



ZSCALER AND HUNTERS DEPLOYMENT GUIDE

Contents

Terms and Acronyms	4
About This Document	6
Zscaler Overview	6
Hunters Overview	6
Audience	6
Software Versions	6
Request for Comments	6
Zscaler and Hunters Introduction	7
ZIA Overview	7
ZPA Overview	7
Hunters SOC Platform Overview	8
Hunters Resources	8
Introduction	9
Integrating Zscaler Cloud NSS with Amazon S3	10
Integrate ZIA Logs into Hunters	11
Start the Connection Process	11
Provide Bucket Access	13
Option 1: Use CloudFormation Template	13
Option 2: Create Manual IAM Access	16
Option 3: Use an Existing IAM Role	22

ZPA Logs	24
Audit Logs	26
User Status Logs	27
Browser Access Logs	28
User Activity Logs	29
Appendix A: Requesting Zscaler Support	30

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
IKE	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
NSS	Nanolog Streaming Service
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SOC	Security Operations Center
SIEM	Security Information and Event Management
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
XFF	X-Forwarded-For (RFC7239)
ZPC	Zscaler Posture Control (Zscaler)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

Trademark Notice

© 2024 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

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.

Hunters Overview

Hunters delivers a Security Operations Center (SOC) Platform that reduces risk, complexity, and cost for security teams. A SIEM replacement, Hunters SOC Platform provides data ingestion, built-in and always up-to-date threat detection, and automated correlation and investigation capabilities, minimizing the time to understand and respond to real threats. To learn more, refer to [Hunters' 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](#)
- [Hunters Resources](#)
- [Appendix A: Requesting Zscaler Support](#)

Software Versions

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

Request for Comments

- **For prospects and customers:** Zscaler values reader opinions and experiences. Contact partner-doc-support@zscaler.com to offer feedback or corrections for this guide.
- **For Zscaler employees:** Contact z-bd-sa@zscaler.com to reach the team that validated and authored the integrations in this document.

Zscaler and Hunters Introduction

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



If you are using this guide to implement a solution at a government agency, some of the content might be different for your deployment. Efforts are made throughout the guide to note where government agencies might need different parameters or input. If you have questions, contact your Zscaler Account team.

ZIA Overview

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of ZIA as a secure internet on-ramp—just make Zscaler your next hop to the internet via one of the following methods:

- Setting up a tunnel (GRE or IPSec) to the closest Zscaler data center (for offices).
- Forwarding traffic via our lightweight Zscaler Client Connector or PAC file (for mobile employees).

No matter where users connect—a coffee shop in Milan, a hotel in Hong Kong, or a VDI instance in South Korea—they get identical protection. ZIA sits between your users and the internet and inspects every transaction inline across multiple security techniques (even within SSL).

You get full protection from web and internet threats. The Zscaler cloud platform supports Cloud Firewall, IPS, Sandboxing, DLP, and Isolation, allowing you to start with the services you need now and activate others as your needs grow.

ZPA Overview

ZPA is a cloud service that provides secure remote access to internal applications running on a cloud or data center using a Zero Trust framework. With ZPA, applications are never exposed to the internet, making them completely invisible to unauthorized users. The service enables the applications to connect to users via inside-out connectivity rather than extending the network to them.

ZPA provides a simple, secure, and effective way to access internal applications. Access is based on policies created by the IT administrator within the ZPA Admin Portal and hosted within the Zscaler cloud. On each user device, software called Zscaler Client Connector is installed. Zscaler Client Connector ensures the user's device posture and extends a secure microtunnel out to the Zscaler cloud when a user attempts to access an internal application.

Zscaler Resources

The following table contains links to Zscaler resources based on general topic areas.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

The following table contains links to Zscaler resources for government agencies.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

Hunters SOC Platform Overview

Hunters SOC Platform empowers security teams to automatically identify and respond to incidents that matter, helping teams mitigate real threats faster and more reliably than SIEM.

Hunters Resources

The following table contains links to Hunters support resources.

Name	Definition
Hunters Help Portal	Help articles and documentation.

Introduction

You must configure Zscaler to send logs to an Amazon S3 bucket via Zscaler's Cloud Nanolog Streaming Service (NSS). This guide provides the necessary actions and steps to configure log forwarding on Zscaler Cloud NSS and integration with Hunters SIEM.

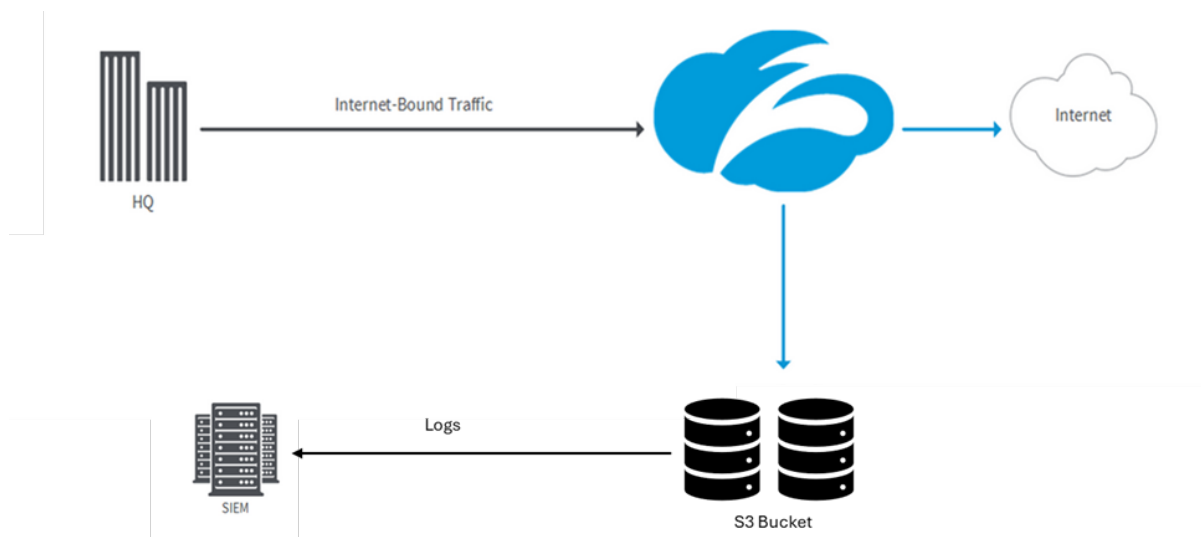


Figure 1. Zscaler and Hunters integration architecture

Integrating Zscaler Cloud NSS with Amazon S3

To learn more about integrating Zscaler Cloud NSS with Amazon S3, see [Zscaler SaaS Security API and Amazon S3 Deployment Guide](#) (page 17 onwards).

Integrate ZIA Logs into Hunters

The following section describes how to integrate ZIA logs into Hunters SOC.

