ZSCALER AND REDSEAL DEPLOYMENT GUIDE

OCTOBER 2023, VERSION 1.0

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)
ZCP	Zscaler Cloud Protection (Zscaler)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

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.

RedSeal Overview

RedSeal helps government agencies and Global 2000 companies see and secure their on-premises and cloud environment. With RedSeal, enterprises improve their resilience to security events by understanding what's on their networks, how it's all connected, and the associated risk. RedSeal protects enterprises by validating that resources are securely configured and continuously monitors compliance to internal and external security mandates. To learn more, refer to RedSeal'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
- RedSeal 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 RedSeal Introduction

Overviews of the Zscaler and RedSeal 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
ZIA Help Portal	Help articles for ZIA.
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.
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.

RedSeal Network Overview

RedSeal Network brings complex hybrid on-premises and multi-cloud networks into one, comprehensive, dynamic visualization. This empowers you to:

- Quickly identify gaps in your infrastructure.
- Leverage bi-directional integration and vulnerability scanners to quickly identify scan coverage.
- Ensure your critical resources aren't exposed to the internet.
- Continuously verify compliance mandates according to industry best practices.

RedSeal Resources

The following table contains links to RedSeal support resources.

Name	Definition
RedSeal Customer Support	Online customer support for RedSeal customers.
RedSeal Resource Center	Online resources for RedSeal solutions.

Setting Up ZIA

Configuring ZIA involves the following four steps:

- Set up a ZIA Admin Role.
- Set up Management User.
- Gather Company ID.
- Copy the API Key

The following image shows the RedSeal Integration.

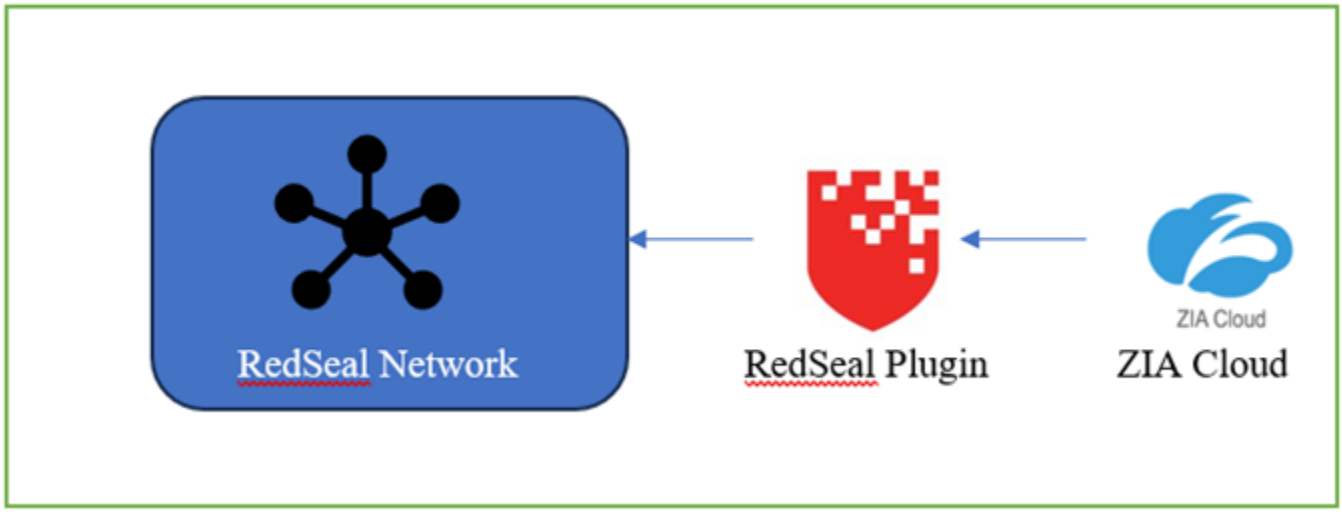

Figure 1. Zscaler and RedSeal integration architecture

Step 1: Set Up a ZIA Admin Role

To set up a ZIA Admin Role:

1. From the ZIA Admin Portal, go to **Administration** > **Role Management**.

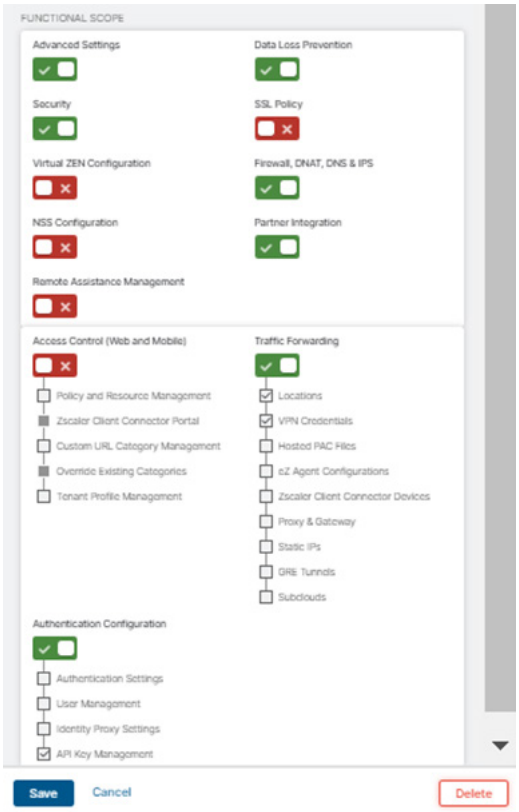

Figure 2. Role Management

2. Click **Add**.

3. In the first sections of the **Add Administrator Role** window, configure the following (all other settings remain at default):
    a. **Name**: Enter a unique name for the role.
    b. **Logs Limit (Days)**: Enter the number of days the role can remain active.
    c. **Dashboard Access**: Set to **View Only**.
    d. **Reporting Access**: Set to **None**.
    e. **Policy Access**: Set to **View Only**.
    f. **Administrators Access**: Set to **View Only**.
    g. **Alerts Access**: Set to **View Only**.
    h. **User Names**: Set to **Obfuscated**.
    i. **Device Information**: Set to **Visible**.

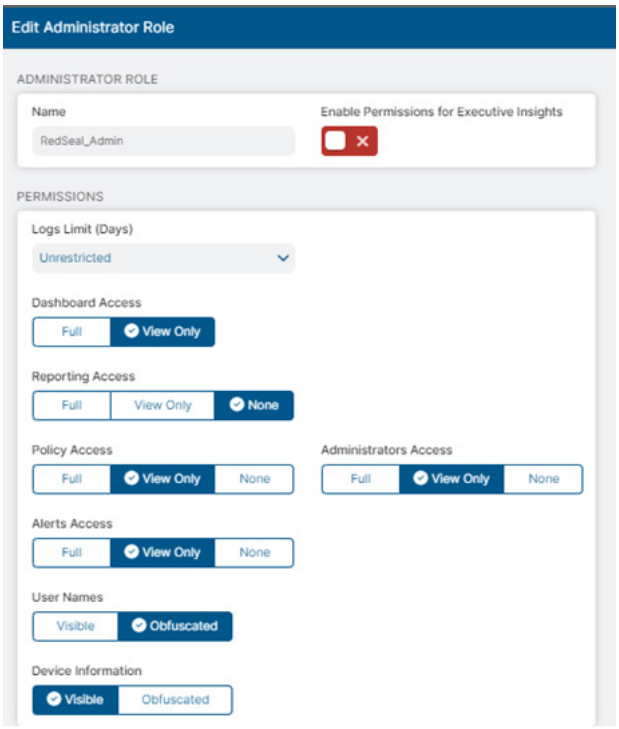

Figure 3. Add Administrator Role

4. In the third section of the **Add Administrator Role** window, enable the following settings (all other settings remain disabled):
   - Advanced Settings
   - Data Loss Prevention
   - Security
   - Firewall, DNAT, DNS & IPS
   - Partner Integration
   - Traffic Forwarding
   - Authentication Configuration
5. Click **Save**.

