# ZSCALER AND ADAPTIVA DEPLOYMENT GUIDE

MAY 2021, VERSION 1.1

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) |
| CDN | Content Delivery Network (Adaptiva) |
| 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.

## Adaptiva Overview

Adaptiva is a leading, global provider of endpoint management and security solutions. The company's products, including OneSite Cloud, Endpoint Health, and Evolve VM empower enterprises to manage and secure endpoints at unparalleled speed and massive scale using the power of peer-to-peer technology. Leading global Fortune 1000 organizations, including T- Mobile, Nokia, HSBC, Walgreens, the U.S. Department of Defense, and the U.S. Department of Homeland Security, use Adaptiva products to eliminate the need for a vast IT infrastructure and automate countless endpoint management and security tasks. To learn more, refer to Adaptiva'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
- Adaptiva 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 Adaptiva Introduction

Overviews of the Zscaler and Adaptiva 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. |

## OneSite Anywhere Overview

OneSite Anywhere is a single-server solution for distributing software and content. By employing a peer-to-peer architecture, OneSite Anywhere allows every endpoint—whether on-premises or remote—to act as both a client and a server ensuring faultless delivery across low-bandwidth connections without overloading the WAN or VPN. This solution supports Microsoft ConfigMgr, Intune, and VMware Workspace ONE, and addresses the high costs, security risks, and inefficiencies associated with traditional content distribution infrastructures.

## Adaptiva Resources

The following table contains links to Adaptiva support resources.

| Name | Definition |
|---|---|
| Adaptiva Product Documentation | Online product documentation for Adaptiva products. |
| Adaptiva Community | Online community for Adaptiva customers. |
| Adaptiva Support | Online support for Adaptiva customers. |

 

# Overview of Zscaler for the Adaptiva OneSite Cloud

Adaptiva is a leading, global provider of endpoint management and security solutions. The company's products, including OneSite Cloud, Endpoint Health, and Evolve VM, empower enterprises to manage and secure endpoints at unparalleled speed and massive scale using the power of peer-to-peer technology. The advantages of OneSite Cloud is the ability to provide content to any device on any network.

This guide covers the configuration of Zscaler Internet Access for Adaptiva OneSite Cloud thus allowing the full functionality of the product.

## Adaptiva OneSite Cloud

With changes to world, workforces are increasingly working away from the enterprise network which has forced many organizations to accelerate their digital transformation efforts to meet new consumer needs and enable employees to work remotely. One of the barriers to that transformation is the ability to deliver content (such as new software, security patches, system updates, operating systems, and applications) to endpoints quickly, securely and without creating network issues. OneSite Cloud helps solve this challenge. OneSite Cloud combines the world's most advanced software distribution engine with a new, revolutionary architecture to seamlessly extend the boundaries of the enterprise network to cover the entire internet.

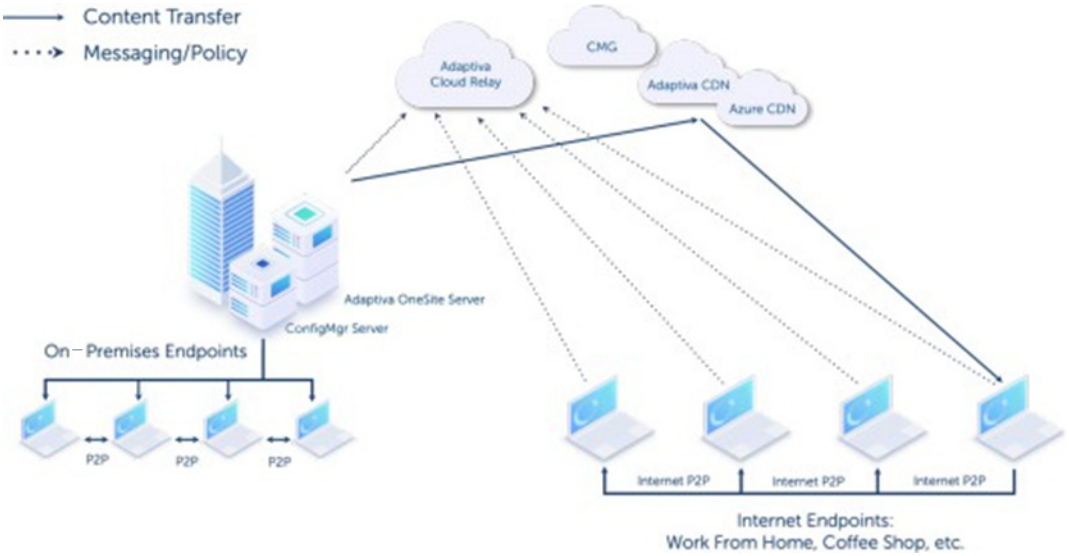


*Figure 1. Network Flow*

## Zscaler and OneSite Cloud Integration

OneSite Cloud with Zscaler integration allows for securely managing endpoints at unprecedented speed and scale regardless of where they are located, along with the ability to control access to endpoints and monitor traffic flow. This allows the ability to distribute content reliably and securely to all endpoints, including those not connected to the corporate network, which is key to enabling a remote workforce and easing the pressure on your corporate network. OneSite Cloud delivers content to endpoints at unprecedented speed and scale regardless of where they are and ensures they stay updated and secure at all times while offloading the WAN and VPN traffic to ensure your network stays highly available for mission-critical applications.

 

## What Makes the OneSite Cloud Unique

- Efficient end-point content delivery: OneSite Cloud client minimizes the need to download content from single sources, and then uses intelligence, not additional infrastructure, to store and distribute that content, thus eliminating the need for hundreds or thousands of servers typically used to distribute software across a large enterprise. The Adaptiva Content Delivery Network built into the OneSite Cloud license eliminates the need to store content on expensive cloud servers, dramatically reducing costs.
- Ease digital transformation: OneSite Cloud helps you transition from a traditional on-premises infrastructure to the Cloud and modern device management at your own speed to make your enterprise more agile and resilient. Breakthrough technologies in OneSite Cloud support a wide array of system management platforms such as Microsoft ConfigMgr, Microsoft Intune, and VMWare Workspace ONE. OneSite Cloud gives you confidence that all devices can receive critical updates no matter how the devices are connected.

 

# Configure OneSite Cloud with ZIA

The following figure shows the integration of OneSite Cloud and ZIA.

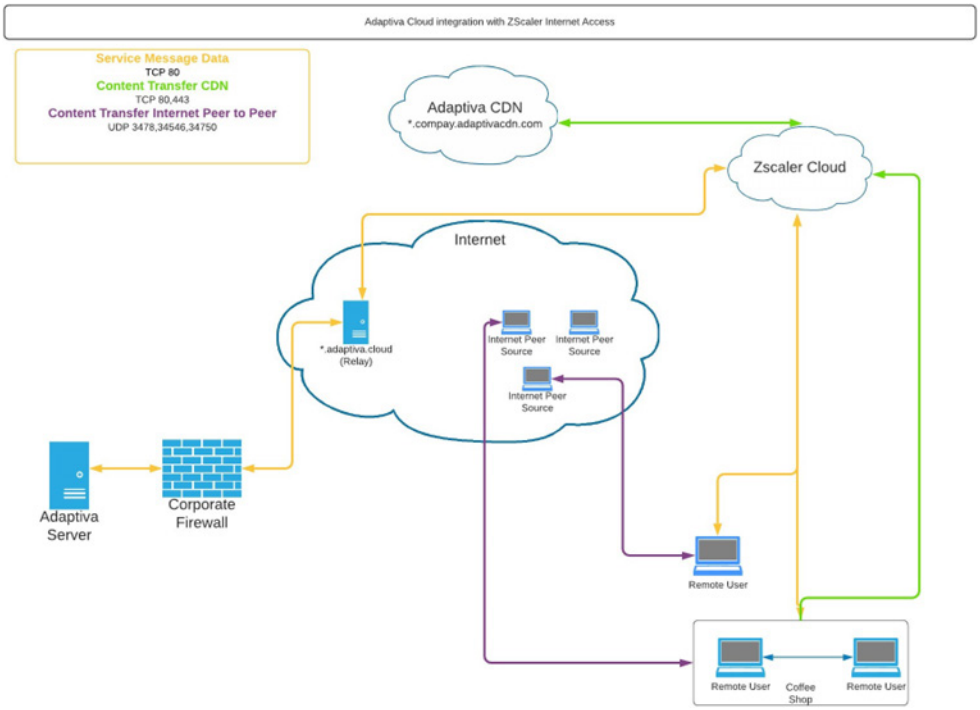


*Figure 2. ZIA Cloud and OneSite Cloud*

## Configure ZIA

Log in to the ZIA Admin Portal.

