ZSCALER AND TUFIN DEPLOYMENT GUIDE

JULY 2023, VERSION 1.0

BUSINESS DEVELOPMENT GUIDE

Contents

©2023 Zscaler, Inc. All rights reserved.

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)
NGFW	Next-Generation Firewall
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SaaS	Software as a Service
SDN	Software-Defined Network
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
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)

©2023 Zscaler, Inc. All rights reserved.

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. For more information, see Zscaler's website or follow Zscaler on Twitter @zscaler.

Tufin Overview

Tufin is the leader in network security policy management and continuous compliance automation. The platform centralizes, automates, and orchestrates network and cloud access for many of the largest organizations in the world. Over 2,900 enterprises have trusted Tufin to implement accurate network changes in minutes instead of days, accelerate secure application deployments, and virtually eliminate manual tasks. As a vendor-agnostic solution designed to integrate network and cloud security processes, Tufin balances security and business agility. To learn more, refer to Tufin'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:

- Appendix A: Requesting Zscaler Support
- Zscaler Resources
- Tufin Resources

Software Versions

This document was authored using the latest version of the 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.

©2023 Zscaler, Inc. All rights reserved.

Zscaler and Tufin Introduction

Overviews of the Zscaler and Tufin applications are described in this section.

ZIA Overview

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of it as a secure internet on-ramp—all you do is 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 the 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, intrusion prevention system (IPS), Sandboxing, data loss prevention (DLP), and Browser 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.

©2023 Zscaler, Inc. All rights reserved.

Tufin SecureTrack+ Overview

Tufin SecureTrack+ offers a holistic view of network access and security configurations, centralizing network security policy management, risk mitigation, and compliance monitoring across your entire enterprise.

Tufin SecureTrack+ centralizes network security policy management, risk mitigation and compliance monitoring across firewalls, NGFWs, routers, switches, SDN and hybrid cloud. SecureTrack+ provides holistic visibility, and consolidates the management of your network segmentation policies across on-premises and cloud. SecureTrack+ allows you to establish a baseline of allowed and blocked traffic between security zones and monitor in real time for violations, making it easier to implement and manage consistent network segmentation.

Tufin SecureTrack+ integrates with Zscaler Cloud Firewall to support the following features:

- Policy visibility for policy type: Firewall Policy Control
- Report generation
- Change analysis and monitoring
- Risks calculation
- Regulatory compliance
- Traffic simulation query
- Policy optimization

Tufin Resources

The following table contains links to Tufin support resources.

Name	Definition
Tufin Support	Online Support for Tufin customers.
Tufin customer log in	Online customer log in site.

©2023 Zscaler, Inc. All rights reserved.

Introduction

SecureTrack+ communicates with ZIA using a REST API. You must create an API Admin with limited permissions on the Zscaler side.

This document describes how to set up the integration, which includes:

- Creating a minimal ZIA Admin with limited role for SecureTrack+ to communicate
- Adding the ZIA service to SecureTrack+

©2023 Zscaler, Inc. All rights reserved.

ZIA Setup

The following sections show how to set up ZIA.

Creating a Role in the ZIA Admin Portal

1. Log in to the ZIA Admin Portal as an administrator.
2. Go to **Administration** > **Authentication** > **Role Management**.

