ZSCALER AND SWIMLANE DEPLOYMENT GUIDE

JULY 2023, VERSION 1.5.10

BUSINESS DEVELOPMENT GUIDE

Contents

Terms and Acronyms 4

Trademark Notice 5

About This Document 6

- Zscaler Overview 6
- Swimlane Overview 6
- Audience 6
- Software Versions 6
- Request for Comments 6

Zscaler and Swimlane Introduction 7

- ZIA Overview 7
- ZPA Overview 7
- Swimlane Turbine Overview 9
- Swimlane Resources 9

System Requirements for an Embedded Cluster Install 10

- External MongoDB Resource Recommendations 11
- Remaining Swimlane Cluster Resources 11
- Resource Utilization Thresholds 11

Deploying the Zscaler Integration 12

- Prerequisites for the Zscaler Integration 12
- Generating an API Key in Zscaler 12
- Create a Task 13
- Configure a Task 15
- Set Triggers 16
- Set Scheduled Trigger 17

Upload the Zscaler Plugin 17

Creating an Asset for Zscaler API Key 18

Create Key Store Entry for Zscaler 19

Appendix A: Requesting Zscaler Support 20

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
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Center
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
XDR	Extended Detection and Response
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.

Swimlane Overview

Swimlane is the leader in cloud-scale, low-code security automation. Supporting use cases beyond SOAR, Swimlane improves the ease with which security teams can overcome process and data fatigue, as well as chronic staffing shortages. Swimlane unlocks the potential of automation beyond the SOC by delivering a low-code platform that serves as the system of record for the entire security organization and enables anyone within the organization to contribute their knowledge and expertise to the protection of the organization. To learn more, refer to Swimlane'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
- Swimlane 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 Swimlane Introduction

Overviews of the Zscaler and Swimlane 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.

ZPA Overview

ZPA is a cloud service that provides secure remote access to internal applications running on a cloud or data center using a Zero Trust framework. With ZPA, applications are never exposed to the internet, making them completely invisible to unauthorized users. The service enables the applications to connect to users via inside-out connectivity rather than extending the network to them.

ZPA provides a simple, secure, and effective way to access internal applications. Access is based on policies created by the IT administrator within the ZPA Admin Portal and hosted within the Zscaler cloud. On each user device, software called Zscaler Client Connector is installed. Zscaler Client Connector ensures the user's device posture and extends a secure microtunnel out to the Zscaler cloud when a user attempts to access an internal application.

Zscaler Resources

The following table contains links to Zscaler resources based on general topic areas.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
ZPC Help Portal	Help articles for ZPC.
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.
ZPA Help Portal	Help articles for ZPA.
ZPC Help Portal	Help articles for ZPC.
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.

Swimlane Turbine Overview

Swimlane Turbine is a low-code security automation platform that combines human and machine intelligence to serve as your system of record for security.

Swimlane built Turbine for the future of automation. It provides flexibility and an environment-agnostic approach to deliver greater value than legacy SOAR, no-code automation, or a combination of SIEM and XDR solutions.

Turbine makes democratized automation possible. It's simpler to deploy and manage than legacy SOAR tools, yet extends visibility and actionability beyond the SOC. Turbine makes automation approachable and integrates with any API so you can unify any workflow, telemetry source or team.

Swimlane Resources

The following table contains links to Swimlane support resources.

Name	Definition
Swimlane Bundle Repository	Download Swimlane software.
Swimlane Knowledge Center	Online Swimlane knowledge repository.
Swimlane Support Portal	Online Swimlane support requests.
Swimlane Community	Online Swimlane user community.

System Requirements for an Embedded Cluster Install

While the Swimlane platform can be installed on a single node for testing, Zscaler recommends a three+ node cluster for production environments to provide redundancy and high availability (HA). Any multiple node cluster must have an odd number of total nodes.

This table details the recommended sizing and data per node:

Components	Single Node	3 Node Cluster - Small	3 Node Cluster - Medium	3 Node Cluster - Large
CPU	8 CPU cores	8 CPU cores	16 CPU cores	32 CPU cores
Memory	32 GB RAM	32 GB RAM	64 GB RAM	128 GB RAM
Storage	600 GB SSD / 3000 IOPS per node	600 GB SSD / 3000 IOPS per node	1 TB SSD / 3000 IOPS per node	1 TB SSD / 3000 IOPS per node
Record Creation Boundaries + Active Users	Records created in a day: 250,000 Total records: 5 million Active users: 10	Records created in a day: 500,000 Total records: 20 million Active users: 30	Records created in a day: 1 million Total records: 20 million Active users: 50	Records created in a day: 1 million Total records: 20 million Active users: 200
Integration Calculations	Integrations in use < 20 average Integration actions/day < 250,000	Integrations in use < 20 average Integration actions/day < 500,000	Integrations in use < 20 average Integration actions/day < 1 million	Integrations in use > 20 average Integration actions/day < 1 million
Pods	API: 1 Tasks: 1 Web: 1 MongoDB: 1	API: 3 Tasks: 3 Web: 3 MongoDB: 3	API: 3 Tasks: 3 Web: 3 MongoDB: 3	API: 6 Tasks: 9 Web: 3 MongoDB: 3

Swimlane does not support spinning disks.

