ZSCALER AND SENTINELONE DEPLOYMENT GUIDE

OCTOBER 2024, VERSION 1.3

BUSINESS DEVELOPMENT GUIDE

Contents

Terms and Acronyms

The following table defines acronyms used in this deployment guide. When applicable, a Request for Change (RFC) is included in the Definition column for your reference.

Acronym	Definition
CA	Central Authority (Zscaler)
CSV	Comma-Separated Values
DLP	Data Loss Prevention
DNS	Domain Name Service
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IKE	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SaaS	Software as a Service
SSL	Secure Socket Layer (RFC6101)
STAR	SentinelOne Storyline Active Response
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
XFF	X-Forwarded-For (RFC7239)
ZCP	Zscaler Cloud Protection (Zscaler)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

Trademark Notice

About This Document

The following section provides an overview of the partners in this integration.

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. To learn more, see Zscaler's website.

SentinelOne Overview

SentinelOne (NYSE: S) is a cybersecurity company with a solution that encompasses AI-powered prevention, detection, response, and hunting across endpoints, containers, cloud workloads, and IoT devices in a single autonomous platform. To learn more, refer to SentinelOne'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
- SentinelOne Resources
- Appendix A: Requesting Zscaler Support

Software Versions

This document was authored using ZIA and ZPA (with Zscaler Client Connector) along with SentinelOne 4.2 or later.

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 SentinelOne Introduction

This section contains overviews of the Zscaler and SentinelOne applications used in this guide.

⚠ 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 onramp— 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 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
ZPA Posture Profiles	Help link for how to configure ZPA posture profiles.
ZPA Access Policies	Help link for how to configure ZPA access policies with a set of configuration examples.
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
ZPA Posture Profiles	Help link for how to configure ZPA posture profiles.
ZPA Access Policies	Help link for how to configure ZPA access policies with a set of configuration examples.
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.

SentinelOne Overview

An overview of the SentinelOne Singularity Extended Detection and Response (XDR) application is described in this section.

SentinelOne Singularity XDR Overview

SentinelOne Singularity XDR unifies and extends detection and response capability across multiple security layers. Singularity XDR provides security teams with centralized end-to-end enterprise visibility, powerful analytics, and automated responses across the complete technology stack. With Singularity XDR, customers can get unified and proactive security measures to defend the entire technology stack, making it easier for your security analysts to identify and stop attacks in progress before the attacks impact the business.

SentinelOne Resources

The following table contains links to SentinelOne support resources.

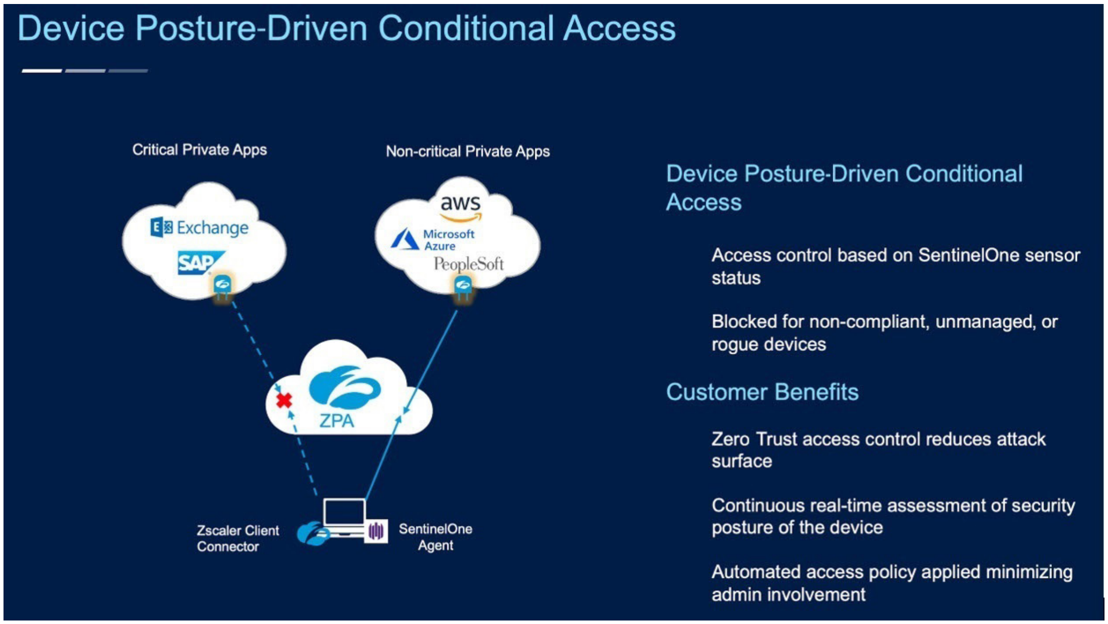
Name	Definition
SentinelOne Customer Portal	Help for SentinelOne Singularity XDR.
SentinelOne Singularity XDR Data Sheet	SentinelOne Singularity XDR data sheet.

Use Case 1: ZPA Posture Check Integration with SentinelOne

In this use case:

- ZPA verifies the presence of a running SentinelOne process on the endpoint as an assessment of end device posture. You can configure ZPA to allow only compliant endpoints (ones that pass the posture check) to access selected applications.
- ZPA evaluates ZPA "Access Policies" for conditional access, which in turn reference device level "posture check profiles." The ZPA administrator can specify (for Windows and Mac workstations) that a SentinelOne agent must be installed and running on the endpoint in order for the endpoint to be granted access to internal applications referenced via ZPA Access policy.

This conceptual diagram is an overview of the integration.



Device Posture-Driven Conditional Access

Device Posture-Driven Conditional Access

Access control based on SentinelOne sensor status

Blocked for non-compliant, unmanaged, or rogue devices

Customer Benefits

Zero Trust access control reduces attack surface

Continuous real-time assessment of security posture of the device

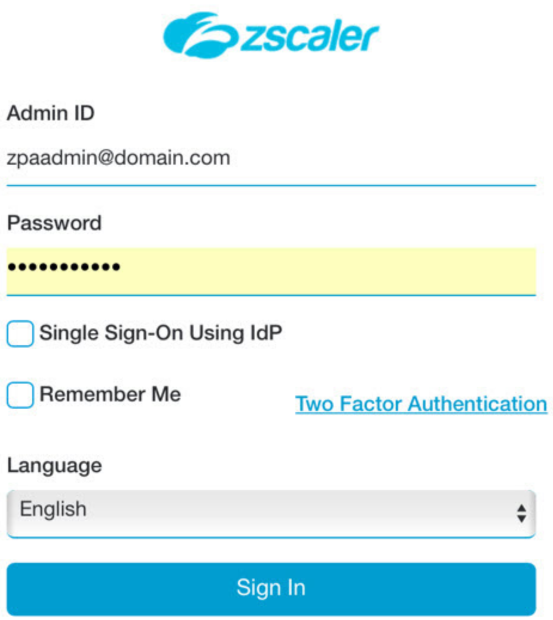
Automated access policy applied minimizing admin involvement

Figure 1. High-Level overview

Configuring ZPA

This guide assumes that you have a working ZPA set up and provides instructions to integrate posture-based conditional access as part of your existing ZPA deployment.

Log in to the ZPA Admin Portal



Admin ID

zpaadmin@domain.com

Password

●●●●●●●●●●●

□ Single Sign-On Using IdP

□ Remember Me

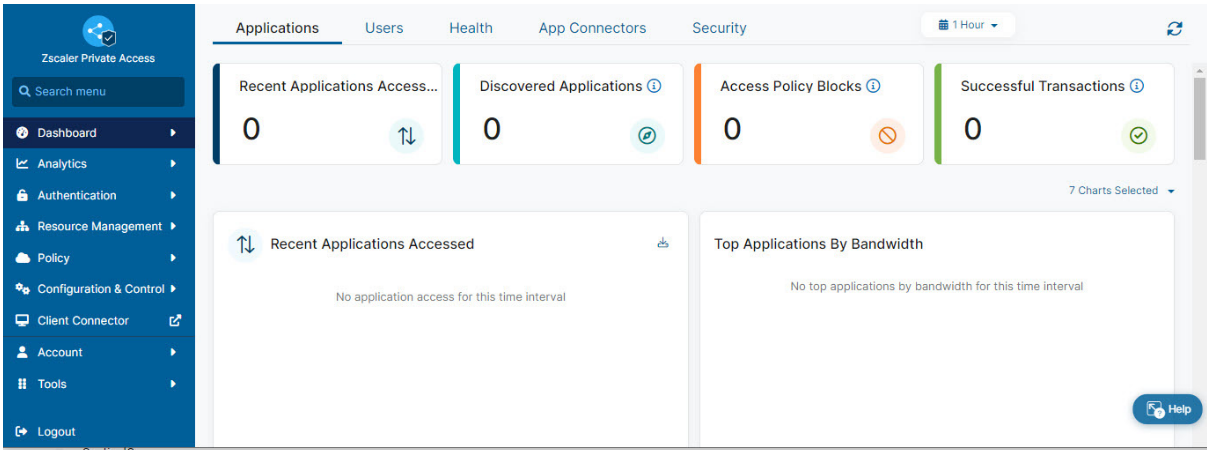
Language

English

Figure 2. Log in to ZPA Admin Portal

Go to Zscaler Client Connector

Click the **Client Connector** icon. This opens the Zscaler Client Connector.



No application access for this time interval

No top applications by bandwidth for this time interval

Figure 3. Click the Client Connector icon

Create New Posture Profile

After logging in to Zscaler Client Connector:

1. Go to **Administration** > **Device Posture**.
2. Click **Add Device Posture Profile**.

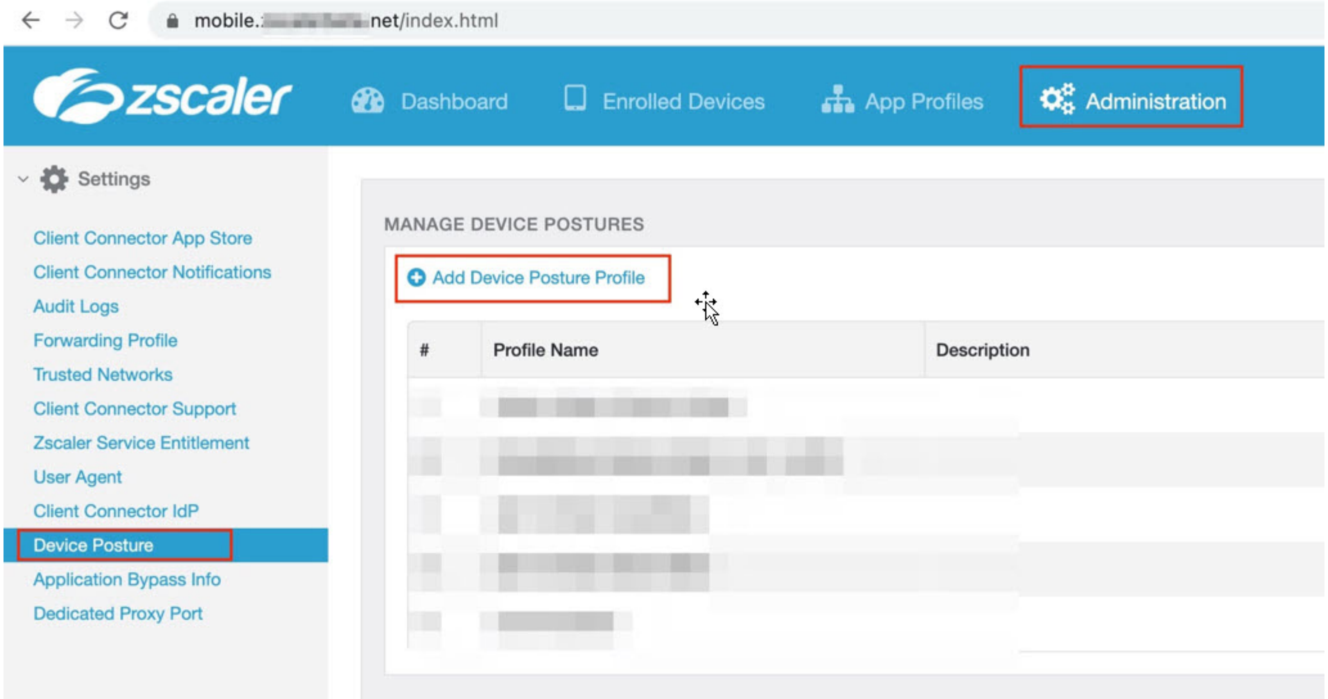


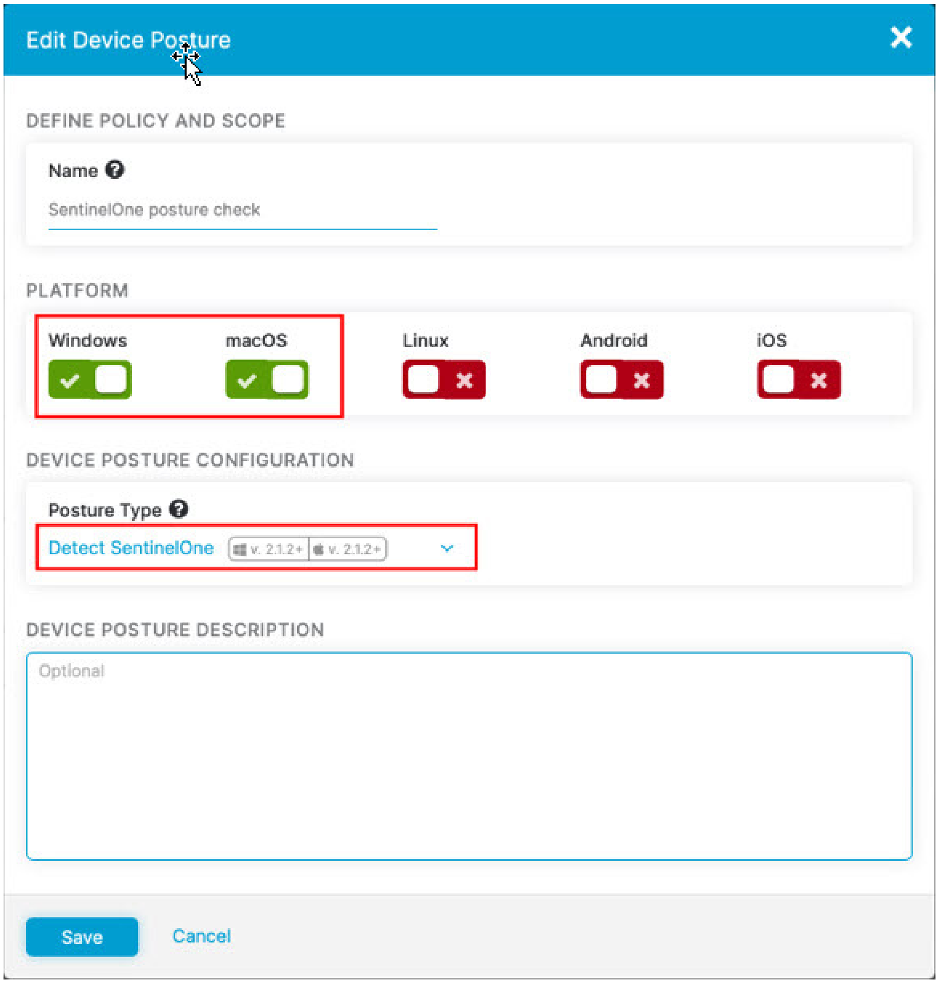
Figure 4. Add a device posture profile

Add a New SentinelOne Posture Profile

Complete the following steps:

1. Select only the **Windows** and **macOS** options.
2. Click the **Posture Type** drop-down menu.
3. Select **Detect SentinelOne**.
4. Name this policy and click **Save**.

This posture profile is referenced in a ZPA access policy. You can set up access policies to allow or deny application access based on whether the posture check passes or fails.


Edit Device Posture

DEFINE POLICY AND SCOPE

Name: SentinelOne posture check

PLATFORM

Windows ✓ macOS ✓ Linux ✗ Android ✗ iOS ✗

DEVICE POSTURE CONFIGURATION

Posture Type: Detect SentinelOne (v. 2.1.2+ | v. 2.1.2+)

DEVICE POSTURE DESCRIPTION

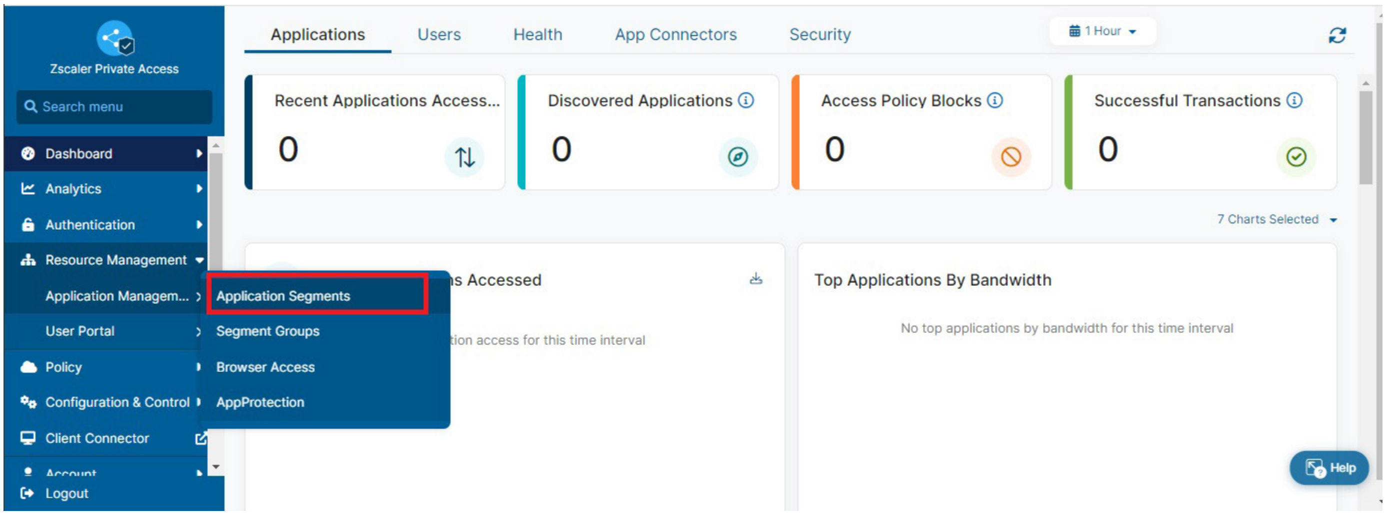
Optional

Figure 5. Add a Detect SentinelOne posture profile

Decide Which Applications Need Conditional Access

From the ZPA Admin Portal, go to **Resource Management** > **Application Management** > **Application Segments**.