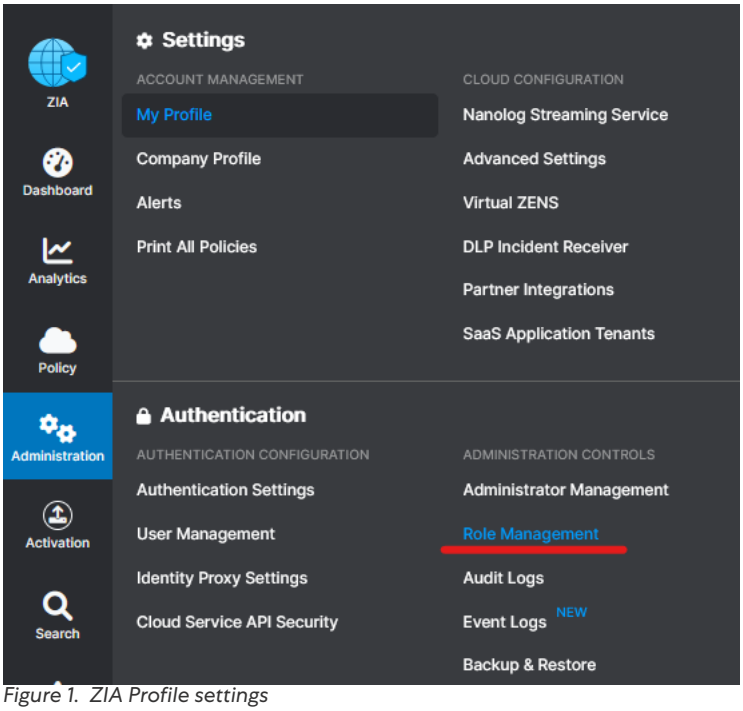

Figure 1. ZIA Profile settings

3. Click **Add Administrator Role**. This role is used by the SecureTrack+ API Admin.
   a. **Name:** Enter a role name.
   b. **Enable Permissions for Executive Insights:** Enabled.
   c. **Logs Limit (Days):** Unrestricted.
   d. **Dashboard Access:** View only.
   e. **Reporting Access:** View only.
   f. **Insights Access:** None.
   g. **Policy Access:** View Only.
   h. **Administrators Access:** View only.
   i. **Alerts Access:** None.
   j. **User Names:** Obfuscated.
   k. **Device Information:** Visible.
   l. **Workflow Access**: Restricted.
   m. **Advance Settings:** Disabled.
   n. **Data Loss Prevention:** Disabled.
   o. **Security:** Disabled.

©2023 Zscaler, Inc. All rights reserved.

p. **SSL Policy:** Disabled.
q. **Virtual ZEN Configuration**: Disabled.
r. **Firewall DNAT, DNS & IPS:** Enabled.
s. **NSS Configuration:** Disabled.
t. **Partner Integration:** Disabled.
u. **Remote Assistance Management:** Disabled.
v. **Access Control:** Enabled.
w. **Traffic Forward:** Enabled.

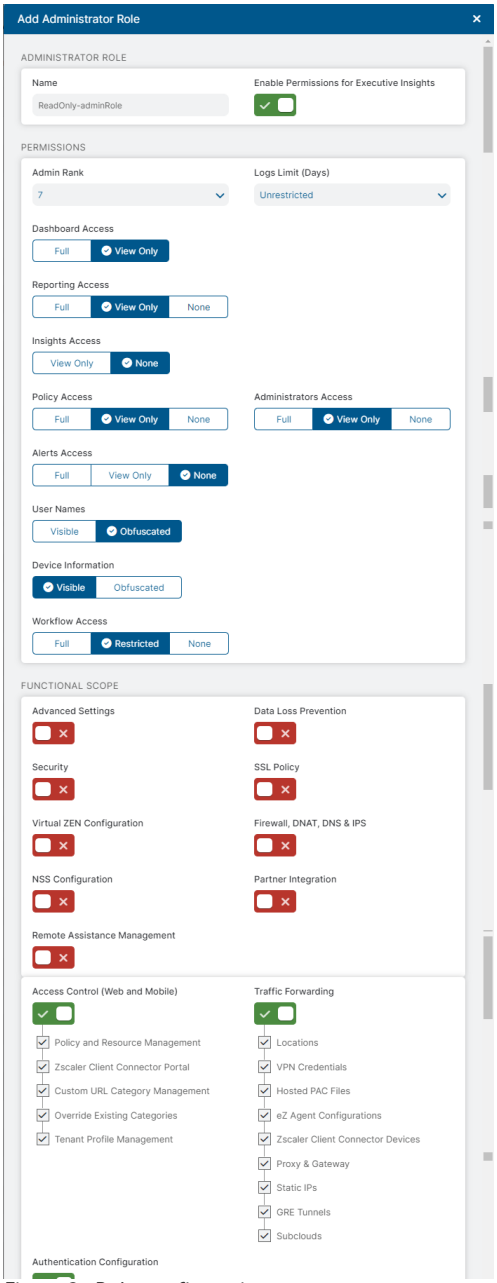

Figure 2. Role configuration

©2023 Zscaler, Inc. All rights reserved.