Start the Connection Process

To start the connection process:

1. Open the Hunters SOC Platform and go to **Data > Data Sources**.

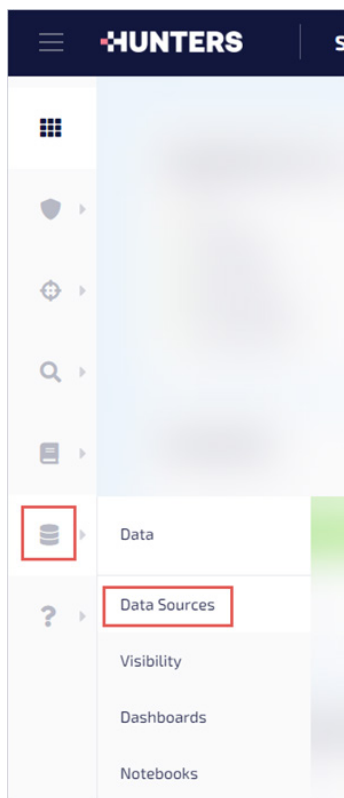


Figure 2. Data Sources

2. Click **+ Add Data Sources**.

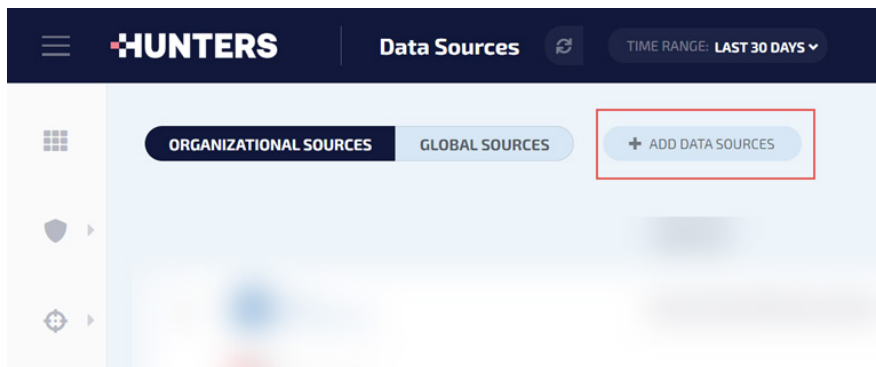


Figure 3. Add Data Sources

3. Search for Zscaler and click **Connect**. The **Zscaler connection** wizard opens.

The screenshot shows the 'Zscaler connection wizard' in the HUNTERS Data Sources interface. The wizard is titled 'ZSCALER' and shows three data types: 'ZSCALER VIS S3 LIST', 'ZSCALER S3 LIST', and 'ZSCALER S3 LIST'. The 'ZSCALER S3 LIST' is selected and expanded, showing fields for 'Zscaler Internet Access (ZIA)' and 'Zscaler ZIA Audit Logs'. The 'ZIA' section has a toggle switch and fields for 'Bucket Name', 'Prefix(es)', and 'KMS Encryption Key ARN(s)'. The 'ZIA Audit Logs' section also has a toggle switch and fields for 'Bucket Name' and 'Prefix(es)'. A 'Test Connection' button is at the bottom.

Figure 4. Zscaler connection wizard

4. Activate the data types you want to connect and provide the following details:

- Bucket Name:** Enter the name of the relevant S3 bucket.
- Prefix(es):** If the bucket contains data that should not be ingested, specify one of the prefixes that can be ingested to confirm necessary access has been granted.



This field supports the prefix structure in which Zscaler logs are shipped: S3bucket/feedtype/feedname=feed_name/year=YYYY/month=MM/day=DD/ epochtime_id1_id2_samesecondcount

- KMS Encryption Key ARN(s):** (Optional) If your bucket is encrypted, provide the encryption KMS key ARN.


Provide Bucket Access

Hunters offers three options you can use to provide the platform with access to your bucket. You must select one of the following options:

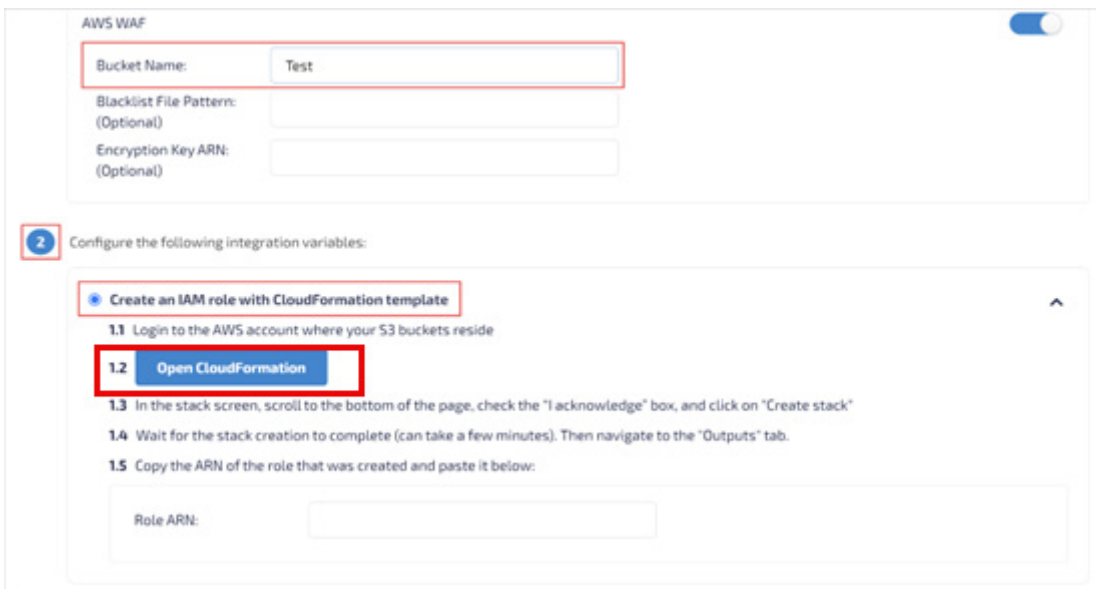
- CloudFormation template: This is the recommended method. After entering a bucket name, the platform generates a CloudFormation template, which runs automatically to provide Hunters with access to the bucket.
- Manually created IAM role: This method requires you to manually create an IAM policy and IAM role on AWS.
- Existing IAM role: Use this method if you already have an existing IAM role set up.

Option 1: Use CloudFormation Template

Hunters allows you access to your bucket using a CloudFormation template. Zscaler recommends using this method if you have the appropriate permissions.

 Before starting the process, make sure you're logged in to your AWS Management Console.

1. On the Hunters SOC Platform connection process, select **Create an IAM role with CloudFormation template**.
2. Click **Open CloudFormation** to open the **Quick Create Stack** page.



The screenshot shows the AWS WAF console interface. At the top, there's a section for 'AWS WAF' with a toggle switch. Below it, there are input fields for 'Bucket Name' (containing 'Test'), 'Blacklist File Pattern: (Optional)', and 'Encryption Key ARN: (Optional)'. A red box highlights the 'Bucket Name' field. Below this, a section titled 'Configure the following integration variables:' contains a list of steps. Step 1.1 is 'Login to the AWS account where your S3 buckets reside'. Step 1.2 is 'Open CloudFormation', which is highlighted with a red box and a blue button. Step 1.3 is 'In the stack screen, scroll to the bottom of the page, check the "I acknowledge" box, and click on "Create stack"'. Step 1.4 is 'Wait for the stack creation to complete (can take a few minutes). Then navigate to the "Outputs" tab.'. Step 1.5 is 'Copy the ARN of the role that was created and paste it below:'. Below the steps, there is a 'Role ARN:' label and an empty input field.

Figure 5. Create an IAM role with CloudFormation template

3. Scroll to the bottom of the page and check **I acknowledge**.
4. Click **Create stack** and wait for the stack creation to complete (it can take a few minutes).
5. After the creation is completed, go to the **Outputs** tab.