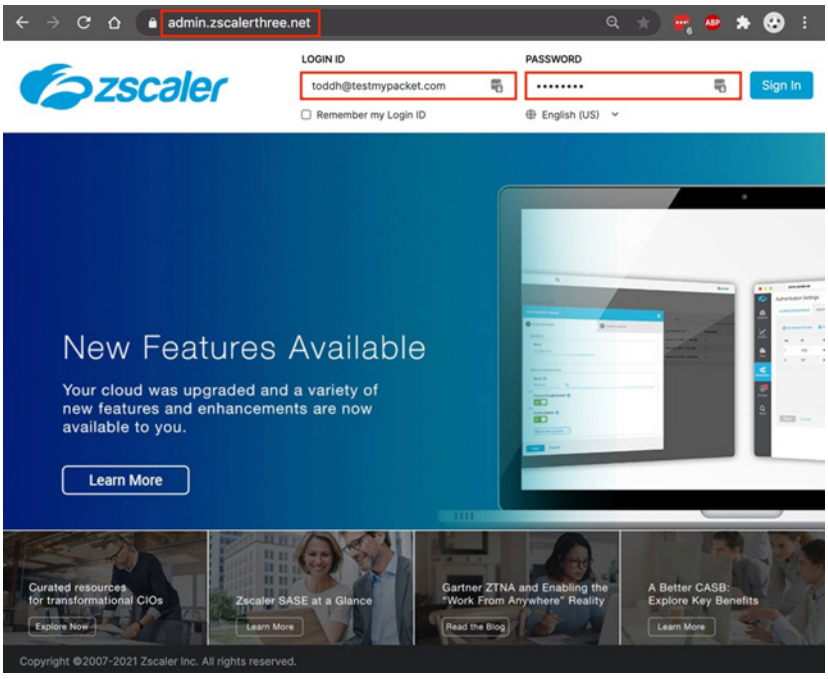


*Figure 3. Connect to ZIA Admin Portal*

 

## Configure Adaptiva Cloud App Policy

Configuring the policy to redirect Adaptiva Messaging to Adaptiva Cloud Relay is required for both server and clients if using Zscaler.

To configure the URL Filtering Rule:

1. Go to **Policy** > **URL & Cloud App Control**.
2. Click **Add URL Filtering Rule**.

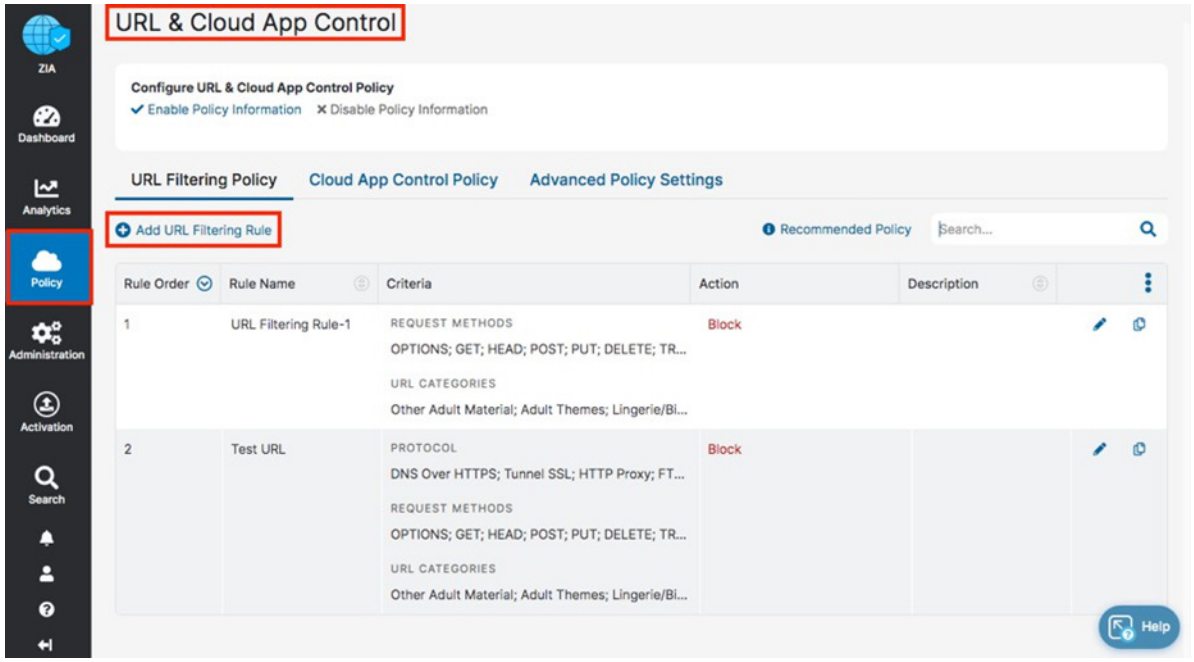


*Figure 4. Add Adaptiva Cloud URL Filtering Rule*

 

## Configure URL Filtering Rule

In the Add URL Filtering Rule window, select the Rule Order based on your current policy processing and enable the rule under Rule Status. Then select the arrow in URL Categories and finally select the Add icon on the URL Selection window to add in Adaptiva Cloud Category.

1. Select the **Rule Order** from the drop-down menu.
2. Enter a name for the **Rule Name** (e.g., `Adaptiva Cloud`).
3. Select **Enable** from the **Rule Status**.
4. Select the drop-down menu in the **URL Categories** field.
5. Select the **Add** icon (blue +) next to the **Search** field on the **URL Selection** window.

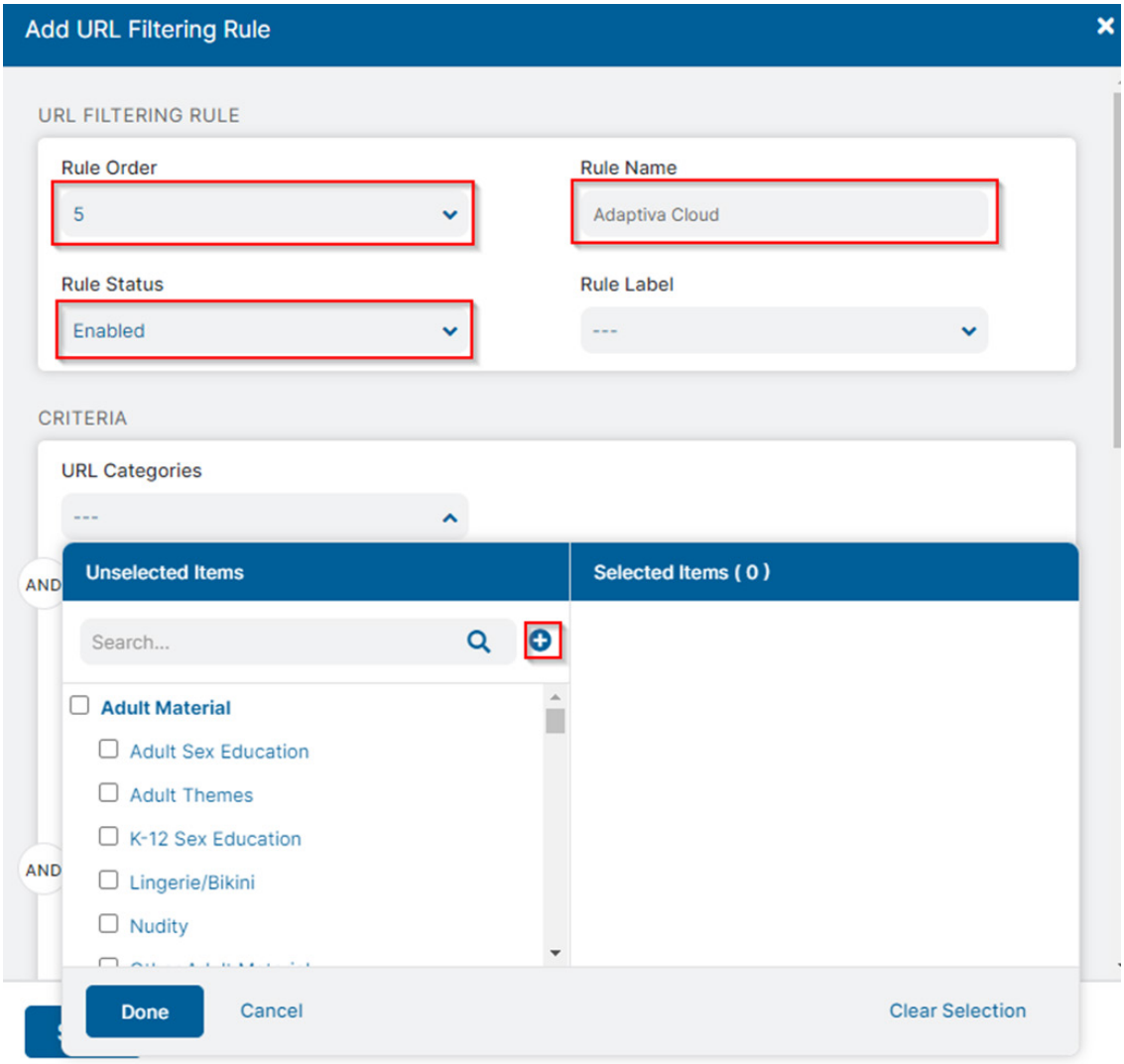


*Figure 5. Configure Adaptiva Filtering Rule*

 

## Configure Adaptiva URL Category

To configure the Adaptiva URL Category:

1. Enter the **Name** (e.g., `Adaptiva Cloud`).
2. Under **Custom URLs**, enter `.adaptiva.cloud`.
3. **(Optional) Description**: Enter the URL category for Adaptiva OneSite Cloud Messaging.
4. Click **Save**.