Creating a User and API Key

Use the following steps to create a user and an API key in ZIA.

1. Go to **Administration** > **Administrator Management** > **Add Administrator**.
2. Configure the options.
   a. **Login ID**: Enter the login ID.
   b. Enter an **Email** and **Name**.
   c. **Role**: Enter the previously created role.
   d. **Status**: Enabled.
   e. **Scope**: Organization.
   f. Set the **Password**.
   g. Click **Save**.

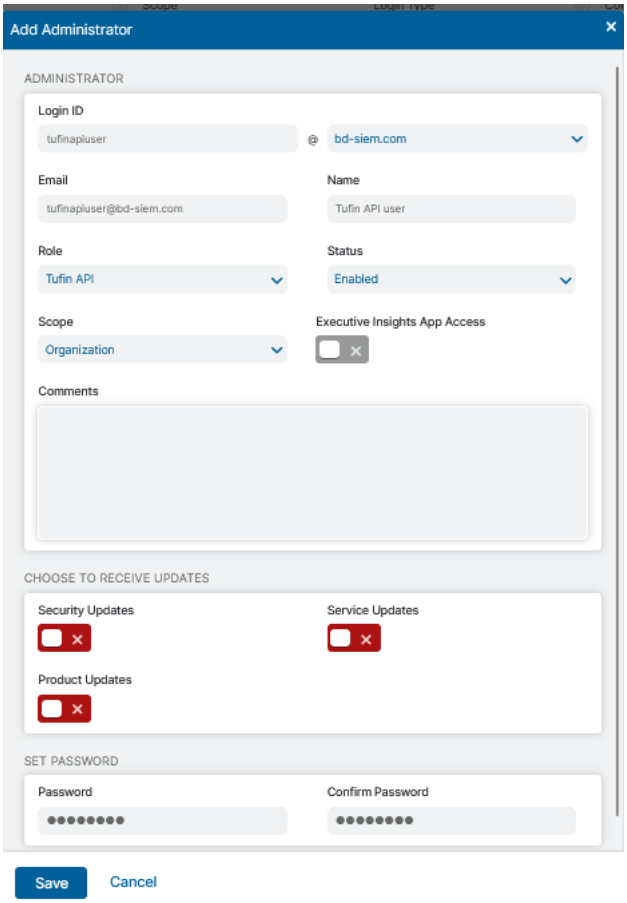

Figure 3. ZIA Administrator configuration

3. Go to **Administration** > **Authentication** > **Cloud Services API Security**.
4. Click the **Add API Key**.

©2023 Zscaler, Inc. All rights reserved.

