbook App	15



Overview


The ThreatConnect® Job App integration with Zscaler Internet Access selects certain URL and Host Indicators in ThreatConnect and adds them to a Zscaler blocklist. The Zscaler Internet Access Playbook App in ThreatConnect can perform several actions in the Zscaler platform, such as managing blocklists, retrieving details on [DLP Dictionaries](#), submitting files to the Zscaler sandbox, and much more.

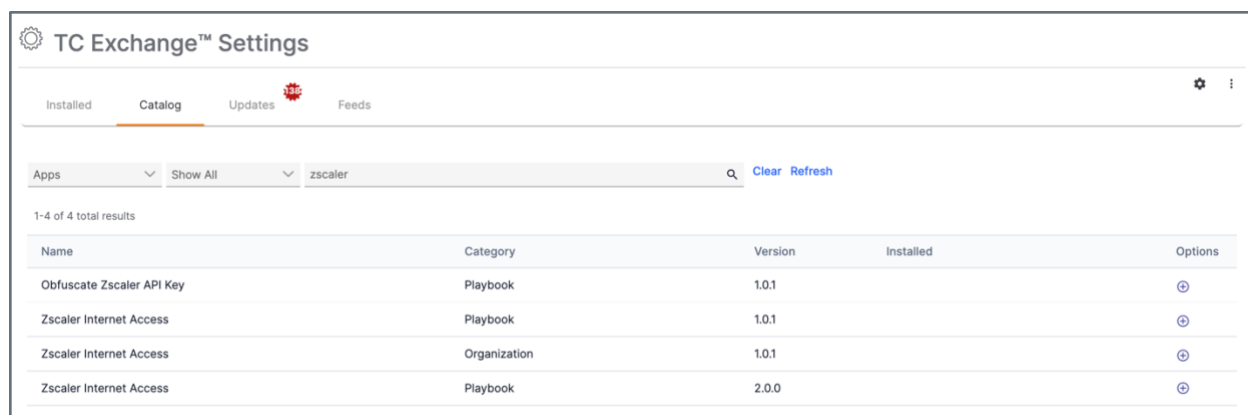
Technical documentation and release notes on these Apps can be found at the following links:

- <https://threatconnect.readme.io/docs/Zscaler-internet-access-job>
- <https://threatconnect.readme.io/docs/Zscaler-internet-access-playbook>

App Installation

Follow the steps in this section to install the Zscaler Internet Access Job and Playbook Apps through TC Exchange™ in ThreatConnect.

1. Log into ThreatConnect with a System Administrator account.
2. On the top navigation bar, hover over **Settings**  and select **TC Exchange Settings**. The **Installed** tab of the **TC Exchange Settings** screen will be displayed.
3. Click the **Catalog** tab. The **Catalog** screen will be displayed.
4. Enter “zscaler” into the search bar to display all available Zscaler Apps on your ThreatConnect instance (Figure 1).



TC Exchange™ Settings				
Installed Catalog Updates Feeds				
Apps Show All zscaler Clear Refresh				
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

- Click **Install** ⊕ in the **Options** column for the Zscaler Internet Access App with “Organization” in the **Category** column. The **Release Notes: Zscaler Internet Access** window will be displayed (Figure 2).



Figure 2

- Allow all organizations:** Select this checkbox if you want to allow all Organizations on the ThreatConnect instance to have access to the App.

Note: If you do not select this checkbox, you can select the Organization(s) that will have permissions to run the App by navigating to the **Installed** tab of the **TC Exchange Settings** screen, locating the **Zscaler Internet Access Job (Organization)** App installed in your Organization, clicking the vertical ellipsis ⋮ in the **Options** column, and selecting **Permissions**.

- Click the **INSTALL** button.

6. Click **Install**  in the **Options** column for the Zscaler Internet Access App with “Playbook” in the **Category** column and the latest version—2.0.0 in this example—in the **Version** column (Figure 1). The **Release Notes: Zscaler Internet Access** window will be displayed (Figure 3).

Important: Always make sure to install the latest version of the App if this is the first time that you are installing it. Older versions can still be used, but will not have the latest features.

