



# ZSCALER AND TINES DEPLOYMENT GUIDE

# Contents

<b>Terms and Acronyms</b>	<b>4</b>
<b>About This Document</b>	<b>6</b>
Zscaler Overview	6
Tines Overview	6
Audience	6
Software Versions	6
Request for Comments	6
<b>Zscaler and Tines Introduction</b>	<b>7</b>
ZIA Overview	7
ZPA Overview	7
Zscaler Resources	7
Tines SOAR Overview	8
Tines Resources	8
<b>Introduction</b>	<b>9</b>
<b>Authenticate ZIA for Use with Tines</b>	<b>11</b>
Get Zscaler API Key	11
Create Zscaler Credentials in Tines	11
Text Type	11
HTTP Request Type	11
Using the Credential in an Action	15
<b>Authenticate ZPA for Use with Tines</b>	<b>16</b>
Prerequisites	16
Obtain API Credentials from ZPA	16
Configure Tines for ZPA Integration	18

Troubleshooting	22
Appendix A: Requesting Zscaler Support	23

## 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
SOAR	Security Orchestration, Automation, and Response
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

© 2024 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at [zscaler.com/legal/trademarks](https://zscaler.com/legal/trademarks) are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

## 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](#).

### Tines Overview

Tines is revolutionizing security automation by empowering organizations to streamline their security operations with powerful, no-code workflows. Designed for modern security teams, Tines allows users to automate repetitive, manual processes, drastically reducing response times and minimizing human error. The platform enables security teams to create and execute dynamic workflows without writing a single line of code, making it accessible to both technical and non-technical users.

With a focus on flexibility and customization, Tines integrates seamlessly with a wide range of tools and services, allowing for efficient data collection, threat detection, and response automation across diverse environments. Trusted by leading organizations globally in commercial and government space, Tines improves incident response, enhances security operations, and drives greater operational efficiency. Operating in the cloud and supporting hybrid environments, Tines offers scalability and the simplicity traditional solutions cannot match.

To learn more, see the [Tines 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](#)
- [Tines 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](mailto:partner-doc-support@zscaler.com) to offer feedback or corrections for this guide.
- **For Zscaler employees:** Contact [z-bd-sa@zscaler.com](mailto:z-bd-sa@zscaler.com) to reach the team that validated and authored the integrations in this document.

# Zscaler and Tines Introduction

Overviews of the Zscaler and Tines 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
<a href="#">ZIA Help Portal</a>	Help articles for ZIA.
<a href="#">ZPA Help Portal</a>	Help articles for ZPA.
<a href="#">Zscaler Tools</a>	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
<a href="#">Zscaler Training and Certification</a>	Training designed to help you maximize Zscaler products.
<a href="#">Submit a Zscaler Support Ticket</a>	Zscaler Support portal for submitting requests and issues.

The following table contains links to Zscaler resources for government agencies.

Name	Definition
<a href="#">ZIA Help Portal</a>	Help articles for ZIA.
<a href="#">ZPA Help Portal</a>	Help articles for ZPA.
<a href="#">Zscaler Tools</a>	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
<a href="#">Zscaler Training and Certification</a>	Training designed to help you maximize Zscaler products.
<a href="#">Submit a Zscaler Support Ticket</a>	Zscaler Support portal for submitting requests and issues.

## Tines SOAR Overview

Tines is a workflow automation platform that helps teams build and automate processes:

- Features: Tines offers a variety of solutions including security, IT, infrastructure, engineering, product, and more.
- How it works: Tines allows users to build workflows using stories, actions, and events. It can perform an unlimited number of steps, including log and threat intelligence searches.
- Security: Tines is designed to be secure and flexible and you can deploy Tines on-premises or in the cloud.
- Scalability: Tines is designed to be scalable for enterprises.
- Integration: You can integrate Tines with any external system.

## Tines Resources

The following table contains links to Tines support resources.

Name	Definition
<a href="#">Tines Knowledge Base</a>	Tines Documentation portal.
<a href="#">Technical Guide</a>	Zscaler Tines Authentication Guide
<a href="#">Zscaler Playbooks</a>	Zscaler x Tines Prebuilt templates



# Introduction

This guide helps users to integrate Tines with Zscaler to enhance threat detection and response efficiency. The following are some of the prebuilt templates available to users



