ZSCALER AND AMAZON Q GENERATIVE AI DATA PROTECTION DEPLOYMENT GUIDE

JUNE 2024, VERSION 1.0

BUSINESS DEVELOPMENT GUIDE

Contents

©2024 Zscaler, Inc. All rights reserved.

©2024 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)
NAT	Network Address Translation
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SaaS	Software as a Service
SIPA	Source IP Anchoring
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
VPC	Virtual Private Cloud
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)

©2024 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. To learn more, see Zscaler's website or follow Zscaler on Twitter @zscaler.

Generative AI Data Protection Overview

This document provides technical implementation guidance to deploy both ZIA and ZPA (for protection of privately deployed AI solutions) to enable data protection on AI platforms for AWS Generative AI solutions. While these techniques are outlined for Amazon Q, you can deploy the DLP inspection techniques to protect other Generative AI solutions such as Amazon bedrock custom applications. Note that Amazon Q allows scanning of documents by web crawling documents stored on Amazon S3 buckets. This document specifically describes how to protect these data repositories with the Zscaler Zero Trust Exchange.

It's important for organizations to implement AI DLP solutions in conjunction with well-defined data protection policies and practices to create a robust defense against data breaches and ensure regulatory compliance. Additionally, user awareness and education play a crucial role in the overall success of a DLP program.

AWS Overview

Amazon Web Services (AWS) (NASDAQ: AMZN) is the world's most comprehensive and broadly adopted cloud platform, offering over 200 fully featured services from data centers globally. Millions of customers—including the fastest-growing startups, largest enterprises, and leading government agencies—are using AWS to lower costs, become more agile, and innovate faster. For more information, refer to Amazon'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
- AWS Resources
- Appendix B: Requesting Zscaler Support

Software Versions

This document was authored using the latest version of Zscaler software.

©2024 Zscaler, Inc. All rights reserved.

Prerequisites

Public AI Data Protection:

- Zscaler Internet Access with data protection enabled.
- SSL TLS Inspection enabled for AI web categories.
- Optional Zscaler Client Connector version 4.2 or later to support End User Notifications for Zscaler Client Connector.

Private (Internal) AI Data Protection:

- Installed Zscaler Application Connector.
- Source IP Anchoring (SIPA) license is required for ZIA.
- Advanced Cloud Firewall (ACFW) license is required for non-HTTP/HTTPS SIPA.
- You must link the ZIA tenant to a ZPA tenant.
- Zscaler Private Access with an Application Connector deployed into a private network supporting an AI solution.
- Have an Application Connector Group for SIPA traffic.
- HTTP/HTTPS SIPA traffic: Zscaler Client Connector with Z-Tunnel 1.0/2.0, Tunnel with Local Proxy (TWLP), or PAC-based access.
- Non-HTTP/HTTPS SIPA traffic: Zscaler Client Connector with Z-Tunnel 2.0 or Z-Tunnel 1.0/TWLP/PAC file with GRE/IPSec tunnel.
- Non-HTTP/HTTPS SIPA: ZIA must intercept the DNS resolution from the client.
- Advanced Cloud Firewall (ACFW) license is required for non- HTTP/HTTPS SIPA.
- Optional Zscaler Digital Experience (ZDX).

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.

©2024 Zscaler, Inc. All rights reserved.

Zscaler and Amazon Q Generative AI Introduction

Overviews of the Zscaler 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.

©2024 Zscaler, Inc. All rights reserved.

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.

Amazon Q Overview

Amazon Q Business is a generative AI–powered assistant that can answer questions, provide summaries, generate content, and securely complete tasks based on data and information in your enterprise systems. It empowers employees to be more creative, data-driven, efficient, prepared, and productive. It allows end users to receive immediate, permissions-aware responses from enterprise data sources with citations, for use cases such as IT, HR, and benefits help desks.

Amazon Q supports creating its data set by using connectors to attach to Amazon S3 buckets and many other supported data stores. This document covers how to protect these data stores and the Amazon Q web crawler used to populate its data sets.

Amazon Bedrock Overview

Amazon Bedrock is a fully managed service that makes high-performing foundation models (FMs) from leading AI startups and Amazon available for your use through a unified API. You can choose from a wide range of foundation models to find the model that is best suited for your use case. Amazon Bedrock also offers a broad set of capabilities to build generative AI applications with security, privacy, and responsible AI. Using Amazon Bedrock, you can easily experiment with and evaluate top FMs for your use cases, privately customize them with your data using techniques such as fine-tuning and Retrieval Augmented Generation (RAG), and build agents that execute tasks using your enterprise systems and data sources.

While this deployment guide specifically focuses on Amazon Q, you can use these same techniques to protect Amazon Bedrock applications.

AWS Resources

The following table contains links to AWS support resources.

Name	Definition
Amazon Q Getting Started	Getting started guide for Amazon Q
Set Up Amazon Bedrock	Online documentation for setting up Amazon Bedrock.
AWS Support	File a Support ticket with AWS.

©2024 Zscaler, Inc. All rights reserved.

Integration Architecture

This guide covers the areas for protecting the data ingested by Amazon Q to respond to user prompts.

The two main sections required to enable protection of the Amazon Q data are:

- Enable Zscaler Cloud Connectors so that all data that Amazon Q consumes are inspected by the Zscaler Zero Trust Exchange.
- Enable the Zscaler CASB out-of-band Amazon S3 bucket scanner.

To set up Amazon Q, refer to the **Amazon Q documentation**.

Typically, you have several sources for Amazon Q to populate the Amazon Q database. To protect these sources, you deploy cloud connectors in a virtual private cloud (VPC), and then have Amazon Q egress through that VPC. All traffic that Amazon Q collects is scanned for malware as well as DLP violations.

The following is an example of data sources that an Amazon Q solution might use::

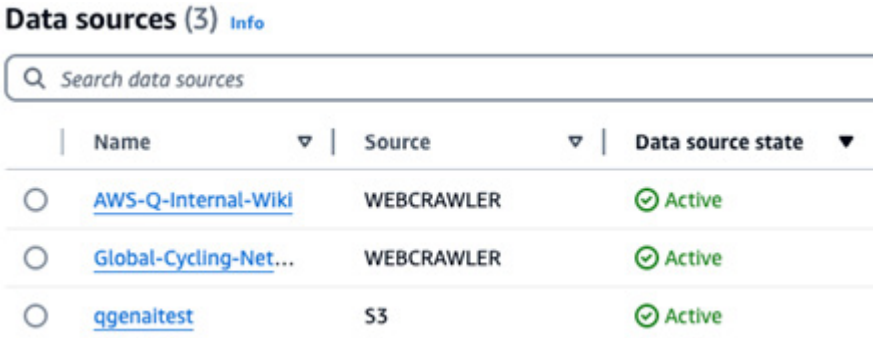

Figure 1. Data sources

You must ensure the web crawler sites go through a VPC that egresses through a cloud connector:

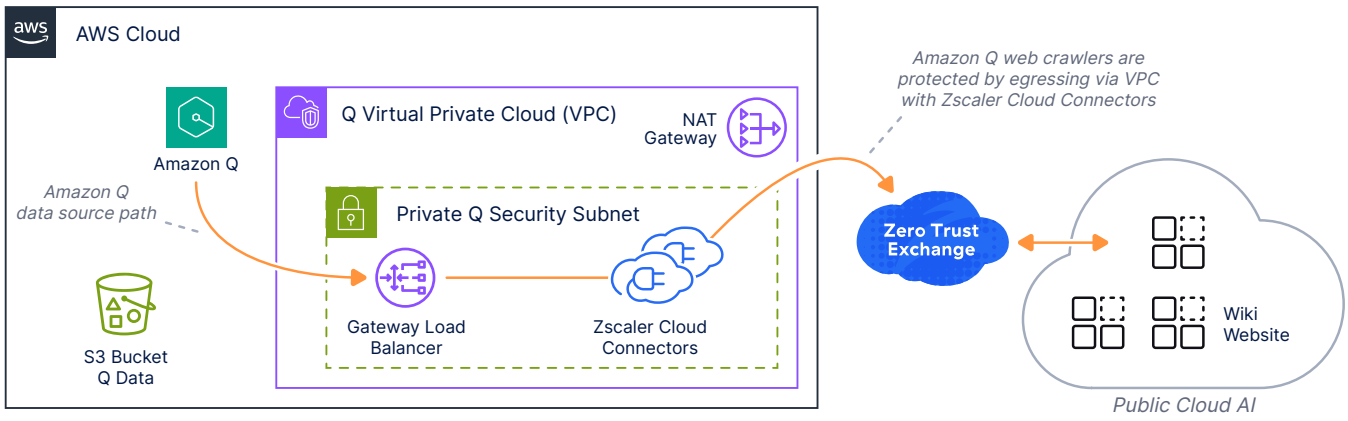

Figure 2. Zscaler and Amazon Q architecture

Set up a VPC with a configured cloud connector that directs the Amazon Q web crawler to the data source. By setting up a Zscaler cloud connector in a VPC, directing traffic to the VPC ensures that all traffic flows through the Zscaler Zero Trust Exchange. This guarantees all traffic that is collected is free from malware and prevents the loss of company confidential information.

©2024 Zscaler, Inc. All rights reserved.

You must set up a VPC with a configured cloud connector that points the Amazon Q web crawler to a data source. To learn more, see Deploying a Zscaler Cloud Connector for Amazon Web Services (government agencies, see Deploying a Zscaler Cloud Connector for Amazon Web Services).

After you have a VPC set up with Zscaler Cloud Connector, the following process shows how to enable Amazon Q for business web crawlers to traverse through your VPC.

1. In the AWS Console under **Amazon Q for Business**, click **Add data source**.

Figure 3. Add data source

2. Select **Web crawler**.

Figure 4. Web crawler

3. Provide the source URLs from where you want to collect data, and then click **Configure VPC and security group**.

Figure 5. Configure VPC and security group

4. Select the VPC you configured with your Cloud Connectors.
5. Select the subnet that is configured to forward traffic to the Cloud Connectors. This allows the Amazon Q web crawler to egress out through the cloud connectors.
6. Select the security group you configured to allow traffic to flow from the Amazon Q web crawler out to the sites from which you want to collect data.

After you configure the web crawler to scan regularly, you see traffic from the user associated with your cloud connector instance. It might have a default name such as **east-1-vpc-01faf2c78bdbd9cbc**.

©2024 Zscaler, Inc. All rights reserved.

Enabling Zscaler Malware and DLP scanning of Amazon S3 Buckets

To learn more about setting up Amazon S3 bucket scanning, see SaaS Security API Deployment and Operations Guide (government agencies, see SaaS Security API Deployment and Operations Guide).

For example, you must scan Amazon Q dataset stored in the Amazon S3 bucket, which is configured in the Amazon Q data sources. The following setup enables the Zscaler Zero Trust Exchange to scan and ensure there are no DLP violations or malware stored on the Amazon S3 bucket.

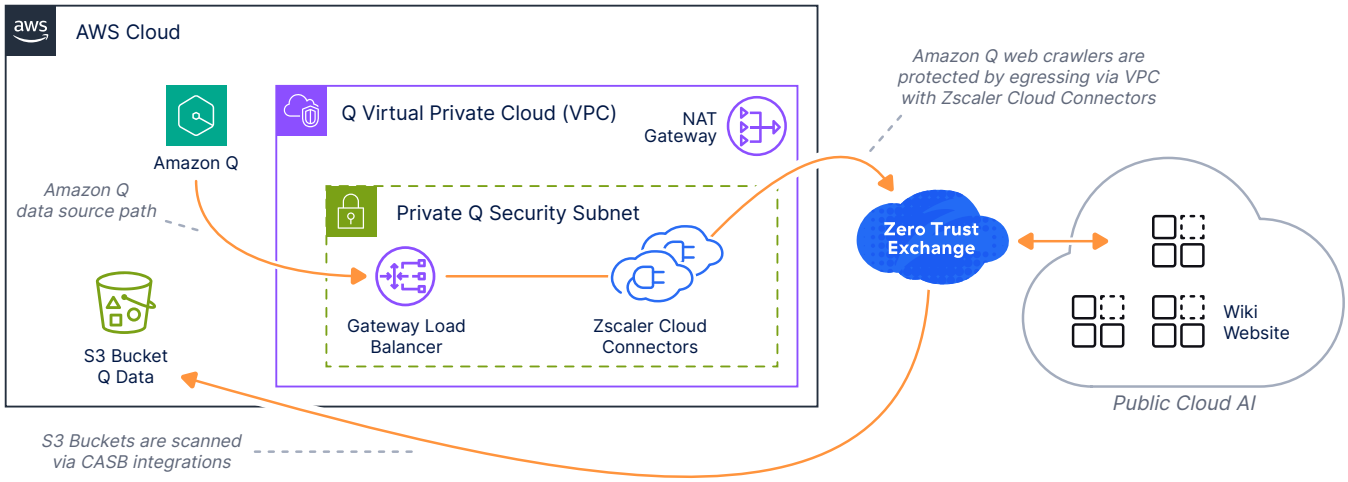

Figure 6. Zscaler and Amazon S3 architecture

To configure your Zscaler Tenant to scan the Amazon S3 bucket:

1. In the ZIA Admin Portal, go to **Administration** > **Cloud Configuration** > **SaaS Application Tenants**.

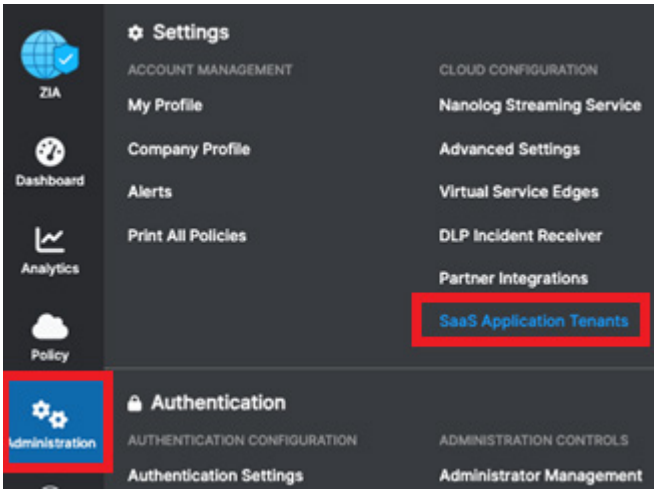

Figure 7. SaaS Application Tenants

©2024 Zscaler, Inc. All rights reserved.

