## Contents

Terms and Acronyms | 4
--- | ---
About This Document | 5
  |  5
  |  5
  |  5
  |  5
  |  5
Zscaler and SentinelOne Introduction | 6
  |  6
  |  6
  |  6
  |  6
  |  6
  |  7
  |  7
  |  7
Use Case 1: ZPA Posture Check Integration with SentinelOne | 8
  |  9
  |  9
  |  9
  |  10
  |  11
  |  12
  |  13
  |  14
  |  15
## Use Case 2: Use the Zscaler XDR App

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>16</td>
</tr>
<tr>
<td>Why Use the App?</td>
<td>16</td>
</tr>
<tr>
<td>Response Overview</td>
<td>16</td>
</tr>
<tr>
<td>SentinelOne Threat Enrichment Overview</td>
<td>16</td>
</tr>
<tr>
<td>Install the App from Singularity Marketplace</td>
<td>17</td>
</tr>
</tbody>
</table>

## Use Case 3: Ingesting Zscaler Logs with Dataset (Scalyr)

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisites</td>
<td>18</td>
</tr>
<tr>
<td>Option A: Cloud to Cloud logging using API</td>
<td>18</td>
</tr>
<tr>
<td>Setup Dataset (if using Dataset API for log ingestion)</td>
<td>20</td>
</tr>
<tr>
<td>Create API key for log ingestion</td>
<td>20</td>
</tr>
<tr>
<td>Apply Parser</td>
<td>20</td>
</tr>
<tr>
<td>Apply Dashboard</td>
<td>21</td>
</tr>
<tr>
<td>Option B: Syslog</td>
<td>21</td>
</tr>
<tr>
<td>Add NSS Server</td>
<td>22</td>
</tr>
<tr>
<td>Setup Dataset (if using NSS VM)</td>
<td>23</td>
</tr>
<tr>
<td>Setup Dataset (Scalyr) agent</td>
<td>23</td>
</tr>
<tr>
<td>Apply Parser</td>
<td>23</td>
</tr>
<tr>
<td>Apply Dashboard</td>
<td>23</td>
</tr>
</tbody>
</table>

## Appendix A: Requesting Zscaler Support

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gather Support Information</td>
<td>24</td>
</tr>
<tr>
<td>Save Company ID</td>
<td>24</td>
</tr>
<tr>
<td>Enter Support Section</td>
<td>25</td>
</tr>
</tbody>
</table>
# Terms and Acronyms

The following terms and acronyms are used in this document.

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

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

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.

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:

- Appendix A: Requesting Zscaler Support
- Zscaler Resources
- SentinelOne Resources

Software Versions

This document was authored using Zscaler Internet Access and Zscaler Private Access (with Zscaler Client Connector) along with SentinelOne 4.2 or later.

Request for Comments

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

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

Zscaler Overview

The Zscaler applications are described in this section.

Zscaler Internet Access (ZIA) Overview

Zscaler Internet Access (ZIA) is a secure Internet and web gateway delivered as a service from the cloud. Think of ZIA as a secure Internet 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 Browser Isolation, allowing you to start with the services you need now and activate others as your needs grow.

Zscaler Private Access (ZPA) Overview

Zscaler Private Access (ZPA) is a cloud service that provides secure remote access to internal applications running on 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, a piece of software called Zscaler Client Connector is installed. Zscaler Client Connector ensures the user’s device posture and extends a secure micro-tunnel 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZIA Help Portal</td>
<td>Help articles for ZIA.</td>
</tr>
<tr>
<td>ZPA Help Portal</td>
<td>Help articles for ZPA</td>
</tr>
<tr>
<td>ZPA Posture Profiles</td>
<td>Help link for how to configure ZPA posture profiles.</td>
</tr>
<tr>
<td>ZPA Access Policies</td>
<td>Help link for how to configure ZPA access policies with a set of configuration examples.</td>
</tr>
<tr>
<td>Zscaler Tools</td>
<td>Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.</td>
</tr>
<tr>
<td>Zscaler Training and Certification</td>
<td>Training designed to help you maximize Zscaler products.</td>
</tr>
<tr>
<td>Submit a Zscaler Support Ticket</td>
<td>Zscaler support portal for submitting requests and issues.</td>
</tr>
</tbody>
</table>
SentinelOne Overview
An overview of the SentinelOne Singularity 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SentinelOne Support portal</td>
<td>Help for SentinelOne Singularity XDR.</td>
</tr>
<tr>
<td>SentinelOne Singularity XDRdatasheet</td>
<td>SentinelOne Singularity XDR data sheet.</td>
</tr>
</tbody>
</table>
Use Case 1: ZPA Posture Check Integration with SentinelOne