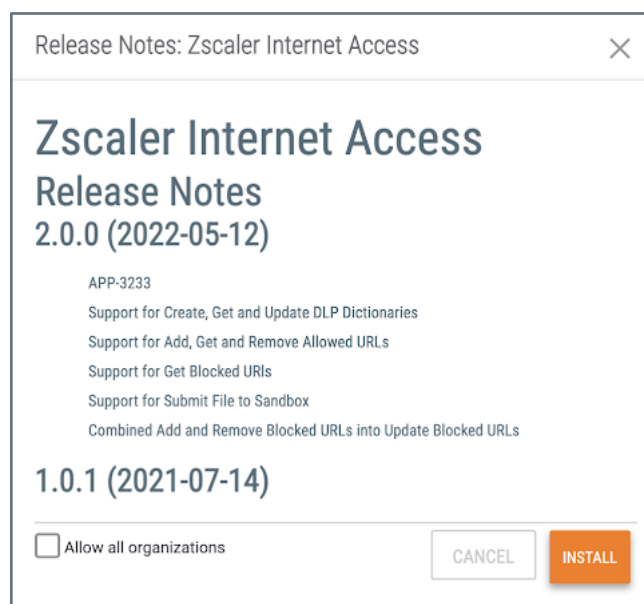



Figure 3


- **Allow all organizations:** Select this checkbox if you want to allow all Organizations on the ThreatConnect instance to have access to the App.

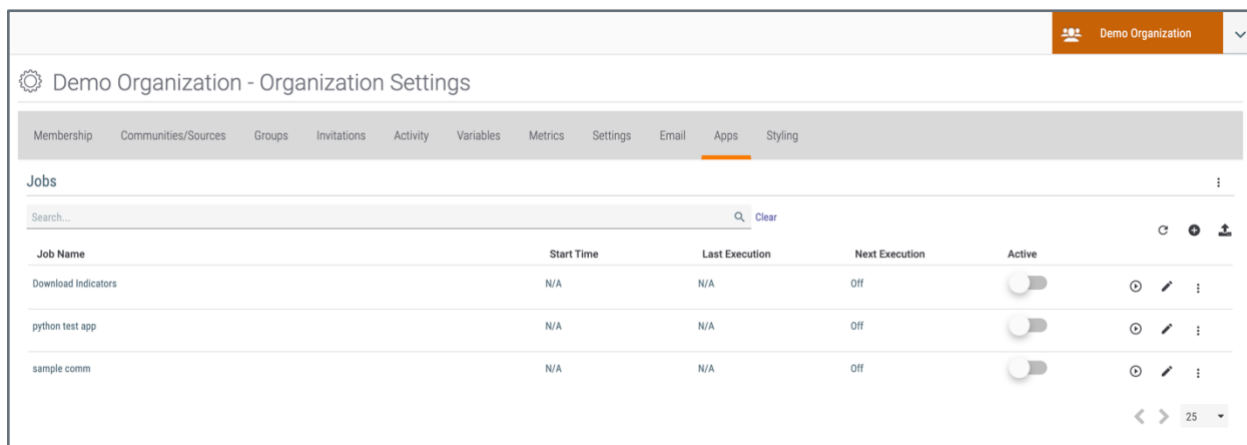
Note: If you do not select this checkbox, you can select the Organization(s) that will have permissions to run the App by navigating to the **Installed** tab of the **TC Exchange Settings** screen, locating the **Zscaler Internet Access** Playbook App installed in your Organization, clicking the vertical ellipsis  in the **Options** column, and selecting **Permissions**.

- Click the **INSTALL** button.

Zscaler Internet Access Job App


Follow the steps in this section to configure and run the Zscaler Internet Access Job App in ThreatConnect and view the results of the App's execution in the Zscaler platform.

