Zscaler and Splunk Deployment Guide

March 2022
Version 1.1

Zscaler Business Development – Solutions Architecture Team
# Table of Contents

**Terms and Acronyms** .................................................................................. 5

**Document Purpose** ..................................................................................... 5

Zscaler Overview ...................................................................................... 5

Splunk Overview ...................................................................................... 5

Audience .................................................................................................... 5

Software Versions .................................................................................... 5

Request for Comments ........................................................................... 6

Zscaler and Splunk Introduction ................................................................ 7

Zscaler Internet Access (ZIA) Overview ............................................... 7

Zscaler Private Access (ZPA) Overview ............................................... 7

Zscaler Resources .................................................................................. 7

Splunk Cloud Overview .......................................................................... 8

Splunk SOAR Overview ........................................................................ 8

Splunk Resources ................................................................................. 8

**Application Architecture** ....................................................................... 9

Data models ............................................................................................. 9

Zscaler log streams ............................................................................... 9

Web and Tunnel Logs ............................................................................ 10

Firewall and DNS logs .......................................................................... 10

Private Access logs ............................................................................... 11

Zscaler APIs ........................................................................................ 11

Python SDK .......................................................................................... 12

Sandbox ................................................................................................ 12

Audit Logs ............................................................................................. 13

**Zscaler Technical Add-on** ....................................................................... 14

Sourcetypes .......................................................................................... 15

Macros .................................................................................................. 15

Splunk CIM ........................................................................................... 15

Modular Inputs ....................................................................................... 16

**Zscaler Splunk App** ............................................................................... 16

Dependencies ........................................................................................ 16
Zscaler and Splunk Deployment Guide

User Interface ............................................................................................................................................. 16
Overview and Connections ......................................................................................................................... 17
Access Control .......................................................................................................................................... 18
Threat Prevention ...................................................................................................................................... 19
Private Access .......................................................................................................................................... 20

Installation and Configuration .................................................................................................................... 21
Zscaler Configuration ................................................................................................................................. 21
Output Strings ........................................................................................................................................... 21

Splunk Configuration ................................................................................................................................. 25
Search Head ................................................................................................................................................ 25
Forwarders (or Indexers) .............................................................................................................................. 25
Network Inputs .......................................................................................................................................... 26
Modular Inputs .......................................................................................................................................... 27
Macro Modification ..................................................................................................................................... 28
Custom Field Mapping ............................................................................................................................... 28

Appendix A: Splunk Configs ..................................................................................................................... 29
Event Types, Tags and Aliases ..................................................................................................................... 29

Appendix B: Splunk Essential Configuration
(Using NSS VM - Stream Syslog Over TCP) .............................................................................................. 40

Configure Zscaler NSS ............................................................................................................................... 40
Add or Create Index .................................................................................................................................... 40
Log into Splunk Instance ............................................................................................................................. 40
Configure New Index in Splunk .................................................................................................................. 40
Add Zscaler Index in Splunk ....................................................................................................................... 42

Create Data Inputs ..................................................................................................................................... 43
Splunk Connect for Syslog ........................................................................................................................... 43
TCP Data Input .......................................................................................................................................... 43
Select the Desired Zscaler Source Type .................................................................................................... 43
Change Default App Context and Default index ....................................................................................... 44
Verify Incoming Logs ................................................................................................................................. 45
Inspect Log Fields .................................................................................................................................... 45
Extracted Log Fields .................................................................................................................................. 46
Verify Splunk’s Zscaler App ....................................................................................................................... 46
Appendix C: Splunk Essential Configuration
(using Cloud-to-Cloud logging - HTTPS POST) .........................................................48
Configure Splunk Cloud to Ingest ZIA Logs over HEC Input .....................................48
  Log into Splunk Cloud Tenant .............................................................................49
  Install Zcaler App and Zcaler TA in Your Cloud Tenant ........................................49
  Create Zcaler Index in Splunk ............................................................................50
  Add Zcaler Index in Splunk ................................................................................50
  Create a new Data Input and HEC token ...............................................................52
  Configure Data Input and HEC token ..................................................................53
  Copy the HEC Token Value ................................................................................57
  Determine the Splunk Cloud API Endpoint to Send Logs To .................................57
Configure Splunk Cloud IDM to Fetch Zcaler Audit Logs and Sandbox Events ..........58
  Log into Splunk IDM Instance ............................................................................59
  Install Zcaler Splunk TA on Splunk IDM Instance .................................................59
  Configure Zcaler Index on Splunk IDM Instance ..................................................60
  Add Zcaler Account Used by Splunk IDM to Make API Calls to ZIA .....................60
  Configure Input for Audit Logs ..........................................................................61
  Fill in the Settings for Fetching ZIA Audit Logs ....................................................62
  Configure Input for Sandbox Events ....................................................................62
  Fill in the Settings for Fetching ZIA Sandbox Events ..........................................63
  Confirm that Both Input Settings are Saved and Enabled ......................................63
Configure Zcaler for Cloud-to-Cloud Logging ...........................................................63
  Navigate to Cloud-to-Cloud Logging Section in ZIA Portal ...................................64
  Setup the Cloud NSS Log Feed (Web) ...................................................................64
  Setup the Cloud NSS Log Feed (Firewall) ..............................................................66
  Add Other Log Sourcetypes ................................................................................68
  Validate NSS Cloud Configuration ......................................................................69
  Verify Splunk’s Zcaler App ..................................................................................70

Appendix D: Using Phantom (SOAR) with Zcaler and Splunk .................................71
Phantom components .............................................................................................71
A Sample Playbook to Showcase Zcaler and Phantom Integration ............................71
Configuring Phantom .............................................................................................73
Create new Event Label in Phantom .......................................................................73
Create Automation User in Phantom ............................................................ 74
Installing Zscaler App on Phantom ............................................................. 75
Search for Zscaler App .............................................................................. 75
Configure Zscaler App .............................................................................. 76
Test Connectivity Between Phantom and Zscaler ........................................ 77
Installing Splunk App on Phantom .............................................................. 78
Search for Splunk App ............................................................................... 78
Configure Splunk App .............................................................................. 79
Test connectivity Between Phantom and Splunk ........................................ 81
Download Zscaler Playbook ...................................................................... 81
Edit the playbook settings ........................................................................ 82
Configuring Splunk .................................................................................. 83
Install Splunk ES App ............................................................................... 83
Manage Threat Intelligence within ES App ............................................... 84
Notable Events and Forwarding to Phantom ............................................. 86
Install Phantom App ................................................................................. 87
Configure Automation User ...................................................................... 88
Verify Events in Phantom ......................................................................... 89
Inspect Actions Taken by Phantom ......................................................... 90

Appendix E: Requesting Zscaler Support .................................................... 91
Gather Support Information ...................................................................... 91
Save Company ID .................................................................................... 91
Enter Support Section ............................................................................. 92

Appendix F: Revision History .................................................................... 94
Terms and Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zscaler</td>
<td>World’s leading SaaS based enterprise security gateway</td>
</tr>
<tr>
<td>Splunk</td>
<td>Market leader in SIEM, SOAR and log analytics</td>
</tr>
<tr>
<td>SIEM</td>
<td>Security Incident and Event Management</td>
</tr>
<tr>
<td>SOAR</td>
<td>Security Orchestration and Automation</td>
</tr>
<tr>
<td>ZIA</td>
<td>Zscaler Internet Access</td>
</tr>
<tr>
<td>ZPA</td>
<td>Zscaler Private Access</td>
</tr>
<tr>
<td>Nanolog</td>
<td>ZIA logging technology</td>
</tr>
<tr>
<td>NSS</td>
<td>Nanolog Streaming Service</td>
</tr>
<tr>
<td>LSS</td>
<td>Log Streaming Service</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>Modular Input</td>
<td>Method of ingesting data in Splunk via scripts and APIs</td>
</tr>
<tr>
<td>TCP Input</td>
<td>Method of ingesting data in Splunk via TCP datagrams</td>
</tr>
<tr>
<td>SOC</td>
<td>Security Operations Centre</td>
</tr>
<tr>
<td>NOC</td>
<td>Network Operations Centre</td>
</tr>
<tr>
<td>CIM</td>
<td>Common Information Model (Splunk defined data model)</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
<tr>
<td>ES</td>
<td>Splunk Enterprise Security (Splunk’s SIEM)</td>
</tr>
<tr>
<td>Phantom</td>
<td>Splunk’s SOAR product</td>
</tr>
</tbody>
</table>

Document Purpose

Zscaler Overview

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

Splunk Overview

Splunk (Trading Index: SPLK), is a world leader in data analytics, security incident management, orchestration and automation. Zscaler traffic, status and access logs provide a rich and voluminous source of data for ingesting into the Splunk platform. This information can then be used to enrich other data sources and generate interesting events related to business services and technology operations. For more information on Splunk, visit www.splunk.com.

Audience

This guide is for network administrators, endpoint and IT administrators, and security analysts responsible for deploying, monitoring, and managing enterprise security systems. This document is targeted and those
interested in learning details of how Zscaler and Splunk interact, as well as providing guidance for integration of Zscaler and Splunk. This may consist of:

- Enterprise, Solution and Security Architects
- SOC and NOC designers and managers
- Splunk designers, implementors, administrators, and operators
- Anyone with a general interest in Zscaler SIEM integration and reference materials

Please note that appendices have been added for those needing a foundational exposure to Splunk and NSS as it relates to this integration. For additional product and company resources, please refer to:

- Appendix E: Requesting Zscaler Support
- Zscaler Resources
- Splunk Resources

Software Versions

This document was authored using the latest versions of ZIA, ZPA, and Splunk Cloud.

Request for Comments

- For Prospects and Customers: We value reader opinions and experiences. Please contact us at partner-doc-support@zscaler.com to offer feedback or corrections for this guide.
- For Zscaler Employees: Please contact z-bd-sa@zscaler.com to reach the team that validated and authored the integrations in this document.

