



ZSCALER SAAS SECURITY AND AMAZON S3 DEPLOYMENT GUIDE

Contents

Terms and Acronyms	4
	6
About This Document	6
Zscaler Overview	6
AWS Overview	6
Audience	6
Software Versions	6
Prerequisite	6
Request for Comments	7
Zscaler and AWS Introduction	8
ZIA Overview	8
Zscaler Resources	8
Amazon Workspaces Overview	9
AWS Resources	9
Initial Zscaler Configuration	10
AWS Configuration (IAM Role)	11
AWS Configuration (Trust Relationship)	13
AWS Configuration (CloudTrail)	14
AWS Configuration (Quarantine Bucket)	16
Finish Zscaler Configuration	17
Integrating Zscaler Cloud NSS with Amazon S3	18
Create a User Group in AWS IAM	18

Create a User and Access Key in AWS IAM	21
Create an S3 Bucket and Folder in Amazon S3	27
Create a Policy Granting the User Group Access to the S3 Bucket in Amazon IAM	32
Add a Cloud NSS Feed in the ZIA Admin Portal	37
Appendix A: Create Trail	39
Appendix B: Testing Notes	41
Appendix C: Requesting Zscaler Support	43

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
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
IAM	Identity and Access Management
IKE	Internet Key Exchange (RFC2409)
IPSec	Internet Protocol Security (RFC2411)
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
S3	Simple Storage Service (Amazon)
SSL	Secure Socket Layer (RFC6101)
XFF	X-Forwarded-For (RFC7239)
ZIA	Zscaler Internet Access
ZPA	Zscaler Private Access

Trademark Notice

© 2025 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

About This Document

This document provides information on how to configure Zscaler and Amazon S3 for deployment. This guide doesn't replace the official [Adding SaaS Application Tenants \(Amazon S3\)](#) help page but provides an alternate view of the process, including additional insights and notes on testing. It is assumed that the reader already has some familiarity with administering both ZIA and AWS.

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. Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) services create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler delivers its services 100% in the cloud and offers the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions can't match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss. For more information, see [Zscaler's website](#) or follow Zscaler on Twitter @zscaler.

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, refer to:

- [Zscaler Resources](#)
- [AWS Resources](#)
- [Appendix C: Requesting Zscaler Support](#)

Software Versions

This document was authored using the latest version of Zscaler Internet Access (ZIA).

Prerequisite

Before you can configure Amazon S3 as a SaaS Application Tenant, you must first enable it for your tenant (it is not enabled by default). Customers can contact their Zscaler Account team to get the S3 tenant enabled for their Company ID (e.g., zscaler.net-12345678).

You can find the Company ID for your specific tenant on the Administration > Organization page. When enabled, an Amazon S3 tile is available as an option when adding a tenant on the Administration > SaaS Application Tenants page.



Make sure that the ZIA Admin Portal Session Timeout (on the Administration > Advanced Settings page) is not set too short during this configuration. Start in the ZIA Admin Portal, and then spend time in the AWS Management Console before returning to the ZIA Admin Portal to finish the configuration.

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 AWS Introduction

Overviews of the Zscaler and AWS 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:

- Set up a tunnel (GRE or IPSec) to the closest Zscaler data center (for offices).
- Forward 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, CASB, 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.
ZIA Test Page	Provides information on your Zscaler cloud.
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.

Amazon Workspaces Overview

[Amazon S3](#) is an object storage service offering industry-leading scalability, data availability, security, and performance. Customers of all sizes and industries can store and protect any amount of data for virtually any use case, such as data lakes, cloud-native applications, and mobile apps. With cost-effective storage classes and easy-to-use management features, you can optimize costs, organize data, and configure fine-tuned access controls to meet specific business, organizational, and compliance requirements.

AWS Resources

The following table contains links to AWS support resources.

Name	Definition
Amazon S3 Help	Amazon Simple Storage Service documentation.
AWS CLI	AWS Command Line Interface documentation.
AWS CloudTrail Help	AWS CloudTrail documentation.
AWS IAM Help	AWS Identity and Access Management (IAM) documentation.

Initial Zscaler Configuration


In the ZIA Admin Portal:

1. Go to **Administration > SaaS Application Tenants** and select **Add SaaS Application Tenant**.
2. Select the **Amazon S3** tile for **step 1 (Choose the SaaS Application Provider)**.

Add SaaS Application Tenant

1 Choose the SaaS Application Provider

Search SaaS Application

Enter the application name 

Popular Applications














 box	 OneDrive	 SharePoint	 Google Drive
 Exchange	 Dropbox	 Gmail	 salesforce
 ShareFile	 GitHub	 servicenow	 amazon S3

Figure 1. Add SaaS Application Tenant

3. Enter a name to use for this S3 tenant in **step 2 (Name the SaaS Application Tenant)**, and then copy the Zscaler Connector Account Number and Zscaler Connector User ARN that are created in **step 3 (Authorize the SaaS Application)** for later use.

Add SaaS Application Tenant

1 Choose the SaaS Application Provider



2 Name the SaaS Application Tenant

Tenant Name

S3 Test

The tenant name must be unique

3 Authorize the SaaS Application

To give Zscaler access to Amazon S3, you must configure an IAM role for the Zscaler S3 Connector. [Learn more](#)

Zscaler Connector Account Number	Zscaler Connector User ARN
012345678901 Copy	arn:aws:iam:012345678901:ser/ZscalerSaaSConnectorZSNet01 Copy

Figure 2. Tenant name

AWS Configuration (IAM Role)

The next steps are also documented in the [Adding SaaS Application Tenants](#) help page (government agencies, see [Adding SaaS Application Tenants](#)) in the **Configure an IAM Role for the Zscaler S3 Connector** section (starting with **step iv**).

1. Log in to the AWS Management Console and go to **Services > IAM**.
2. Click **Access Management > Roles** in the left-side navigation.
3. Click **Create Role**.

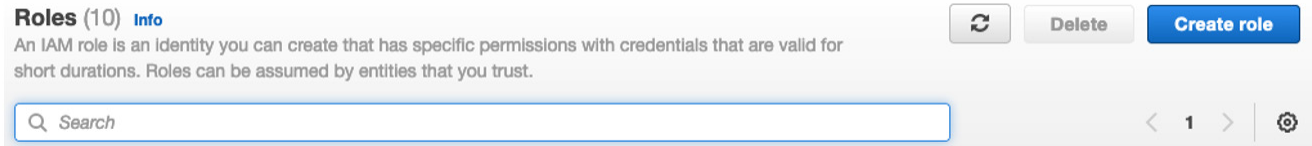
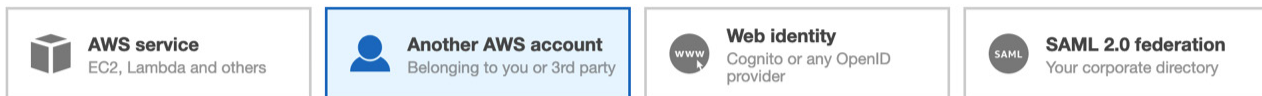


Figure 3. Create Role

4. Click the **Another AWS account** tile as the type of trusted entity.

Select type of trusted entity



Allows entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

Account ID* ⓘ

Options

☐ Require external ID (Best practice when a third party will assume this role)

☐ Require MFA ⓘ

Figure 4. Trusted entity type

5. Enter the **Zscaler Connector Account Number** that you copied earlier in the **Account ID** field, and make sure both **Options** are deselected.
6. Click **Next: Permissions** located at the bottom of the screen.

Specify accounts that can use this role

Account ID* ⓘ

Options

☐ Require external ID (Best practice when a third party will assume this role)

☐ Require MFA ⓘ

Figure 5. Which accounts can use the role

- Enter `AmazonS3FullAccess` into the search area, and select the policy name when found. Click **Next: Tags** located at the bottom of the screen.

▼ Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy

↺

Filter policies ▼

Showing 1 result

	Policy name ▼	Used as
<input checked="" type="checkbox"/>	 AmazonS3FullAccess	None

Figure 6. Attach permissions policies

- Add tags if needed, and then click **Next: Review** located at the bottom of the screen.

Add tags (optional)

IAM tags are key-value pairs you can add to your role. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this role. [Learn more](#)

Key	Value (optional)	Remove
<input type="text" value="connector"/>	<input type="text" value="zscaler"/>	✕
<input type="text" value="Add new key"/>	<input type="text"/>	

You can add 49 more tags.

Figure 7. Add tags

- Enter a **Role name** to use for this role.
- (Optional) Provide a description.
- Click **Create role** located at the bottom of the screen.

Create role

1

2

3

4

Review

Provide the required information below and review this role before you create it.

Role name*

Use alphanumeric and '+=, @-_' characters. Maximum 64 characters.


Role description

Maximum 1000 characters. Use alphanumeric and '+=, @-_' characters.

Trusted entities

The account 012345678901

Policies

 AmazonS3FullAccess [↗](#)

Permissions boundary

Permissions boundary is not set

The new role will receive the following tag

Key	Value
connector	zscaler

* Required

Cancel

Previous

Create role

Figure 8. Create role

AWS Configuration (Trust Relationship)

The next steps are also documented in the [Adding SaaS Application Tenants](#) help page (government agencies, see [Adding SaaS Application Tenants](#)) in the **Edit the Trust Relationship** section.

1. Search for the newly created role by entering `Zscaler` into the search area, and selecting the role name when found.

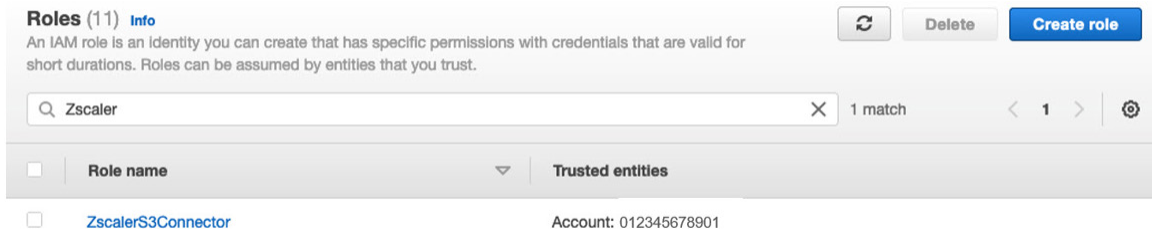


Figure 9. Roles

2. Click the **Trust relationships** tab, and then click **Edit trust relationship**.

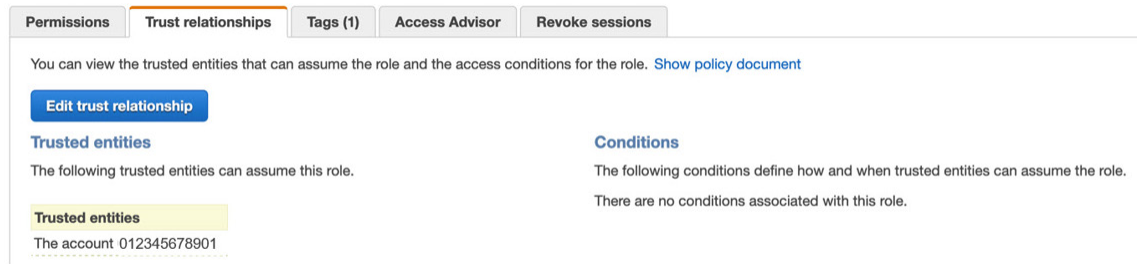


Figure 10. Trust relationships

3. Under **Policy Document**, replace the default AWS value with the **Zscaler Connector User ARN** that you copied earlier and click **Update Trust Policy**.