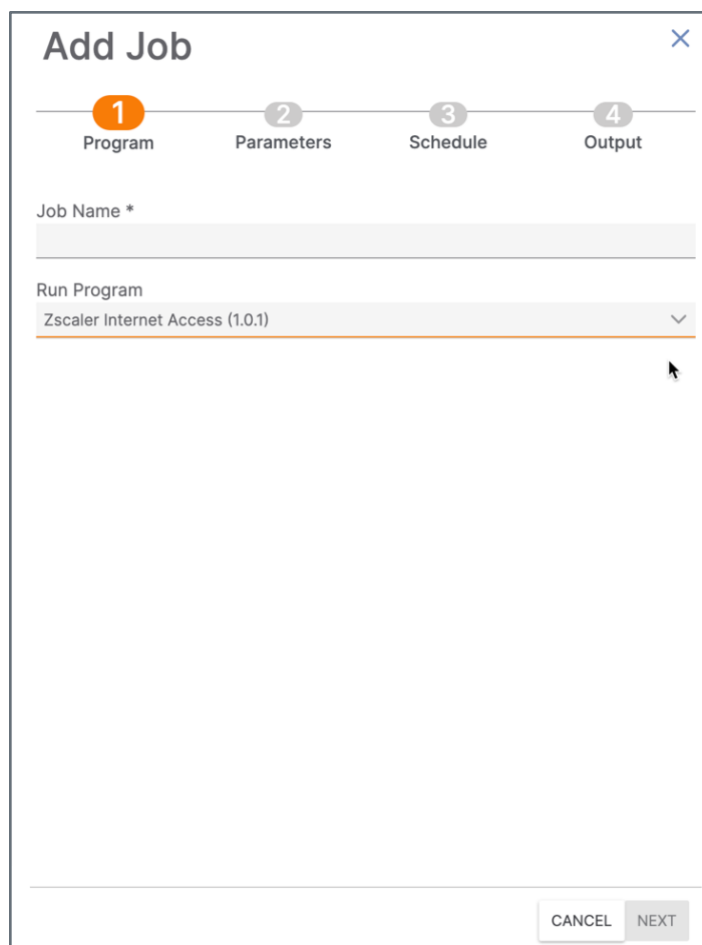
1. Log into ThreatConnect with an account with an [Organization role](#) of Organization Administrator.
2. On the top navigation bar, hover over **Settings**  and select **Org Settings**. The **Membership** tab of the **Organization Settings** screen will be displayed.
3. Confirm that there is a user with a System role of **API User** in your Organization. If not, then [create an API User](#).
4. Click the **Apps** tab. The **Jobs** view of the **Apps** screen will be displayed (Figure 4).



Job Name	Start Time	Last Execution	Next Execution	Active
Download Indicators	N/A	N/A	Off	<input type="checkbox"/>
python test app	N/A	N/A	Off	<input type="checkbox"/>
sample comm	N/A	N/A	Off	<input type="checkbox"/>

Figure 4

5. Click **Add**  at the top right of the table. The **Program** screen of the **Add Job** drawer will be displayed (Figure 5).



The 'Add Job' dialog box features a title bar with a close button (X) in the top right corner. Below the title bar is a progress indicator with four steps: 1. Program (highlighted with an orange circle), 2. Parameters, 3. Schedule, and 4. Output. The main content area includes a 'Job Name *' text input field, a 'Run Program' dropdown menu with 'Zscaler Internet Access (1.0.1)' selected, and a large empty text area below it. At the bottom right, there are 'CANCEL' and 'NEXT' buttons.

Figure 5

- **Job Name:** Enter a name for the Job.
 - **Run Program:** Select **Zscaler Internet Access (1.0.1)** from the dropdown.
 - Click the **NEXT** button.
6. The **Parameters** screen of the **Add Job** drawer will be displayed (Figure 6).

Add Job

1

2

3

4

Program

Parameters

Schedule

Output

Api User *

Select...

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

Logging Level *

Info

CANCEL

PREVIOUS

NEXT

Figure 6

Note: Parameters with an asterisk (*) next to their name are required.

- **API User:** Select the API user to retrieve Indicators from ThreatConnect.
- **Zscaler Host:** Select the Zscaler Internet Access host URL that matches your login URL for Zscaler.
- **API Key:** Enter the Zscaler Internet Access API key used for authentication.
- **Username:** Enter the Zscaler Internet Access username that is used to log into the Zscaler host.
- **Password:** Enter the Zscaler Internet Access password associated with the Username.



- **Custom URL Category:** Enter the Zscaler URL category into which Indicators from ThreatConnect will be grouped and added in the Zscaler Internet Access host.
- **Owner:** Select the ThreatConnect [owner](#) from which Indicators will be retrieved.
- **Indicators:** Select the type(s) of Indicators to send to the Zscaler Internet Access host. Both options (**Host** and **URL**) are selected by default.
- **Tag(s) to Select:** Enter a comma-separated list of ThreatConnect [Tags](#) on which to filter Indicators.
- **Minimum Threat Rating:** Select the minimum [Threat Rating](#) that an Indicator must have in order to be added to the Zscaler Internet Access host.
- **Minimum Confidence Rating:** Select the minimum [Confidence Rating](#) that an Indicator must have in order to be added to the Zscaler Internet Access Host
- **Logging Level:** Select the level of verbosity of the logging output for the App.
- Click the **NEXT** button.