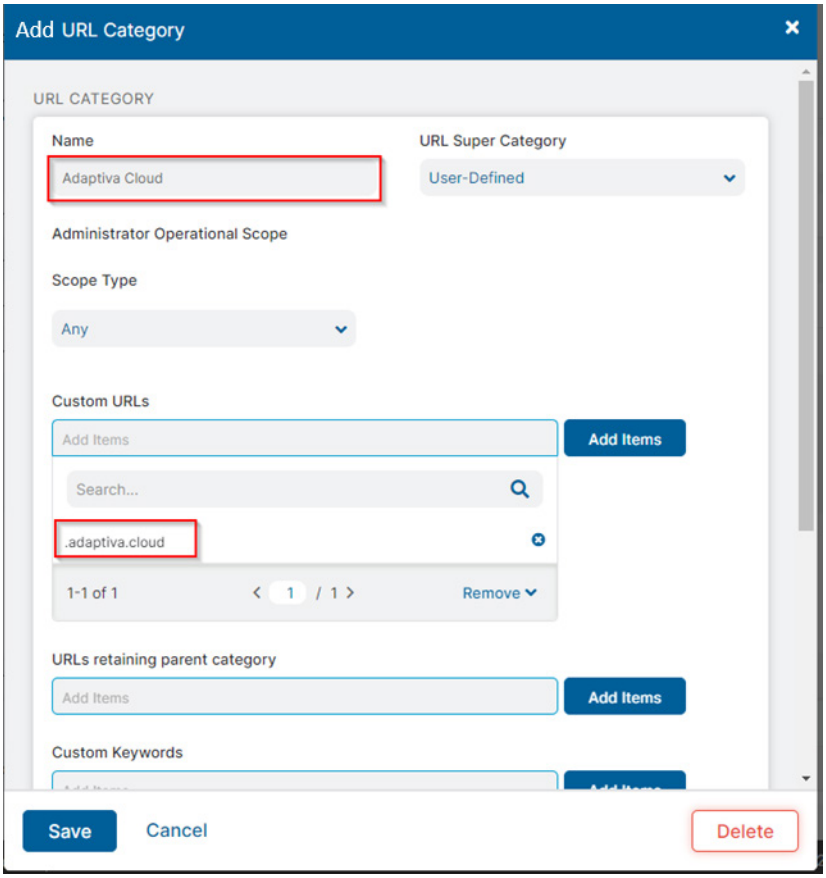


*Figure 6. Configure URL Category*

 

5. Scroll to fill in the remaining fields:
   a. For **Request Methods**, select **CONNECT**, **HEAD**, **GET**, and **POST**.
   b. For **Protocols**, select **HTTP** and **HTTPS**.
   c. For **Web Traffic**, select **Allow**.
   d. Select **Save** to complete the configuration.

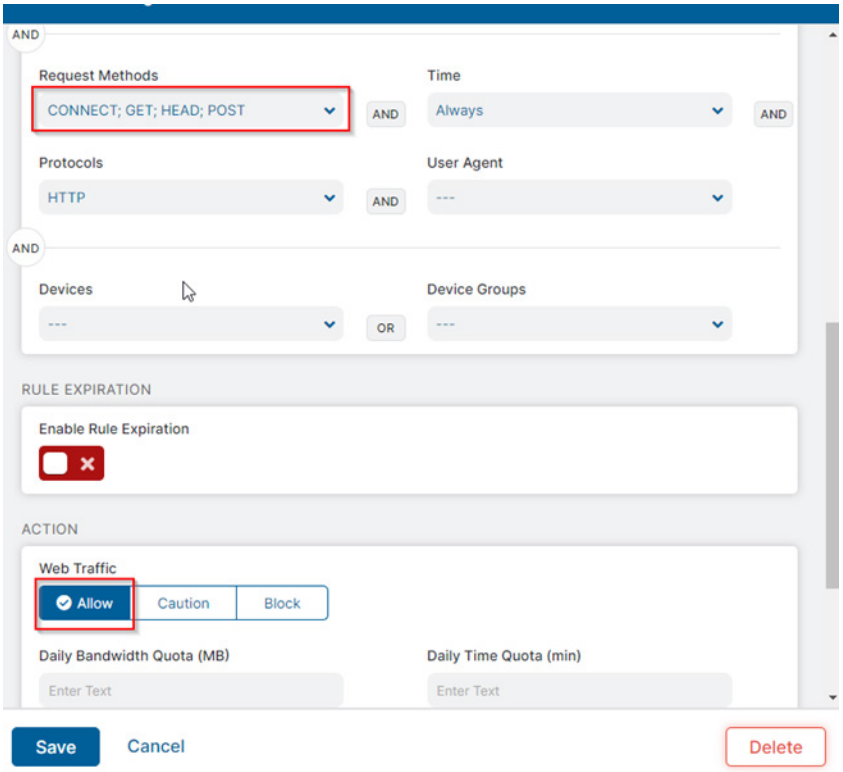


*Figure 7. Configure Adaptiva Cloud URL Category*

The configured Adaptiva Cloud policy is complete.

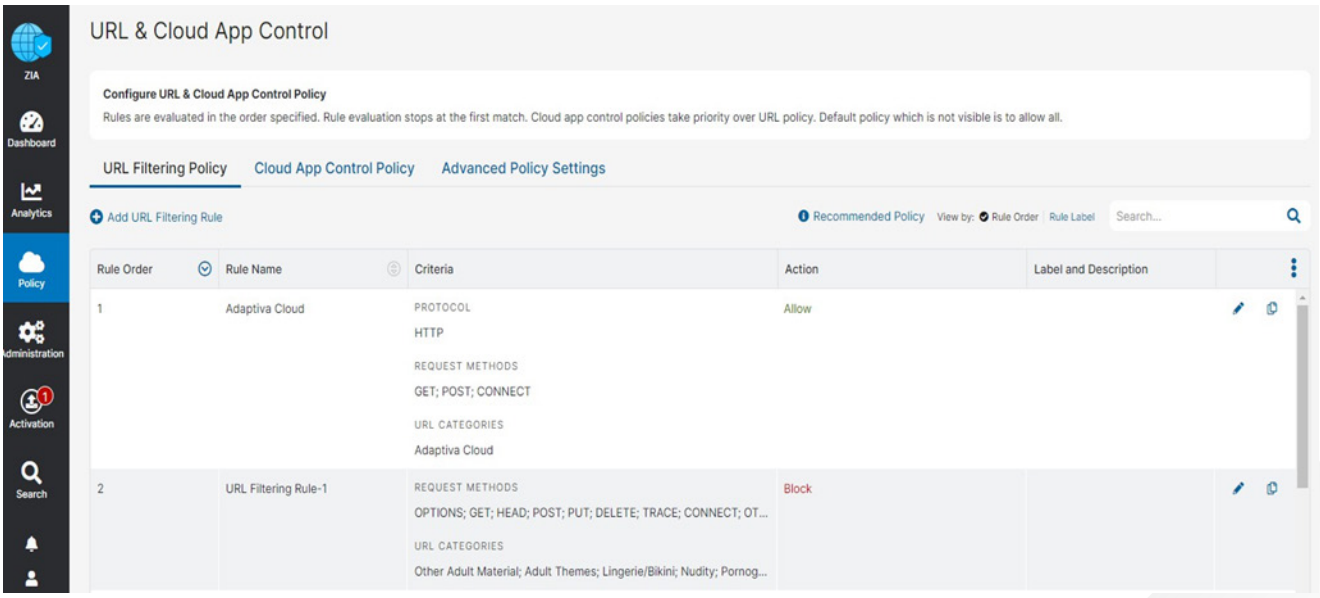


*Figure 8. Finished Adaptiva cloud policy*

 

## Configure Adaptiva CDN Policy

Next, repeat the steps for creating Adaptiva CDN Policy to allow downloads from CDN for client devices if using Zscaler. The server only needs it to validate CDN functionality from the Adaptiva Server.

To launch the Add URL Filtering Rule window:

1. Go to **Policy** > **URL & Cloud App Control**.
2. Click **Add URL Filtering Rule**. The **Add URL Filtering Rule** window appears.