Figure 11. Policy document

4. Under **Summary**, copy the **Role ARN** for later use (as the IAM Role ARN).

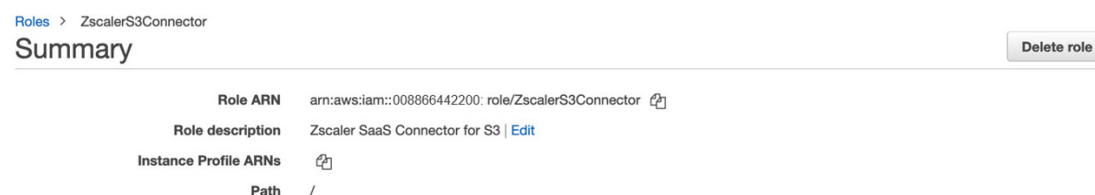


Figure 12. Role ARN

AWS Configuration (CloudTrail)

The next steps are also documented in the [Adding SaaS Application Tenants](#) help page (government agencies, see [Adding SaaS Application Tenants](#)) in the **Obtain the CloudTrail Bucket ARN** section.



The S3 bucket selected for the trail won't be available to scan in the **SaaS Security Scan Configuration**, as it is marked **Internal**.

1. Go to **Services > CloudTrail**, and click **Trails** located in the left-side navigation.

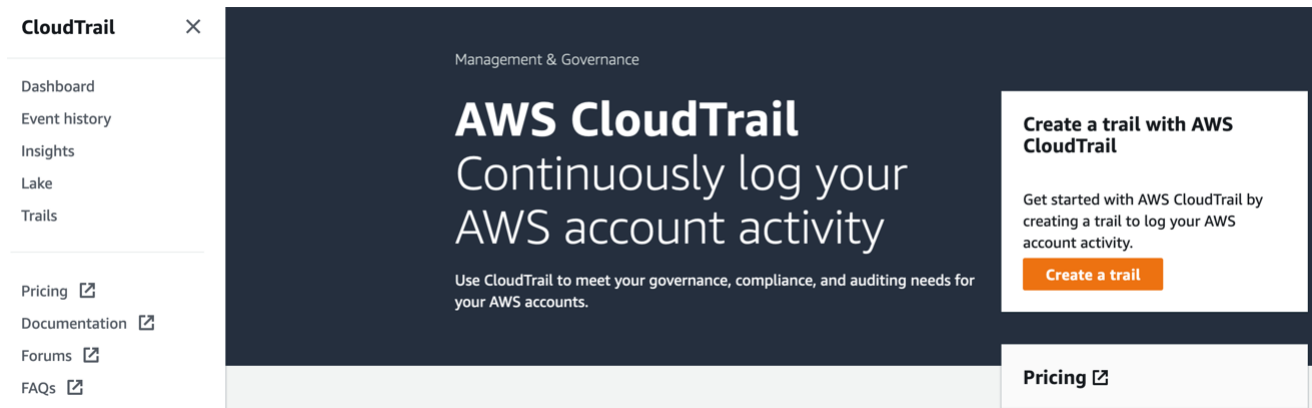


Figure 13. Create a CloudTrail



In the [Adding SaaS Application Tenants](#) help (government agencies, see [Adding SaaS Application Tenants](#)), **step iii** under **section c** shows an existing trail. If you don't already have a trail, you must create one. See [Appendix A: Create Trail](#) on how to create a trail before proceeding.

2. Select the trail name to use from the list.

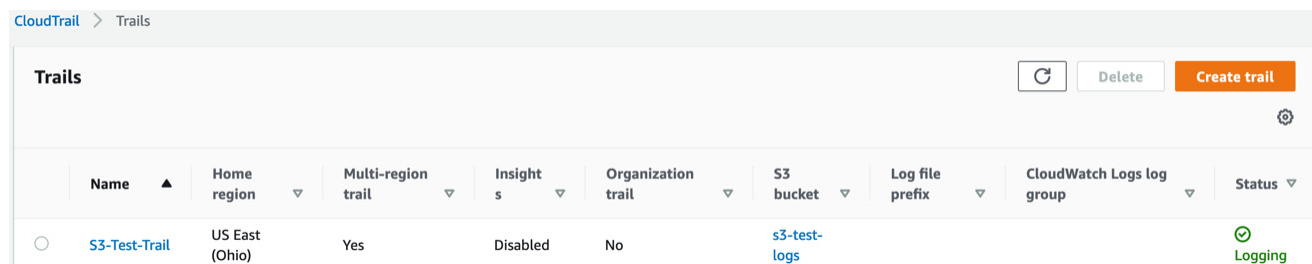


Figure 14. Select CloudTrail name

3. Click the Trail log location (in blue) in **General details**.

S3-Test-Trail Delete Stop logging

General details Edit

Trail logging Logging	Trail log location s3-test-logs/AWSLogs/008866442200	Log file validation Enabled	SNS notification delivery Disabled
Trail name S3-Test-Trail	Last log file delivered January 18, 2022, 15:30:09 (UTC-06:00)	Last file validation delivered -	Last SNS notification -
Multi-region trail Yes	Log file SSE-KMS encryption Not enabled		
Apply trail to my organization Not enabled			

Figure 15. CloudTrail general details

4. On the **Objects** tab, click the **CloudTrail/** name.

Objects **Properties**

Objects (2)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Refresh Copy S3 URI Copy URL Download Open Delete Actions Create folder

Upload

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	CloudTrail-Digest/	Folder	-	-	-
<input type="checkbox"/>	CloudTrail/	Folder	-	-	-

Figure 16. CloudTrail objects

5. Click the **Properties** tab, and copy the **Amazon Resource Name (ARN)** to use later (as the CloudTrail Bucket ARN).

Objects **Properties**

Folder overview

AWS Region US East (Ohio) us-east-2	S3 URI s3://s3-test-logs/AWSLogs/008866442200/CloudTrail/	Amazon Resource Name (ARN) arn:aws:s3:::s3-test-logs/AWSLogs/008866442200/CloudTrail/
---	--	--

Figure 17. CloudTrail properties

AWS Configuration (Quarantine Bucket)

The next steps are documented in the [Adding SaaS Application Tenants](#) help page in the **Create a Quarantine Bucket** section.



In the **Amazon S3** area of [Adding SaaS Application Tenants](#), (government agencies, see [Adding SaaS Application Tenants](#)) **step ii** of **Create a Quarantine Bucket** details creating a new bucket to use for quarantined files. If you already have a bucket, you don't need to create one. However, verify that the following settings match **step iii** of the procedure described in the online documentation. A directory called Zscaler_Quarantine is created in this bucket, but only when malware files are quarantined.

- **Block all public access:** Select.
- **Bucket Versioning:** Disable.
- **Server-side encryption:** Disable.

The S3 bucket selected for use with the quarantined files is not available in the SaaS Security Scan Configuration and is marked **Internal**.

1. Go to **Services > S3** and click **Buckets** in the left-side navigation.
2. Record the name of the S3 bucket identified as the **Quarantine bucket** (either existing or newly created). You must refer to this name later.

Buckets (4) [Info](#) Refresh Copy ARN Empty Delete Create bucket

Buckets are containers for data stored in S3. [Learn more](#)

Search: 1 match

	Name ▲	AWS Region ▼	Access ▼	Creation date ▼
<input type="radio"/>	s3-test-logs	US East (Ohio) us-east-2	Bucket and objects not public	January 18, 2022, 10:18:22 (UTC-06:00)

Figure 18. Buckets configuration

Finish Zscaler Configuration

To complete the Zscaler configuration:

1. From the ZIA Admin Portal, go to **Administration > SaaS Application Tenants**.
2. Click **Add SaaS Application Tenant**.
3. Enter the details for the fields in **step 4 (Register the SaaS Application)**.
4. Click **Save**.



- You can find your AWS Account ID in the user details in the upper right-hand corner of the AWS Management Console. You can find Information on how to obtain your AWS Account ID in the [AWS docs](#).
- The **Quarantine Bucket Name** is the name that you copied in the **Quarantine Bucket** configuration.
- The **IAM Role ARN** is the role ARN that you copied earlier during the **Trust Relationship** configuration.
- The **CloudTrail Bucket ARN** is the Amazon Resource Name (ARN) that you copied earlier during the **CloudTrail** configuration.

4 Register the SaaS Application

Enter the Zscaler S3 Connector details so the Zscaler service can connect to Amazon S3. [Learn more](#)

AWS Account ID	IAM Role ARN
0088-6644-2200	iam::008866442200:role/ZscalerS3Connector
Quarantine Bucket Name	CloudTrail Bucket ARN
s3-test-logs	s3-test-logs/AWSLogs/008866442200/CloudTrail/

Figure 19. Register the SaaS Application

5. Save and activate so the status is **Validating**.

No.	Application	Tenant Name	Status
1	Amazon S3	S3 Tenant	● Validating

Figure 20. S3 Tenant validating

6. After a short period, when access is successful, the status is **Active**. Proceed with configuring policy.

No.	Application	Tenant Name	Status
1	Amazon S3	S3 Tenant	● Active

Figure 21. S3 Tenant active

Integrating Zscaler Cloud NSS with Amazon S3

This section provides information for integrating Zscaler Cloud Nanolog Streaming Service (NSS) and Amazon S3.

With a subscription to Zscaler's Cloud NSS, you can enable direct cloud-to-cloud streaming of ZIA traffic logs into Amazon S3. Log data is stored in S3 in containers called buckets.

The integration of Cloud NSS and Amazon S3 provides long-term log retention, preprocessing of log data before ingestion, and compatibility with analytics solutions that can easily read log data from S3 buckets.

To learn more about the geoavailability and qualifications for Cloud NSS, contact Zscaler Support.

Create a User Group in AWS IAM

To create an AWS IAM user group:

1. Log in to the AWS Management Console.
2. In the search bar, enter **IAM** and select **IAM**.

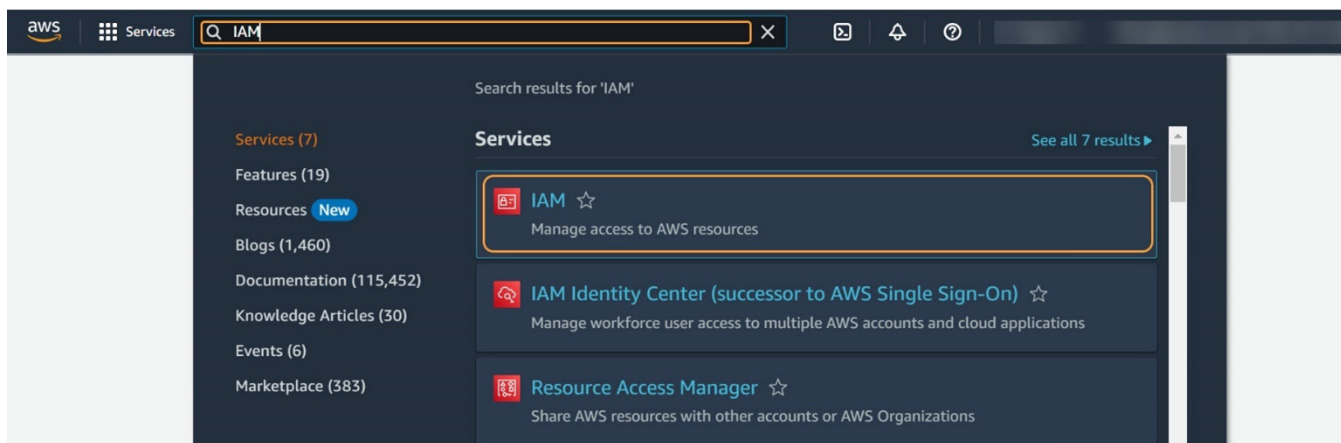


Figure 22. Search for Identity and Access Management (IAM) in AWS Management Console