7. The **Schedule** screen of the **Add Job** drawer will be displayed (Figure 7).

Add Job ×

1 Program 2 Parameters 3 **Schedule** 4 Output

ⓘ Scheduled job timezone GMT

Schedule Daily ▾

☒ At 11:18

☐ Every 1 hour ▾ hour between 11:00 AM ▾ and Midnight ▾

CANCEL PREVIOUS NEXT

Figure 7



- **Schedule:** Select the frequency of Job runs.
- **At:** Select this option to schedule a specific time for Job runs, and use the corresponding field to enter the Job run time.
- **Every:** Select this option to schedule Job runs to occur at intervals, and use the corresponding fields to set the specific frequency and interval.
- Click the **NEXT** button.

8. The **Output** screen of the **Add Job** drawer will be displayed (Figure 8).

Figure 8

- **Enable Notifications:** Select this checkbox to receive notifications with the results of Job runs. If this checkbox is not selected, none of the other options in this step will be available.
- **Email Address:** Enter the email address to which notifications should be sent.




- **Notify on Job Result:** Select the checkbox(es) for the type(s) of Job results for which notification emails will be sent.

Note: It is recommended to enable notifications for partial failures and failures.

- **Attachments:** Select the **Include Log Files** checkbox to include log files in notification emails.
 - Click the **SAVE** button.
9. The **Jobs** view on the **Apps** screen will now show the Job created for the Zscaler Internet Access App. Toggle the switch in the **Active** column for the Job on to activate the Job (Figure 9).

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	<input checked="" type="checkbox"/>

Figure 9

10. Once the Job is run (either by waiting until the date and time in the **Next Execution** column or by clicking  to run the Job immediately), the **Last Execution** column will display the status of the run. If the status is “Error” or “Partial Error,” there was an issue with the run, usually because of authentication issues, data mismatches, or API errors. If the status is “Running,” then the Job is currently running. If the Job completes successfully, the status will be “Completed.”
11. Once the Job has successfully completed, navigate to **Administration** → **Access Control** → **URL Categories** in the Zscaler platform to view the result of the run (Figure 10). If no custom categories were set, the URL and Host Indicators will automatically get added to the Zscaler blocklist.

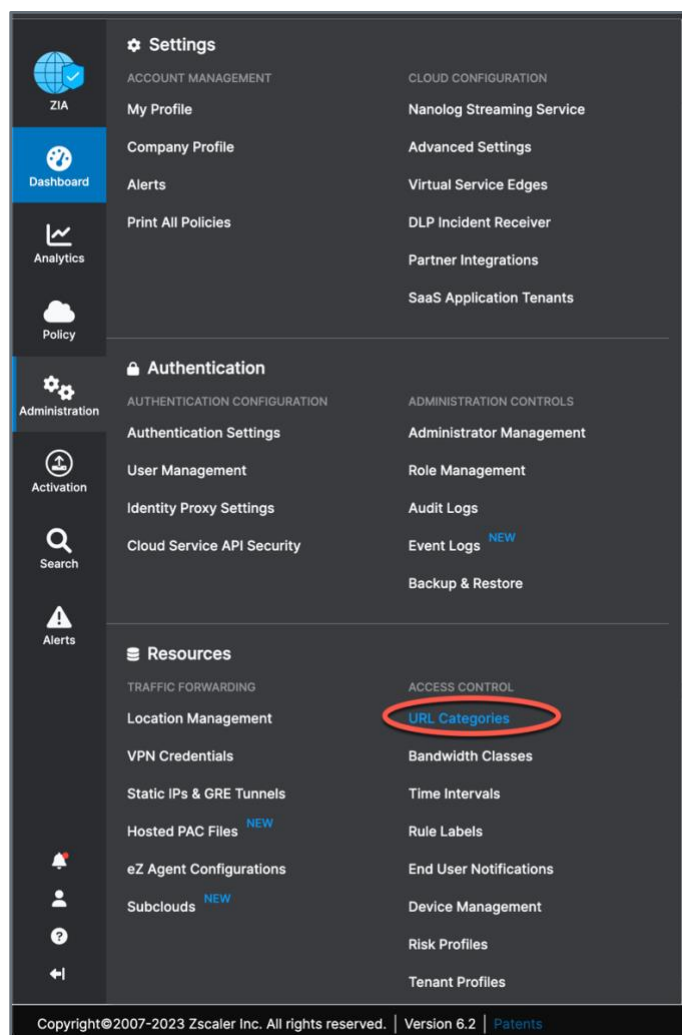


Figure 10

12. From the **URL Categories** screen, click on the **User-Defined** section to view all custom URL categories. Locate the **ThreatConnect TI** section (Figure 11).