This page lists applications that ZPA can access. Select one of these applications and reference it in an access policy so that access to the application is granted based on the end device's posture.



Recent Applications Access...	Discovered Applications	Access Policy Blocks	Successful Transactions
0	0	0	0

...s Accessed

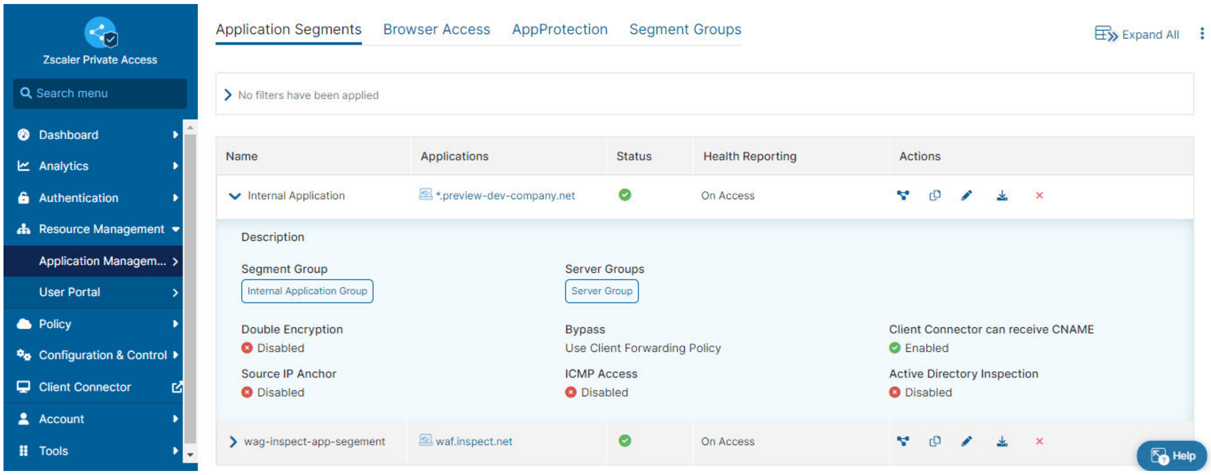
...tion access for this time interval

Top Applications By Bandwidth

No top applications by bandwidth for this time interval

Figure 6. Go to Application Segments

In the following example, ZPA can access applications that are hosted under the domain *.bd-dev.com, based on the posture of the end device.



No filters have been applied

Name	Applications	Status	Health Reporting	Actions
Internal Application	*.preview-dev-company.net	✓	On Access	
wag-inspect-app-segement	waf.inspect.net	✓	On Access	

Description

Segment Group: Internal Application Group

Server Groups: Server Group

Double Encryption: Disabled

Bypass: Use Client Forwarding Policy

Client Connector can receive CNAME: Enabled

Source IP Anchor: Disabled

ICMP Access: Disabled

Active Directory Inspection: Disabled

Figure 7. Decide which application needs conditional access

Set Up an Access Policy

From the ZPA Admin Portal, go to **Policy** > **Access Policy**.

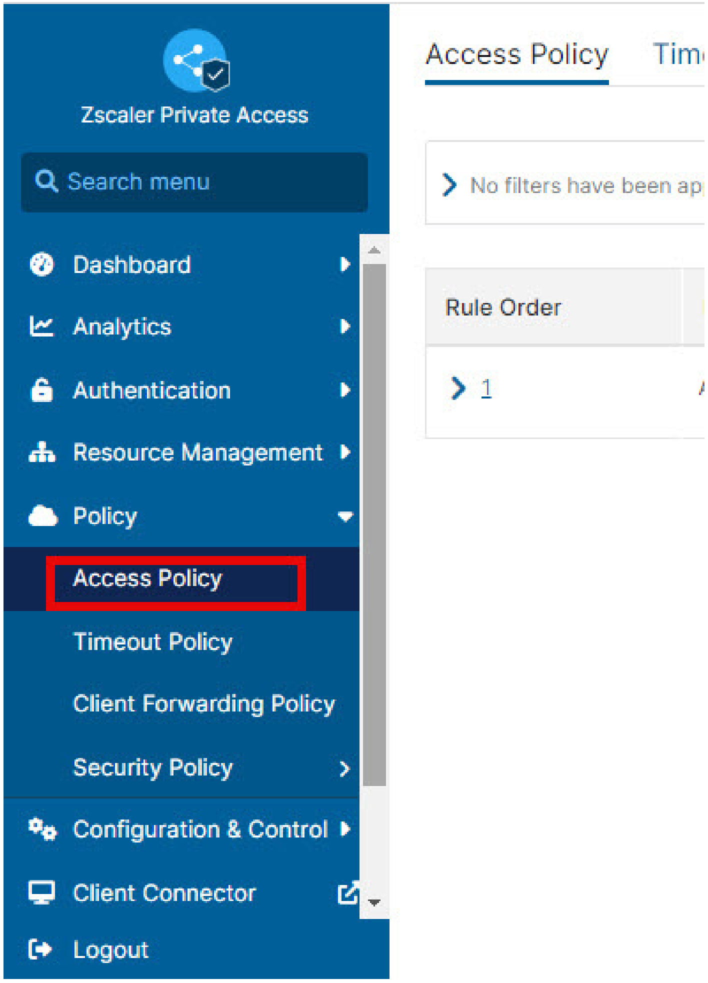


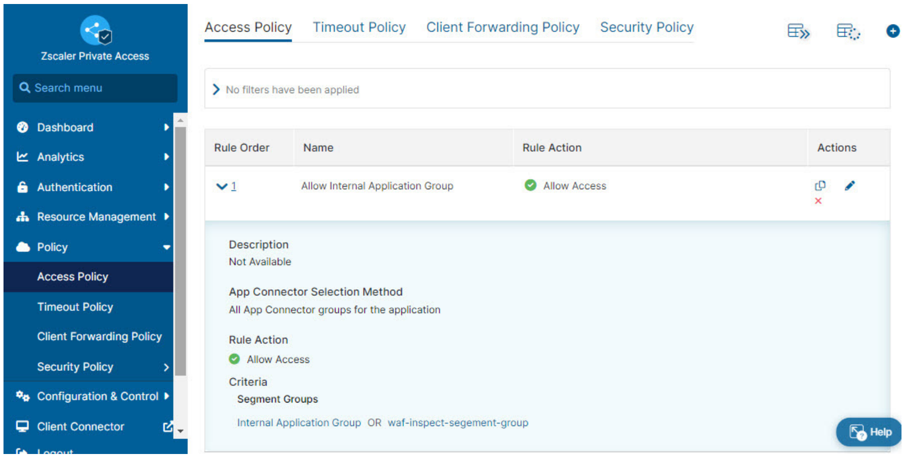
Figure 8. Set up an Access Policy

Tie the Posture Profile to This Access Policy

On the **Access** Policy tab, click **Add Rule** and reference the previously created posture profile. You can set up different access policies to protect different internal applications.

A customizable (and optional) notification message is displayed to the end users when application access is allowed or denied, informing them about the policy evaluation.

In this example, an access policy was added to block user access to the application if the SentinelOne posture check fails (Rule#1). If SentinelOne is not running on the endpoint, Rule#1 is marked true, and access is blocked. Otherwise, the policy evaluation proceeds to Rule#2 (which grants application access).



No filters have been applied

Rule Order	Name	Rule Action	Actions
1	Allow Internal Application Group	Allow Access	

Description
Not Available

App Connector Selection Method
All App Connector groups for the application

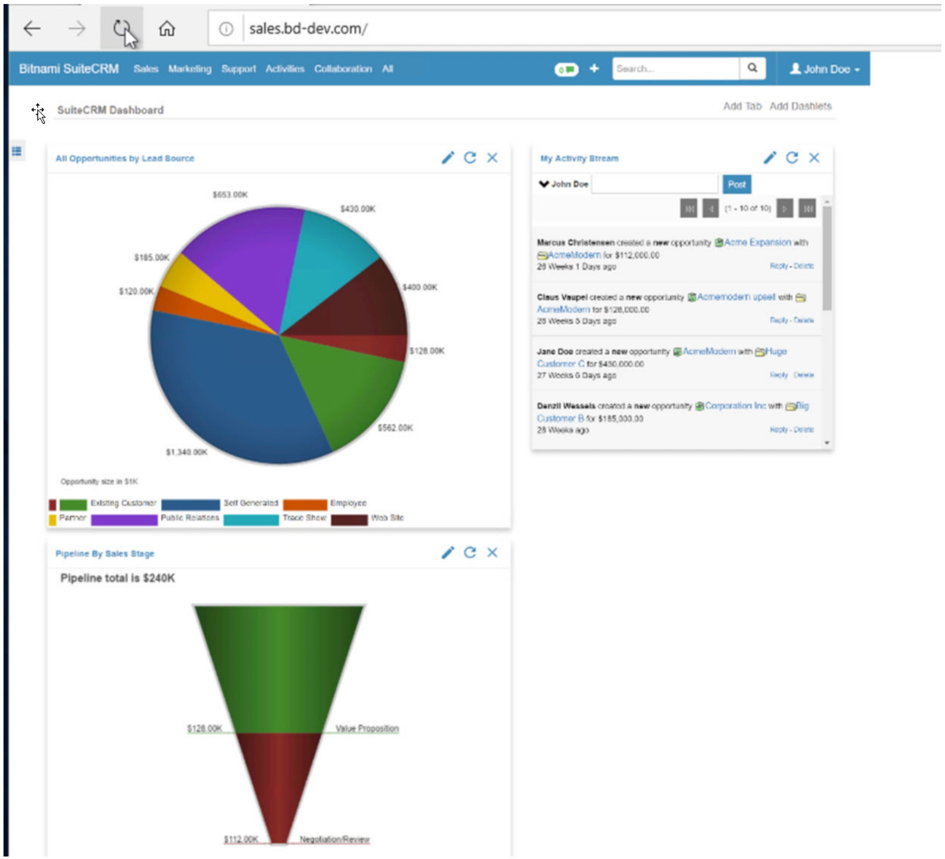
Rule Action
Allow Access

Criteria
Segment Groups
Internal Application Group OR waf-inspect-segement-group

Figure 9. Set up an access policy

Verify Conditional Access from an Endpoint

The endpoint accesses the application if the endpoint device has a SentinelOne agent installed and running. Otherwise, access is blocked by ZPA.



Marcus Christensen created a **new** opportunity Acme Expansion with AcmeModern for $112,000.00
28 Weeks 1 Days ago
Reply - Delete

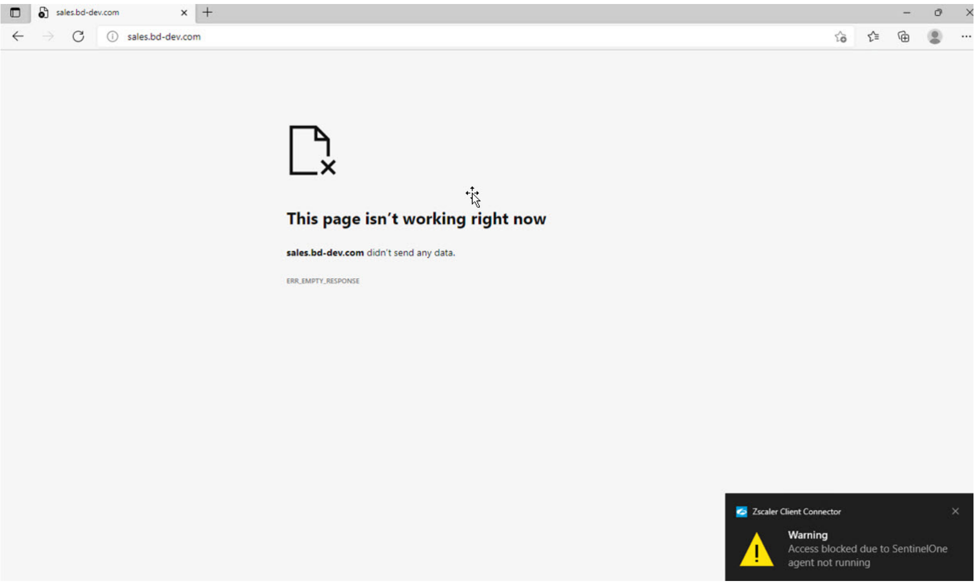
Claus Vaupel created a **new** opportunity Acmemodern upsell with AcmeModern for $128,000.00
28 Weeks 5 Days ago
Reply - Delete

Jane Doe created a **new** opportunity AcmeModern with Huge Customer C for $430,000.00
27 Weeks 6 Days ago
Reply - Delete

Denzil Wessels created a **new** opportunity Corporation Inc with Big Customer B for $185,000.00
28 Weeks ago
Reply - Delete

Figure 10. Access granted from an endpoint that has a SentinelOne agent installed and running

If access is blocked, the following message is displayed.



This page isn't working right now

sales.bd-dev.com didn't send any data.

ERR_EMPTY_RESPONSE

Zscaler Client Connector

Warning
Access blocked due to SentinelOne agent not running

Figure 11. Access blocked from an endpoint if the SentinelOne agent is not running

Use Case 2: SentinelOne XDR and Zscaler Internet Access

The Zscaler XDR app configures automatic and manual response actions initiated from SentinelOne towards Zscaler. The app also enables automatic threat enrichment, adding Zscaler data into SentinelOne detected threats.

Prerequisites

You must set up the following in advance for the integration to work:

- Configure a System for Cross-Domain Identity Management (SCIM) integration with an Identity Provider (IdP).
- Create an empty user Group on the IdP that is pushed to ZIA for use by SentinelOne. You shouldn't make any modifications to this user-group on the IdP after user-group creation. SentinelOne XDR makes SCIM API calls to ZIA to move users in and out of this group.
- Create restrictive ZIA traffic enforcement policies (URL filtering, Cloud App Control, file type control, etc.) that references the user group defined in the previous bullet.

Why Use the App?

By installing the Zscaler XDR app (which is not the Zscaler Client Connector), you can accelerate threat containment, limiting their speed and reach. With so many publicly hosted applications now holding critical data, rapidly blocking access to that data can help prevent data exfiltration. Rapid network quarantining also helps block communication to malicious servers and prevent lateral movement. By using this app in conjunction with native SentinelOne response abilities and other SentinelOne automatic response XDR apps, threat containment goes beyond the endpoint to the identity and network.

When you enable the app enrichment capability, you benefit because you can see more data points in your SentinelOne threats. The app's enrichment capabilities help you uncover user privilege because you can see the user department and whether the user is a ZIA admin. The enrichment data also shows which Zscaler groups a user is in and any comments an admin has added about that user. URLs involved in the incident are checked against Zscaler threat intelligence databases for context enrichment, and files are submitted to the Zscaler Cloud Sandbox for on-demand detonation.

Response Overview

The XDR response action adds the impacted device user to a predefined user group in ZIA. You can customize your automatic and manual response, and you can make the response as strict or permissive as fits your organization's needs. You can configure the Zscaler policy for the user group to block all traffic, block traffic to certain sites, or even force the user into browser isolation.

The automatic action uses five different conditions that trigger the app. The app can move the user identified in the threat to the predefined Zscaler policy in the following scenarios:

1. For all threats (i.e., suspicious and malicious).
2. For all malicious threats.
3. For all threats manually identified by a SentinelOne user via the **Mark as Threat** action.
4. For all threats manually reviewed and marked as **True positive**.
5. For all threats on specific, designated STAR rules.

SentinelOne Threat Enrichment Overview

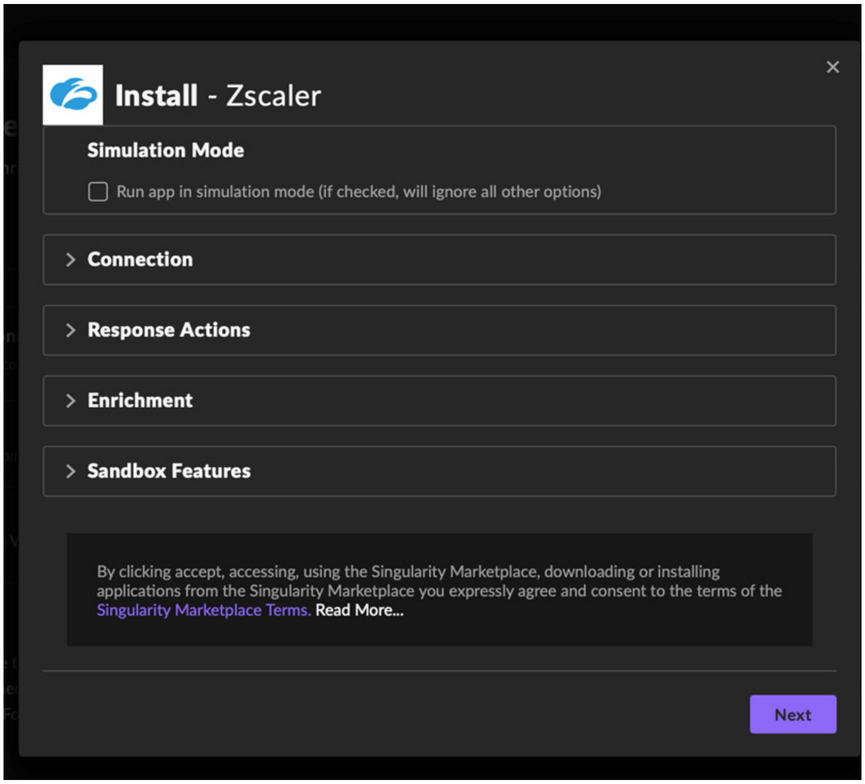
After detecting a threat, SentinelOne calls the APIs of all vendors that have enabled enrichment integrations (including Zscaler). XDR parses the API responses for the most critical information, which is then added to the threat notes and threat XDR feed. The enrichment card includes the most relevant Zscaler user information, including:

- If the ID matches an admin user.
- Comments on the user.
- The department to which the user belongs.
- The names and comments of groups to which the user belongs.
- (Optional) Zscaler XDR app can call ZIA APIs to look up reputation of any URLs encountered by SentinelOne while analyzing a threat.
- (Optional) Zscaler XDR can also submit files to Zscaler cloud sandbox for on-demand detonation.

Install the App from SentinelOne Singularity Marketplace

To install the app:

1. Open the Marketplace dashboard.
2. From the catalog of all apps, choose **Zscaler**.
3. Enter the relevant information to configure the app



By clicking accept, accessing, using the Singularity Marketplace, downloading or installing applications from the Singularity Marketplace you expressly agree and consent to the terms of the Singularity Marketplace Terms. Read More...