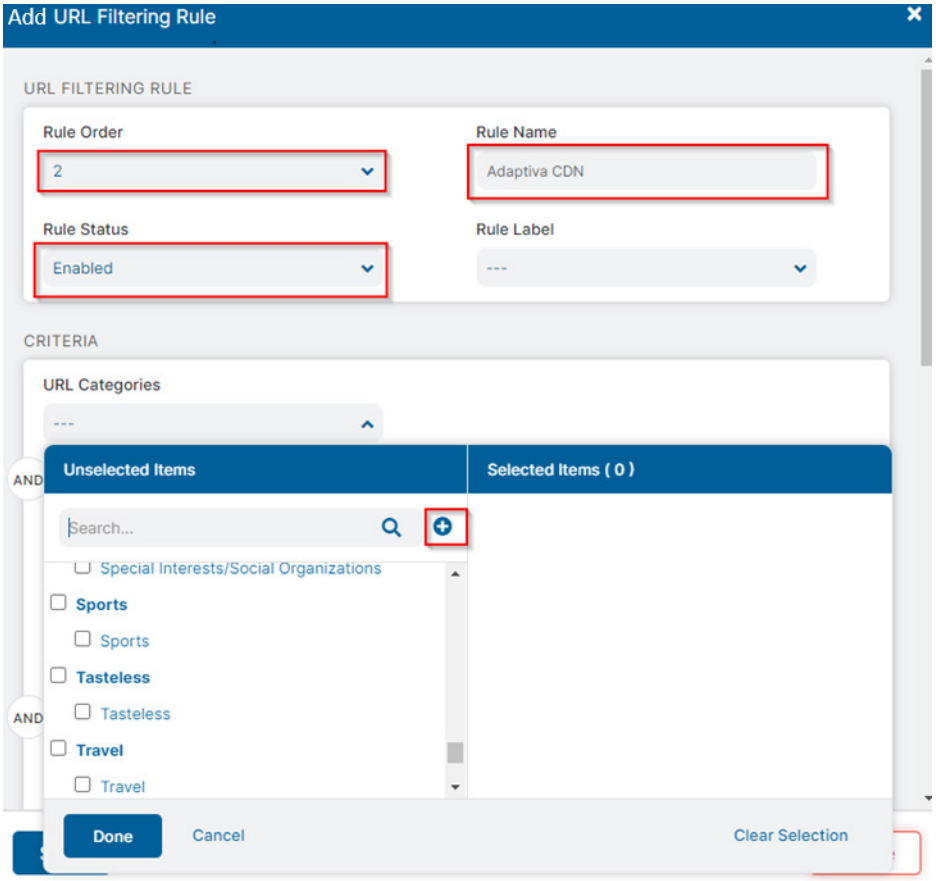


*Figure 9. Configure Adaptiva Cloud Policy*

In the Add URL Filtering Rule window, select the Rule Order based on your current policy processing and enable the rule under Rule Status. Then select the arrow in URL Categories and finally select the Add icon (blue +) on the URL Selection window to add in Adaptiva Cloud Category.

1. Select the **Rule Order** from the drop-down menu.
2. Enter a name in the **Rule Name** field (e.g., `Adaptiva Cloud`).
3. Select **Enable** from the **Rule Status** drop-down menu.
4. Select the drop-down menu in the **URL Categories** field (e.g., `Adaptiva Cloud`).
5. Select the **Add** icon (blue +) next to the **Search** field on the **URL Selection** window.

 

## Add Adaptiva CDN URL

To add the Adaptiva CDN URL:

1. Enter a **Name** (e.g., `Adaptiva CDN`).
2. Under **Custom URLs**, enter `.adaptivacdn.cloud`.
3. **(Optional) Description**: Enter the URL category for Adaptiva CDN.
4. Click **Save**.

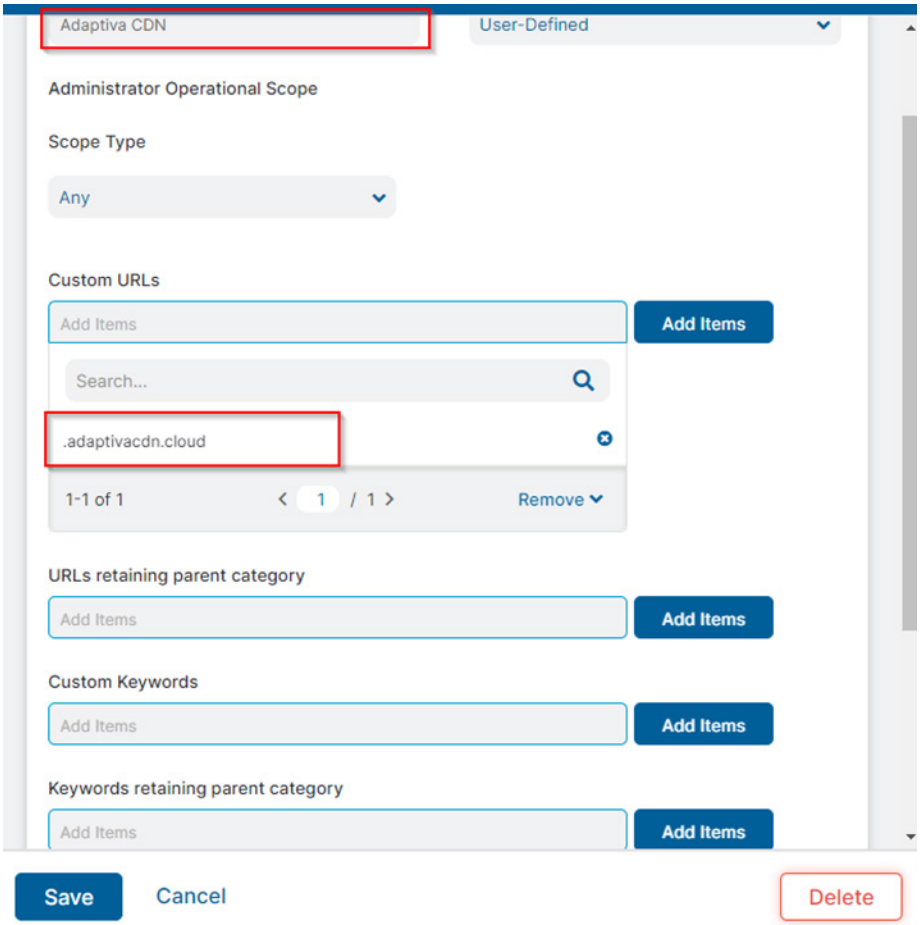


*Figure 10. Add Adaptiva CDN URL Category*

 

5. Scroll to fill in the remaining fields:
   a. For **Request Methods**, select **CONNECT**.
   b. For **Protocols**, select **HTTP Proxy**, and **SSL**.
   c. For **Web Traffic**, select **Allow**.
   d. Select **Save** to complete the configuration.

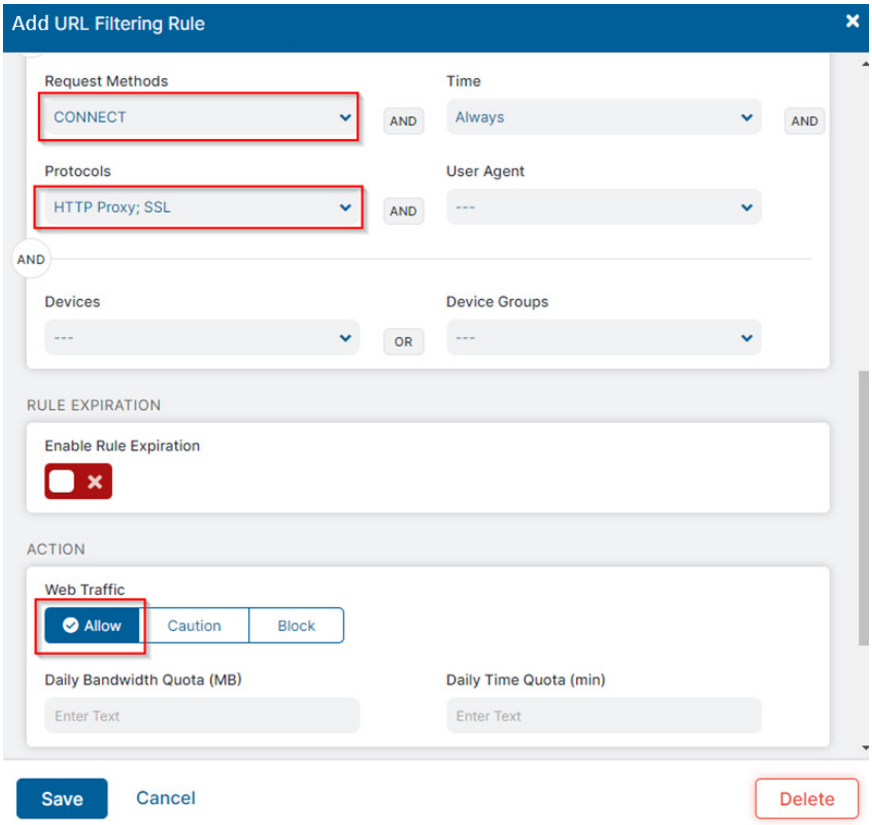


*Figure 11. Add URL Filtering Category*

The rule name appears in the URL & Cloud App Control page.