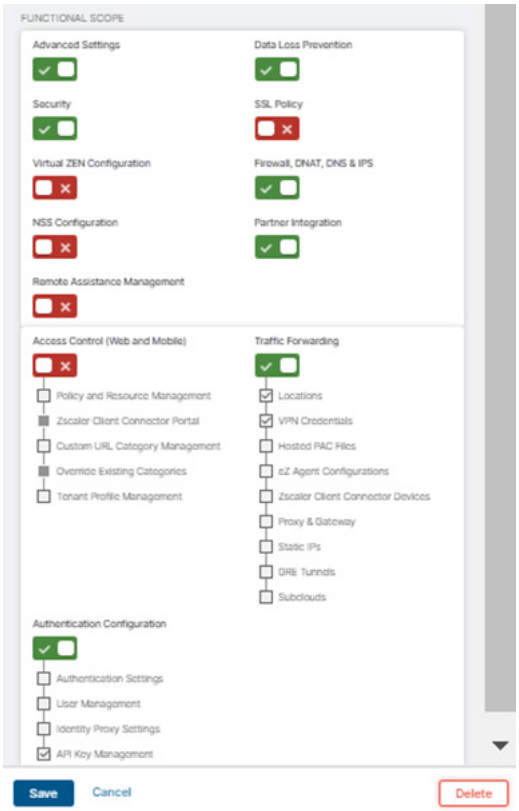

Figure 4. Role Management Settings

Step 2: Set Up a Management User

To set up a management user:

1. From the ZIA Admin Portal, go to **Administration** > **Administrator Management**.

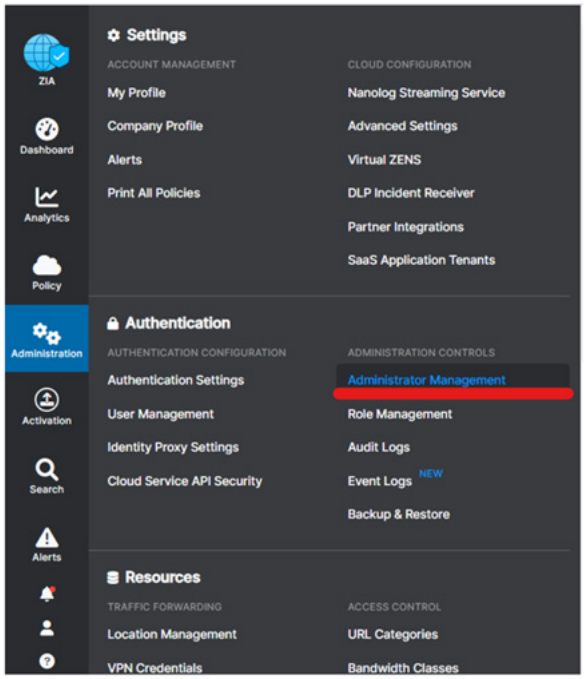

Figure 5. Add Administrator

2. Click **Add**.

3. In the **Add Administrator** window, configure the following settings:
   a. **Login ID**: Enter the user ID and domain name used to log in to RedSeal.
   b. **Email**: Enter the user email address.
   c. **Name**: Enter a username.
   d. **Role**: Select the correct role from the drop-down menu.
   e. **Status**: Select **Enabled**.
   f. **Scope**: Select **Organization**.
   g. **Security Updates**: Set to **Disabled**.
   h. **Service Updates**: Set to **Disabled**.
   i. **Executive Insights App Access**: Leave as-is.
   j. **Product Updates**: Set to **Disabled**.
   k. **Password**: Enter a password for the administrator.
   l. **Confirm Password**: Confirm the password.
4. Click **Save**.