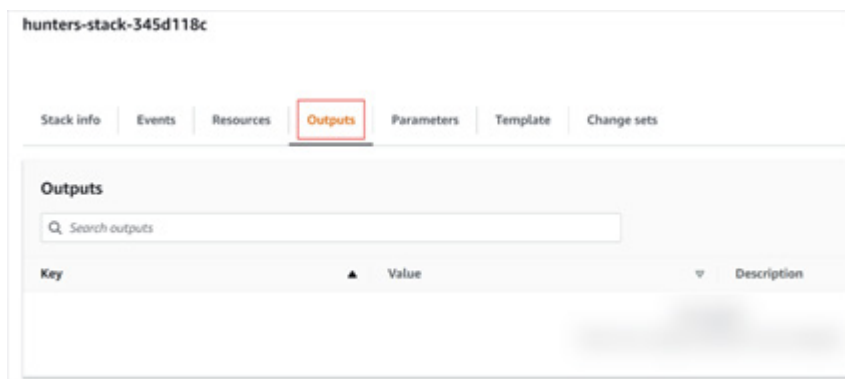


Figure 6. Outputs

6. Copy the ARN of the role that was created.
7. Return to the Hunters SOC Platform and paste the **Role ARN** in the relevant field.

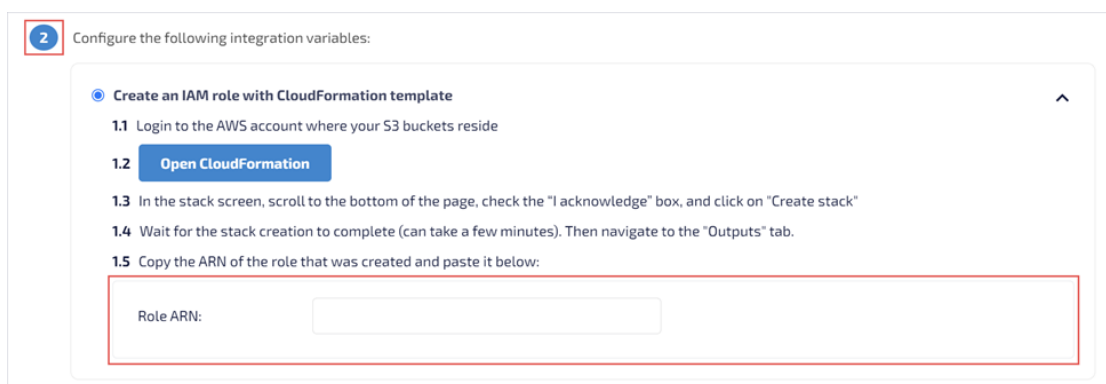


Figure 7. Role ARN



Make sure you've filled a bucket name for each of the data types selected in [Start the Connection Process](#).

8. Click **Test Connection** to make sure the setup was successful.
9. Click **Create Integration** to complete the process.



The permissions given to the IAM Role, `lamHuntersRole`, are the permissions granted by the IAM Managed Policy, `lamHuntersPolicy`. These permissions include:

- Amazon S3: The IAM Role can perform the following actions on the specified S3 buckets (provided in `BucketNames`):
 - `s3:ListBucket`: Lists the objects in the bucket.
 - `s3:GetObject`: Retrieves the objects in the bucket.
 - `s3:GetBucketLocation`: Retrieves the region where the bucket resides.
 - `s3:GetBucketNotification`: Gets the bucket notification configuration, which includes topic configuration and other notification settings.
 - `s3:PutBucketNotification`: Sets the bucket notification configuration, which includes topic configuration and other notification settings.
- Amazon KMS: If KMS ARNs are provided in the `KmsARNs` parameter:
 - `kms:Decrypt`: The IAM Role can use the specified KMS keys to decrypt data.
- Amazon SNS: The IAM Role can perform the following actions on SNS topics whose names start with `hunters?ingestion*`:
 - `sns:ListSubscriptionsByTopic`: Lists all the subscriptions to a specific topic.
 - `sns:GetTopicAttributes`: Retrieves all the attributes of a topic.
 - `sns:SetTopicAttributes`: Sets the attributes of a topic.
 - `sns:CreateTopic`: Creates a new topic.
 - `sns:TagResource`: Adds a tag to a specified topic.
 - `sns:Publish`: Sends messages to a topic.
 - `sns:Subscribe`: Subscribes to a topic to receive messages published to it.
 - `sns:Unsubscribe`: Unsubscribes from a topic.
 - `sns>DeleteTopic`: Deletes a topic.
- Additionally, the IAM Role can perform the following actions without restrictions on resources:
 - `s3:ListAllMyBuckets`: Lists all S3 buckets in the account.
 - `sns:ListTopics`: Lists all SNS topics in the account.

Option 2: Create Manual IAM Access

This section describes how to create manual IAM access.

Create an IAM Policy

After creating the bucket, you'll create an AWS IAM Policy. This allows Hunters to access the necessary resources for retrieving data from the bucket.



Hunters required permissions:

- s3:ListAllMyBuckets: Allows Hunters to list all buckets in your AWS account (but not read them).
- s3:ListBucket: Allows Hunters to list the specific bucket you're defining in the policy.
- s3:GetObject: Allows Hunters to retrieve objects in the specific bucket (logs placed in the bucket).
- s3:GetBucketLocation: Allows Hunters to determine the AWS Region in which the bucket is located.
- kms:Decrypt: Allows Hunters to decrypt the bucket contents, if you are using a customer-managed KMS key to encrypt the bucket contents.

1. In the [AWS Management Console](#), search for Identity and Access Management, then select **IAM**.

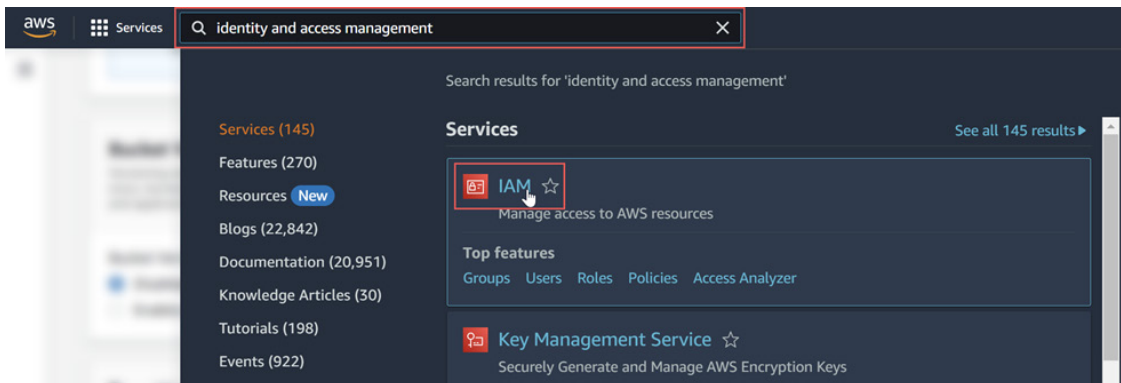


Figure 8. Identity & Access Management (IAM)

2. From the left-side navigation, select **Policies** and then click **Create policy**. The **Create policy** window is displayed.

