ZSCALER AND DARKTRACE DEPLOYMENT GUIDE

AUGUST 2021, VERSION 5.1

BUSINESS DEVELOPMENT GUIDE

Contents

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
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

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.

Darktrace Overview

Darktrace is a global leader in AI for cybersecurity that keeps organizations ahead of the changing threat landscape every day. Founded in 2013, Darktrace provides the essential cybersecurity platform, protecting organizations from unknown threats using its proprietary AI that learns from the unique patterns of life for each customer in real time. The Darktrace ActiveAI Security Platform delivers a proactive approach to cyber resilience with pre-emptive visibility into security posture, real-time threat detection, and autonomous response—securing the business across cloud, email, identities, operational technology, endpoints, and network. Breakthrough innovations from Darktrace's R&D teams in Cambridge, UK, and The Hague, Netherlands have resulted in over 200 patent applications filed. Darktrace's platform and services are supported by over 2,400 employees around the world who protect nearly 10,000 customers across all major industries globally. To learn more, refer to Darktrace'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
- Darktrace 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 Darktrace Introduction

Overviews of the Zscaler and Darktrace 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.
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.
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.

Darktrace ActiveAI Security Platform Overview

The Darktrace ActiveAI Security Platform is designed for your Security Operations Center to eliminate alert triage, perform investigations, and rapidly detect and respond to known and unknown threats, while exposing risk gaps across your technologies and processes so your team can shift to a proactive cyber approach. The solution is built on self-learning AI that continuously trains from your ever-changing business data wherever it is deployed, with further enrichment from external threat intelligence and third-party alerting

Darktrace Resources

The following table contains links to Darktrace support resources.

Name	Definition
Darktrace Customer Portal	Online support portal for Darktrace customers.
Darktrace Community	Online community for Darktrace users.

Darktrace and ZIA

The Darktrace and ZIA integration ingests weblogs from a ZIA device to simulate connection data. Web events produced by the Zscaler logging are associated with a device of the same hostname. If a device of that hostname does not already exist, Darktrace creates a new device. Connection events created from Zscaler logs are available to core Darktrace analysis and accessible in Advanced Search.

Devices that have ZIA simulated connectivity associated are automatically tagged with the ZIA tag.

Requirements

- A Darktrace appliance running v4.1 or later and optionally a Darktrace vSensor or hardware probe configured to receive logs.
- A Zscaler ZIA instance with Collect Device Owner Information and Collect Machine Hostname Information enabled.
- A configured Nanolog Streaming Service (NSS) setup with a local NSS server able to contact a Darktrace Master appliance or Probe (hardware or virtualized) over the required port (1514). A Zscaler NSS subscription is required.
- Access to the ZIA Admin Portal to configure NSS feeds.

Considerations

- Packet data is not available for connections constructed from Zscaler ZIA logs.
- Connections are only created for protocols included in the ZIA logs and are limited by the data provided within the log.

Due to the lack of source port information in ZIA logs, simulated connections are assigned to port 18000.

Deploying the ZIA Integration

The following sections describe how to deploy the Zscaler and and Darktrace integration.

Darktrace Configuration

To configure Darktrace:

1. Access the Darktrace master intended to receive the Zscaler logs. Within the **Threat Visualizer**, go to the **System Config** page in the main menu under **Admin**.
2. Select **Modules** from the left-side navigation.
3. Locate the **Telemetry** subsection, select **Zscaler ZIA** from the available options. Ensure the module is enabled in the dialog that opens.
4. Click **Details** to display the log output format. Record this securely, as it is required for configuration later.
5. Returning to the **Modules** page, locate the **Telemetry** subsection. Click **Config**. A new dialog opens.
6. Select the appliance or probe that logs to which logs are sent. In the **Log Input Allowed IPs** field, enter the IP address of the Zscaler device sending the logs.
7. **Save** the changes.

Zscaler Configuration

To configure ZIA:

1. Access the ZIA Admin Portal as a user with permission to configure NSS feeds.
2. Go to **Administration** > **Nanolog Stream Service** and select NSS feeds from the available table.
3. Click **Add NSS Feed**.
4. Enter a descriptive **Name** for the feed and ensure it is **Enabled**.
5. Select the **NSS Server** located locally to the master appliance or vSensor. Enter the IP of the master appliance or vSensor/hardware probe intended to receive the logs.
6. Set the **Destination Type** and enter the **TCP Port** as `1514`.
7. Ensure the **SIEM Rate** is **Unlimited** and set the **Log Type** to **Web Log**.
8. Set **Feed Output Type** to **Custom** and paste the output format retrieved from the **Darktrace Threat Visualizer** configuration page into the **Feed Output Format** field.
9. **Save** the changes.

