Configuration Guide
Configuration Guide

Zscaler can be configured with the CTIX application in two ways.

1. As an enrichment tool - Configure Zscaler as an enrichment tool to enrich threat data such as hash, domain, or URLs in the CTIX application. See Configuring Zscaler as an enrichment tool.

2. As an internal application - Configure Zscaler as an internal application in CTIX to support your organization’s security operations. The CTIX application can then send whitelisted and blacklisted URLs to Zscaler. See Configuring Zscaler as an internal application.
Requirements

Configuring Zscaler as an enrichment tool

Zscaler is available as an app in the CTIX application. Follow the below steps to configure the app in the CTIX application and get started:

1. Navigate to the Enrichment Management module. This section displays the list of all available apps.

2. Use the search bar to locate ZScaler and click the app to open the configuration page.

3. Select Add New Account

4. Provide a name for your account and enter other authentication details such as Base URL, Username, Password, and API Key.

5. After finishing, click Save. Your account will be created successfully. You can also create multiple accounts to manage different connector actions as required.
6. The ZScaler connector in CTIX has the following actions to enrich URL, hash, or domain. Select and enable as you need.

a. Retrieve URL Detail
b. Update Whitelist URLs
c. Update Blacklist URLs
Defining quota

Quota defines the number of hits or calls that you can make to your Zscaler account to fetch information that enhances your intel for a defined time period.

1. From the Administration icon, select the Enrichment Management module.

2. Click Enrichment Tools.

3. Select Zscaler. The page for the specific tool opens with Feed Enrichment Type(s) displayed.

4. On a specific account, click the ellipse (...) and select Manage.

5. Click Edit.

6. On the Edit Account page, select the Quota tab.

7. Choose the Quota duration and enter the limit for that duration.

8. Enter a Start Date and Time for the Quota duration.

9. Select Do not poll after the quota limit to delete the intel that is in the enrichment queue after quota limits are exceeded. Enrichment will not happen for any pending intel.

10. Select Carry forward the remaining intel to carry forward the pending intel so that it can be enriched using the next available quota.

11. Select Usage alert to receive email alert notifications when you are approaching your quota limits for Zscaler.

12. Enter the email addresses in Internal Recipients. These email recipients will receive email notifications on quota limits.
Configuring Zscaler as an internal application

1. Navigate to the Integration Management module

2. Select Internal Application and then select Network Security tab.

3. Select Zscaler card.

4. Configure the account on the top right-hand corner by clicking on the ellipses and selecting the Manage option.
5. Select **Add New Account**.

6. Provide a name for your account and enter other authentication details such as Base URL, Username, Password, and API Key.

7. After finishing, click **Save**. Your account will be created successfully. You can also create multiple accounts to manage different connector actions as required.

8. Select **Manage Actions**.

9. Select an Action and enable it and click **Save**.