



# ZSCALER AND CYWARE DEPLOYMENT GUIDE

# Contents

<b>Terms and Acronyms</b>	<b>3</b>
<b>About This Document</b>	<b>5</b>
Zscaler Overview	5
Cyware Overview	5
Audience	5
Software Versions	5
Request for Comments	5
<b>Zscaler and Cyware Introduction</b>	<b>6</b>
ZIA Overview	6
CTIX Overview	7
Cyware Resources	7
<b>Configuration Guide</b>	<b>8</b>
Configuring Zscaler as an Enrichment Tool	8
Defining Quota	10
Configuring Zscaler as an Internal Application	10
<b>Appendix A: Requesting Zscaler Support</b>	<b>12</b>

## 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)
CERT	Computer Emergency Response Team
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
IKE	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
ISAC	Information Sharing and Analysis Center
MSSP	Managed Security Service Provider
MAEC	Malware Attribute Enumeration and Characterization
PFS	Perfect Forward Secrecy
PSK	Pre-Share Key
SOAR	Security Orchestration, Automation, and Response
SSL	Secure Socket Layer (RFC6101)
STIX	Structured Thread Information eXpression
TIP	Threat Intelligence Platform
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](#).

### Cyware Overview

Cyware delivers an innovative approach to cybersecurity that unifies threat intelligence, automation, threat response, and vulnerability management with data insights gleaned from assets, users, malware, attackers, and vulnerabilities. Cyware's Cyber Fusion platform integrates SOAR and TIP technology, enabling collaboration across siloed security teams. Cyware is widely deployed by enterprises, government agencies, and MSSPs, and is the leading threat intelligence sharing platform for global ISACs and CERTs. To learn more, refer to [Cyware'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](#)
- [Cyware 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 Cyware Introduction

Overviews of the Zscaler and Cyware 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.

## 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="#">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="#">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.

## CTIX Overview

Cyware Threat Intelligence eXchange (CTIX) is an intelligent client-server exchange that leverages advanced technologies like Artificial Intelligence and Machine Learning to automatically ingest, analyze, correlate and act upon the threat data ingested from multiple external sources and internally deployed security tools. CTIX comes with the capability to systematically convert, store, and organize actionable threat data from various structured formats including STIX 1.x, STIX 2.0, XML, JSON, Cybox, OpenIOC, MAEC, and unstructured formats such as Email, RSS Feeds, Threat Blogs, etc., making it a truly format-agnostic Threat Intelligence Platform.

## Cyware Resources

The following table contains links to Cyware support resources.

Name	Definition
<a href="#">Cyware Support</a>	Online support for Cyware products.

# Configuration Guide

You can configure Zscaler 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 allowlisted and denylisted URLs to Zscaler. See [Configuring Zscaler as an Internal Application](#).

## Configuring Zscaler as an Enrichment Tool

Zscaler is available as an app in the CTIX application. Perform the following steps to configure the app in the CTIX application:

1. Go 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.

## Enrichment Management

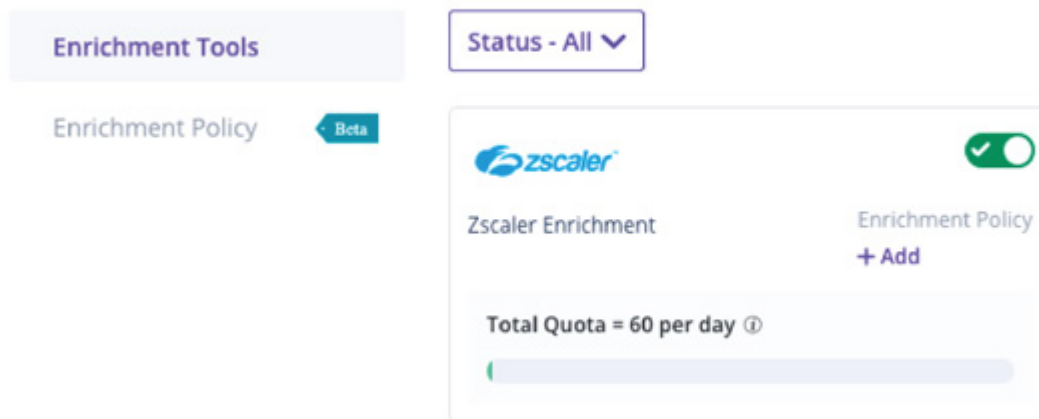
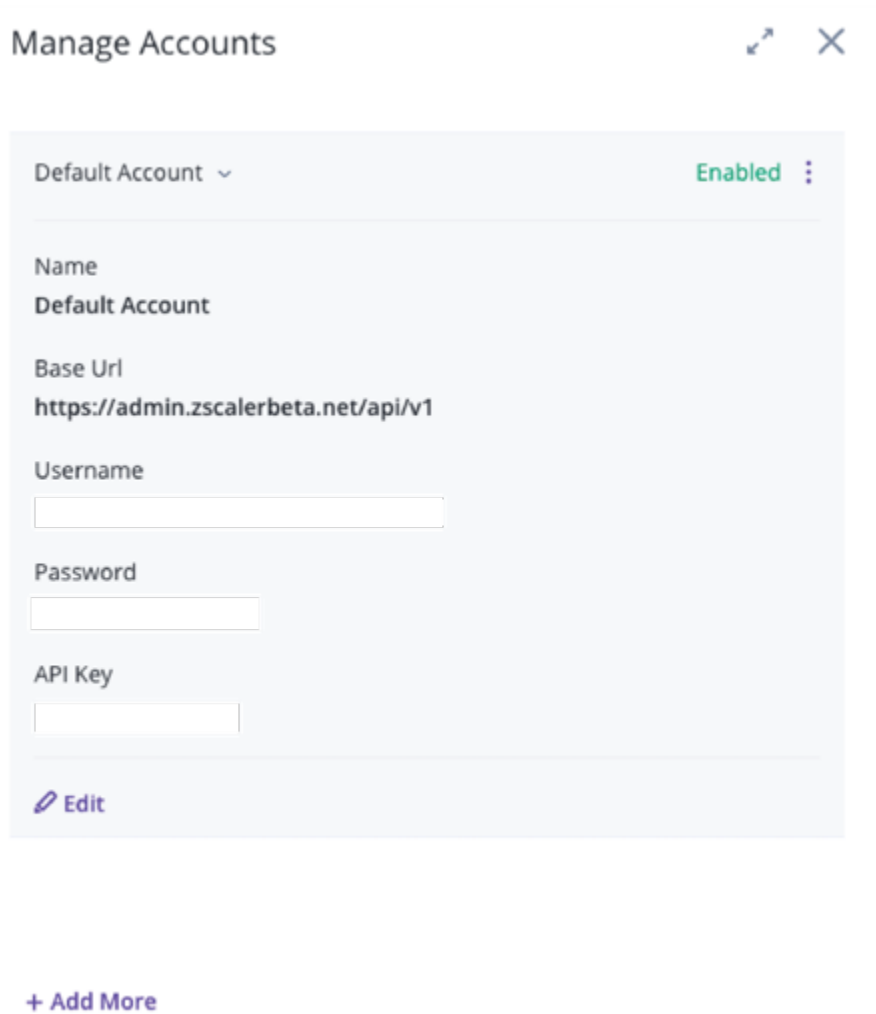


Figure 1. Enrichment Management



3. Select **Add New Account**.
4. Enter 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 is created successfully. You can also create multiple accounts to manage different connector actions as required.



The screenshot shows a 'Manage Accounts' window with a close button (X) and a share icon. It features a 'Default Account' dropdown menu, a status indicator 'Enabled' with a three-dot menu, and a form with the following fields: 'Name' (set to 'Default Account'), 'Base Url' (set to 'https://admin.zscalerbeta.net/api/v1'), 'Username' (empty), 'Password' (empty), and 'API Key' (empty). An 'Edit' button is at the bottom left, and a '+ Add More' button is at the bottom center.

Figure 2. Manage Accounts

6. The Zscaler connector in CTIX has the following actions to enrich URL, hash, or domain. Select and enable as needed.
  - Retrieve URL Detail
  - Update Allowlist URLs
  - Update Denylist 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 vertical ellipsis icon 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 doesn't 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 receive email notifications on quota limits.

## Configuring Zscaler as an Internal Application

1. Go to the **Integration Management** module.
2. Select **Internal Applications** and then select the **Network Security** tab.