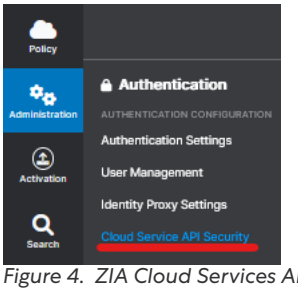

Figure 4. ZIA Cloud Services API Security

5. Copy and save the API key and base URL.

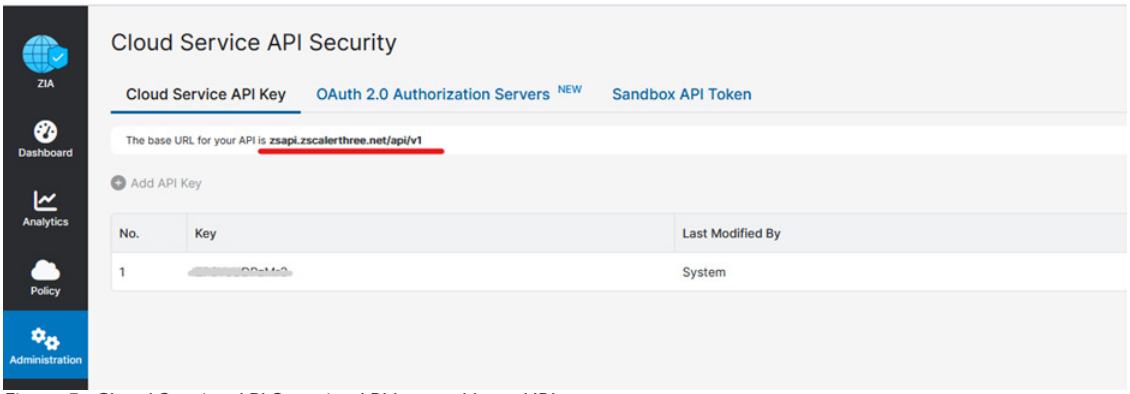

Figure 5. Cloud Service API Security API key and base URL

Activating Changes

If the ZIA Admin Portal shows the Activation icon with a number indicator, activate the changes made by going to Activation and pressing the Activate button.

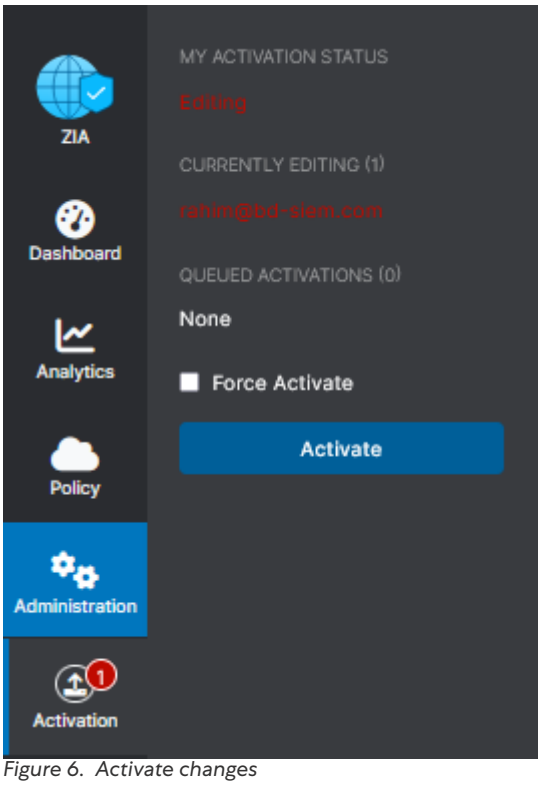

Figure 6. Activate changes

©2023 Zscaler, Inc. All rights reserved.

Tufin SecureTrack+ Setup

The following sections demonstrate setting up Tufin.

Adding ZIA Devices

1. In Tufin Orchestration Suite (TOS) Aurora, go to **Monitoring** > **Manage Devices**.
2. Select **Zscaler** > **ZIA Cloud Firewall**.