Figure 1. Prebuilt templates

Users have the option to use prebuilt workflows with Zscaler

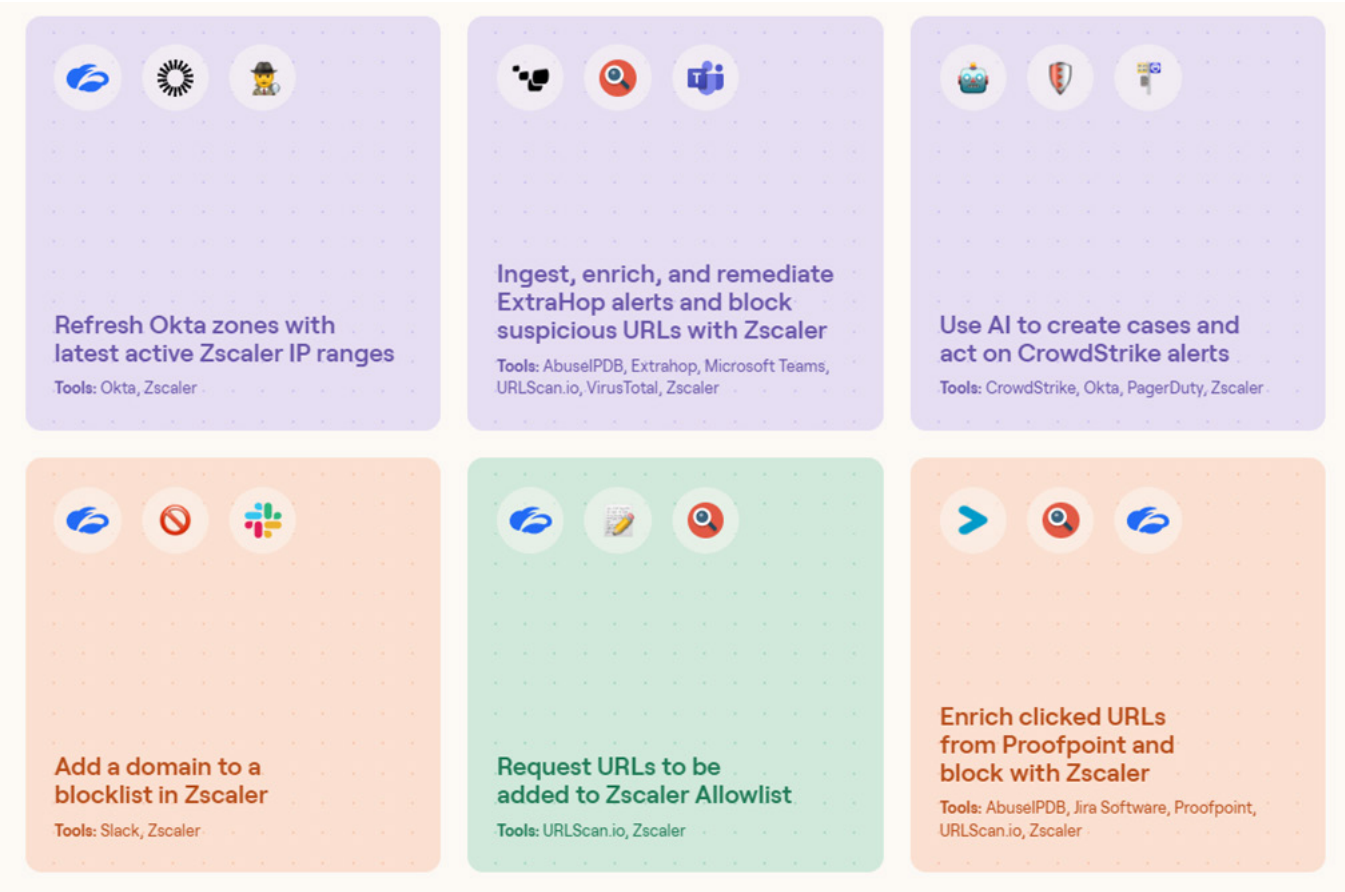


Figure 2. Prebuilt workflows

## Authenticate ZIA for Use with Tines

The following section details the steps required to authenticate Zscaler for use with Tines.

### Get Zscaler API Key

To get an API key from Zscaler:

1. Log in to your ZIA Admin Portal.
2. Go to **Administration** > **Cloud Service API Key Security** and copy the **API key**.
  - a. If one is not present, click **Add API Key** to create one. To learn more, see [Zscaler Cloud Service API Key](#) (government agencies, see [Zscaler Cloud Service API Key](#)).

### Create Zscaler Credentials in Tines

You need four credentials:

- Three text types:
  - Zscaler Username
  - Zscaler User Password
  - Zscaler API Key
- One HTTP request type: Zscaler

#### Text Type

To create a text type credential:

1. Log in to your Tines tenant.
2. Go to the team using the API, and click **Credential**.
3. Click **+ New Credential**, and select **Text**.
4. Input the values for the Zscaler credential:
  - a. **Name:** Enter a name (required).
  - b. **Description:** Enter a description (optional).
  - c. **Value:** Enter the API Key (required).
5. Optional:
  - a. **Domains:** Ensure this credential is only used when making HTTP requests to specific domains.
  - b. **Access:** What other teams can also use the API.
6. Click **Save**.

#### HTTP Request Type

To create an HTTP request type:

1. Click **+ New Credential** and select **HTTP Request**.
2. Input the values for the Zscaler credential:
  - a. **Name:** Enter a name (required).
  - b. **Description:** Enter a description (optional).

- c. **URL:** `https://zsapi.<Zscaler Cloud Name>/api/v1/authenticatedSession`  
 • <Zscaler Cloud Name> is the name provisioned for your organization by Zscaler (e.g., zsapi.zscalerbeta.net).

d. **Content Type:** Select **JSON**.

e. **Method:** Enter **Post**.

f. **Payload:** Copy the following object and paste into the Plain code section:

```
{
  "apiKey": "<<ZSCALER_OBFUSCATE_API_KEY(LOCAL.credential, LOCAL.timestamp)>>",
  "username": "<<CREDENTIAL.zscaler_username>>",
  "password": "<<CREDENTIAL.zscaler_user_password>>",
  "timestamp": "<<LOCAL.timestamp>>"
}
```

g. **Local values:** Click **+ Option**, select **Local values**, and paste the following into the Plain code section:

```
{
  "timestamp": "<<DATE('now', '%s%L')>>",
  "credential": "<<CREDENTIAL.zscaler_api_key>>"
}
```

h. Click **Run options** and make sure you get a successful response.