Figure 12. Zscaler XDR app

You can gather Zscaler SCIM information from the ZIA Admin Portal at **Administration** > **Authentication Settings** > **Identity Providers**. Select the **Edit** icon, which opens the **IdP Configuration** window. You can find the **Base URL** and the **Bearer Token** in the **Provisioning Options** section of the configuration.

   a. Enter the **Zscaler SCIM IDP Base URL name**. Example: `https://scim.scalerthree.net/1234/4567/scim`.
   b. Enter the **Zscaler SCIM bearer token**.
   c. Enter the **Company domain**.

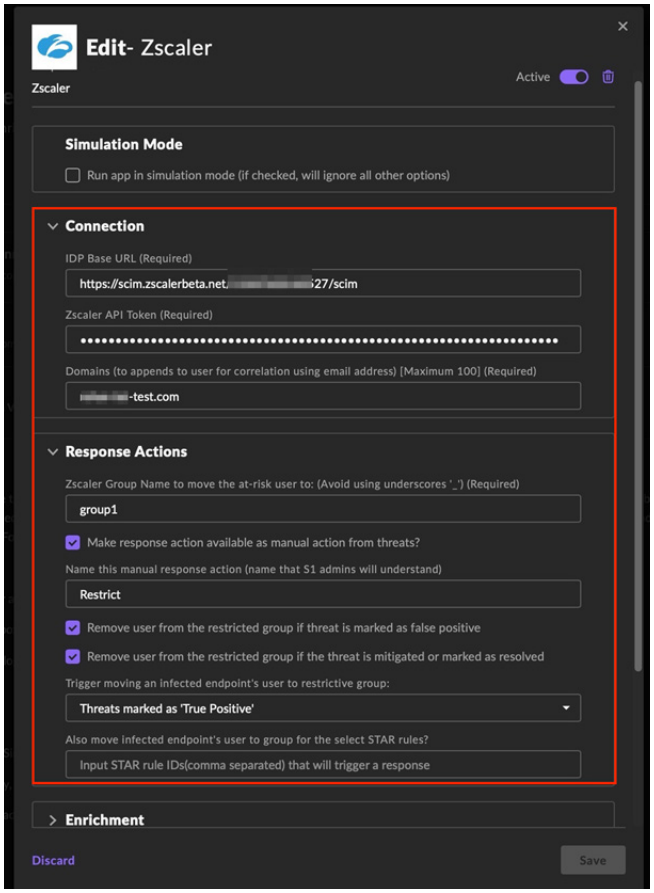
> You can configure more than one domain using a comma-separated list. Example input: `@domain.com`, `@abccompany.com`.

   d. Enable **Enrichment**, if desired.

4. (Optional) Enable Automatic Response Options.
   a. Enable **Automatically move "last logged in user" to new Zscaler group**.
   b. Enable when to trigger a response. Choose from:
      - **All threats**
      - **All malicious threats**
      - **All threats "marked as threat" by the user**
      - **When a threat is marked as True Positive**
      - **When STAR active response triggers a threat** (fill in the STAR rule ID to trigger a response)
   c. If you selected to trigger the app based on STAR threats, ensure you input which STAR rules to use.
5. Select when to remove the user from the more restrictive group:
   - When the threat is mitigated.
   - When the threat is marked as a False Positive.

   If neither is selected, the action isn’t automatically reversed. An admin must manually reverse the action in Zscaler.

6. Enable **Manual Response actions** if you want users to act manually after reviewing a threat.



Simulation Mode

☐ Run app in simulation mode (if checked, will ignore all other options)

Connection

IDP Base URL (Required)

https://scim.zscalerbeta.net/[redacted]27/scim

Zscaler API Token (Required)

••

Domains (to appends to user for correlation using email address) [Maximum 100] (Required)

[redacted]-test.com

Response Actions

Zscaler Group Name to move the at-risk user to: (Avoid using underscores '_') (Required)

group1

☑ Make response action available as manual action from threats?

Name this manual response action (name that S1 admins will understand)

Restrict

☑ Remove user from the restricted group if threat is marked as false positive

☑ Remove user from the restricted group if the threat is mitigated or marked as resolved

Trigger moving an infected endpoint's user to restrictive group:

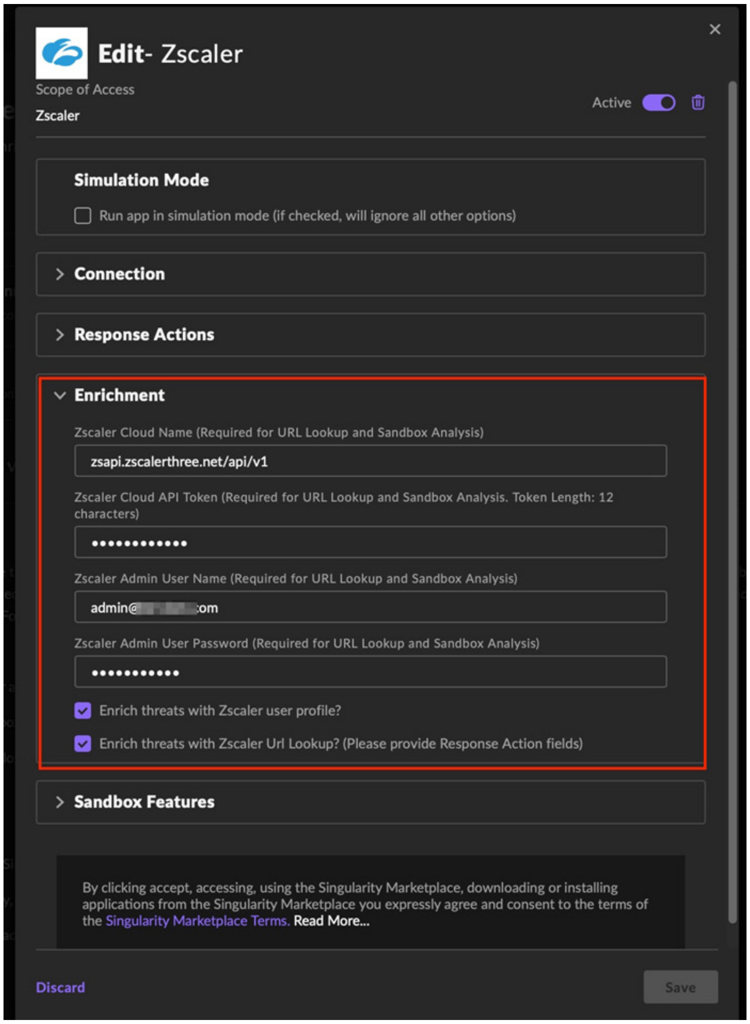
Threats marked as 'True Positive'

Also move infected endpoint's user to group for the select STAR rules?

Input STAR rule IDs(comma separated) that will trigger a response

Figure 13. Configure Zscaler XDR app and enable SCIM integration

7. Zscaler XDR app calls ZIA APIs to look up the reputation of any URLs encountered by SentinelOne while analyzing a threat. To activate the API calls, configure the **Enrichment** section of the XDR app with your ZIA API key and admin credentials.



Edit- Zscaler

Scope of Access

Zscaler

Active

Simulation Mode

☐ Run app in simulation mode (if checked, will ignore all other options)

Connection

Response Actions

Enrichment

Zscaler Cloud Name (Required for URL Lookup and Sandbox Analysis)

zsapi.zscalerthree.net/api/v1

Zscaler Cloud API Token (Required for URL Lookup and Sandbox Analysis. Token Length: 12 characters)

••••••••••••

Zscaler Admin User Name (Required for URL Lookup and Sandbox Analysis)

admin@[redacted]om

Zscaler Admin User Password (Required for URL Lookup and Sandbox Analysis)

•••••••••••

☑ Enrich threats with Zscaler user profile?

☑ Enrich threats with Zscaler Url Lookup? (Please provide Response Action fields)

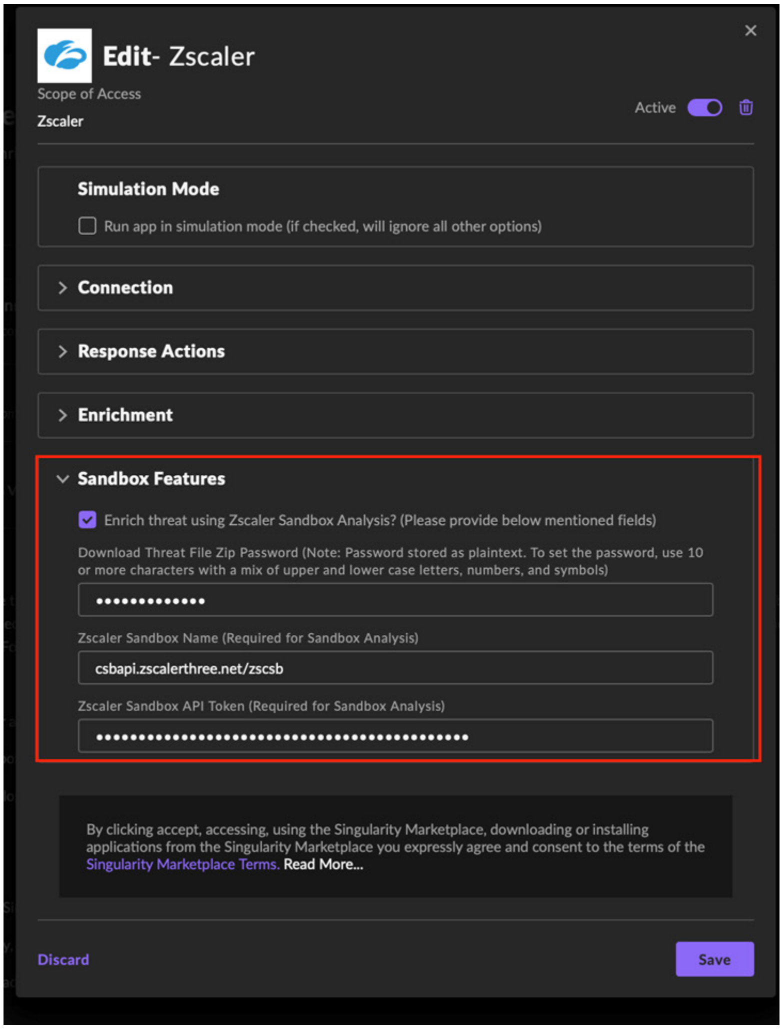
Sandbox Features

By clicking accept, accessing, using the Singularity Marketplace, downloading or installing applications from the Singularity Marketplace you expressly agree and consent to the terms of the Singularity Marketplace Terms. Read More...

Figure 14. Configure Zscaler XDR app for user and URL enrichment

8. Zscaler XDR can submit files to Zscaler Cloud Sandbox for on-demand detonation. File contents are uploaded to ZIA for sandbox analysis by SentinelOne via an API call. When available, the detailed sandbox report is downloaded and displayed in the SentinelOne console to provide additional context to the admin. This requires a ZIA license to submit files to Cloud Sandbox via API. To learn more about API credentials, see ZIA sandbox submission credentials (government agencies, see ZIA sandbox submission credentials).

   To download a threat file, the ZIP password must be at least 10 characters and include a mix of uppercase, lowercase, and special characters.



Edit- Zscaler

Scope of Access

Zscaler

Active

Simulation Mode

□ Run app in simulation mode (if checked, will ignore all other options)

Sandbox Features

☑ Enrich threat using Zscaler Sandbox Analysis? (Please provide below mentioned fields)

Download Threat File Zip Password (Note: Password stored as plaintext. To set the password, use 10 or more characters with a mix of upper and lower case letters, numbers, and symbols)

•••••••••••••

Zscaler Sandbox Name (Required for Sandbox Analysis)

csbapi.zscalerthree.net/zscsb

Zscaler Sandbox API Token (Required for Sandbox Analysis)

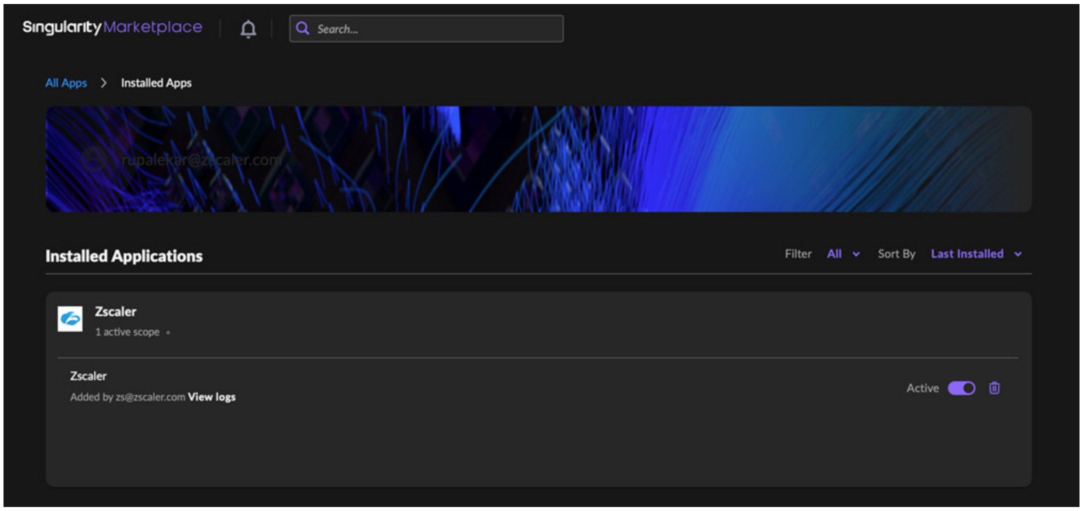
••

By clicking accept, accessing, using the Singularity Marketplace, downloading or installing applications from the Singularity Marketplace you expressly agree and consent to the terms of the Singularity Marketplace Terms. Read More...

Figure 15. Configure Zscaler XDR app for ZIA sandbox submission

9. Click **Save**.

10. Select a scope to install this app to and click **Install**. When all credentials are configured correctly, app Activation is successful.



Installed Applications

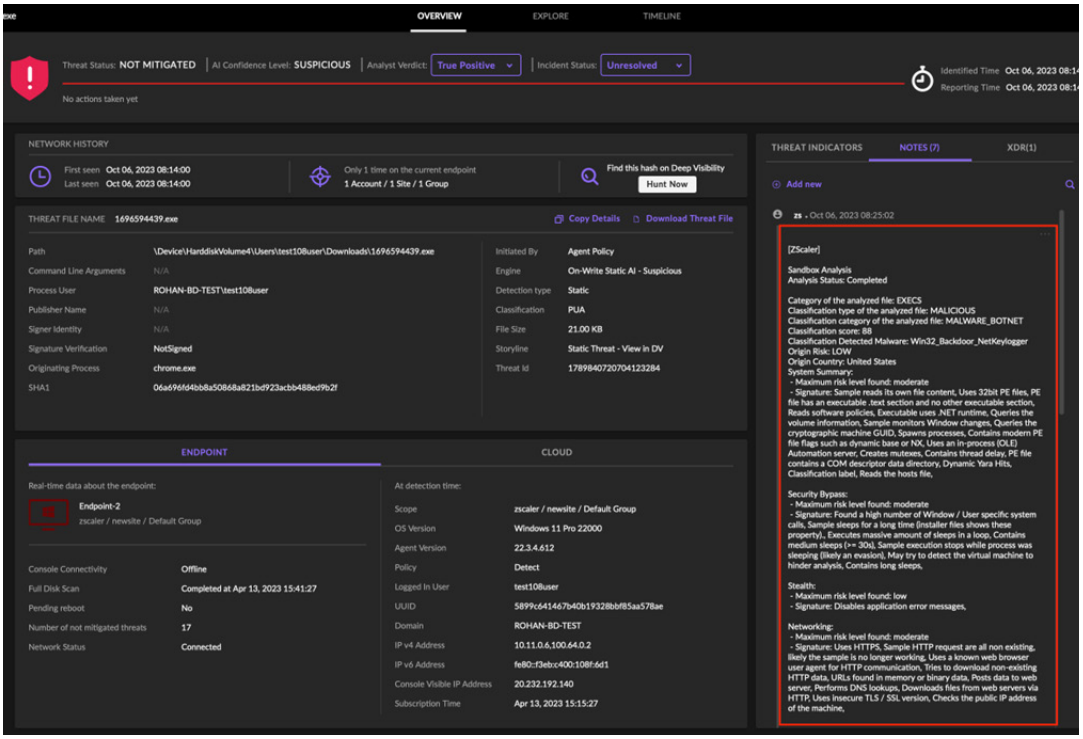
Zscaler
1 active scope

Zscaler
Added by zs@zscaler.com View logs

Active

Figure 16. Activating Zscaler XDR app

The following image shows a ZIA Sandbox report.



