



Siemplify



SIEMPLIFY - ZSCALER DEPLOYMENT GUIDE

REV 1.0

Table of Contents

An Introduction to Siemplify.....	3
Prerequisites	3
ZIA Configuration	3
Enabling Zscaler API Access	3
Creating a Zscaler API Key.....	4
Creating an Administrative Role for Siemplify	6
Adding an Administrative Account for Siemplify	6
Committing the Changes.....	7
Configuration on Siemplify	8
Actions Overview	10
Support and Resources	11
Siemplify.....	11
Zscaler	11

An Introduction to Siemplify

The Siemplify Security Operations Platform is an intuitive, holistic workbench that makes security operations smarter, more efficient, and more effective. Siemplify combines security orchestration, automation and response (SOAR) with context-driven case management, investigation, and machine learning to make analysts more productive, security engineers more effective, and managers more informed about SOC performance.

Unlike other SOAR products that focus solely on automation or other limited use cases, Siemplify provides a complete SOC workbench that combines a single, intuitive experience that analysts love with a powerful context-driven engine that security engineers can easily customize for any use case. From its rich library of playbooks to built-in shift handover, crisis management, and reporting, only Siemplify delivers everything security operations teams need for cutting-edge incident response.

Prerequisites

- Zscaler account enabled with API access
- Administrator access to Zscaler to create user and API keys
-

ZIA Configuration

Configuration on the Zscaler side is needed to create a restricted account for API access. At a high level, the steps taken on Zscaler Internet Access (ZIA) interface will include:

- Enabling API access
- Creating an API key
- Creating a limited administrative role for Recorded Future
- Adding an administrator account for Recorded Future
- Committing all the changes

Enabling Zscaler API Access

Start by requesting API access to be added at the Zscaler support portal, <https://help.zscaler.com/submit-ticket>. Once access has been enabled, you will receive notification and can move to the next step. If you already have API access enabled, this step is unnecessary.

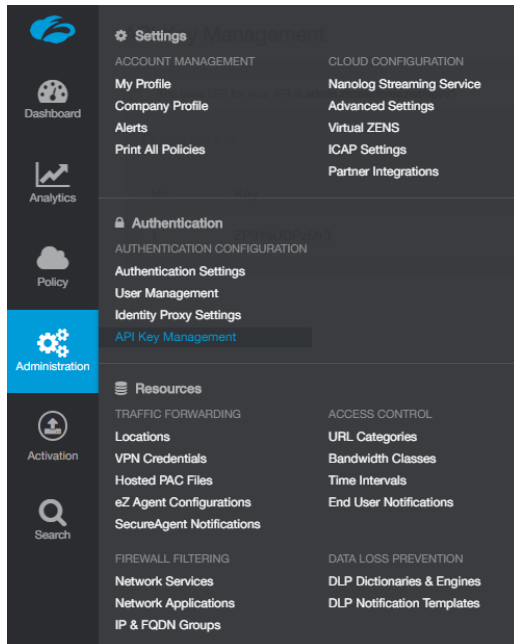
The screenshot shows the Zscaler Help Portal interface. On the left is a navigation menu with options: Documentation, Customer Service, Training & Certification, and Tools. The main content area is titled 'Submit Ticket' and includes a 'Submit Ticket' button in the top right. Below the title, there is a note for US Government Customers (FedRAMP) and a link to the ZscalerGov Help Portal. The form contains the following fields: Product (ZIA), Contact Email (abc@company.com), Issue Subject (with placeholder 'Enter issue subject'), CC List (with instruction 'Separate multiple email addresses with a comma'), and Description (with placeholder 'Write here...').