If you have created searches, reports, dashboards or other useful functionality which you think could be used by the within the app, please submit them for inclusion into the next version of the Zscaler Splunk App:

- Email: splunk-support@zscaler.com
- Zscaler Community Products > Cloud Reporting and Management
Zscaler and Splunk Deployment Guide

Zscaler and Splunk Introduction

Below are overviews of the Zscaler and CrowdStrike applications described in this section. Zscaler and Splunk share a large joint customer base where our technologies may interact, the companies have a mutual partnership. In order to ease integration of our capabilities into our customer’s environments, Zscaler has developed a ‘Splunk App” which simplifies the ingestion of Zscaler generated data into the Splunk platform. This Splunk App will make the overall integration process between our technologies more accessible for our joint customers.

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 it as a secure Internet onramp—all you do is 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 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 and Link</th>
<th>Description</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>
</tbody>
</table>
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.

Splunk Cloud Overview

Splunk Cloud Platform provides a complete suite of self-service service capabilities for you to ingest data, customize data retention settings, customize user roles and centralized authentication, configure searches and dashboards, update your IP Allow List and perform app management. Splunk Cloud Platform collects, searches, monitors, reports, and analyzes all of your real-time and historical machine data using a cloud service that is centrally and uniformly delivered by Splunk to its large number of cloud customers. In addition, you can use the Cloud Monitoring Console (CMC) to holistically monitor the data consumption and health of your Splunk Cloud Platform environment. Finally, ensure your Operational Contacts are kept up-to-date.

Splunk Phantom Overview

Splunk Phantom is a security orchestration, automation, and response (SOAR) application that provides security orchestration, automation and response capabilities that empowers your SOC. Splunk Phantom allows security analysts to work smarter, not harder, by automating repetitive tasks; triage security incidents faster with automated detection, investigation, and response; increase productivity, efficiency and accuracy; and strengthen defenses by connecting and coordinating complex workflows across their team and tools. Splunk Phantom also supports a broad range of security functions including event and case management, integrated threat intelligence, collaboration tools and reporting.

Splunk Resources

The following table contains links to Splunk support resources.

<table>
<thead>
<tr>
<th>Name and Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splunk Documentation</td>
<td>Splunk platform online documentation.</td>
</tr>
<tr>
<td>Splunk Cloud help</td>
<td>Splunk Cloud online help articles.</td>
</tr>
<tr>
<td>Splunk SOAR help</td>
<td>Splunk SOAR online help articles.</td>
</tr>
<tr>
<td>Splunk Common Information</td>
<td>Description of Splunk’s CIM.</td>
</tr>
<tr>
<td>Model (CIM)</td>
<td></td>
</tr>
<tr>
<td>Phantom Demonstration</td>
<td>Video demonstration of Phantom capabilities and uses.</td>
</tr>
<tr>
<td>Splunk and Zscaler partner page</td>
<td>Splunk’s Zscaler partner page.</td>
</tr>
</tbody>
</table>
# Application Architecture

Zscaler’s integration with Splunk follows Splunk’s well defined framework for Splunk App. Splunk App is designed specifically to be installed and run in a Splunk environment. The app itself is separated into two discreet parts, the technical add-on, and the Zscaler Splunk App.

The app takes advantage of several technologies in order to ingest data from Zscaler, which consist of log streams generated from customer environments and the retrieval of data from Zscaler’s APIs. The diagram below shows these various interfaces.

---

**Figure 1. Application architecture**

The interfaces are detailed in the following sections.

## Data models

Zscaler and Splunk joint customers require Zscaler logging data in a format compatible with Splunk’s Common Information Model (CIM) data model. The Zscaler Technical Add-On maps all Zscaler NSS fields into CIM compatible types, as well as tagging all events where relevant to specific CIM data model(s).

## Zscaler log streams

Zscaler streams logs into the customer environments, facilitated by Zscaler-supplied virtual machines that execute in a customer’s (or partner’s) hosted compute environment.

These virtual machines attach to the Zscaler cloud via outbound connections and receive encrypted and tokenized logs to stream into customer log collection and SIEM platforms. The table below describes the various log streams.

<table>
<thead>
<tr>
<th>Log Type</th>
<th>Streaming Technology</th>
<th>Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy</td>
<td>NSS - Web</td>
<td>VMware, AWS, and Azure</td>
</tr>
<tr>
<td>Tunnel</td>
<td>NSS - Web</td>
<td>VMware, AWS, and Azure</td>
</tr>
<tr>
<td>Component</td>
<td>NSS Feed Output Format</td>
<td>Log Sources</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Firewall</td>
<td>NSS - CWF</td>
<td>VMware, AWS, and Azure</td>
</tr>
<tr>
<td>DNS</td>
<td>NSS - CWF</td>
<td>VMware, AWS, and Azure</td>
</tr>
<tr>
<td>Alert</td>
<td>NSS – CWF/Web</td>
<td>VMware, AWS, and Azure</td>
</tr>
<tr>
<td>App Auth</td>
<td>LSS</td>
<td>RedHat compatible (see doc for version specifics)</td>
</tr>
<tr>
<td>App Access</td>
<td>LSS</td>
<td>RedHat compatible (see doc for version specifics)</td>
</tr>
<tr>
<td>Browser Access</td>
<td>LSS</td>
<td>RedHat compatible (see doc for version specifics)</td>
</tr>
<tr>
<td>Proxy</td>
<td>NSS - Web</td>
<td>VMware, AWS, and Azure</td>
</tr>
</tbody>
</table>

**Web and Tunnel Logs**

A dedicated Zscaler NSS server delivers Zscaler web and tunnel logs. Event streams are generated for the following log types:

- **Proxy logs**: all access logs processed by Zscaler proxy
- **Tunnel logs**: up or down tunnel events and summary usage statistics
- **Alerts**: system alerts for events such as connectivity loss

Details for all possible fields and formats can be found below:

- NSS Feed Output Format: Web Logs
- Adding NSS Feeds for Tunnel Logs
- Adding NSS Feeds for Alerts

There is a dedicated Splunk event type for each of these log streams, detailed in the Sourcetypes section.

**Figure 2. Zscaler NSS web and tunnel data in Splunk**

**Firewall and DNS logs**

A dedicated Zscaler NSS server delivers Zscaler Firewall and DNS logs. Event streams are generated for the following log types:

- **Cloud Firewall logs**: all access logs processed by Zscaler firewall
- **DNS logs**: logs for DNS traffic where DNS traffic is sent via Zscaler
- **Alerts**: system alerts for events such as connectivity loss

You can find details for all possible fields and formats at the following links:

- NSS Feed Output Format: Firewall Logs
- NSS Feed Output Format: DNS Logs
- Adding NSS Feeds for Alerts
These log streams have a dedicated Splunk event type, detailed in the `Sourcetypes` section.

![ZIA and ZPA Diagram](image)

**Figure 3. Zscaler NSS firewall and DNS data in Splunk**

**Private Access logs**

A dedicated Zscaler NSS server delivers Zscaler web and tunnel logs. Event streams are generated for the following log types:

- **Connector status logs**: events generated as attach to the clouds and utilization statistics
- **User activity logs**: a record for each application access processed by ZPA via Zscaler App
- **User status logs**: Authentication logs as end users authenticate to the Private Access service
- **Browser access logs**: a record for each application access processed by ZPA via Browser Access

Details for all possible fields and formats can be found at the following links:

- [About App Connector Status Log Fields](#)
- [About User Activity Log Fields](#)
- [About User Status Log Fields](#)
- [About Browser Access Log Fields](#)

These log streams have a dedicated Splunk event type, detailed in the `Sourcetypes` section.

![ZPA and Splunk Diagram](image)

**Figure 4. Zscaler LSS ZPA data in Splunk**

**Zscaler APIs**

Zscaler runs a number of open APIs for customer use, which include read and write functions. The current Splunk integration focuses on read functions for Zscaler Sandbox detonation reports and Zscaler Admin audit logs. Full specifications for the Zscaler API can be found in the [API Reference](#).

Splunk makes use of these APIs via Splunk modular inputs. Both Sandbox and audit logs have dedicated Splunk event types, detailed in the `Sourcetypes` section.
Figure 5. Zscaler APIs used by Splunk modular inputs

NOTE
Phantom has existing write integrations to Zscaler API, details of these integrations are not in scope for this document.

Python SDK
The Splunk App contains several scripts that interface with the Zscaler API, including a fork of a private SDK used by a number of Zscaler technology partners. An unofficial version of the original SDK can be located at the Zscaler Python SDK GitHub repository.

The raw scripts and SDK can be found in the bin/ directory of the Technical Add-On.

Sandbox
The Zscaler Sandbox is used by customers to detonate unknown file samples, and determines if there’s malicious behavior.

When the Sandbox analyzes files, the end user recipient might be quarantined or allowed to download the file. The outcome is determined by customer-specific Sandbox policies. The latest policy constructs can be found in Configuring the Sandbox Policy.

Sandbox detonation results are significant to customers, since a malicious verdict indicates a possibly compromised user or risky user behavior that could jeopardize business. As such, Zscaler has made full Sandbox reporting a product feature and includes the capability to pull detailed sandbox post-detonation reports via API calls. Zscaler’s Splunk technical add-on ingests these events, and the Zscaler Splunk App produces a number of derived reports.
Audit Logs

An audit log is generated as administrators access the Zscaler console and make changes within the console. Zscaler makes these events available via the Zscaler API since they often must be archived outside of Zscaler. You can configure the Splunk Technical Add-On to ingest these logs.

Once configured, the modular input tracks the state of the most recent log retrieval, then requests the delta for any logs generated since the last successful retrieval.
The Zscaler Technical Add-On does all the hard work in accessing and processing Zscaler event information. This includes:

- Enabling compatibility with Splunk’s CIM data model
- Connecting to Zscaler APIs including modular input configuration
- Defining source types and search macros

The Add-On is a requirement for the Zscaler Splunk App as the App takes advantage of many configurations and components defined in the Add-On.

You can download the Add-On can from the Splunk Base.
Sourcetypes
The below sourcetypes are defined in the Zscaler Technical Add-On, and cover all the current possible inputs. Actual use of the sourcetypes might vary depending on what a bundle and features to which a Zscaler customer subscribed.