URL Categories • Max: 25k Used: 8726					
URL Categories (Predefined: 106, Custom: 7) TLD Categories					
Add URL Category Expand All Collapse All URL Search...					
NAME	44	---	---	---	
TC_Category					
ADMINISTRATOR OPERATIONAL SCOPE					
Any					
NAME	1	---	---	---	
TCCatFixed					
ADMINISTRATOR OPERATIONAL SCOPE					
Any					
NAME	8529	---	---	---	
ThreatConnect TI					
ADMINISTRATOR OPERATIONAL SCOPE					
Any					
User-Defined	---	---	---	---	
NAME	8	---	---	---	
zscalerdemo-playbook					
ADMINISTRATOR OPERATIONAL SCOPE					
Any					
NAME	77	---	---	---	
ZscalerDemoRun					
ADMINISTRATOR OPERATIONAL SCOPE					
Any					
Vehicles	---	---	---	---	
Vehicles	---	---	---	---	
Legal Liability	---	---	---	---	

Figure 11

13. Click the pencil icon to the right of the **ThreatConnect TI** section to edit the category and view the URLs and Hosts that are blocked (Figure 12).

Edit URL Category

URL CATEGORY

NameThreatConnect TI

URL Super CategoryUser-Defined

Administrator Operational Scope

Scope TypeAny

Custom URLs

Add Items

Search...

0-4.top00000017.foo00000028.foo00000044.foo00000045.foo

1-500 of 85291 / 18Remove

URLs Retaining Parent Category

Add Items

Custom Keywords

Add Items

Keywords Retaining Parent Category


Add Items

SaveCancelDelete

Figure 12

Zscaler Internet Access Playbook App

Follow the steps in this section to add the Zscaler Internet Access Playbook App to a Playbook, configure the App within the Playbook, and view the results of the Playbook's execution in the Zscaler platform.

1. Log into ThreatConnect with an account with a non-read-only [Organization role](#) (that is, any role other than Read Only User or Read Only Commenter).
2. Navigate to the [Playbooks screen](#), and [create a new Playbook](#).
3. To add the Zscaler Internet Access App to the Playbook, click Apps  on the [side navigation bar](#) of the [Playbook Designer](#) and enter “zscaler” in the search bar. Click on the Zscaler Internet Access App in the search results. The App will be added to the design pane (Figure 13). See [Adding an App](#) for further information.