• Location of token from response: `SPLIT(zscaler.headers['set-cookie'], ';') |> FIRST(%)`

3. **(Optional) Domains:** Ensure this credential is only used when making HTTP requests to specific domains
4. **(Optional) Access:** What other teams can also use the API.
5. Click **Save**.

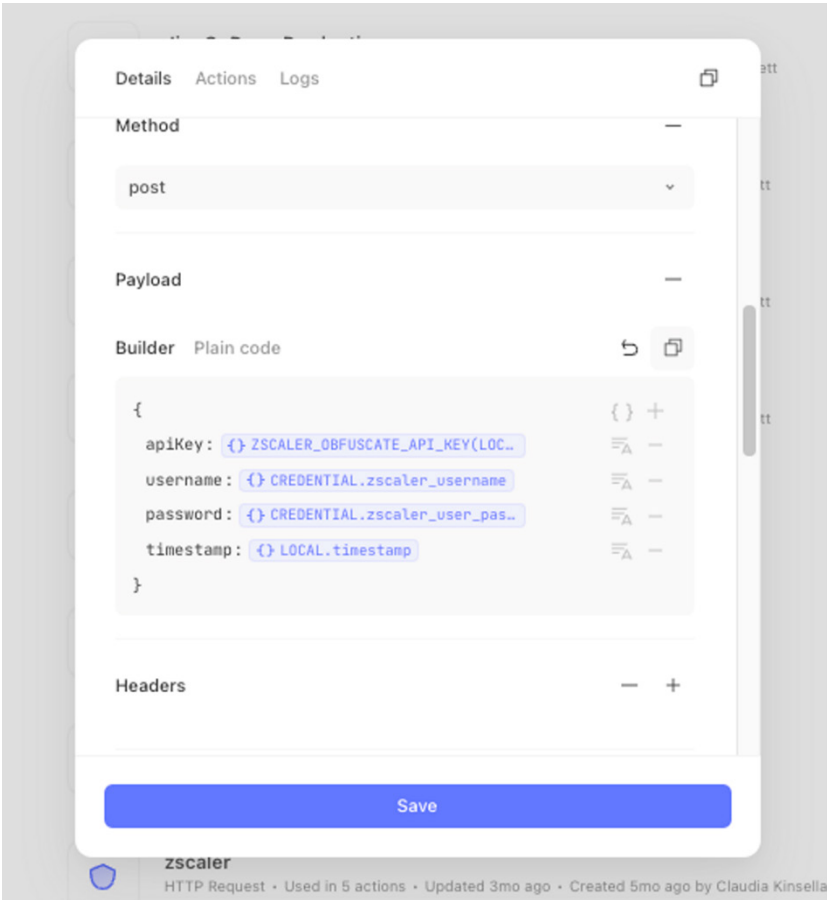


Figure 3. Credentials

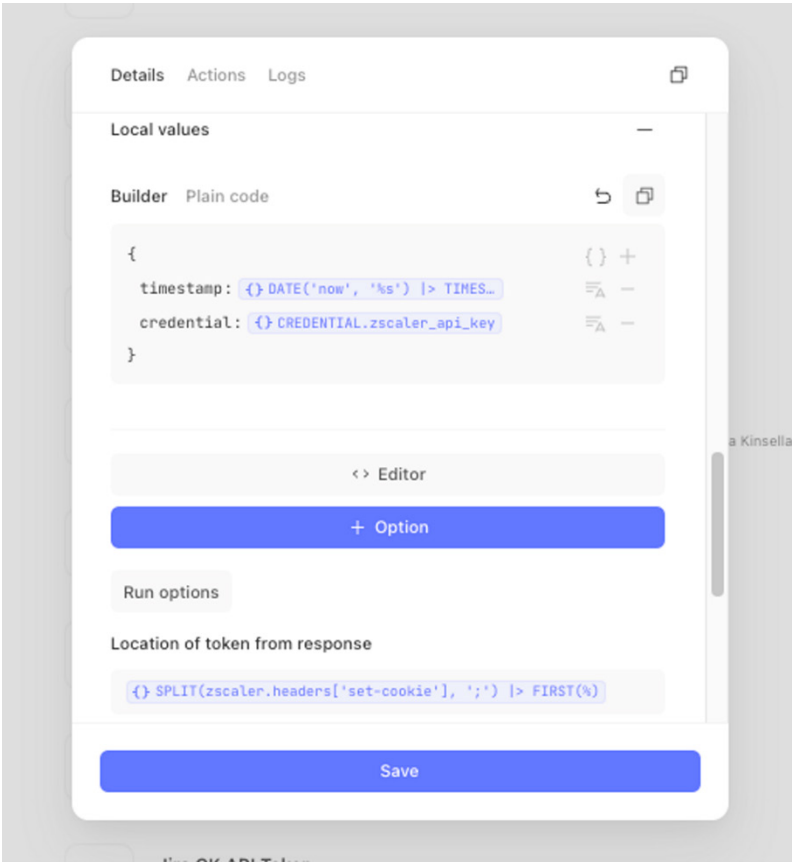


Figure 4. Credentials

To learn more about creating credentials in Tines, refer to the [Tines documentation](#).

To learn more about Tines and Zscaler stories, refer to the [Tines story library](#).