External MongoDB Resource Recommendations

The following table illustrates the resource recommendations (per node) for a standalone MongoDB deployment. These values can be subtracted from the system requirements when allocating resources for the remainder of the Swimlane pods. For more information about deploying on an External MongoDB cluster, refer to Swimlane's Knowledge Center.

Components	Single Node	3 Node Cluster - Sm	3 Node Cluster - Med	3 Node Cluster - Lg
CPU	4 CPU Cores	4 CPU Cores	8 CPU Cores	8 CPU Cores
Memory	16 GB RAM	16 GB RAM	16 GB RAM	32 GB RAM
Storage	300 GB SSD / 3000 IOPS per node	300 GB SSD / 3000 IOPS per node	700 GB SSD / 3000 IOPS per node	700 GB SSD / 3000 IOPS per node

Remaining Swimlane Cluster Resources

The following table illustrates the resources necessary for the remainder of Swimlane if you are using external MongoDB resources:

Components	Single Node	3 Node Cluster - Sm	3 Node Cluster - Med	3 Node Cluster - Lg
CPU	4 CPU Cores	4 CPU Cores	8 CPU Cores	24 CPU Cores
Memory	16 GB RAM	16 GB RAM	48 GB RAM	96 GB RAM
Storage	300 GB SSD / 3000 IOPS per node	300 GB SSD / 3000 IOPS per node	300 GB SSD / 3000 IOPS per node	300 GB SSD / 3000 IOPS per node

Resource Utilization Thresholds

All nodes must stay under certain resource utilization thresholds to ensure that pods always have available resources to operate in. If any of the following thresholds are exceeded on a node, all pods on that node are removed until the resource utilization is addressed:

Resource	Threshold
Memory	Less than 100 Mebibytes (MiB) Available
Disk Space (/var/lib/containerd partition)	Less than 15% Available
Disk Space (/var/lib/kubelet partition)	Less than 10% Available
Disk Inodes (/var/lib/kubelet partition)	Less than 5% Available

Deploying the Zscaler Integration

Zscaler uses the Zscaler REST API to integrate with Swimlane. This guide shows you how to upload and set up this integration.

Prerequisites for the Zscaler Integration

This bundle requires API Subscription. To find your subscription:

1. Log in to your ZIA Admin Portal.
2. Go to **Administration** > **Company Profile** > **Subscriptions**. Contact Zscaler Support to enable this feature if it is not among your subscriptions.
3. After the API Subscription is enabled, go to **Administration** > **API Key Management** to retrieve API Key.

Generating an API Key in Zscaler

In your ZIA Admin Portal, go to **Administration** > **API Key Management**.

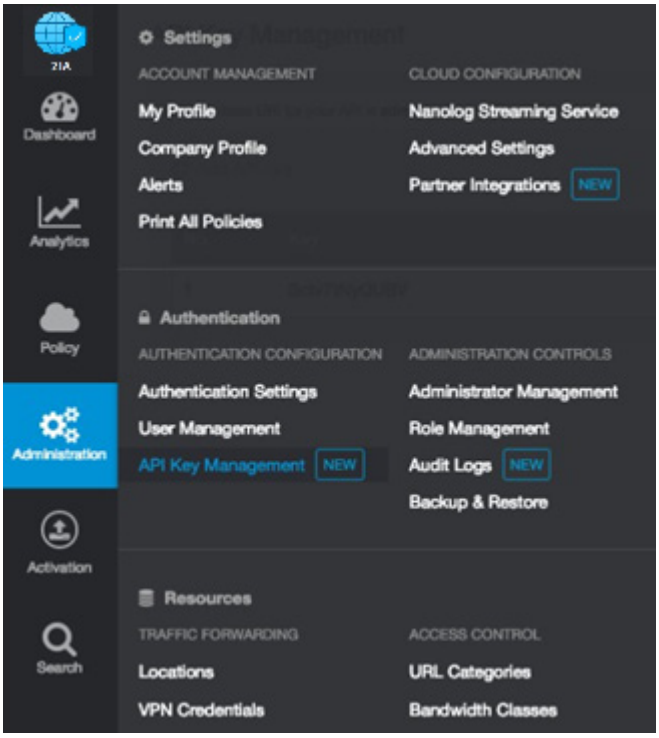

Figure 1. API Key Management

Create a Task

A Swimlane task is an action or series of actions that consist of input, configuration details, output, and triggers. Tasks in Swimlane can be very complex and can contain multiple input and output variables.