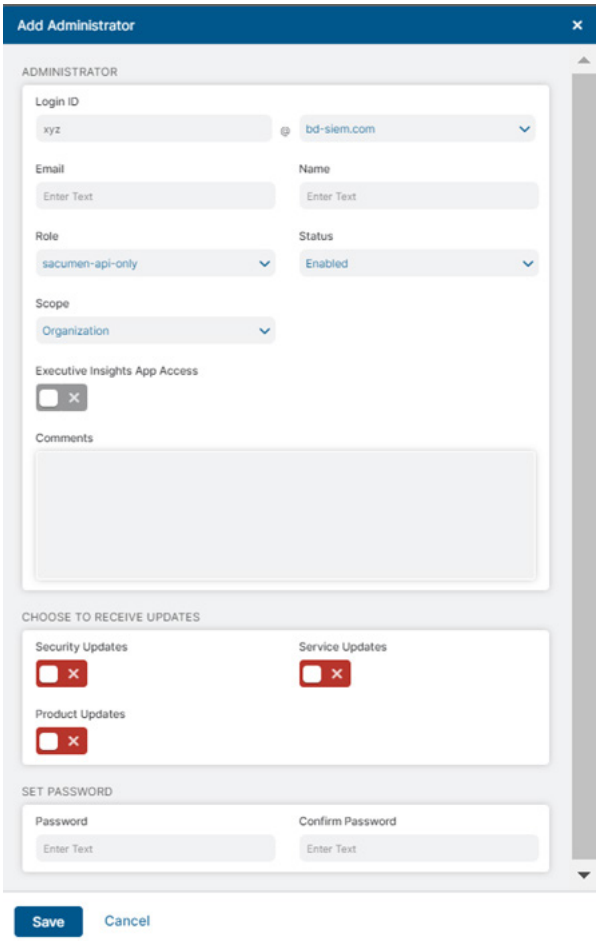

Figure 6. Add Administrator Settings

Step 3: Get the Company ID

From the ZIA Admin Portal, go to **Administration** > **Company Profile**.

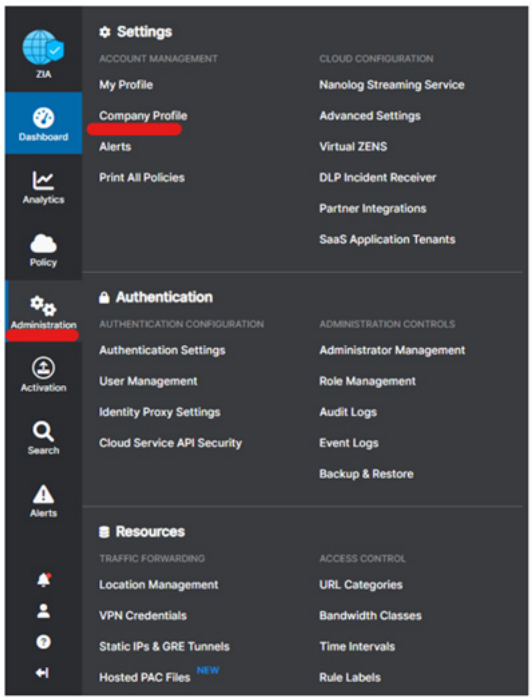

Figure 7. Company Profile

Step 4: Get the API Key

From the ZIA Admin Portal, go to **Administration** > **Cloud Service API Security**.