## Using the Credential in an Action

Make sure the Header configuration for your Zscaler credential is:

```
"cookie": "<<CREDENTIAL.zscaler>>"
```

The following is an example Zscaler action you can copy and paste onto your storyboard in Tines:

```
{
  "standardLibVersion": "32",
  "actionRuntimeVersion": "4",
  "agents": [
    {
      "disabled": false,
      "name": "Create Admin User",
      "description": "Creates an admin or auditor user",
      "options": {
        "url": "https://admin.zscaler.net/api/v1/adminUsers",
        "contentType": "application_json",
        "method": "post",
        "payload": {
          "loginName": "johnsmith@acme.com",
          "userName": "John Smith",
          "email": "johnsmith@acme.com",
          "role": {
            "id": 2322
          },
          "password": "AeQ9E5w8B$",
          "rank": 7,
          "name": "Read only",
          "policyAccess": "READ_ONLY",
          "dashboardAccess": "READ_WRITE",
          "reportAccess": "READ_WRITE",
          "analysisAccess": "READ_ONLY",
          "userNameAccess": "READ_ONLY",
          "adminAcctAccess": "NONE",
          "permissions": [
            "CUSTOM_URL_CAT",
            "ADVANCED_SETTINGS",
            "COMPLY",
            "FIREWALL_DNS",
            "SECURE",
            "SSL_POLICY",
            "VZEN_CONFIGURATION",
            "PARTNER_INTEGRATION",
            "LOCATIONS",
            "VPN_CREDENTIALS",
            "HOSTED_PAC_FILES",
            "EZ_AGENT_CONFIGURATIONS",
            "SECURE_AGENT_NOTIFICATIONS",
            "AUTHENTICATION_SETTINGS",
            "USER_MANAGEMENT",
            "IDENTITY_PROXY_SETTINGS",
            "APIKEY_MANAGEMENT",
            "OVERRIDE_EXISTING_CAT",
            "REMOTE_ASSISTANCE_MANAGEMENT"
          ],
          "logsLimit": "UNRESTRICTED",
          "roleType": "ORG_ADMIN"
        },
        "headers": {
          "cookie": "<<CREDENTIAL.zscaler>>"
        }
      },
      "position": {
        "x": 735,
        "y": 1215
      },
      "type": "httpRequest",
      "timeSavedUnit": "minutes",
      "timeSavedValue": 0,
      "monitorAllEvents": false,
      "monitorFailures": false,
      "monitorNoEventsEmitted": null,
      "recordType": null,
      "recordWriters": [],
      "form": null,
      "cardIconName": "httpRequest",
      "createdFromTemplateGuid": "8eed5d2f44abb9a27905037f99400921a997b97b4d2639374ca915aa3ebc4560",
      "createdFromTemplateVersion": null,
      "originStoryIdentifier": "cloud:aa47f8215c6f30a0dcdb2a36a9f4168e:d4c15df0f02ba4789095426607003199"
    }
  ],
  "links": [],
  "diagramNotes": []
}
```

## Authenticate ZPA for Use with Tines

The following sections describe how to authenticate ZPA for use with Tines.

### Prerequisites

Make sure the following prerequisites are met:

- Tines Account: Ensure you have administrative access to your Tines account.
- Zscaler ZPA Account: Ensure you have administrative access to your Zscaler ZPA account.
- API Access: Obtain necessary API credentials for both Tines and Zscaler ZPA.
- Network Access: Ensure that the network where Tines operates can reach Zscaler ZPA endpoints.

### Obtain API Credentials from ZPA

To obtain API credentials from ZPA:

1. Log in to your Zscaler Admin Portal.

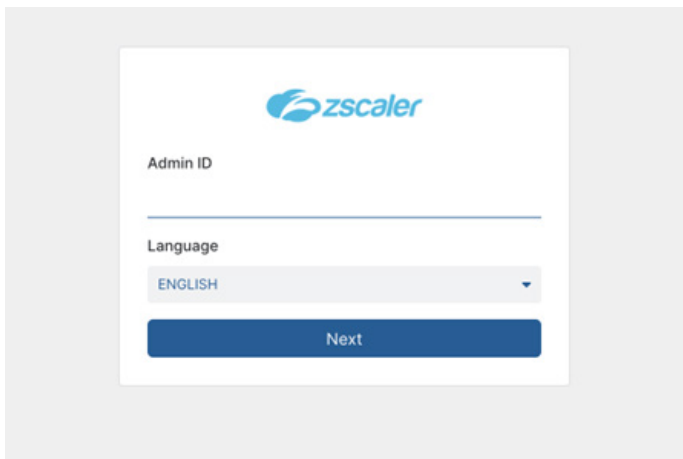


Figure 5. ZPA Admin Portal

2. Go to **Administration > Public API > API Keys**.

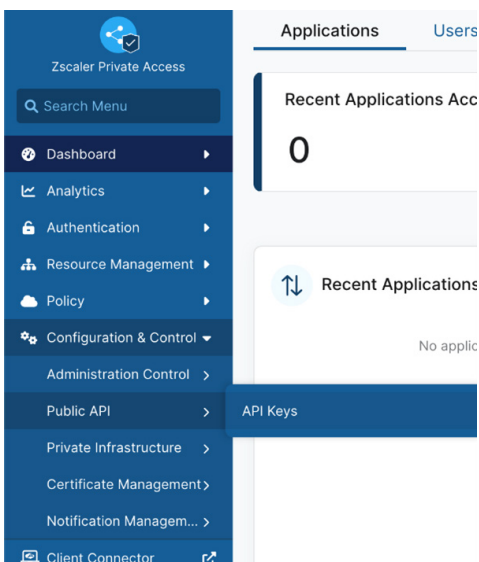


Figure 6. API Keys



3. Click **Add API Key**.

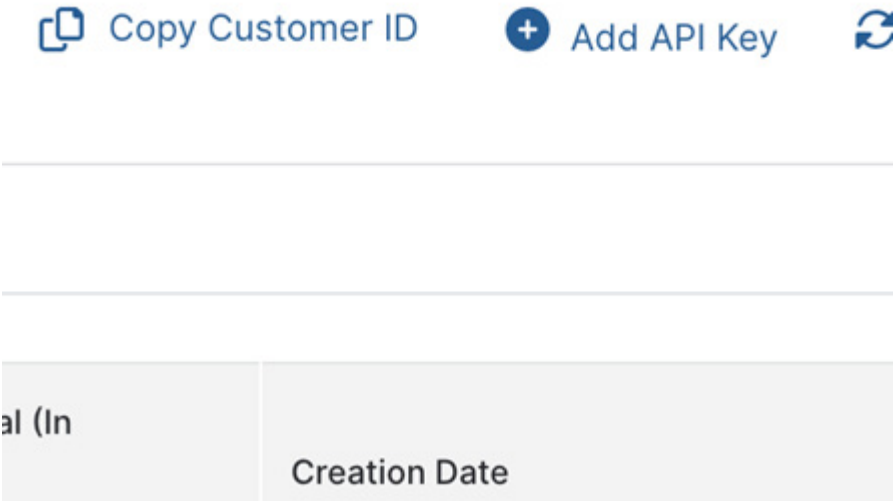


Figure 7. Add API Key

4. Enter a **Name** (e.g., Tines Integration).
5. Enter a **Session Validity Interval**.

A screenshot of a 'Add API Key' configuration dialog. It has a title bar with 'Add API Key' and a close button. The form contains three fields: 'Name' with the value 'tines-1', 'Status' with radio buttons for 'Enabled' (selected) and 'Disabled', and 'Session Validity Interval (In Seconds)' with the value '3600'. At the bottom are 'Save' and 'Cancel' buttons.

Figure 8. Configure API Key

6. Copy the **Secret Key** and save it. You use this to authenticate with the Tines platform.

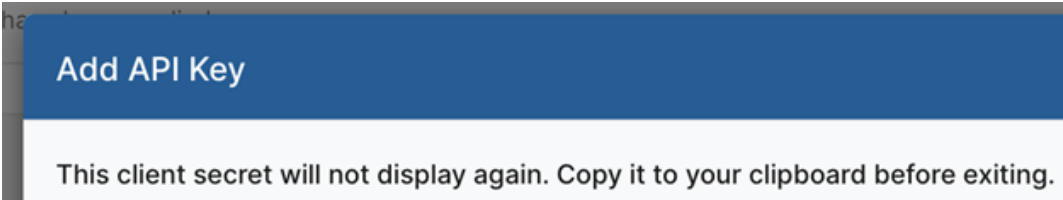


Figure 9. Secret Key

7. Copy the **Customer ID** and save it. You use this to build your authentication method in Tines.

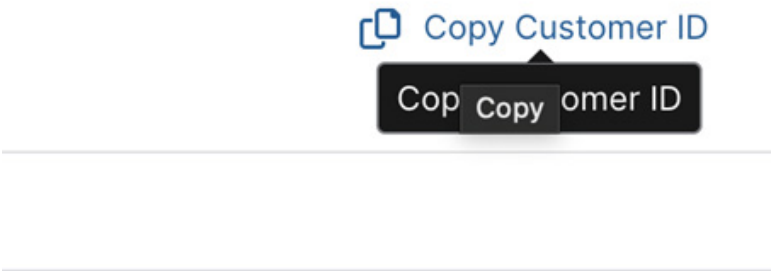


Figure 10. Customer ID

## Configure Tines for ZPA Integration

To configure Tines for ZPA integration:

1. Access your Tines account using your credentials.

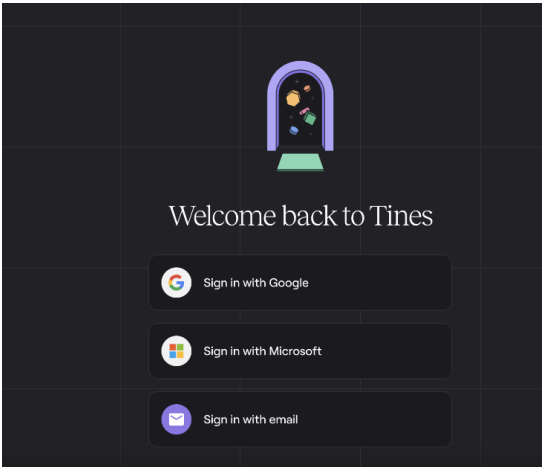


Figure 11. Tines log in

2. From the **Your drafts** drop-down menu, click **Credentials** to access the **Tines Credentials store**:

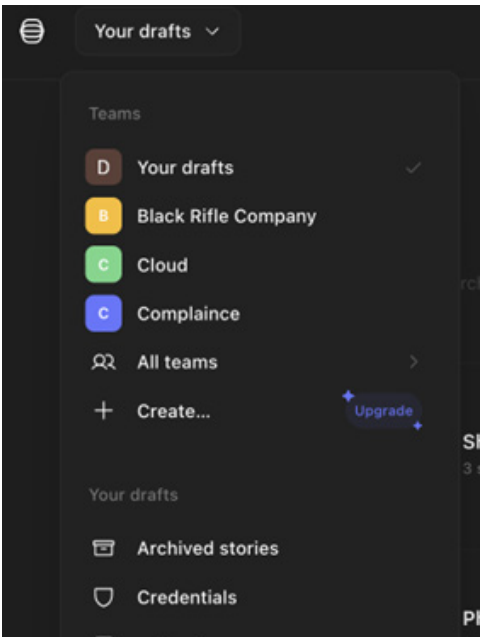


Figure 12. Tines store

3. Click **Configure HTTP Request**.

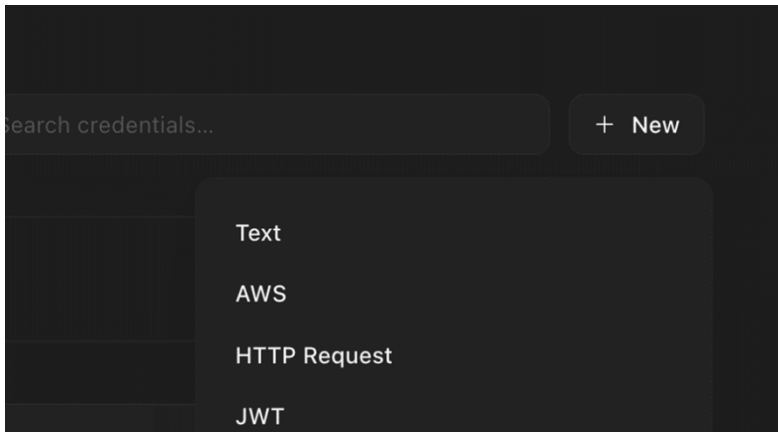


Figure 13. Configure HTTP Request

4. To configure the Authentication:
  - a. Enter a **Name** (e.g., `zscaler_zpa`).
  - b. Enter a **Description** for the credential.
  - c. Enter the **URL** (e.g., `https://config.zpabeta.net/signin`).
  - d. Scroll down to **Content Type** and continue.

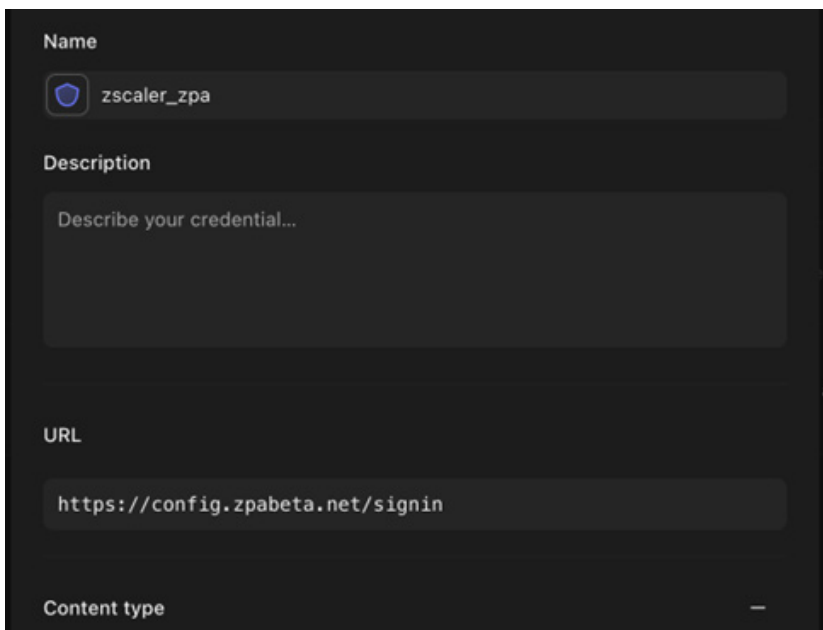


Figure 14. Authentication

5. In the **Content type** section:
  - a. Select the **Form** from the drop-down options.
  - b. Select the **Method** from drop-down options.
  - c. Enter a **Payload** using the **Builder** (if applicable).