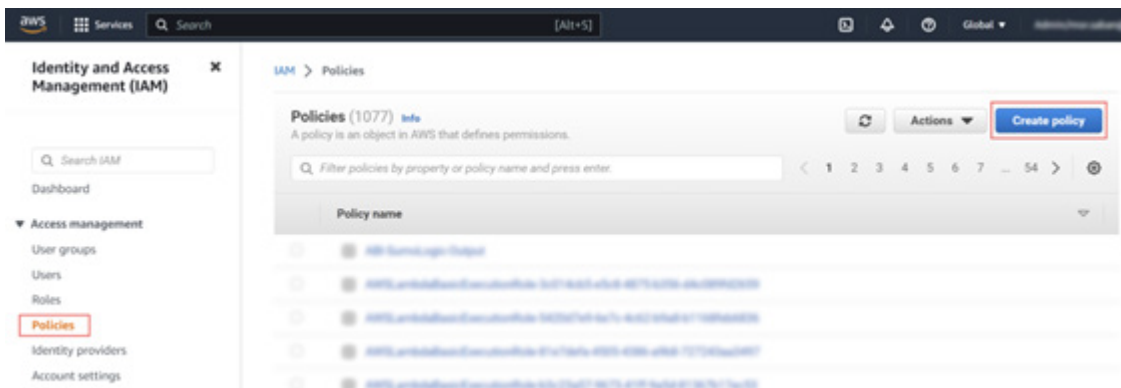


Figure 9. Create Policy

3. Go to the **JSON** tab and replace its content with the following code. Use the code under the relevant heading based on your encryption method. If you don't have encryption, use the code under Amazon S3 Managed Keys.



Make sure you have an appropriate key policy set up:

KMS Customer Managed Keys

Use the following code if your bucket is encrypted using KMS Customer-Managed Keys. Make sure to replace **<BUCKET-NAME-HERE>**.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:ListAllMyBuckets",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::<BUCKET-NAME-HERE>",
        "arn:aws:s3:::<BUCKET-NAME-HERE>/*"
      ]
    }
  ]
}
```



Make sure you have an appropriate key policy set up:

Amazon S3 Managed Keys

Use the following code if your bucket is encrypted using KMS Customer-Managed Keys. Make sure to replace **<BUCKET-NAME-HERE>** with your actual bucket name.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:ListAllMyBuckets",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::<BUCKET-NAME-HERE>",
        "arn:aws:s3:::<BUCKET-NAME-HERE>/*"
      ]
    }
  ]
}
```

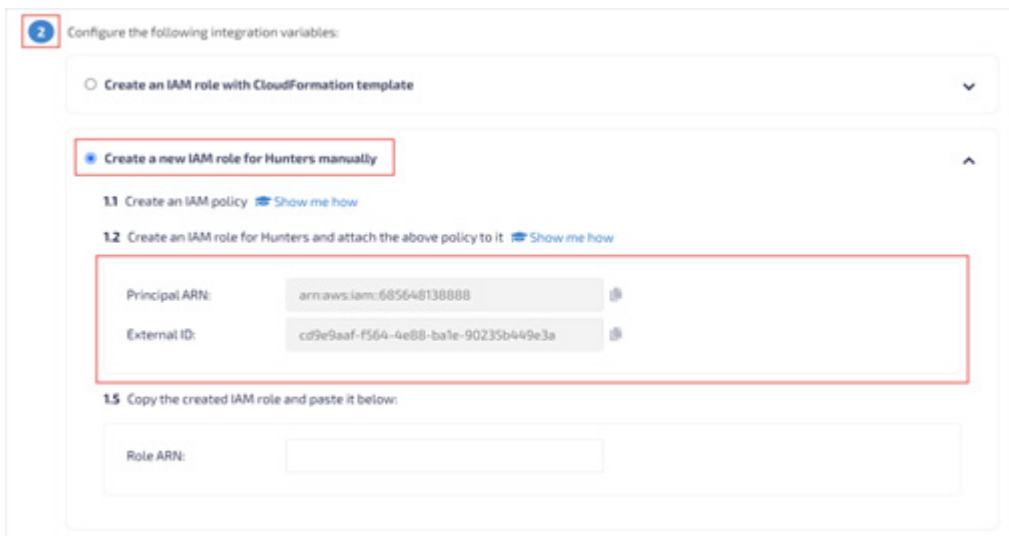
4. Click **Next** to skip the **Tags** option.
5. Enter a name for the IAM policy (e.g., `HuntersBucketAccess`) and click **Create policy**.

Create an IAM Role

With the policy created, you must create an IAM role that Hunters assumes to access the buckets defined via the policy created in [Option 2: Create Manual IAM Access](#). This process requires switching between the Hunters SOC Platform and your AWS Management Console.

On the Hunters SOC Platform:

1. Open the Hunters SOC Platform and go to the connection process you previously started.
2. Select **Create a new IAM role for Hunters manually**.
3. Locate the **Principal ARN** and **External ID**. Keep the tab open for later use.



The screenshot shows a configuration page titled "Configure the following integration variables:". It has two main sections: "Create an IAM role with CloudFormation template" (disabled) and "Create a new IAM role for Hunters manually" (selected and highlighted with a red box). Under the selected section, there are two steps: "1.1 Create an IAM policy" and "1.2 Create an IAM role for Hunters and attach the above policy to it". Below these steps, there are two input fields: "Principal ARN" with the value "arn:aws:iam::685648138888" and "External ID" with the value "cd9e9aaf-f564-4e88-ba1e-90235b449e3a". Both fields are highlighted with a red box. At the bottom, there is a field for "Role ARN" which is currently empty.

Figure 10. Principal ARN and External ID

On AWS:

1. Return to AWS Management Console. Search for Identity and Access Management, then select **IAM**.

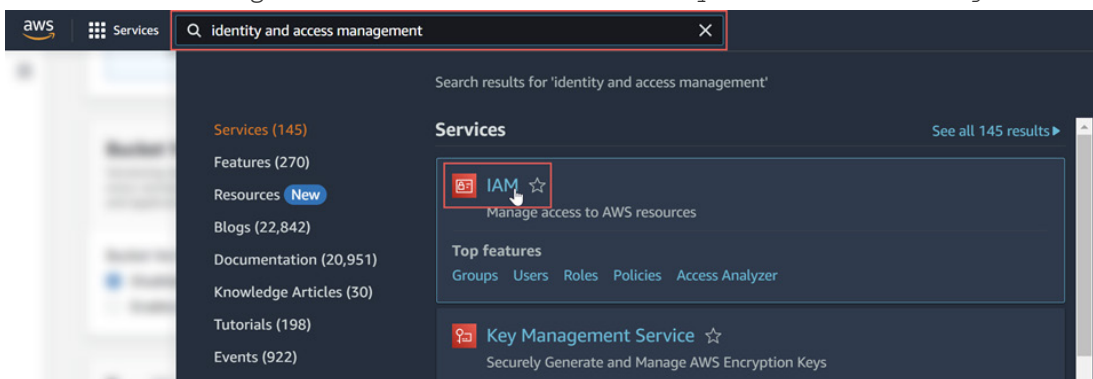


Figure 11. Identity & Access Management (IAM)