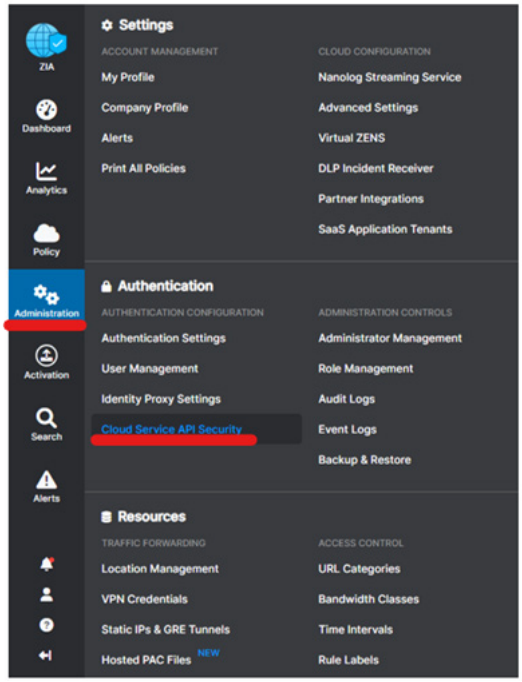

Figure 8. Cloud Service API Security

Set Up the RedSeal Network

To set up the RedSeal network:

1. Open RedSeal Network and chose **File**.
2. Import to set up a new **Data Collection Task**.

Item	Description
Hostname (Required)	Select related Zscaler URL (Embedded)
Zscaler Company ID	Gather from ZIA Admin Portal
Preferred Name	Rename the device as desired
Include Location	Enter a location name to include
Exclude Location	Enter a location name to exclude