- Note that there are no pre-configured data inputs. Data inputs must be configured by the Splunk Admin as per the Network Inputs and Modular Inputs sections. Splunk’s best practice is to not permit the definition of network inputs in a Splunk app.

<table>
<thead>
<tr>
<th>Sourcetype</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>zscalernss-web</td>
<td>ZIA Proxy Logs</td>
</tr>
<tr>
<td>zscalernss-tunnel</td>
<td>ZIA Tunnel Logs–up or down events and aggregate traffic stats</td>
</tr>
<tr>
<td>zscalernss-fw</td>
<td>ZIA Firewall Logs</td>
</tr>
<tr>
<td>zscalernss-dns</td>
<td>ZIA DNS Logs</td>
</tr>
<tr>
<td>zscalernss-alerts</td>
<td>System Alerts from Zscaler NSS (Proxy and Firewall)</td>
</tr>
<tr>
<td>zscalerlss-zpa-connector</td>
<td>ZPA Connector Logs</td>
</tr>
<tr>
<td>zscalerlss-zpa-app</td>
<td>ZPA Application Access Logs</td>
</tr>
<tr>
<td>zscalerlss-zpa-auth</td>
<td>ZPA User Authentication Logs</td>
</tr>
<tr>
<td>zscalerlss-zpa-bba</td>
<td>ZPA Browser Access Logs</td>
</tr>
<tr>
<td>zscalerapi-zia-audit</td>
<td>ZIA Administrative Audit Logs</td>
</tr>
<tr>
<td>zscalerapi-zia-sandbox</td>
<td>ZIA detailed Sandbox detonation Logs</td>
</tr>
</tbody>
</table>

Macros
Splunk Macros are used to shortcut frequently used sets of search commands. The Technical Addon defines several search macros to:

- Ease dashboard creation and the underlying reports
- Create a simple configuration point to specify a customer’s Zscaler data index

The search macros below are defined in the Zscaler Technical Add-On, and are used extensively throughout the Add-On and App. Zscaler suggests that any additional searches and reports created by Splunk admins and operators leverage these macros.

You might need to modify these macros depending on your Splunk configuration. The .

Macro Modification section contains more information.

Splunk CIM
Zscaler implemented the Splunk CIM to integrate tightly with Splunk enterprise security. The Zscaler Technical Add-On defines all the necessary field aliases and event tags to be compatible with Splunk’s CIM.

Zscaler tags events of the following types, models:

- Web and Proxy
- Security and Malware
- Firewall and IPS
- VPN
Modular Inputs

Zscaler’s Technical Add-On takes advantage of Splunk’s modular inputs to connect to Zscaler’s APIs for Sandbox and admin logs. You can configure each API configured separately, and multiple instances can be called should there be a need to ingest logs from multiple Zscaler tenants. Details of how to implement configurations can be found in *Modular Inputs* section.

The modular inputs are written in Python and are engineered to be compatible with Splunk Cloud (although full Splunk Cloud validation hasn’t occurred). Modular inputs use Zscaler and Splunk SDKs. The Zscaler SDK simplifies access to Zscaler APIs, and the Splunk SDK secures API keys and passwords and leverages Splunk search and state-tracking.

All modular input files are in the */bin* section of the Technical Add-On.

Zscaler Splunk App

The Zscaler Splunk App front-ends all the Zscaler data ingested into Splunk. This includes a large volume of saved searches and dashboards. The app’s menu is laid out similar to core Zscaler capabilities of Access Control, Threat Prevention, Private Access, and Data Protection. You can drill down into each area (with the exemption of Data Protection, which is currently in development).

![Figure 10. Splunk app menu](image)
You can download the app can be downloaded from the [Splunk Base](https://splunkbase.splunk.com/app/4297/).

Dependencies

The Zscaler Splunk App is dependent on:

- Zscaler’s Technical Add-On (Mandatory)
- Missile Map (Optional)

Missile Map is used for a single animated visualization. While it improves the look and visual display, it’s a non-essential function of the app.

User Interface

The Splunk App is the visual component of Zscaler’s Splunk integration. Other CIM-compatible Splunk tools or apps also visualize Zscaler data, but the App leverages a number of fields that are not part of the Splunk CIM. Below you will find a series of screenshots from the Splunk App.

The Zscaler Splunk App can serve as a useful base for you to create your own Zscaler oriented searches, reports, and dashboards.
Overview and Connections

Figure 11. Zscaler overview

Figure 12. Connections - visualizations
Access Control

Figure 13. Access control

Figure 14. Access control
Threat Prevention

Figure 15. Threat overview

Figure 16. Sandbox
Private Access

Figure 17. Private Access overview

Figure 18. Private Access health
Installation and Configuration

Zscaler Configuration

You must configure Zscaler to send data into Splunk. Follow Zscaler’s existing documentation to setup the base configuration of NSS, LSS, and API access. The relevant reference links are:

- About Nanolog Streaming Service
- About the Log Streaming Service
- About Cloud Service API Key Management

Output Strings

The Splunk App uses fields not included in the base output fields. Each of your LSS and NSS feeds must be configured as follows:

NSS Web

```
%{yy}-%{mth}-%{dd} %2d{hh}:%2d{mm}:%2d{ss} treason=%{reason} tevent_id=%{recordid} tprotocol=l=%{proto} taction=%{action} ttransactionsize=%{totalsize} tresponsesize=%{respsize} trequestsizem=%{reqsize} turlcategory=%{urlcat} \tserverip=%{sip} \tclienttranstime=%{ctime} trequestmethod=%{reqmethod} treferer="%{referer}" tuseragent="%{ua}" tproduct=NSS \tlocation=%{location} \tClientIP=%{cip} \tstatus=%{respcode} tuser=%{login} turl="%{eurl}" \tvendor=Zscaler \thostname=%{host} \tcclientpublicIP=%{cintip} \tthreatcategory=%{malwarecat} \tthreatname=%{threatname} \tfiletype=%{filetype} tappname=%{appname} tpagerisk=%{riskscore} \tddepartment=%{dept} \turlsecurecategory=%{urlsupercat} \ttappclass=%{appclass} \tdlpengine=%{dlpdict} \tfileclass=%{fileclass} \tbwthrottle=%{bwthrottle} \tservertranstime=%{stime} tmd5=%{bamd5} \tcontenttype=%{contenttype} ttrafficredirectmethod=%{trafficredirectmethod} \truellabel=%{rulelabel} \tmodule=%{module} \tproductversion=%{productversion} \treqdatasize=%{reqdatasize} \tresphdrsize=%{resphdrsize} \trespsize=%{respsize} \trespversion=%{respversion} \ttz=%{tz} 
```
%s{datetime}\tRecordtype=%s{tunnelactionname}\ttunneltype=%s{tunneltype}\tuser=%s{vpncredentialname}\tlocation=%s{locationname}\tsourceip=%s{sourceip}\tdestinationip=%s{destvip}\tsourceport=%d{srcport}\ttxbytes=%lu{txbytes}\trxbytes=%lu{rxbytes}\tdpdrec=%d{dpdrec}\tvendor=Zscaler\tproduct=tunnel_sample

IKE Phase 1
%s{datetime}\tRecordtype=%s{tunnelactionname}\ttunneltype=IPSEC IKE\d{ikeversion}\tuser=%s{vpncredentialname}\tlocation=%s{locationname}\tsourceip=%s{sourceip}\tdestinationip=%s{destvip}\tsourceport=%d{srcport}\tdestipstart=%d{dstport}\tlifetime=%d{lifetime}\tlifebytes=%d{lifebytes}\tspi=%d{spi}\talgo=%s{algo}\tauthentication=%s{authentication}\tauthtype=%s{authtype}\tvendor=Zscaler\tproduct=IKEv1

IKE Phase 2
%s{datetime}\tRecordtype=%s{tunnelactionname}\ttunneltype=IPSEC IKE\d{ikeversion}\tuser=%s{vpncredentialname}\tlocation=%s{locationname}\tsourceip=%s{sourceip}\tdestinationip=%s{destvip}\tsourceportstart=%d{srcportstart}\tdestinationportstart=%d{destportstart}\tsrcipstart=%s{srcipstart}\tsrcipend=%s{srcipend}\tsrcipstart=%s{srcipstart}\tsrcipend=%s{srcipend}\tlifetime=%d{lifetime}\tlifebytes=%d{lifebytes}\tspi=%d{spi}\talgo=%s{algo}\tauthentication=%s{authentication}\tauthtype=%s{authtype}\tpolicydirection=%s{policydirection}\tvendor=Zscaler\tproduct=IKEv2

Tunnel Event
%s{datetime}\tRecordtype=%s{tunnelactionname}\ttunneltype=%s{tunneltype}\tuser=%s{vpncredentialname}\tlocation=%s{locationname}\tsourceip=%s{sourceip}\tdestinationip=%s{destvip}\tsourceport=%d{srcport}\tevent=%s{event}\teventreason=%s{eventreason}\tvendor=Zscaler\tproduct=tunnel

NSS CFW
datetime=%s{time}\tuser=%s{ologin}\tddepartment=%s{dept}\tlocationname=%s{location}\tcport=%d{cport}\tcfport=%d{cfport}\tssport=%d{ssport}\tcip=%s{cip}\ttcip=%s{tcip}\tdsip=%s{dsip}\tssip=%s{ssip}\tspi=%d{spi}\tsip=%s{ssip}\ttstateful=%s{stateful}\taggregate=%s{aggregate}\tnwsvc=%s{nwsvc}\tnwapp=%s{nwapp}\tpproto=%s{ipproto}\tpipcat=%s{ipcat}\tdestcountry=%s{destcountry}\tavduration=%d{avduration}\trulelabel=%s{rulelabel}\tinbytes=%d{inbytes}\toutbytes=%d{outbytes}\tduration=%d{duration}\tdurationms=%d{durationms}\tnumsessions=%d{numsessions}\tvendor=Zscaler\tproduct=fw

