



Zscaler and Cybereason Deployment Guide

Contents

| | |
|---|---------------|
| Integrating Zscaler Internet Access with Cybereason XDR | 3 |
| Step 1: In Cybereason Connect, setup an On-Site Collector | 4 |
| Step 2: In ZIA Admin Portal, Add an NSS Server | 9 |
| Step 3: In ZIA Admin Portal, Add an NSS Feed | 10 |
| Step 4: In Cybereason Connect, Complete the Integration | 12 |
| Integrating Zscaler Private Access with Cybereason XDR | 13 |

Integrating Zscaler Internet Access with Cybereason XDR

The combination of Zscaler and Cybereason provides a multi-layer block & detect approach against drive-by-compromise, command-and-control, unknown network connections, account takeover, and ransomware.

Telemetry and critical events from Zscaler Internet Access (ZIA) are streamed to Cybereason XDR, where suspicious events across your environment are correlated into MalOps (Malicious Operations), a visual timeline of any high-severity incident.

The standard integration involves forwarding logs from ZIA into Cybereason XDR.

To do this, you will use Cybereason Connect & ZIA Nanolog Streaming Service.

Setting up the integration can be done in 4 major steps:

- 1 In Cybereason Connect, setup an On-Site Collector & Agent**
- 2 In ZIA Admin Portal, Add an NSS Server**
- 3 In ZIA Admin Portal, Add an NSS Feed**
- 4 In Cybereason Connect, Complete the Integration**

Note: Steps 1 and 2 require provisioning VMs to facilitate data transfer. Specifications and various options are detailed in each section.

Step 1

In Cybereason Connect, setup an On-Site Collector

In this step, we will deploy an On-Site Collector and its Agent. The Agent is a log forwarder that collects logs and securely transmits them to Cybereason XDR.

You will need:

1. Virtual machine (VM) running Linux with Docker and [Docker Compose](#) (version 3.9 or higher) installed.
2. The VM must run one of the supported Linux operating systems, which include Debian, Ubuntu, RHEL, and SUSE.
3. Your VM must meet these minimum system requirements:
 - 1.5 GB RAM
 - 2 CPUs. If you expect transmission over 10,000 events per second, plan between 4 and 6 CPUs.
 - 100 MB free disk space

On the Virtual Machine, allow communication to the following addresses, ports, and protocols to enable communication with Cybereason XDR:

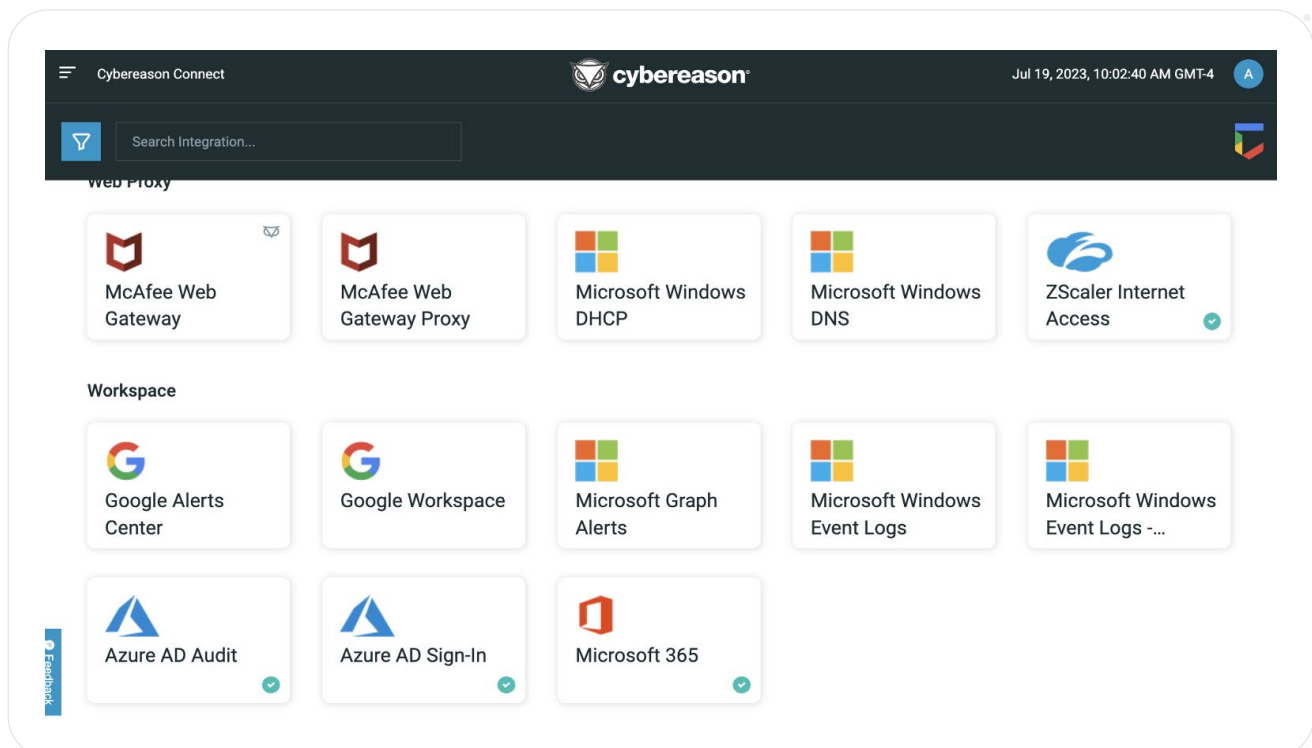
Next, for the relevant addresses for your region, add a firewall rule exception for this address to enable communication with your Cybereason platform:

| Connection Protocol | Destination | Port |
|---------------------|---|------|
| TCP | malachiteingestion-pa.googleapis.com | 443 |
| TCP | europa-malachiteingestion-pa.googleapis.com | 443 |
| TCP | europa-west2-malachiteingestion-pa.googleapis.com | 443 |
| TCP | asia-southeast1-malachiteingestion-pa.googleapis.com | 443 |
| TCP | australia-southeast1-malachiteingestion-pa.googleapis.com | 443 |
| TCP | accounts.google.com | 443 |
| TCP | gcr.io | 443 |
| TCP | oauth2.googleapis.com | 443 |
| TCP | storage.googleapis.com | 443 |

With this foundation ready, let's head to Cyberreason Connect.

| Region | Address | Countries Included |
|----------------|--|---|
| US East | connect-us-e1-1.cybereason.net/onPrem/* | <ul style="list-style-type: none"> • United States • Canada |
| EU West | connect-eu-w1-1.cybereason.net/onPrem/* | <ul style="list-style-type: none"> • Belgium • France • Germany • Italy • Netherlands • Switzerland • United Kingdom |
| APAC Northeast | connect-as-ne1-1.cybereason.net/onPrem/* | <ul style="list-style-type: none"> • Japan • South Korea |
| APAC Southeast | connect-as-se1-1.cybereason.etn/onPrem/* | <ul style="list-style-type: none"> • Australia • Indonesia • Singapore |

1. In the Cyberreason Connect screen, select Zscaler Internet Access.




2. In the Access Details section for the integration, in the Name field, give the integration instance a name (e.g. ZIA-XDR).
3. In the Site name field, select an existing site or create a new one.
4. Cybereason recommends you use separate sites for different physical locations from which you are

Investigation
Functions

IDS/IPS
Product category

Name*

On-Site Collector 

To connect this integration you need to select a collector from the list or create a new one.

Site name*

retrieving logs. If, for example, you have multiple different offices in which you have installed your firewall platform, you may want to create a site for each of those offices and have a different collector for each office.

5. Click Generate Collector (if you are creating a new site) or Download Collector (if you select a previously created site).

On-Site Collector ?

To connect this integration you need to select a collector from the list or create a new one.

Site name*

TLV

Generate Collector

Cancel Connect

The deployment.zip file downloads to your machine.

In the Cybereason Connect screen, click Get Credentials.

A new browser tab opens with the credentials in JSON syntax:

```
{  
  "jwt": "<JWT token>",  
  "artifactoryPassword": "<password>"  
}
```

6. The Cybereason platform generates both of these values. You should not modify either of these credentials as modification of the credentials will cause the collector agent to not communicate with your Cybereason platform.

NOTE: These credentials are valid for 24 hours after generation. If you do not install the collector on your VM within 24 hours, you will need to generate the credentials again.

7. Copy the value of the jwt key and save it to a file with a .txt suffix.
8. Note the password in a secure location, as you will need it later in the process.
9. Move the .txt file with the value of the jwt key and the deployment.zip file to the VM machine you prepared for the on-site collector agent.