In this use case:

- Zscaler Private Access (ZPA) verifies the presence of a running SentinelOne process on the endpoint as an assessment of end device posture. ZPA can be configured 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](image)

**Figure 1. High-Level overview**
Configuring Zscaler Private Access (ZPA)

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

Log into ZPA Admin Portal

![ZPA Admin Portal Login](image)

Admin ID
zpaadmin@domain.com

Password

☐ Single Sign-On Using IdP

☐ Remember Me

Language
English

Sign In

Figure 2. Log into ZPA Admin Portal

Navigate to Zscaler Client Connector

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

![Zcaler Client Connector](image)

Figure 3. Click the Zcaler Client Connector icon
Create New Posture Profile

After logging into Zscaler Client Connector:

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

![Add a device posture profile](image-url)

*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. Access policies can be setup to allow or deny application access based on whether the posture check passes or fails.

![Edit Device Posture](image)

*Figure 5. Add a detect SentinelOne posture profile*
Decide Which Applications Need Conditional Access

Within the ZPA Admin Portal, navigate to Administration > Application Segment.

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

![Application Segments](image)

Figure 6. Navigate to application segments

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

![Application Segment Display](image)

Figure 7. Decide which application needs conditional access
Set Up an Access Policy

Within the ZPA Admin Portal, navigate to **Administration > Access Policy**.

Figure 8. Setup an access policy
Tie the Posture Profile to This Access Policy

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

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

In this example, we added an access policy 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).

![Setup an access policy](image)
Verify Conditional Access from an Endpoint

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

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

Figure 11. Access blocked from an endpoint if the SentinelOne agent is not running
Use Case 2: Use the Zscaler XDR App

The Zscaler XDR app configures automatic and manual response actions from SentinelOne for Zscaler. The app also enables automatic threat enrichment, bringing Zscaler data into SentinelOne 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) configured.
- Create an API token via the Zscaler ZIA console (or other means).
- Create an empty Security Group on the IdP that is pushed to Zscaler for use by SentinelOne. Existing security IdP groups cannot be used as the database will be out of sync between the IdP and Zscaler.
- Create a Zscaler security policy using the SentinelOne Security Group.

Why Use the App?

By installing the Zscaler app, 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.

Customers who enable the app enrichment capability benefit from seeing more data points in their SentinelOne threats. The app’s enrichment capabilities help uncover user privilege, as it shows the user department and whether the user is an admin in Zscaler. The enrichment data also shows which Zscaler groups the user is in and any comments an admin has added to that user.

Response Overview

The XDR response action places the user of the infected device to a predefined policy in Zscaler. This approach means your automatic and manual response is customizable. Your response can be as strict or permissive as fits your organization. Through configuring the Zscaler policy with the group the user is placed in, you can set it 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.
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 a specific, designated STAR rule(s).

SentinelOne Threat Enrichment Overview

The Zscaler app can also add data to a SentinelOne threat. This happens automatically when a threat is received by the cloud from the agent. Threat enrichments can only be on or off, and they cannot be added to some threats but not others.
Upon receiving a threat, SentinelOne calls the APIs of all vendors that have enrichment integrations enabled. With Zscaler, the User API is searched, looking for matches based on username. Zscaler parses the API responses for the most critical info, 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 which the user belongs.