ZIA logs are received by the master appliance or probe and begin to populate connection and hostname data within the Threat Visualizer.

Darktrace and ZPA

In ZPA environments, remote users initiate connections to internal resources through a ZPA App Connector located locally in an organization's private network. Darktrace observes connectivity from the ZPA App Connector to these internal resources but is unable to resolve these connections back to a specific end user or IP address.

The Zscaler ZPA and Darktrace integration ingests User Activity logs produced by ZPA, where connectivity patterns seen in network traffic are matched back to originating remote users. Devices that have connectivity mapped through ZPA ingestion are automatically tagged with the ZPA tag.

Requirements

- A Darktrace appliance running v4.1 or later and optionally a Darktrace vSensor or hardware probe configured to receive logs.
- A ZPA environment with a configured Log Streaming Service (LSS) setup, and an App Connector able to contact a Darktrace Master appliance or Probe (hardware or virtualized) over the required port.
- Darktrace master instances and probes accept UDP and TCP log input on port 1514 plain text and TLS-encrypted TCP on port 6514. The appropriate port and transfer protocol depends on the configuration of your Zscaler environment and the output supported by the vendor.
- Access to the ZPA Admin Portal to configure LSS feeds.

Considerations

Zscaler does not guarantee log data will be transmitted if connectivity is lost between ZPA and the local App Connectors. When connectivity is restored, up to 15 minutes of lost log data might be retransmitted, but this is also not guaranteed.

Deploying the ZPA Integration

The following sections describe deploying the Darktrace and ZPA integration.

Darktrace Configuration

To configure Darktrace:

1. Access the Darktrace master intended to receive the Zscaler logs. Within the **Threat Visualizer**, go to the **System Config** page in the main menu under **Admin**.
2. Select **Modules** from the left-side navigation.
3. Locate the **Telemetry** subsection, select **Zscaler ZPA** from the available options. A new dialog opens.
4. Ensure the module is **Enabled**.
5. Click **Details** to display the log output format. Record this securely as it is required for configuration later.
6. Return to the **Modules** page and locate the **Telemetry** subsection. Click **Config**. A new dialog opens.
7. Select the appliance or probe to which logs are sent. In the **Log Input Allowed IPs** field, enter the IP address of the Zscaler device sending the logs.
8. **Save** the changes.

ZPA Configuration

To configure ZPA:

1. Access the ZPA Admin Portal as a user with permission to configure LSS feeds.
2. Go to **Administration** > **Log Receivers** and select **Log Receivers** from the available table.
3. Click **Add Log Receiver**.
4. In the **Log Receiver** tab, provide a descriptive name and description for the log feed.
5. Enter the IP of the master appliance or vSensor/hardware probe intended to receive the logs.
6. Enter the **TCP Port** and select whether TLS encryption is desired. Darktrace master instances and probes accept UDP and TCP log input on port 1514 plain text and TLS encrypted TCP on port 6514. The appropriate port and transfer protocol depends on the configuration of your Zscaler environment and the output formats supported by the vendor.
7. Select the **Application Connector** group located locally to the master appliance or vSensor that can send logs.
8. Click **Next**. The **Log Stream** tab appears.
9. Set the **Log Type** to **User Activity**.
10. Set the **Log Template** to **JSON**, then paste the output format retrieved from the Darktrace Threat Visualizer config page into the **Log Stream Content** field.
11. Optionally, restrict the logs sent to **Darktrace** in the **Policy** section.
12. Click **Next**.
13. In the **Review** tab, confirm the settings and **Save** the new receiver.

ZPA logs are received by the master appliance or probe and begin to populate within the Threat Visualizer.

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**.

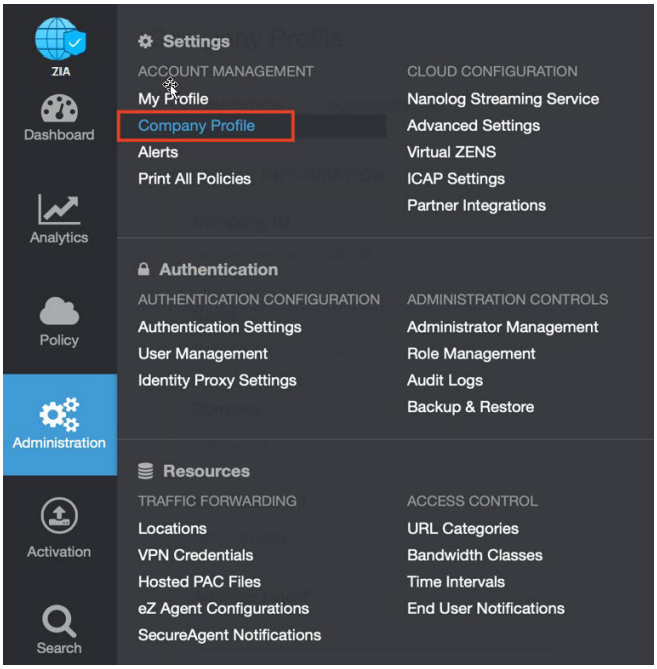

Figure 1. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.