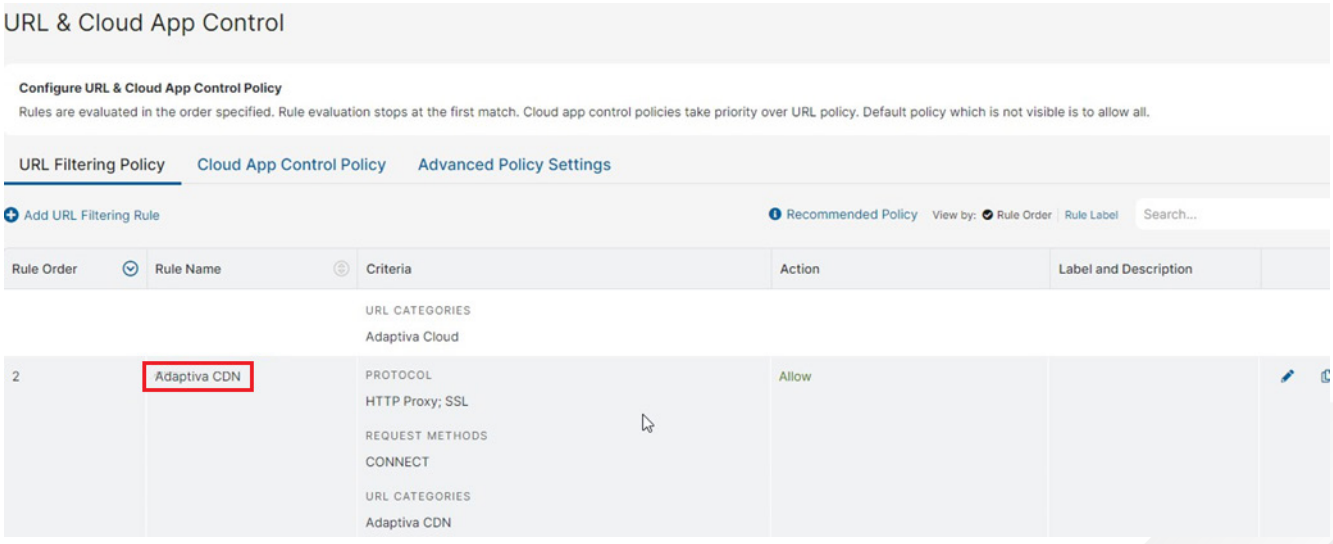


*Figure 12. Adaptiva CDN URL & Cloud App Control*

 

## Configure S3 Bucket Policy

If the Adaptiva Server is connected through Zscaler, then create an Adaptiva S3 Bucket Policy. Launch the URL Filtering wizard using the following steps (if Amazon AWS isn't allowed).

If Amazon AWS is allowed, the minimum configuration required for the server to access for the connection is Protocols HTTP, HTTP Proxy, HTTPS, SSL, Tunnel SSL, Request Methods of Connect, Delete, Get, Options, Put, and Post.

To configure an Adaptiva S3 Bucket Policy:

1. Go to **Policy** > **URL & Cloud App Control**.
2. Select **Add URL Filtering Rule**. The Add URL Filtering Rule window appears.

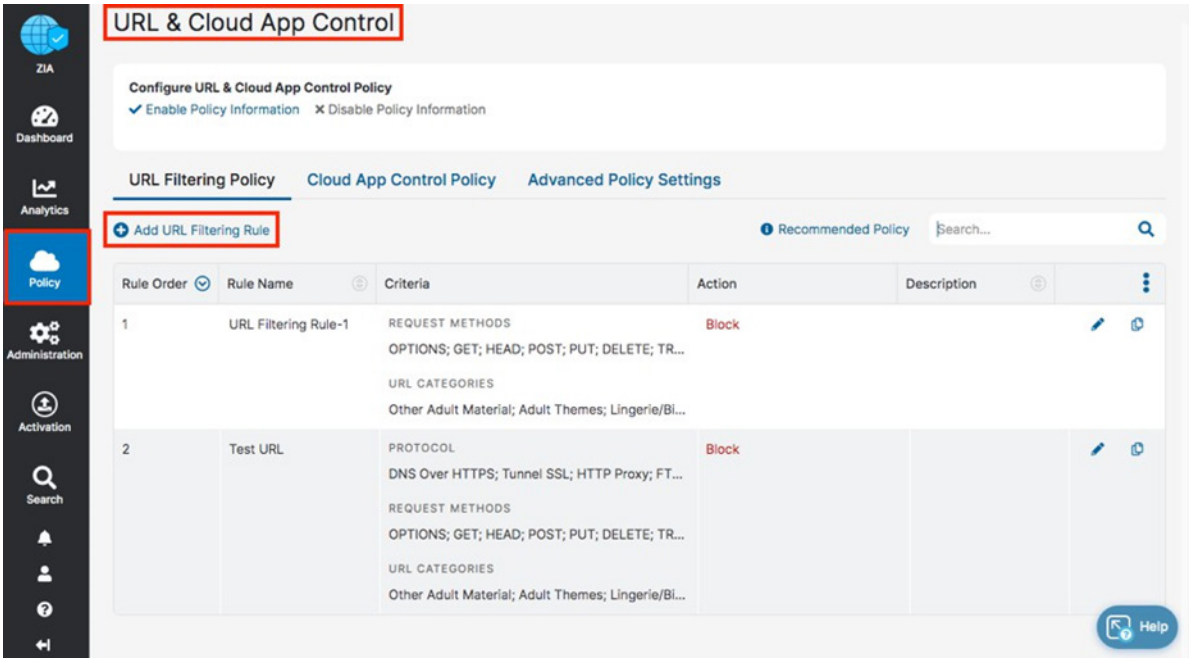


*Figure 13. Configure S3 Bucket Policy*

In the Add URL Filtering Rule window, select the Rule Order based on your current policy processing and enable the rule under Rule Status. Then select the arrow in URL Categories and finally select the Add icon (blue +) on the URL Selection window to add in Amazon AWS Category.

1. Select the **Rule Order** from the drop-down menu.
2. Enter a name in the **Rule Name** field (e.g., `Amazon AWS`).
3. Select **Enable** from the **Rule Status** drop-down menu.
4. Select the drop-down menu in the **URL Categories** field (e.g., `Amazon AWS`).

 

## Add Adaptiva S3 Bucket URL

To add Adaptiva S3 bucket URL:

1. Select the **Add** icon (blue +) sign next to the **Search** field on the **URL Selection** window.
2. Enter a **Name** (e.g., `Amazon AWS`).
3. Under **Custom URLs**, enter `.amazonaws.com`.
4. **(Optional) Description**: Enter the URL category for Amazon AWS.
5. Click **Save**.

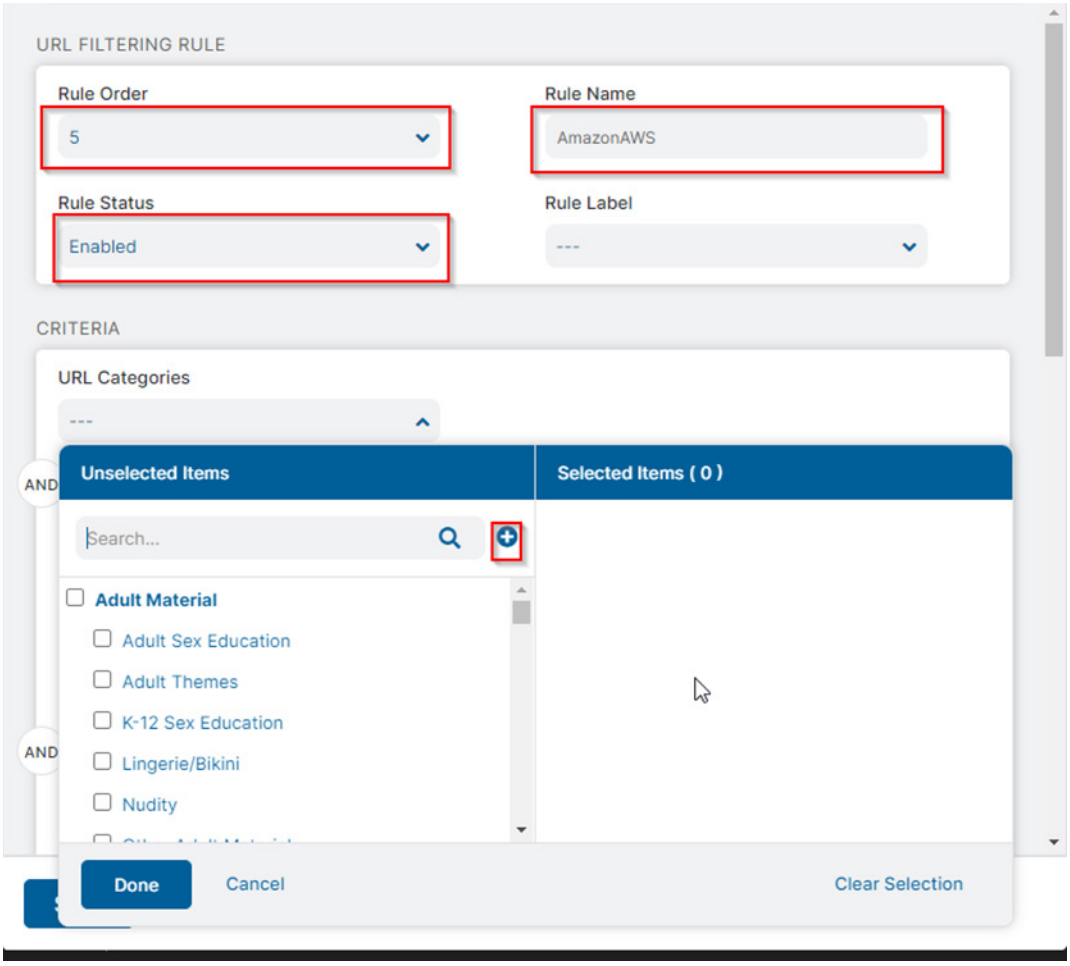


*Figure 14. Add Adaptiva S3 Bucket Category*

 

6. Scroll to fill in the remaining fields.
    a. For **Request Methods**, select **Connect**, **Delete**, **Get**, **Options**, **Put**, and **Post**.
    b. For **Protocols**, select **HTTP**, **HTTP Proxy**, **HTTPS**, **SSL**, and **Tunnel SSL**.
    c. For **Web Traffic**, select **Allow**.
    d. Select **Save** to complete the configuration.