NSS DNS
datetime=%s{time}\tuser=%s{ologin}\tddepartment=%s{dept}\tlocation=%s{location}\taction=%s{action}\trule=%s{rulelabel}\tdnat=%s{dnat}\ttthesis=%s{thesis}\tstateful=%s{stateful}\taggregate=%s{aggregate}\tnwsvc=%s{nwsvc}\ttclt_cip=%s{cip}\tsrv_dip=%s{cip}\bsthemy=%s{bmy}\tvendor=Zscaler\tproduct=dnss

NSS Alert

Web

<%d{syslogid}>%s{Monthname} %2d{Dayofmonth}
%02d{Hour}:%02d{Minutes}:%02d{Seconds} [%s{Deviceip}] ZscalerNSS:
%s{Eventinfo}\n
Firewall

<%d{syslogid}>%s{Monthname} %2d{Dayofmonth}
%02d{Hour}:%02d{Minutes}:%02d{Seconds} [%s{Deviceip}] ZscalerNSS:
%s{Eventinfo}\n
LSS Connector

{"LogTimestamp": %j{LogTimestamp:time},"Customer": %j{Customer},"SessionID":
%j{SessionID},"SessionType": %j{SessionType},"SessionStatus":
%j{SessionStatus},"Version": %j{Version},"Platform": %j{Platform},"ZEN":
%j{ZEN},"Connector": %j{Connector},"ConnectorGroup":
%j{ConnectorGroup},"PrivateIP": %j{PrivateIP},"PublicIP":
%j{PublicIP},"Latitude": %f{Latitude},"Longitude":
%f{Longitude},"CountryCode": %j{CountryCode},"TimestampAuthentication":
%j{TimestampAuthentication:iso8601},"TimestampUnAuthentication":
%j{TimestampUnAuthentication:iso8601},"CPUUtilization":
%d{CPUUtilization},"MemUtilization": %d{MemUtilization},"ServiceCount":
%d{ServiceCount},"InterfaceDefRoute": %j{InterfaceDefRoute},"DefRouteGW":
%j{DefRouteGW},"PrimaryDNSResolver": %j{PrimaryDNSResolver},"HostUpTime":
%j{HostUpTime},"ConnectorUpTime": %j{ConnectorUpTime},"NumOfInterfaces":
%d{NumOfInterfaces},"BytesRxInterface":
%d{BytesRxInterface},"PacketsRxInterface":
%d{PacketsRxInterface},"ErrorsRxInterface":
%d{ErrorsRxInterface},"DiscardsRxInterface":
%d{DiscardsRxInterface},"BytesTxInterface":
%d{BytesTxInterface},"PacketsTxInterface":
%d{PacketsTxInterface},"ErrorsTxInterface":
%d{ErrorsTxInterface},"DiscardsTxInterface":
%d{DiscardsTxInterface},"TotalBytesRx": %d{TotalBytesRx},"TotalBytesTx":
%d{TotalBytesTx},"vendor": "Zscaler", "product": "zpa_auth_connector"}\n
LSS App

NOTE
Zscaler recommends that “reauthBlock” be filtered (excluded) (navigate to Log Receiver > Log Stream > Session > reauthBlock) from the LSS stream as this variable can generate excess log volume from unattended client machines.

{"LogTimestamp": %j{LogTimestamp:time},"Customer": %j{Customer},"SessionID":
%j{SessionID},"ConnectionID": %j{ConnectionID},"InternalReason":
%j{InternalReason},"ConnectionStatus": %j{ConnectionStatus},"IPProtocol":
%d{IPProtocol},"DoubleEncryption": %d{DoubleEncryption},"Username":
%j{Username},"ServicePort": %d{ServicePort},"ClientPublicIP":
%j{ClientPublicIP},"ClientPrivateIP": %j{ClientPrivateIP},"ClientLatitude":
LSS Auth

{"LogTimestamp": %j{LogTimestamp:time},"Customer": %j{Customer},"Username": %j{Username},"SessionID": %j{SessionID},"SessionStatus": %j{SessionStatus},"Version": %j{Version},"ZEN": %j{ZEN},"CertificateCN": %j{CertificateCN},"PrivateIP": %j{PrivateIP},"PublicIP": %j{PublicIP},"CountryCode": %j{CountryCode},"TimestampAuthentication": %j{TimestampAuthentication},"TimestampUnAuthentication": %j{TimestampUnAuthentication},"TotalBytesRx": %d{TotalBytesRx},"TotalBytesTx": %d{TotalBytesTx},"vendor": "Zscaler", "product": "zpa_auth"

LSS Browser Access

Splunk Configuration

Prior to installing the App and Technical Add-on, Splunk architects or designers needs to determine where each component should be installed. These decisions can affect the overall Splunk design and enterprise change controls when implementing Zscaler Logs and APIs into Splunk.

*Search Head*

The Zscaler Splunk app can be installed exclusively on any Splunk search head. The App does not need any forwarding or index time execution.

If taking advantage of Zscaler’s Sandbox APIs, the Zscaler Technical Add-On needs to be installed on a search head as the App leverages saved Splunk Searches and Alerts to find any files pending execution in the Zscaler sandbox.

*Forwarders (or Indexers)*

Install the Zscaler Technical Add-On on either the Splunk heavy forwarders or indexers that receive the TCP data inputs for the Zscaler sourcetypes (the receivers of NSS and LSS streams). This lets Zscaler tag events and alias fields for the Splunk CIM (note the Zscaler App takes advantage of CIM tagged and mapped data model).

Zscaler follows normal Splunk WebUI- or CLI-based installation methods:

- The App and TA can be downloaded from the following locations:
  - [Zscaler Splunk App](#)
  - [Zscaler Technical Add-On for Splunk](#)
Network Inputs

Zscaler NSS and LSS streams are typically sent to Splunk via network inputs. This may inbuilt Splunk TCP input or prepossessed using Splunk Connect for Syslog (SC4S). Splunk recommends SC4S as the preferred solution.

Details for SC4S can be located here at this link: Welcome to Splunk Connect for Syslog!

Figure 19. Example Splunk TCP inputs
Example Configuration

**Figure 20. Example Splunk TCP inputs**

Note the UEBA above is an artifact of a non-Zscaler App and is not relevant to the Zscaler configuration.

**Modular Inputs**

Zscaler APIs are addressed via Splunk modular inputs. These can be seen, set, and configured in the TA’s setup page, and there is a specific configuration for each input type. Splunk best practice is using a Global Account for the API user, password, and key, and a setup screen when adding each input.

**Figure 21. Adding a global account**
Figure 22. Modular input configuration example (Sandbox)

Take care when defining the interval that you stay within your API rate limits. Details can be found here: API Rate Limit Summary.

**Macro Modification**

Your preexisting Splunk environment might use an index name different to what Zscaler’s Splunk App and Technical Add On expect. In this case, modify the macros.conf (or create a local/macros.conf) and override the “index= zscalerlogs” to match the index name used within your Splunk environment.

For example, if you use the name “zscalerlogs” you can change each macro definition as follows:

```
definition = index= zscalerlogs sourcetype=“zscalemss-dns”
```

Figure 23. Macro modification example

**Custom Field Mapping**

The Zscaler Splunk App and Technical Add-On look for field names as outlined above Output Strings. If you use different field names you or the Splunk admin need to:

1. Change your Zscaler log stream configurations to match what the app is expecting
2. Defined local field aliases to align to what the app is expecting
Appendix A: Splunk Configs

Event Types, Tags and Aliases

```
[Zscaler_CFW]
search = (sourcetype=zscalermss-fw)

[Zscaler_DNS]
search = (sourcetype=zscalermss-dns)

[Zscaler_Proxy_General]
search = (sourcetype=zscalermss-web)

[Zscaler_Proxy_DLP]
search = (sourcetype=zscalermss-web ruletype="DLP")

[Zscaler_ZPA]
search = (sourcetype=zscalerlss-zpa-app) OR (sourcetype=zscalerlss-zpa-auth) OR (sourcetype=zscalerlss-zpa-connector)

[Zscaler_Proxy_Malware]
search = (sourcetype="zscalermss-web" threatname!="None")

[Zscaler_Sandbox]
search = (sourcetype=zscalerapi-zia-sandbox)

[Zscaler_Audit]
search = (sourcetype=zscalerapi-zia-audit)
```

Figure 24. eventtypes.conf

```
[eventtype=Zscaler_DNS]
dns = enabled
network = enabled
resolution = enabled
```
[eventtype=Zscaler_CFW]
communicate = enabled
network = enabled

[eventtype=Zscaler_Proxy_General]
communicate = enabled
d = enabled
network = enabled
performance = enabled
proxy = enabled
session = enabled
start = enabled
web = enabled

[eventtype=Zscaler_Proxy_Malware]
attack = enabled
ids = enabled
malware = enabled

[eventtype=Zscaler_Proxy_DLP]
dl = enabled
incident = enabled

[eventtype=Zscaler_ZPA]
authentication = enabled
communicate = enabled
d = enabled
network = enabled
performance = enabled
session = enabled
start = enabled
vpn = enabled