3. In the left-side navigation, go to **Access Management** > **User groups**.

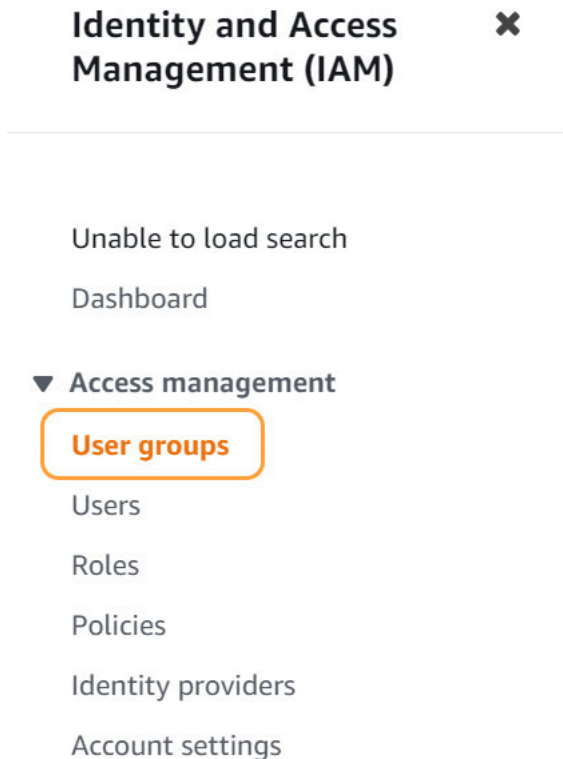


Figure 23. AWS IAM menu with User groups selected

4. Click **Create group**. The **Create user group** page appears.

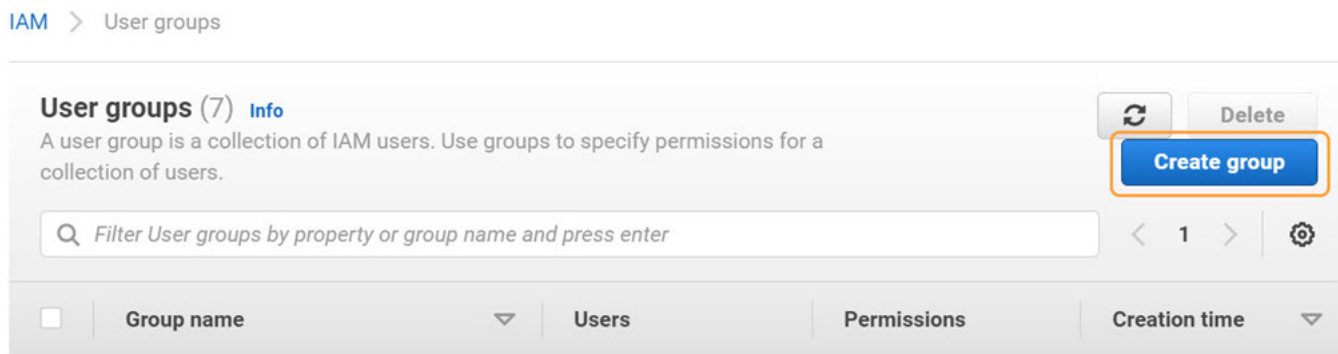


Figure 24. User groups page in AWS IAM with Create group button selected

5. On the **Create user group** page, create a user group:
 - a. Enter a name for the user group (e.g., `Zscaler_Group_Test`).

[IAM](#) > [User groups](#) > Create user group

Create user group

Name the group

User group name

Enter a meaningful name to identify this group.

Maximum 128 characters. Use alphanumeric and '+=, @-_' characters.

Figure 25. Create user group wizard in AWS IAM showing Name the group field

- b. Skip the options to add users and attach permissions policies.
 - c. Click **Create group**. You are redirected to the **User groups** page and a success message appears.



[IAM](#) > [User groups](#)

Figure 26. Success message in AWS IAM after a user group was created

Create a User and Access Key in AWS IAM

To create a user and access key in AWS IAM:

1. In the left-side navigation of IAM, go to **Access Management > Users**.

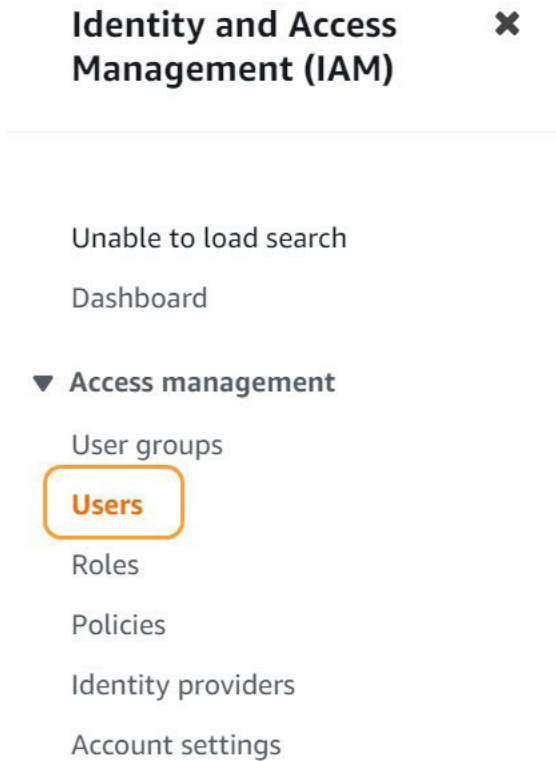


Figure 27. AWS IAM menu with Users selected

2. Click **Add users**. The **Create user** wizard appears.

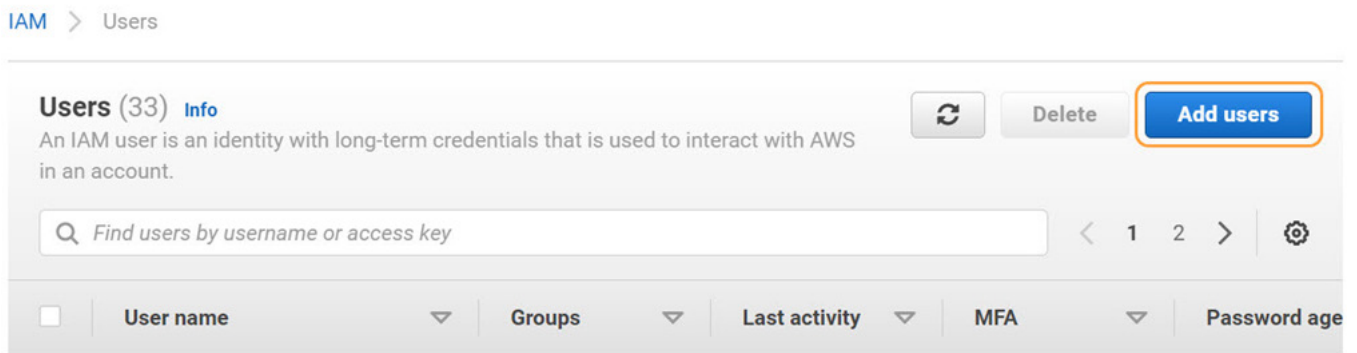


Figure 28. Users page in AWS IAM with Add users button selected

3. In the **Create user** wizard, create a user:
 - a. Enter a user name (e.g., `Zscaler_User_Test`), then click **Next**.

IAM > Users > Create user

Step 1

Specify user details

Step 2

Set permissions

Step 3

Review and create

Specify user details

User details

User name

Zscaler_User_Test

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☐ Enable console access - optional

Enables a password that allows users to sign in to the AWS Management Console.

[For programmatic access, you can generate access keys after you create the user. Learn more](#)

Cancel

Next

Figure 29. Set user details field in AWS IAM

- b. Add the user to the newly created user group (e.g., `Zscaler_Group_Test`), then click **Next**.

IAM > Users > Create user

Step 1

Specify user details

Step 2

Set permissions

Step 3

Review and create

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

☒ Add user to group

Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ Copy permissions

Copy all group memberships, attached managed policies, and inline policies from an existing user.

☐ Attach policies directly

Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

User groups (1/10)

Q Zscaler_Group X



Create group

1 match < 1 >

<input checked="" type="checkbox"/>	Group name	Users	Attached policies	Created
<input checked="" type="checkbox"/>	Zscaler_Group_Test	0	None	2022-12-13 (1 mont...

► Permissions boundary - optional

Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. [Learn more](#)

Cancel

Previous

Next

Figure 30. Adding a user to a user group in AWS IAM

- c. Review your choices, then click **Create user**.

Permissions summary

< 1 >

Name	Type	Used as
Zscaler_Group_Test	Group	Permissions group

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

Cancel Previous **Create user**

Figure 31. Create user wizard in AWS IAM

You are redirected to the **Users** page and a success message appears.

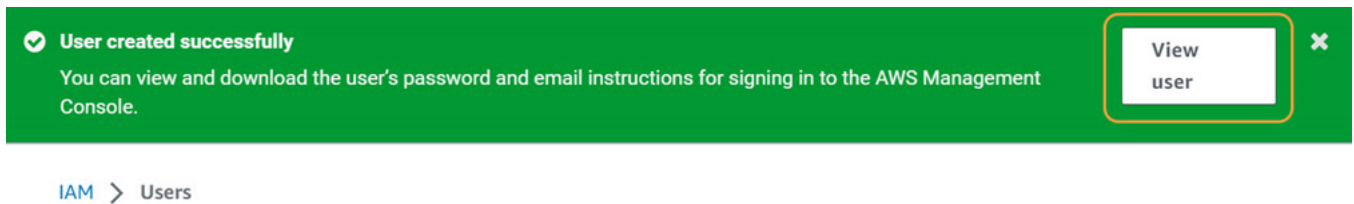


Figure 32. Success message in AWS IAM after a user was created

4. Click **View user** in the success message, or use the search bar to find the user by name, then select the new user.

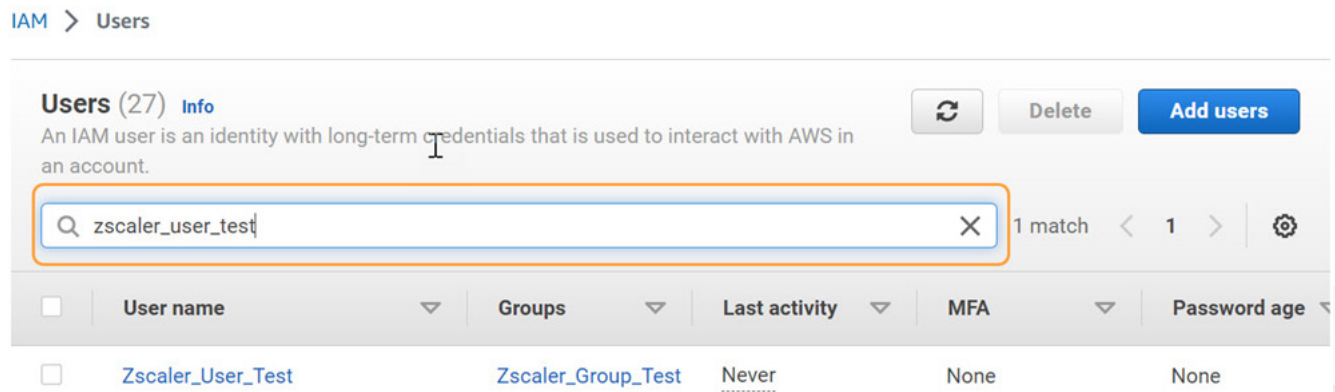


Figure 33. Users page in AWS IAM with search bar

5. On the **Summary** page for the newly created user, scroll down and click the **Security credentials** tab.

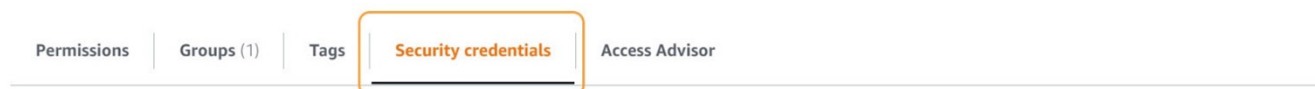


Figure 34. Security credentials tab in user Summary page in AWS IAM

6. On the **Security credentials** tab, scroll down to the **Access keys** section and click **Create access key**. The **Create access key** wizard appears.