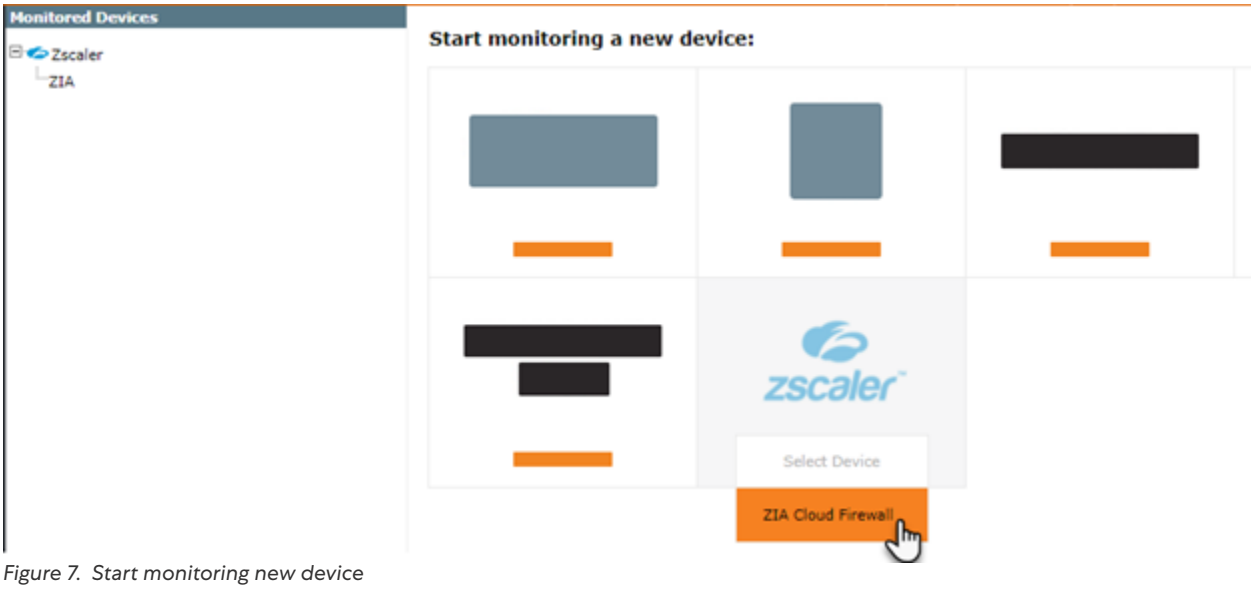

Figure 7. Start monitoring new device

3. Enter a **Name for Display**.

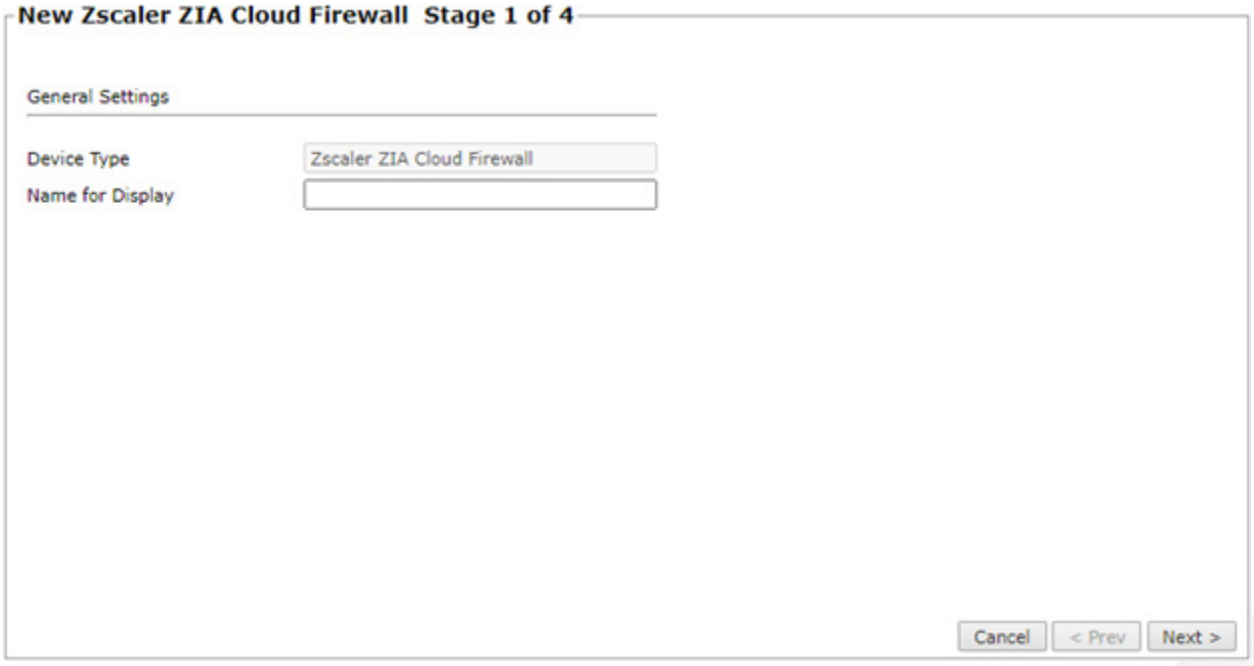

Figure 8. General Settings

©2023 Zscaler, Inc. All rights reserved.

4. Click **Next**.
5. Enter the ZIA credentials, including the API key, the relevant Zscaler Cloud login domain, and click **Next**.
6. Paste the API key you copied earlier. See step 5 of **Creating a User and API Key**.