2. Click **Add SaaS Application Tenant** and then click the Amazon S3 bucket.

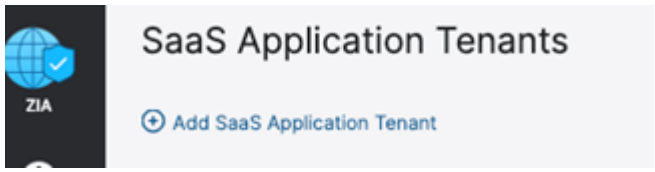

Figure 8. Add SaaS Application Tenant

Configure the tenant to match the fields shown in the following image (with your information). To learn more about configuring the IAM roles, see Zscaler Adding Application Tenants Help (government agencies, see Zscaler Adding Application Tenants Help).

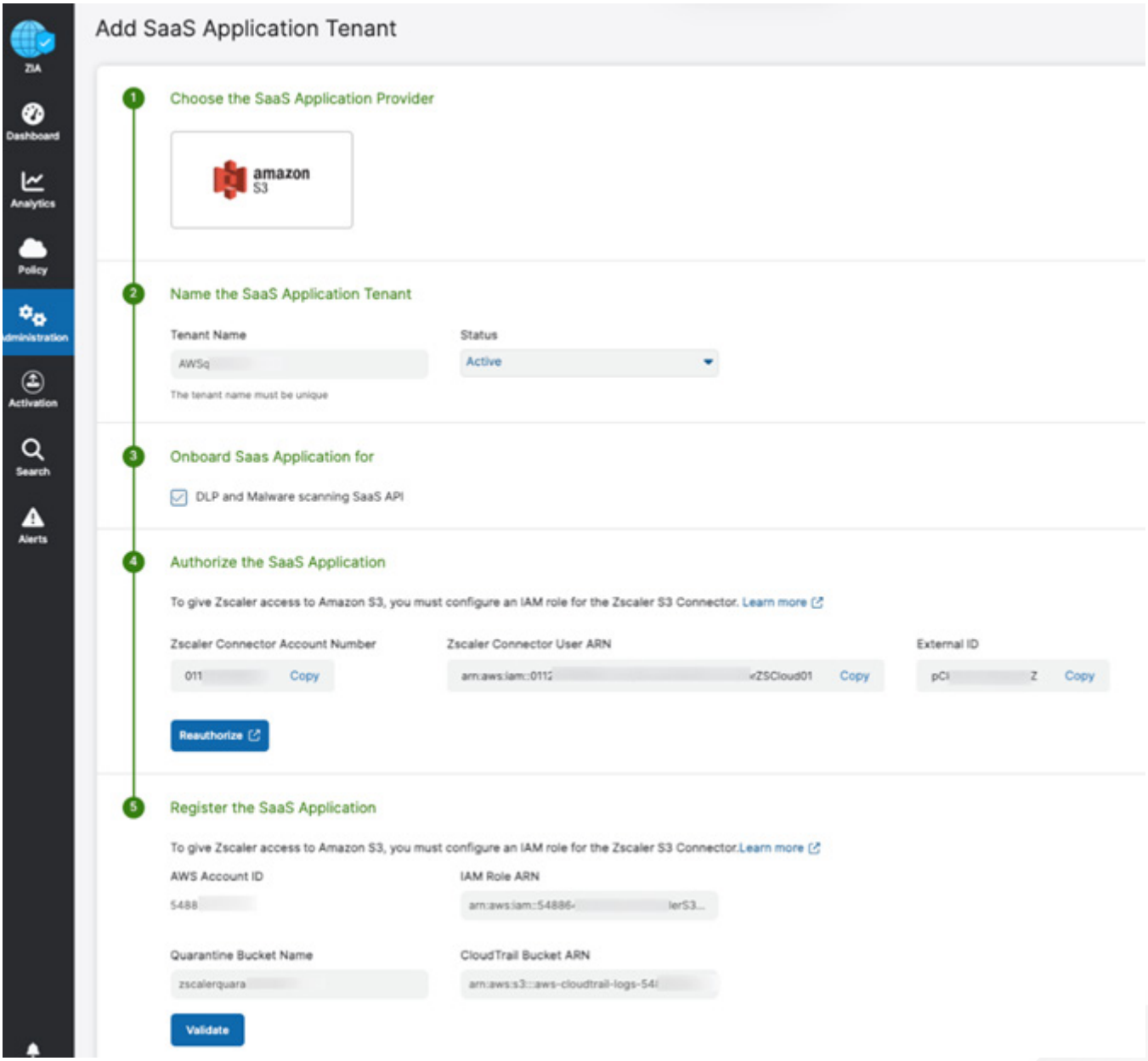

Figure 9. Add SaaS Application Tenant

©2024 Zscaler, Inc. All rights reserved.

Configure Zscaler Policy Scans

After authorizing the SaaS Application Tenant for Amazon S3, configure the scans in your Zscaler policy:

1. In the ZIA Admin Portal, go to the **Policy** > **SaaS Security API** > **SaaS Security API Control**.

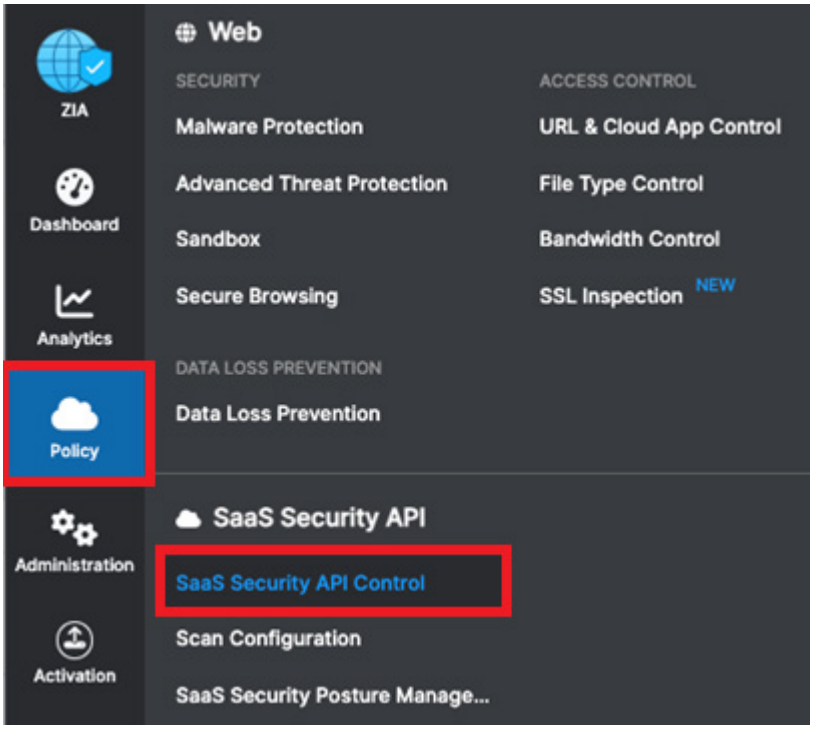

Figure 10. SaaS Security API Control

©2024 Zscaler, Inc. All rights reserved.

2. Click **Add DLP Rule** and configure the settings to match the fields shown in the following image. After you have enabled the DLP rule, set up scans.

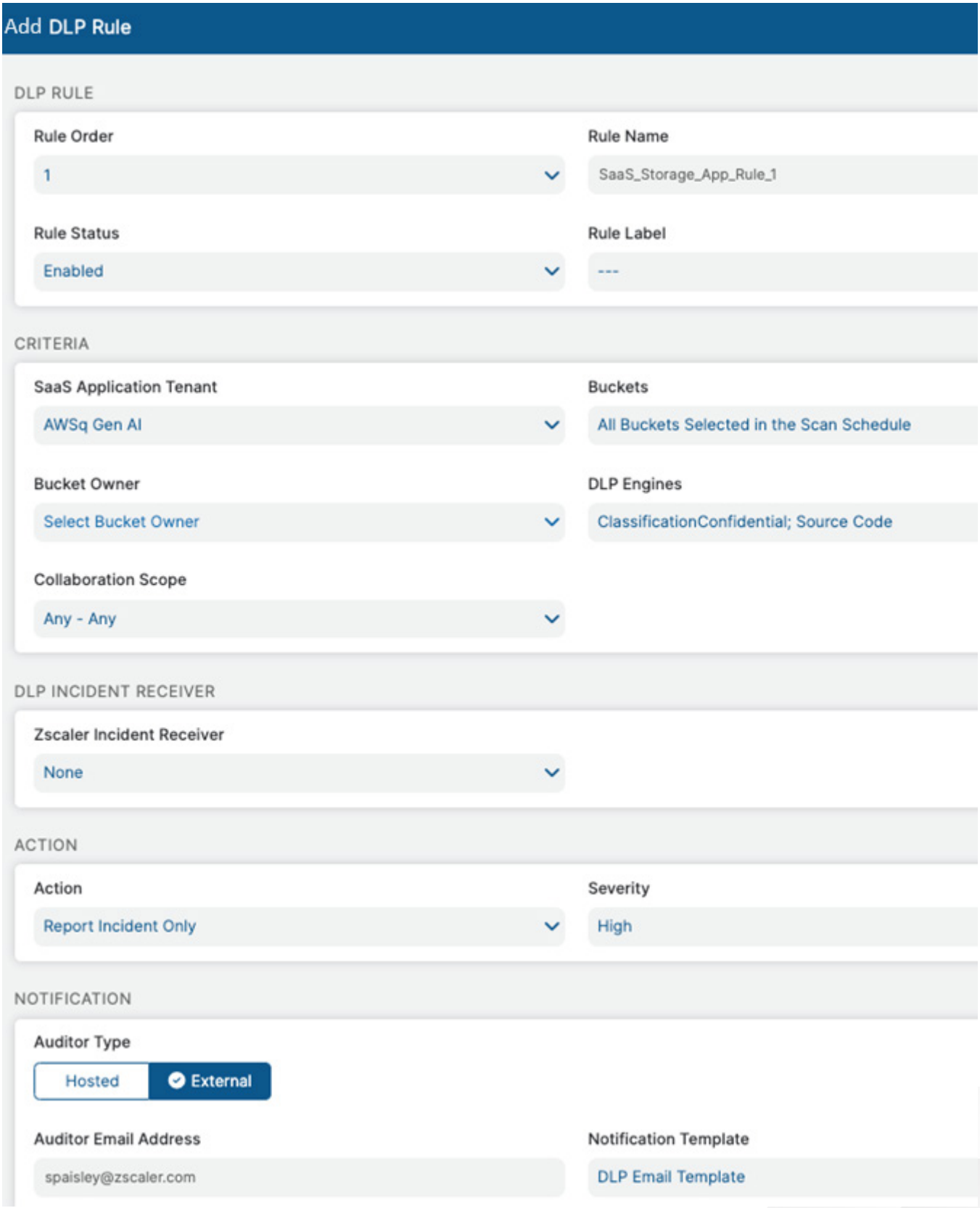

Figure 11. Add DLP Rule

©2024 Zscaler, Inc. All rights reserved.