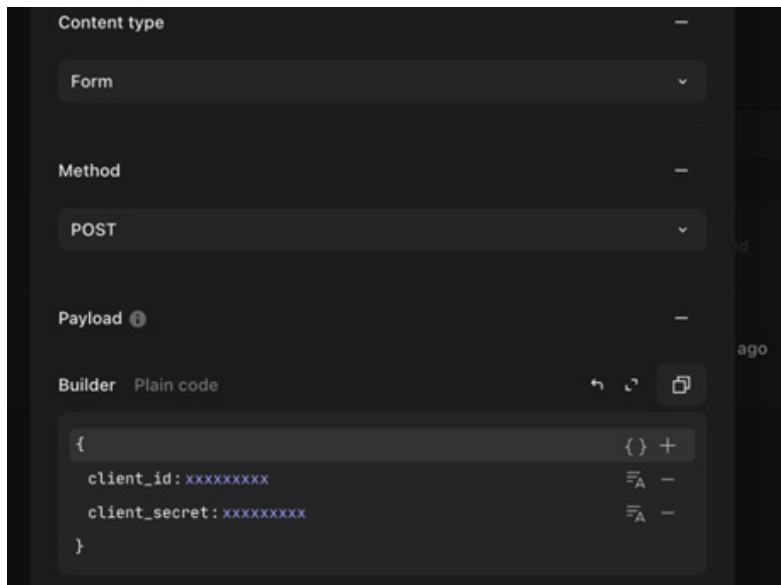


Figure 15. Request Body

6. Click **Save and run request**.

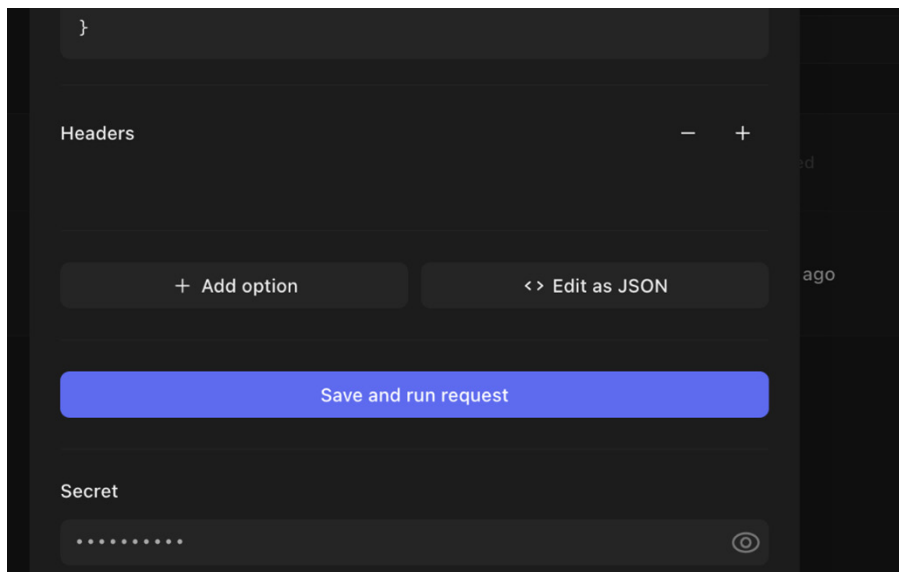
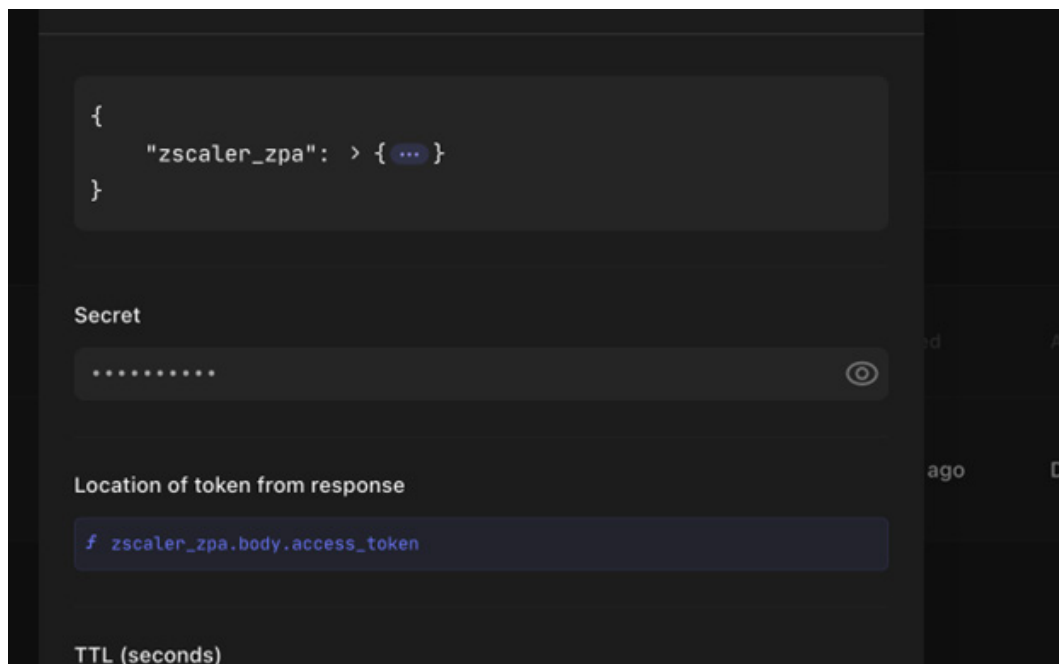


Figure 16. Save and run request

7. Add the path to pass the access token into a credential parameter.



The screenshot displays the configuration interface for a credential parameter in the Zscaler console. At the top, a JSON snippet is shown: 

```
{  "zscaler_zpa": > { ... }}
```

. Below this, the parameter is labeled "Secret" with a masked input field (dots) and an eye icon to toggle visibility. The "Location of token from response" field contains the path `f zscaler_zpa.body.access_token`. The "TTL (seconds)" field is visible at the bottom.

Figure 17. Credential parameter

## Troubleshooting

The following are troubleshooting tips:

- Authentication Issues: Ensure that the API key used in the Authorization header is correct and has the necessary permissions.
- Endpoint Error: Verify the Zscaler ZPA API endpoint URL and ensure it is correctly configured in the HTTP request.
- Permission Errors: Check the API key permissions in the ZPA Admin Portal and ensure that the key has access to the required resources.