2. From the left-side navigation, select **Roles** and click **Create role**. The **Create role** window is displayed.

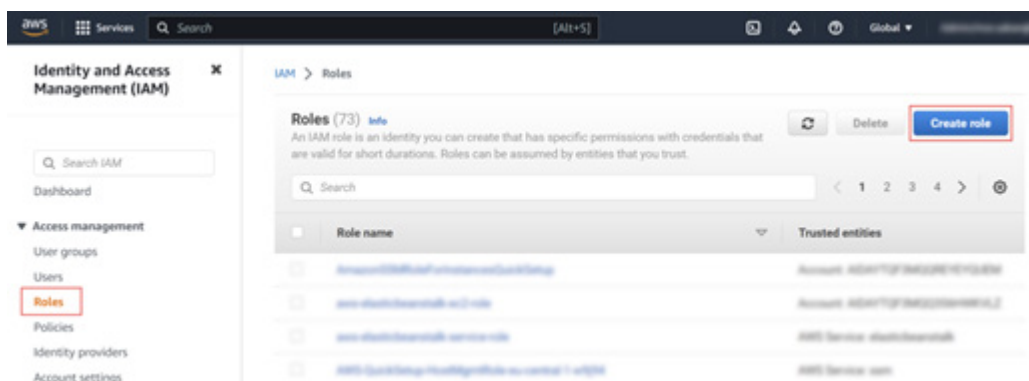


Figure 12. Create role

3. Select **AWS account** and then **Another AWS account**.

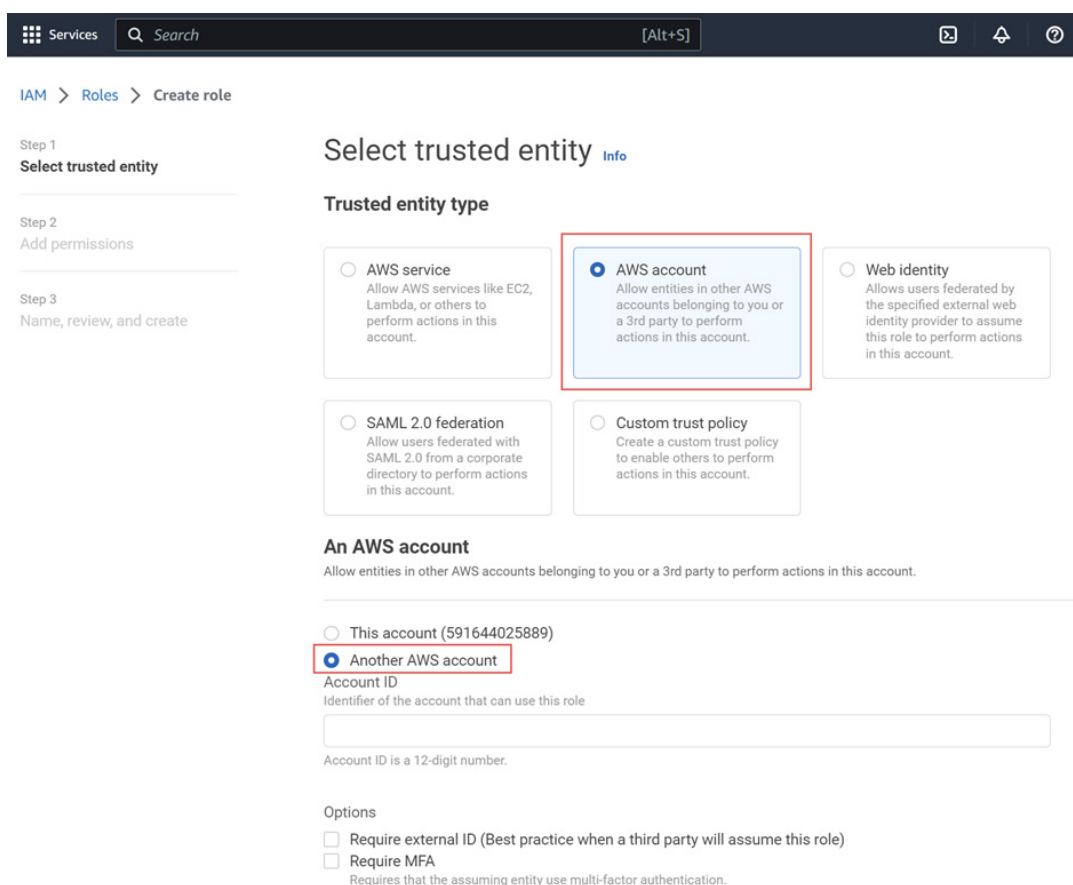
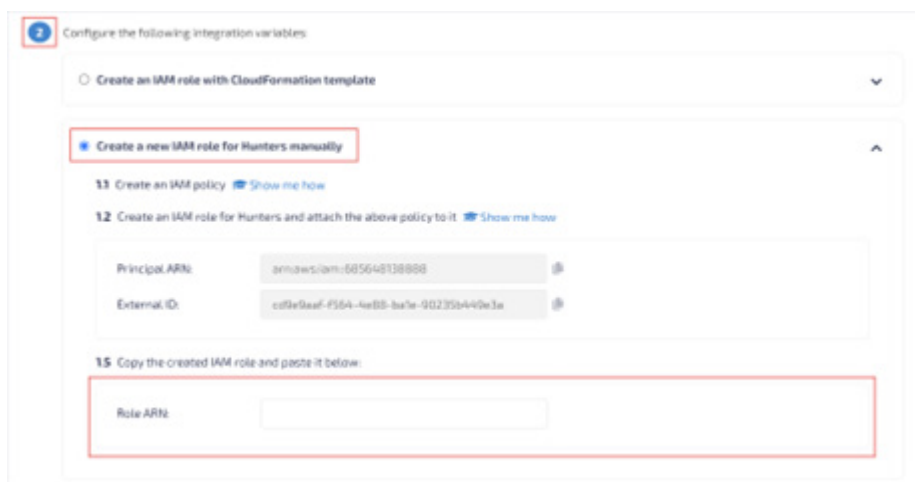


Figure 13. AWS account

4. Enter 685648138888 in the **Account ID** field.
5. Select **Require External ID** and use the external ID value.
6. Click **Next**.
7. In the **Add Permissions** section, select the policy that was just created in HuntersBucketAccess.
8. Click **Next**.
9. Name the role `hunters-assume-role` and enter a short description.
10. Click **Create role**.
11. Copy the **Role ARN** provided by AWS.

On the Hunters SOC Platform:

1. Return to the connection page on Hunters.
2. Paste the **Role ARN** into the **Role ARN** field.



2 Configure the following integration variables:

☐ Create an IAM role with CloudFormation template

☒ Create a new IAM role for Hunters manually

1.1 Create an IAM policy [Show me how](#)

1.2 Create an IAM role for Hunters and attach the above policy to it [Show me how](#)

Principal ARN:

External ID:

1.5 Copy the created IAM role and paste it below:

Role ARN:

Figure 14. Role ARN

3. Click **Test Connection** to make sure the setup is successful.
4. Click **Create Integration** to complete the process.

Option 3: Use an Existing IAM Role

If you already have an existing IAM role, use the following steps:

1. Open the [AWS Management Console](#). Search for Identity and Access Management, and then select **IAM**.

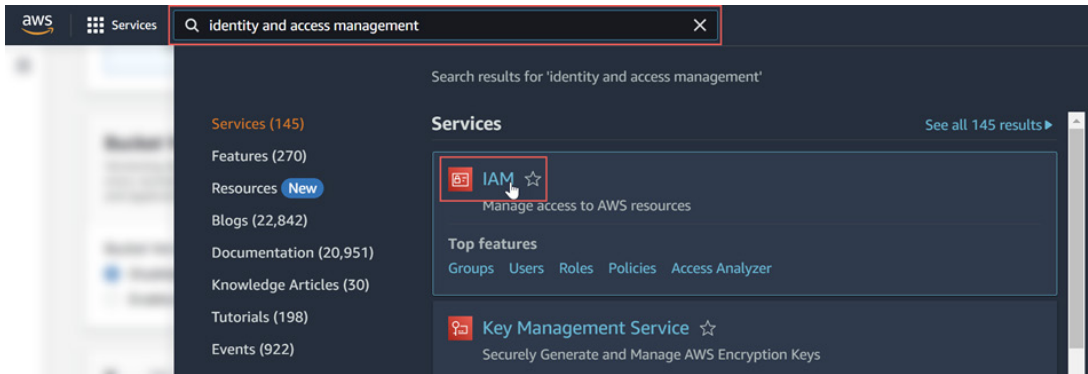


Figure 15. Identity & Access Management (IAM)

2. From the left-side navigation, select **Roles**.
3. Find the relevant role and select it.
4. Under the **Summary** section, copy the role ARN.