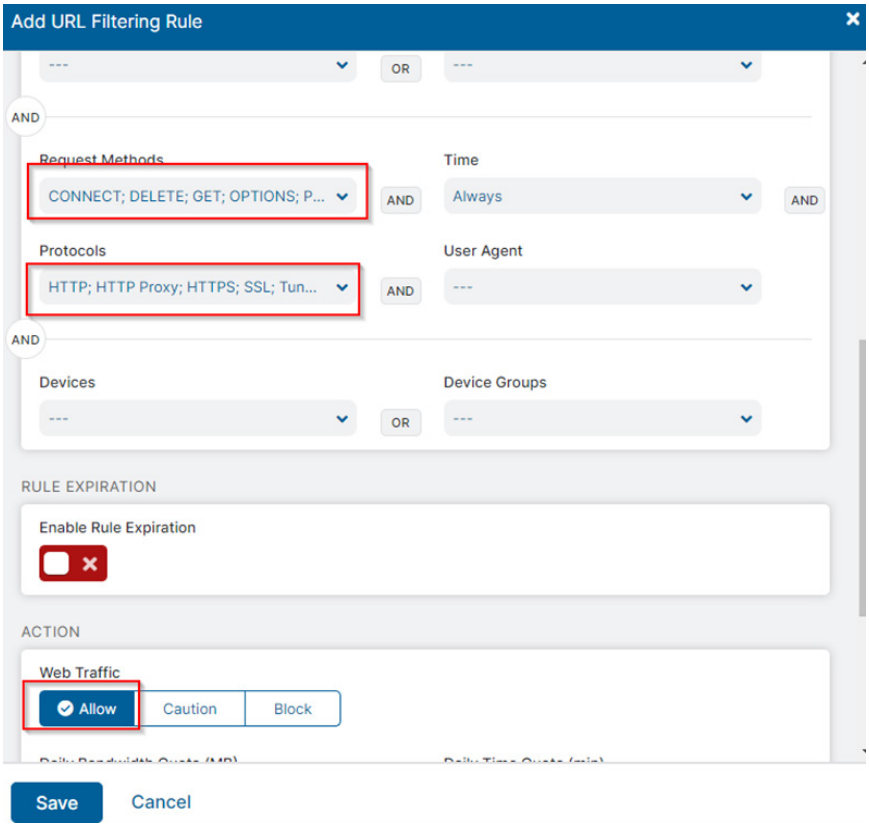


*Figure 15. Add Adaptiva S3 Bucket Category*

The Adaptiva S3 Bucket appears in the URL & Cloud App Control page.

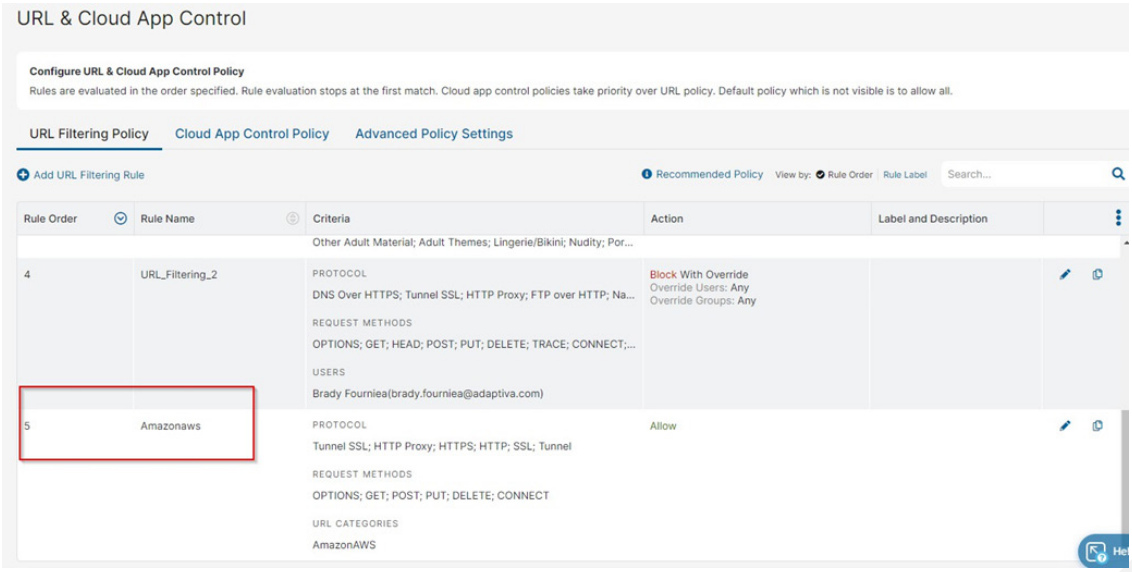


*Figure 16. Adaptiva S3 Bucket URL & Cloud App Control*

 

## Activate Policy Changes

Be sure to activate the new settings.

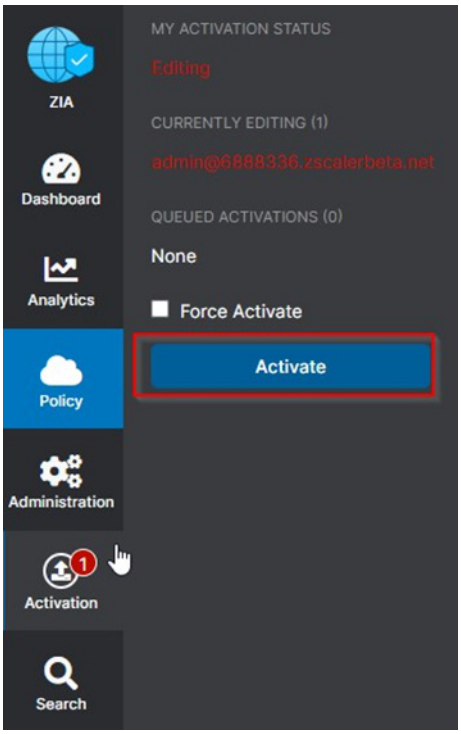


*Figure 17. Activate changes*

 

# Zscaler Client Configuration

Depending on the tunnel version in use, additional configuration is required.

From the ZIA Admin Portal, go to **Dashboard** > **Zscaler Client Connector Portal**.

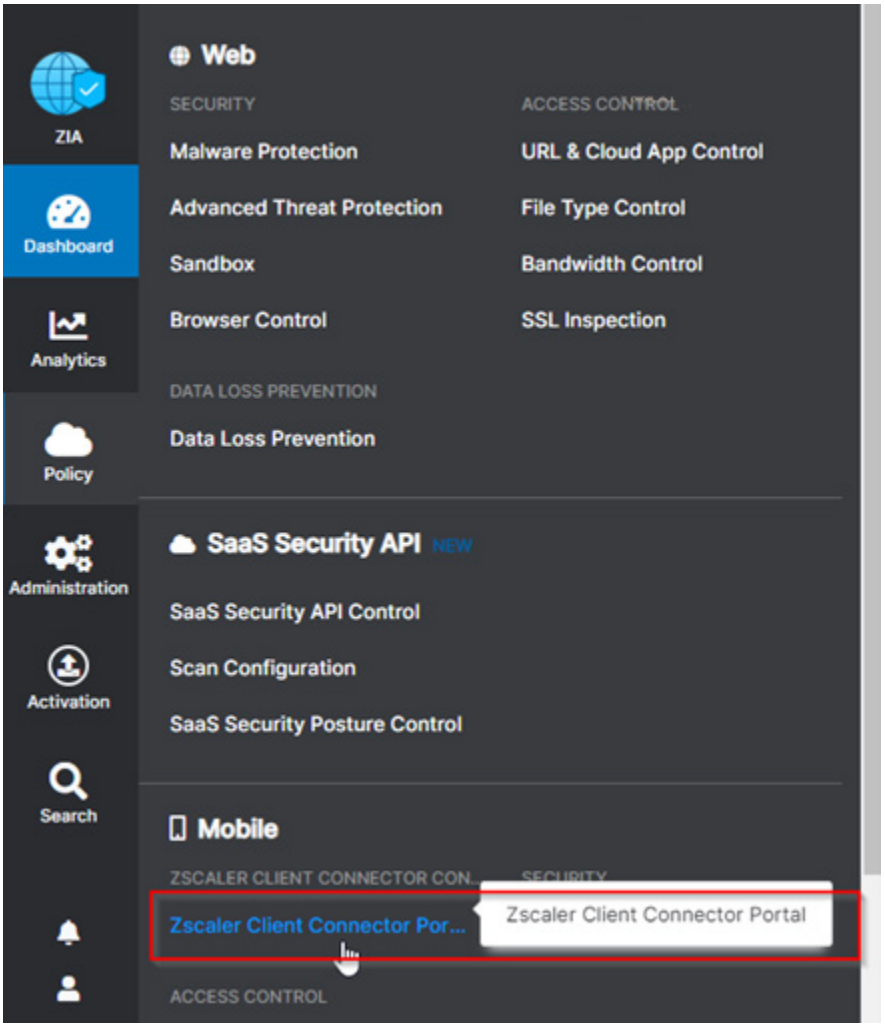


*Figure 18. Zscaler Client Connector Portal*

If the Forwarding Profile Tunnel version is set to Z-Tunnel 1.0, no additional settings are needed.