10. Unpack the deployment.zip file on the VM machine.
 - If you use minikube to expand the deployment.zip file, make sure you mount both the deployment.zip file and the .txt file with the JWT key value.
 - In the unpacked deployment.zip file, run the deployment script with this command:
sh deployment.sh <path to the .txt file> '<password from generated credentials>'
11. In the command above, make sure you update the path to the real path with your file and the password you noted earlier.
 - Ensure that the machine on which you run this file has access to the artifactory location used in the container installation. This location is found in the deployment.sh file found inside the deployment.zip package.
12. In the Cybereason Connect screen, enter the relevant Port and Protocol you set up in the integration configuration prior to installing the on-site collector agent.

After you run the script to start the on-site collector agent, the following message should display in the command window and the logs of the Docker container on the VM machine running the agent:

```
Starting to listen for <protocol> syslog on <address>:<port>.
```

The actual protocol, address, and port in your logs may differ depending on the configuration you performed in the other platform.

When Cybereason XDR receives the logs successfully, you find the following log entries in the Docker container logs on the VM machine running the on-site collector agent:

```
Accepting new syslog TCP connection.
```

```
Batch (<number_of_logs>, <integration>) successfully uploaded.
```

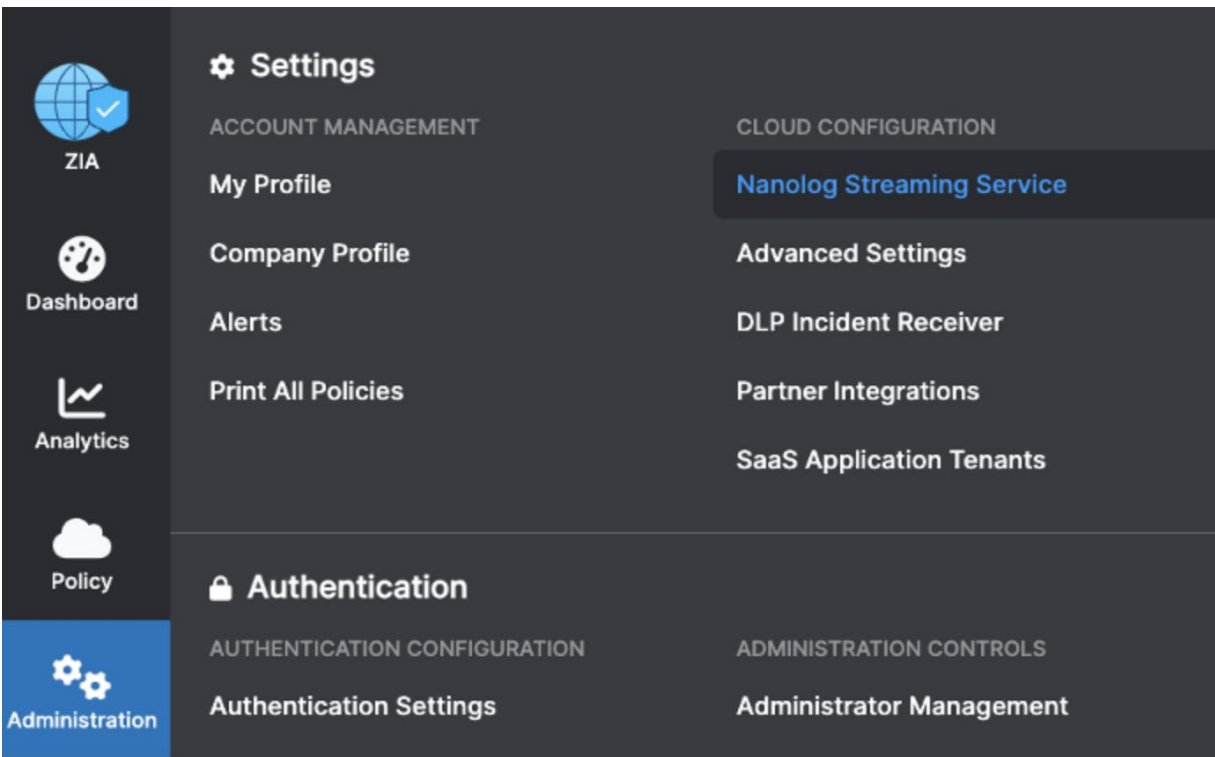
The first time you start the on-site collector agent, it may take a few minutes for the logs to arrive in your Chronicle instance and your Cybereason platform. You may need to wait approximately ten minutes to begin to see the data in your Cybereason XDR Dashboard.

If you have issues with the collector agent, see [Troubleshooting Problems with the XDR On-Site Collector Agent \(NEST Documentation\)](#).