3. Select **L2 & L3 Devices**.
4. Select **Zscaler Cloud**.

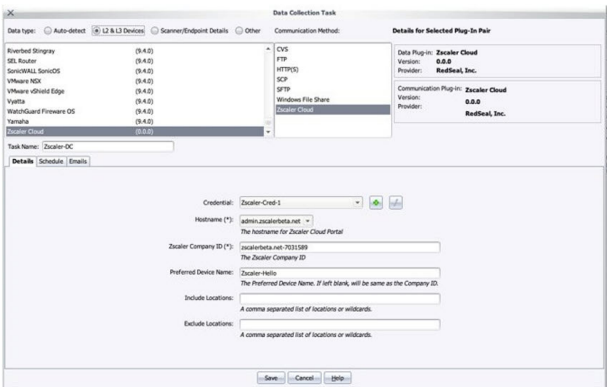

Figure 9. Data Collection task

5. Add new credentials as shown in the following image.

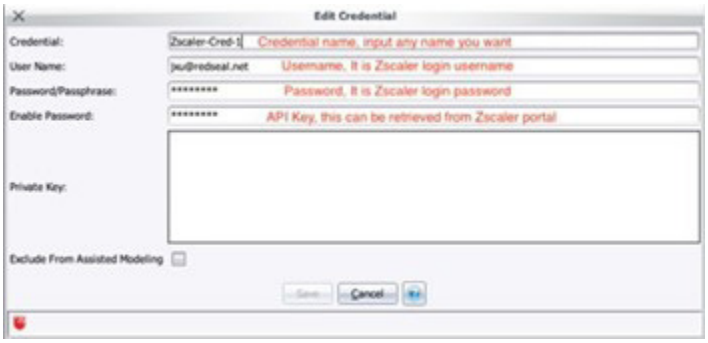

Figure 10. Edit Credentials

6. Verify the integration on RedSeal Network by going to the **Maps & Views** tab.

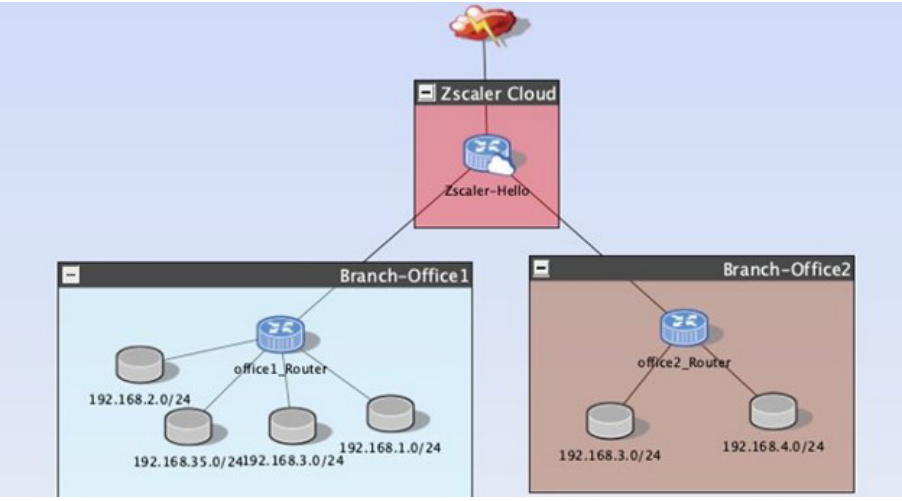