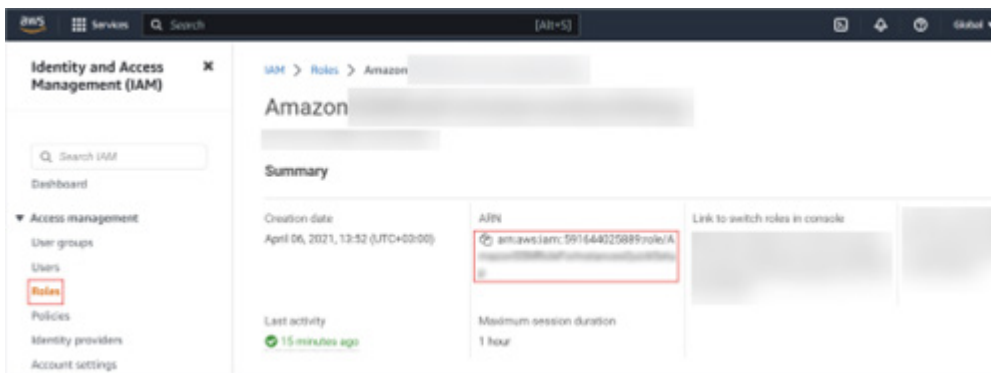
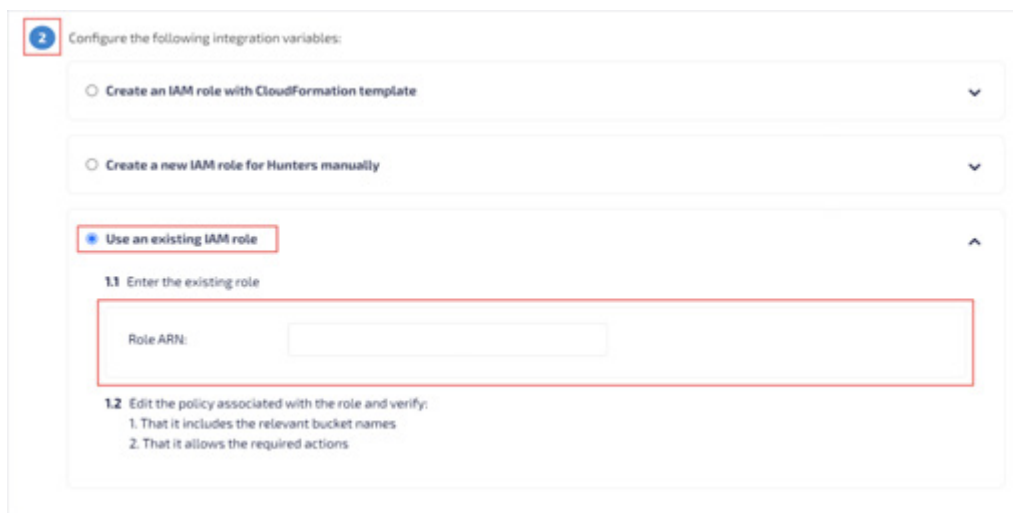


Figure 16. Role ARN

5. Return to the AWS connection process on Hunters.
6. Select **Use an existing IAM role**.
7. Paste the **Role ARN** into the **Role ARN** field.



The screenshot shows a configuration window titled 'Configure the following integration variables:'. It contains three radio button options: 'Create an IAM role with CloudFormation template', 'Create a new IAM role for Hunters manually', and 'Use an existing IAM role'. The third option is selected and highlighted with a red box. Below this, under the heading '1.1 Enter the existing role', there is a text input field labeled 'Role ARN:' which is also highlighted with a red box. Below the input field, under the heading '1.2 Edit the policy associated with the role and verify:', there are two numbered instructions: '1. That it includes the relevant bucket names' and '2. That it allows the required actions'.

Figure 17. Use an existing Role ARN

8. Click **Test Connection** to make sure the setup is successful.
9. Click **Create Integration** to complete the process.

ZPA Logs

ZPA sends its logs securely to Hunters via the Log Streaming Service (LSS). LSS is deployed using two components: a log receiver and a ZPA App Connector. LSS resides in ZPA and initiates a log stream through a ZPA Public Service Edge. The App Connector resides in your company's enterprise environment. It receives the log stream and then forwards it to a log receiver.

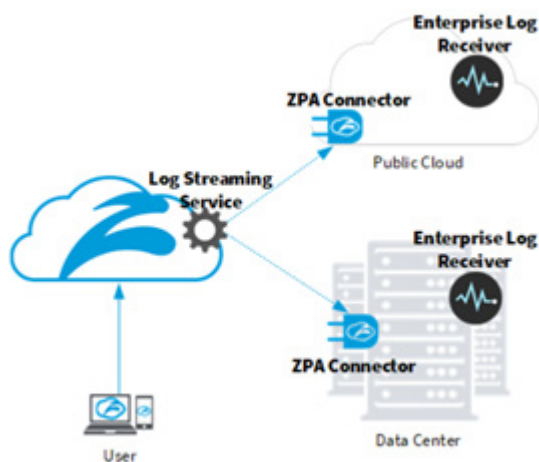


Figure 18. ZPA log architecture

For details in setting up the LSS log receiver, see [About Log Streaming Service](#) (government agencies, see [About Log Streaming Service](#)).

Hunters can parse ZPA Users Status, User Activity, App Connector Status, and Audit logs.

To learn more about the details on the fields that these log types provide, see:

- [About User Activity Log Fields](#) (government agencies, see [About User Activity Log Fields](#)).
- [About User Status Log Fields](#) (government agencies, see [About User Status Log Fields](#)).
- [About Audit Log Fields](#) (government agencies, see [About Audit Log Fields](#)).
- [About App Connector Status Log Fields](#) (government agencies, see [About App Connector Status Log Fields](#)).

The expected format of the logs is the NDJSON format as exported by Zscaler. Zscaler recommends that you log the full schema. However, you can share and ingest any subset of the fields.

Log in to the ZPA Admin Portal and go to **Configuration & Control > Private Infrastructure > Log Receivers**.