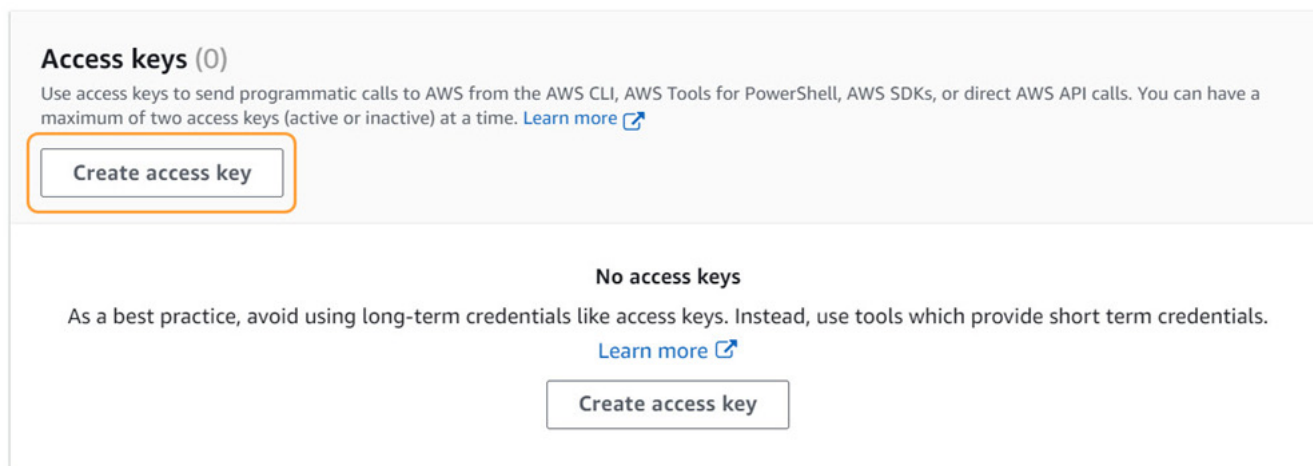


Figure 35. Access keys section in the Security credentials tab on the user Summary page in AWS IAM

7. In the **Create access key** wizard, create an access key:

a. Select a use case, then click **Next**.

Step 1

Access key best practices & alternatives

Step 2 - optional

Set description tag

Step 3

Retrieve access keys

Access key best practices & alternatives

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

☐ **Command Line Interface (CLI)**

You plan to use this access key to enable the AWS CLI to access your AWS account.

☐ **Local code**

You plan to use this access key to enable application code in a local development environment to access your AWS account.

☐ **Application running on an AWS compute service**

You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

☐ **Third-party service**

You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

☐ **Application running outside AWS**

You plan to use this access key to enable an application running on an on-premises host, or to use a local AWS client or third-party AWS plugin.

☒ **Other**

Your use case is not listed here.



It's okay to use an access key for this use case, but follow the best practices:

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access keys when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the [Best practices for managing AWS access keys](#).

Cancel

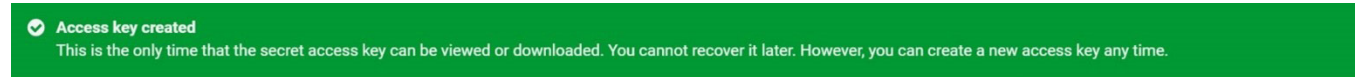
Next

Figure 36. Create access key wizard in AWS IAM

- b. Click **Create access key**.

Figure 37. Create access key wizard in AWS IAM with Create access key button selected

A success message appears.



IAM > Users > Zscaler_User_Test > Create access key

Figure 38. Success message in AWS IAM after an access key was created

- c. Click **Download .csv file** to download and save a CSV file containing the access key ID and secret access key required for creating a Cloud NSS feed in the ZIA Admin Portal.

Figure 39. Download .csv file button in Create user wizard in AWS IAM



This is the only time that you can view or download the secret access key.

- d. Click **Done** to close the **Create access key** wizard.

Create an S3 Bucket and Folder in Amazon S3

To create an S3 bucket and folder in Amazon S3:

1. In the search bar at the top of the screen, enter S3 and select **S3**.

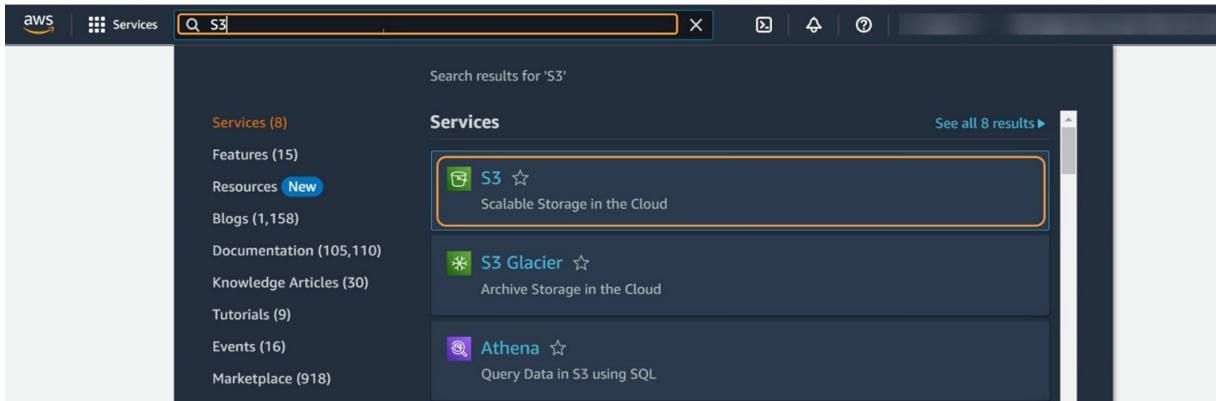


Figure 40. Search for S3 in AWS Management Console

2. In the left-side navigation, go to **Buckets**.

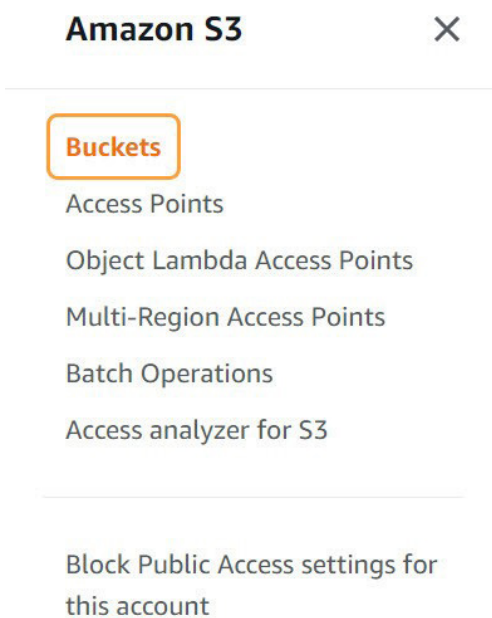


Figure 41. Amazon S3 menu with Buckets selected

3. Click **Create bucket**. The **Create bucket** page appears.

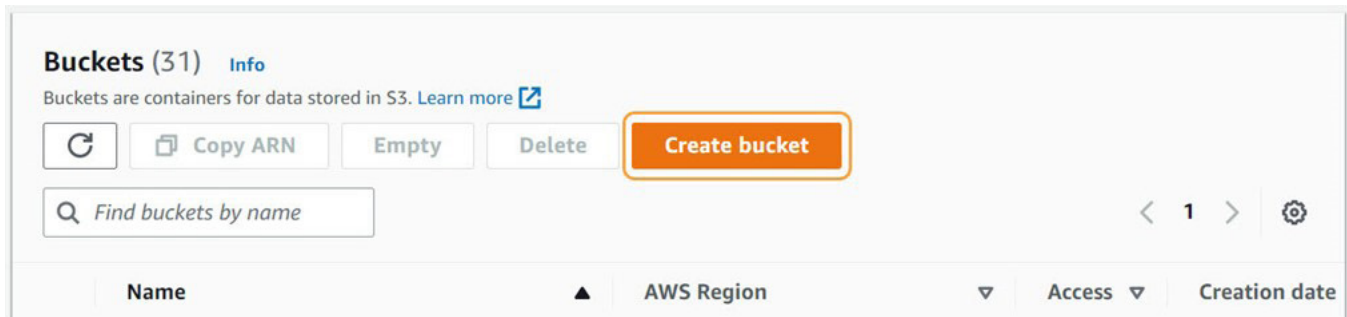


Figure 42. Buckets page in Amazon S3 with Create bucket button selected

4. On the **Create bucket** page, create a bucket:
 - a. Enter a name for the bucket (e.g., `zscaler-bucket-test`). The bucket name is part of its Amazon Resource Name (ARN), which is required for creating a policy in AWS.

Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name

zscaler-bucket-test

Bucket name must be globally unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

Figure 43. Create bucket wizard in Amazon S3 with Bucket name field



S3 buckets cannot use an underscore (`_`) due to Amazon S3 bucket naming convention. Please use a hyphen (`-`) if you want separation in the S3 name characters.

- b. Select your **AWS Region**. The region is part of the URL required for creating a Cloud NSS feed in the ZIA Admin Portal.

General configuration

Bucket name

zscaler-bucket-test

Bucket name must be globally unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region

US West (Oregon) us-west-2

Figure 44. Create bucket wizard in Amazon S3 with AWS Region field

- c. (Optional) Maintain the default configurations for the remaining settings (e.g., **Bucket Versioning**, **Default encryption**, etc.).
 - d. Click **Create bucket**.

After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel

Create bucket

Figure 45. Create bucket button in Amazon S3

You are redirected to the **Buckets** page and a success message appears.

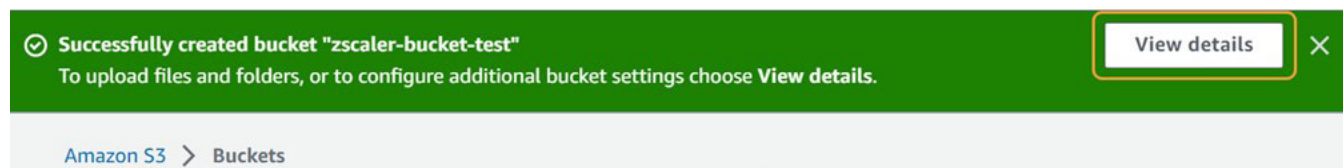


Figure 46. Success message in Amazon S3 after a bucket was created

- Click **View details** in the success message, or use the search bar to find the bucket by name, then select the new bucket.