Figure 11. Maps & Views tab

7. Verify the **Detailed Path** with from the Incident Investigation Interface.

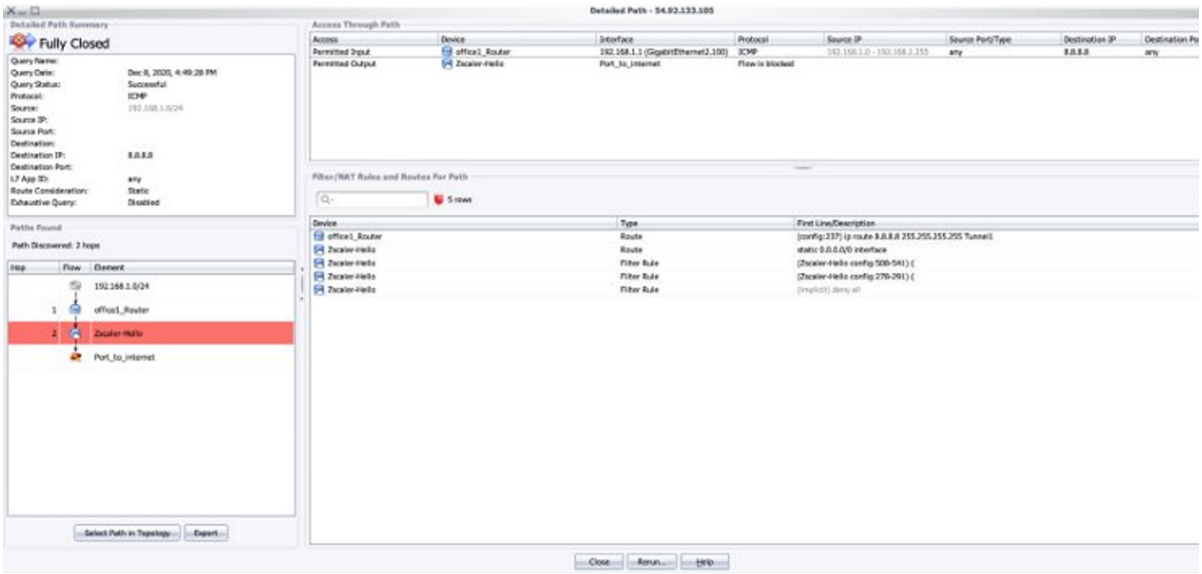

Figure 12. Incident Investigation Interface

8. Verify the populated **Access Rules**.

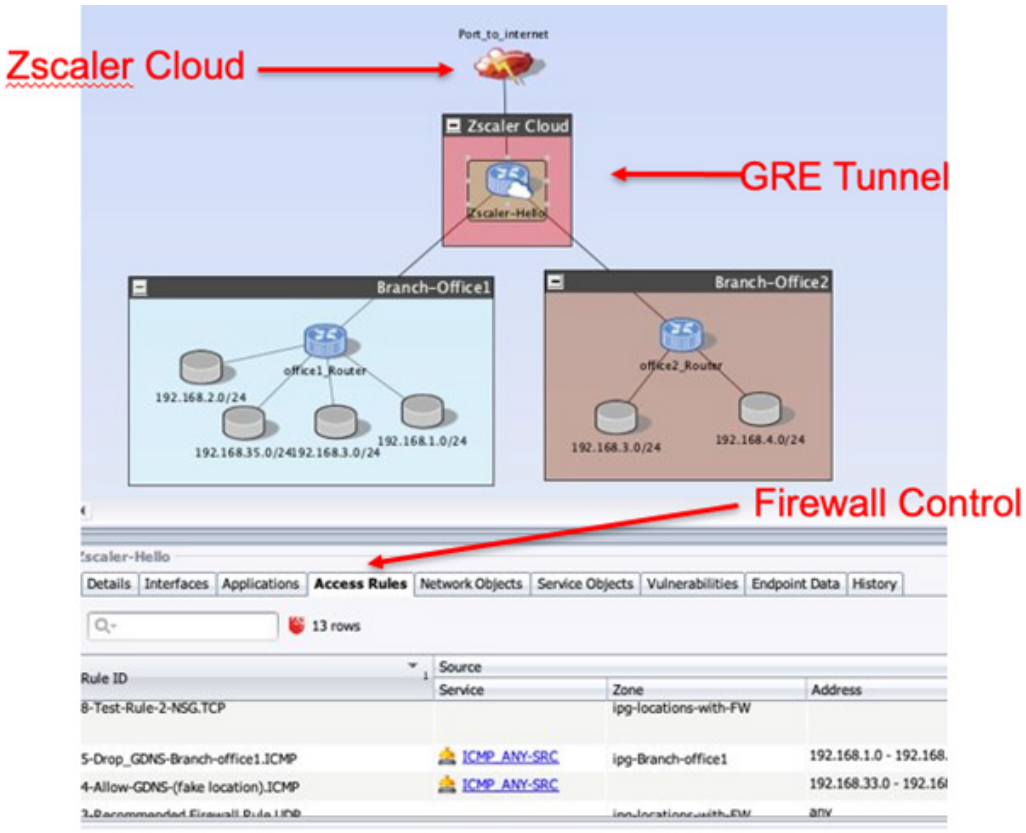

Figure 13. Access Rules

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**.

