ZSCALER SAAS SECURITY API AND AMAZON S3 DEPLOYMENT GUIDE
Contents

Terms and Acronyms 4
About This Document 4
  Zscaler Overview 4
  AWS Overview 4
  Audience 4
  Software Versions 5
  Request for Comments 5
Zscaler and AWS Introduction 5
  Zscaler Overview 5
    Zscaler Internet Access (ZIA) Overview 5
    Zscaler Resources 5
    Amazon Workspaces Overview 6
    AWS Resources 6
About this Guide 6
  Prerequisite 6
Initial Zscaler Configuration 7
AWS Configuration (IAM Role) 8
AWS Configuration (Trust Relationship) 10
AWS Configuration (CloudTrail) 11
AWS Configuration (Quarantine Bucket) 13
Finish Zscaler Configuration 14
Appendix A: Create Trail 15
Appendix B: Testing Notes 16

Appendix C: Requesting Zscaler Support 19

Gather Support Information 19
   Save Company ID 19
   Enter Support Section 20
## Terms and Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>Central Authority (Zscaler)</td>
</tr>
<tr>
<td>CSV</td>
<td>Comma-Separated Values</td>
</tr>
<tr>
<td>DPD</td>
<td>Dead Peer Detection (RFC 3706)</td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation (RFC2890)</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange (RFC2409)</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security (RFC2411)</td>
</tr>
<tr>
<td>PFS</td>
<td>Perfect Forward Secrecy</td>
</tr>
<tr>
<td>PSK</td>
<td>Pre-Shared Key</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer (RFC6101)</td>
</tr>
<tr>
<td>XFF</td>
<td>X-Forwarded-For (RFC7239)</td>
</tr>
<tr>
<td>ZIA</td>
<td>Zscaler Internet Access (Zscaler)</td>
</tr>
<tr>
<td>ZEN</td>
<td>Zscaler Enforcement Node (Zscaler)</td>
</tr>
<tr>
<td>ZPA</td>
<td>Zscaler Private Access (Zscaler)</td>
</tr>
</tbody>
</table>

## About This Document

### Zscaler Overview

Zscaler (Nasdaq: **ZS**), enables the world’s leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) services create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler delivers its services 100% in the cloud and offers the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions can’t match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss. For more information on Zscaler, visit [www.zscaler.com](http://www.zscaler.com) 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 on AWS, visit [aws.amazon.com](http://aws.amazon.com).

### 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, please refer to:

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

This document was authored using the latest version of Zscaler Internet Access, 6.1.

Request for Comments

- For Prospects and Customers: We value reader opinions and experiences. Please contact us at 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

Zscaler Overview

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

Zscaler Internet Access (ZIA) Overview

Zscaler Internet Access (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, CASB, and Browser 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZIA Help Portal</td>
<td>Help articles for ZIA.</td>
</tr>
<tr>
<td>ZIA Test Page</td>
<td>Provides information on your Zscaler cloud.</td>
</tr>
<tr>
<td>Zscaler Tools</td>
<td>Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.</td>
</tr>
<tr>
<td>Zscaler Training and Certification</td>
<td>Training designed to help you maximize Zscaler products.</td>
</tr>
<tr>
<td>Submit a Zscaler Support Ticket</td>
<td>Zscaler support portal for submitting requests and issues.</td>
</tr>
</tbody>
</table>
Amazon Workspaces Overview

Amazon Simple Storage Service (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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon S3 Help</td>
<td>Amazon Simple Storage Service documentation.</td>
</tr>
<tr>
<td>AWS CLI</td>
<td>AWS Command Line Interface documentation.</td>
</tr>
<tr>
<td>AWS CloudTrail Help</td>
<td>AWS CloudTrail documentation.</td>
</tr>
<tr>
<td>AWS IAM Help</td>
<td>AWS IAM documentation.</td>
</tr>
</tbody>
</table>

About this Guide

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.

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).