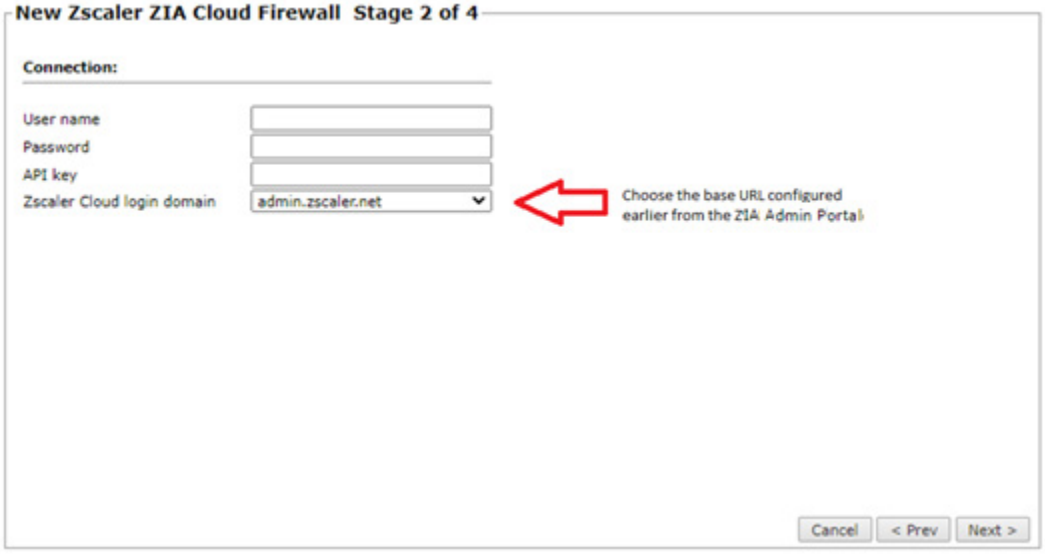

Figure 9. Connection settings

7. In **Monitoring Settings**, do the following:
   a. To use real-time monitoring and timing settings from the **Timing** page, select **Default**. Otherwise, select **Custom** and configure the monitoring mode and settings.
   b. For **Periodic Polling**, select **Custom settings** and configure the **Polling frequency**: How often TOS Aurora fetches the configuration from each device. If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.
   c. Click **Next**.

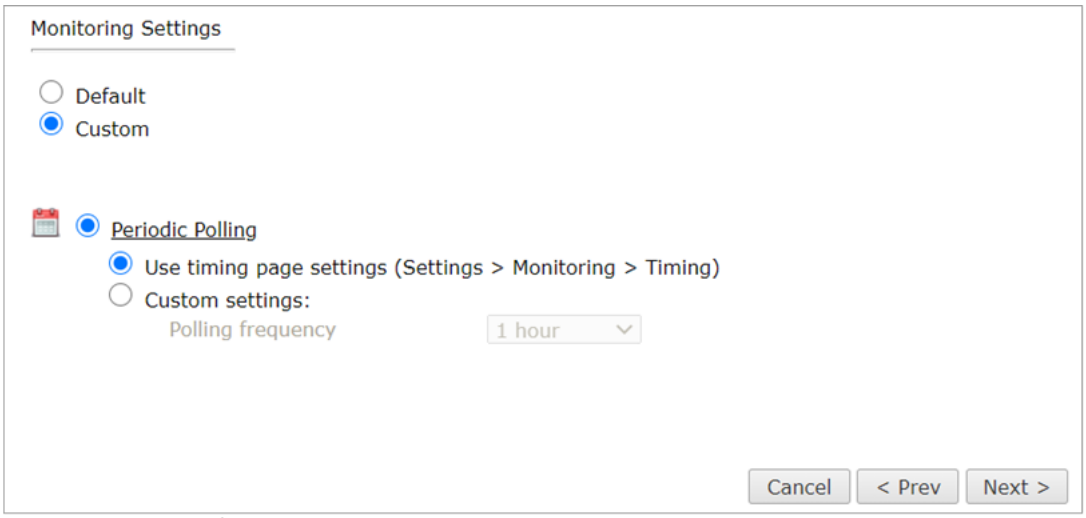

Figure 10. Monitoring Settings

8. Click **Save**.

The Zscaler ZIA Cloud Firewall device appears in the Monitored Devices tree.