### Integration Management

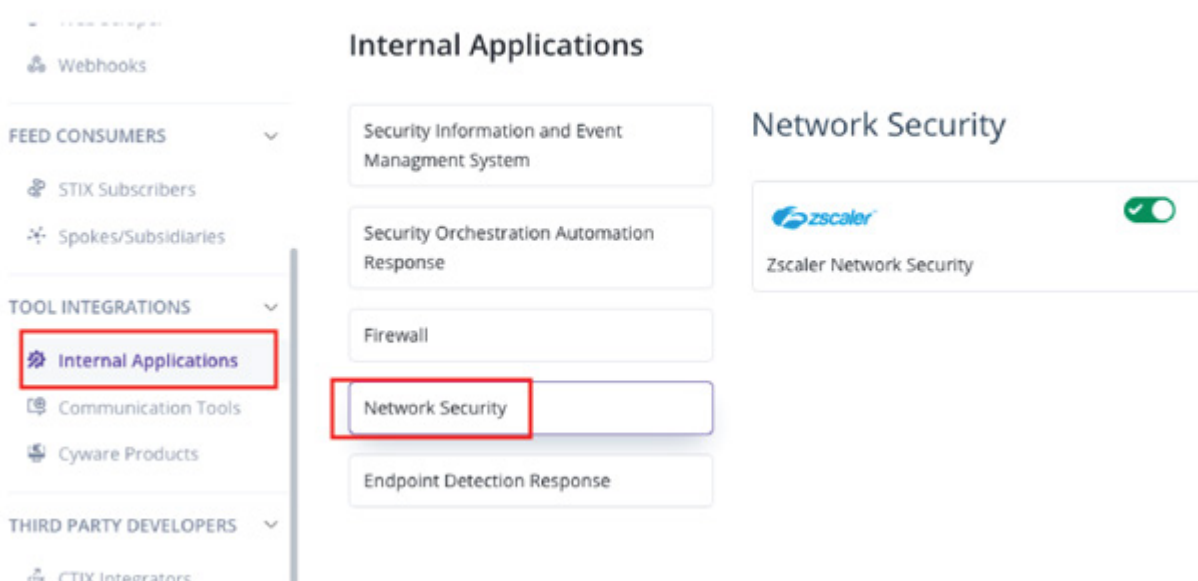


Figure 3. Integration Management

3. Select the **Zscaler** tile.
4. Configure the account on the top right-hand corner by clicking the vertical ellipsis icon and selecting the **Manage** option.

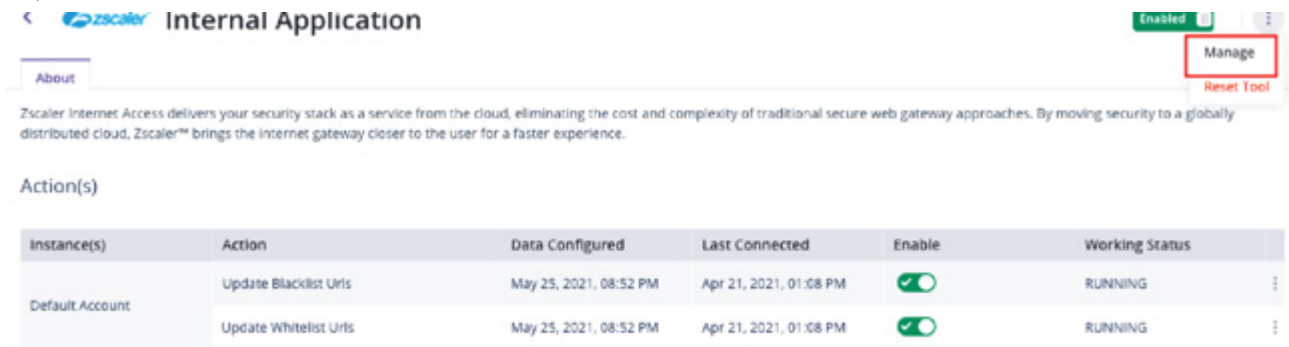




Figure 4. Internal Applications


5. Select **Add New Account**.
6. Enter 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 is created successfully. You can also create multiple accounts to manage different connector actions as required.

< Add Instance  


Instance Name\*  
new instance

Base Url\*  
https://admin.zscalerbeta.net/api/v1

Username\*  
charles sanders

Password\*  
\*\*\*\*\* 

API Key\*  
XX

☒ Verify SSL 

Save

Figure 5. Add Instance

8. Select **Manage Actions**.
9. Select an **Action**, enable it, and click **Save**.

## 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**.

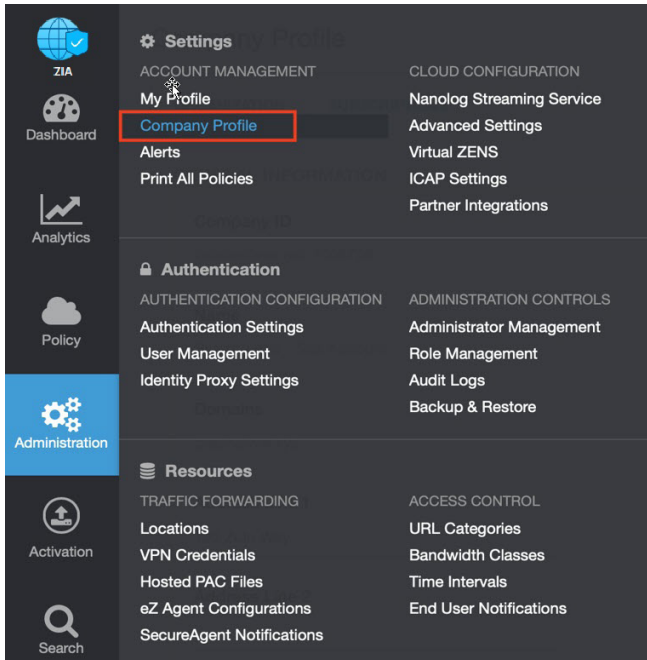


Figure 6. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.