3. Go to **Policy** > **SaaS Security API** > **Scan Configuration**.

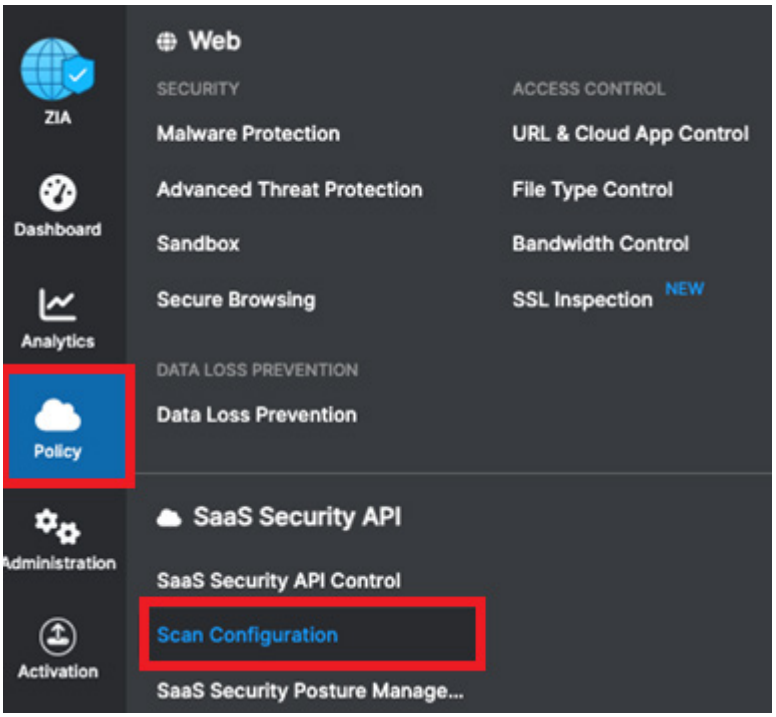

Figure 12. Scan Configuration

4. Select the Amazon S3 bucket that is configured as the Amazon Q Business Data Source.

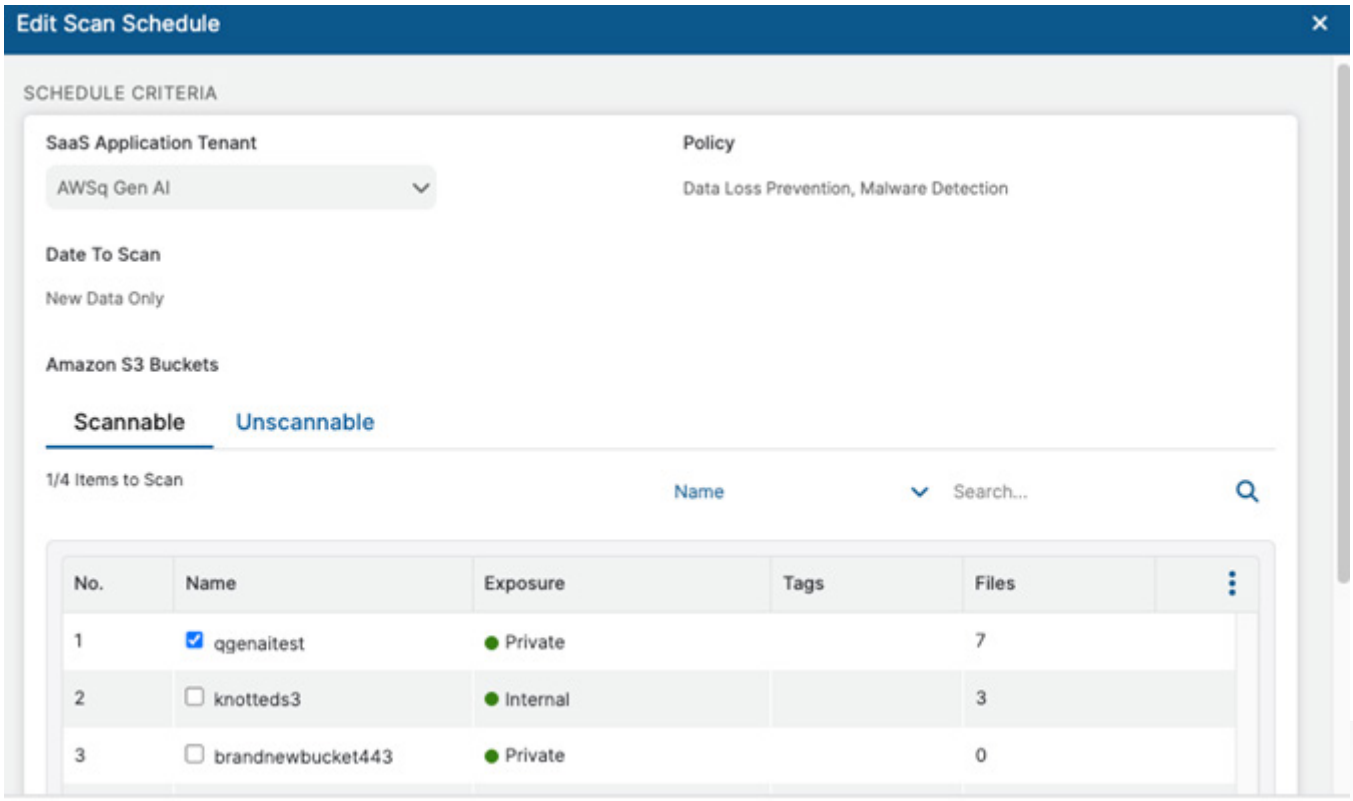

Figure 13. Edit Scan Schedule

5. Click **Save** and **Activate** your policy. Amazon Q business data sources are now protected.

©2024 Zscaler, Inc. All rights reserved.

The DLP policies in the Zero Trust Exchange provide a method to both protect the Generative AI solutions such as Amazon Bedrock and Amazon Q, and also ensure that end users are only allowed sanctioned AI tools.

The following diagram shows end users and corporate users added. All the work to develop DLP and Security policies are immediately implemented on the organization. You can also ensure users do not access public AI websites by blocking attempts, and then redirecting them to sanctioned corporate assets.

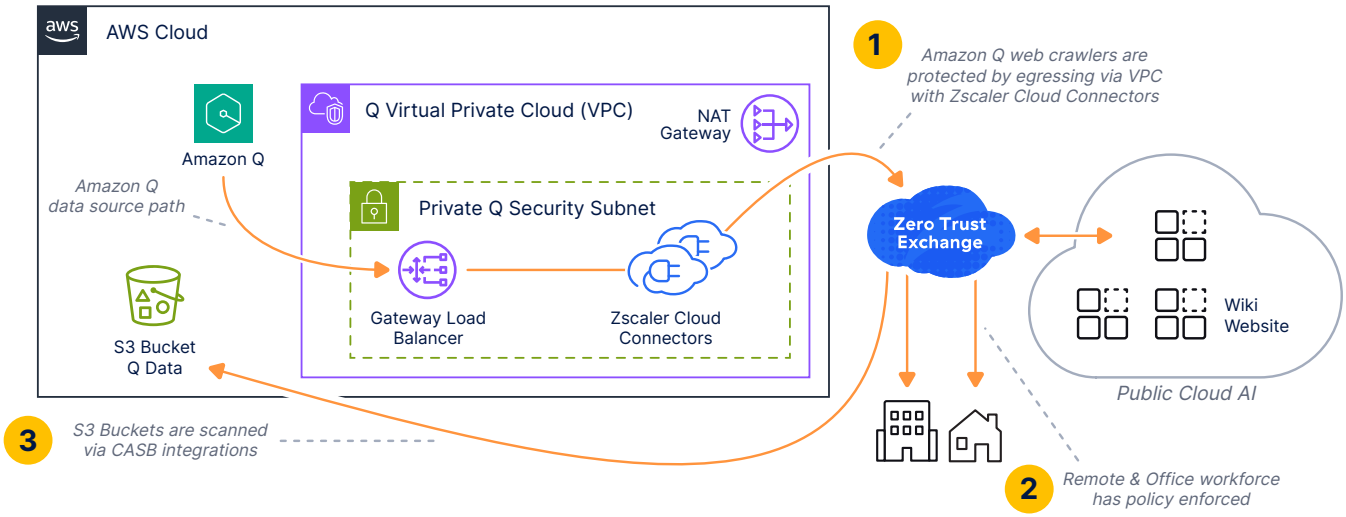

Figure 14. Implemented policies for end users and corporate users

©2024 Zscaler, Inc. All rights reserved.

Zscaler Data Protection Overview

You can use the Zscaler DLP engines to detect data, allow or block transactions, and notify your organization's auditor when a user's transaction triggers a DLP rule. If your organization has a third-party DLP solution, Zscaler can forward information about transactions that trigger DLP policy to your third-party solution via secure Internet Content Adaptation Protocol (ICAP). However, Zscaler does not take ICAP responses from your DLP solution. Zscaler only monitors or blocks content according to the policy you configure, then forwards information about transactions so that your organization can take necessary remediation steps.

By default, the Zscaler service evaluates inline DLP policy rules according to rule order, with evaluation stopping at the first match. However, if Evaluate All Rules mode is enabled for your organization, you can instead have the Zscaler service evaluate all rules, enforcing the rule with the most restrictive action.

You must first delete all existing inline DLP rules before you change the way the Zscaler service evaluates rules. To learn more, see **Configuring DLP Policy Rules with Evaluate All Rules Mode Enabled** (government agencies, **Configuring DLP Policy Rules with Evaluate All Rules Mode Enabled**).

Configure a DLP Policy for Private and Public AI Data Protection

The following sections describe configuring DLP policies for private and public AI data protection.

DLP with Content Inspection

AI DLP with content inspection can use predefined dictionaries, custom dictionaries, or exact data match algorithms to detect specific kinds of information in your users' traffic and activities to AI sites. The Zscaler service provides predefined dictionaries that you can modify and, in some cases, clone. You can also create custom dictionaries for content not covered by predefined dictionaries.

©2024 Zscaler, Inc. All rights reserved.

Configure DLP Dictionaries

Use DLP dictionaries and engines as defined, or modify them to suit your needs. You can also create custom dictionaries or engines. Skip this procedure if you don't want to modify or create custom DLP dictionaries and engines for AI Data Protection.

To add a custom DLP dictionary.

1. Go to **Administration** > **DLP Dictionaries & Engines**.
2. Click **Add DLP Dictionary**.
3. In the **Add DLP Dictionary** window:
   a. **Name**: Enter a name for the dictionary.
   b. **Dictionary Type**: Select a type from the drop-down menu.
      - **Patterns & Phrases**: If selected, the Patterns & Phrases sections appear, where you can add patterns, phrases, and apply actions to them. To learn more, see Defining Patterns for Custom DLP Dictionaries and Defining Phrases for Custom DLP Dictionaries (government agencies, see Defining Patterns for Custom DLP Dictionaries and Defining Phrases for Custom DLP Dictionaries)

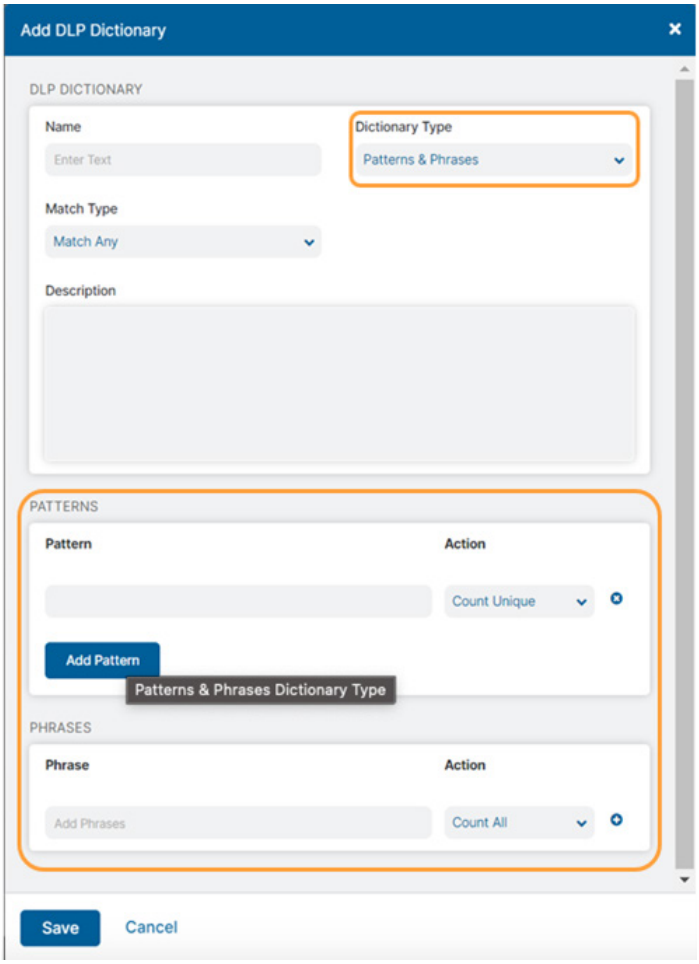

Figure 15. Add DLP Dictionary Patterns & Phrases

©2024 Zscaler, Inc. All rights reserved.

- **Microsoft Information Protection (MIP)**: If selected, the MIP labels appear in the following table, where you can select the MIP labels. To learn more, see Adding an MIP Account and Defining Microsoft Information Protection Labels for Custom DLP Dictionaries (government agencies, see Adding an MIP Account and Defining Microsoft Information Protection Labels for Custom DLP Dictionaries).