Threat Status: NOT MITIGATED | AI Confidence Level: SUSPICIOUS | Analyst Verdict: True Positive | Incident Status: Unresolved

No actions taken yet

Identified Time Oct 06, 2023 08:14
Reporting Time Oct 06, 2023 08:14

NETWORK HISTORY

First seen Oct 06, 2023 08:14:00
Last seen Oct 06, 2023 08:14:00

Only 1 time on the current endpoint
1 Account / 1 Site / 1 Group

Find this hash on Deep Visibility

THREAT FILE NAME 1696594439.exe

Path	\Device\HarddiskVolume4\Users\test108user\Downloads\1696594439.exe	Initiated By	Agent Policy
Command Line Arguments	N/A	Engine	On-Write Static AI - Suspicious
Process User	ROHAN-BD-TEST\test108user	Detection type	Static
Publisher Name	N/A	Classification	PUA
Signer Identity	N/A	File Size	21.00 KB
Signature Verification	NotSigned	Storyline	Static Threat - View in DV
Originating Process	chrome.exe	Threat Id	1789840720704123284
SHA1	06a696fd4bb8a50868a821bd923acbb488ed9b2f		

Real-time data about the endpoint:

Endpoint-2
zscaler / newsite / Default Group

Console Connectivity	Offline
Full Disk Scan	Completed at Apr 13, 2023 15:41:27
Pending reboot	No
Number of not mitigated threats	17
Network Status	Connected

At detection time:

Scope	zscaler / newsite / Default Group
OS Version	Windows 11 Pro 22000
Agent Version	22.3.4.612
Policy	Detect
Logged In User	test108user
UUID	5899c641467b40b19328bbf85aa578ae
Domain	ROHAN-BD-TEST
IP v4 Address	10.11.0.6,100.64.0.2
IP v6 Address	fe80::f3eb:c400:108f:6d1
Console Visible IP Address	20.232.192.140
Subscription Time	Apr 13, 2023 15:15:27

zs • Oct 06, 2023 08:25:02

```
[ZScaler]

Sandbox Analysis
Analysis Status: Completed

Category of the analyzed file: EXECS
Classification type of the analyzed file: MALICIOUS
Classification category of the analyzed file: MALWARE_BOTNET
Classification score: 88
Classification Detected Malware: Win32_Backdoor_NetKeylogger
Origin Risk: LOW
Origin Country: United States
System Summary:
 - Maximum risk level found: moderate
 - Signature: Sample reads its own file content, Uses 32bit PE files, PE
file has an executable .text section and no other executable section,
Reads software policies, Executable uses .NET runtime, Queries the
volume information, Sample monitors Window changes, Queries the
cryptographic machine GUID, Spawns processes, Contains modern PE
file flags such as dynamic base or NX, Uses an in-process (OLE)
Automation server, Creates mutexes, Contains thread delay, PE file
contains a COM descriptor data directory, Dynamic Yara Hits,
Classification label, Reads the hosts file,

Security Bypass:
 - Maximum risk level found: moderate
 - Signature: Found a high number of Window / User specific system
calls, Sample sleeps for a long time (installer files shows these
property)., Executes massive amount of sleeps in a loop, Contains
medium sleeps (>= 30s), Sample execution stops while process was
sleeping (likely an evasion), May try to detect the virtual machine to
hinder analysis, Contains long sleeps,

Stealth:
 - Maximum risk level found: low
 - Signature: Disables application error messages,

Networking:
 - Maximum risk level found: moderate
 - Signature: Uses HTTPS, Sample HTTP request are all non existing,
likely the sample is no longer working, Uses a known web browser
user agent for HTTP communication, Tries to download non-existing
HTTP data, URLs found in memory or binary data, Posts data to web
server, Performs DNS lookups, Downloads files from web servers via
HTTP, Uses insecure TLS / SSL version, Checks the public IP address
of the machine,
```

Figure 17. ZIA Sandbox report in SentinelOne console

Use Case 3: Ingesting Zscaler Logs with DataSet (Scalyr)

You can use DataSet to ingest ZIA logs and leverage Zscaler data. There are two options for forwarding ZIA logs to DataSet: via the DataSet's log ingestion API (preferred) or by deploying an NSS VM and a DataSet agent.

Prerequisites

You must have the following in advance for the integration to work:

- Admin access to SentinelOne and DataSet console.
- Admin access to ZIA Admin Portal.

Option A: Cloud-to-Cloud Logging Using API

Setting up RESTful forwarding is the Zscaler recommendation for forwarding ZIA logs:

1. Log in and go to **Administration** > **Cloud Configuration** > **Nano Streaming Service** > **Cloud NSS Feeds** > **Add Cloud NSS Feed**.

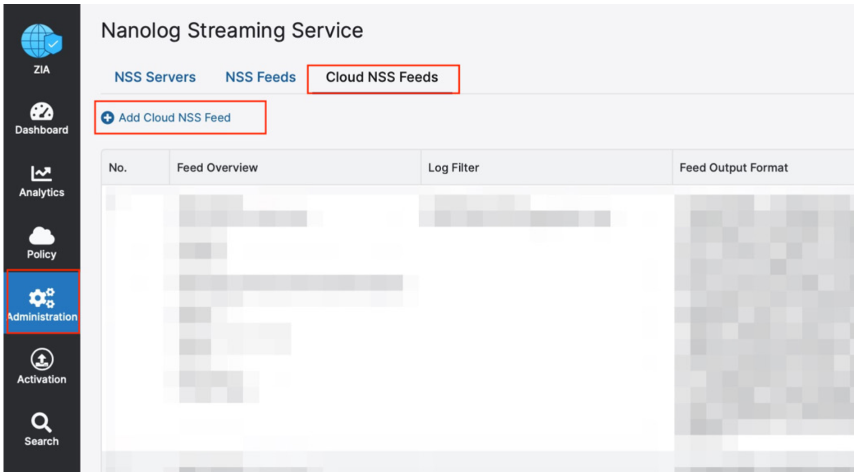
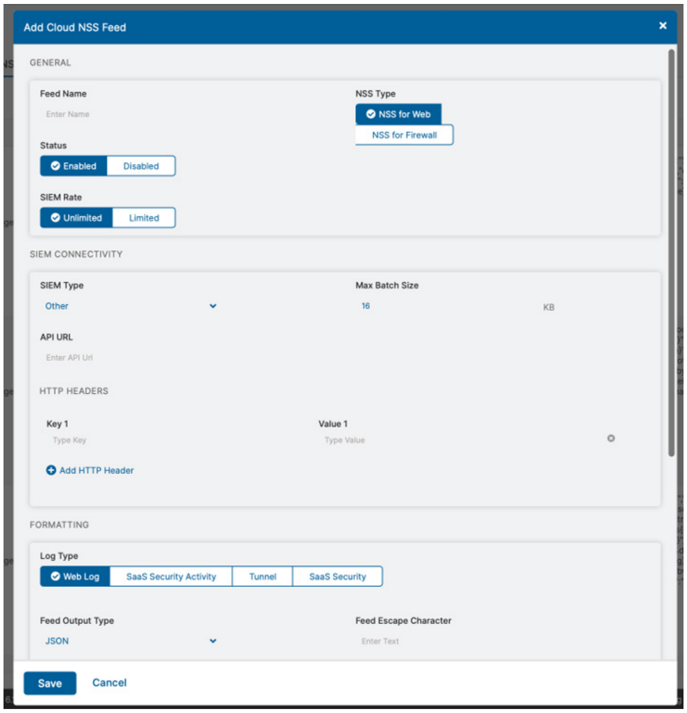


Figure 18. Go to cloud-to-cloud logging section in ZIA

2. Configure the field:
   - **Feed name**: {{desired_name}}
   - **API URL**: https://app.scalyr.com/api/uploadLogs?serverHost={{desired_host_name}}&logfile={{desired_logfile_name}}&parser=zscaler&token={{DataSet_write_log_key}}

> The host portion of the API URL (i.e. , "app.scalyr.com") might be different depending on the location of your DataSet tenant. To find your data in DataSet, use the query:
>
> ```
> serverHost contains "desired_host_name" OR logfile contains "desired_log_file_name"
> OR  parser contains "zscaler"
> ```
>
> Replace the values in the API URL as desired.

   - **Feed Output Type**: JSON
   - **SIEM Type**: Other
   - **HTTP Headers**: Content-Type application/gzip
   - **Log Type**: {{desired_log_type}} (i.e., Web/Firewall/DNS, etc.)



Add Cloud NSS Feed

GENERAL

Feed Name: Enter Name

NSS Type: ● NSS for Web | NSS for Firewall

Status: ● Enabled | Disabled

SIEM Rate: ● Unlimited | Limited

SIEM CONNECTIVITY

SIEM Type: Other

Max Batch Size: 16 KB

API URL: Enter API Url

HTTP HEADERS

Key 1: Type Key

Value 1: Type Value

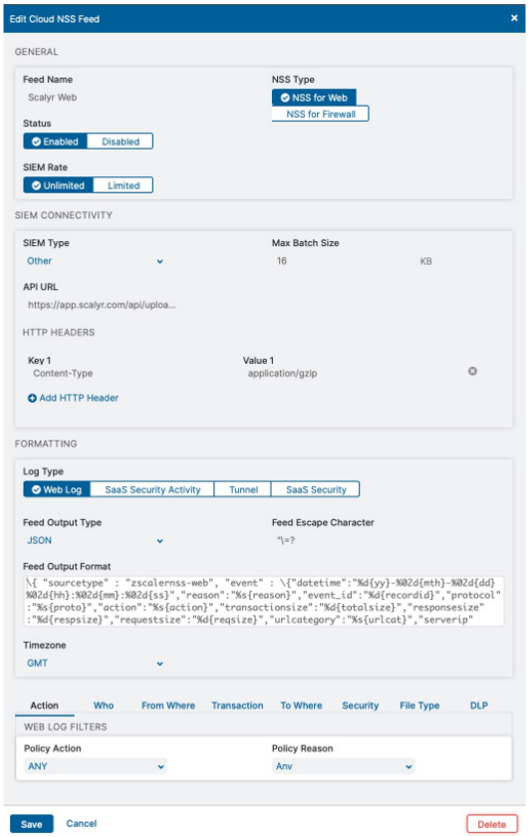
FORMATTING

Log Type: ● Web Log | SaaS Security Activity | Tunnel | SaaS Security

Feed Output Type: JSON

Feed Escape Character: Enter Text

Figure 19. Configure Cloud NSS Feed



GENERAL

Feed Name: Scalyr Web

NSS Type: NSS for Web

Status: Enabled

SIEM Rate: Unlimited

SIEM CONNECTIVITY

SIEM Type: Other

Max Batch Size: 16 KB

API URL: https://app.scalyr.com/api/uploa...

HTTP HEADERS

Key 1: Content-Type

Value 1: application/gzip

FORMATTING

Log Type: Web Log

Feed Output Type: JSON

Feed Escape Character: "\=?

Feed Output Format:

```
\{ "sourcetype" : "zscalernss-web", "event" : \{"datetime":"%d{yy}-%02d{mth}-%02d{dd}
%02d{hh}:%02d{mm}:%02d{ss}","reason":"%s{reason}","event_id":"%d{recordid}","protocol"
:"%s{proto}","action":"%s{action}","transactionsize":"%d{totalsize}","responsesize"
:"%d{respsize}","requestsize":"%d{reqsize}","urlcategory":"%s{urlcat}","serverip"
```

Timezone: GMT

WEB LOG FILTERS

Policy Action: ANY

Policy Reason: Anv

Figure 20. Example with all fields populated (Web)

If using an NSS-VM-based approach, copy the following log format and paste it into the **Feed Output Format**. Also, set the **Feed Output Type** to **Custom** for web logs, and add **,** \" (comma, backslash, double quote) to the **Feed Escape Character** list.

```
\{ "sourcetype" : "zscalernss-web", "event" : \{"datetime":"%d{yy}-%02d{mth}-
%02d{dd} %02d{hh}:%02d{mm}:%02d{ss}","reason":"%s{reason}","event_id":
"%d{recordid}","protocol":"%s{proto}","action":"%s{action}","transactionsize":
"%d{totalsize}","responsesize":"%d{respsize}","requestsize":"%d{reqsize}",
"urlcategory":"%s{urlcat}","serverip":"%s{sip}","clienttranstime":"%d{ctime}",
"requestmethod":"%s{reqmethod}","refererURL":"%s{ereferer}","useragent":
"%s{eua}","product":"NSS","location":"%s{elocation}","ClientIP":"%s{cip}",
"status":"%s{respcode}","user":"%s{elogin}","url":"%s{eurl}","vendor":
"Zscaler","hostname":"%s{ehost}","clientpublicIP":"%s{cintip}",
"threatcategory":"%s{malwarecat}","threatname":"%s{threatname}","filetype":
"%s{filetype}","appname":"%s{appname}","pagerisk":"%d{riskscore}",
"department":"%s{edepartment}","urlsupercategory":"%s{urlsupercat}",
"appclass":"%s{appclass}","dlpengine":"%s{dlpeng}","urlclass":"%s{urlclass}",
"threatclass":"%s{malwareclass}","dlpdictionaries":"%s{dlpdict}","fileclass":
"%s{fileclass}","bwthrottle":"%s{bwthrottle}","servertranstime":"%d{stime}",
"contenttype":"%s{contenttype}","unscannabletype":"%s{unscannabletype}",
"deviceowner":"%s{deviceowner}","devicehostname":"%s{devicehostname}"\}\}
```

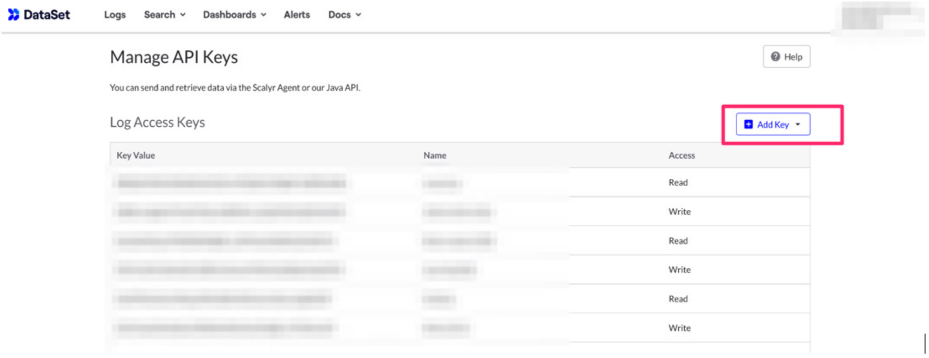
3. Set up DataSet. See Set Up DataSet (if Using DataSet API for Log Ingestion).

Set Up DataSet (if Using DataSet API for Log Ingestion)

You must set up DataSet to integrate with ZIA logs.

Create API key for log ingestion

1. Use DataSet's uploadLogs api endpoint. (Zscaler pushes gzipped logs into DataSet.)
2. As a DataSet admin, create a DataSet API key with log write access.



Manage API Keys

You can send and retrieve data via the Scalyr Agent or our Java API.

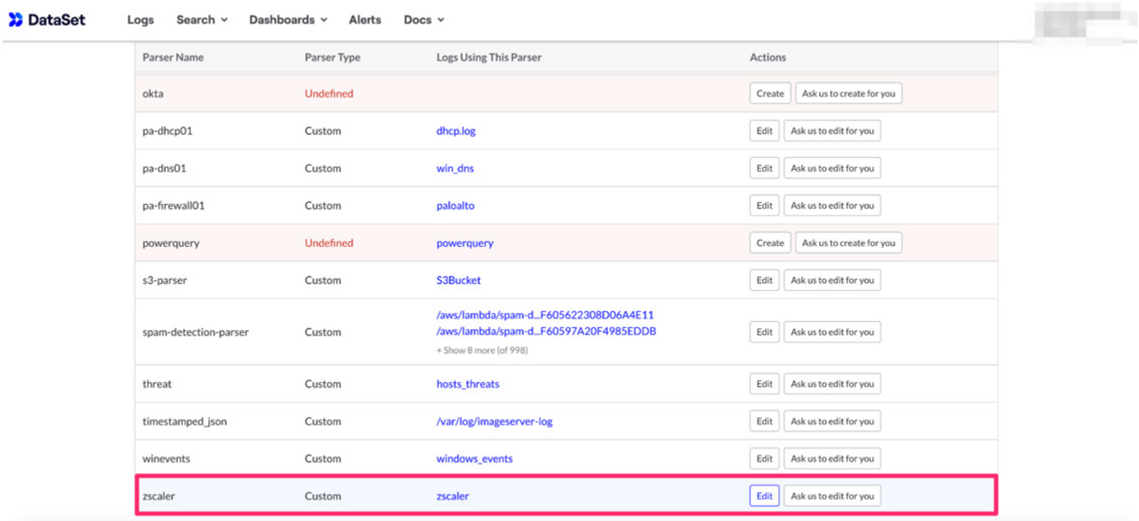
Log Access Keys

Key Value	Name	Access
[redacted]	[redacted]	Read
[redacted]	[redacted]	Write
[redacted]	[redacted]	Read
[redacted]	[redacted]	Write
[redacted]	[redacted]	Read
[redacted]	[redacted]	Write

Figure 21. Manage API keys

Apply Parser

1. Select the **Zscaler parser** on the Parser page.
2. **Apply** the Zscaler parser.



Parser Name	Parser Type	Logs Using This Parser	Actions
okta	Undefined		Create Ask us to create for you
pa-dhcp01	Custom	dhcp.log	Edit Ask us to edit for you
pa-dns01	Custom	win_dns	Edit Ask us to edit for you
pa-firewall01	Custom	paloalto	Edit Ask us to edit for you
powerquery	Undefined	powerquery	Create Ask us to create for you
s3-parser	Custom	S3Bucket	Edit Ask us to edit for you
spam-detection-parser	Custom	/aws/lambda/spam-d...F605622308D06A4E11 /aws/lambda/spam-d...F60597A20F4985EDDB + Show 8 more (of 998)	Edit Ask us to edit for you
threat	Custom	hosts_threats	Edit Ask us to edit for you
timestamped_json	Custom	/var/log/imageserver-log	Edit Ask us to edit for you
winevents	Custom	windows_events	Edit Ask us to edit for you
zscaler	Custom	zscaler	Edit Ask us to edit for you

Figure 22. Apply parser

3. Paste this API key into the ZIA Admin Portal by going to **Administration** > **Cloud Service API Security** > **Cloud Service API Key**.

Apply Dashboard

1. Select the **Dashboards** drop-down menu and then click **New Dashboard**.
2. Select **Edit JSON**.
3. Apply **Zscaler Dashboard**.