©2023 Zscaler, Inc. All rights reserved.

Verify Revision Retrieval

After you have connected Zscaler to TOS Aurora, you can verify successful revision retrieval in TOS.

On the Revisions Status page, you can see the revision status information for every device monitored by SecureTrack+, including ZIA.

1. In TOS Aurora, go to **Monitoring** > **Revisions Status**.
2. Verify the revision retrieval for the ZIA device was completed successfully.

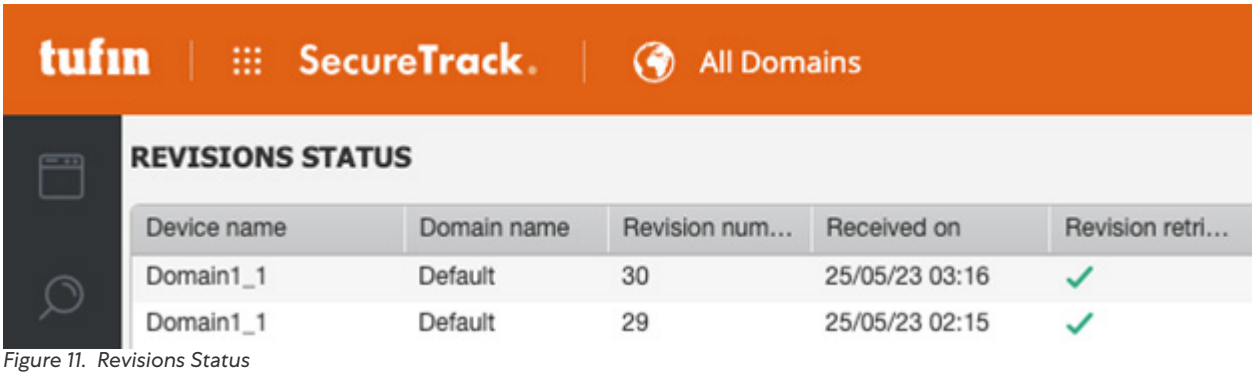

Figure 11. Revisions Status

©2023 Zscaler, Inc. All rights reserved.

Appendix A: Requesting Zscaler Support

If you need Zscaler Support for provisioning certain services or to help troubleshoot configuration and service issues, it is available 24/7/365. To contact Zscaler Support, go to **Administration** > **Settings** > **Company Profile**.

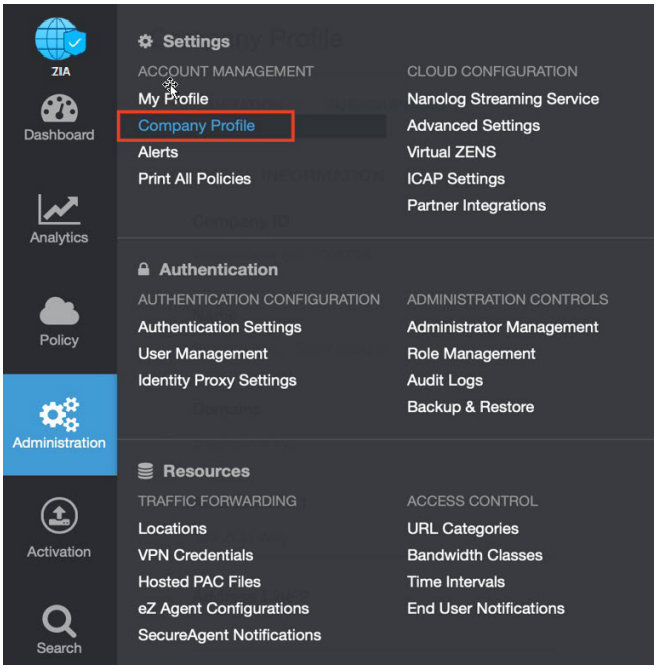

Figure 12. Collecting details to open support case with Zscaler TAC

Save Company ID

Copy your Company ID.