Use Swimlane's task creation process to fine-tune the tasks that you want an application to run.

To create a new task:

1. In the Swimland workspace, go to **Integrations** > **Tasks**.
2. Click the **Plus (+)** menu icon, and then select **Create a task**. Alternatively, scroll down the page until you see your application and then click **Create a Task**. In **Create a Task**, Swimlane lists plugin actions.

Figure 2. Create a task

3. Filter by vendor (on the right-side of the page), or type a task, plugin action, or vendor into the filter field. After you find your desired task type, click **Create**.
4. If your task is eligible to be forked, you can also select **Fork** when creating your new task. A forked task is copied as an editable Python script.

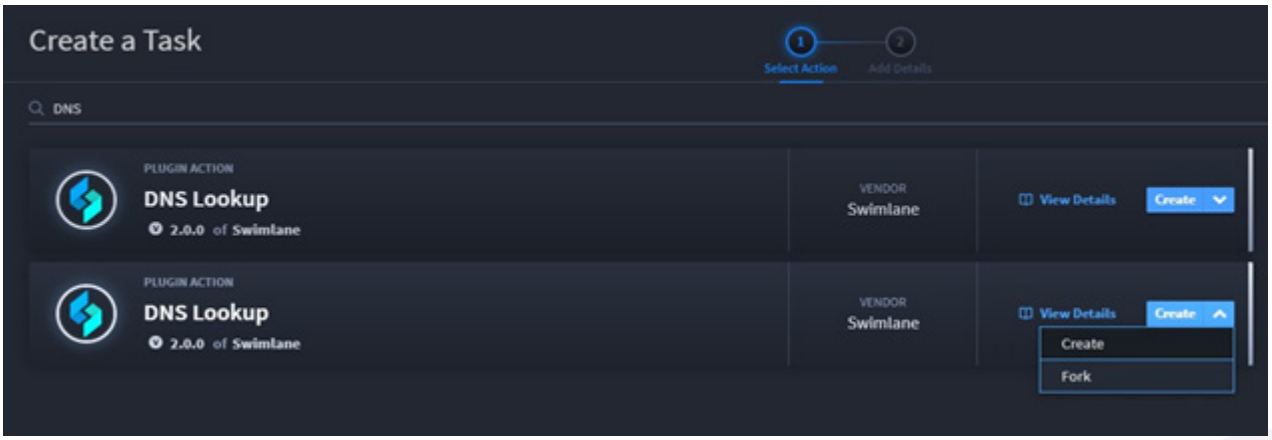

Figure 3. Create a task window

5. Swimlane prompts you to name your task. Associate it with a related application or applet, or leave it as a common task. Applications and applets can only use common tasks or tasks associated with them. You must provide a unique name for your task to save it.

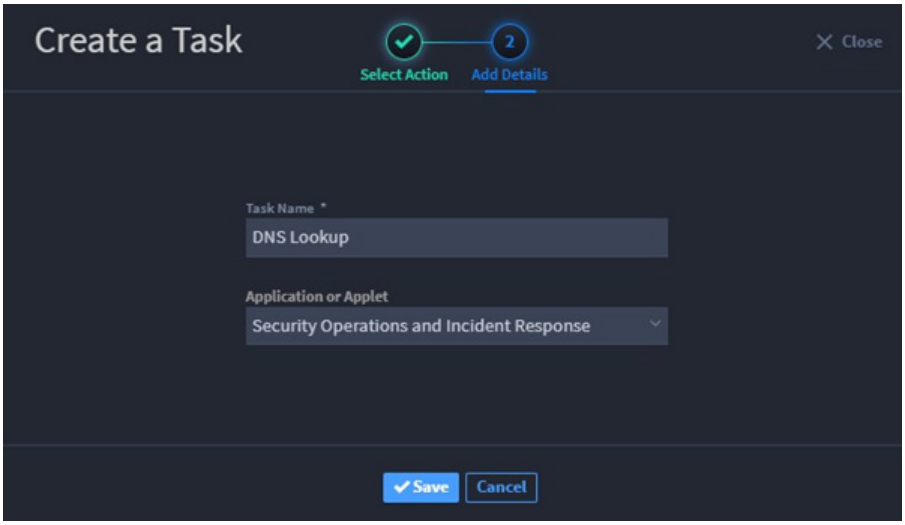

Figure 4. Name the task

6. On the **Integrations** > **General** tab, rename the task, provide a description, select or create an asset, set the appropriate ROI usage metrics, and enable or disable the task. You can also see the task parent and the task type for each task.