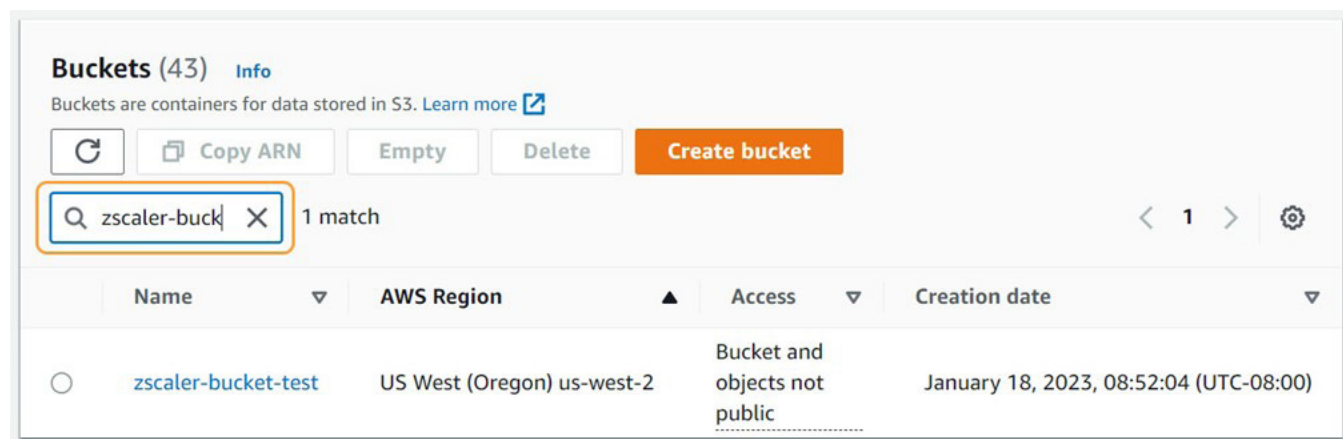


Figure 47. Search for bucket in Amazon S3

- On the **Objects** tab of the bucket page, click **Create folder**. The **Create folder** page appears.

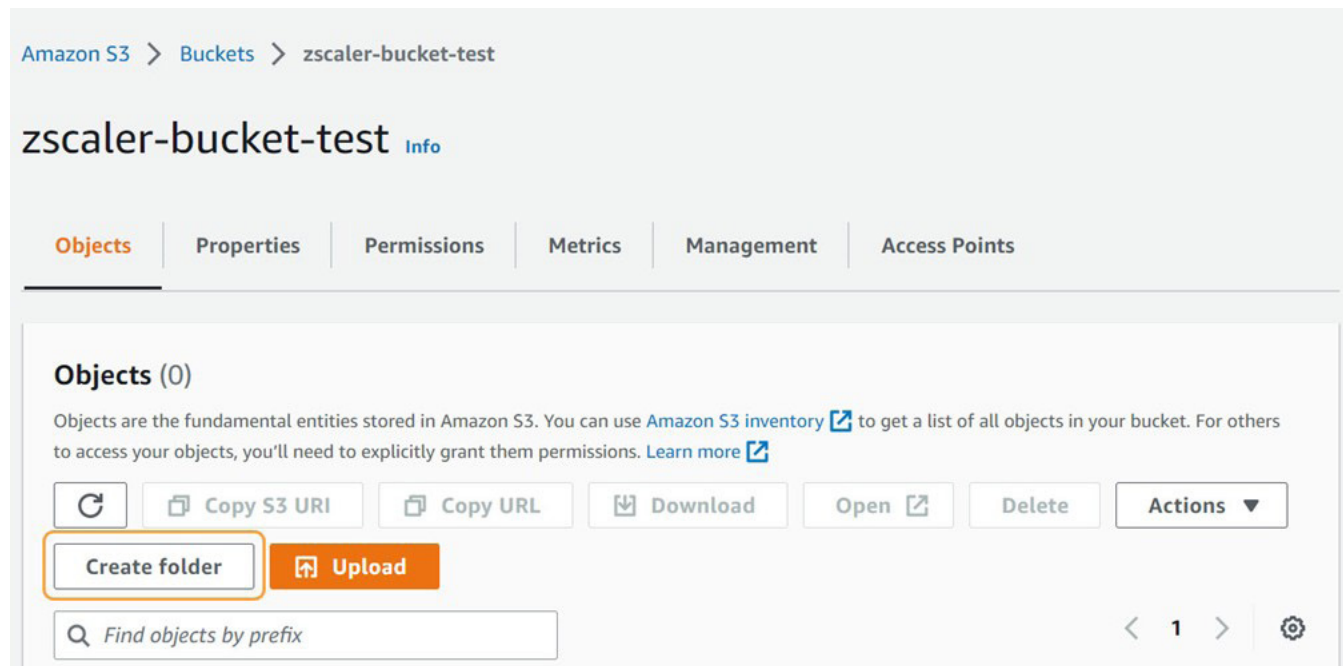


Figure 48. Bucket overview page in Amazon S3 with Create folder button selected

7. On the **Create folder** page, create a folder:
 - a. Enter a **Folder name** (e.g., logs-test).

Amazon S3 > Buckets > zscaler-bucket-test > Create folder

Create folder [Info](#)

Use folders to group objects in buckets. When you create a folder, S3 creates an object using the name that you specify followed by a slash (/). This object then appears as folder on the console. [Learn more](#)

ⓘ Your bucket policy might block folder creation

If your bucket policy prevents uploading objects without specific tags, metadata, or access control list (ACL) grantees, you will not be able to create a folder using this configuration. Instead, you can use the [upload configuration](#) to upload an empty folder and specify the appropriate settings.

Folder

Folder name

 /

Folder names can't contain "/". See rules for naming [↗](#)

[Cancel](#) [Create folder](#)

Figure 49. Create folder page in Amazon S3 showing the Folder name field

- b. Maintain the default **Server-side encryption** settings and click **Create folder**.

Server-side encryption

Server-side encryption protects data at rest.

ⓘ The following settings apply only to the new folder object and not to the objects contained within it.

Encryption key type [Info](#)

☒ Amazon S3-managed keys (SSE-S3)

☐ AWS Key Management Service key (SSE-KMS)

[Cancel](#) [Create folder](#)

Figure 50. Create folder page in Amazon S3 with Create folder button selected

You are redirected to the bucket page and a success message appears.



Figure 51. Success message in Amazon S3 after a folder was created

8. Select the folder and click **Copy URL**. Save the URL (e.g., `https://zscaler-bucket-test.s3.us-west-2.amazonaws.com/logs-test/`) required for creating a Cloud NSS feed in the ZIA Admin Portal. The name of your region (e.g., `us-west-2`) must be present in the URL.

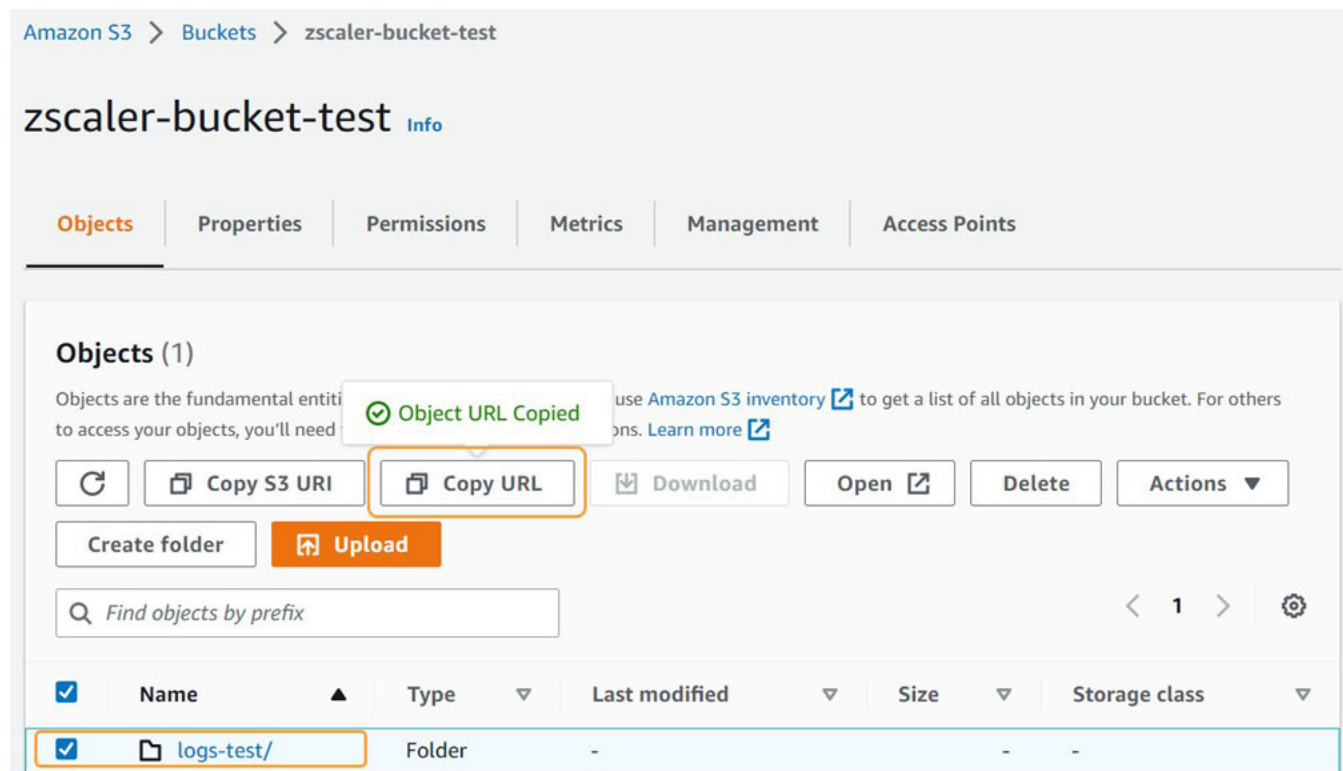


Figure 52. Bucket overview page in Amazon S3 with folder and Copy URL button selected

- Click the **Properties** tab, then copy and save the ARN (e.g., `arn:aws:s3:::zscaler-bucket-test`) required for creating a policy in AWS.

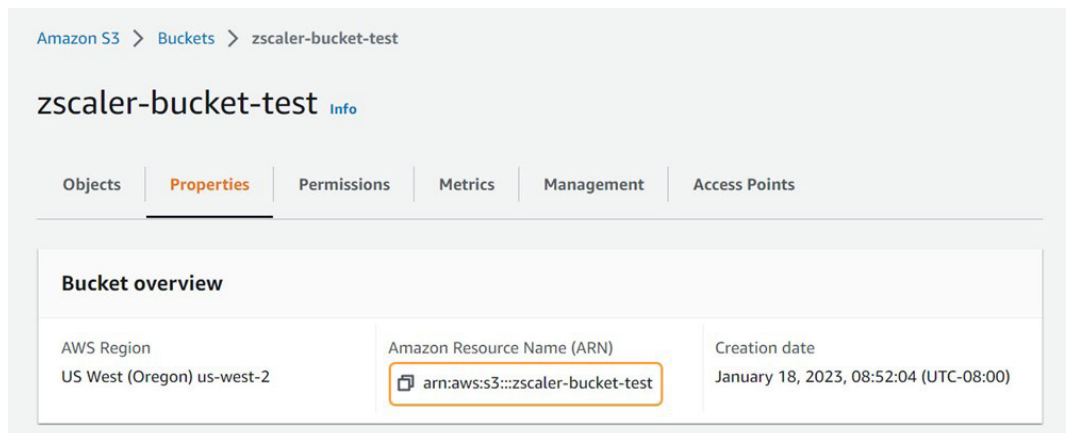


Figure 53. Bucket Properties and ARN in Amazon S3

Create a Policy Granting the User Group Access to the S3 Bucket in Amazon IAM

A policy is a JSON document in AWS that specifies who has access to AWS resources and what actions they can perform on those resources. You can attach a policy to an identity (e.g., user group) or resource (e.g., S3 bucket) to define its permissions. To learn more, refer to the [AWS documentation](#).

To integrate with Cloud NSS, the user group (e.g., `Zscaler_Group_Test`) needs permission to perform the `PutObject` action on the S3 bucket (e.g., `zscaler-bucket-test`). The `PutObject` action adds an object to a bucket. The user must have `WRITE` permissions to perform the `PutObject` action. To learn more, refer to the [AWS API Reference documentation](#).