Figure 25. tags.conf

```
[zscalemss-alerts]
pulldown_type = 1
category = Network & Security
description = Zscaler NSS System Alerts

[zscalemss-dns]
EVAL-vendor_product = Zscaler_ZIA_Firewall
FIELDALIAS-clt_sip_as_src = clt_sip AS src
FIELDALIAS-clt_sip_as_src_ip = clt_sip AS src_ip
FIELDALIAS-dns_req_as_query = dns_req AS query
FIELDALIAS-dns_reqtype_as_record_type = dns_reqtype AS record_type
FIELDALIAS-dns_resp_as_answer = dns_resp AS answer
FIELDALIAS-durationms_as_response_time = durationms AS response_time
FIELDALIAS-srv_dip_as_dest = srv_dip AS dest
FIELDALIAS-srv_dip_as_dest_ip = srv_dip AS dest_ip
FIELDALIAS-srv_dport_as_dest_port = srv_dport AS dest_port
pulldown_type = 1
category = Network & Security
description = Zscaler DNS Control Logs

[zscalemss-web]
EVAL-action = lower(action)
EVAL-app = Zscaler
EVAL-dlp_type = "Inline Gateway"
EVAL-duration = clienttranstime + servertranstime
EVAL-dvc = "Zscaler Cloud Proxy"
EVAL-dvc_zone = "Cloud Proxy"
EVAL-vendor_product = "Zscaler_ZIA_Proxy"
FIELDALIAS-ClientIP_as_src = ClientIP AS src
```
FIELDALIAS-ClientIP_as_src_ip = ClientIP AS src_ip
FIELDALIAS-aob_gen_zscalernss_web_alias_1 = protocol AS transport
FIELDALIAS-aob_gen_zscalernss_web_alias_2 = user AS src_user
FIELDALIAS-aob_gen_zscalernss_web_alias_3 = dlpengine AS severity
FIELDALIAS-aob_gen_zscalernss_web_alias_4 = threatname AS signature
FIELDALIAS-aob_gen_zscalernss_web_alias_5 = contenttype AS http_content_type
FIELDALIAS-aob_gen_zscalernss_web_alias_6 = hostname AS dest
FIELDALIAS-clientpublicIP_as_src_translated_ip = clientpublicIP AS src_translated_ip
FIELDALIAS-clienttranstime_as_response_time = clienttranstime AS response_time
FIELDALIAS-department_as_src_user_bunit = department AS src_user_bunit
FIELDALIAS-dlpdictionaries_as_signature = dlpdictionaries AS signature
FIELDALIAS-filename_as_file_name = filename AS file_name
FIELDALIAS-md5_as_file_hash = md5 AS file_hash
FIELDALIAS-referrerURL_as_http_referrer = refererURL AS http_referrer
FIELDALIAS-requestmethod_as_http_method = requestmethod AS http_method
FIELDALIAS-requestssize_as_bytes_in = requestsize AS bytes_in
FIELDALIAS-responsesize_as_bytes_out = responsesize AS bytes_out
FIELDALIAS-serverip_as_dest_ip = serverip AS dest_ip
FIELDALIAS-serverip_as_dest_translated_ip = translated_ip hostname AS dest
FIELDALIAS-threatcategory_as_category = threatcategory AS category
FIELDALIAS-transactionsize_as_bytes = transactionsize AS bytes
FIELDALIAS-urlcategory_as_category = urlcategory AS category
FIELDALIAS-useragent_as_http_user_agent = useragent AS http_user_agent
REPORT-ta_builder_internal_use_kv_format_results_for_zscalernss_web =
ta_builder_internal_use_kv_format_results_for_zscalernss_web
category = Network & Security
description = Zscaler Web/Proxy Logs
pulldown_type = 1

[zscalerlss-zpa-app]
EVAL-app = Zscaler
EVAL-vendor_product = Zscaler_ZPA

FIELDALIAS-aob_gen_zscalerlss_zpa_app_alias_1 = ServerIP AS dest_ip
FIELDALIAS-aob_gen_zscalerlss_zpa_app_alias_2 = ClientPublicIP AS src_ip
FIELDALIAS-aob_gen_zscalerlss_zpa_app_alias_4 = Application AS app
FIELDALIAS-aob_gen_zscalerlss_zpa_app_alias_5 = ServicePort AS dest_port
FIELDALIAS-aob_gen_zscalerlss_zpa_app_alias_6 = ConnectorPort AS src_port
FIELDALIAS-aob_gen_zscalerlss_zpa_app_alias_7 = Host AS dest

SHOULD_LINEMERGE = 0
category = Network & Security
description = Zscaler ZPA App Logs
pulldown_type = 1

[zscalerlss-zpa-auth]
EVAL-app = Zscaler

FIELDALIAS-aob_gen_zscalerlss_zpa_auth_alias_1 = Username AS user
FIELDALIAS-aob_gen_zscalerlss_zpa_auth_alias_3 = PublicIP AS src
FIELDALIAS-aob_gen_zscalerlss_zpa_auth_alias_4 = SessionStatus AS action
FIELDALIAS-aob_gen_zscalerlss_zpa_auth_alias_5 = Application AS app
FIELDALIAS-aob_gen_zscalerlss_zpa_auth_alias_6 = ServicePort AS dest_port
FIELDALIAS-aob_gen_zscalerlss_zpa_auth_alias_7 = ConnectorPort AS src_port
FIELDALIAS-aob_gen_zscalerlss_zpa_auth_alias_8 = Host AS dest

SHOULD_LINEMERGE = 0
category = Network & Security
description = Zscaler ZPA Auth Logs
pulldown_type = 1

[zscalerlss-zpa-connector]
EVAL-app = Zscaler

FIELDALIAS-aob_gen_zscalerlss_zpa_connector_alias_1 = Application AS app
FIELDALIAS-aob_gen_zscalerlss_zpa_connector_alias_2 = ServicePort AS dest_port
FIELDALIAS-aob_gen_zscalerlss_zpa_connector_alias_3 = ConnectorPort AS src_port
FIELDALIAS-aob_gen_zscalerfss_zpa_connector_alias_4 = Host AS dest

SHOULD_LINEMERGE = 0
category = Network & Security
description = Zscaler ZPA Connector Logs
pulldown_type = 1

[zscalerfss-fw]
EVAL-action = eval action=if(like(action, "%Allow"), "allowed", action)
EVAL-app = Zscaler
EVAL-bytes = inbytes + outbytes
EVAL-vendor_product = Zscaler_ZIA_Firewall
FIELDALIAS-cdip_as_dest_ip = cdip AS dest_ip
FIELDALIAS-cdport_as_dest_port = cdport AS dest_port
FIELDALIAS-csip_as_src = csip AS src
FIELDALIAS-csip_as_src_ip = csip AS src_ip
FIELDALIAS-csport_as_src_port = csport AS src_port
FIELDALIAS-csport_as_src_translated_port = csport AS src_translated_port
FIELDALIAS-inbytes_as_bytes_in = inbytes AS bytes_in
FIELDALIAS-locationname_as_src_zone = locationname AS src_zone
FIELDALIAS-outbytes_as_bytes_out = outbytes AS bytes_out
FIELDALIAS-proto_as_protocol = proto AS protocol
FIELDALIAS-proto_as_transport = proto AS transport
FIELDALIAS-sdip_as_dest = sdip AS dest
FIELDALIAS-sdip_as_dest_translated_ip = sdip AS dest_translated_ip
FIELDALIAS-sdport_as_dest_translated_port = sdport AS dest_translated_port
FIELDALIAS-tsip_as_src_translated_ip = tsip AS src_translated_ip
category = Network & Security
description = Zscaler Firewall Logs
pulldown_type = 1

[zscalerapi-zia-audit]
TRUNCATE=0

category = Network & Security

description = Zscaler ZIA Admin Audit Logs

pulldown_type = 1

FIELDALIAS-cloudname = "log{}.AA in Cloud" AS cloudname
FIELDALIAS-action = "log{}.Action" AS action
FIELDALIAS-category = "log{}.Category" AS category
FIELDALIAS-src_ip = "log{}.Client IP" AS src_ip
FIELDALIAS-interface = "log{}.Interface" AS interface
FIELDALIAS-post_action = "log{}.Post Action" AS post_action
FIELDALIAS-pre_action = "log{}.Pre Action" AS pre_action
FIELDALIAS-resource = "log{}.Resource" AS resource
FIELDALIAS-result = "log{}.Result" AS result
FIELDALIAS-sub_category = "log{}.Subcategory" AS sub_category
FIELDALIAS-time = "log{}.Time" AS time
FIELDALIAS-user = "log{}.User" AS user

[zscalerapi-zia-sandbox]

TRUNCATE=0

category = Network & Security

description = Zscaler Sandbox detonation reports

pulldown_type = 1

FIELDALIAS-class_category = "Full Details.Classification.Category" AS class_category
FIELDALIAS-class_detect_mal = "Full Details.Classification.DetectedMalware" AS class_detect_mal
FIELDALIAS-class_score = "Full Details.Classification.Score" AS class_score
FIELDALIAS-class_type = "Full Details.Classification.Type" AS class_type
FIELDALIAS-exploit_risk = "Full Details.Exploit{}.Risk" AS exploit_risk
FIELDALIAS-exploit_sig = "Full Details.Exploit{}.Signature" AS exploit_sig
FIELDALIAS-exploit_sig_source = "Full Details.Exploit{}.SignatureSources{}" AS exploit_sig_source
FIELDALIAS-file_size = "Full Details.FileProperties.FileSize" AS file_size
FIELDALIAS-file_type = "Full Details.FileProperties.FileType" AS file_type
FIELDALIAS-file_cert_issuer = "Full Details.FileProperties.Issuer" AS file_cert_issuer
FIELDALIAS-file_hash = "Full Details.FileProperties.MD5" AS file_hash
FIELDALIAS-md5 = "Full Details.FileProperties.MD5" AS md5
FIELDALIAS-file_cert_root = "Full Details.FileProperties.RootCA" AS file_cert_root
FIELDALIAS- sha1 = "Full Details.FileProperties.SHA1" AS sha1
FIELDALIAS-ssdeep = "Full Details.FileProperties.SSDeep" AS ssdeep
FIELDALIAS-sha2 = "Full Details.FileProperties.Sha256" AS sha2
FIELDALIAS-sha256 = "Full Details.FileProperties.Sha256" AS sha256
FIELDALIAS-net_risk = "Full Details.Networking{}.Risk" AS net_risk
FIELDALIAS-net_sig = "Full Details.Networking{}.Signature" AS net_sig
FIELDALIAS-net_sig_source = "Full Details.Networking{}.SignatureSources{}" AS net_sig_source
FIELDALIAS-country = "Full Details.Origin.Country" AS country
FIELDALIAS-language = "Full Details.Origin.Language" AS language
FIELDALIAS-orig_risk = "Full Details.Origin.Risk" AS orig_risk
FIELDALIAS-persist_risk = "Full Details.Persistence{}.Risk" AS persist_risk
FIELDALIAS-persist_sig = "Full Details.Persistence{}.Signature" AS persist_sig
FIELDALIAS-persist_sig_source = "Full Details.Persistence{}.SignatureSources{}" AS persist_sig_source
FIELDALIAS-bypass_risk = "Full Details.SecurityBypass{}.Risk" AS bypass_risk
FIELDALIAS-bypass_sig = "Full Details.SecurityBypass{}.Signature" AS bypass_sig
FIELDALIAS-bypass_sig_source = "Full Details.SecurityBypass{}.SignatureSources{}" AS bypass_sig_source
FIELDALIAS-stealth_risk = "Full Details.Stealth{}.Risk" AS stealth_risk
FIELDALIAS-stealth_sig = "Full Details.Stealth{}.Signature" AS stealth_sig
FIELDALIAS-stealth_sig_source = "Full Details.Stealth{}.SignatureSources{}" AS stealth_sig_source
FIELDALIAS-category = "Full Details.Summary.Category" AS category
FIELDALIAS-duration = "Full Details.Summary.Duration" AS duration
FIELDALIAS-start_time = "Full Details.Summary.StartTime" AS start_time
FIELDALIAS-status = "Full Details.Summary.Status" AS status
FIELDALIAS-risk = "Full Details.SystemSummary{}.Risk" AS risk
FIELDALIAS-signature = "Full Details.SystemSummary{}.Signature" AS signature
FIELDALIAS-sig_source = "Full Details.SystemSummary().SignatureSources()" AS sig_source