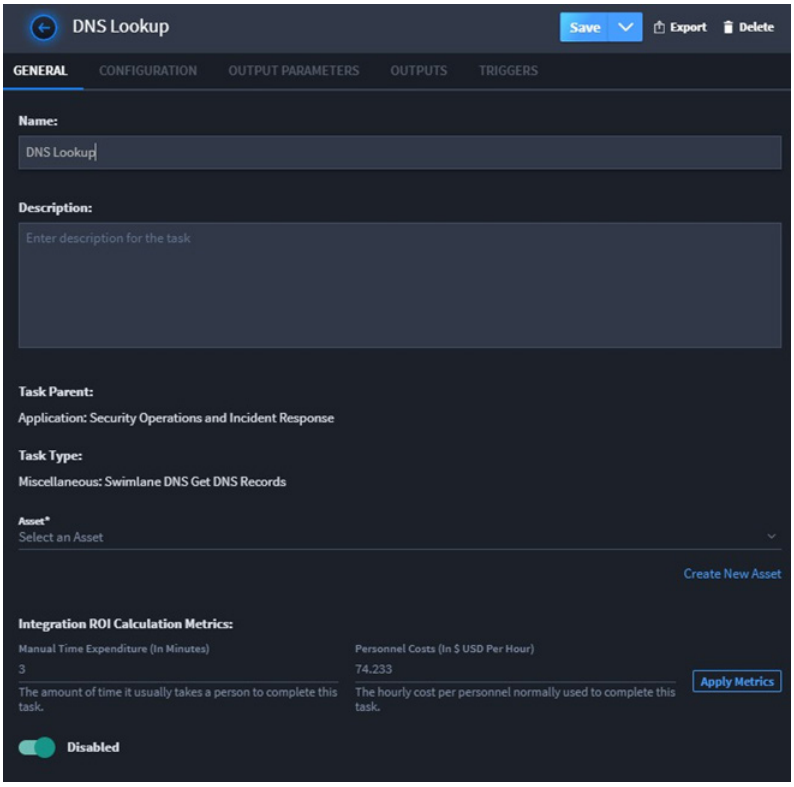

Figure 5. Configure task

By default, a task is enabled upon creation.

You can also set up Usage Metrics for this task. Usage Metrics track the time and cost you are saving by automating this task.

To set Usage Metrics, under Integration ROI Calculation Metrics, fill out the Manual Time Expenditure and Personnel Costs fields so that the value of the automation is calculated in Usage Metrics.

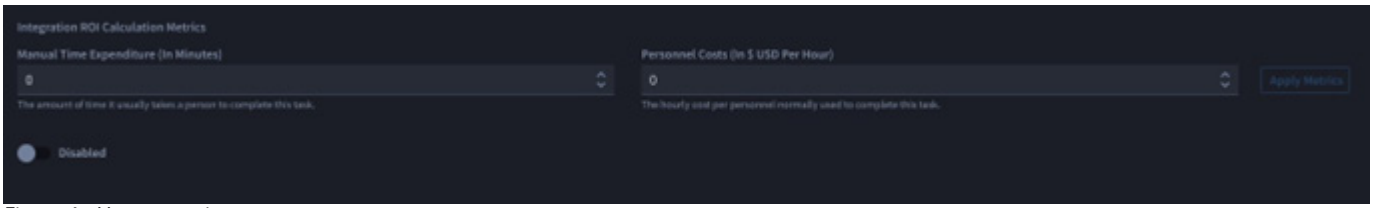

Figure 6. Usage metrics

Configure a Task

To configure a task, go to **Integration** > **Configuration**.

Depending on the type of task created, the configurable task details vary. Most tasks have a set of inputs that must be configured in a form, but others (e.g., Python or Powershell scripts) require a text editor.