 

If the Forwarding Profile Tunnel version is set to Z-Tunnel 2.0, the following configuration edits are needed on the App Profile.

1. Click **App Profiles**.
2. Click **Add Windows Policy** if you are creating a new client connector policy. Otherwise, select and modify an existing policy.

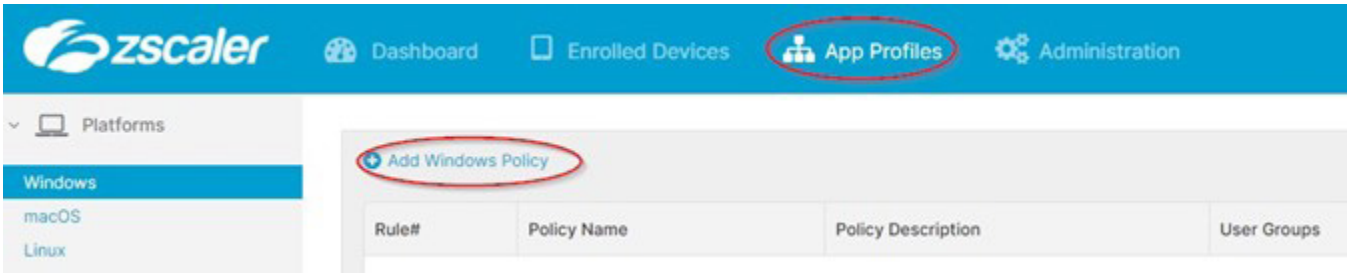


*Figure 19. Add Windows Policy*

3. Select the **Target Group** or users.
4. Select the **Forwarding Profile**.

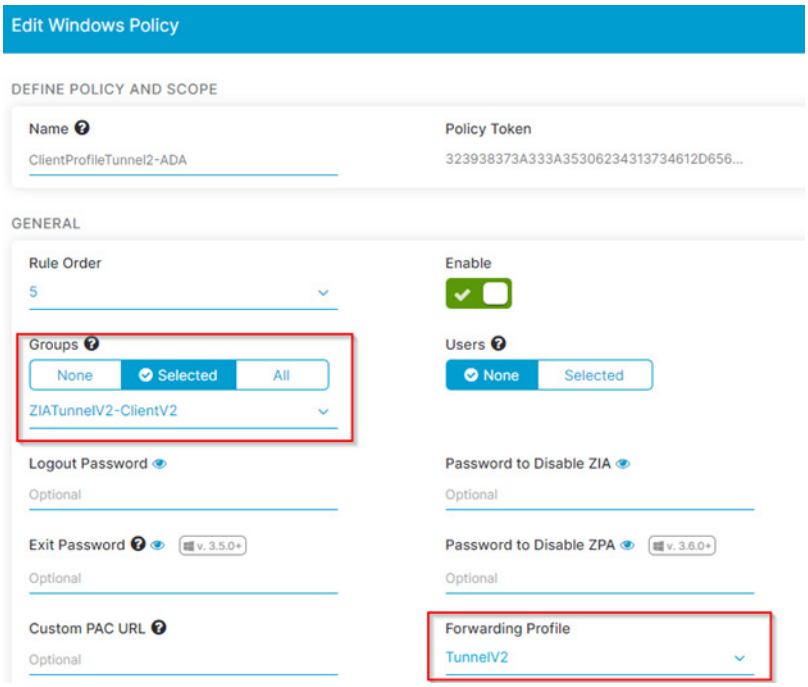


*Figure 20. Forwarding Profile*

 

5. Add in **Destination Exclusions** for Adaptiva Client internet peer-to-peer.

   ```
   23.92.176.216:3478:udp,64.46.111.34:3478:udp,74.201.204.182:3478:udp,63.25
   1.235.52:3478:udp,117.20.40.52:3478:udp,*:34546:udp,*:34750:udp
   ```

6. Click **Save**.

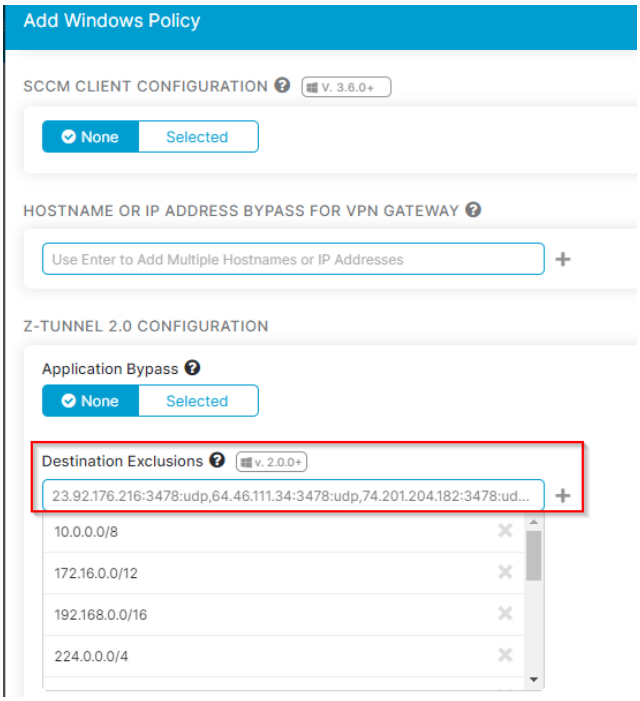


*Figure 21. Add Windows Policy*

## Adaptiva Client Setting

Additional proxy configuration might be needed for the Adaptiva client. This configuration can vary depending on the version of the Adaptiva version installed within the customer environment. To learn more, refer to the [Adaptiva documentation]. If the default client setting does not work, perform the following configuration.

1. Open the Adaptiva Web UI.
2. Select **Client Setting Policies** from the **Global Settings** menu.

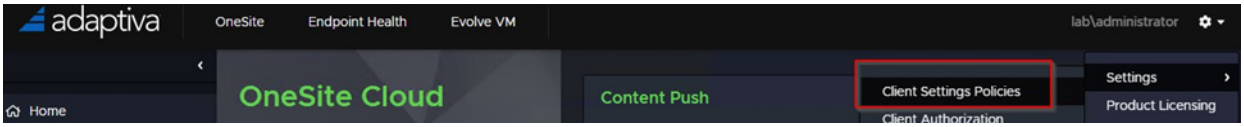


*Figure 22. Global Settings*

3. Select **New** to create a new client settings policy.

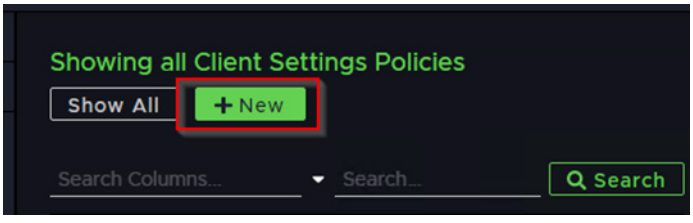


*Figure 23. New client settings policy*

 

4. Enter the **Name** of the client settings profile.
5. Set the **Priority** to `2` or higher.
6. Set the target group or SCCM collection to which this policy is applied.