Step 2

In ZIA Admin Portal, Add an NSS Server

In this step, you will deploy a NSS VM. This VM pulls logs from Zscaler and pushes the logs via syslog to Cybereason XDR. Note that logs are sent in the clear. It is therefore highly recommended to have the NSS VM deployed within the same network as the on-site collector.



1. Log in and navigate to Administration > Cloud Configuration > Nano Streaming Service.
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 XDR Collector to stream plain text, uncompressed ZIA logs to the Agent.
3. Refer to the NSS VM deployment guide for your platform:
[NSS Deployment Guide for Microsoft Azure](#)
[NSS Deployment Guide for Amazon Web Services](#)
[NSS Deployment Guide for VMware vSphere](#)

Step 3

In ZIA Admin Portal, Add an NSS Feed

With that complete, we can now define Zscaler events to send.

Head to Administration > Nanolog Streaming Service > NSS Feeds.

The screenshot shows the 'Add NSS Feed' configuration page in the ZIA Admin Portal. The page is titled 'Add NSS Feed' and includes a notification: 'Thanks for evaluating the service - Please contact sales to purchase a license.' The configuration fields are as follows:

- Feed Name:** Enter Text
- NSS Type:** NSS for Web
- NSS Server:** NONE
- Status:** Enabled (selected), Disabled
- SIEM Destination Type:** IP Address (selected), FQDN
- SIEM IP Address:** Enter Text
- SIEM TCP Port:** Enter Text
- SIEM Rate:** Unlimited (selected), Limited
- Log Type:** Web Log
- Feed Output Type:** CSV
- Feed Escape Character:** ,\
- Feed Output Format:**

```
[%time], [%login], [%proto], [%eur], [%action], [%appname], [%apploss], [%d{respsize}], [%d{respsize}], [%s{urlclass}], [%s{urlsupercat}], [%s{urlcat}], [%s{mlwarecat}], [%s{threatname}], [%d{riskscore}], [%s{dipeng}], [%s{dlodict}], [%s{location}], [%s{dept}], [%s{cip}], [%s{sip}], [%s{reamethod}], [%s{respcode}], [%s{ua}], [%s{referer}], [%s{ruletype}], [%s{rulelabel}], [%s{contenttype}], [%s{unscannabletype}], [%s{deviceowner}], [%s{devicehostname}], [%s{keyprotectiontype}]\n
```
- Timezone:** GMT
- Duplicate Logs:** Disabled

- Feed Name: Fill in, e.g. ZIA-XDR Integration
- NSS Server: What you setup in previous step.
- SIEM IP Address, TCP Port: Connect On-Site Collector details
- Log Type: Web Logs
- Feed Output Type: Custom
- Feed Escape Character: ,\
- Copy the following log format and paste it into the Feed Output Format.

```
\{ "sourcetype" : "zscalernss-web", "event" : \{"datetime":"%d{yy}-%02d{mth}-%02d{dd} %02d{h-  
h}:%02d{mm}:%02d{ss}", "reason":"%s{rea-  
son}", "event_id":"%d{recordid}", "protocol":"%s{proto}", "action":"%s{action}", "transactionsize":"%d{totals  
ize}", "responsesize":"%d{respsize}", "requestsiz":"%d{reqsize}", "urlcategory":"%s{urlcat}", "serverip":"%s{  
sip}", "clienttranstime":"%d{ctime}", "requestmethod":"%s{reqmethod}", "referrerURL":"%s{ereferer}", "user  
agent":"%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{cint  
ip}", "threatcategory":"%s{malwarecat}", "threatname":"%s{threatname}", "filetype":"%s{filetype}", "appna  
me":"%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{bwthrott  
le}", "servertranstime":"%d{stime}", "contenttype":"%s{contenttype}", "unscannabletype":"%s{unscannable  
type}", "deviceowner":"%s{deviceowner}", "devicehostname":"%s{devicehostname}"\}
```