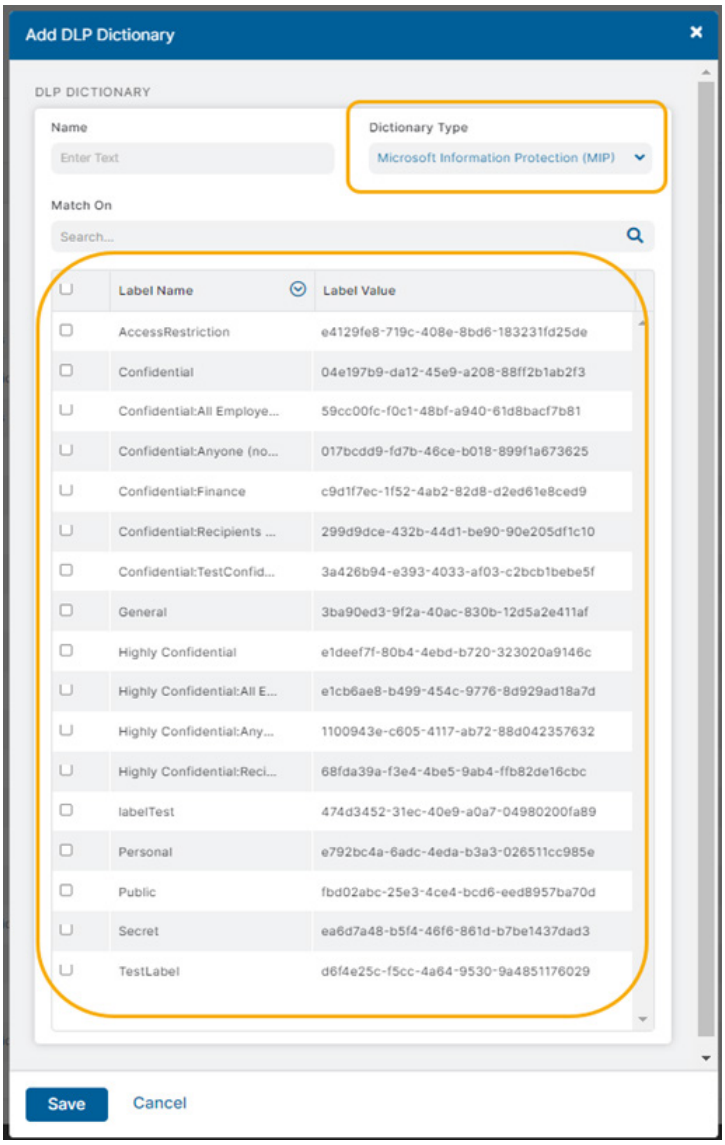

Figure 16. Add DLP Dictionary Microsoft Information Protection

©2024 Zscaler, Inc. All rights reserved.

- **Indexed Document Match**: If selected, the **Indexed Document Match** section appears, where you can select existing IDM templates and choose match accuracy levels for those templates. To learn more, see Creating an Indexed Document Match Template and Defining IDM Match Accuracy for Custom DLP Dictionaries (government agencies, see Creating an Indexed Document Match Template and Defining IDM Match Accuracy for Custom DLP Dictionaries).

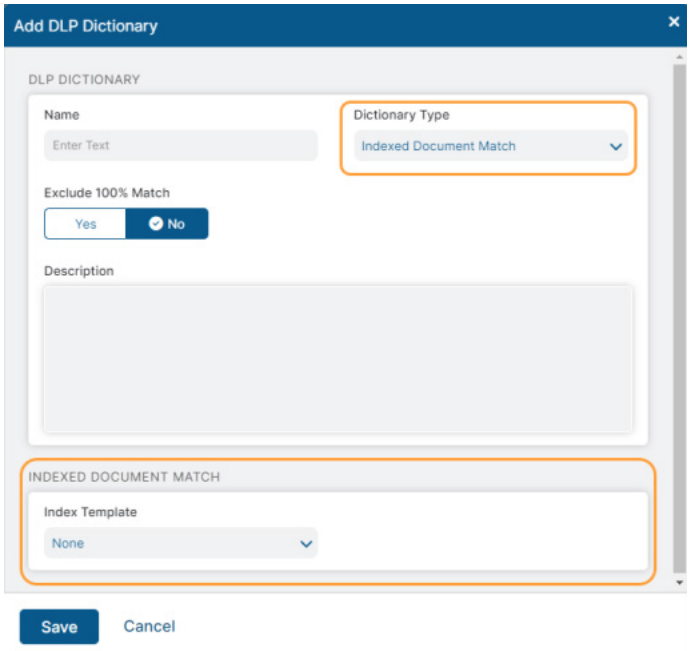

Figure 17. Add DLP Dictionary Index Document Match

- **Exact Data Match**: If selected, the **Exact Data Match** (EDM) section appears, where you can select existing EDM templates and add data fields from those templates. To learn more, see Creating an Exact Data Match Template and Defining Exact Data Match Fields for Custom DLP Dictionaries (government agencies, see Creating an Exact Data Match Template and Defining Exact Data Match Fields for Custom DLP Dictionaries).

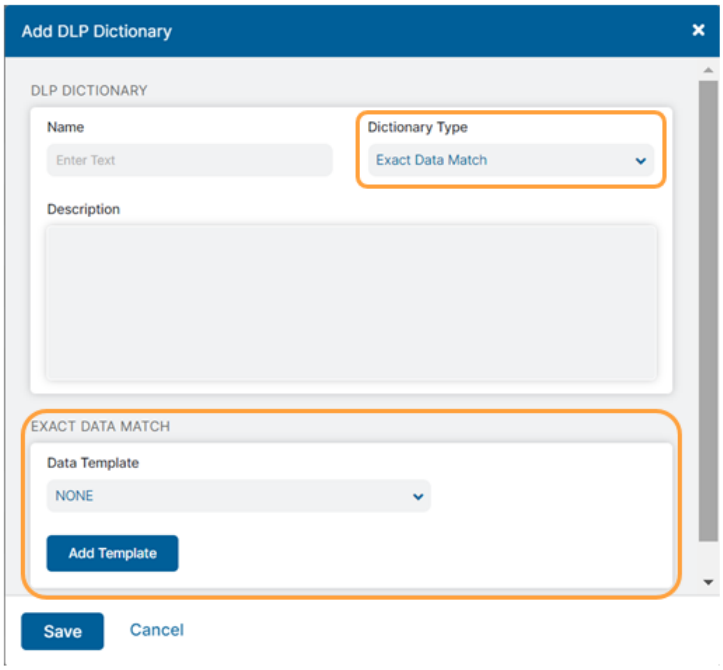

Figure 18. Add DLP Dictionary Exact Data Match

©2024 Zscaler, Inc. All rights reserved.

c. **Match Type**: This is only applicable if you are configuring a Patterns & Phrases type dictionary. Select a Match Type from the drop-down menu to configure how the dictionary triggers when matching patterns and phrases.
   - **Match Any**: This is the default setting. If selected, the dictionary triggers when a transaction matches any one of the dictionary's patterns or phrases.
   - **Match All**: If selected, the dictionary triggers when a transaction matches all of the dictionary's patterns and phrases.

d. **Description**: (Optional) Enter a description for the dictionary.

4. Click **Save** and **Activate** the change.

Configure DLP Engine

Adding a custom DLP engine is one of the tasks you can complete when configuring DLP policy rules.

You can add a custom DLP engine on the Add DLP Engine window or through the Cloud Service API (government agencies, see Cloud Service API).

To add a custom DLP Engine.

1. Go to **Administration** > **DLP Dictionaries & Engines**.
2. In the **DLP Engines** tab, click **Add DLP Engine**.
3. In the **Add DLP Engine** window, enter the **Name** for the custom DLP engine.
4. In the **Engine Builder** section, add operators and DLP dictionaries to build an expression. You can see your expression in the **Expression Preview**.

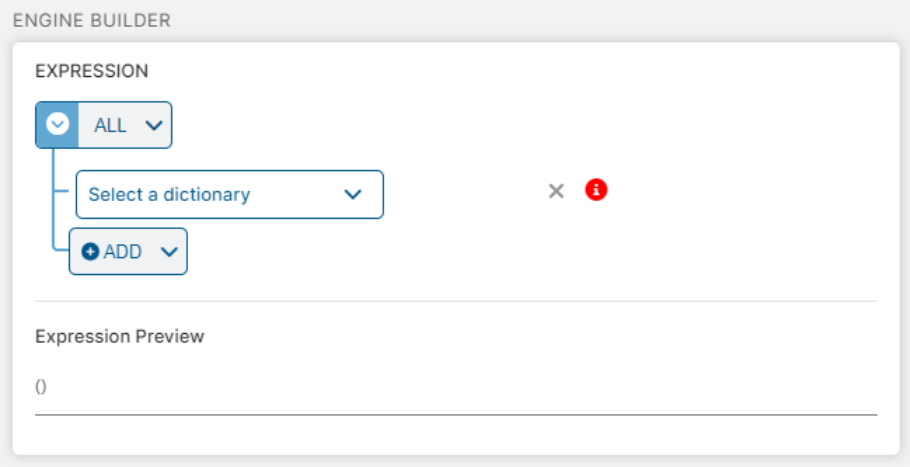

Figure 19. Zscaler Internet Access Engine Builder

5. Under **Expression**:
   a. Select an operator to build your expression. The operators include All (AND), Any (OR), Exclude (AND NOT), and Sum. The Sum operator is available for count-based DLP dictionaries (e.g., Credit Cards, Social Security Numbers, etc.) and allows you to specify the sum total of matches that trigger a group of dictionaries specified in the DLP engine.
   b. Select a dictionary from the drop-down menu, then specify a match count (government agencies, see match count) as needed.
   c. Click **Add** to add a Dictionary or a Subexpression. Click the **Remove** icon to delete dictionaries or subexpressions.

©2024 Zscaler, Inc. All rights reserved.

- If you use the **Sum** operator, select two or more predefined or custom DLP dictionaries. You must set a value for the match count. You can enter any value less than 1,000.
- If you use the **All**, **Any**, or **Exclude** operators, you must select a predefined or custom DLP dictionary. Certain dictionaries require you to set a value for the match count. You can enter any value less than 1,000.
- If you click **Subexpression**, you must select an operator. The operators include **All** (AND), **Any** (OR), **Exclude** (AND NOT), and **Sum**. The Sum operator is available for count-based DLP dictionaries (e.g., Credit Cards, Social Security Numbers, etc.) and allows you to specify the sum total of matches that trigger a group of dictionaries specified in the subexpression

d. Continue adding dictionaries and operators to the expression as needed. At each level, you can create up to 4 subexpressions, use up to 4 operators, and add up to 16 dictionaries per operator.

e. (Optional) For **Description**, enter any additional notes or information. The description cannot exceed 255 characters.

6. Click **Save** and **Activate** the change.

Define Policy Rules

To define your policy rules:

1. Go to **Policy** > **Data Loss Prevention**.
2. Click **Add** and select **Rule With Content Inspection**.
3. In the **Add DLP Rule** window:
   a. **Rule Order**: Policy rules are evaluated in ascending numerical order (Rule 1 before Rule 2, and so on), and the Rule Order reflects this rule's place in the order. You can change the value, but if you've enabled Admin Ranking, the assigned Admin Rank determines the Rule Order values you can select.
   b. **Admin Rank**: Enter a value from 0–7 (0 is the highest rank). Your assigned admin rank determines the values you can select. You cannot select a rank that is higher than your own. The rule's Admin Rank determines the value you can select in Rule Order so that a rule with a higher Admin Rank always precedes a rule with a lower Admin Rank.
   c. **Rule Name**: Enter a unique name for the DLP rule or use the default name.
   d. **Rule Status**: An enabled rule is actively enforced. A disabled rule is not actively enforced, but does not lose its place in the Rule Order; the service skips it and moves to the next rule.
   e. **Rule Label**: Select a rule label to associate it with the rule. To learn more, see **About Rule Labels** (government agencies, see **About Rule Labels**).
4. Define the following Criteria:
   a. **DLP Engines**: Select **Any** to choose all DLP engines for this rule, or select up to 4 engines. You can search for DLP engines or click the **Add** icon to create a new DLP engine.
   b. The **Match Only** option takes effect for both **Allow** and **Block** rule actions. You can select **Match Only** to configure how engines must trigger in order for the service to take action. To learn more, see **DLP Policy Configuration Example: Match Only** (government agencies, see **DLP Policy Configuration Example: Match Only**).
5. For **Public AI Sites**, select the in-scope AI site under the **URL Categories** or **Cloud Applications**.
6. For **Private AI Sites**:
   a. **ZPA Application Segment**: Select **Any** to apply the rule to all **ZPA application segments** (government agencies, see **ZPA application segments**), or select up to 255 ZPA application segments. You can also search for ZPA application segments.

©2024 Zscaler, Inc. All rights reserved.

b. **File Type**: From the drop-down menu, choose the file types for the rule. You can create DLP policy rules that apply just to content sent via specific file types. **Policies that reference Zscaler DLP engines** (government agencies, see **Policies that reference Zscaler DLP engines**) support different file types than policies that reference external DLP engines. Zscaler DLP engines can scan files of up to 100 MB. For an archived file, the size of individual files when decompressed can also be a maximum of 100 MB.

c. **Minimum Data Size**: Enter the minimum size requirement that data must meet before the DLP rule applies. The default minimum data size, 0 KB, means there is no minimum data size requirement.

d. **Users**: You can specify how the DLP rule applies to your users.

- Choose **Include** to apply the rule to selected users and no other users. From the drop-down menu, choose **Any** to apply the rule to all users or select up to 4 users.
- Choose **Exclude** to apply the rule to all other users and not selected users. You can select up to 256 users.

e. **Groups**: You can specify how the DLP rule applies to your groups.