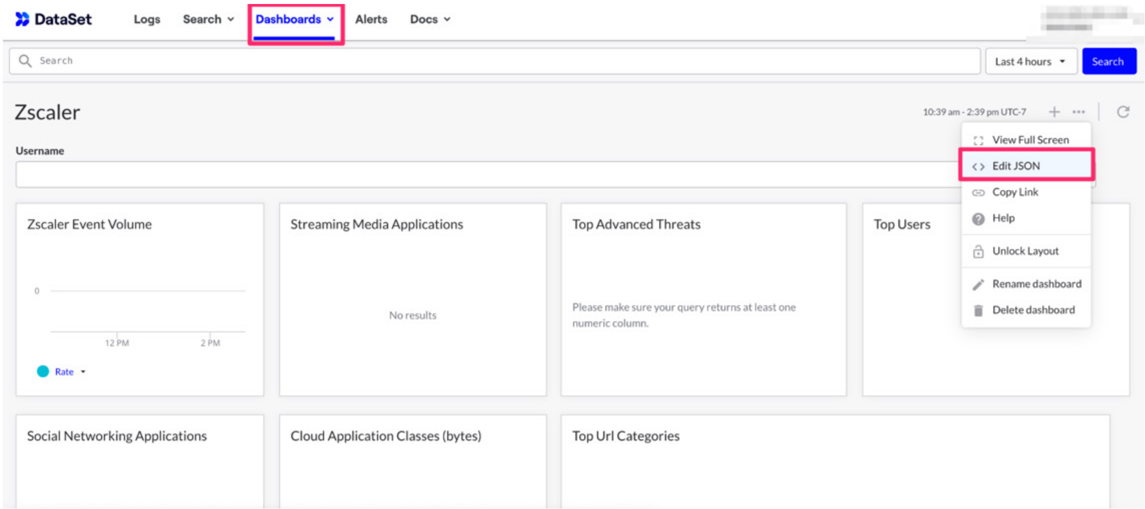


Figure 23. Apply Zscaler dashboard

Option B: Syslog

1. Log in and go to **Administration** > **Cloud Configuration** > **Nano Streaming Service**.

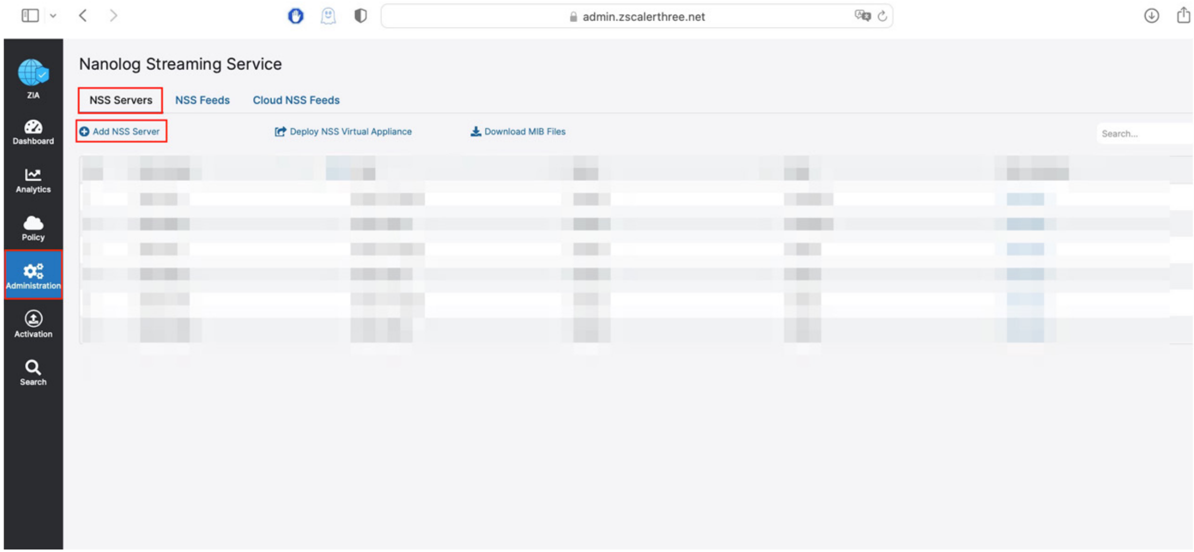


Figure 24. Go to the NSS section in ZIA

2. Deploy the NSS Server (VM). This NSS VM makes an outbound TLS connection to ZIA to get the encrypted, compressed logs from Zscaler's logging plane, and initiates a separate TCP connection to the Scalyr agent to stream plain text, uncompressed ZIA logs to that Scalyr agent.

Since communication from the NSS VM to the Scalyr agent is in plain text, you can start the NSS VM on the same network as the Scalyr agent.

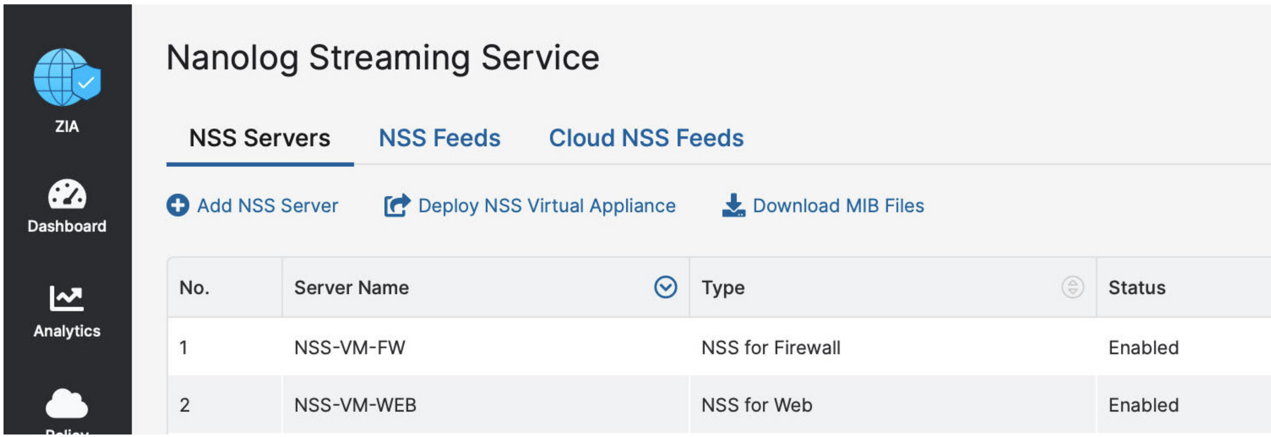
3. See the NSS VM deployment guide for your platform:
   - NSS Deployment Guide for Microsoft Azure (government agencies, see NSS Deployment Guide for Microsoft Azure).
   - NSS Deployment Guide for Amazon Web Services (government agencies, see NSS Deployment Guide for Amazon Web Services).
   - NSS Deployment Guide for VMware vSphere (government agencies, see NSS Deployment Guide for VMware vSphere).

Add NSS Server

Before you set up an NSS server on the ZIA Admin Portal, you must enter information about your traffic and users so that the Zscaler service can compute the appropriate resources for your NSS. The NSS buffers logs for at least one hour. If a SIEM goes offline for maintenance, or if the connection between the NSS and the SIEM is disrupted, the NSS sends buffered logs when the connection is re-established. The amount of memory required to buffer the logs is incorporated into the VM spec computation. The buffer size increases proportionally to the amount of RAM allocated to the NSS.

To add an NSS server:

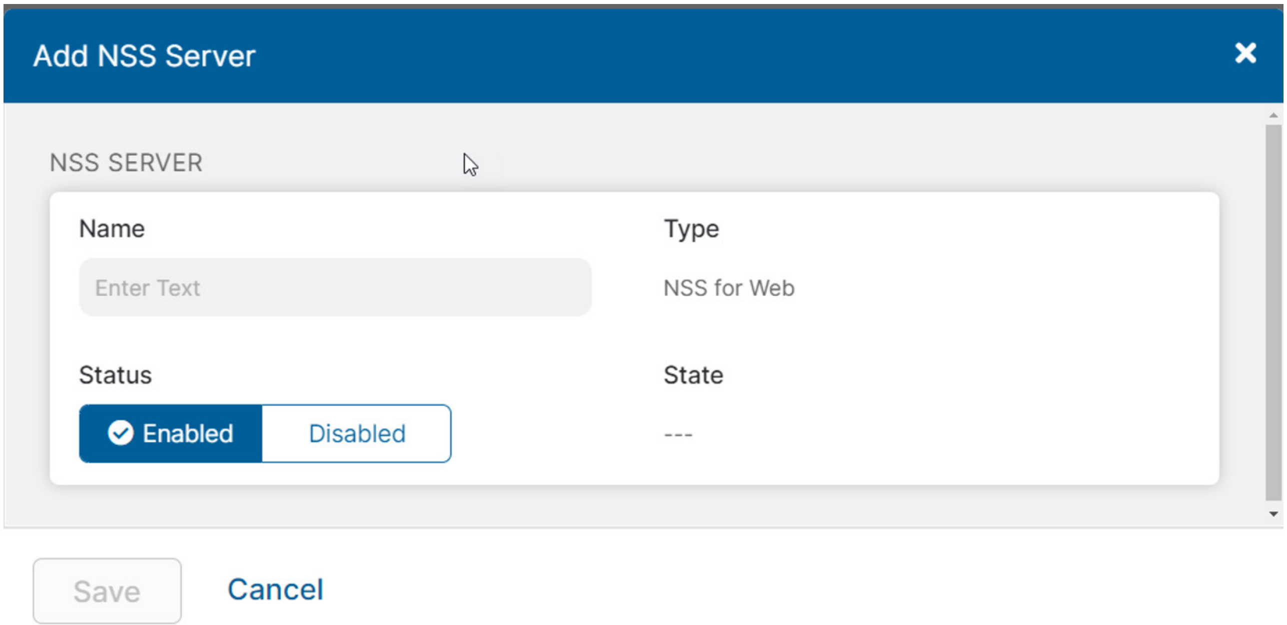
1. Go to **Administration** > **Nanolog Streaming Service**.



No.	Server Name	Type	Status
1	NSS-VM-FW	NSS for Firewall	Enabled
2	NSS-VM-WEB	NSS for Web	Enabled

Figure 25. Go to Nanolog Streaming Service

2. In the **NSS Servers** tab, click **Add NSS Server**.
3. In the **Add NSS Server** window:
   - **Name**: Enter a name for the NSS.
   - **Type**: **NSS for Web** is selected by default. If you are configuring an NSS for firewall logs, select **NSS for Firewall**.
   - **Status**: The NSS is **Enabled** by default.



Add NSS Server

NSS SERVER

Name: Enter Text

Type: NSS for Web

Status: ● Enabled ○ Disabled

State: ---

Figure 26. Add NSS Server

4. Click **Save**.
5. Click **Download** in the **SSL Certificate** column of the NSS that you are configuring, and then save the certificate. You'll upload the certificate to the desired platform.
6. Deploy the DataSet agent on the NSS server.
7. Set up the DataSet syslog monitor.
8. Point the NSS server to the Syslog Monitor.
9. Set up DataSet. See Set Up DataSet (if Using NSS VM).

Set Up DataSet (if Using NSS VM)

You must set up DataSet to integrate with ZIA logs.

Set Up DataSet (Scalyr) Agent

1. Set up DataSet Agent on a separate VM.
2. Install Syslog monitor to listen on a port on the local network.

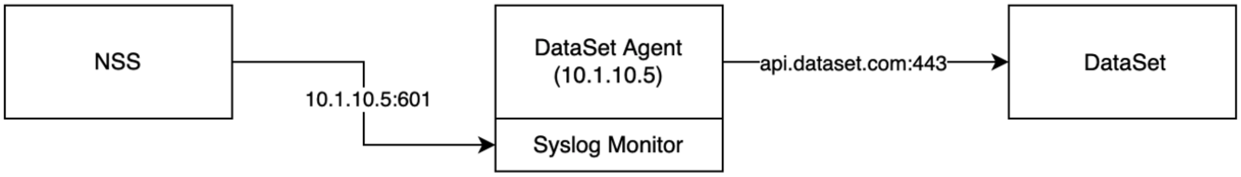
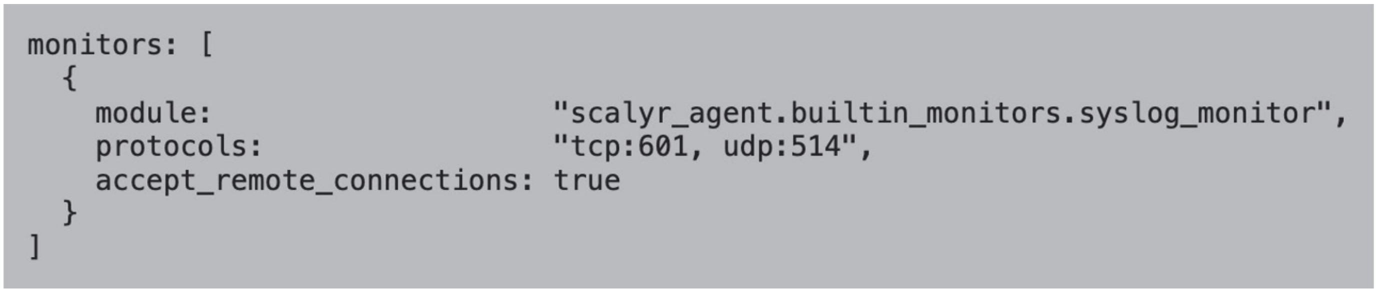


Figure 27. Syslog monitor

The following is a monitor configuration example.

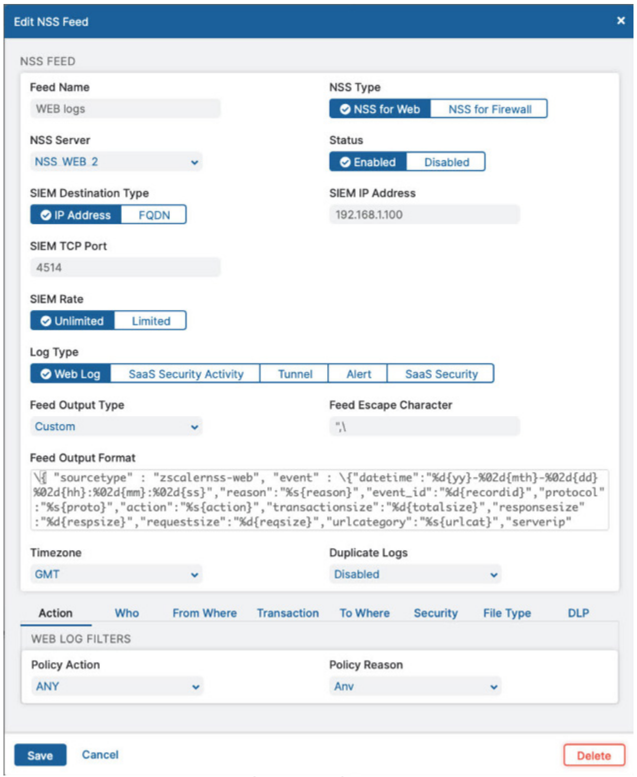


```
monitors: [
  {
    module:                    "scalyr_agent.builtin_monitors.syslog_monitor",
    protocols:                 "tcp:601, udp:514",
    accept_remote_connections: true
  }
]
```

Figure 28. Example Monitor Config

3. If using an NSS-VM-based approach for web logs, you must copy the following log format and paste it into the **Feed Output Format**. Also, set the **Feed Output Type** to **Custom** for web logs, and add **,\"** (comma, backslash, double quote) to the **Feed Escape Character** list.

```
\{ "sourcetype" : "zscalernss-web", "event" : \{"datetime":"%d{yy}-
%02d{mth}-%02d{dd} %02d{hh}:%02d{mm}:%02d{ss}","reason":"%s{reason}","event_
id":"%d{recordid}","protocol":"%s{proto}","action":"
%s{action}","transactionsize":"%d{totalsize}","responsesize":"
%d{respsize}","requestsize":"%d{reqsize}","urlcategory":"%s{urlcat}",
"serverip":"%s{sip}","clienttranstime":"%d{ctime}","requestmethod":
"%s{reqmethod}","refererURL":"%s{ereferer}","useragent":"%s{eua}",
"product":"NSS","location":"%s{elocation}","ClientIP":"%s{cip}",
"status":"%s{respcode}","user":"%s{elogin}","url":"%s{eurl}","vendor":
"Zscaler","hostname":"%s{ehost}","clientpublicIP":"%s{cintip}",
"threatcategory":"%s{malwarecat}","threatname":"%s{threatname}",
"filetype":"%s{filetype}","appname":"%s{appname}","pagerisk":
"%d{riskscore}","department":"%s{edepartment}","urlsupercategory":
"%s{urlsupercat}","appclass":"%s{appclass}","dlpengine":"%s{dlpeng}",
"urlclass":"%s{urlclass}","threatclass":"%s{malwareclass}",
"dlpdictionaries":"%s{dlpdict}","fileclass":"%s{fileclass}","bwthrottle":
"%s{bwthrottle}","servertranstime":"%d{stime}","contenttype":"%s{contenttype}",
"unscannabletype":"%s{unscannabletype}","deviceowner":"%s{deviceowner}",
"devicehostname":"%s{devicehostname}"\}\}
```



Feed Name: WEB logs

NSS Type: ● NSS for Web | NSS for Firewall

NSS Server: NSS_WEB_2

Status: ● Enabled | Disabled

SIEM Destination Type: ● IP Address | FQDN

SIEM IP Address: 192.168.1.100

SIEM TCP Port: 4514

SIEM Rate: ● Unlimited | Limited

Log Type: ● Web Log | SaaS Security Activity | Tunnel | Alert | SaaS Security

Feed Output Type: Custom

Feed Escape Character: ",\

Feed Output Format:

```
\{ "sourcetype" : "zscalernss-web", "event" : \{"datetime":"%d{yy}-%02d{mth}-%02d{dd}
%02d{hh}:%02d{mm}:%02d{ss}","reason":"%s{reason}","event_id":"%d{recordid}","protocol"
:"%s{proto}","action":"%s{action}","transactionsize":"%d{totalsize}","responsesize"
:"%d{respsize}","requestsize":"%d{reqsize}","urlcategory":"%s{urlcat}","serverip"
```

Timezone: GMT

Duplicate Logs: Disabled

Policy Action: ANY

Policy Reason: Any

Figure 29. Edit NSS Feed (web logs)

4. If using an NSS-VM-based approach for firewall logs, you must copy the following log format and paste it into the **Feed Output Format**. Also, set the **Feed Output Type** to **Custom** for firewall logs.

```
\{ "sourcetype" : "zscalernss-fw", "event" :\{"datetime":"%s{time}","user":
"%s{elogin}","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}"\}\}
```

Apply Parser

1. Select the **Zscaler parser** on the **Parser** page.
2. **Apply** the Zscaler parser.

Apply Dashboard

1. Select the **Dashboards** drop-down menu and then click **New Dashboard**.
2. Click **Edit JSON**.
3. **Apply** Zscaler Dashboard.

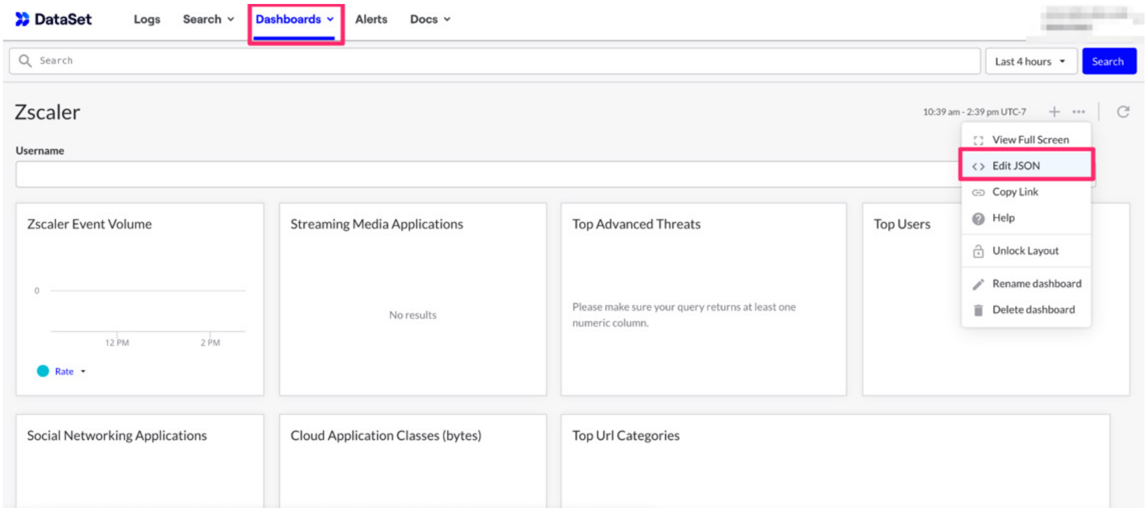


Figure 30. Apply Zscaler dashboard

Use Case 4: Contextualizing Risk–Avalor UVM and SentinelOne

Avalor's Data Fabric and Unified Vulnerability Management (UVM) solution ingests, normalizes, and unifies data across enterprise security and business systems to deliver actionable insights, analytics, and operational efficiencies.