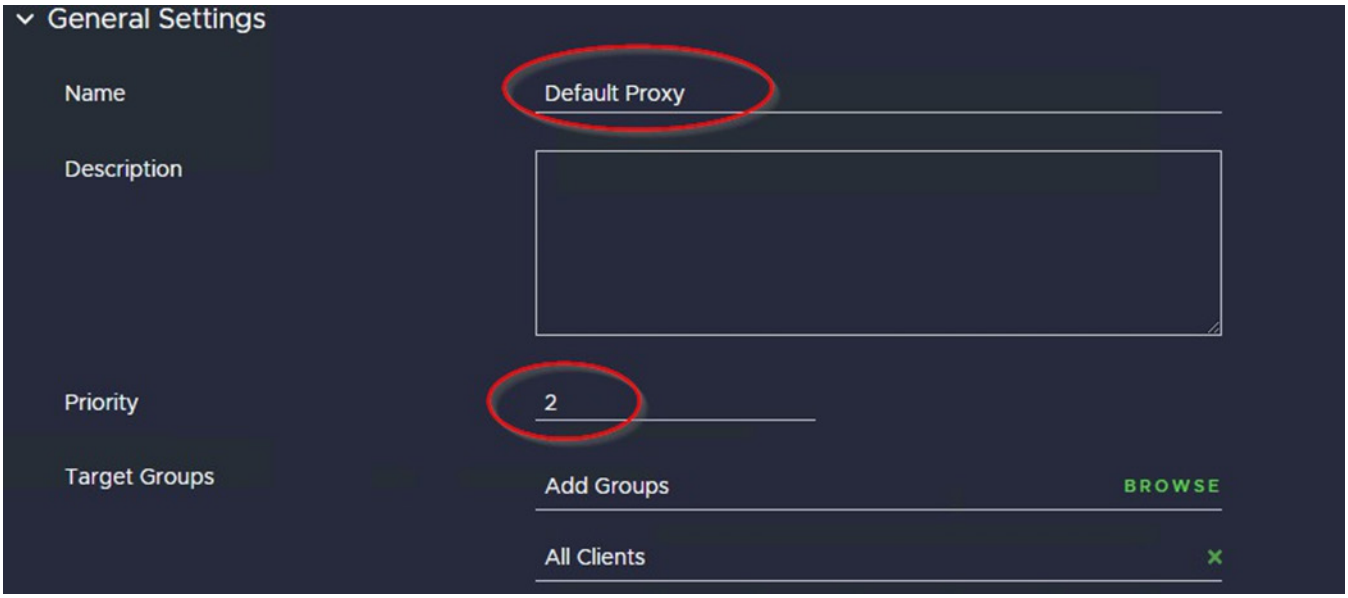


*Figure 24. Configure global settings*

7. Select **Add Settings**.

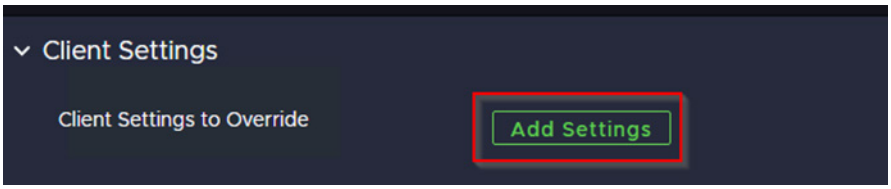


*Figure 25. Add Settings*

8. Enter `Proxy` in the search box.
9. Select **Custom Proxy Port**.
10. Select **Custom Proxy Server.**
11. Select **Prefer User Proxy**.

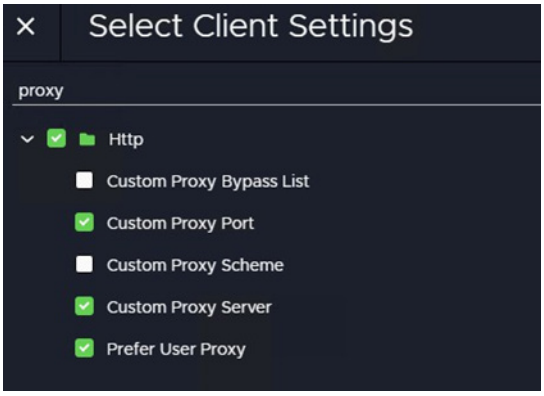


*Figure 26. Select Client Settings*

 

12. Enter `9000` for the **Custom Proxy Port**.
13. Enter `127.0.0.1` for the **Custom Proxy Server**.
14. Enter `False` for the **Prefer User Proxy**.
15. 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**.

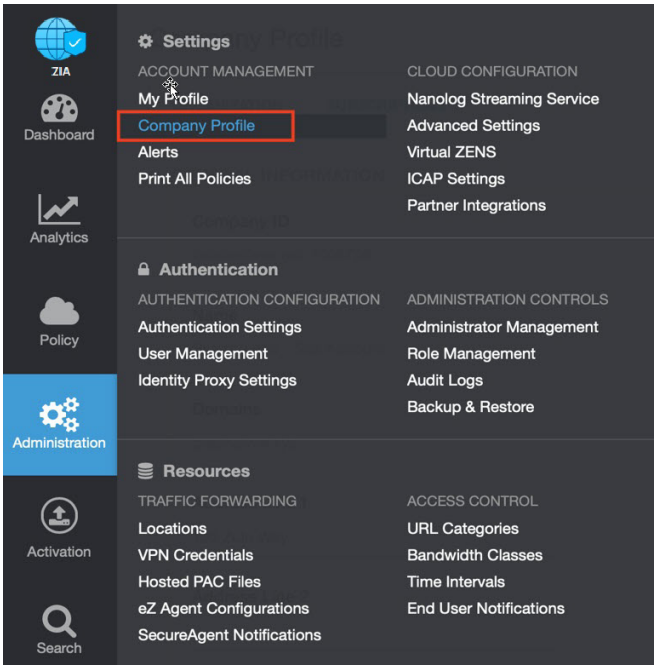


*Figure 27. Collecting details to open support case with Zscaler TAC*

2. Copy your **Company ID**.

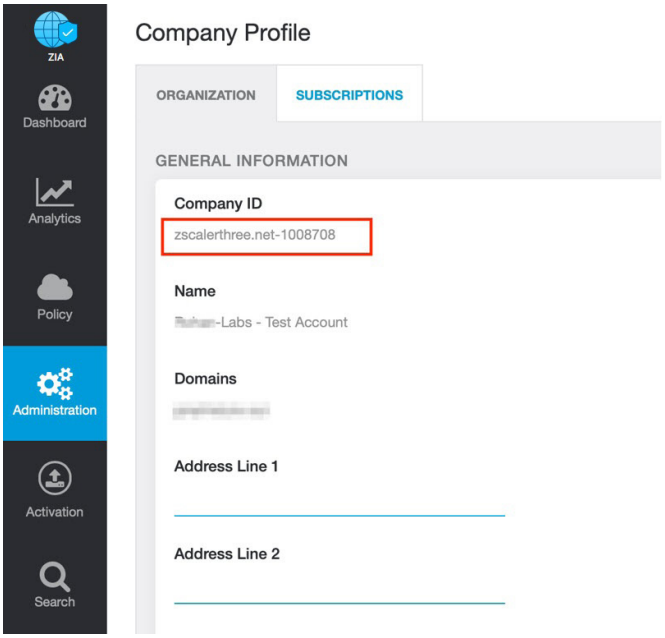


*Figure 28. Company ID*

 

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

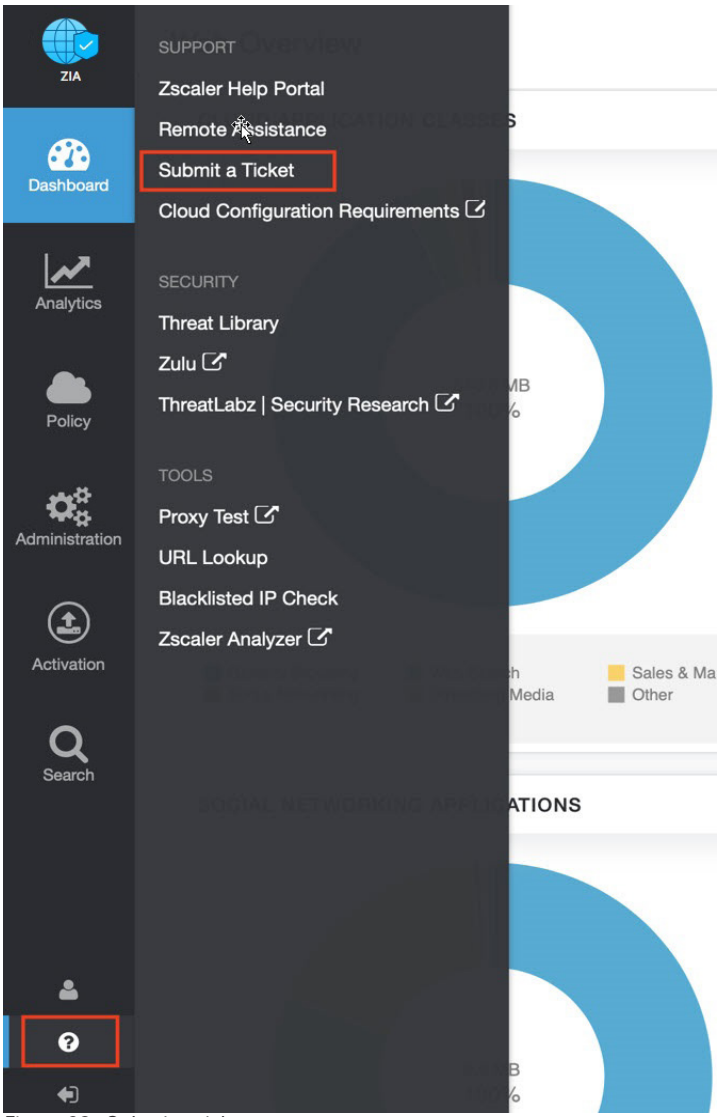


*Figure 29. Submit a ticket*

 