- Choose **Include** to apply the rule to selected groups and no other groups. From the drop-down menu, choose **Any** to apply the rule to all groups or select up to 8 groups.
- Choose **Exclude** to apply the rule to all other groups and not selected groups. You can select up to 256 groups.

f. **Departments**: You can specify how the DLP rule applies to your departments.

- Choose **Include** to apply the rule to selected departments and no other departments. From the drop-down menu, choose **Any** to apply the rule to all departments or select up to 8 departments.
- Choose **Exclude** to apply the rule to all other departments and not selected departments. You can select up to 256 departments.

g. **User Risk Profile**: Select the user risk score levels to which the rule applies. Selecting no value ignores this criterion in the policy evaluation. Users are assigned a risk score based on their browsing activities. A range of risk scores is grouped as a risk score level:

- **Low**: Level with user risk scores ranging from 0 to 29.
- **Medium**: Level with user risk scores ranging from 30 to 59.
- **High**: Level with user risk scores ranging from 60 to 79.
- **Critical**: Level with user risk scores ranging from 80 to 100.

h. **Locations**: Select **Any** to apply the rule to all **locations** (government agencies, see **locations**) or select up to 8 locations. You can also search for a location or click the **Add** icon to add a new location.

i. **Location Groups**: Select **Any** to apply the rule to all **location groups** (government agencies, see **location groups**) or select up to 32 location groups. You can also search for a location group.

j. **Time**: Select **Always** to apply this rule to all **time intervals** (government agencies, see **time intervals**) or select up to two time intervals. You can also search for a time interval or click the **Add** icon to add a new time interval.

k. **Protocols**: Select the protocols to which the rule applies.

- **HTTP**: Data transactions and file uploads from HTTP websites.
- **HTTPS**: Data transactions and file uploads from HTTPS websites encrypted by TLS/SSL.
- **Native FTP**: Data transactions and file uploads from native FTP servers.

l. **Inspect Downloads**: Enable this option to allow DLP inspection for content downloaded from specific AI apps. If this option is enabled, you must choose at least one application segment. If disabled, the DLP rule only applies to content sent to cloud apps.

©2024 Zscaler, Inc. All rights reserved.

m. (Optional) For **DLP Incident Receiver**, complete one of the following tasks:
   - If you don't have a third-party DLP solution or don't want to forward content, leave the following **Zscaler Incident Receiver** or **ICAP Receiver** field as **None**.
   - If you want to forward the transactions captured by this policy rule to a DLP incident receiver:
     - For **Incident Receiver**, select whether the DLP incident receiver is an **ICAP receiver** or a **Zscaler Incident Receiver**.
     - Select the applicable **ICAP Receiver** or **Zscaler Incident Receiver** from the drop-down menu. You must configure your ICAP receivers or Zscaler Incident Receivers (government agencies, see ICAP receivers or Zscaler Incident Receivers) in order to complete this step.

n. Select the **Action** for the rule. You can **Allow** or **Block** transactions that match the rule. If you select **Allow**, the service allows and logs the transaction. If you select **Block**, the service blocks and logs the transaction.

o. (Optional) Configure an email notification for the rule. If you do not select an auditor and notification template, a notification is not sent for this rule.
   - For **Auditor Type**, select whether the auditor is from a **Hosted database** or **External** to your organization.
   - Select the **Auditor**:
     - If the auditor is from a hosted database, select or search for the auditor.
     - If the auditor is external, enter the auditor's email address.
   - Select a Notification Template, if you configured one (government agencies, see configured one) You can also search for a notification template or click the **Add** icon to add a new notification template.

p. (Optional) Configure **Client Connector Notification**. You can **Enable** or **Disable** Client Connector notifications for the rule when violations occur. The field is only available if you enable the **Web DLP Violations** option for your organization on the **End User Notifications** page in the ZIA Admin Portal and you select the **Action** as **Block** for the rule. See Using the Zscaler Notification Framework (government agencies, see Using the Zscaler Notification Framework)

q. (Optional) Enter a **Description** including additional notes or information. The description cannot exceed 10,240 characters.

©2024 Zscaler, Inc. All rights reserved.

7. Click **Save** and **Activate** the change.

You can combine public and private AI sites under a single policy if required.

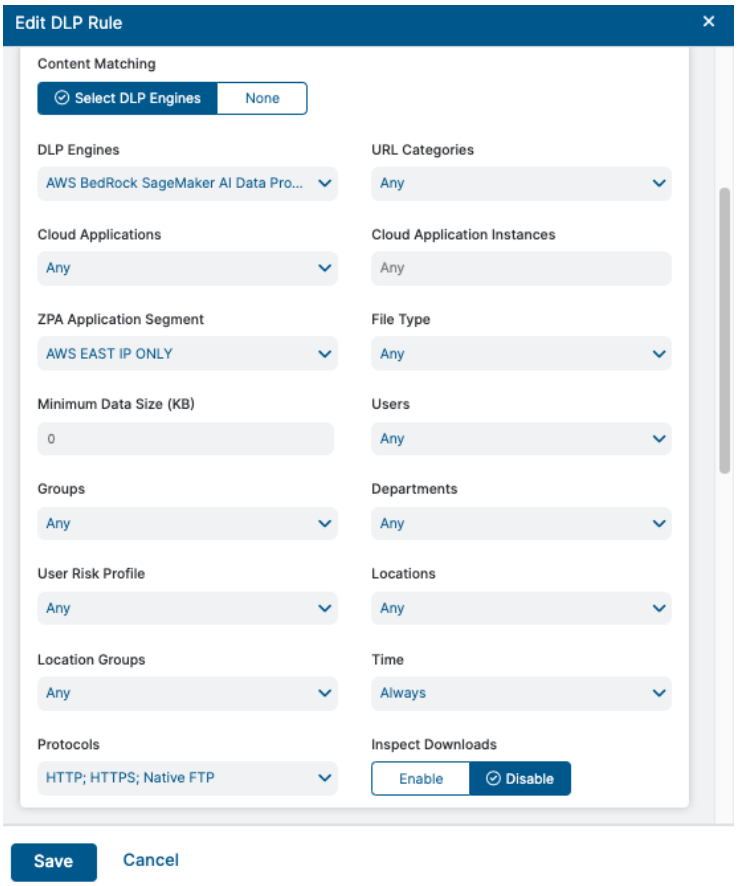

Figure 20. Zscaler Internet Access DLP Rule

©2024 Zscaler, Inc. All rights reserved.

Configure the Zscaler Notification Framework

Optionally, you can configure various settings for user notifications in Zscaler Client Connector. Some of these settings are enabled after a user's device is enrolled in the Zscaler service and you can change them in the Zscaler Client Connector.

There are two types of notifications: the default Windows-based notification system and Zscaler's Notification Framework. While both notification systems provide the same informational messages, users cannot disable notifications from the Zscaler Notification Framework in Windows settings.

Zscaler notifications are displayed in the bottom right corner of the screen. Up to 5 notifications can appear and they time out after 5 seconds. You can move and dismiss these notifications by clicking anywhere on the window.

Configure the Zscaler Notification Framework as follows:

1. In the Zscaler Client Connector, go to **Administration** > **Client Connector Notifications**.
2. Click the **End User Notifications** tab and select from the following options:
    a. **Enable Notifications by Default**: This setting is enabled when a user is enrolled. Users can turn this option off from the Zscaler Client Connector.
    b. **Enable App Updates Notifications**: Select this option to have users receive app upgrade notifications.
    c. **Enable Service Status Notifications**: Select this option to have users receive status notifications for Zscaler Services, such as when a service is in Disaster Relief (DR) mode.
    d. **Enable ZIA Notifications**: Select this option to have users receive notifications from ZIA, such as DLP notifications.
    e. **Enable Notifications for ZPA reauthentication**: Select this option to prompt users for authentication. This option is enabled after a user is enrolled. Users can turn off this option from Zscaler Client Connector.
    f. **Show ZPA Reauthentication Notifications Every (In Minutes)**: Select this option to show ZPA reauthentication notifications at a specific time interval. This setting is enabled by default. Enter a value from 2 to 1440 to set the interval in minutes.
    g. **Custom Timer (In Seconds)**: Use this option to set the time the notification displays for the user. Enter a time between 5 and 60 seconds.
    h. **Enable Persistent Notifications**: This setting is enabled by default and displays critical notifications until the user dismisses them. Critical notifications include ZPA reauthentication, captive portal detection, request for a system reboot, and packet capture.
    i. **ZIA Notification Persistent**: When enabled, this option overrides the custom timer and makes notifications persistent.

©2024 Zscaler, Inc. All rights reserved.

3. Click **Save**.

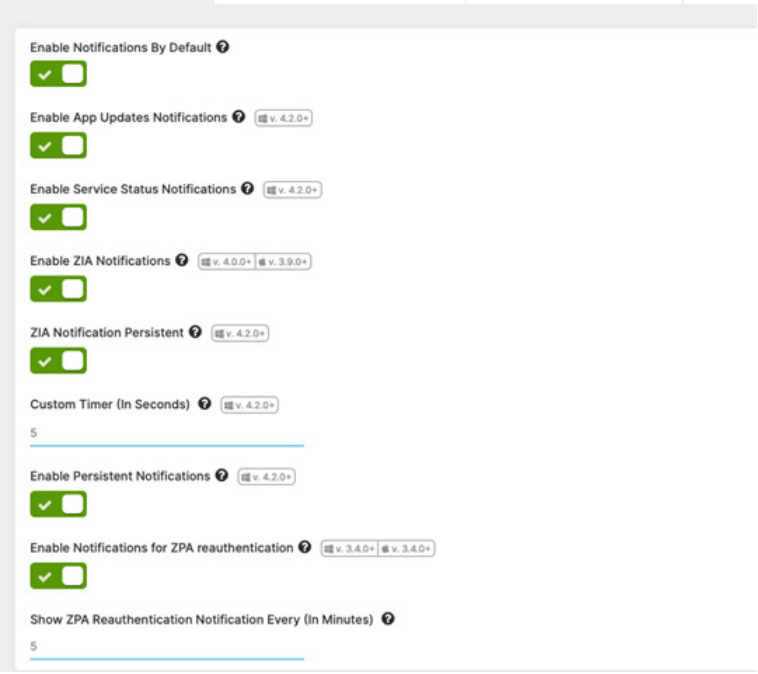

Figure 21. Enable ZIA Notifications

Use ZIA Notification Persistence carefully. Based on ZIA policy, users might have several DLP block notifications.

You must enable the notification framework per application profile.

Windows

To enable the Zscaler Notification Framework on Windows devices:

1. In the Zscaler Client Connector Portal, go to **App Profiles**.
2. Click **Add Windows Policy**.
3. Enable **Use Zscaler Notification Framework**.
4. Click **Save**.

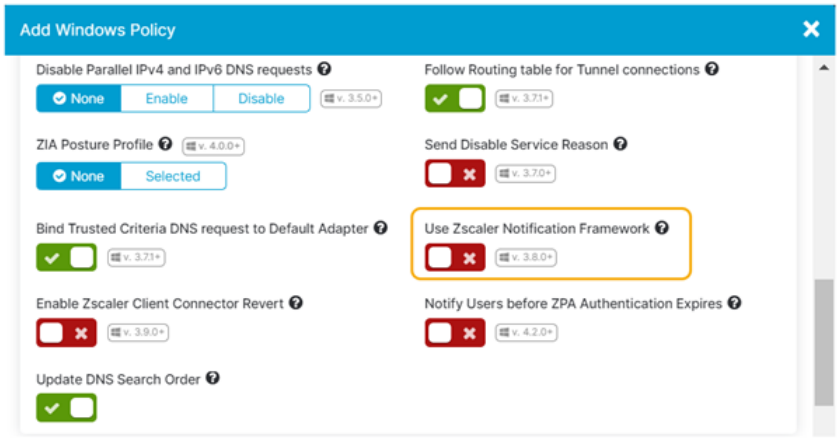

Figure 22. Enable Windows Notification Framework

©2024 Zscaler, Inc. All rights reserved.

macOS

To enable the Zscaler Notification Framework on macOS devices:

1. In the Zscaler Client Connector Portal, go to **App Profiles**.
2. Click **Add macOS Policy**.
3. Enable **Use Zscaler Notification Framework**.
4. Click **Save**.

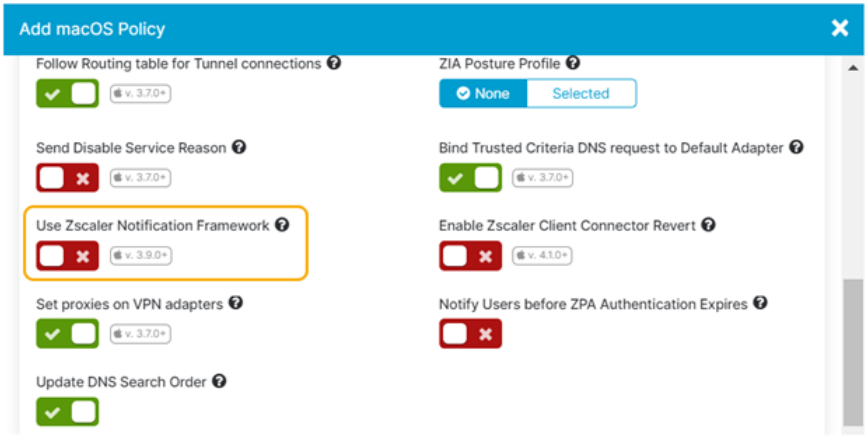

Figure 23. Enable macOS Notification Framework

©2024 Zscaler, Inc. All rights reserved.