The Company ID for your specific tenant can be found on the Administration > Organization page. Once enabled, an Amazon S3 tile should be available as an option when adding a tenant on the Administration > SaaS Application Tenants page.

It may be good to make sure that the ZIA Admin UI 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 portal before returning to the ZIA Admin Portal to finish the configuration.
Initial Zscaler Configuration

In the ZIA Admin Portal navigate to the Administration > SaaS Application Tenants page and click on Add SaaS Application Tenant.

Select the Amazon S3 tile for Step 1 (Choose the SaaS Application Provider).

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.
AWS Configuration (IAM Role)

The next steps are also documented in the Adding SaaS Application Tenants help page in the Configure an IAM Role for the Zscaler S3 Connector section (starting with step iv).

Log into the AWS portal and navigate to Services > IAM and click on Access Management > Roles in the left navigation pane.

1. Click on the Create Role button.

![Create Role](image)

Figure 3. Create Role

2. Click on the Another AWS account tile as the type of trusted entity.

![Trusted entity type](image)

Figure 4. Trusted entity type

3. Enter the Zscaler Connector Account Number copied earlier in the Account ID text box, and make sure both options are de-selected.

4. Click on the Next: Permissions button at the bottom.

![Specify accounts that can use this role](image)

Figure 5. Which accounts can use the role
5. Type in “AmazonS3FullAccess” into the search area and select the policy name found. Click on the **Next: Tags** button at the bottom.

![Attach permissions policies](image)

**Figure 6. Attach permissions policies**

6. Add tags if needed, and then click on the **Next: Review** button at the bottom.

![Add tags](image)

**Figure 7. Add tags**

7. Enter a **Role** name to use for this role and (optionally) a description and click the **Create role** button at the bottom.

![Create role](image)

**Figure 8. Create role**
AWS Configuration (Trust Relationship)

The next steps are also documented in the Adding SaaS Application Tenants help page in the Edit the Trust Relationship section.

1. Search for the newly created role by typing “Zscaler” into the search area and click on the role name found.

![Roles](image9)

Figure 9. Roles

2. Click on the Trust relationships tab and then click on the Edit trust relationship button.

![Trust relationships](image10)

Figure 10. Trust relationships

3. In the Policy Document text box, replace the default AWS value with the Zscaler Connector User ARN copied earlier and click the Update Trust Policy button at the bottom.

![Policy Document](image11)

Figure 11. Policy document

4. At the top of the Summary page, copy the Role ARN for later use (as the IAM Role ARN).

![Role ARN](image12)

Figure 12. Role ARN
AWS Configuration (CloudTrail)

The next steps are also documented in the Adding SaaS Application Tenants help page 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 API Scan Configuration as it is marked Internal.

1. Navigate to Services > CloudTrail and click on Trails in the left navigation pane.

In the Adding SaaS Application Tenants help, step iii under section c shows an existing trail. If you don’t already have one you need to create one. Please refer to Appendix A: Create Trail on how to create a trail before proceeding.

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

In the Adding SaaS Application Tenants help, step iii under section c shows an existing trail. If you don’t already have one you need to create one. Please refer to Appendix A: Create Trail on how to create a trail before proceeding.
3. Click on the Trail log location (in blue) in **General details**.

![CloudTrail general details](image)

4. In the **Objects** tab click on the **CloudTrail** name.

![CloudTrail objects](image)

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

![CloudTrail properties](image)
AWS Configuration (Quarantine Bucket)

The next steps are documented in the Adding SaaS Application Tenants help page in the Create a Quarantine Bucket section.

Step ii, section d of Adding SaaS Application Tenants details creating a new bucket to use for quarantined files. If you already have a bucket you don't need to create one, but please verify that the settings below 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 to be used for the quarantined files won't be available in the SaaS Security API Scan Configuration as it is marked **Internal**.

Navigate to Services > S3 and click on Buckets in the left navigation pane. Record the name of the S3 bucket used as the Quarantine bucket (either existing or newly created) for later.