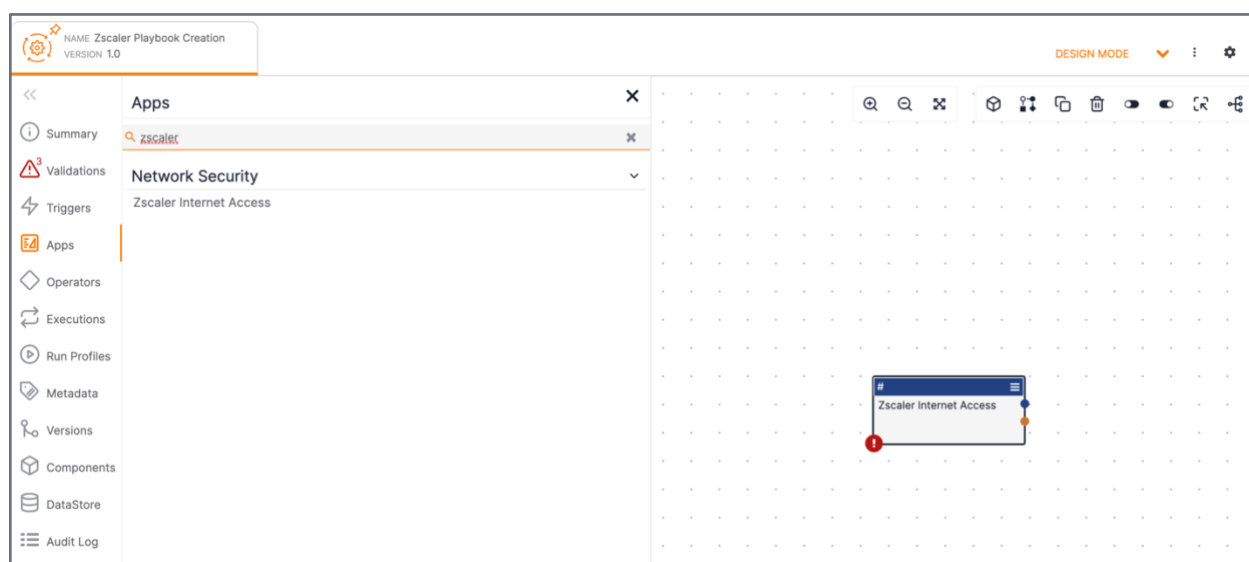


Figure 13

4. If desired, move the App in the design pane, and then double-click the App to open the **Edit App** configuration pane on the left side of the screen. It is recommended to toggle the **Inline Steps** slider on so that all the configuration steps are displayed (Figure 14).



The screenshot shows the 'Edit App' configuration window for 'Zscaler Internet Access'. The window has a title bar with a close button (X). Below the title bar, the app name 'Zscaler Internet Access' is displayed. To the right of the app name is a toggle switch for 'Inline Steps' which is currently turned on, and a document icon. The main configuration area is divided into several sections: 'Job Name *' with a text field containing 'Zscaler Internet Access'; 'Action' with a dropdown menu showing 'Create a DLP Dictionary'; 'Connection' with fields for 'Zscaler Host *' (containing 'https://zsapi.zscaler.net'), 'API Key *', 'Username *', and 'Password *'; 'Configure' with a 'Name *' field, a 'Match Type *' dropdown set to 'Match All' with a 'String' button, and sections for 'Phrases' and 'Patterns' each with 'Key' and 'Value' input fields and a plus icon; and 'Advanced' with a note 'No inputs to complete in this section.' At the bottom right are 'CANCEL' and 'SAVE' buttons.

Figure 14

Note: Parameters with an asterisk (*) next to their name are required. Click **Display Documentation** at the upper right of the **Edit App** pane to view information about the App, including its version, a description, input parameters, and output variables. Release notes and more detailed action, description, and parameter information may be found at [Zscaler Internet Access: Playbook](#).

- **Job Name:** Enter a name for the App that represents its function within the Playbook.

- **Action:** Select the mode of operation for the App. See [Zscaler Internet Access: Playbook](#) for descriptions of all options in the dropdown.
 - **Zscaler Host:** Enter the base URL for your Zscaler instance.
 - **API Key:** Enter your Zscaler API key.
 - **Username:** Enter your Zscaler API admin email address.
 - **Password:** Enter your Zscaler API admin password.
 - **Configure:** The fields displayed in this section are specific to the selected action. See [Zscaler Internet Access: Playbook](#) for descriptions of all possible fields.
 - **Advanced:** The fields, if any, displayed in this section are specific to the selected action. See [Zscaler Internet Access: Playbook](#) for descriptions of all possible fields.
 - Click the **SAVE** button.
5. Add, configure, and [connect](#) a [Trigger](#), other [Apps](#), and [Operators](#) to complete the Playbook logic. Then [activate](#) the Playbook and [execute](#) it as desired. Figure 15 shows a simple Playbook using the Zscaler Internet Access Playbook App. You can also use multiple Zscaler Internet Access Playbook Apps utilizing different actions in a single Playbook.