Appendix A: ZPA and ZIA Configuration for Private AI Data Protection

To properly configure and run a Source IP Anchor, ensure the following conditions are met:

- Configure Application Connectors with a private IP address and NAT'd to a public IP address.
- Do not expose the Application Connector by configuring a public IP address directly on the Application Connector interface.
- Application Connector's public IP address is the anchored source IP address.
- Ensure the firewall allows the Application Connector to reach the destination server.

Source IP Anchoring uses ZIA forwarding policies and ZPA Application Connectors to selectively forward the application traffic to the appropriate destination servers. You can configure forwarding rules in the ZIA Admin Portal to forward Source IP Anchored traffic to ZPA through ZIA threat and data protection engines.

Integration Architecture for Amazon Q

The following diagram shows a typical design pattern for Generative AI and Zscaler configured and deployed to protect Generative AI.

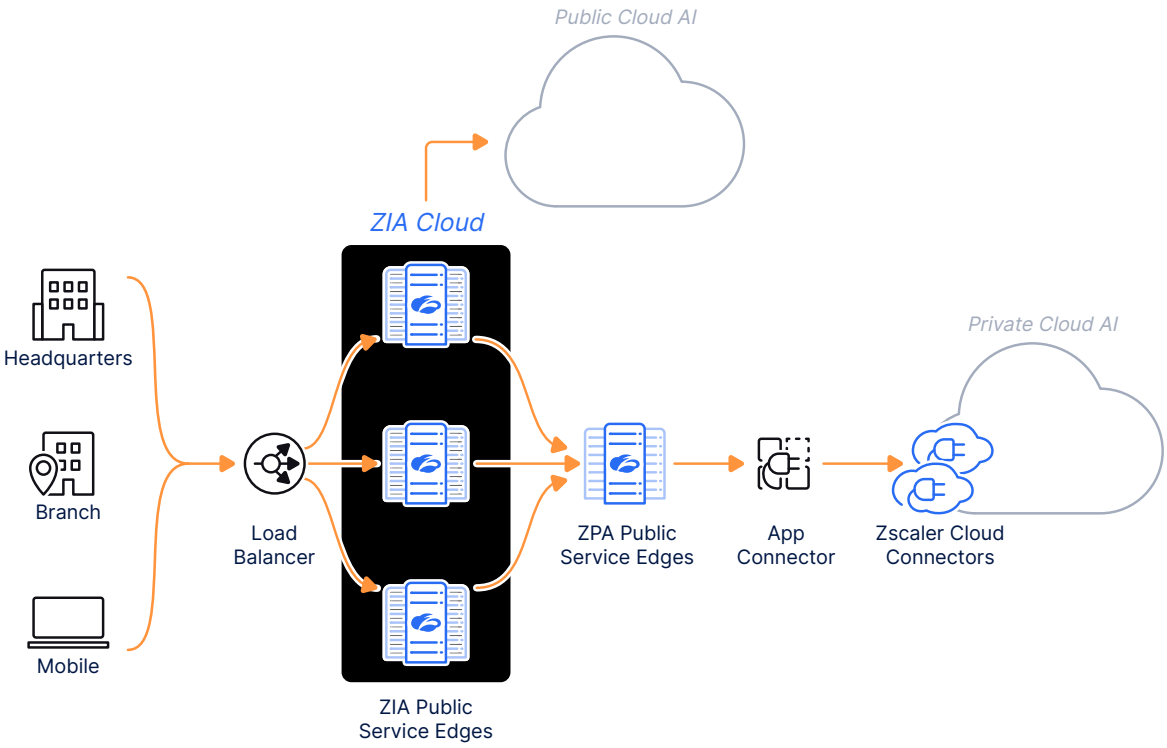

Figure 24. ZIA and ZPA Data Protection

©2024 Zscaler, Inc. All rights reserved.

Configure Application Segment

Create and configure an application segment that uses Source IP Anchoring. Ensure you enable the Source IP Anchor option and select Use Client Forwarding Policy under the Bypass field while configuring the application segment.

1. Log in to the ZPA Admin Portal.
2. Go to **Resource Management** > **Application Management** > **Application Segment**.
   a. Click the Ellipsis in the right-side of the window and click **Add Application Segment**.
   b. Enter a Segment Name in the **Name** field.
   c. Verify **Status** is set to **Enabled**.
   d. Set **SourceIP Anchor** to **Enabled**.

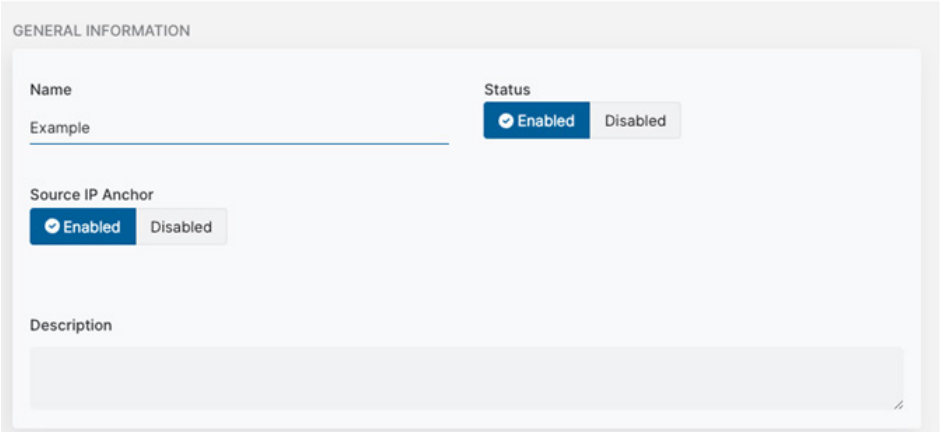

Figure 25. Add Application Segment Source IP Anchor

   e. In **Additional Configuration**, set **Bypass** to **Use Client Forwarding Policy**.
   f. Complete the remaining configuration steps for Application Segment configuration by following Configuring Defined Application Segments (government agencies, see Configuring Defined Application Segments).
3. Click **Save**.

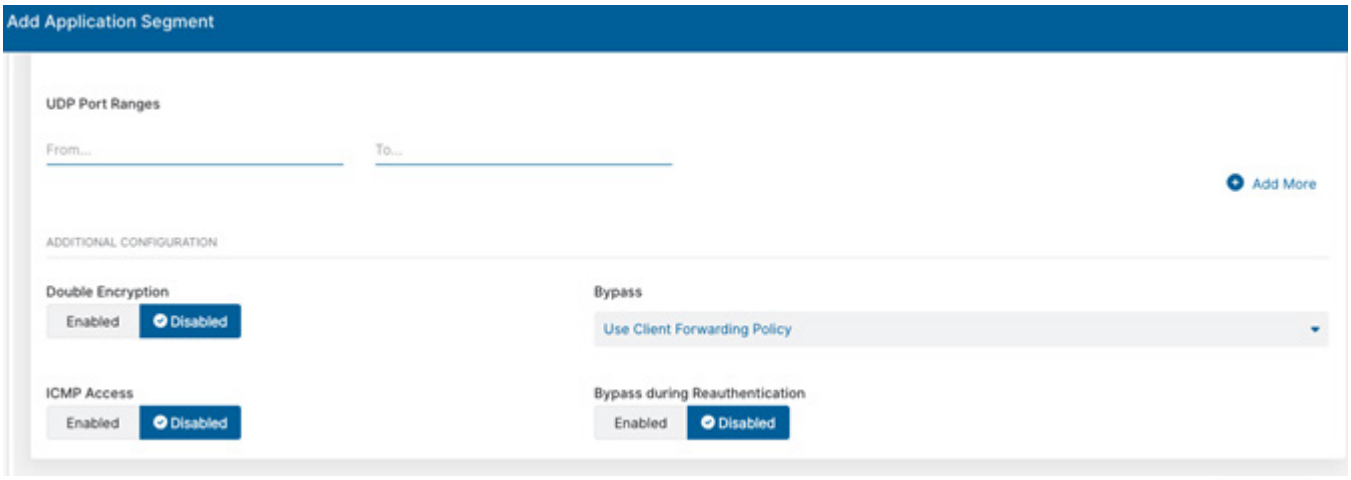

Figure 26. Add Application Segment Bypass

©2024 Zscaler, Inc. All rights reserved.

Configure ZPA Client Forwarding Policy

Configure a client forwarding policy for the application segment. Create separate client forwarding policy rules for IP address-based and domain-based applications.

For IP address-based applications, select the Only Forward Allowed Applications rule action for Source IP Anchoring application segments.

For IP address-based applications, configure the following rule:

1. In the ZPA Admin Portal, go to **Policy** > **Client Forwarding Policy**.
2. Click **Add Rule**.
3. Enter the Client Forwarding Policy Name in the **Name** field.
4. (Optional) Enter the Client Forwarding Policy Description in the **Description** field.
5. In **Rule Action**, select **Only Forward Allowed Applications**.
6. Click **Add Criteria**:
   a. Select **Applications**.
   b. In the **Application Segments** drop-down menu, select the SIPA Application Segment created in Configure Application Segment earlier.
7. Click **Save**.

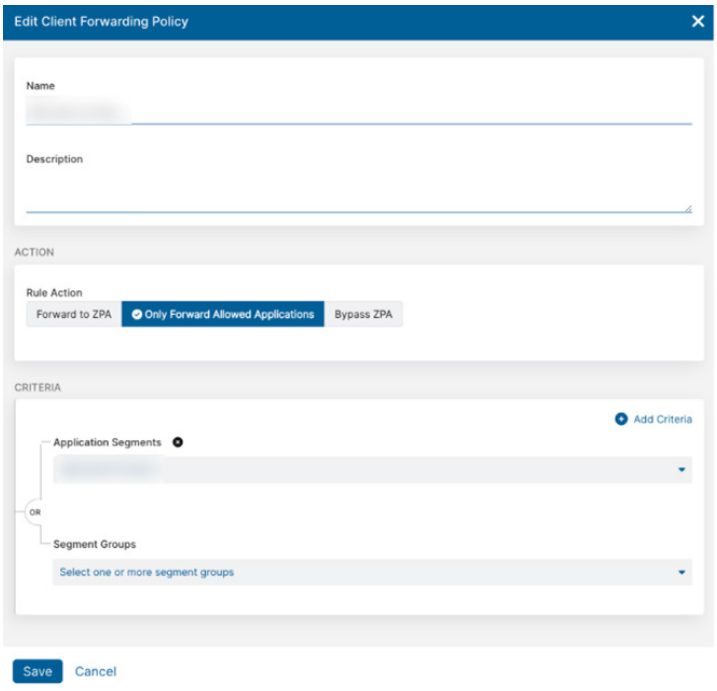

Figure 27. Add Client Forwarding Policy—Only Forward Allowed Applications

For domain-based applications, configure the following two rules:

- Rule 1: Select the Bypass ZPA rule action for Source IP Anchoring Segment Groups and **Client Types** > **Client Connector** as described in Rule 1: Enable the Bypass ZPA Rule Action.
- Rule 2: Select the Forward to ZPA rule action for Source IP Anchoring Segment Groups and **Client Types** > **ZIA Public Service Edge** as described in Rule 2: Enable the Forward to ZPA Rule Action.

©2024 Zscaler, Inc. All rights reserved.

Rule 1: Enable the Bypass ZPA Rule Action

1. In the ZPA Admin Portal, go to **Policy** > **Client Forwarding Policy**.
2. Click **Add Rule**.
3. Enter the Client Forwarding Policy Name in the **Name** field.
4. (Optional) Enter the Client Forwarding Policy Description in the **Description** field.
5. In **Rule Action**, select **Bypass ZPA**.
6. Click **Add Criteria**.
   a. Select **Applications**.
   b. In the **Application Segments** drop-down menu, select the SIPA Application Segment created in [Configure Application Segment] earlier.
7. Click **Add Criteria**:
   a. Select **Client Types**.
   b. In the **Client Types** drop-down menu, select **Client Connector**.
8. Click **Save**.