![Buckets configuration](image-url)

*Figure 18. Buckets configuration*
Finish Zscaler Configuration

To complete Zscaler configuration:

1. Back in the ZIA Admin Portal on the **Add SaaS Application Tenant** page, enter the details for **Step 4 (Register the SaaS Application)** and click the **Save** button at the bottom.

   - Your AWS Account ID can be found in the user details in the upper right-hand corner of the AWS portal. Detailed info on obtaining your AWS Account ID can be found in the [AWS docs](#).
   - The **Quarantine Bucket Name** is the one you copied in the previous step.
   - The **IAM Role ARN** is the role ARN you copied earlier (in the **Trust Relationship** configuration).
   - The **CloudTrail Bucket ARN** is Amazon Resource Name (ARN) you copied earlier (in the **CloudTrail** configuration).

2. Once saved and activated, the status shows as **Validating**.

3. After a short period, if access was successful, the status shows **Active**. Proceed with configuring policy.

---

- Your AWS Account ID can be found in the user details in the upper right-hand corner of the AWS portal. Detailed info on obtaining your AWS Account ID can be found in the [AWS docs](#).
- The **Quarantine Bucket Name** is the one you copied in the previous step.
- The **IAM Role ARN** is the role ARN you copied earlier (in the **Trust Relationship** configuration).
- The **CloudTrail Bucket ARN** is Amazon Resource Name (ARN) you copied earlier (in the **CloudTrail** configuration).
Appendix A: Create Trail

You can create a trail under Services > CloudTrail > Trails by clicking on the Create trail button at the top or at the bottom.

1. In Step 1 (Choose trail attributes) you must enter a name for the trail and either choose an existing S3 bucket to use or create a new one. The Log file SSE-KMS encryption option is enabled by default. For the purposes of this guide I have disable it. (If you chose to leave it enabled, please refer to the Info link in the UI for more information).

2. Click the Next button at the bottom to continue to the next step.

3. In Step 2, select the Events > Event types you want to log, and the Data event > Data event type to use as the source (S3 in this case).
4. Click the **Next** button at the bottom to continue to the next step.

**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**

- **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.

- **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 23. Management events**

**Data event: S3**

**Data event type**

- Choose the source of data events to log.

  - **S3**

**Log selector template**

- **Log all events**

**Figure 24. Data event**

5. After review in **Step 3 (Review and create)**, click the **Create trail** button at the bottom to continue.
Appendix B: Testing Notes

Configuring the SaaS Security API control policy is documented in the Configuring the SaaS Security API Control Policy help page.

When configuring the Data Loss Prevention and the Malware Detection policy you need to select Public Cloud Storage at the top for each page to create a policy for your S3 SaaS application tenant.

As stated in the note on the help page 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 were selected in the Scan Schedule).

Once you save the Scan Configuration, click the Start icon to start the process. This changes the Status to Running.
DLP and Malware incident information can be found in the following locations:

- Analytics > SaaS Assets Summary Report (see sample below)
- Analytics > SaaS Security Report > Assets
- Analytics > SaaS Security Insights (see sample below)

**SaaS Assets Summary Report**

- Total Incidents: 9
  - DLP Violations: 1
  - Malware: 8
- 17 files scanned

**SaaS Security Insights**

- Incident Type: Malware Detection
- Incidents Trend over the Last 7 Days

---

**Figure 28. SaaS assets summary report**

**Figure 29. SaaS security insights**
Appendix C: Requesting Zscaler Support

Gather Support Information

You might need Zscaler support for provisioning certain services, or to help troubleshoot configuration and service issues. Zscaler support is available 24/7 hours a day, year-round. To contact Zscaler support, select Administration > Settings > Company profile.

![Company Profile](image)

Figure 30. Collecting details to open support case with Zscaler TAC

Save Company ID

Copy your Company ID.

![Company Profile](image)

Figure 31. Company ID
Enter Support Section

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

Figure 32. Submit a ticket