[zscalerlss-zpa-bba]
EVAL-app = Zscaler
EVAL-vendor_product = Zscaler_ZPA
FIELDALIAS-aob_gen_zscalerlss_zpa_app_alias_1 = ServerIP AS dest_ip
FIELDALIAS-aob_gen_zscalerlss_zpa_app_alias_2 = ClientPublicIP AS src_ip
FIELDALIAS-aob_gen_zscalerlss_zpa_app_alias_4 = Application AS app
FIELDALIAS-aob_gen_zscalerlss_zpa_app_alias_5 = ServicePort AS dest_port
FIELDALIAS-aob_gen_zscalerlss_zpa_app_alias_6 = ConnectorPort AS src_port
FIELDALIAS-aob_gen_zscalerlss_zpa_app_alias_7 = Host AS dest
SHOULD_LINEMERGE = 0
category = Network & Security
description = Zscaler ZPA Browser Access Logs
pulldown_type = 1

Figure 26. props.conf

[z-dns]
definition = index=zscaler sourcetype="zscalernss-dns"
iseval = 0

[z-fw]
definition = index=zscaler sourcetype="zscalernss-fw"
iseval = 0

[z-web]
definition = index=zscaler sourcetype="zscalernss-web"
iseval = 0

[z-sandbox]
definition = index=zscaler sourcetype="zcalerapi-zia-sandbox"
iseval = 0
[z-audit]
definition = index=zscaler sourcetype="zscaler-api-zia-audit"
iseval = 0

[z-index]
definition = index=zscaler
iseval = 0

[z-zpa]
definition = index=zscaler sourcetype="zscaler-lss-zpa"
iseval = 0

[z-zpa-app]
definition = index=zscaler sourcetype="zscaler-lss-zpa-app"
iseval = 0

[z-zpa-auth]
definition = index=zscaler sourcetype="zscaler-lss-zpa-auth"
iseval = 0

[z-zpa-con]
definition = index=zscaler sourcetype="zscaler-lss-zpa-connector"
iseval = 0

[z-webuser-list]
definition = tstats prestats=false local=false summariesonly=true count from datamodel=Web where nodename=Web.Proxy by Web.user | rename Web.user AS user
iseval = 0

[z-zpauser-list]
definition = tstats count AS "Count of VPN" from datamodel=Network_Sessions where (nodename = All_Sessions.VPN) groupby All_Sessions.user prestats=true | stats dedup_splitvals=t count AS "Count of VPN" by All_Sessions.user | sort limit=100 All_Sessions.user | fields - _span | rename All_Sessions.user AS user | fillnull "Count of VPN" | fields user, "Count of VPN"
iseval = 0

Figure 27. macros.conf
Appendix B: Splunk Essential Configuration (Using NSS VM-Stream Syslog Over TCP)

This appendix details how to perform the initial integration between Splunk and Zscaler for logs that are streamed to a Splunk instance from ZIA using Syslog over plaintext TCP.

Configure Zscaler NSS

Zscaler configuration guides are available on the below links. An overview of NSS can be located at About Nanolog Streaming Service.

Deploy NSS

- NSS Deployment Guide for Microsoft Azure
- NSS Deployment Guide for Amazon Web Services
- NSS Deployment Guide for VMWare vSphere
- Networking NSS Virtual Appliances
- Troubleshooting Deployed NSS Servers

Add NSS Feeds

- Adding NSS Feeds

Add or Create Index

This section requires Admin access to a working instance of Splunk.

Log into Splunk Instance

By default, Splunk login portal listens on TCP port 8000. Login using your admin username and password by connecting to your Splunk instance over HTTPS.

Configure New Index in Splunk

The index is the repository for Splunk Enterprise data. Splunk Enterprise transforms incoming data into events, which it stores in indexes.
Splunk Enterprise manages indexes to facilitate flexible searching and fast data retrieval, eventually archiving them according to a user-configurable schedule.

![Log flow pipeline diagram]

*Figure 29. Log flow pipeline*
After logging into Splunk, navigate to **Settings > Indexes > New Index.**

![Figure 30. View indexes](image)

**Add Zscaler Index in Splunk**

Zscaler creates an index titled “zscaler”. Since the Splunk App for Zscaler looks for data written at index “zscaler” by default, setting “index=zscaler” allows us to use the Splunk App for Zscaler out of the box.

In the **New Index** dialog, type “zscaler” without quotes (case sensitive) and hit **Save.**

![Figure 31. Add Zscaler index in Splunk](image)
Create Data Inputs

*Splunk Connect for Syslog*

Syslog is Splunk’s preferred method of ingesting high volumes of data. Details can be located at [Welcome to Splunk Connect for Syslog!](#)

**TCP Data Input**

Navigate to Settings > Data Inputs > TCP (Add new).

This brings you to following screen. This step configures Splunk to listen on TCP using port 514. NSS only supports TCP, but you can configure the destination port. Most administrators use port “514” as it is the default port for UDP-based syslog. After configuring SIEM port, click **Next**.

![Configure new TCP input](image)

**Select the Desired Zscaler Source Type**

When Splunk indexes data, it does so from a source entity that provides data for Splunk to extract (e.g., Windows event logs or *nix syslogs). Splunk tags incoming data with a "source" field as it gets indexed. The source type is an indicator for the type of data, so that Splunk knows how to properly format and extract it as it comes in. It's also a convenient way to categorize data, as you can use Splunk search to display all data of a certain source type.

For example, Windows event logs, NSS web logs, NSS Firewall logs are all sourcetypes.

If multiple web NSS servers send logs to the same Splunk instance, they all belong to the same sourcetype, but each one of these servers constitute an independent source.
Splunk apps use sources and sourcetypes to extract knowledge from the data they index. Type “zscaler” to display all possible Zscaler-specific sourcetypes. Please select the option based on the kind of Zscaler logs sent to Splunk.

**Figure 33. Select desired Zscaler source type**

**Change Default App Context and Default index**

On the same page as before:

1. Select **Zscaler Splunk App** as the App context
2. select **zscaler** as the index from the drop-down menu
3. Click **Review** and then **Submit**.

**Figure 34. Change default app context**
Verify Incoming Logs

Click **Start Searching** to verify that logs are flowing from Zscaler into Splunk.

![TCP input has been created successfully.](image)

**Figure 35. Verify incoming logs**

Inspect Log Fields

This displays only the logs that from Zscaler.

![Inspect log fields](image)

**Figure 36. Inspect log fields**
Extracted Log Fields

Verify that the index and sourcetype of the incoming logs match what you set up earlier.

Figure 37. View extracted log fields

Verify Splunk’s Zscaler App

Navigate to Apps > Zscaler Splunk App.

It should be populated with incoming Zscaler data.

Figure 38. Verify Splunk Zscaler app
If a particular panel is not getting populated, click on the magnifying glass next to it. This shows the query that the panel is running behind the scenes to help with troubleshooting.

![Verify Splunk Zcaler app](image-url)

**Figure 39. Verify Splunk Zcaler app**
Appendix C: Splunk Essential Configuration (using Cloud-to-Cloud logging- HTTPS POST)

This appendix details initial integration between the Splunk Cloud and Zscaler Internet Access (ZIA) if logs are streamed to the Splunk Cloud instance from ZIA using HEC input on the Splunk cloud.

Cloud NSS is a cloud-to-cloud log streaming service that allows you to stream logs directly from the ZIA cloud into a supported cloud-based SIEM, without the need to deploy an NSS VM for web or Firewall. The service supports all ZIA log types: web, SaaS security, tunnel, Firewall, and DNS.

When you subscribe to the service, you can configure cloud NSS feeds for each log type to an HTTPS API-based log collector hosted on your cloud SIEM. Rather than deploying, managing, and monitoring on-premises NSS VMs, customers can simply configure an HTTPS API feed that pushes logs using HTTP POST from the Zscaler cloud service into an HTTPS API endpoint on the SIEM. For the Splunk cloud, this is the HEC input.

Please contact Zscaler support to request access to this service.

Figure 40. High-level overview of cloud-to-cloud logging

Customers can subscribe to Cloud NSS, which allows direct cloud-to-cloud log streaming for all types of ZIA logs into a Splunk instance.

The following links provide information about cloud-to-cloud logging:

- NSS as service for cloud to cloud logging
- About Cloud NSS Feeds

Add NSS Feeds

- Adding Cloud NSS Feeds

Configure Splunk Cloud to Ingest ZIA Logs over HEC Input

This section requires admin access to a working instance of Splunk cloud.