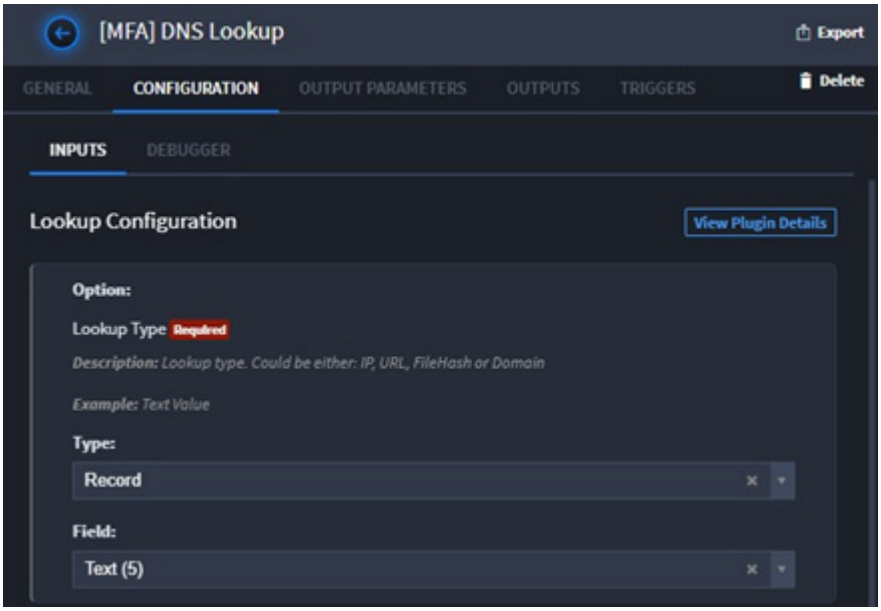

Figure 7. Configure a task

You can also reference the plugin details for the plugin that is associated with the task by clicking **View Plugin Details**.

In addition, you configure the outputs as well. Swimlane's automapping helps you step through the process of output mapping.

For detailed information about input and output configuration, refer to:

- Configure Task Input
- Configure Task Output

Set Triggers

Go the **Integrations** > **Triggers** tab to specify the conditions that will cause this task to run. You can trigger tasks by the following conditions:

- Scheduled: Task runs by a specified time frame.
- Email: Task runs when a specified email is received.
- Record Save: Task runs whenever a specified record is saved in the associated application.
- Integration: Task runs when an integration runs.

You can also schedule a custom trigger with a valid cron expression.

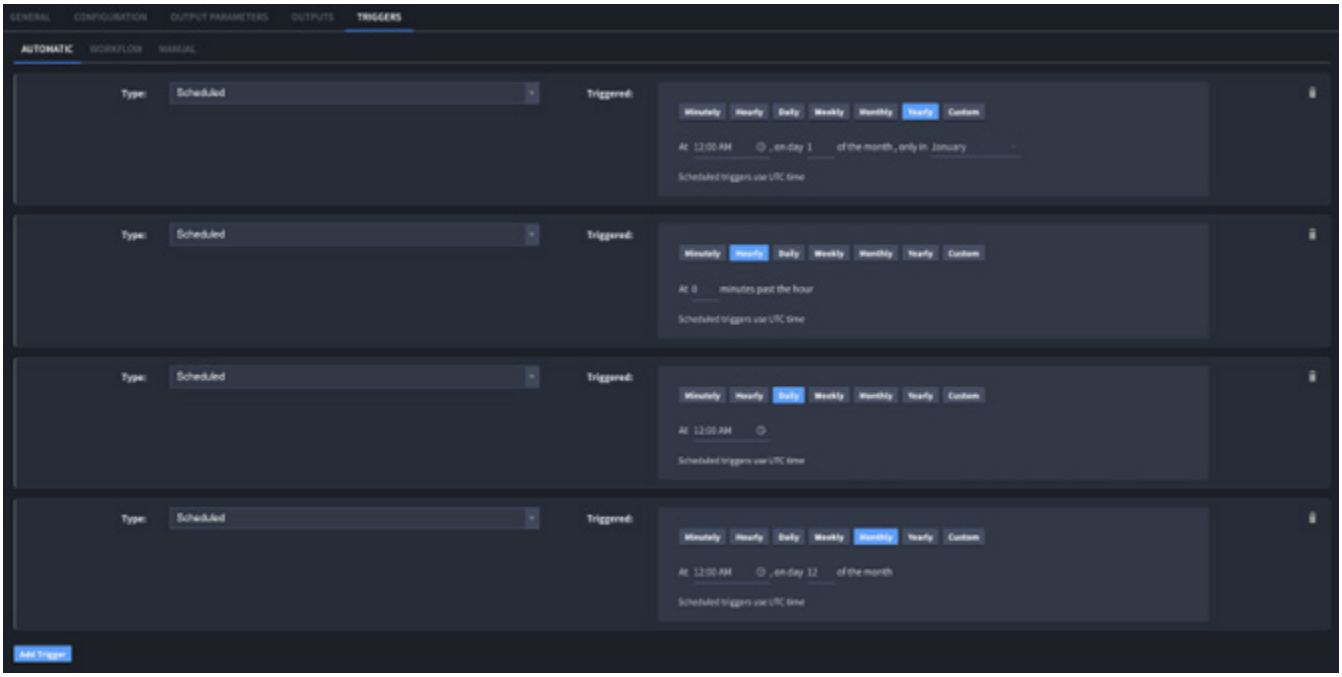

Figure 8. Triggers

Tasks can be referenced from workflow or from an integration button in Swimlane's Application Builder. The Workflow tab shows any workflow actions that are associated with the current task.