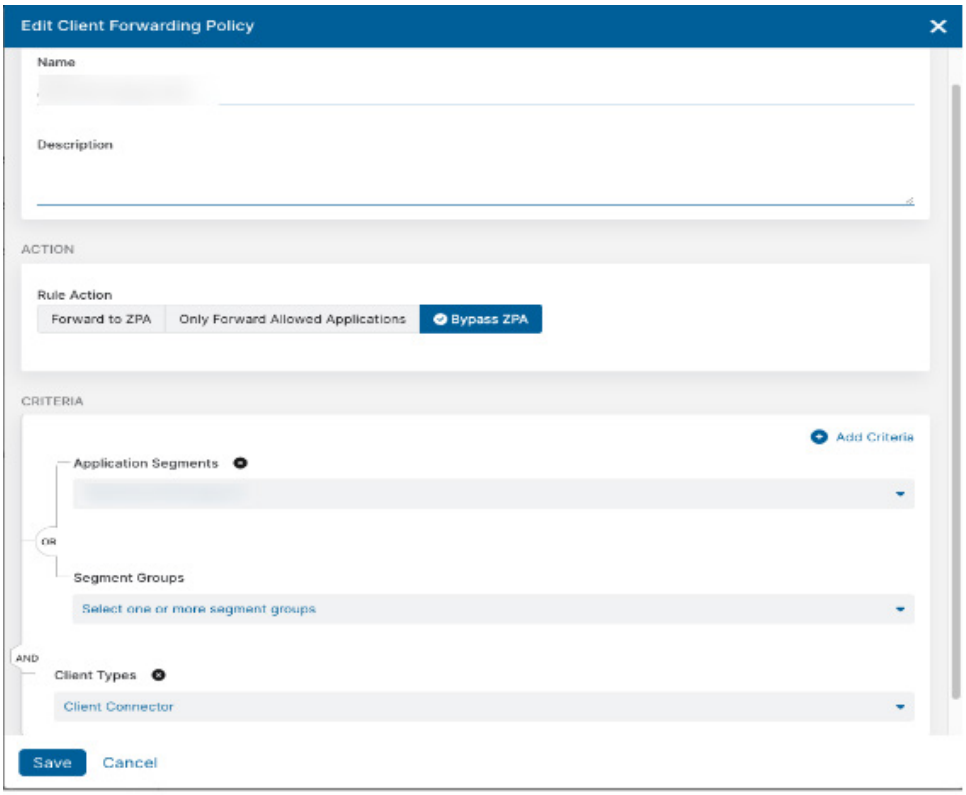

Figure 28. Add Client Forwarding Policy—Bypass ZPA

©2024 Zscaler, Inc. All rights reserved.

Rule 2: Enable the Forward to ZPA Rule Action

1. Go to **Policy** > **Client Forwarding Policy**.
2. Click **Add Rule**.
3. Enter the Client Forwarding Policy Name in the **Name** field.
4. (Optional) Enter the Client Forwarding Policy Description in the **Description** field.
5. In **Rule Action**, select **Forward to ZPA**.
6. Click **Add Criteria**.
   a. Select **Applications**.
   b. In the **Application Segments** drop-down menu, select the SIPA Application Segment created in Configure Application Segment earlier.
7. Click **Add Criteria**:
   a. Select **Client Types**.
   b. In the **Client Types** drop-down menu, select **ZPA Service Edge**.
8. Click **Save**.

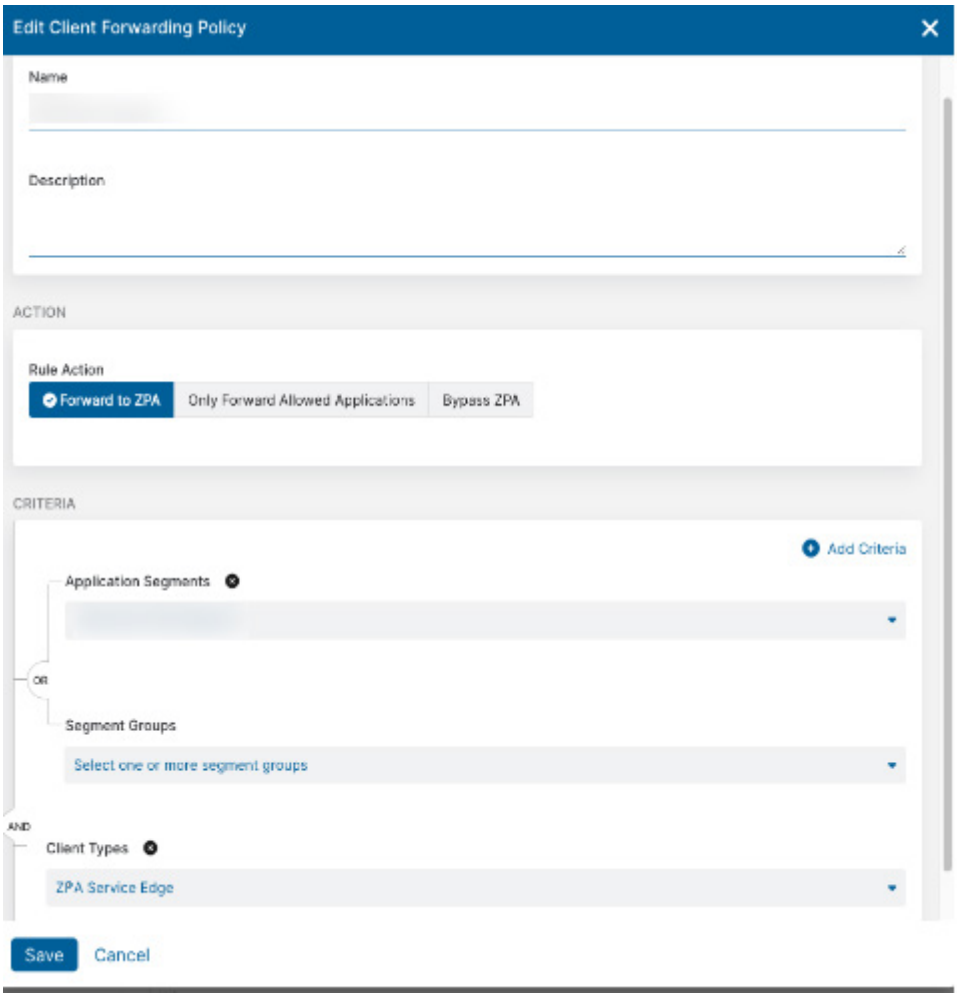

Figure 29. Add Client Forwarding Policy—Forward to ZPA

©2024 Zscaler, Inc. All rights reserved.

Configure ZPA Access Policy

The following steps create and configure an access policy for the application segment. Create separate access policy rules for IP address-based and domain-based applications. For IP address-based applications, select the Allow Access rule action and add only the ZIA Public Service Edge client type for the application segments. For domain-based applications, allow the Source IP Anchoring client (ZIA Public Service Edge client type) to access the applications.

For IP Address-Based Applications

Configure the following rules.

Allow Access Rule Action and Add Only the ZIA Public Service Edge

1. Go to **Policy** > **Access Policy**.
2. Click **Add Rule**.
3. Enter the Access Policy Name in the **Name** field.
4. (Optional) Enter the Access Policy Description in the **Description** field.
5. In **Rule Action**, select **Allow Access**.
6. Click **Add Criteria**:
   a. Select **Applications**.
   b. In the **Application Segments** drop-down menu, select the SIPA Application Segment created in Configure Application Segment earlier.
7. Click **Add Criteria**:
   a. Select **Client Types**.
   b. In the **Client Types** drop-down menu, select **ZPA Service Edge**.
8. Click **Save**.

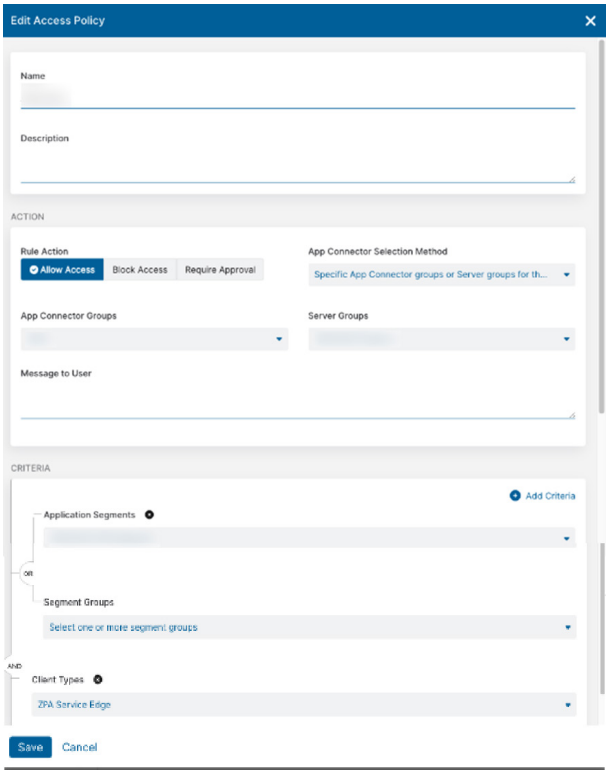

Figure 30. Add Access Policy—Allow Access Public Service Edge Only

©2024 Zscaler, Inc. All rights reserved.

For Domain-Based Applications

Configure the following rule:

1. Go to **Policy** > **Access Policy**.
2. Click **Add Rule**.
3. Enter the Access Policy Name in the **Name** field.
4. (Optional) Enter the Access Policy Description in the **Description** field.
5. In **Rule Action**, select **Allow Access**.
6. Click **Add Criteria**:
   a. Select **Applications**.
   b. In the **Application Segments** drop-down menu, select the SIPA Application Segment created in Configure Application Segment earlier.
7. Click **Add Criteria**:
   a. Select **Client Types**.
   b. In the **Client Types** drop-down menu, select **ZPA Service Edge**.
8. Click **Save**.

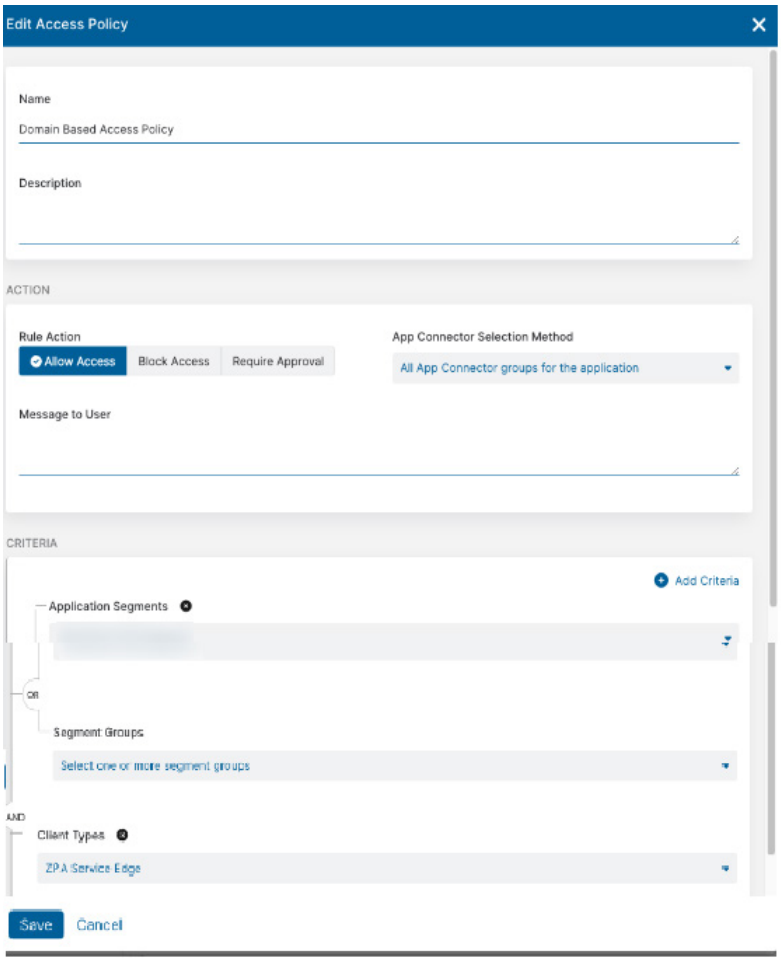

Figure 31. Add Access Policy—Allow Access Public Service Edge Only Domain Access policy

©2024 Zscaler, Inc. All rights reserved.

To learn more, see Configuring Client Forwarding Policies (government agencies, see Configuring Client Forwarding Policies).

If configuration is required for source IP direct for disaster recovery mode, see Understanding Source IP Anchoring Direct (government agencies, see Understanding Source IP Anchoring Direct).

Configure ZPA Gateway

Configure ZPA gateways on the ZIA Admin Portal to map it to the ZPA server groups and the associated application segments that require Source IP Anchoring.

1. Log in to the ZIA Admin Portal.
2. Go to **Administration** > **Zscaler Private Access**.
3. Click **Add Gateway for ZPA**. The **Add Gateway for ZPA** window is displayed.
4. From the **Server Group** drop-down menu, select the server group that you configured on ZPA for Source IP Anchoring. All the application segments that are associated with the selected server group for which Source IP Anchoring is enabled appear in the **Application Segment** field.
5. Click **Save** and **Activate** the changes.