Creating a Zscaler API Key

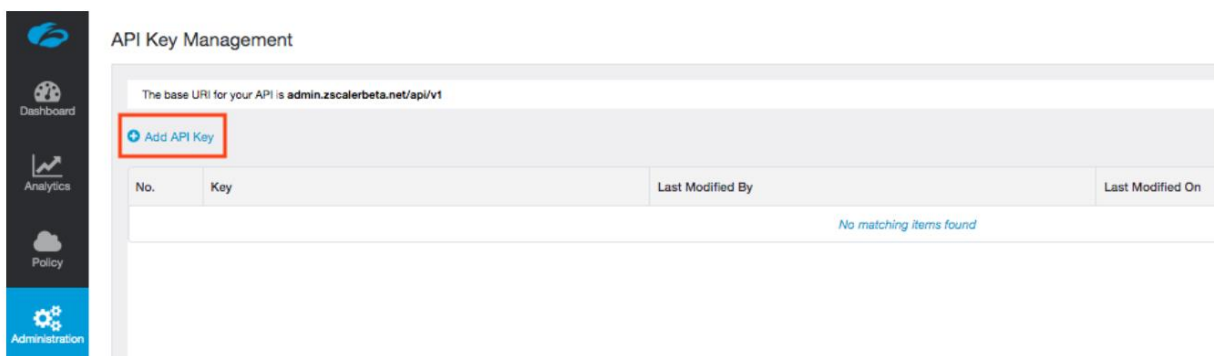
First, we will setup the Zscaler side of this service. Log into Zscaler using your administrator account. If you are unable to log in using your administrator account, contact support at <https://help.zscaler.com/submit-ticket>.

The screenshot shows the Zscaler login page. On the left is the Zscaler logo. On the right is a login form with the following elements: 'LOGIN ID' field with placeholder 'Type Your Login ID...', 'PASSWORD' field with placeholder 'Type Your Password...', a 'Remember my Login ID' checkbox, and a 'Sign In' button. Below the form, the language is set to 'English (US)'. The background of the page features a cityscape at night with glowing network lines.

To create an API key, navigate to: Administration > API Key Management



Next, press “Add API Key”



Once this is performed, the API Key is generated automatically and shown on the screen.

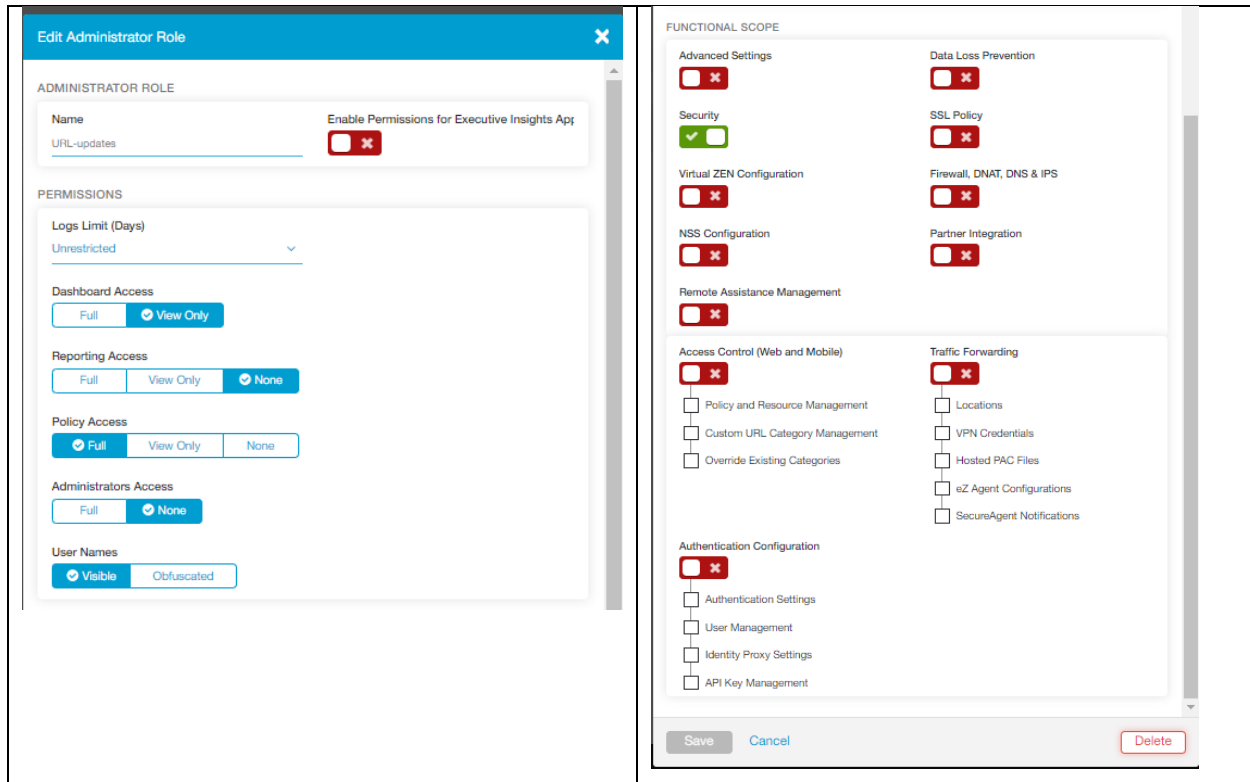
Take note of the base URI and the Key.