The following steps demonstrate how Avalor UVM can leverage SentinelOne assets, threats, and vulnerabilities, combined with data from other sources, to contextualize and calculate personalized risk assessments for the organization.

Step 1: Ensure the Prerequisites are Met

Ensure there is network connectivity from the Avalor UVM Admin Portal to the SentinelOne Singularity portal on HTTPS port 443.

Step 2: Create or Regenerate an API Key in Singularity Operations Center

First, log in to the SentinelOne platform:

1. Click your **(Username)** > **My Profile**.

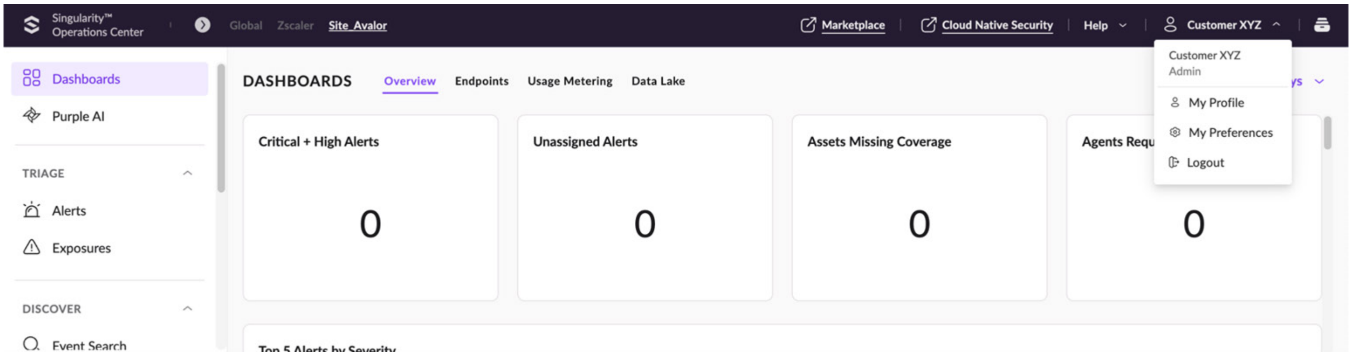
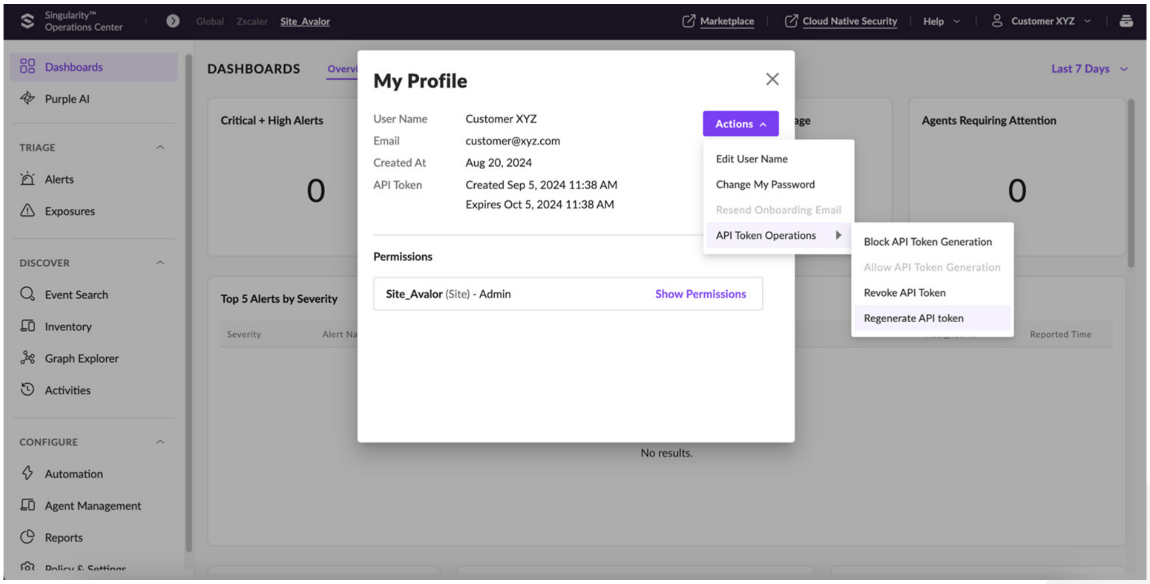


Figure 31. My Profile

2. Click **Actions**.
3. In the **API Token Operations** menu, click **Regenerate API Token** (alternatively, click **Generate API Token**).
4. Enter the **Description**.



My Profile

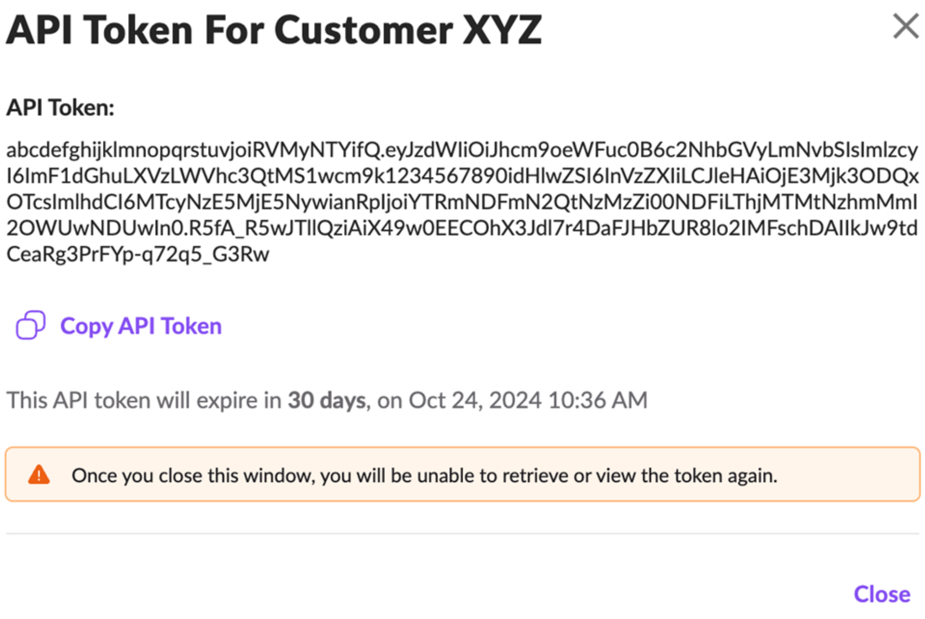
User Name Customer XYZ
Email customer@xyz.com
Created At Aug 20, 2024
API Token Created Sep 5, 2024 11:38 AM
Expires Oct 5, 2024 11:38 AM

Permissions

Site_Avalor (Site) - Admin

Figure 32. Regenerate API token

5. Copy the API Token.



API Token For Customer XYZ

API Token:

abcdefghijklmnopqrstuvjoiRVMyNTYifQ.eyJzdWliOiJhcm9oeWFuc0B6c2NhbGVyLmNvbSIsImlzcyI6ImF1dGhuLXVzLWVhc3QtMS1wcm9k1234567890idHlwZSI6InVzZXIiLCJleHAiOjE3Mjk3ODQxOTcsImlhdCI6MTcyNzE5MjE5NywianRpIjoiYTRmNDFmN2QtNzMzZi00NDFiLThjMTMtNzhmMmI2OWUwNDUwIn0.R5fA_R5wJTllQziAiX49w0EECOhX3Jdl7r4DaFJHbZUR8lo2IMFschDAIIkJw9tdCeaRg3PrFYp-q72q5_G3Rw

This API token will expire in **30 days**, on Oct 24, 2024 10:36 AM

Once you close this window, you will be unable to retrieve or view the token again.

Figure 33. API token

Step 3: Configure the Avalor UVM Data Connectors—SentinelOne Assets

From the Avalor UVM Admin Portal:

1. Click **Configure**.

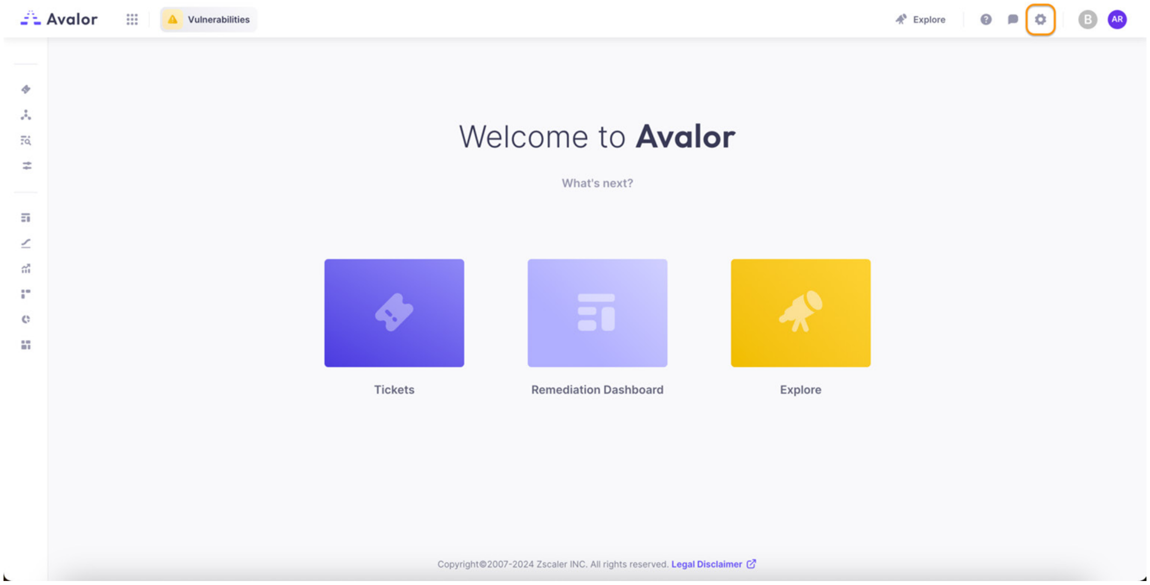


Figure 34. Configure

2. Click **Create**.
3. Click the **SentinelOne Assets** connector.

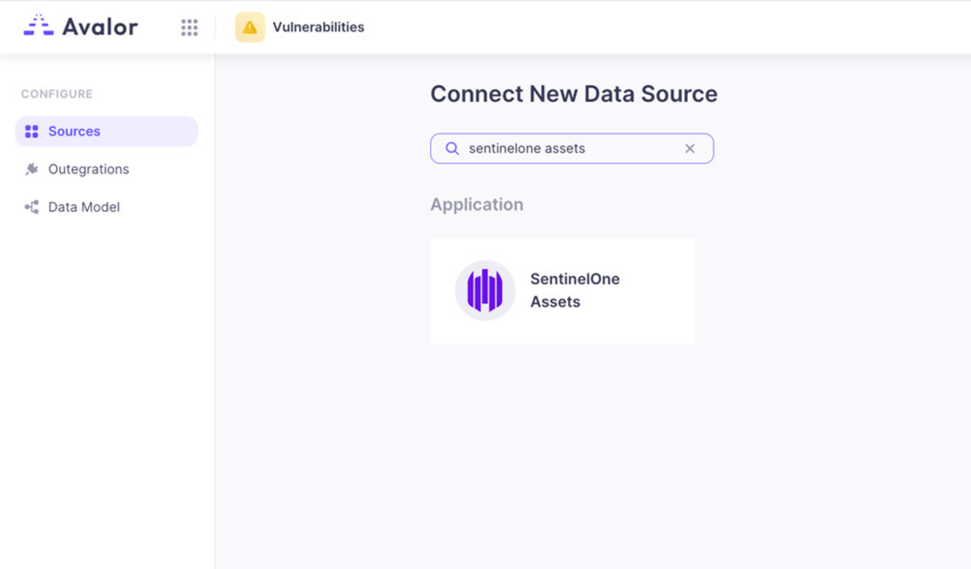
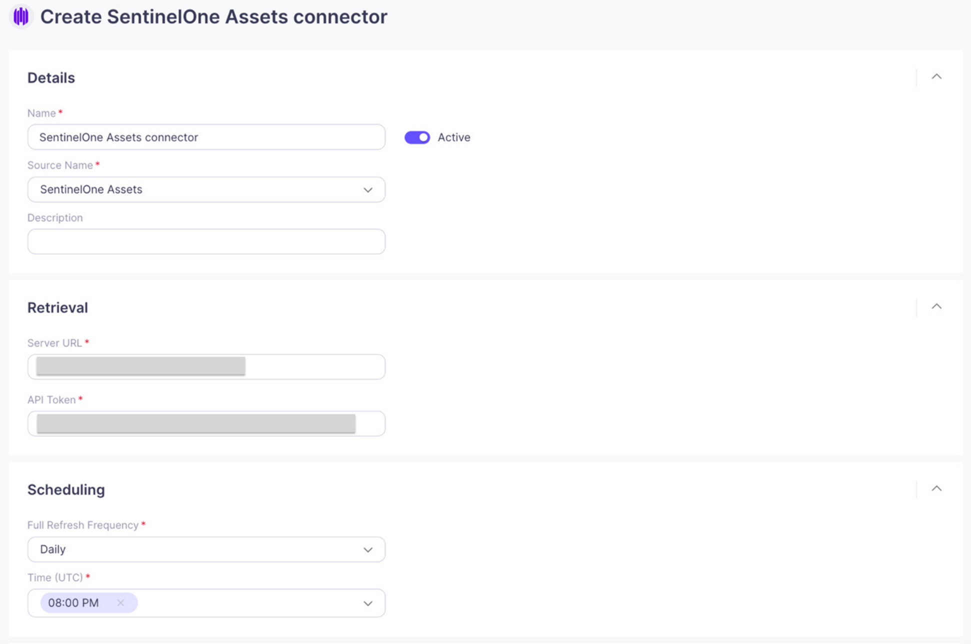


Figure 35. Connect New Data Source

4. Enter a **Name** for the Data Connector.
5. Toggle the **Active** switch to enable the Data Connector.
6. For **Server URL**, enter the portal URL for Singularity Operations Center (i.e., https://usea1.sentinelone.net).
7. Enter the **API Token** copied from Step 2: Create or Regenerate an API Key in Singularity Operations Center.
8. Enter the **Time** of day the connector should fetch updated information. Zscaler recommends you set the timing for SentinelOne to have the appropriate time to scan and update its findings so that the DataConnector can retrieve updated information.


Create SentinelOne Assets connector

Details

Name *: SentinelOne Assets connector
Active: ●
Source Name *: SentinelOne Assets
Description:

Retrieval

Server URL *:
API Token *:

Scheduling

Full Refresh Frequency *: Daily
Time (UTC) *: 08:00 PM

Figure 36. SentinelOne Assets connector

9. Click **Save**.
10. Click **Test** to verify the reachability of the SentinelOne platform.

Step 4: Configure the Avalor UVM Data Connectors—SentinelOne Threats

From the Avalor UVM Admin Portal:

1. Click **Configure**.

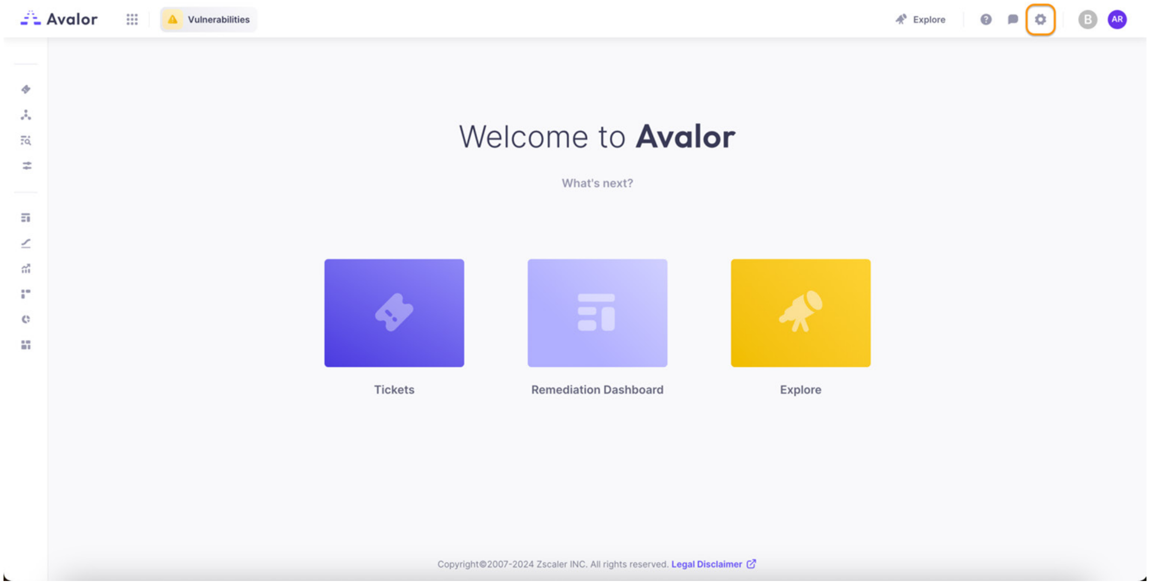


Figure 37. Configure

2. Click **Create**.
3. Click the **SentinelOne Threats** connector.

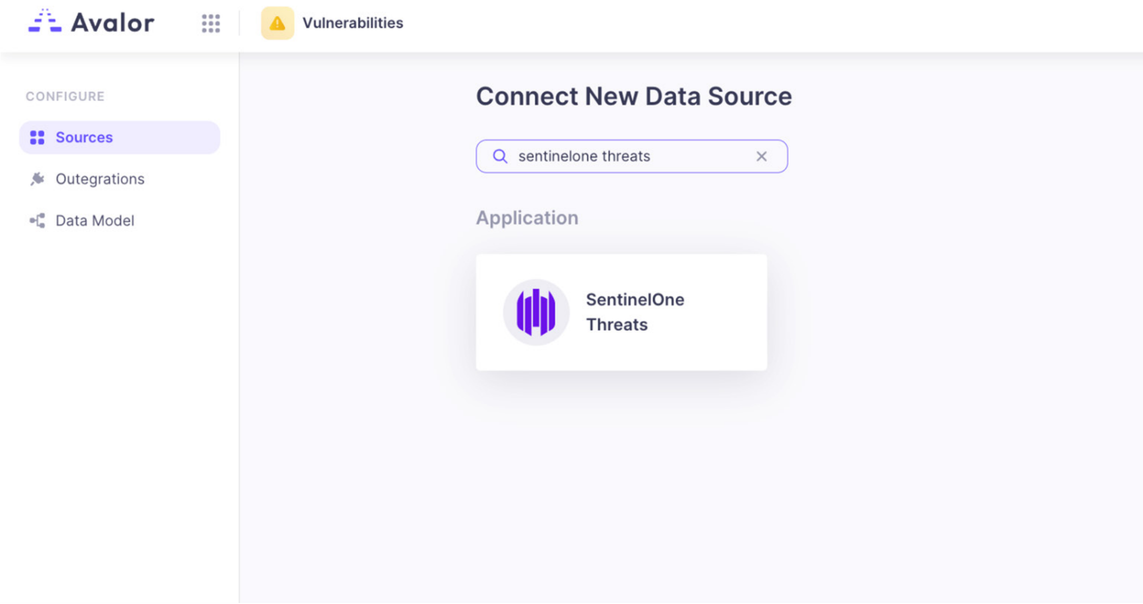
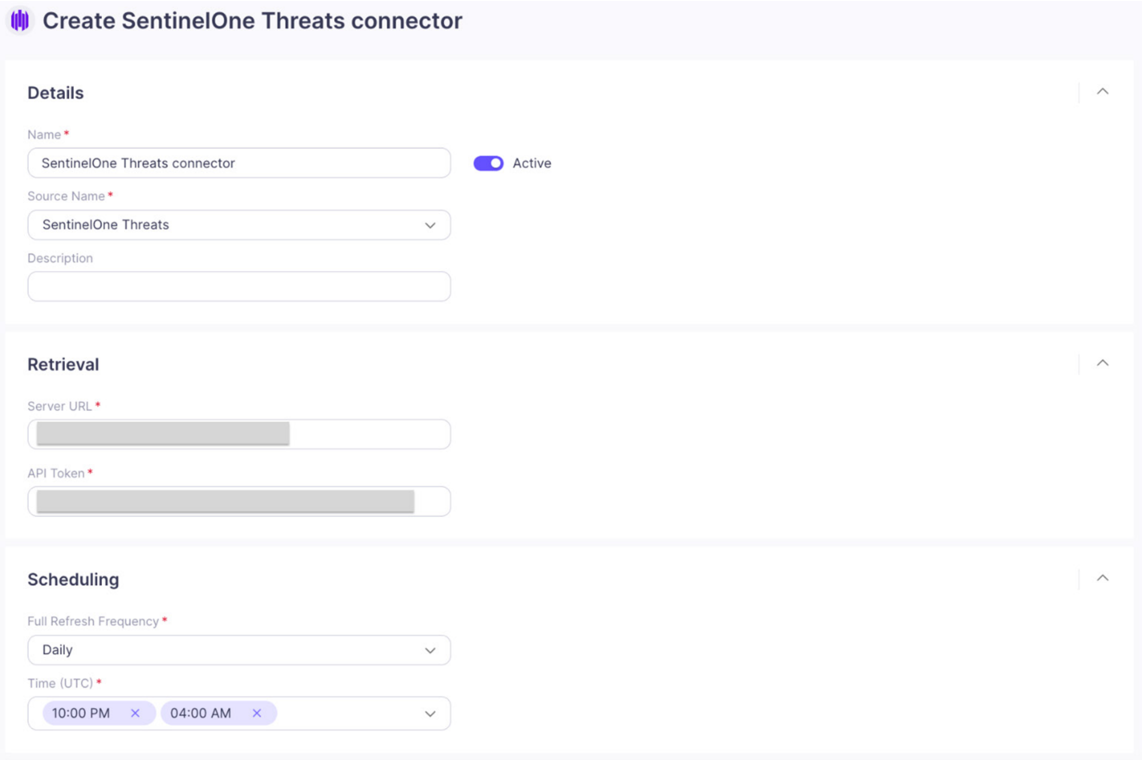


Figure 38. SentinelOne Threats

4. Enter a **Name** for the Data Connector.
5. Toggle the **Active** switch to enable the Data Connector.
6. Enter the portal **Server URL** for Singularity Operations Center (i.e., https://usea1.sentinelone.net).
7. Enter the **API Token** copied from Step 2: Create or Regenerate an API Key in Singularity Operations Center.
8. Enter the **Time** of day the connector should fetch updated information. Zscaler recommends you set the timing for SentinelOne to have the appropriate time to scan and update its findings so that the Data Connector can retrieve updated information.
9. Click **Save**.



Create SentinelOne Threats connector

Details

Name * SentinelOne Threats connector

Active: on

Source Name * SentinelOne Threats

Description

Retrieval

Server URL * [redacted]

API Token * [redacted]

Scheduling

Full Refresh Frequency * Daily

Time (UTC) * 10:00 PM, 04:00 AM

Figure 39. Threats Source created

10. Click **Test** to verify the reachability of the SentinelOne platform.

Step 5: Configure the Avalor UVM Data Connectors—SentinelOne Vulnerabilities

From the Avalor UVM Admin Portal:

1. Click **Configure**.

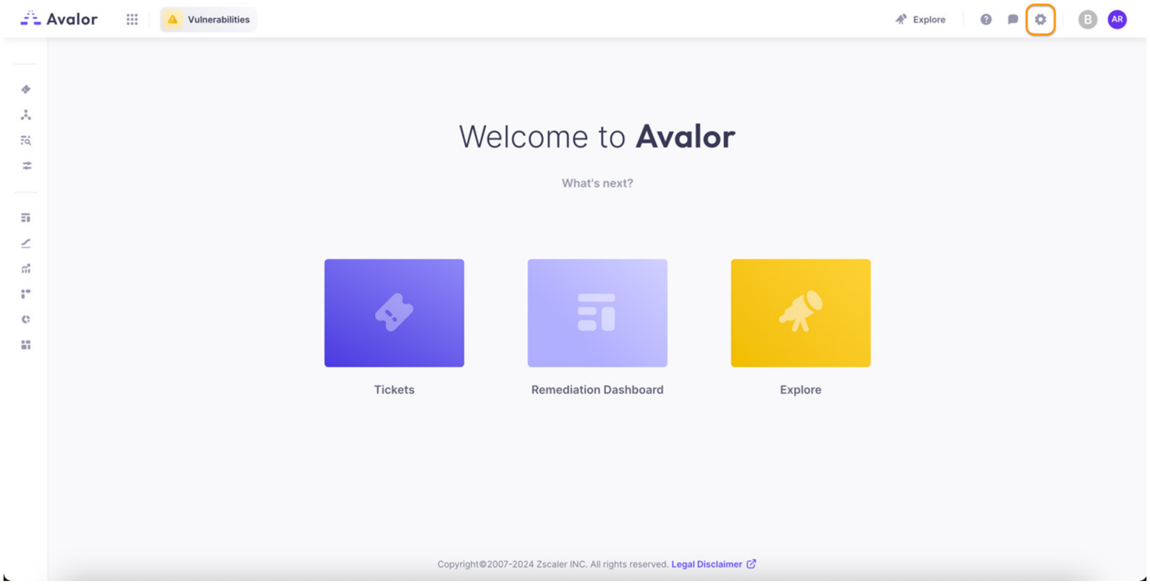


Figure 40. Configure

2. Click **Create**.
3. Click the **SentinelOne Vulnerabilities** connector.

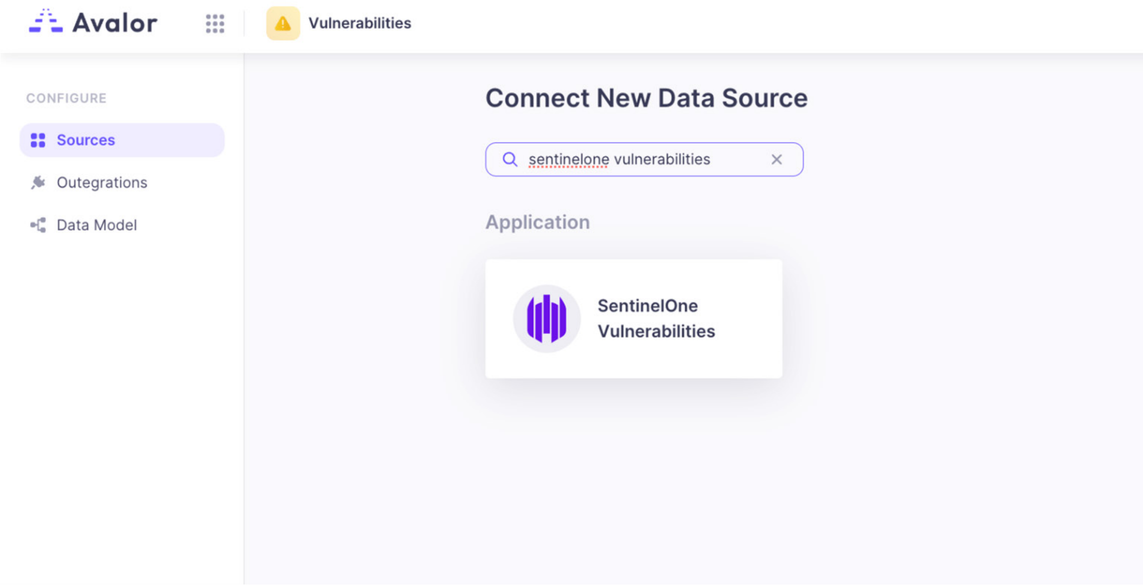
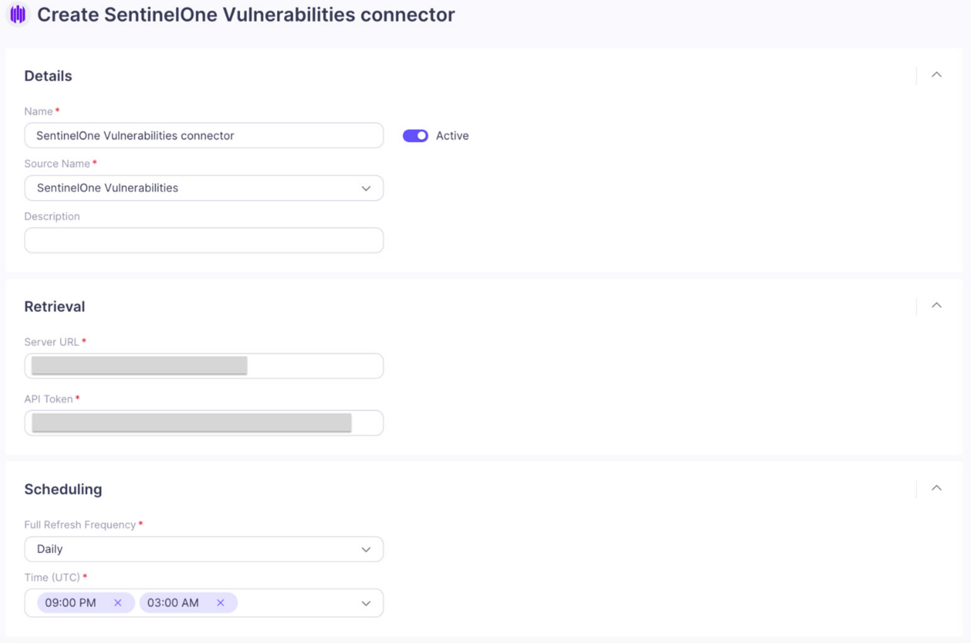


Figure 41. SentinelOne Vulnerabilities

4. Enter a **Name** for the Data Connector.
5. Toggle the **Active** switch to enable the Data Connector.
6. Enter the portal **Server URL** for Singularity Operations Center (i.e., https://usea1.sentinelone.net).
7. Enter the **API Token** copied from Step 2: Create or Regenerate an API Key in Singularity Operations Center.
8. Enter the **Time** of day the connector should fetch updated information. Zscaler recommends you set the timing for SentinelOne to have the appropriate time to scan and update its findings so that the Data Connector can retrieve updated information.
9. Click **Save**.



Create SentinelOne Vulnerabilities connector

Details

Name *: SentinelOne Vulnerabilities connector

Active

Source Name *: SentinelOne Vulnerabilities

Description:

Retrieval

Server URL *: [redacted]

API Token *: [redacted]

Scheduling

Full Refresh Frequency *: Daily

Time (UTC) *: 09:00 PM ×, 03:00 AM ×

Figure 42. Vulnerabilities Source created

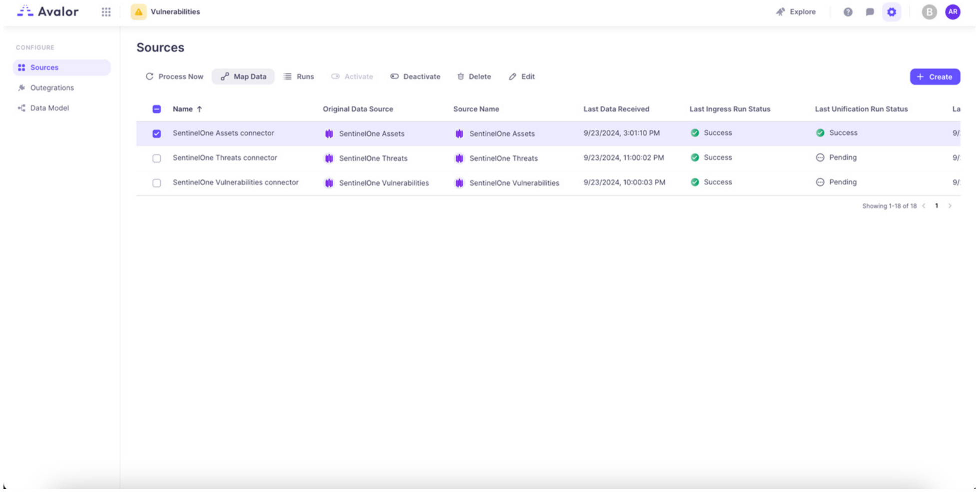
10. Click **Test** to verify the reachability of the SentinelOne platform.

Step 6: Review and Adjust Data Model Mapping

Avalor UVM automatically maps ingested data to the default Data Model, so analysis can begin right away. However, many data sources also provide additional data points that might provide additional context to risk prioritization.

The following example shows how to map the Has EDR Data Model entity to the ingested SentinelOne Asset data so that this field can be used as a mitigating score factor when calculating risk. From the Avalor UVM Sources page:

1. Select the SentinelOne Assets connector configured in Step 5: Configure the Avalor UVM Data Connectors—SentinelOne Vulnerabilities.
2. Click **Map Data**.



Sources

☐	Name ↑	Original Data Source	Source Name	Last Data Received	Last Ingress Run Status	Last Unification Run Status	La
☑	SentinelOne Assets connector	SentinelOne Assets	SentinelOne Assets	9/23/2024, 3:01:10 PM	Success	Success	9/
☐	SentinelOne Threats connector	SentinelOne Threats	SentinelOne Threats	9/23/2024, 11:00:02 PM	Success	Pending	9/
☐	SentinelOne Vulnerabilities connector	SentinelOne Vulnerabilities	SentinelOne Vulnerabilities	9/23/2024, 10:00:03 PM	Success	Pending	9/

Showing 1-18 of 18 ‹ 1 ›

Figure 43. Map Data

3. In the **Map SentinelOne Assets connector** window:
    a. Review the ingested data fields in the left-side column.
    b. Review the **Data Model Entities** in the right-side column.
    c. (Optional) Click **Add Entity** to create a custom **Entity** within the Data Model to map to.
    d. Review the default mappings in the center column.
    e. Double-click **Has EDR** in the right-side column to bring it into the center column.
    f. Click the **Function Editor** link to set an expression for the **Entity**.
    g. Change the **Value Editor** tab to **Value** and enter `True` in the blank field.

