Integrating ThreatStream with Zscaler

The ThreatStream integration with Zscaler enables the forwarding of IP addresses, domains, and URLs to Zscaler on a daily basis for blocking. A maximum of 25,000 observables per day will be forwarded based on a search query that you define.

Setting up the integration is a two part process. You must first activate the integration on the ThreatStream user interface and then configure a filtering policy within Zscaler to block the observables sent by ThreatStream. Before activating the integration, ensure that the following prerequisites are met:

- On Zscaler, your organization must have a Service Account with API access
- (Recommended) On Zscaler, create a dedicated Administrator Role and Administrator User for the integration. See Adding Admins in the Zscaler documentation for more information.
- On ThreatStream, your organization must have purchased a ThreatStream Tier 2 integration bundle

Activating the Zscaler Integration in ThreatStream

To activate the Zscaler integration on ThreatStream:

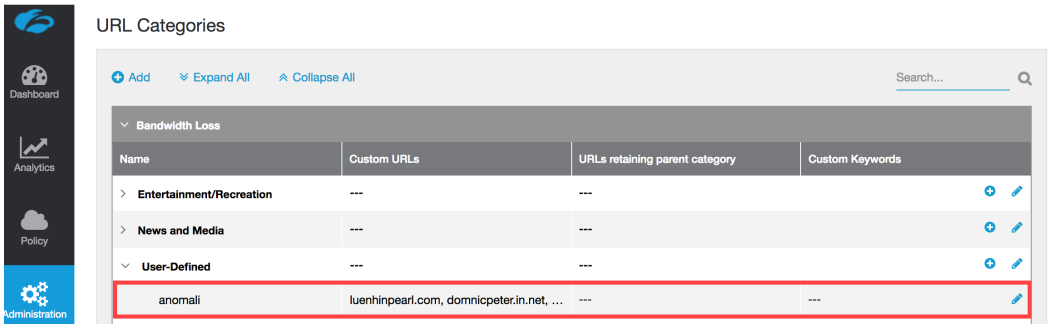
1. In the top navigation bar, click  and then **Integrations**.
2. Click **Activate** in the Zscaler box.
3. Enter your Zscaler **API Base URI**. See Getting Started in the Zscaler API documentation for information on retrieving the base URI.
4. Enter the **Username** associated with the dedicated Zscaler Administrator that you created.
5. Enter the **Zscaler Password** associated with the dedicated Zscaler Administrator that you created.
6. Enter your **Zscaler API Key**.

Tips:
- See Getting Started in the Zscaler API documentation for information on retrieving your API key.
- See About API Key Management in the Zscaler API documentation for information on regenerating your API key.

7. Enter a **Search Query** that defines the subset of data you want to send to Zscaler.
8. Click **Save**.

Finalizing Integration Configuration in Zscaler

To finalize integration setup, you must configure a URL Filtering Policy to block the observables sent to Zscaler from ThreatStream. By default, observables are stored on Zscaler under User Defined URL Categories within *anomali*, as displayed below.



The URL Filtering Policy you create must be configured to block the *anomali* category. See Configuring the URL Filtering Policy for more information.

After configuring the URL Filtering Policy, integration setup is complete.