Additional details can be found at <https://help.zscaler.com/zia/about-api-key-management>.

Creating an Administrative Role for Siemplify

Start by creating a role that will limit permissions to updating the URL blacklists. Navigate to: **Administration -> Role Management -> Add Administrator.**

Create a new role, **URL-updates** is and set the permissions as shown below. Save the changes.



Adding an Administrative Account for Siemplify

Next, an administrative account needs to be assigned to the newly created role. Navigate to: **Administration -> Administrator Management -> Add Administrator.**

Set the **Login ID** and **Password** fields for this new account. Be sure to select **URL-updates** as the role for this account.

Add Administrator

ADMINISTRATOR

Login ID

Email

Name

Role
URL-updates

Scope
Organization

Executive Insights App Access

Comments

CHOOSE TO RECEIVE UPDATES

Security Updates

Service Updates

Product Updates

SET PASSWORD

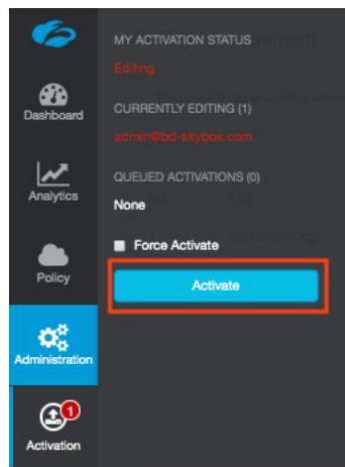
Password

Confirm Password

Save Cancel

Committing the Changes

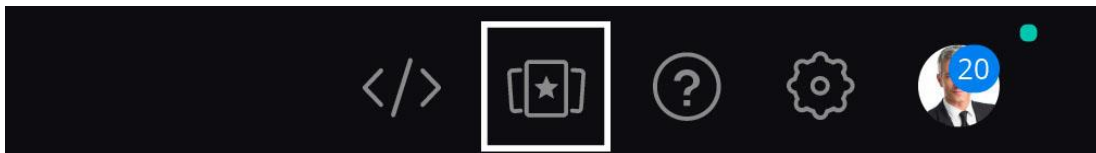
To activate all the changes, go to **Activation** and press the **Activate** button.