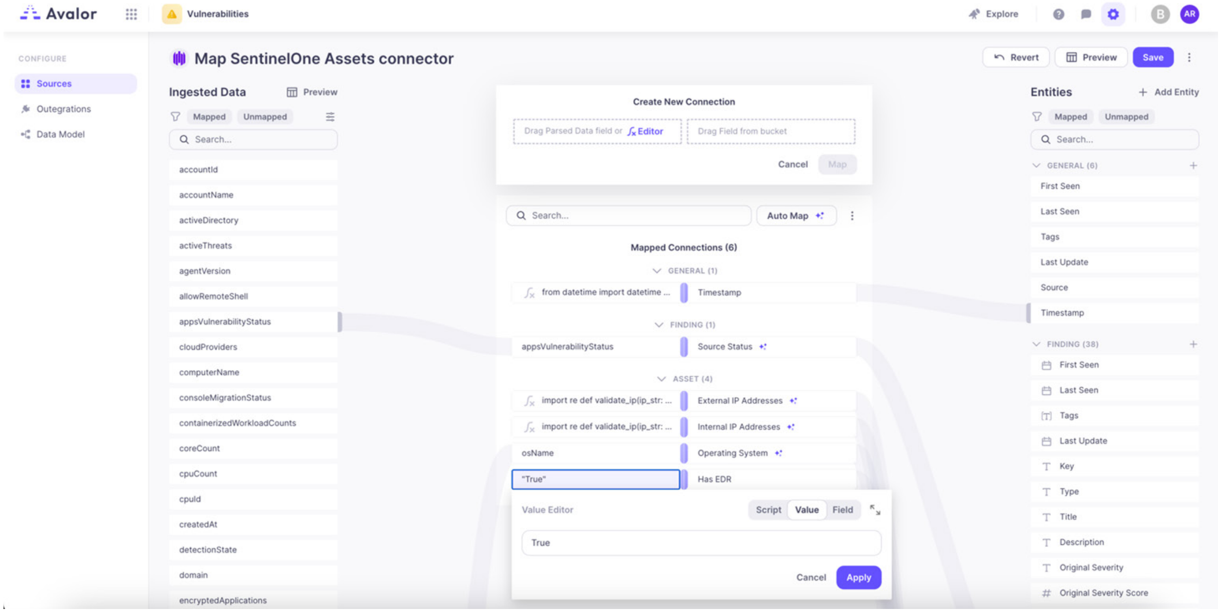
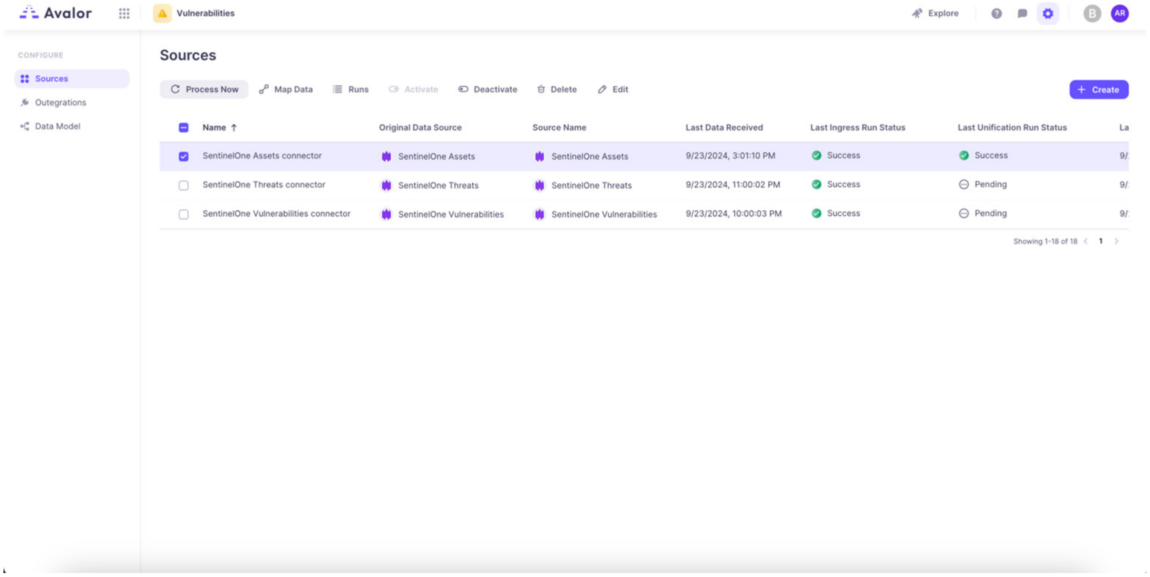


Figure 44. Has EDR

    h. Click **Map**.
    i. (Optional) Click the **Preview** button to review the updated Data Model mappings.
    j. Click **Save**.

4. In the **Data Sources** page, select the **SentinelOne Assets** connector and click **Process Now**.



Sources

☐	Name ↑	Original Data Source	Source Name	Last Data Received	Last Ingress Run Status	Last Unification Run Status	La
☑	SentinelOne Assets connector	SentinelOne Assets	SentinelOne Assets	9/23/2024, 3:01:10 PM	✓ Success	✓ Success	9/
☐	SentinelOne Threats connector	SentinelOne Threats	SentinelOne Threats	9/23/2024, 11:00:02 PM	✓ Success	Pending	9/
☐	SentinelOne Vulnerabilities connector	SentinelOne Vulnerabilities	SentinelOne Vulnerabilities	9/23/2024, 10:00:03 PM	✓ Success	Pending	9/

Showing 1-18 of 18 ‹ 1 ›

Figure 45. Process Now

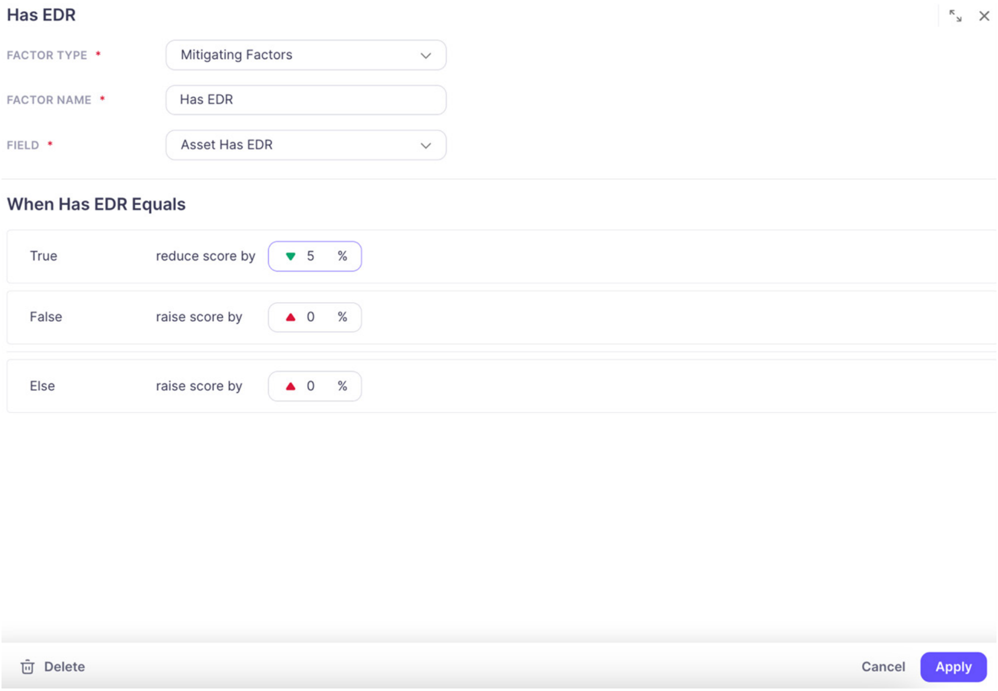
Step 7: Review and Adjust Risk Scoring

After ingested data has been normalized and mapped to the Data Model, Avalor UVM evaluates the risk.

The following example shows how the Has EDR entity is added as a mitigating factor for risk scoring. A value of True reduces the risk calculation (since the asset has mitigating software installed). A value of False increases the risk calculation (since the asset has a higher vulnerability without EDR).

From the **Vulnerabilities** tab in the Avalor dashboard (Remediation Hub):

1. In the left-side pane, select **Settings** > **Score**.
2. Click **Add Factor** in the **Risk & Mitigating Factors** section.
3. In the **Add new factor modal**:
    a. Choose **Mitigating Factors** for **Factor Type** (Mitigating Factors generally lower risk scoring, while Risk Factors generally increase risk scoring).
    b. Enter a **Name**.
    c. Choose **Asset Has EDR** for **Field**.
    d. In the **Boolean login** section, under **True**, enter a percentage by which the risk is reduced.



Has EDR

FACTOR TYPE * Mitigating Factors

FACTOR NAME * Has EDR

FIELD * Asset Has EDR

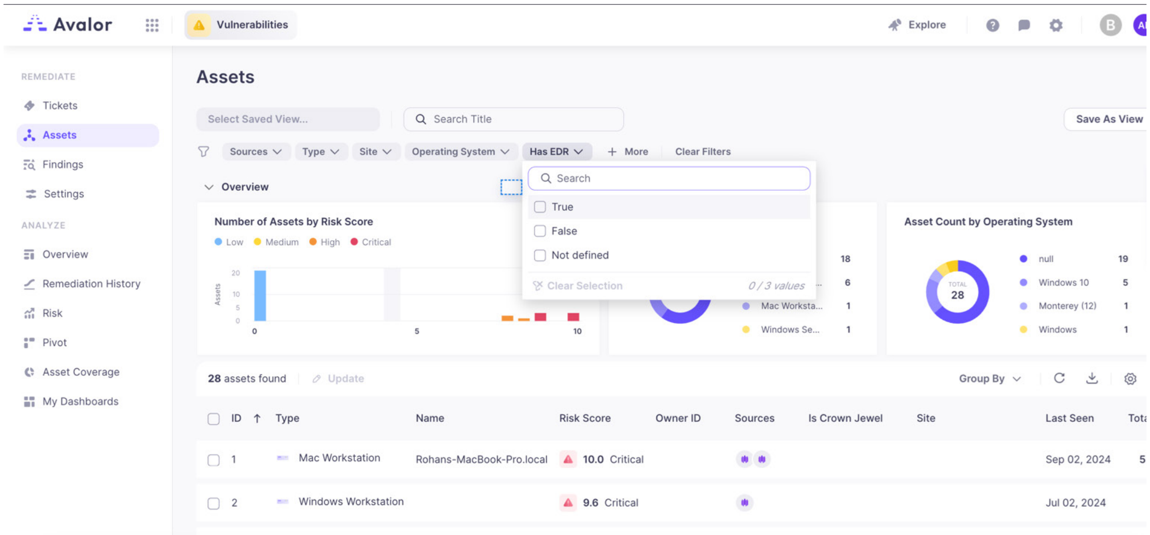
When Has EDR Equals

True	reduce score by	▼ 5 %
False	raise score by	▲ 0 %
Else	raise score by	▲ 0 %

Figure 46. Adjusting Risk Scoring

    e. Click **Apply**.

4. In the left-side pane, select the **Assets** dashboard. From the **Assets** dashboard:
   a. Set a filter by clicking **More** and adding **Has EDR**.

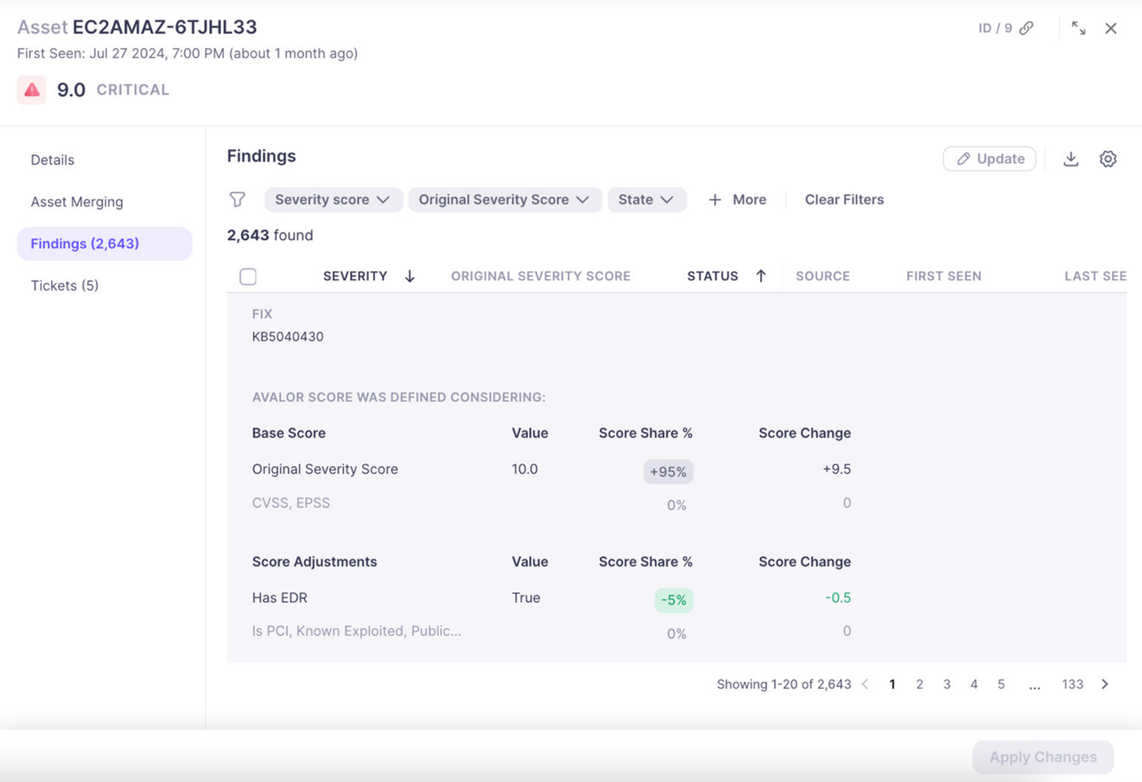


28 assets found

□	ID ↑	Type	Name	Risk Score	Owner ID	Sources	Is Crown Jewel	Site	Last Seen	Tota
□	1	Mac Workstation	Rohans-MacBook-Pro.local	10.0 Critical					Sep 02, 2024	5
□	2	Windows Workstation		9.6 Critical					Jul 02, 2024	

Figure 47. Filtered Assets

   b. Click your **Assets** in the filtered list.
   c. In the **Asset** modal that appears, click the **Findings** tab.
   d. Click one of the **Findings**.
   e. Review the output (notice the **Score Adjustments** section and whether **Has EDR** has modified the risk scoring).



Asset EC2AMAZ-6TJHL33

First Seen: Jul 27 2024, 7:00 PM (about 1 month ago)

9.0 CRITICAL

2,643 found

□	SEVERITY ↓	ORIGINAL SEVERITY SCORE	STATUS ↑	SOURCE	FIRST SEEN	LAST SEE

FIX
KB5040430

AVALOR SCORE WAS DEFINED CONSIDERING:

Base Score	Value	Score Share %	Score Change
Original Severity Score	10.0	+95%	+9.5
CVSS, EPSS		0%	0

Score Adjustments	Value	Score Share %	Score Change
Has EDR	True	-5%	-0.5
Is PCI, Known Exploited, Public...		0%	0

Figure 48. Risk Scoring

Appendix A: 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**.

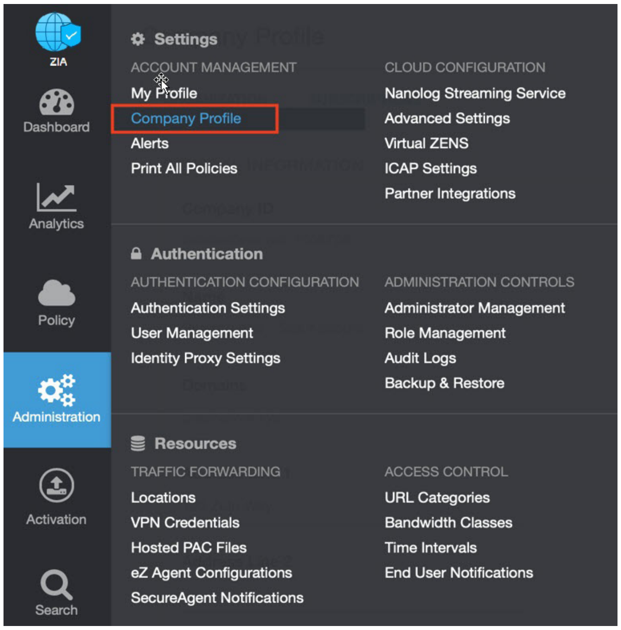
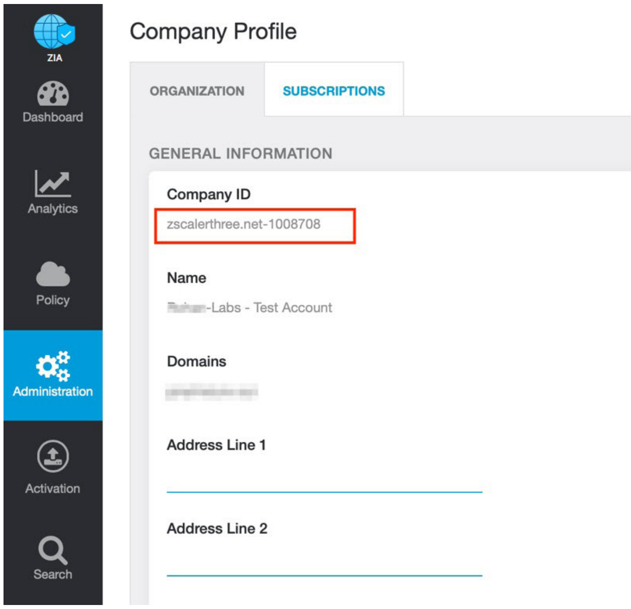


Figure 49. Collecting details to open support case with Zscaler TAC

2. Copy your Company ID.



Company ID
zscalerthree.net-1008708

Name
[redacted]-Labs - Test Account

Domains
[redacted]

Address Line 1

Address Line 2

Figure 50. Company ID

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

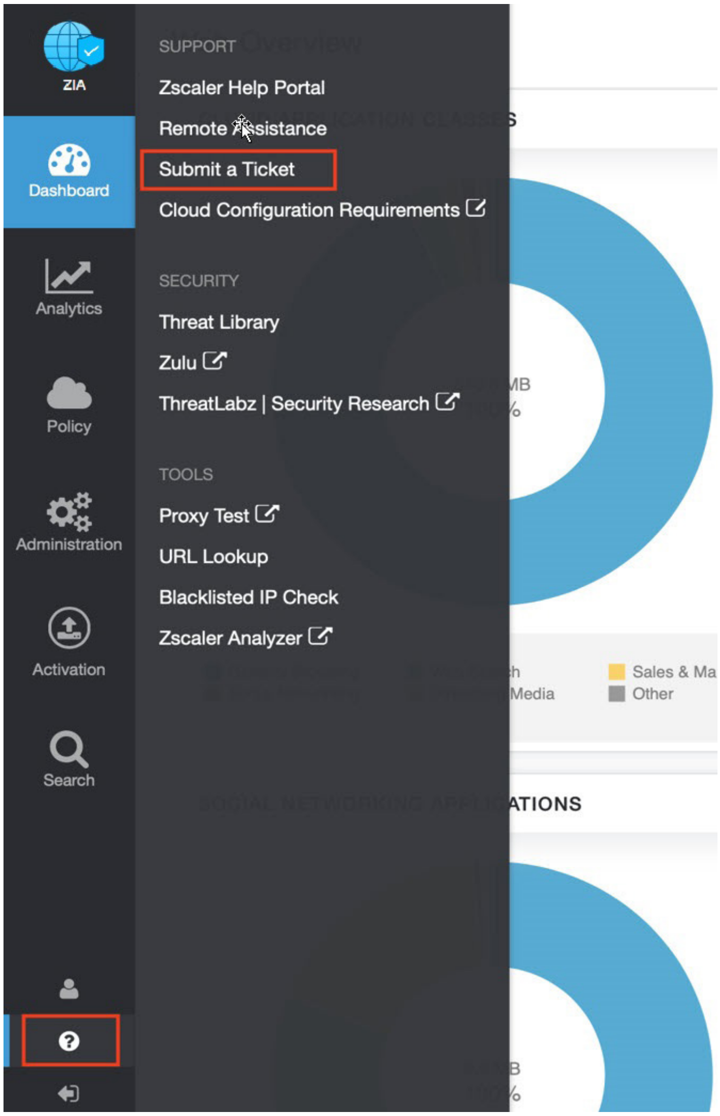


Figure 51. Submit a ticket