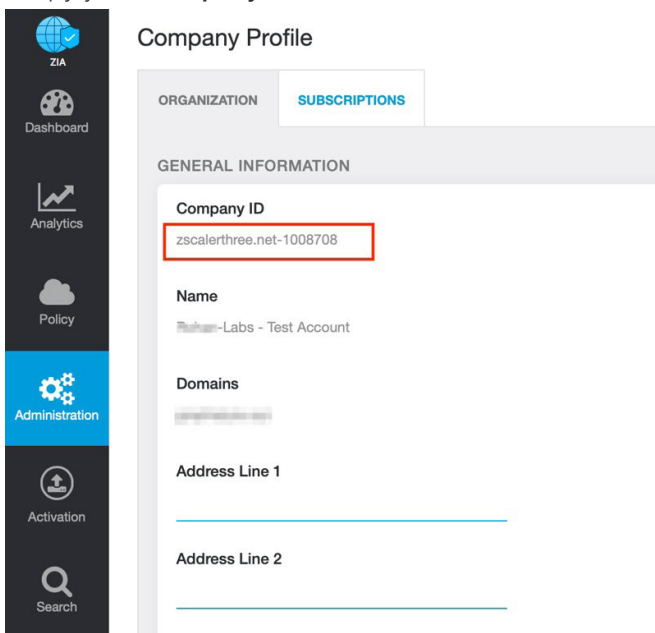


Figure 7. Company ID

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

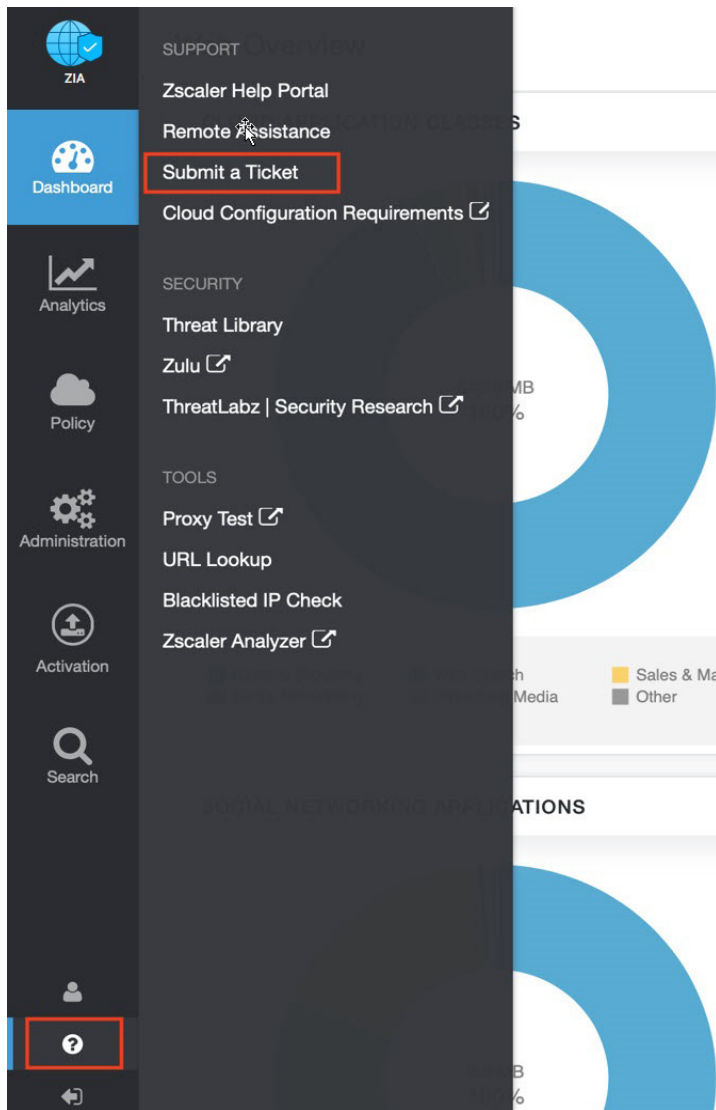


Figure 8. Submit a ticket