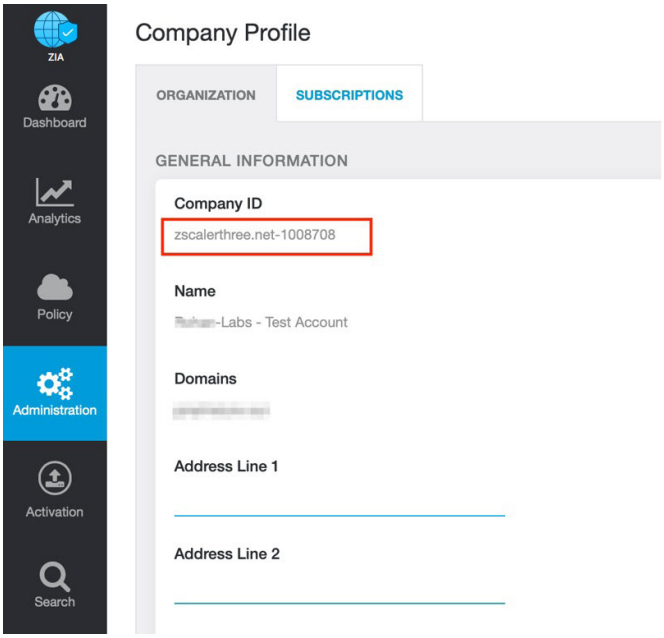

Figure 13. Company ID

©2023 Zscaler, Inc. All rights reserved.

Enter Support Section

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

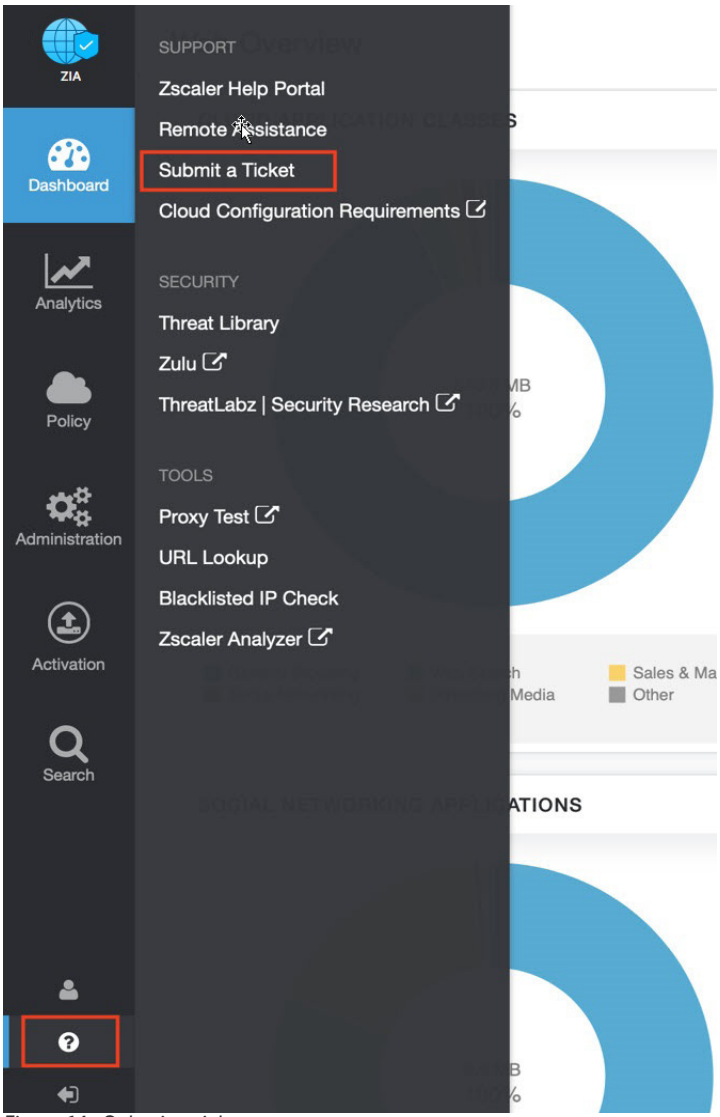

Figure 14. Submit a ticket

©2023 Zscaler, Inc. All rights reserved.