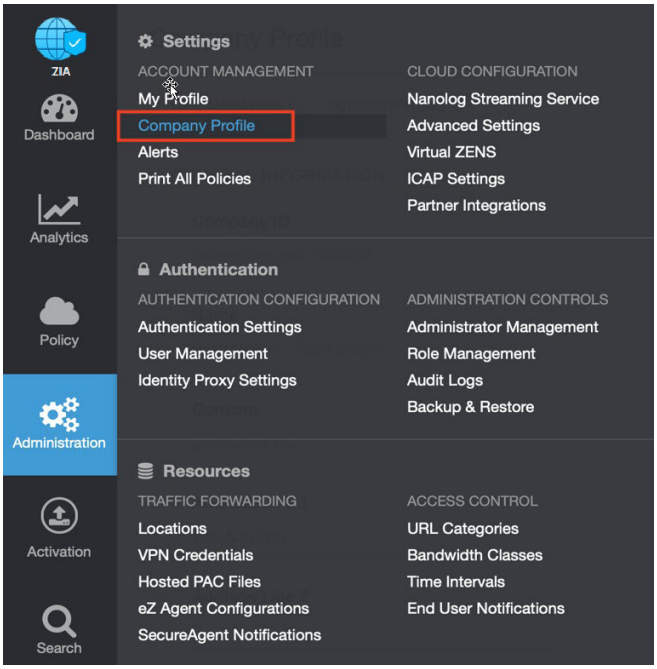

Figure 14. Collecting details to open support case with Zscaler TAC

2. Copy your Company ID.

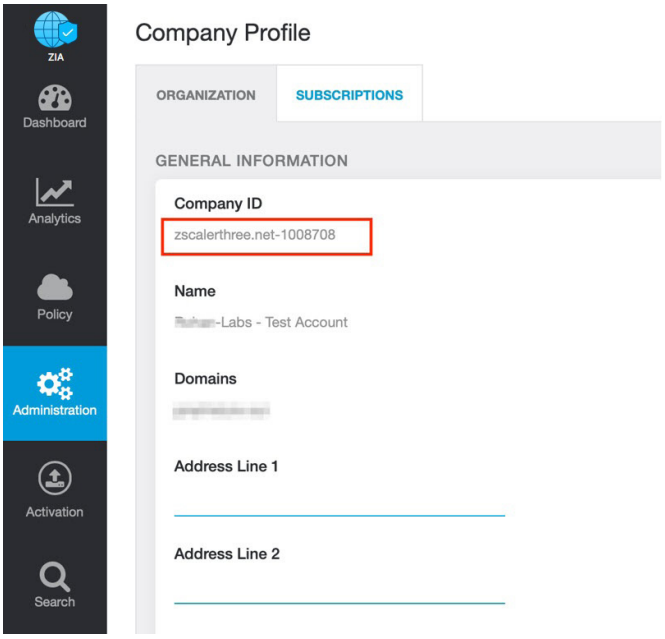

Figure 15. Company ID

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

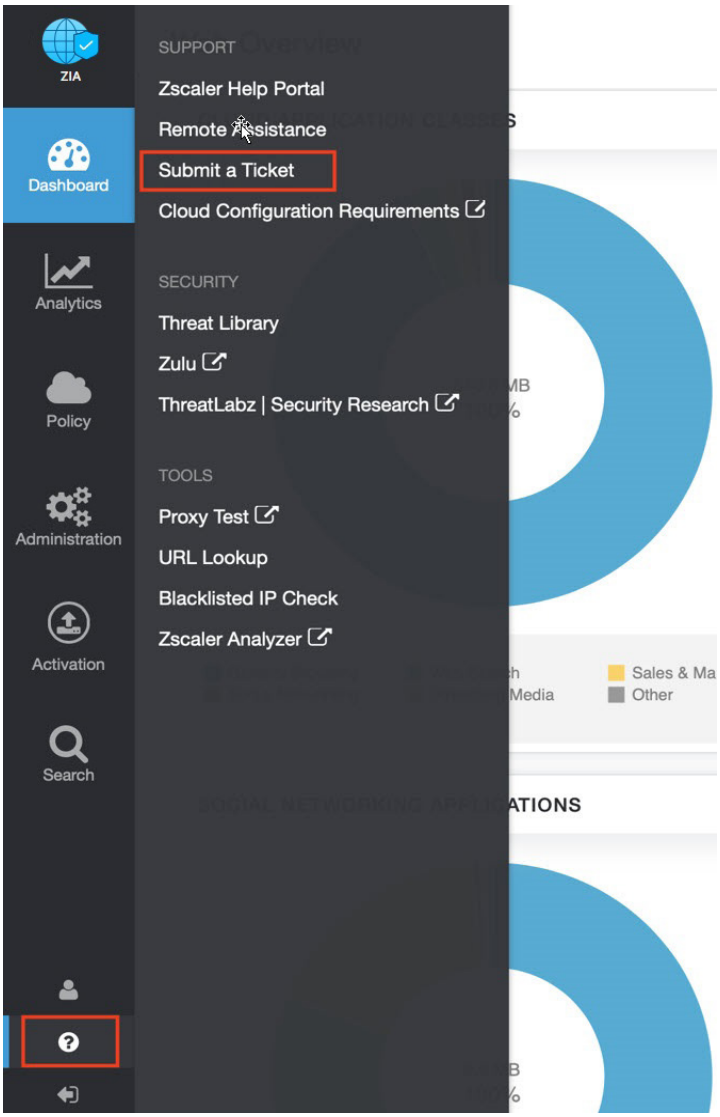

Figure 16. Submit a ticket