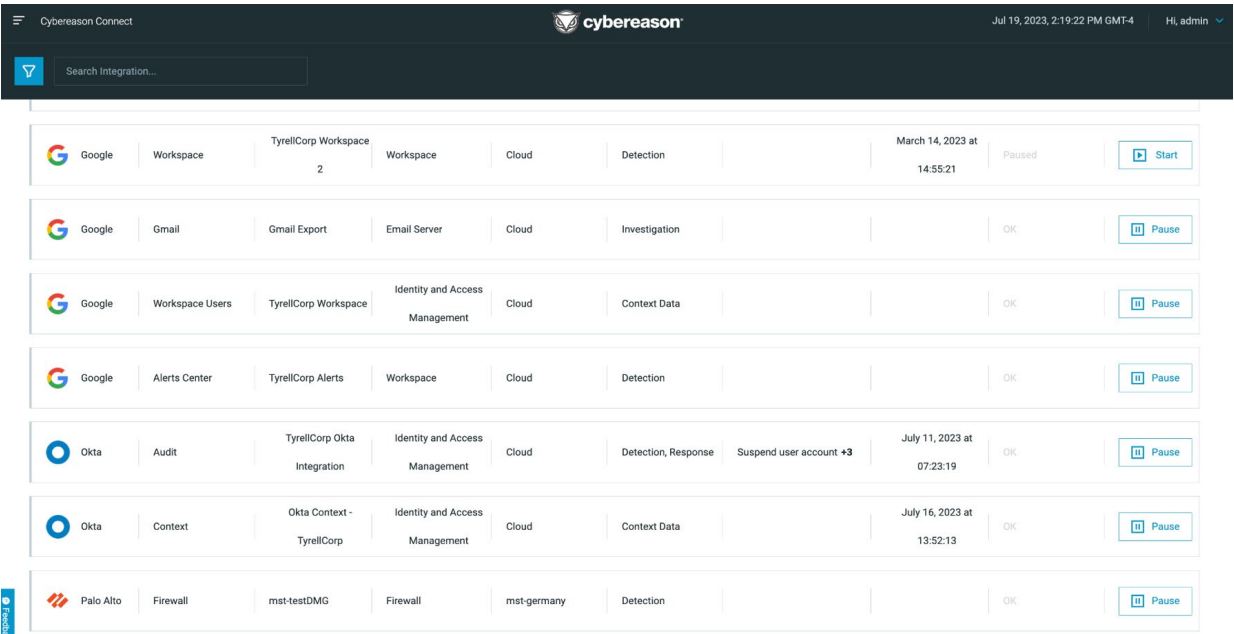
Note: When you copy text from PDF, it can introduce line-breaks. You can use a tool like <https://codebeautify.org/remove-line-breaks> to fix.

Step 4

In Cybereason Connect, Complete the Integration

After you enable the log exports, you are ready to set up the information in Connect.

1. From Cybereason Connect, select ZScaler Internet Access (ZIA).
2. In the right side of the Connect screen, provide a Name for the integration.
3. In the On-Site Collector details, in the Site name field, select the same site you used when you downloaded the on-site collector.
4. Below the Site name field, enter the Protocol and Port for the on-site collector. Click Connect.
If the connection between your Cybereason platform and your on-site collector is successful, the Connect screen displays a message indicating the valid credentials.
If there are any errors in the configuration details, you will see an error message in the Access Details pane to help you resolve the error.
You can then view the status of your integration in the My Integrations tab. The status should indicate Pending and will update to OK once the data feed from ZIA is established.



The screenshot displays the Cybereason Connect interface. At the top, there is a search bar labeled "Search Integration...". Below it, a list of integrations is shown, each with a status indicator and a control button. The integrations are as follows:

| Provider | Product | Integration Name | Category | Protocol | Details | Status | Action | |
|-----------|-----------------|-----------------------------|--------------------------------|-------------|---------------------|--|--------|-------|
| Google | Workspace | TyrellCorp Workspace 2 | Workspace | Cloud | Detection | March 14, 2023 at 14:55:21 | Paused | Start |
| Google | Gmail | Gmail Export | Email Server | Cloud | Investigation | | OK | Pause |
| Google | Workspace Users | TyrellCorp Workspace | Identity and Access Management | Cloud | Context Data | | OK | Pause |
| Google | Alerts Center | TyrellCorp Alerts | Workspace | Cloud | Detection | | OK | Pause |
| Okta | Audit | TyrellCorp Okta Integration | Identity and Access Management | Cloud | Detection, Response | Suspend user account *3 July 11, 2023 at 07:23:19 | OK | Pause |
| Okta | Context | Okta Context - TyrellCorp | Identity and Access Management | Cloud | Context Data | July 16, 2023 at 13:52:13 | OK | Pause |
| Palo Alto | Firewall | mst-testDMG | Firewall | mst-germany | Detection | | OK | Pause |