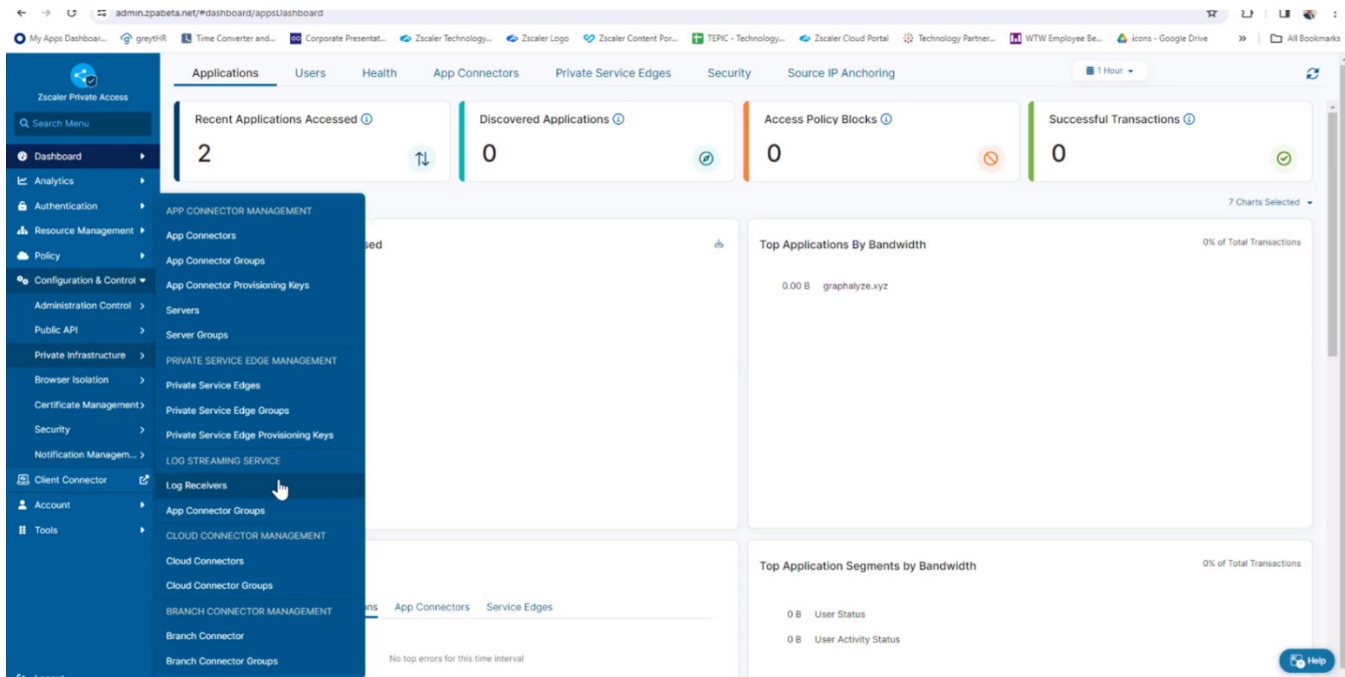


Figure 19. ZPA Log Receivers

Audit Logs

The following images show the ZPA Audit Logs.

Add Log Receiver [X]

1 Log Receiver 2 Log Stream 3 Review

Name
Hunter Audit Logs

Description

Domain or IP Address
Test.hunter.security

TCP Port
4514

TLS Encryption
Enabled Disabled

App Connector Groups
Connector Group1

Next Previous Cancel

Figure 20. Add Log Receiver

The following shows the ZPA Log Streams.

Add Log Receiver [X]

1 Log Receiver 2 Log Stream 3 Review

CONFIGURATION

Log Type
Audit Logs

Log Template
JSON

Log Stream Content

```
{
  "ModifiedTime": "%j{modifiedTime:iso8601}",
  "CreationTime": "%j{creationTime:iso8601}",
  "ModifiedBy": "%d{modifiedBy}",
  "RequestID": "%j{requestId}",
  "SessionID": "%j{sessionId}",
  "AuditOldValue": "%j{auditOldValue}",
  "AuditNewValue": "%j{auditNewValue}",
  "AuditOperationType": "%j{auditOperationType}",
  "ObjectType": "%j{objectType}",
  "ObjectName": "%j{objectName}",
  "ObjectID": "%d{objectId}",
  "CustomerID": "%d{customerId}",
  "User": "%j{modifiedByUser}",
  "ClientAuditUpdate": "%d{clientAuditUpdate}"
}
```

Next Previous Cancel

Figure 21. Add Audit Logs

User Status Logs

The following images show the ZPA Status Logs.

Add Log Receiver [X]

1 Log Receiver 2 Log Stream 3 Review

Name
Hunter User StatusLogs

Description

Domain or IP Address
Test.hunter.security

TCP Port
4514

TLS Encryption
Enabled Disabled

App Connector Groups
Connector Group1

Next Previous Cancel

Figure 22. Add Log Receiver

The following shows the ZPA Log Streams.

Add Log Receiver [X]

1 Log Receiver 2 Log Stream 3 Review

CONFIGURATION

Log Type
User Status

Log Template
JSON

Log Stream Content

```
{
  "LogTimestamp": "%{LogTimestamp:time}",
  "Customer": "%{Customer}",
  "Username": "%{Username}",
  "SessionID": "%{SessionID}",
  "SessionStatus": "%{SessionStatus}",
  "Version": "%{Version}",
  "ZEN": "%{ZEN}",
  "CertificateCN": "%{CertificateCN}",
  "PrivateIP": "%{PrivateIP}",
  "PublicIP": "%{PublicIP}",
  "Latitude": "%f{Latitude}",
  "Longitude": "%f{Longitude}",
  "CountryCode": "%{CountryCode}",
  "TimestampAuthentication": "%{TimestampAuthentication:iso8601}",
  "TimestampUnAuthentication": "%{TimestampUnAuthentication:iso8601}",
  "TotalBytesRx": "%d{TotalBytesRx}",
  "TotalBytesTx": "%d{TotalBytesTx}",
  "Idp": "%{Idp}",
  "Hostname": "%{Hostname}",
  "Platform": "%{Platform}",
  "ClientType": "%{ClientType}",
  "TrustedNetworks": "[%{TrustedNetworks}]",
  "TrustedNetworksNames": "[%{TrustedNetworksNames}]",
  "SAMLAttributes": "%{SAMLAttributes}",
  "PosturesHit": "[%{PosturesHit}]"
}
```

POLICY

SAML and SCIM Attributes Client Type Connection: Status Code

SAML and SCIM Attributes [Select IdP]

Next Previous Cancel

Figure 23. Add User Status Logs

Browser Access Logs

The following images show the ZPA Browser Access Logs.

Add Log Receiver [X]

1 Log Receiver 2 Log Stream 3 Review

Name
Hunter Browser Access Logs

Description

Domain or IP Address
Test.hunter.security

TCP Port
4514

TLS Encryption
Enabled Disabled

App Connector Groups
Connector Group1

Next Previous Cancel

Figure 24. Add Log Receiver

The following shows the ZPA Log Streams.

Add Log Receiver [X]

1 Log Receiver 2 Log Stream 3 Review

CONFIGURATION

Log Type
Browser Access

Log Template
JSON

Log Stream Content

```
{
  "LogTimestamp": "%j{LogTimestamp:time}",
  "ConnectionID": "%j{ConnectionID}",
  "Exporter": "%j{Exporter}",
  "TimestampRequestReceiveStart": "%j{TimestampRequestReceiveStart:iso8601}",
  "TimestampRequestReceiveHeaderFinish": "%j{TimestampRequestReceiveHeaderFinish:iso8601}",
  "TimestampRequestReceiveFinish": "%j{TimestampRequestReceiveFinish:iso8601}",
  "TimestampRequestTransmitStart": "%j{TimestampRequestTransmitStart:iso8601}",
  "TimestampRequestTransmitFinish": "%j{TimestampRequestTransmitFinish:iso8601}",
  "TimestampResponseReceiveStart": "%j{TimestampResponseReceiveStart:iso8601}",
  "TimestampResponseReceiveFinish": "%j{TimestampResponseReceiveFinish:iso8601}",
  "TimestampResponseTransmitStart": "%j{TimestampResponseTransmitStart:iso8601}",
  "TimestampResponseTransmitFinish": "%j{TimestampResponseTransmitFinish:iso8601}",
  "TotalTimeRequestReceive": "%d{TotalTimeRequestReceive}",
  "TotalTimeRequestTransmit": "%d{TotalTimeRequestTransmit}",
  "TotalTimeResponse"
}
```

Next Previous Cancel

Figure 25. Add Browser Access Logs

User Activity Logs

The following images show the ZPA Activity Logs.