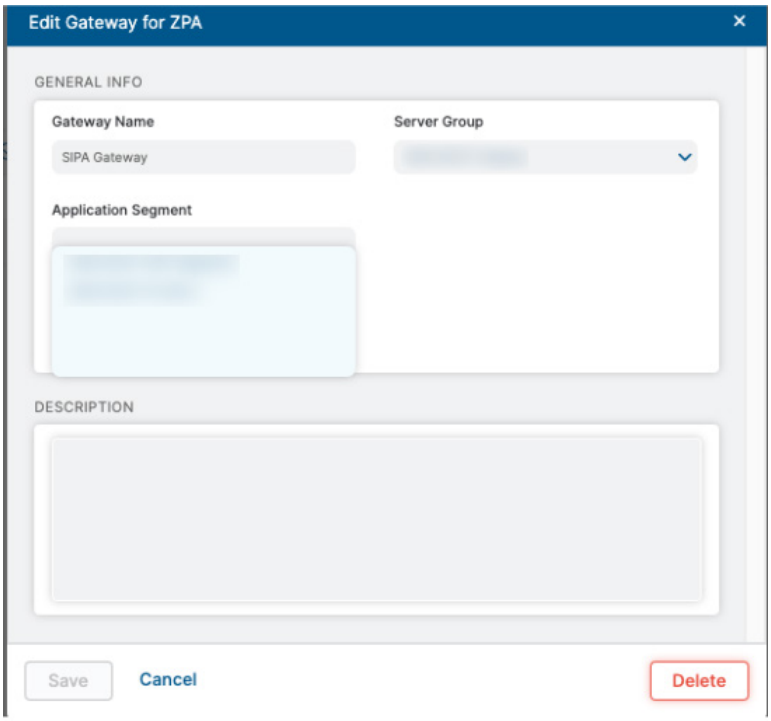

Figure 32. Add Gateway for ZPA

To learn more, see Saving and Activating Changes in the ZIA Admin Portal (government agencies, Saving and Activating Changes in the ZIA Admin Portal).

©2024 Zscaler, Inc. All rights reserved.

Configure Forwarding Policy for ZPA

Zscaler uses forwarding control policies to forward selective Zscaler traffic to specific endpoints. For example, if you want to forward web traffic to a third-party proxy service or if you want to forward application traffic to a ZPA App Connector, you can configure your forwarding policy with appropriate rules.

The following steps configure forwarding policies to forward ZIA traffic for Source IP Anchoring. Zscaler provides a predefined forwarding rule, ZIA Inspected ZPA Apps, enabled by default. This rule forwards all ZPA application segment traffic for ZIA inspection that has the Inspect Traffic with ZIA field enabled in the ZPA Admin Portal. You cannot edit this rule.

1. Go to **Policy** > **Forwarding Control**.
2. Click **Add Forwarding Rule**. The **Add Forwarding Rule** window is displayed.
3. Under the **Forwarding Rule Section**, configure the following attributes.
    a. **Rule Order**: Enter the order of the rule. Policy rules are evaluated in ascending numerical order (Rule 1 before Rule 2, and so on), and the Rule Order reflects this rule's place in the order. You can change the value based on your requirements. However, if you've enabled Admin Rank, your assigned admin rank determines the Rule Order values you can select.
    b. **Rule Name**: Enter a user-friendly name for the rule. The Forwarding Control automatically creates a rule name, which you can change. The maximum length is 31 characters.
    c. **Forwarding Method**: Select **ZPA**.
    d. Under **Action Forward to ZPA Gateway**, select the gateway created in Configure ZPA Gateway.
    e. Under **Criteria**, select **Destination** and **Application Segment**. Select the application segment created in Configure Application Segment.
4. Click **Save** and **Activate** the changes.

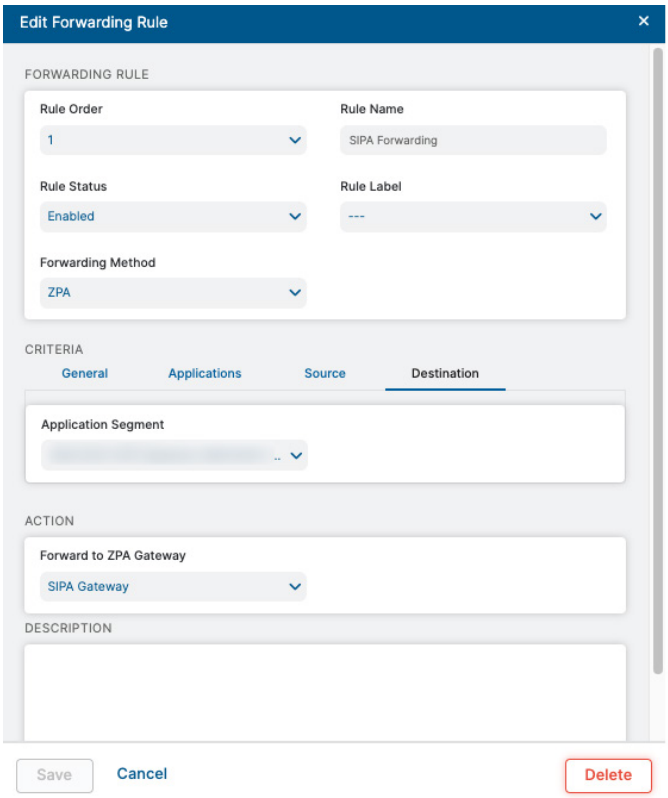

Figure 33. Forwarding Control

©2024 Zscaler, Inc. All rights reserved.

Configure DNS Control

Configure Source IP Anchoring for all traffic forwarded to the ZIA Admin Portal, enable the appropriate preconfigured DNS filtering rule.

1. Go to **Policy** > **DNS Control**.
   a. For location users, enable the **ZPA Resolver for Locations** rule.
   b. For remote users, enable the **ZPA Resolver for Road Warrior** rule.
2. Ensure that these DNS rules are the top rules (i.e., Rule 1 and Rule 2) to configure Source IP Anchoring. The DNS rules are associated with the respective preconfigured IP pools under **Administration** > **IP & FQDN Groups** > **IP Pool**. You can edit the IP pools based on your needs. To learn more, see **About IP Pool** (government agencies, see **About IP Pool**). Any change in the IP pool is reflected in the **Action** column of the respective DNS rule when the rule is enabled.

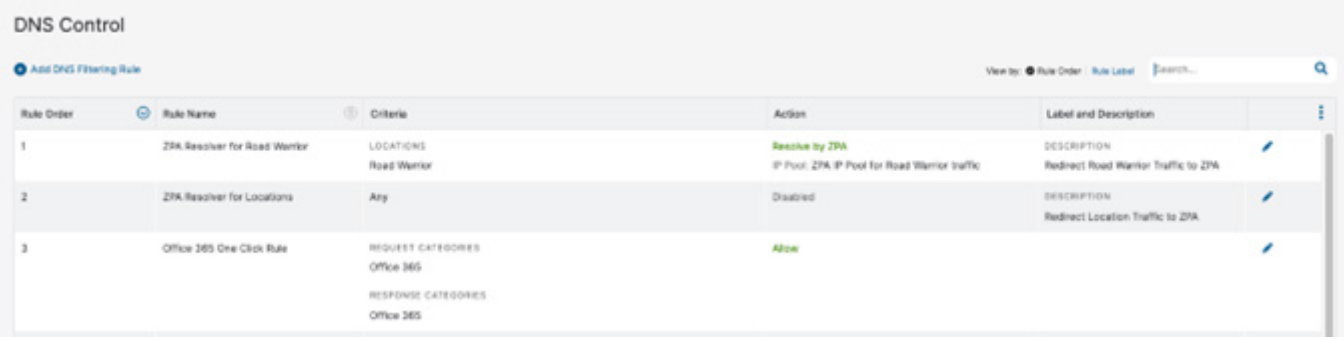

Figure 34. DNS Control

When the ZPA Resolver for Road Warrior rule is disabled, the remote user traffic automatically falls under the ZPA Resolver for Locations rule instead of blocking the traffic. Therefore, Zscaler does not recommend disabling the ZPA Resolver for the Road Warrior rule.

To support Source IP Anchoring for Zscaler Tunnel (Z-Tunnel) 1.0 traffic, you must enable the Enable Firewall for Z-Tunnel 1.0 and PAC Road Warriors option under Administration > Advanced Settings.

Zscaler also recommends having open firewall rules for the Source IP Anchoring pools while sending DNS traffic to the Zscaler service for the Source IP Anchoring domains (i.e., set the Action column on the Firewall Filtering policy to Allow for the Source IP Anchoring pools).

©2024 Zscaler, Inc. All rights reserved.

Appendix B: 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**.

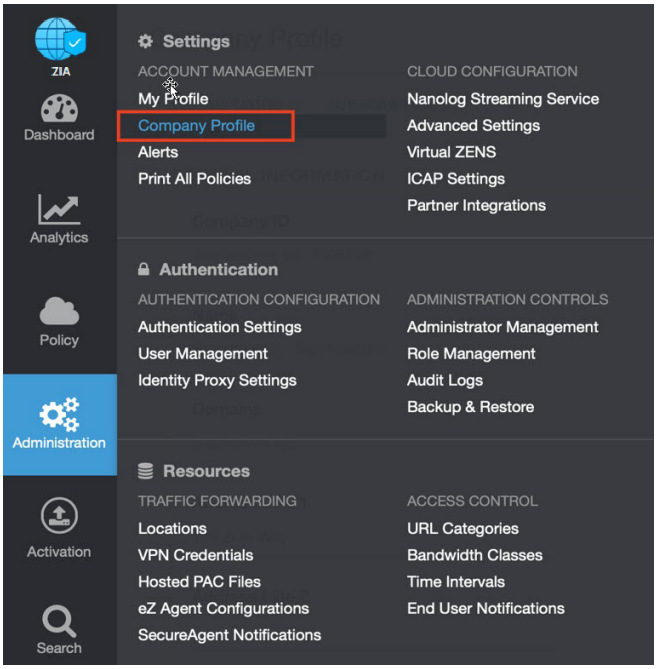

Figure 35. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.

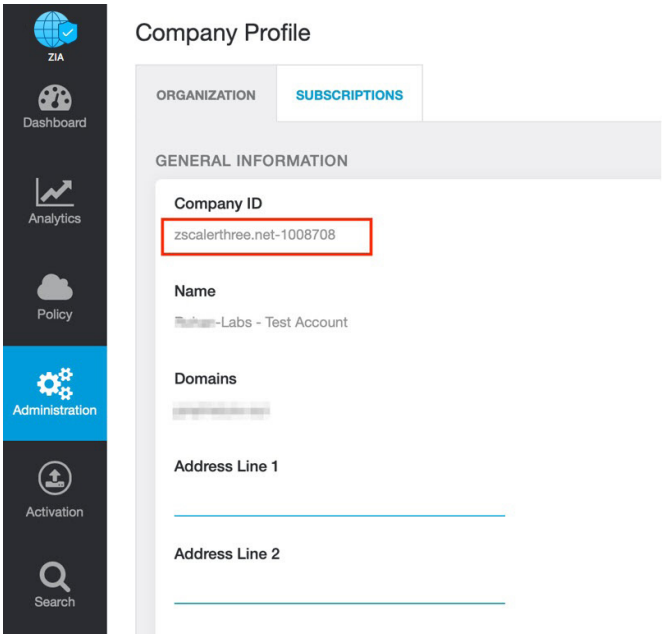

Figure 36. Company ID

©2024 Zscaler, Inc. All rights reserved.

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

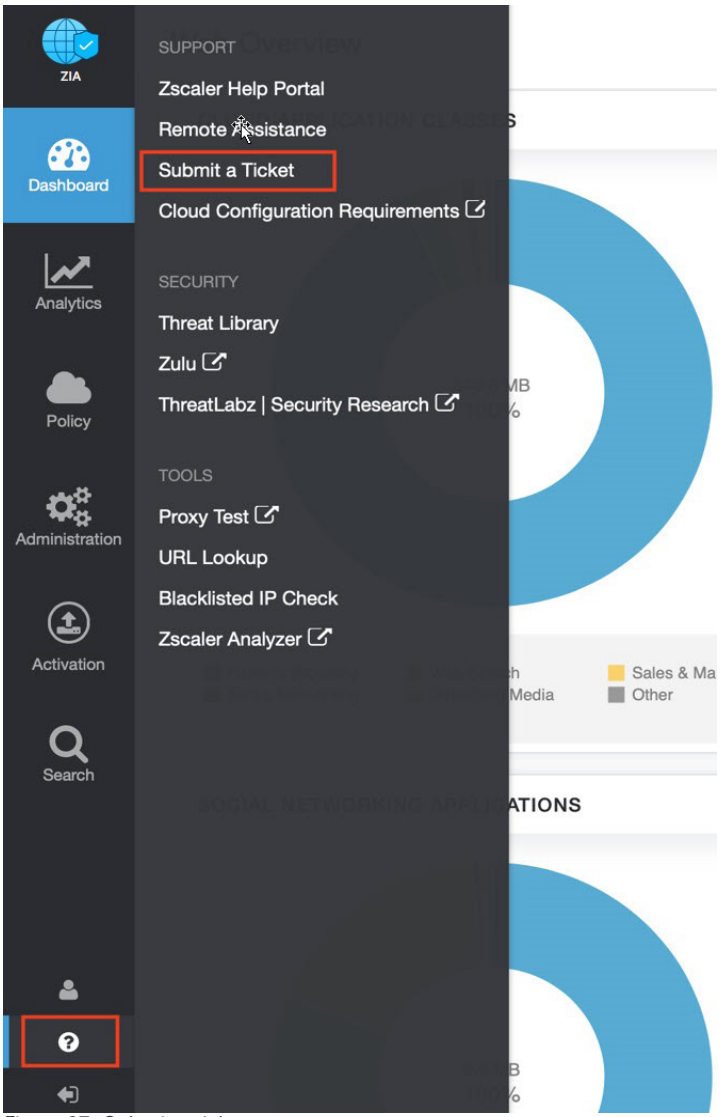

Figure 37. Submit a ticket

©2024 Zscaler, Inc. All rights reserved.