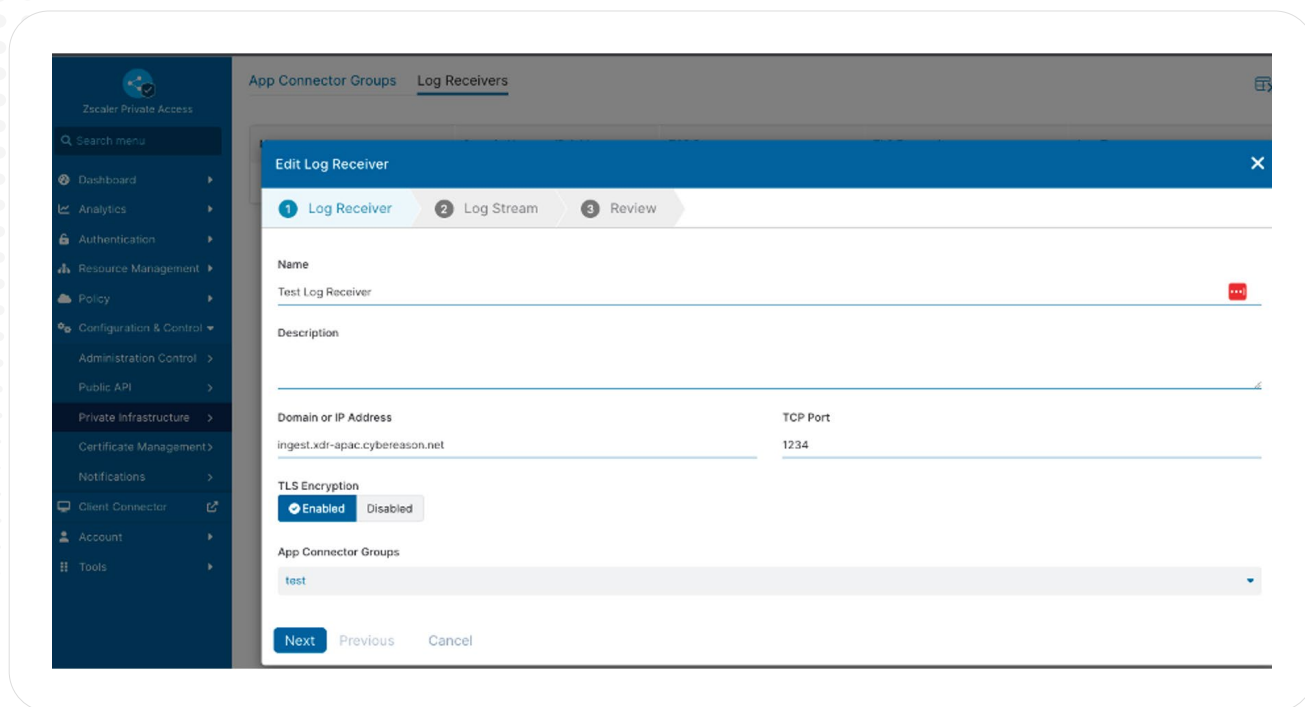
Integrating Zscaler Private Access with Cybereason XDR

When you send data from your ZScaler Private Access (ZPA) instance to Cybereason XDR, you export logs with a dedicated app connector and LSS (Log Streaming Service).

Use the steps below to configure and deploy the app connector.

1. Deploy an app connector on the appropriate platform for your organization. For details on how to deploy app connectors on different platforms, see the App Connector Deployment Guides for Supported Platforms section in the ZScaler Private Access documentation.
It is recommended that this app connector is dedicated to log collection.
2. Create a new app connector group just for logging.
3. Determine the external IP address for your app connector. You will need this for ACL restrictions later in the configuration process.
4. Provide the IP address for your app connector to your Cybereason XDR team.
You will receive a domain name and port dedicated to your data ingestion, with a separate port for each log type, from your Cybereason XDR team.
5. In your Zscaler dashboard, navigate to the Configure and Control > Private Infrastructure > Log Receivers screen.
6. In the Log Receivers screen, click Add Log Receiver.
7. In the dialog box, enter the domain and port you received from your Cybereason XDR team.
8. Set the TCP Encryption option to Enabled.

9. Select the app connector group you created previously.
The configuration should look similar to the example below:



10. Select Next.
11. For the log type, select User Activity.
12. For the log template, select JSON.
13. In the Policy section, select the Client types tab.
14. In the Client types tab, set the value to ZPA LSS.
15. Select Next and then Save.

The data ingestion will begin after the app connector has updated automatically.

You will need to repeat the steps above if you received additional ports for other log types from your Cybereason XDR team.



About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at zscaler.com or follow us on Twitter [@zscaler](https://twitter.com/zscaler).

© 2023 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, and ZPA™ 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.