Add Log Receiver [X]

1 Log Receiver 2 Log Stream 3 Review

Name
Hunter User Activity Logs

Description

Domain or IP Address
Test.hunter.security

TCP Port
4514

TLS Encryption
Enabled **Disabled**

App Connector Groups
Connector Group1

Next Previous Cancel

Figure 26. Add Log Receiver

The following shows the ZPA Log Streams.

Add Log Receiver [X]

1 Log Receiver 2 Log Stream 3 Review

CONFIGURATION

Log Type
User Activity

Log Template
JSON

Log Stream Content
%d{PolicyProcessingTime},"ServerSetupTime": %d{ServerSetupTime},"TimestampConnectionStart":
%j{TimestampConnectionStart:iso8601},"TimestampConnectionEnd": %j{TimestampConnectionEnd:iso8601},"TimestampCATx":
%j{TimestampCATx:iso8601},"TimestampCARx": %j{TimestampCARx:iso8601},"TimestampAppLearnStart":
%j{TimestampAppLearnStart:iso8601},"TimestampZENFirstRxClient": %j{TimestampZENFirstRxClient:iso8601},"TimestampZENFirstTxClient":
%j{TimestampZENFirstTxClient:iso8601},"TimestampZENLastRxClient": %j{TimestampZENLastRxClient:iso8601},"TimestampZENLastTxClient":
%j{TimestampZENLastTxClient:iso8601},"TimestampConnectorZENSetupComplete":

POLICY

SAML and SCIM Attributes Application Segments Segment Groups Client Types Connection: Status Code

SAML and SCIM Attributes [+ Select IdP](#)

Next Previous Cancel

Figure 27. Add User Activity Logs

Appendix A: Requesting Zscaler Support

If you need Zscaler Support to provision certain services or to help troubleshoot configuration and service issues, it is available 24/7/365.

To contact Zscaler Support:

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

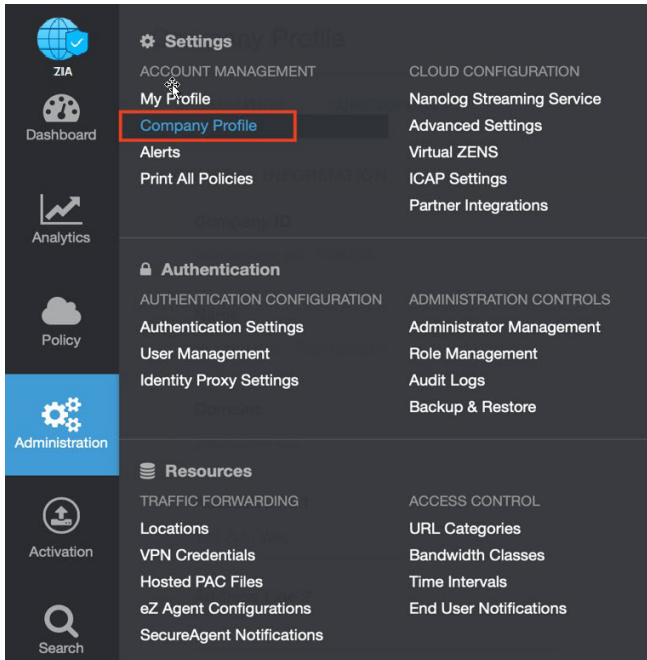


Figure 28. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.

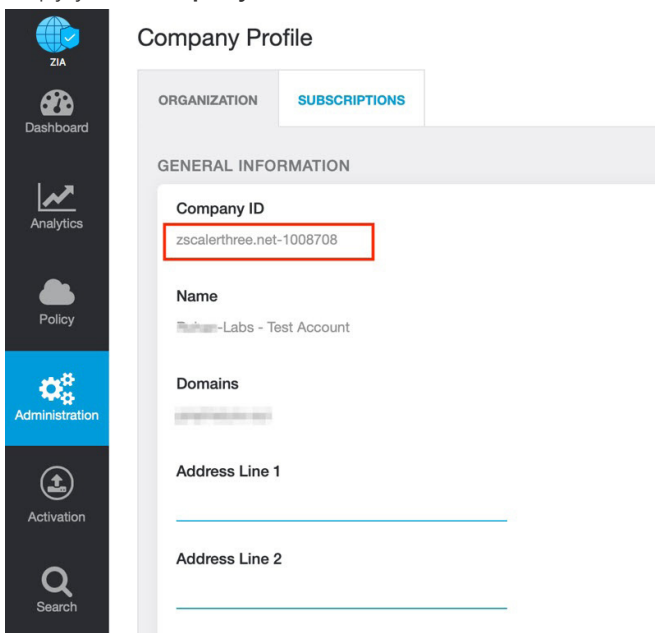


Figure 29. Company ID

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

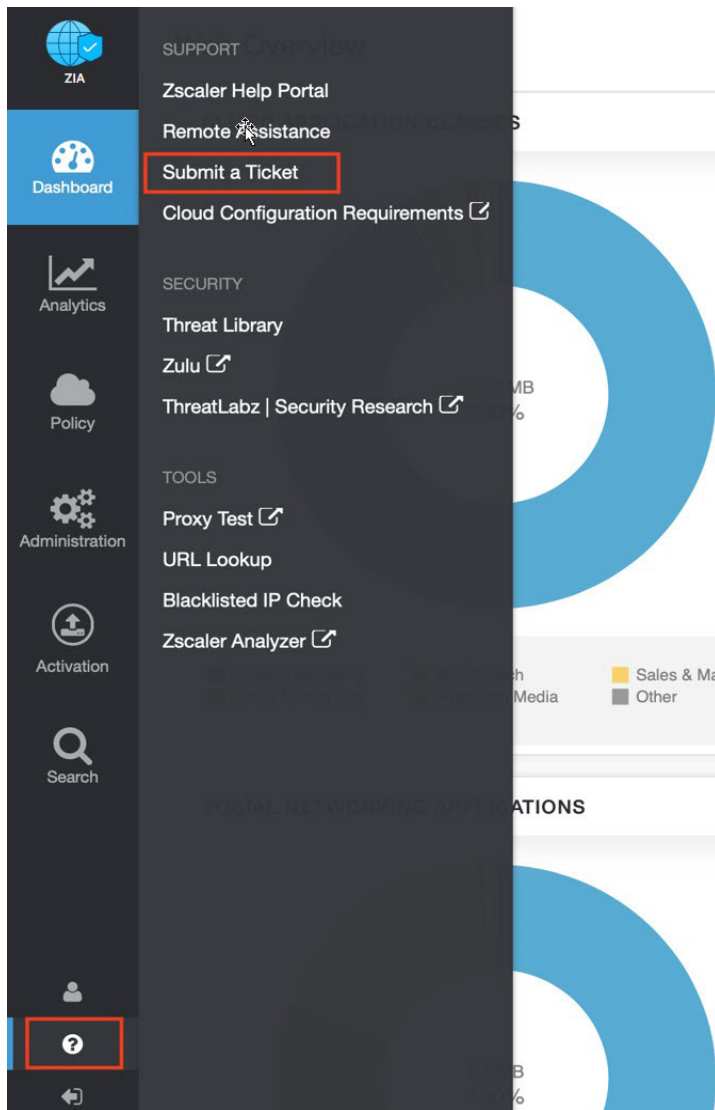


Figure 30. Submit a ticket