The Splunk HTTP Event Collector (HEC) sends data and application events to a Splunk deployment over the HTTPS. HEC uses a token-based authentication model. You can generate a token and then configure a logging library or HTTP client with the token to send data to HEC in a specific format. The HEC token that is created from the steps below needs to be pasted later into the ZIA Admin Portal. While the HEC token is a must in this deployment, in addition customers can optionally restrict which public source IPs are allowed to send logs to their Splunk cloud stack. Customers should get in touch with Splunk support to employ any IP-level “allow lists.”
Log into Splunk Cloud Tenant

After logging in, navigate to Apps > Find more App and search for “zscaler”.

Customers can install “Zscaler Splunk App” on their Splunk cloud tenant.

**IMPORTANT**

Customers need to contact the Splunk cloud support team to get “Zscaler Technical Add-on (TA)” installed in their Splunk cloud tenant.

Figure 41. Log into Splunk Cloud tenant

Install Zscaler App and Zscaler TA in Your Cloud Tenant

Figure 42. Install Zscaler App and TA
Create Zscaler Index in Splunk

After installing Zscaler App and TA, navigate to Settings > Indexes > New Index.

Add Zscaler Index in Splunk

In the New Index dialog, type “zscaler” (case sensitive) and hit Save.

Since the Splunk App for Zscaler looks for data written at index “zscaler” by default, setting “index=zscaler” allows us to use the Splunk App for Zscaler out of the box.
Zscaler does not have a specific recommendation for **Max raw data size**, **Searchable time**, or **Dynamic Data Storage**. These values depend entirely on customer setup, amount of logs, cost associated with storage in Splunk cloud, etc., and vary from customer to customer.

[Split has documentation regarding these settings.](#)

![New Index](image)

*Figure 44. Add Zscaler index in Splunk*
Create a new Data Input and HEC token

After creating index in previous step, navigate to **Settings > Data Input.**

**Figure 45. Navigate to data inputs**

The following screen appears. Click the option to **Add new** input.

**Figure 46. Create new input**
Configure Data Input and HEC token

Now create an HEC token. This is a 32-character long unique token that is part of every POST API call from ZIA to the Splunk cloud. It works as an authorization token and is part of each HTTP POST API call made from the Zscaler logging service to the Splunk cloud.

**NOTE**
Do not enable indexer acknowledgement.

Provide a token name. Leave the rest of options at default settings and click **Next**.

*Figure 47. Configuring HEC token and input*
In this example, we are sending ZIA WEB logs to the Splunk cloud. Thus, the sourcetype selected in this example is “zscalernss-web”. Please change the sourcetype to match the log type that you wish to ingest (for example, “zscalernss-fw”, “zscalernss-dns” etc.).

**Figure 48. Configuring HEC token and input (cont.)**
This brings you to the review screen. Confirm the settings and click **Submit**.

**Figure 49. Review the setup**
This opens the following screen. The token may take a few minutes to get deployed in Splunk cloud.

![Token deployment screen](image)

**Token is being deployed.**

- Track deployment progress
- Configure your inputs by going to Settings > Data Inputs

**Token Value**: F74DF5F6-1A49-44F4-98EE-CE233

- **Start Searching**: Search your data now or see examples and tutorials.
- **Extract Fields**: Create search-time field extractions. Learn more about fields.
- **Add More Data**: Add more data inputs now or see examples and tutorials.
- **Download Apps**: Apps help you do more with your data. Learn more.
- **Build Dashboards**: Visualize your searches. Learn more.

*Figure 50. Wait for token to be deployed*
Copy the HEC Token Value

Once the token is deployed, navigate back to Setting > Data Input > HTTP Event Collector.

You will see the 32-character long HEC token on this screen. Make a note of this token for use in the ZIA Admin Portal later. In Splunk, HEC tokens are tied to different sourcetypes (Zscaler’s sourcetypes: web, Firewall, DNS etc.).

NOTE

Create separate HEC tokens for each of the Zscaler log source types. For example, create an HEC token used for zscaler-ss-web only, a separate HEC token used by zscaler-ss-fw only, and a separate HEC token just for zscaler-ss-dns etc. This allows for better scaling and renewing and invalidating HEC tokens in the future, if needed, without affecting other Zscaler sourcetypes.

Figure 51. Note down HEC token

Determine the Splunk Cloud API Endpoint to Send Logs To

The Splunk API endpoint “host” to send logs to depends on your Splunk cloud deployment. Please refer to Set up and use HTTP Event Collector in Splunk Web to determine the “host” portion. We will use JSON-formatted log messages.

The “endpoint” portion is always “/services/collector”, and endpoint “/services/collector/raw” does not come into play.
Write down the complete API URL corresponding to your Splunk cloud instance.

**Send data to HTTP Event Collector on Splunk Cloud instances**

Depending on the type of Splunk Cloud that you use, you must send data using a specific URI for HEC.

The standard form for the HEC URI in self-service Splunk Cloud is as follows:

```
<protocol>://input=<host>:<port>///<endpoint>
```

The standard form for the HEC URI in managed Splunk Cloud is as follows:

```
<protocol>://http-inputs=<host>:<port>///<endpoint>
```

Where:
- `<protocol>` is either `http` or `https`
- `<host>` is the Splunk instance that runs HEC
- `<port>` is the HEC port number
  - 8088 on self-service Splunk Cloud instances
  - 443 on managed Splunk Cloud instances
- `<endpoint>` is the HEC endpoint you want to use. In many cases, you use the `/services/collector` endpoint for JavaScript Object Notation (JSON)-formatted events or the `services/collector/raw` endpoint for raw events
- For self-service Splunk Cloud plans, you must pre-pend the hostname with `input-`
- For managed Splunk Cloud plans, pre-pend the hostname with `http-inputs-`

**NOTE**

If you do not include these prefixes before your Splunk Cloud hostname when you send data, the data cannot reach HEC.

**Figure 52. Figure out Splunk Cloud API endpoint to send logs to**

**Configure Splunk Cloud IDM to Fetch Zscaler Audit Logs and Sandbox Events**

Inputs Data Manager (IDM) is a Splunk instance within a Splunk Cloud Stack that sets up and configures modular and scripted inputs. As a part of a stack, IDM is managed by Splunk. IDM is a unique instance, meaning that it exists independently and separately from a search head, and does not belong to a search or indexing cluster. Zscaler Splunk TA needs to be installed on IDM (customers must contact Splunk support).

Zscaler username, password, and API credentials will be configured on the Splunk TA installed on IDM. This initiates API calls from the Splunk cloud to Zscaler to fetch audit logs and Sandbox reports.

**NOTE**

Customers would also need to request Splunk cloud support team to enable “Scheduled search” capabilities on their IDM. This setting is disabled in Splunk cloud by default.

The [Splunk IDM Overview](#) documentation contains more information.
Log into Splunk IDM Instance

Log into Splunk cloud IDM

Install Zscaler Splunk TA on Splunk IDM Instance

After logging in, navigate to Apps > Find more Apps and search for “zscaler”.

Customers need to contact Splunk cloud support team to get Zscaler Technical Add-On (TA) installed in their Splunk cloud tenant. Zscaler Splunk App doesn’t need to be installed on IDM.

Figure 53. Log into Splunk cloud IDM

Figure 54. Install Zscaler App and TA
**Configure Zscaler Index on Splunk IDM Instance**

After Zscaler Splunk TA is installed on Splunk IDM, navigate to **Settings > Indexes** and create a new “zscaler” index.

Click **Save** after filling in the details.

![New Index](image)

*Figure 55. Add Zscaler Index in Splunk IDM*

**Add Zscaler Account Used by Splunk IDM to Make API Calls to ZIA**

Head over to **Configuration > Account > Add.**

![Configuration](image)

*Figure 56. Create new account in Splunk IDM*
Fill in the Zscaler credentials pertinent to your ZIA tenant and save the settings by clicking Add.

Figure 57. Fill in ZIA credentials in Splunk IDM

Configure Input for Audit Logs

In IDM, head over to Inputs > Create New Input. First, configure input for fetching “Zscaler Audit Logs”.

Figure 58. Add audit logs input in Splunk IDM
Fill in the Settings for Fetching ZIA Audit Logs

After filling in the details, hit Add. Settings may take a few minutes to take effect.

![Add Zscaler Audit Logs](image)

**Figure 59. Save Audit Logs input in Splunk IDM**

Configure Input for Sandbox Events

In IDM, head over to Inputs > Create New Input. Now configure input for fetching “Zscaler Sandbox Events”.

![Add Sandbox events input in Splunk IDM](image)

**Figure 60. Add Sandbox events input in Splunk IDM**
Fill in the Settings for Fetching ZIA Sandbox Events

After filling in the details, hit Add. Settings may take a few minutes to take effect.

![Add Zscaler Sandbox Events](image)

**Figure 61. Save Sandbox events input in Splunk IDM**

Confirm that Both Input Settings are Saved and Enabled

You should now be able to see the audit log and Sandbox events settings under the Inputs section on IDM. Confirm that they are Enabled.

![Splunk inputs](image)

**Figure 62. Confirm that both inputs are enabled in Splunk IDM**

Configure Zscaler for Cloud-to-Cloud Logging

Customers can subscribe to Cloud NSS, which allows direct cloud-to-cloud log streaming for all types of ZIA logs into a Splunk instance. Rather than deploying, managing, and monitoring on-premises NSS VMs, customers can configure an HTTP or HTTPS API feed that pushes logs from the Zscaler cloud service into an HTTPS API endpoint on the SIEM. This is the HEC input for the Splunk cloud. Steps below show how to setup the log feed for web logs. Customers need to repeat these steps to setup other Zscaler log types (e.g., Firewall or DNS logs).
Navigate to Cloud-to-Cloud Logging Section in ZIA Portal

After logging into ZIA admin portal, navigate to Administration > Nanolog Streaming Service > Cloud NSS Feeds > Add Cloud NSS Feed.

![Image of ZIA portal with Cloud NSS Feeds section highlighted]

**Figure 63. Navigate to cloud-to-cloud logging section in ZIA**

Setup the Cloud NSS Log Feed (Web)

Select Splunk as the SIEM type from the drop-down.