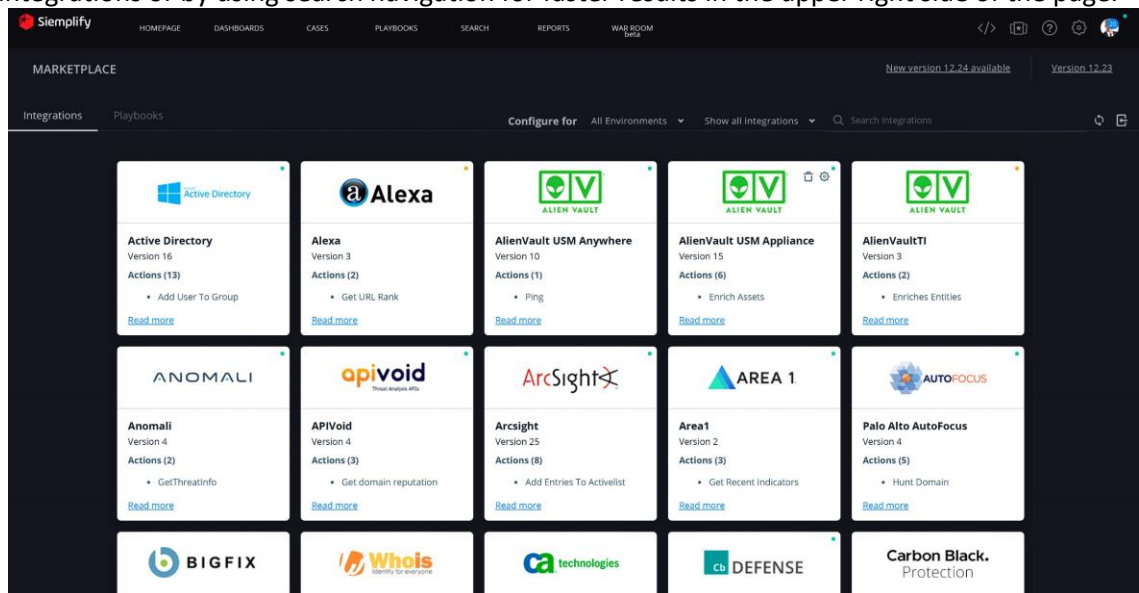
Configuration on Siemplify

To install and configure Zscaler integration on Siemplify, complete the following steps:

1. Navigate to the Siemplify Marketplace on the upper right corner of the screen.



2. Search for Zscaler integration in the Marketplace interface by either scrolling through the list of integrations or by using search navigation for faster results in the upper right side of the page.



3. Click on  button to install integration.



Zscaler


Version 1

Actions (10)

- Add To Blacklist
- Add To Whitelist
- Get Blacklist
- Get Sandbox Report
- Get Url Categories

[Read more](#)



4. The “orange circle” on the right corner of the integration shows that the integration is not configured. To do that, move the mouse cursor to the upper right corner on the integration window. The configuration menu will appear. Click on the  button to start configuring the integration.



Zscaler

Version 1

Actions (10)

- Add To Blacklist
- Add To Whitelist
- Get Blacklist
- Get Sandbox Report
- Get Url Categories

[Read more](#)

5. Input your required information and check the relevant field to Verify SSL in the Configuration screen. Click “Save”.

6. Once the integration has been successfully configured, the orange circle will change to a green one. Make sure to click Refresh for this to display.

Actions Overview

Listed below are the currently supported API based actions in Siemplify for Zscaler, as well as samples for their JSON results as they appear in the Siemplify platform.

1. Add to Blacklist
Adds an IP/Domain/URL to blacklist
2. Add to Whitelist
Adds an IP/Domain/URL to whitelist
3. Get Blacklist
Get the currently entities in blacklist
4. Get Sandbox Report
Get a full report for an MD5 hash of a file that was analyzed by the sandbox
5. Get URL Categories
Gets information about all URL categories.

6. Get Whitelist
Gets information about all URL categories.
7. Lookup Entity
Look up the categorization of a URL/Domain/IP
8. Remove from Blacklist
Removes a URL/Domain/IP from the blacklist.
9. Remove from Whitelist
Removes a URL/Domain/IP from the blacklist.

Support and Resources

Siemplify

The official user facing documentation can be found [here](#). This link contains in depth installation guides, how-to's, SDK documentation, architecture information and more. If further technical support is required, please email Siemplify at support@siemplify.co and we will be happy to help.

Zscaler

Zscaler: Getting Started

<https://help.zscaler.com/zia/getting-started>

Zscaler Knowledge Base:

<https://support.zscaler.com/hc/en-us/?filter=documentation>

Zscaler Tools:

<https://www.zscaler.com/tools>

Zscaler Training and Certification:

<https://www.zscaler.com/resources/training-certification-overview>

Zscaler Submit a Ticket:

<https://help.zscaler.com/submit-ticket>

ZIA Test Page

<http://ip.zscaler.com/>