1. Click **Add/Edit Workflow** to associate a task with a new workflow action. The **Manual** tab displays any layout objects associated to the task in **Application Builder**.
2. Click **Open Application Builder** to edit the application.

Tasks that are triggered by an integration to update a specific value in a record are set to only affect the value once. This was designed so that integration record value changes do not run in a continual loop.

Set Scheduled Trigger

To set a scheduled trigger:

1. In your task, go to **Triggers** and select the trigger type **Scheduled**.
2. Select how often you would like the task triggered. You can specify minutes, hourly, daily, weekly, monthly, yearly, or custom.

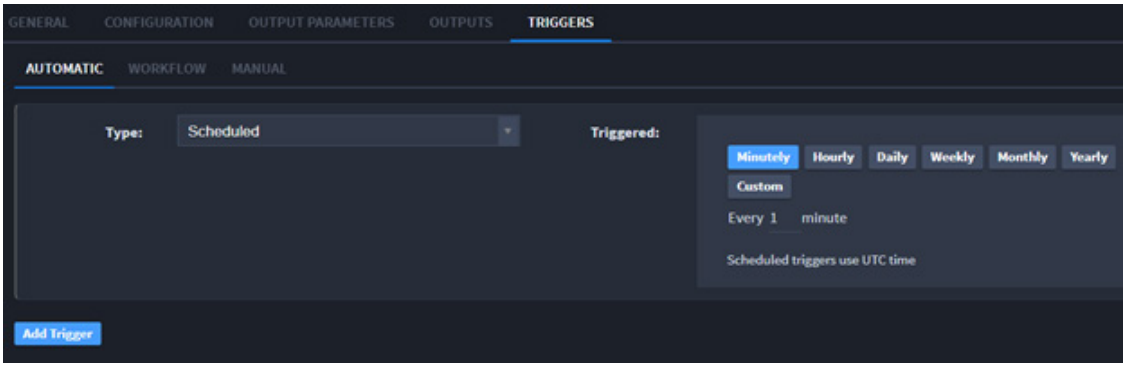

Figure 9. Triggers

3. Click **Save**.

Upload the Zscaler Plugin

To download the Zscaler plugin:

1. Go to Swimlane's website.
2. Click the blue download button and save the plugin.

To upload a new plugin:

1. From the global navigation panel in Swimlane, select **Integrations**.
2. From the **Integrations** taskbar, click the **Plugins** tab and then click the **Plus** menu icon .
3. On the **Upload Plugins** dialog, drag and drop the plugin files or click **Browse** to locate and select the plugin files.

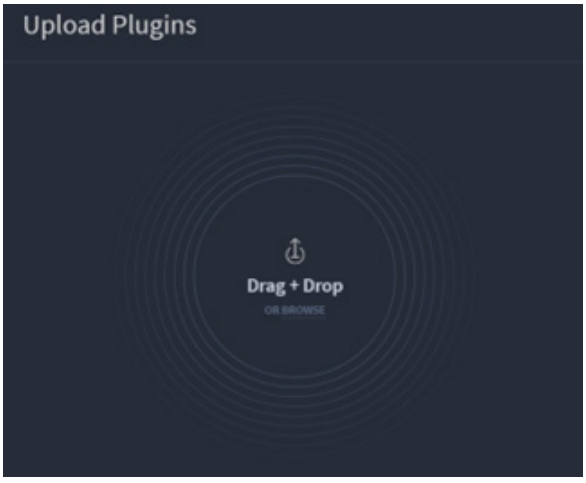

Figure 10. Upload Plugins

When you upload a plugin, you introduce the library or utilities for interacting with the third-party software into Swimlane. For most plugins, your next step is to create an asset with credentials from the plugin library.

Creating an Asset for Zscaler API Key

Assets are reusable, structured, and product-specific objects that contribute to the success of Swimlane tasks by handling secure authentication and configuration specifications for external systems.

To create a new asset:

1. Go to **Integrations** > **Assets** and click the **Plus** menu icon.

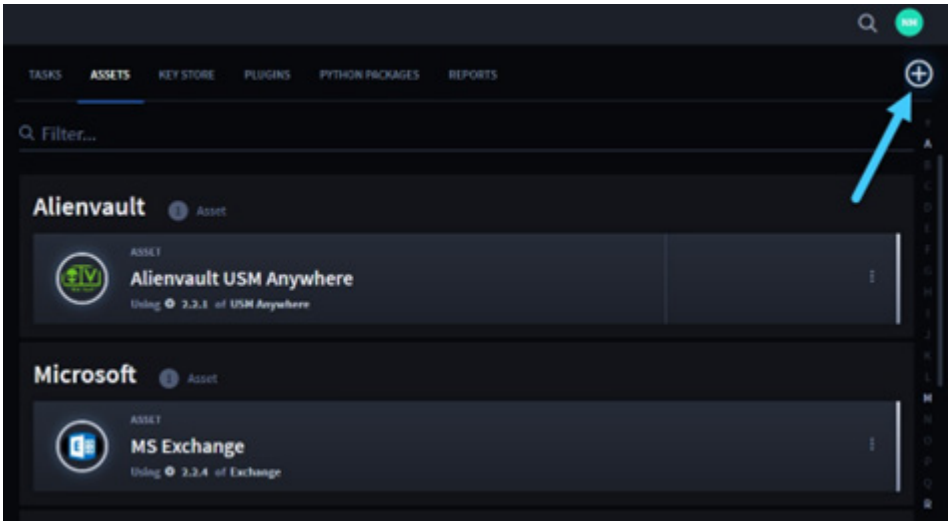

Figure 11. Create Asset

2. On **Select an Asset Type**, review the available asset types. When you find the plugin asset you need, click **Select**.
3. On **Configure Your Plugin Asset**, set the asset's parameters. You can also edit the existing **Asset Name** and **Asset Description**.

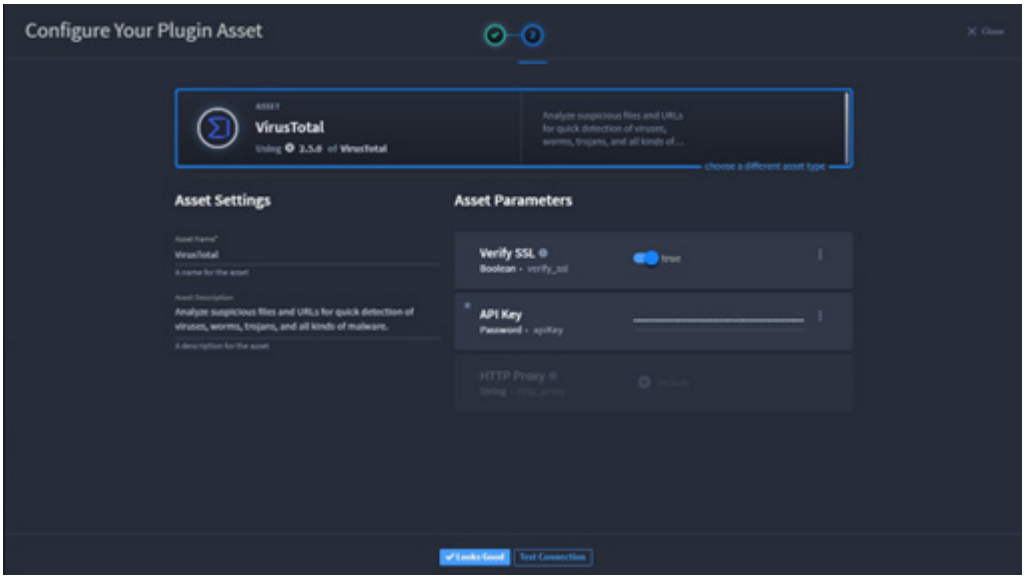

Figure 12. Configure Your Plugin Asset

4. If the parameters you set on the asset include any API key or other connective details, you can test the active connection of the asset within Swimlane. Click **Test Connection** and ensure you get the resulting `Asset Test Successful` message.
5. On **Configure Your Plugin Asset**, click **Looks Good**.

After an asset is configured, you can use it with any new or existing task.

Create Key Store Entry for Zscaler

Use the Key Store to encrypt sensitive information such as passwords, tokens, etc., and leverage the values in your actions.

1. From **Integrations**, select the **Key Store** tab.
2. To add a key, click **Add (+)**. New fields appear at the bottom of the list of keys.
3. Complete the **Key Name** and **Encrypted Value** fields, and then click the checkmark to save the key record.
4. Enter as many key and value pairs as needed.

The values are encrypted in Swimlane's database.

.

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**.