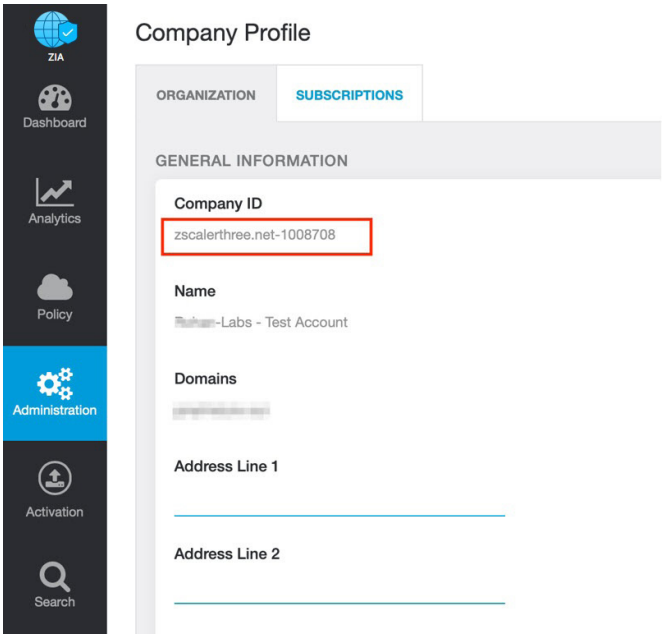

Figure 2. Company ID

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

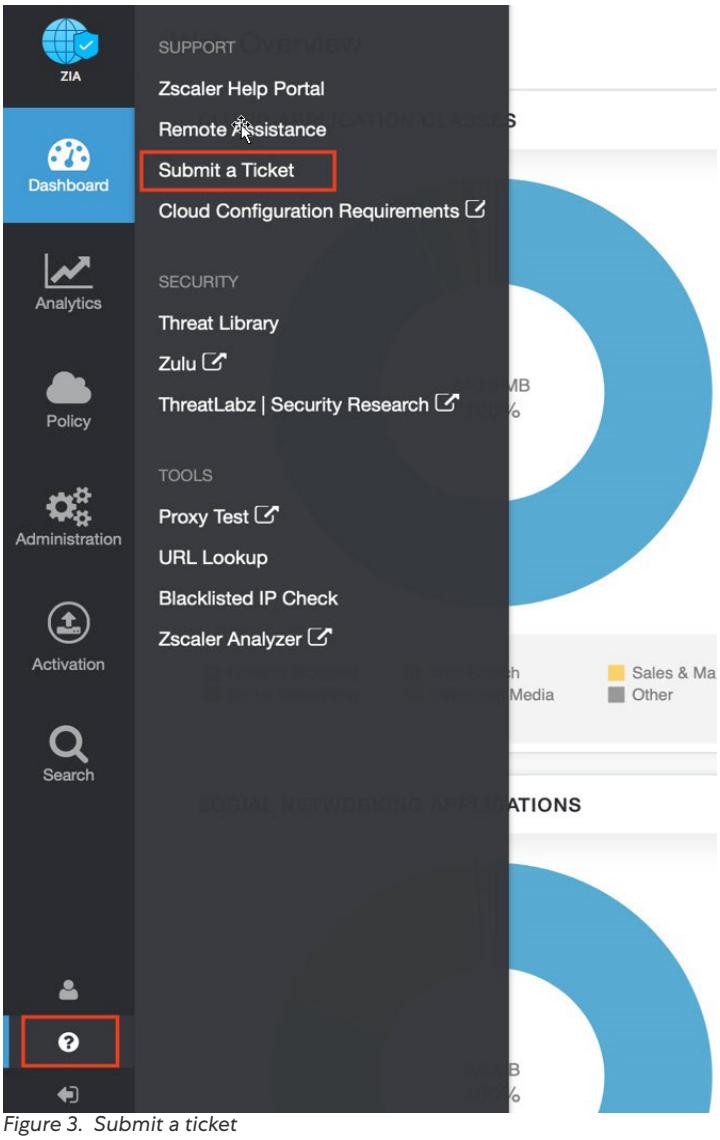

Figure 3. Submit a ticket