**Install the App from Singularity Marketplace**

To install the app:

1. Open the **Marketplace** dashboard.
2. From the **Zero Trust Network** category, choose **Zscaler XDR Integration**.
3. Enter the relevant information to configure the app. The Zscaler information can be gathered from the ZIA portal at **Administration > Authentication Settings > Identity Providers**.
4. Select the blue pencil to edit the active IdP which brings up the IdP configuration window. The **Base URL** and the **Bearer Token** can be found in the **Provisioning Options** section of the configuration.
   - Zscaler SCIM IDP Base URL name. Example: https://scim.scalerthree.net/1234/4567/scim
   - Zscaler SCIM bearer token
   - Company domain

More than one domain can be configured using a comma separated list. Example input: @domain.com, @abccompany.com

- Enable **Enrichment**, if desired.
- Answer all the questions about automatic response actions.

5. Enable **Automatically move “last logged in user” to new Zscaler group**.
6. Enable when this response fires. Choose from the five options outlined above. If multiple options are selected, they are treated as an “AND”, triggering on all selected scenarios.
7. If you selected to trigger the app based on STAR threats, ensure you input which STAR rules to use.
8. 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 will never be automatically reversed and an admin will have to manually reverse it the action in Z by someone

Reversing the response action via Option A, “when the threat is mitigated”, risks that the endpoint compromise has been remediated but that the compromised identity is still compromised.

9. Enable **Manual Response actions** if you want users to act manually after reviewing a threat.
10. When finished, click **Next**. Now select a scope to install this app to and click **Install**.
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 following in advance for the integration to work:

- Admin access to SentinelOne and Dataset console.
- Admin access to ZIA console.

Option A: Cloud to Cloud logging using API

Setting up RESTful forwarding is the best option for forwarding ZIA logs:

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

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

The host portion of the API URL (i.e., “app.scalyr.com” above) might be different depending on the location of your Dataset tenant.

Dataset tip: 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)
3. Setup Dataset (see Setup Dataset (if using Dataset API for log ingestion)).
Setup 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. Zscaler pushes gzipped logs into Dataset using Dataset's `uploadLogs api` endpoint.
2. Dataset admin must create a Dataset API key with `log write access`. This API key is later pasted into the ZIA console.

![Manage API keys](image)

Apply Parser

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

![Apply parser](image)
Apply Dashboard

1. Select the **Dashboard** dropdown and then click **New Dashboard**.
2. Select **… > Edit Json**.
3. Apply **Zscaler Dashboard**.

![Apply dashboard]

Figure 17. Apply dashboard

Option B: Syslog

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

![NSS section in ZIA]

Figure 18. Navigate 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 plaintext, uncompressed ZIA logs to that Scalyr agent.

3. Refer to the NSS VM deployment guide for your platform:
   - [NSS Deployment Guide for Azure](#)
   - [NSS Deployment Guide for AWS](#)
   - [NSS Deployment Guide for vSphere](#)
Add NSS Server

Before you set up an NSS server on the 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 buffers the logs and sends them once 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.

![Figure 19. Navigate to Nanolog Streaming Service](image)

2. From the NSS Servers tab, click Add NSS Server.

3. The Add NSS Server window appears:
   - Enter a Name for the NSS.
   - NSS for Web is selected by default. If you are configuring an NSS for firewall logs, select NSS for Firewall.
   - The NSS is Enabled by default.

![Figure 20. Add NSS Server](image)
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. Setup the Dataset syslog monitor.
8. Point the NSS server to the Syslog Monitor.
9. Setup Dataset (see **Setup Dataset (if using NSS VM)**).

### Setup Dataset (if using NSS VM)

You must set up Dataset to integrate with ZIA logs.

#### Setup Dataset (Scalyr) agent

1. Setup Dataset Agent on a separate VM (link)
2. Install Syslog monitor to listen on a port on the local network (link)

![Figure 21. Syslog monitor](image)

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

*Figure 22. Example Monitor Config*

#### Apply Parser

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

#### Apply Dashboard

1. Select the **Dashboard** dropdown and then click **New Dashboard**.
2. Click ... > **Edit Json**.
3. **Apply** Zcaler Dashboard.
Appendix A: Requesting Zscaler Support

This section describes how to access your Zscaler support team.

Gather Support Information

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

![Company Profile](image)

Figure 23. Collecting details to open support case with Zscaler TAC

Save Company ID

Copy your Company ID.

![Company Profile](image)

Figure 24. Company ID
Enter Support Section

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

Figure 25. Submit a ticket