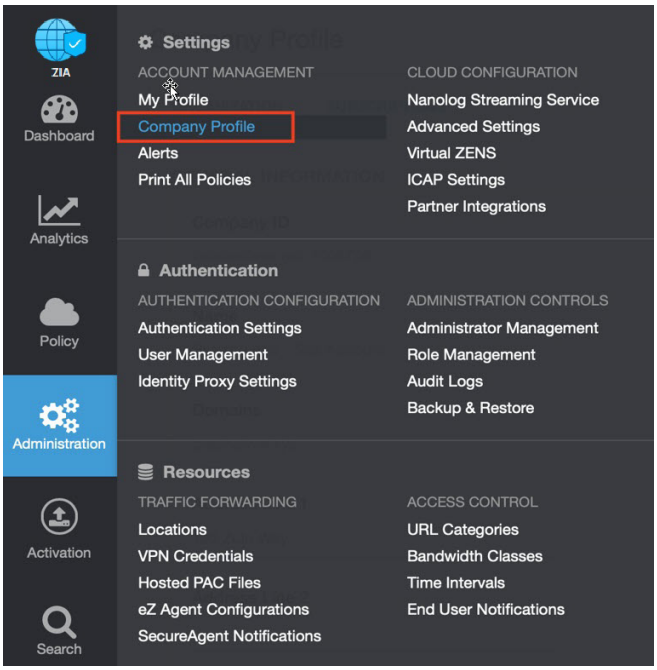

Figure 13. Collecting details to open support case with Zscaler TAC

2. Copy your Company ID.

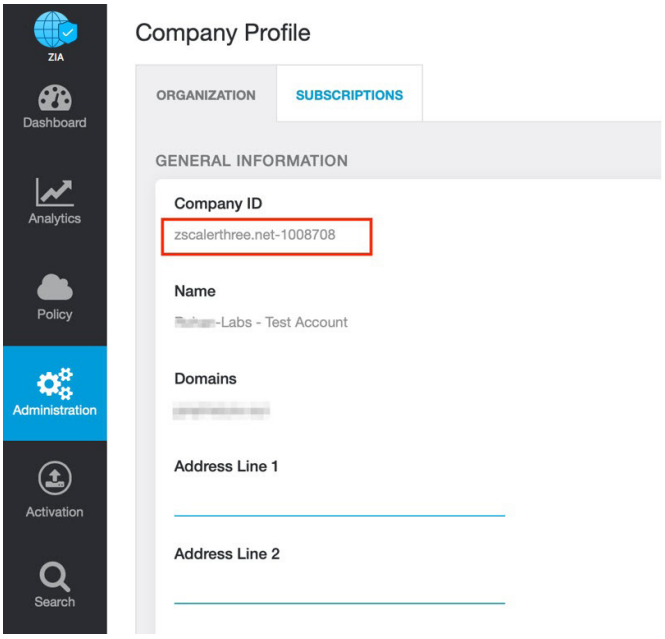

Figure 14. Company ID

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

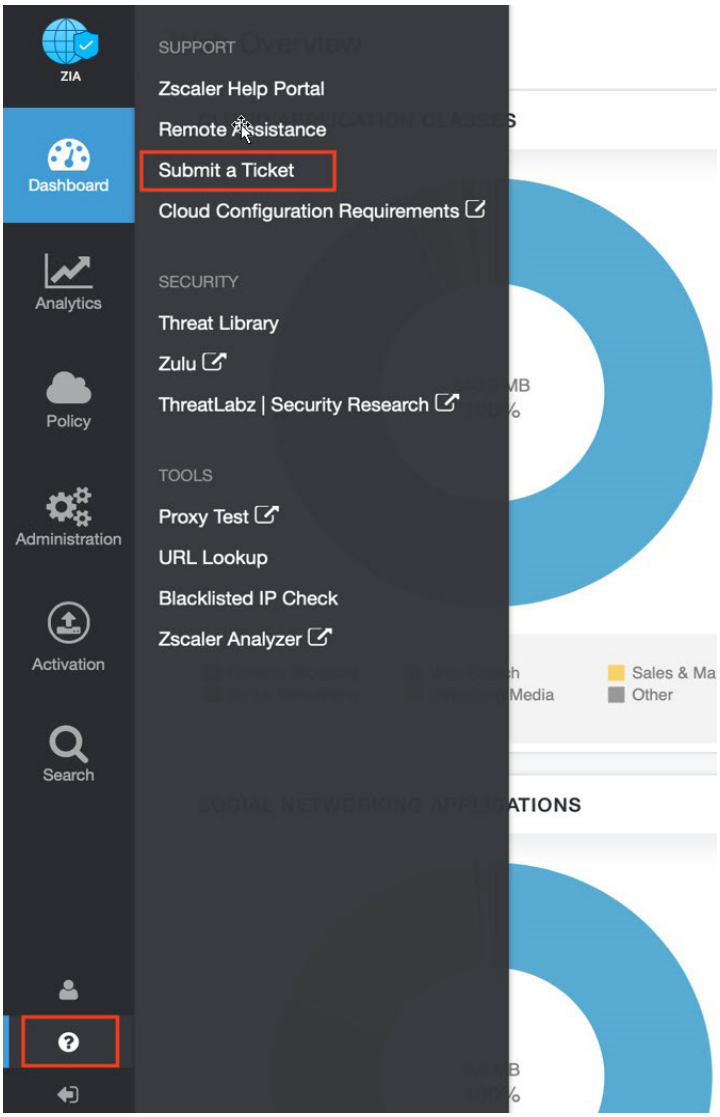

Figure 15. Submit a ticket