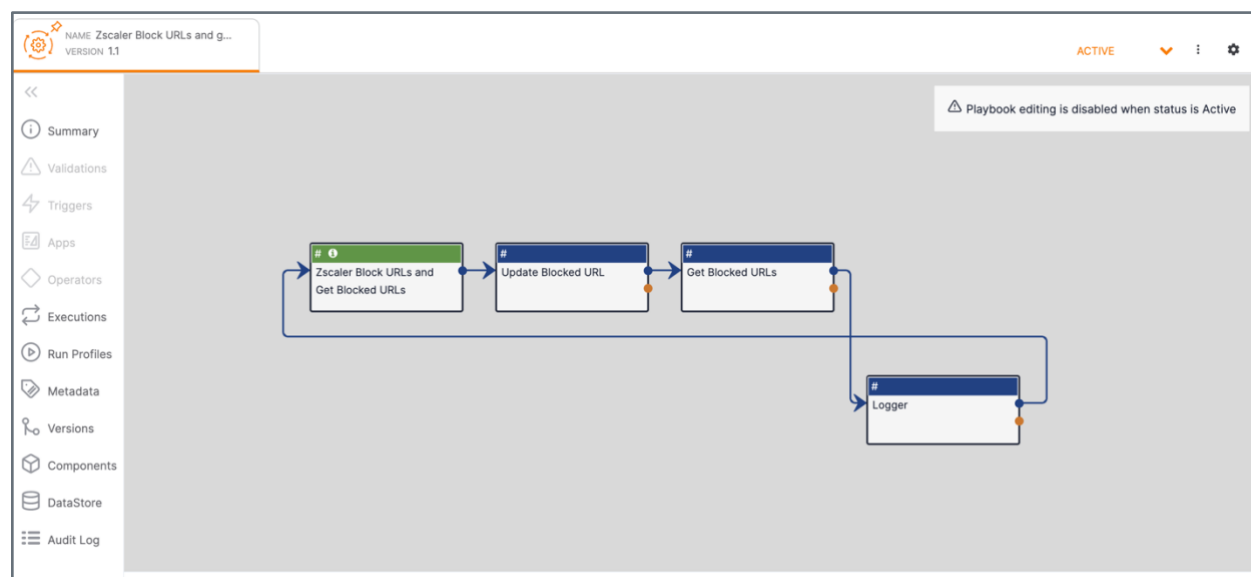


Figure 15

6. Once a Playbook that uses the Zscaler Internet Access App has successfully executed, you can view the results of the Playbook execution in the Zscaler platform. For example, you can see the results of the **Update Blocked URLs** action by navigating to **Policy → Security → Advanced Threat Protection** (Figure 16).

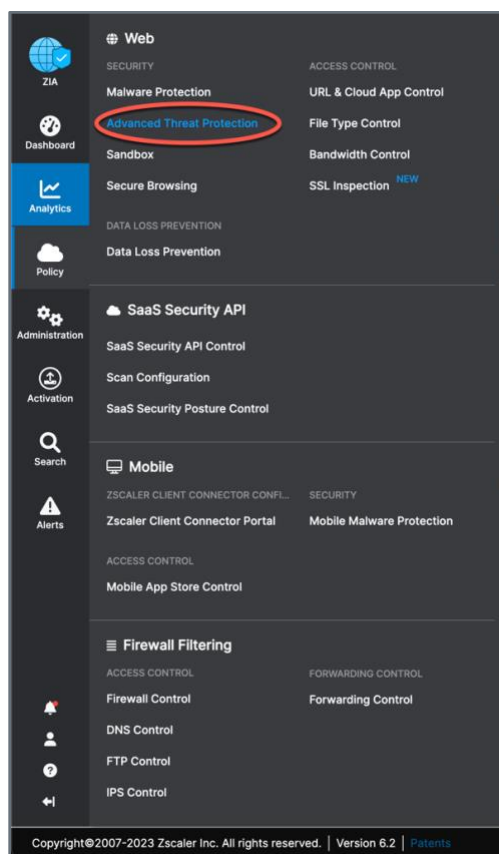


Figure 16

7. Scroll down to the **Blocked Malicious URL** section to verify that the Indicator the Playbook processed (the **109.206.243.207** Address Indicator in this example) was added (Figure 17).

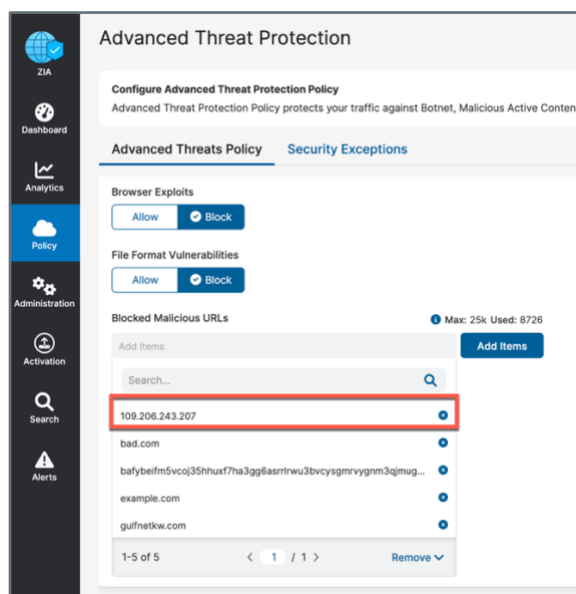


Figure 17