To create a policy granting the user group `PutObject` access to the S3 bucket:

- Go to the IAM Management Console.
- In the left-side navigation, go to **Access management > Policies**.

Identity and Access Management (IAM)

Unable to load search

Dashboard

▼ Access management

User groups

Users

Roles

Figure 54. AWS IAM menu with Policies selected

3. Click **Create policy**. The **Create policy** wizard appears.

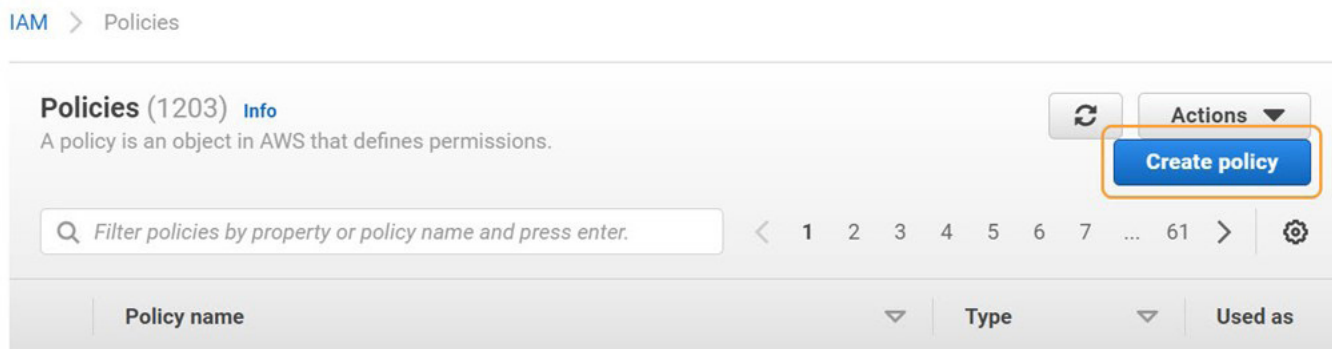


Figure 55. Policies page in AWS IAM with Create policy button selected

4. In the **Create policy** wizard, create a policy:
 - a. Click the **JSON** tab.

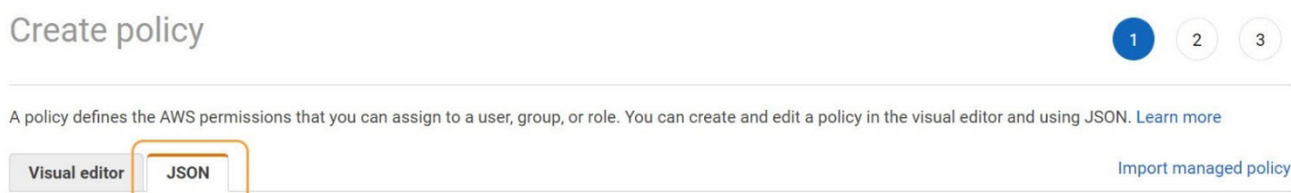


Figure 56. Create policy wizard in AWS IAM showing JSON tab

- b. In the **JSON editor**, write a policy that allows PutObject access to the S3 bucket (e.g., zscaler-bucket-test). See the following example.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PutObjectActions",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::zscaler-bucket-test/*"
      ]
    }
  ]
}
```

- c. Click **Next: Tags**.
- d. Click **Next: Review**.

Create policy

1 2 3

Add tags - optional
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add tag

You can add up to 50 more tags.

Cancel Previous **Next: Review**

Figure 57. Create policy wizard in AWS IAM showing Tags screen

- e. Enter a name for the policy (e.g., `zscaler_policy_test`).

Review policy

Name* zscaler_policy_test

Use alphanumeric and '+=, @-.' characters. Maximum 128 characters.

Description

Maximum 1000 characters. Use alphanumeric and '+=, @-.' characters.

Figure 58. Review policy page in AWS IAM showing Name field

- f. Review the policy **Summary** information and click **Create policy**.

Summary

Filter

Service	Access level	Resource	Request condition
Allow (1 of 363 services) Show remaining 362			
S3	Limited: Write	BucketName string like zscaler_policy_test, ObjectPath string like All	None

Tags

Key	Value
No tags associated with the resource.	

Cancel Previous **Create policy**

Figure 59. Policy Summary page in AWS IAM with Create policy button selected

You are redirected to the **Policies** page and a success message appears.



[IAM](#) > Policies

Figure 60. Success message in AWS IAM after a policy was created

5. Attach the policy to the newly created user group:

- a. Click the link in the success message, or use the search bar to filter the policies by name, then select the new policy (e.g., `zscaler_policy_test`). The policy **Summary** page appears.

[IAM](#) > Policies

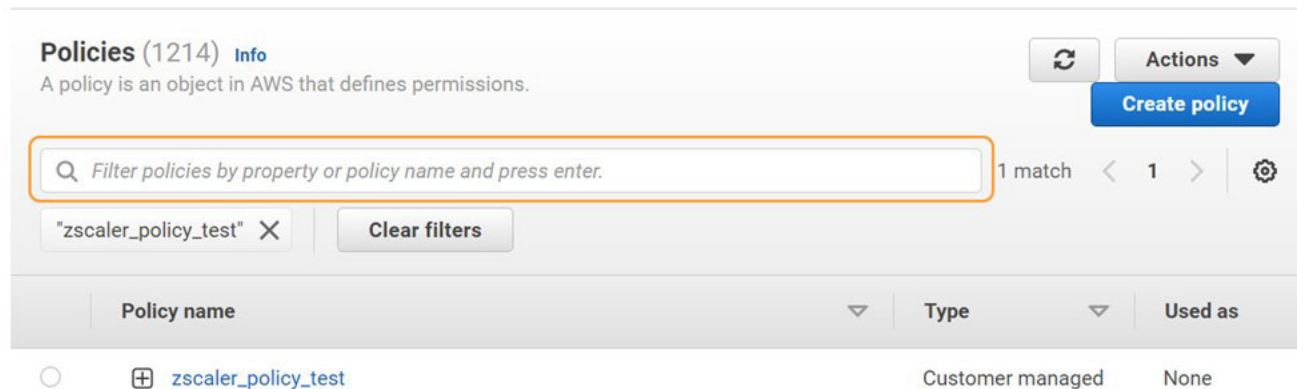


Figure 61. Search for policy in AWS IAM

- b. On the policy **Summary** page, click the **Policy usage** tab, then click **Attach**. The **Attach policy** page appears.

[Policies](#) > `zscaler_policy_test`

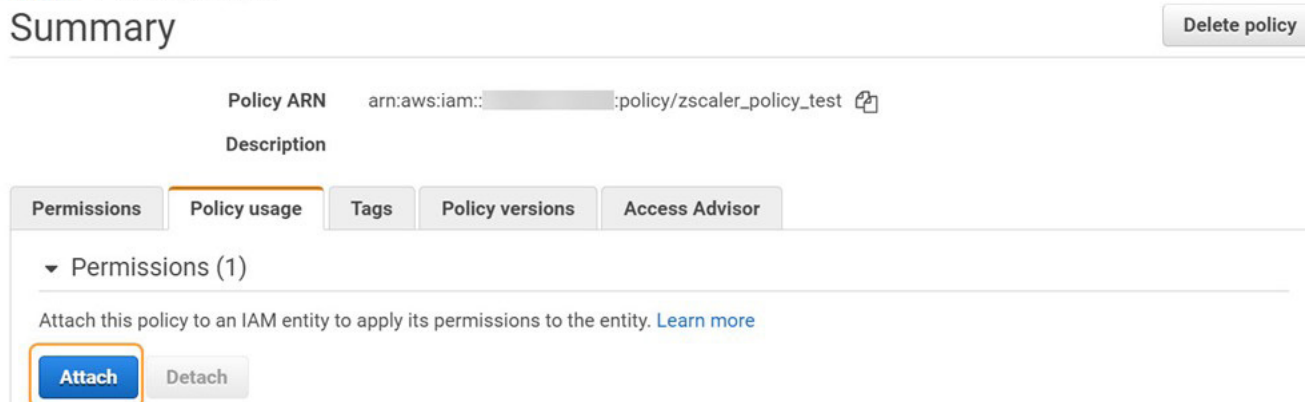


Figure 62. Attach button in Policy usage tab in AWS IAM

- c. On the **Attach policy** page, search for and select the newly created user group (e.g., `zscaler_group_test`), then click **Attach policy**.

Attach policy

Attach the policy to users, groups, or roles in your account

Filter: Filter	Q zscaler_group_test	Showing 1 result
<input checked="" type="checkbox"/> Name	Type	
<input checked="" type="checkbox"/> Zscaler_Group_Test	Group	

Cancel

Attach policy

Figure 63. Attach policy page with user group selected for attachment in AWS IAM

You are redirected to the **Summary** page, which shows the user group (e.g., `zscaler_group_test`) under **Permissions**.

[Policies](#) > `zscaler_policy_test`

Summary

Delete policy

Policy ARN `arn:aws:iam:::policy/zscaler_policy_test`

Description

Permissions Policy usage Tags Policy versions Access Advisor

Permissions (1)

Attach this policy to an IAM entity to apply its permissions to the entity. [Learn more](#)

Attach

Detach

Filter: Filter

Q Search

Showing 1 result

☐ Name

Type

☐ Zscaler_Group_Test

Group

Figure 64. Policy Summary page in AWS IAM with user group attached

Add a Cloud NSS Feed in the ZIA Admin Portal

See [Adding Cloud NSS Feeds](#) (government agencies, see [Adding Cloud NSS Feeds](#)) and select the type of feed (e.g., Web Logs) that you want to configure. The following fields require specific inputs:

- **SIEM Type:** Select **S3**.
- **AWS Access Id:** Enter the access key ID for the user created in AWS.
- **AWS Secret Key:** Enter the secret access key for the user created in AWS.
- **Max Batch Size:** Enter the recommended maximum batch size based on the log type. For Web and Firewall log types, the recommended maximum batch size is 8 MB. For DNS, Tunnel, and all other log types (e.g., SaaS Security), it is 1 MB.
- **S3 Folder URL:** Enter the URL of the folder created in the S3 bucket (e.g., `https://zscaler-bucket-test.s3.us-west-2.amazonaws.com/logs-test/`).
- **Feed Output Type:** Select **JSON**.
- **Feed Escape Character:** Enter `,` `\` (comma, backslash, quote).
- **Feed Output Format:** Zscaler recommends adding `"time": "%d{epochtime}"` to the **Feed Output Format**. See the following feed output formats by log type.
 - For [Cloud NSS Feeds for Web Logs](#) (government agencies, see [Cloud NSS Feeds for Web Logs](#)), copy and paste the prepopulated **Feed Output Format** with the following:

```
\{"time" : "%d{epochtime}", "act": "%s{action}", "reason": "%s{reason}",
"app": "%s{proto}", "dhost": "%s{ehost}", "dst": "%s{sip}", "src": "%s{cintip}",
"sourceTranslatedAddress": "%s{cip}", "in": "%d{respsize}", "out": "%d{reqsize}",
"request": "%s{eurl}", "requestContext": "%s{ereferer}", "outcome": "%s{respcode}",
"requestClientApplication": "%s{ua}", "requestMethod": "%s{reqmethod}",
"suser": "%s{ellogin}", "spriv": "%s{elocation}", "externalId": "%d{recordid}",
"fileType": "%s{filetype} ", "destinationServiceName": "%s{appname}",
"cat": "%s{urlcat}", "deviceDirection": "1", "cn1": "%d{riskscore}",
"cn1Label": "riskscore", "cs1": "%s{dept}", "cs1Label": "dept",
"cs2": "%s{urlcat}", "cs2Label": "urlcat", "cs3": "%s{malwareclass}",
"cs3Label": "malwareclass", "cs4": "%s{malwarecat}", "cs4Label": "malwarecat",
"cs5": "%s{threatname}", "cs5Label": "threatname", "cs6": "%s{bamd5}",
"cs6Label": "md5hash", "rulelabel": "%s{rulelabel}", "ruletype": "%s{ruletype}",
"urlclass": "%s{urlclass}", "DeviceVendor": "Zscaler" , "DeviceProduct": "NSSWeblog"
,"devicemodel": "%s{devicemodel}"}\}
```



PDF files add line breaks to preserve the source text formatting. When copying code from a PDF into the Feed Output Format, you must remove any line breaks from the text.

Copy the code text and paste it into [this tool](#) (or one similar) to remove the line breaks. When cleaned, copy the code from the tool and paste it into the Feed Output Format.

- For [Cloud NSS Feeds for Firewall Logs](#) (government agencies, see [Cloud NSS Feeds for Firewall Logs](#)) copy and paste the prepopulated **Feed Output Format** with the following:

```
\{"datetime":"%s{time}","user":"%s{ellogin}","department":"%s{edepartment}","locationname":"%s{elocation}","cdport":"%d{cdport}","csport":"%d{csport}","sdport":"%d{sdport}","ssport":"%d{ssport}","csip":"%s{csip}","cdip":"%s{cdip}","ssip":"%s{ssip}","sdip":"%s{sdip}","tsip":"%s{tsip}","tunsport":"%d{tsport}","tuntype":"%s{ttype}","action":"%s{action}","dnat":"%s{dnat}","stateful":"%s{stateful}","aggregate":"%s{aggregate}","nwsvc":"%s{nwsvc}","nwapp":"%s{nwapp}","proto":"%s{ipproto}","ipcat":"%s{ipcat}","destcountry":"%s{destcountry}","avgduration":"%d{avgduration}","rulelabel":"%s{erulelabel}","inbytes":"%ld{inbytes}","outbytes":"%ld{outbytes}","duration":"%d{duration}","durationms":"%d{durationms}","numsessions":"%d{numsessions}","ipsrulelabel":"%s{ipsrulelabel}","threatcat":"%s{threatcat}","threatname":"%s{ethreatname}","deviceowner":"%s{deviceowner}","devicehostname":"%s{devicehostname}"\}
```



PDF files add line breaks to preserve the source text formatting. When copying code from a PDF into the Feed Output Format, you must remove any line breaks from the text.

Copy the code text and paste it into [this tool](#) (or one similar) to remove the line breaks. When cleaned, copy the code from the tool and paste it into the Feed Output Format.

- For [Cloud NSS Feeds for DNS Logs](#) (government agencies, see [Cloud NSS Feeds for DNS Logs](#)) copy and paste the prepopulated **Feed Output Format** with the following:

```
\{"datetime":"%s{time}","user":"%s{ellogin}","department":"%s{edepartment}","location":"%s{elocation}","reqaction":"%s{reqaction}","resaction":"%s{resaction}","regrulelabel":"%s{regrulelabel}","resrulelabel":"%s{resrulelabel}","dns_reqtype":"%s{reqtype}","dns_req":"%s{req}","dns_resp":"%s{res}","srv_dport":"%d{sport}","durationms":"%d{durationms}","clt_sip":"%s{cip}","srv_dip":"%s{sip}","category":"%s{domcat}","respipcategory":"%s{respipcat}","deviceowner":"%s{deviceowner}","devicehostname":"%s{devicehostname}"\}
```



When logs are streaming, Zscaler creates a file for every batch of logs with the following path (id1 and id2 represent internal IDs): S3bucket/feedtype/feedname=feed_name/year=YYYY/month=MM/day=DD/epochtime_id1_id2_samesecondcount

See the following example: zscaler-bucket-test/_weblog/feedname=s3test_feed/year=2023/month=01/day=23/1674506076_40960_24_2

If you do not include %d{epochtime} in the **Feed Output Format**, the file path substitutes ingestiontime for epochtime. Ingestion time is when the NSS uploads the feed to the S3 bucket.

You can specify the file extension (e.g., GZIP) of the log data stored in your configured S3 bucket, according to your integration requirements. To enable and set the file extension, contact Zscaler Support.

If you require further assistance, contact Zscaler Support.

Appendix A: Create Trail

Create a trail under **Services > CloudTrail > Trails** by clicking **Create trail**.

1. Enter a name for the trail and either choose an existing S3 bucket to use or create a new S3 bucket. The **Log file SSE-KMS encryption** option is enabled by default. In this example, it is disabled. (If you chose to leave it enabled, refer to the **Info** link in the UI for more information.)
2. Click **Next**.

Choose trail attributes

General details

A trail created in the console is a multi-region trail. [Learn more](#)

Trail name
Enter a display name for your trail.

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

☐ Enable for all accounts in my organization
To review accounts in your organization, open AWS Organizations. [See all accounts](#)

Storage location [Info](#)

☐ Create new S3 bucket
Create a bucket to store logs for the trail.

☒ Use existing S3 bucket
Choose an existing bucket to store logs for this trail.

Trail log bucket name
Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

Prefix - optional

Logs will be stored in s3-test-logs/AWSLogs/008866442200

Log file SSE-KMS encryption [Info](#)

☐ Enabled

Figure 65. CloudTrail general details

3. Select the **Events > Event types** that you want to log, and the **Data event > Data event type** to use as the source. In the following example, it is **S3**.

4. Click **Next**. The following figure shows a management event.

Choose log events

Events [Info](#)
 Record API activity for individual resources, or for all current and future resources in AWS account. [Additional charges apply](#)

Event type
 Choose the type of events that you want to log.

☒ **Management events**
Capture management operations performed on your AWS resources.

☒ **Data events**
Log the resource operations performed on or within a resource.

☒ **Insights events**
Identify unusual activity, errors, or user behavior in your account.

Management events [Info](#)
 Management events show information about management operations performed on resources in your AWS account.

i No additional charges apply to log management events on this trail because this is your first copy of management events.

API activity
 Choose the activities you want to log.

☒ **Read** ☒ **Write**

☐ **Exclude AWS KMS events**

☐ **Exclude Amazon RDS Data API events**

Figure 66. Management events

The following image shows a data event.

▼ Data event: S3 Remove

Data event type
 Choose the source of data events to log.

S3 ▼

Log selector template

Log all events ▼

Figure 67. Data event

5. Click **Create trail**.

Appendix B: Testing Notes

Configuring the Data at Rest Scanning Policy is documented in the [Understanding the Data at Rest Scanning Policy](#) help page (government agencies, see [Understanding the Data at Rest Scanning Policy](#)).

When configuring the **Data Loss Prevention** and the **Malware Detection** policy, you must select **Public Cloud Storage** at the top of each page to create a policy for your S3 SaaS application tenant. The following figure shows DLP scans:

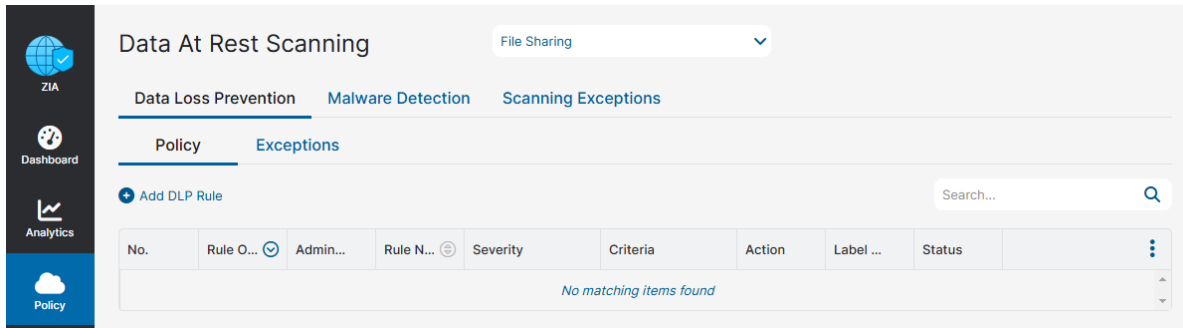


Figure 68. Data at Rest Scanning Policy – DLP

The following figure shows malware scans:

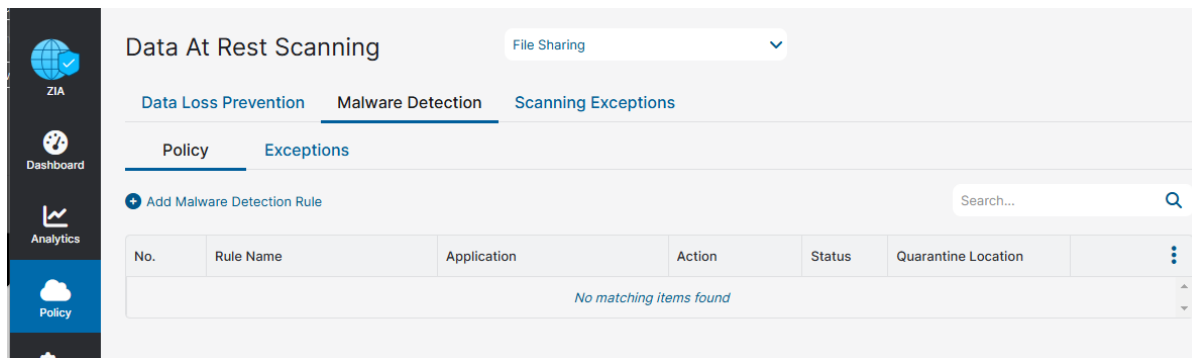


Figure 69. Data at Rest Scanning Policy – Malware Detection

You cannot select specific buckets for each of these policies until you have configured the **Scan Schedule** and selected all possible buckets to include. Then you can go back into the **DLP** and **Malware** policies (select **Public Cloud Storage** at the top again) to select specific buckets (if multiple buckets were selected in the Scan Schedule).

After you save the **Scan Configuration**, click **Start**. This changes the **Status** to **Running**.

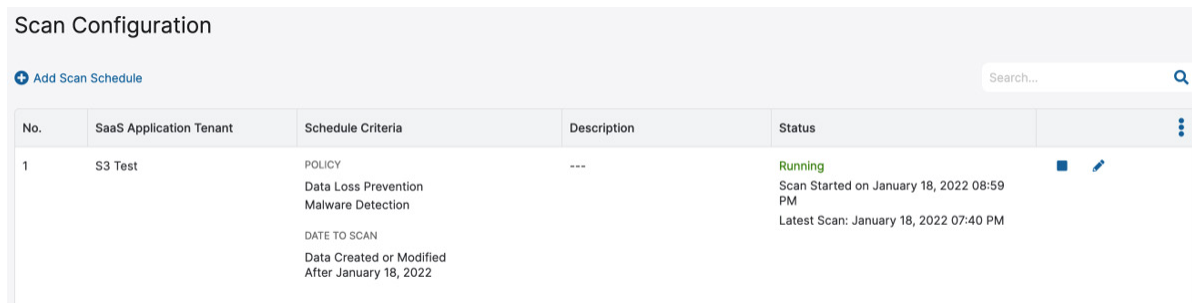


Figure 70. SaaS configuration

You can find information about DLP and Malware incidents in the following locations:

- **Analytics > SaaS Assets Summary Report**
- **Analytics > SaaS Security Report > Assets**
- **Analytics > SaaS Security Insights**

The following figure shows an SaaS assets summary report.

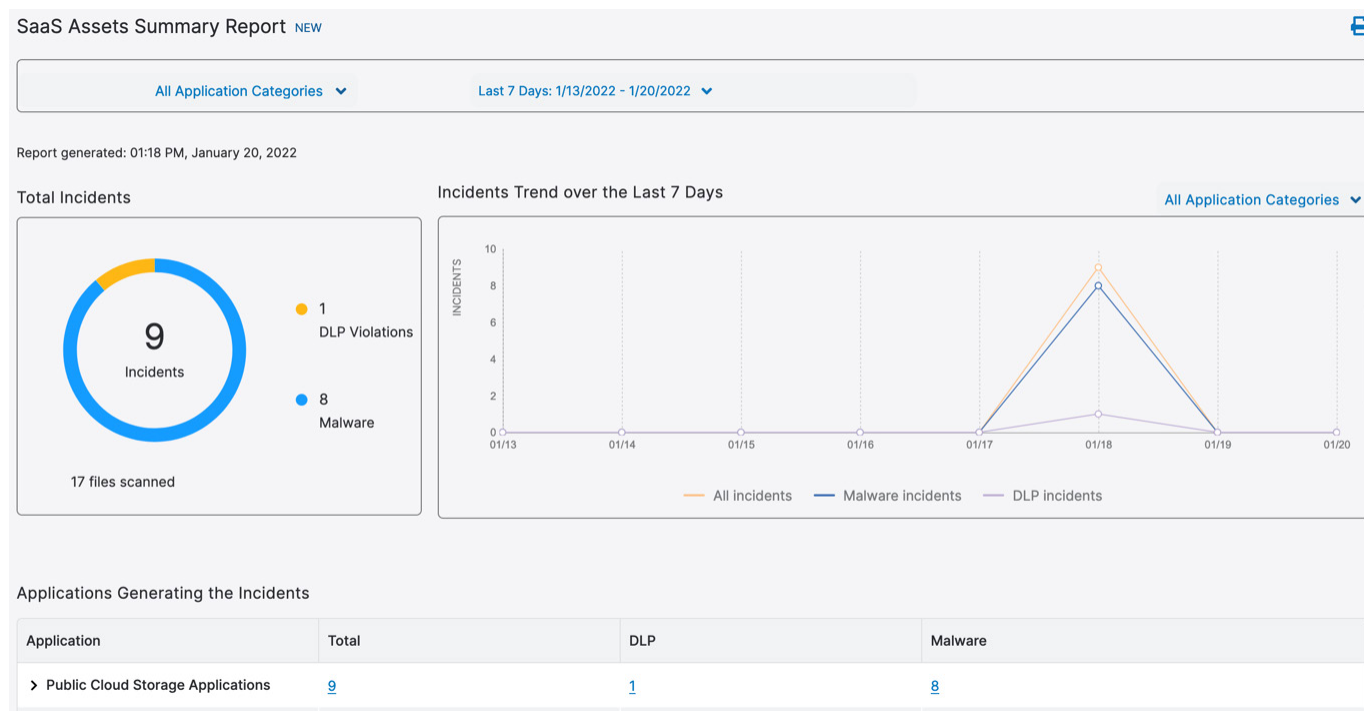


Figure 71. SaaS assets summary report

The following figure shows an SaaS security insight report.

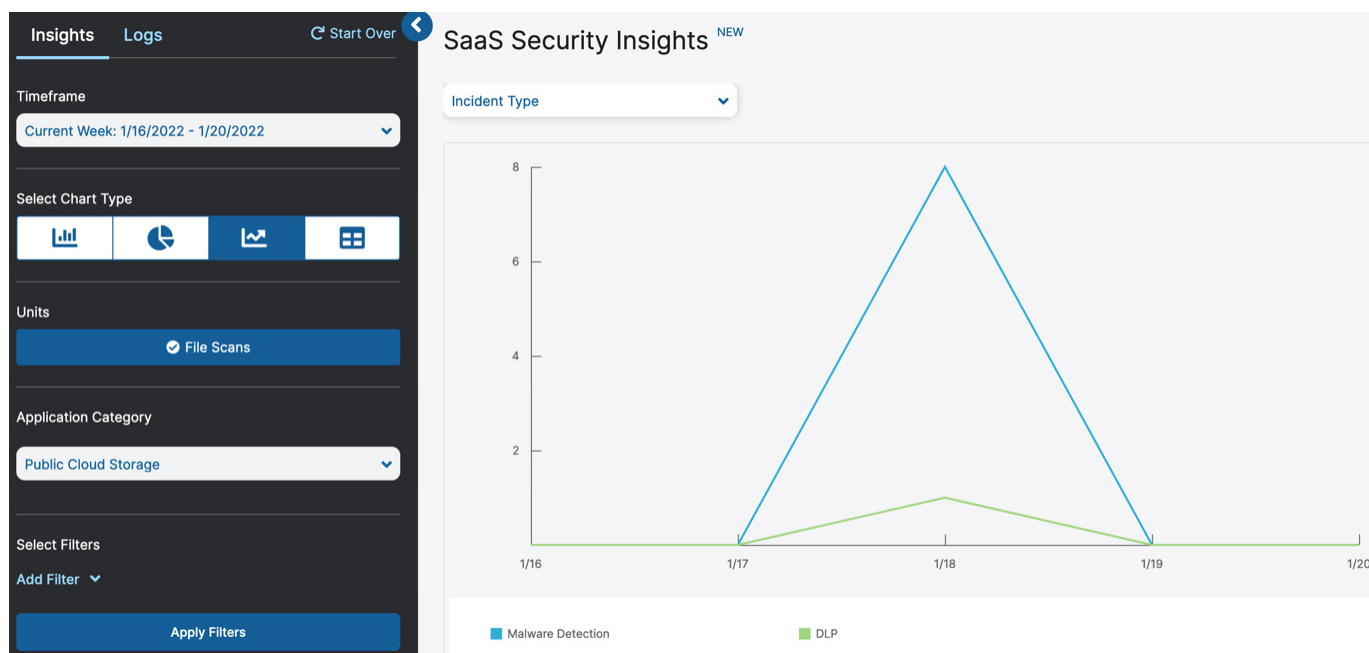


Figure 72. SaaS security insights

Appendix C: Requesting Zscaler Support

You might need Zscaler Support for provisioning certain services, or to help troubleshoot configuration and service issues. Zscaler Support is available 24/7/365. To contact Zscaler Support,

1. Go to **Administration > Settings > Company Profile**.

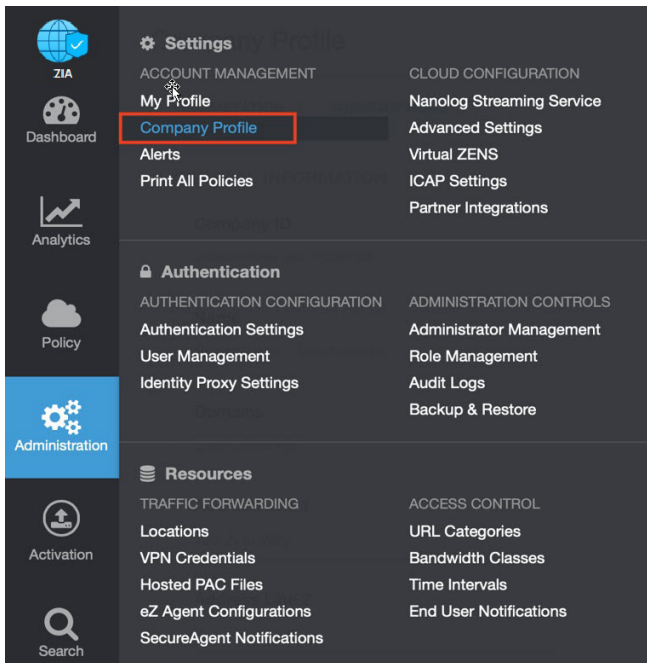


Figure 73. Collecting details to open support case with Zscaler TAC

2. Copy your Company ID.

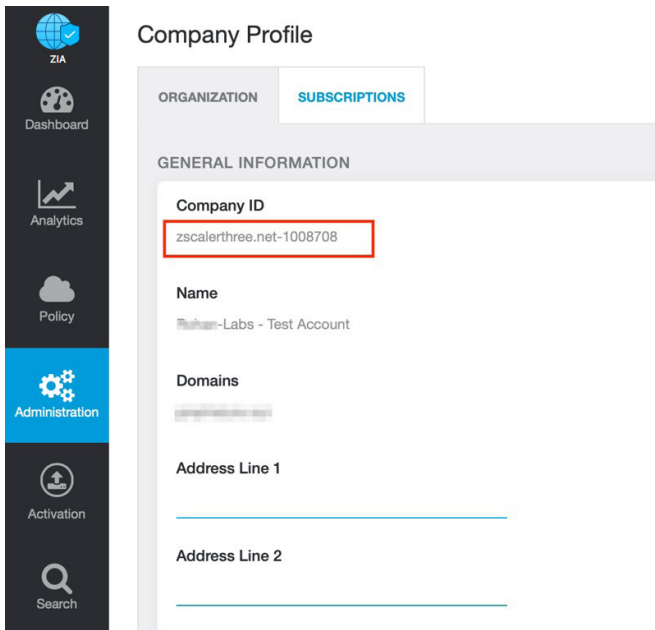


Figure 74. Company ID

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

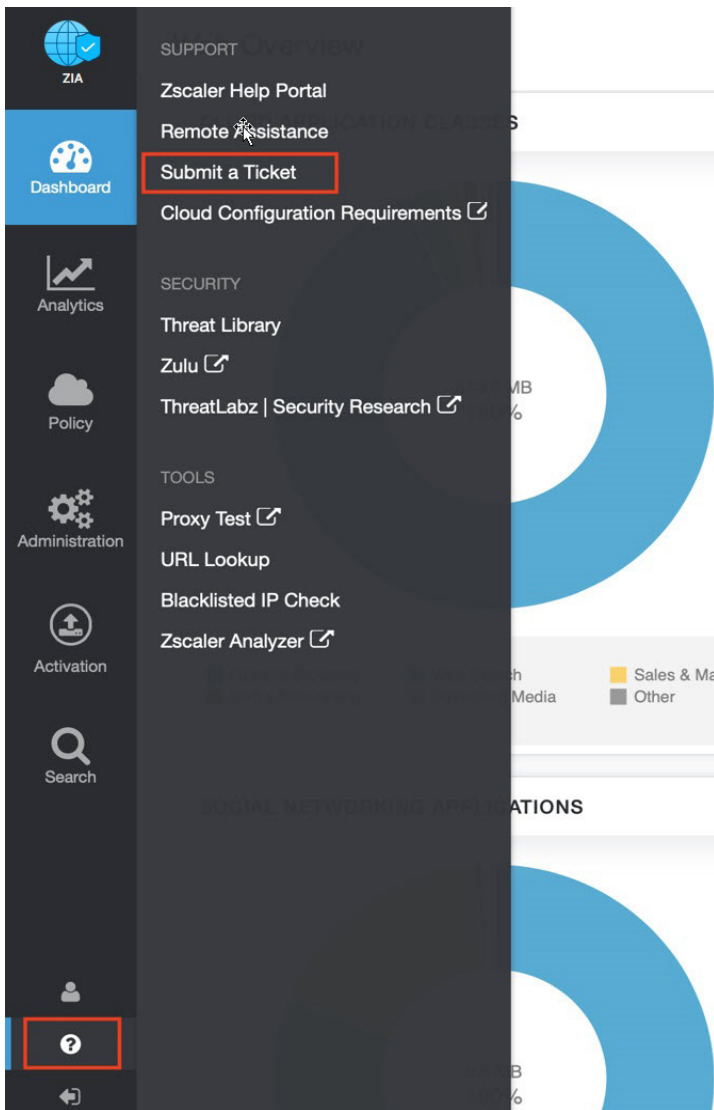


Figure 75. Submit a ticket