# 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**.

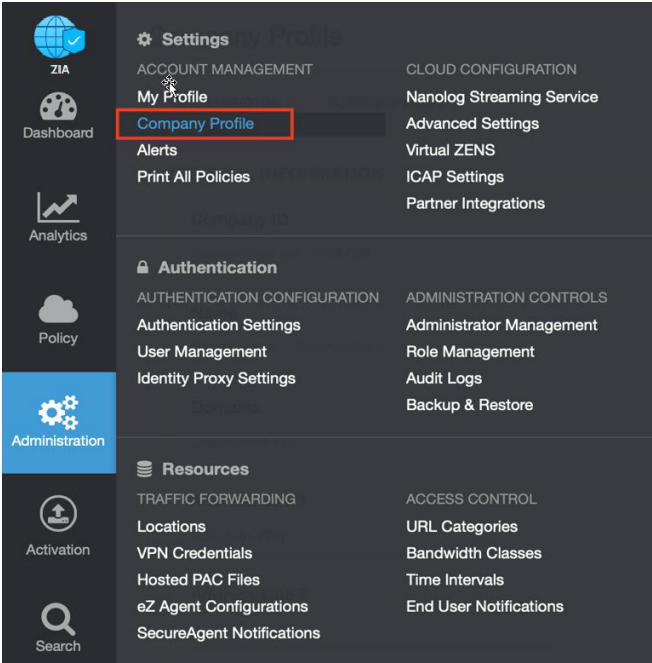


Figure 18. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.

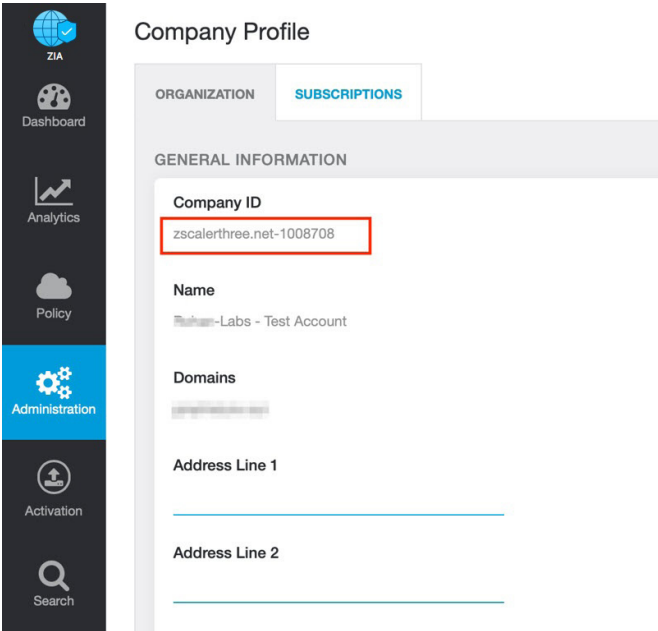


Figure 19. Company ID

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

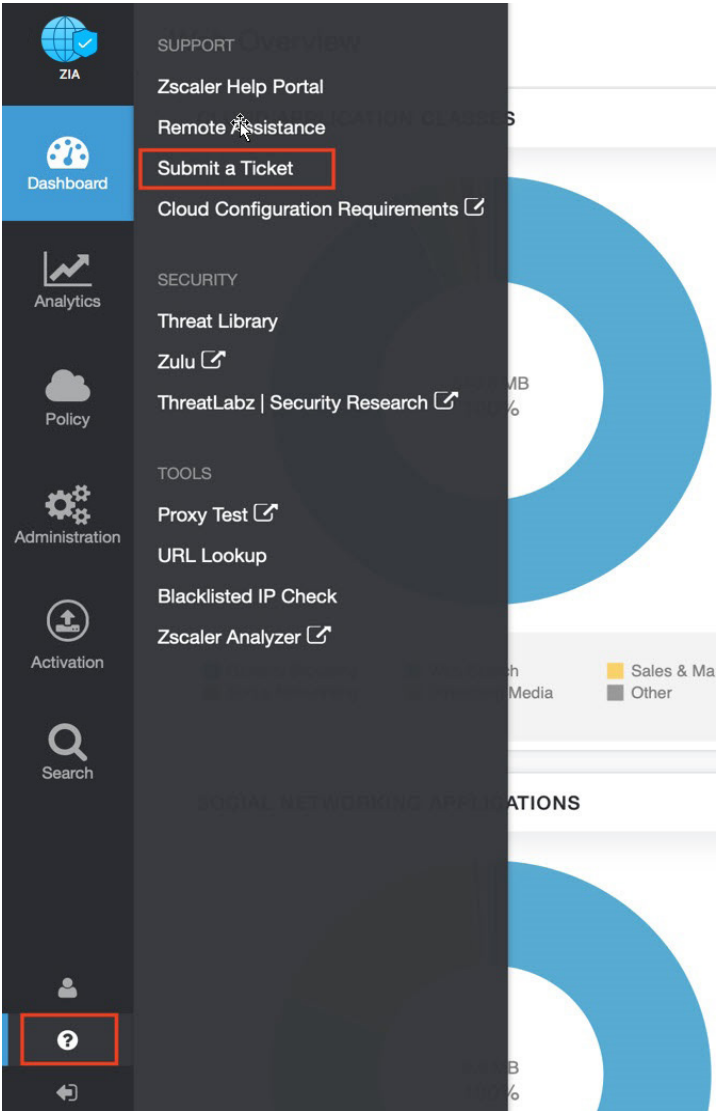


Figure 20. Submit a ticket