The API URL is a Splunk URL dependent on customer’s Splunk cloud stack.

**NOTE**

Add “?auto_extract_timestamp=true” at the end of the Splunk cloud API endpoint. For example, if your Splunk API URL is:

```plaintext
https://http-inputs-partnerstack05.splunkcloud.com:443/services/collector
```

then, while configuring it in ZIA UI, you should configure it as:

```plaintext
https://http-inputs-partnerstack05.splunkcloud.com:443/services/collector?auto_extract_timestamp=true
```

Authorization header contains the relevant Splunk HEC token created in previous steps.

In the Add Cloud NSS Feed dialog, **Key1** is “Authorization”. **Value1** is the HEC token in the format “Splunk XXX-XXX-XXX” (replace XXX with actual HEC token value).
Feed Output Type is JSON from the drop down. Save config after filling in required parameters. Add \" (comma, backslash, double quotes) to the Feed Escape Character list.

**Figure 64. Configure cloud NSS feed**
**Figure 65. Example with all fields populated (web)**

**Setup the Cloud NSS Log Feed (Firewall)**

Select **Splunk** as the **SIEM Type** from the drop-down.

The API URL is a Splunk URL, dependent on customer’s Splunk cloud stack.
NOTE
Add “?auto_extract_timestamp=true” at the end of the Splunk cloud API endpoint.
For example, if your Splunk API URL is:

https://http-inputs-partnerstack05.splunkcloud.com:443/services/collector

then, while configuring it in ZIA UI, you should configure it as:

https://http-inputs-partnerstack05.splunkcloud.com:443/services/collector?auto_extract_timestamp=true

Authorization header contains the relevant Splunk HEC token created in previous steps.

In the Add Cloud NSS Feed dialog, Key1 is “Authorization”. Value1 is the HEC token in format “Splunk XXX-XXX-XXX” (replace XXX with actual HEC token value).

Select the Feed Output Type of JSON from the drop down. Add ",\" (comma, backslash, double quotes) to the Feed Escape Character list. In the Feed Output Format, change the “sourcetype” to “zscalernss-fw”.

After filling in required parameters, click Save.

Figure 66. Configure cloud NSS feed
Repeat the steps above to add other log sourcetypes (for example, DNS logs, tunnel logs, etc.).

Make sure to edit the feed output format to “zscalernss-dns”, “zscalernss-tunnel”, etc. Refer to the table in the Sourcetypes section for a list of sourcetypes.
Validate NSS Cloud Configuration

Once the config is saved, click the icon shown in screenshot below to verify connectivity from ZIA cloud to Splunk cloud. This sends a sample or test log message from the ZIA cloud to Splunk. Cloud-to-cloud connectivity is verified if Splunk sends the expected response.

**Figure 68. Verify connectivity to Splunk cloud**

Once the connectivity is verified, the **Connectivity Test** column changes from **Validation Pending** to **Validation Successful**.

**Figure 69. Splunk cloud connectivity verified**
Verify Splunk’s Zscaler App

Log back into your Splunk cloud tenant and navigate to Apps > Zscaler Splunk App.

It should be populated with incoming Zscaler log data.

![Verify Splunk Zscaler app](image)

**Figure 70. Verify Splunk Zscaler app**

If you see a particular panel not populated, click on the magnifying glass next to it. This shows you the query that the panel is running behind the scenes, which helps with troubleshooting.

![Access individual searches within Splunk Zscaler app](image)

**Figure 71. Access individual searches within Splunk Zscaler app**
Appendix D: Using Phantom (SOAR) with Zscaler and Splunk

Splunk Phantom is a security orchestration, automation, and response (SOAR) system. The Splunk Phantom platform combines security infrastructure orchestration, playbook automation, and case management capabilities to integrate your team, processes, and tools to help you orchestrate security workflows, automate repetitive security tasks, and quickly respond to threats.


Phantom components

![Phantom components diagram](image)

Figure 72. Phantom components

A Sample Playbook to Showcase Zscaler and Phantom Integration

This sample playbook leverages Splunk, Splunk ES, Phantom, and Zscaler NSS logs for threat hunting using custom threat feeds.

In the example, ZIA NSS logs are streamed to Splunk (SIEM). Phantom talks to the ZIA tenant as well as the Splunk instance to which NSS logs are being sent.
A custom threat feed (IOC type: malicious Domains) that the customer subscribes to is ingested into Splunk ES (which is part of Splunk). Splunk ES then looks for an overlap between domains on the threat feed and incidents of them being accessed via ZIA in the past (over an adjustable interval). If it finds an overlap, a notable event is created by Splunk ES and sent to Phantom.

Phantom then checks to see if Zscaler currently classifies this domain as malicious. If Zscaler classifies this domain as malicious, Phantom triggers a search in NSS logs that were consumed by Splunk to look at historical data (time range is adjustable) and try to find which users have accessed those domains.

If Zscaler doesn’t classify them as malicious, Phantom adds the domain to the customer’s ZIA disallowed list and then looks at historical data (time range is adjustable) to find which users have accessed those domains by triggering a search over NSS logs that were consumed by Splunk.

Phantom then send an email to network admin detailing which users were exposed to these domains, along with relevant timestamps.

**NOTE**

In steps below, we’ll enable a Phantom instance to communicate with Splunk and Zscaler. We will also configure a sample playbook which will be used to automate threat hunting. This is just an example of what is achievable by leveraging Phantom abilities with Zscaler’s APIs. Customers can (and should) build their own playbooks to implement their custom use cases.

---

**Zscaler**
- Generates (ZIA) logs that get sent to Splunk (SIEM)

**Splunk ES**
- Splunk ES subscribes to various threat feeds
- ES runs correlation searches against Zscaler logs and threat feeds
- Based on correlation, if needed, ES creates notable events and feeds them to Phantom

**Phantom**
- Phantom playbooks get triggered based on these notable events
- Playbook actions connect to Zscaler via REST API and add IP and Domain to tenant level ZIA custom blacklist, if required.
- Playbook also emails security admins, details about which users were exposed to this domain
Configuring Phantom

The following steps assume that you have Admin access to the Phantom instance.

*Create new Event Label in Phantom*

Splunk sends events to Phantom with this label. Phantom playbook is triggered only for events that contain this label.

This is a way to limit a playbook to take actions only on specific kind of events.

Navigate to **Administration > Event Settings > Label Settings** and then **+ Label**.

![Image](image_url)

*Figure 73. Create event label in Phantom*

We will name it “from_correlation_splunk_search”.

![Image](image_url)

*Figure 74. Create event label in Phantom*
Create Automation User in Phantom

This username is used by Splunk to communicate with Phantom.

Navigate to **Administration > Users** and create a new automation user with following settings.

![Create User](image)

**Figure 75. Create automation user in Phantom**

Click on username we created and copy the section shown below for your record. This is used by Splunk to authenticate with Phantom.

![Edit User](image)

**Figure 76. Create automation user in Phantom**
Installing Zscaler App on Phantom

Log into Phantom and navigate to Apps.

Search for Zscaler App

Search for “zscaler”. Head over to Unconfigured Apps > Configure new Asset.

Figure 77. Navigate to Apps section in Phantom

Figure 78. Search for Zscaler app in Phantom
Configure Zscaler App

As shown below, the Asset Info tab takes free form text input. Name your asset as per your organization’s naming conventions.

![Zscaler App Configuration](image)

**Figure 79. Configure Zscaler app in Phantom**

Fill out Asset Settings with your pertinent ZIA tenant details as shown below.
After filling all the details, **Save** and then click **Test Connectivity**.

![Zscaler and Splunk Deployment Guide](image)

**Figure 80. Configure Zscaler app in Phantom**

**Test Connectivity Between Phantom and Zscaler**

If all the information is filled in correctly, the connectivity test should pass and you should get result similar to the one shown below.

![Zscaler and Splunk Deployment Guide](image)

**Figure 81. Test connectivity between Phantom and Zscaler**
Installing Splunk App on Phantom

**Figure 82. Install Splunk app**

**Search for Splunk App**

Search for “splunk”.

Head over to Unconfigured Apps > Configure New Asset.

**Figure 83. Search for Zscaler app in Phantom**
**Configure Splunk App**

The **Asset Info** tab takes free form text input. Name your asset as per your organization’s naming conventions.

![Configure Splunk App](image)

*Figure 84. Configure asset info*

Fill out **Asset Settings** with your pertinent Splunk details as shown below. Make sure that communication from Phantom to Splunk on port 8089 is permitted by the network.

![Configure Splunk app in Phantom](image)

*Figure 85. Configure Splunk app in Phantom*
Under **Ingest Settings**, set the **Polling Interval** per your operational needs. In this document, we set it to one minute.

![Splunk app screenshot](image)

**Figure 86.**
**Test connectivity Between Phantom and Splunk**

If all the information is filled in correctly, the connectivity test should pass, and you should get a result like one shown below.

![Testing Connectivity](image)

*Figure 87. Test connectivity between Phantom and Splunk*

**Download Zscaler Playbook**

Download Zscaler playbook using [this link](#) and import it into your Phantom instance.

![Import Playbook](image)

*Figure 88. Upload sample playbook to Phantom*

This playbook does a correlation search against known malicious IP and domains and the customer’s ZIA logs. If a malicious IP and domain is found in these logs, the playbook checks if that IP and domain is already on that customer’s Zscaler disallow list.

If it is, then no action is taken.

If it is not on the disallow list, Phantom checks how Zscaler classifies this IP and domain. If Zscaler classifies it as “Unknown”, Phantom updates Zscaler’s disallow list via an API call.
Edit the playbook settings

Navigate to playbooks and open the one that we imported. Edit the playbook properties and mark it as Active.

Also change Operates on to the label we created earlier in the dropdown and click Save.

Figure 89. Change playbook status to active
Configuring Splunk

*Install Splunk ES App*

After logging into your Splunk instance, click on **Splunk Apps** and search for “enterprise security”.

Install the Splunk ES app.

![Splunk ES app screenshot](image)

**Figure 90. Splunk ES app**

![Search and install Splunk Enterprise Security screenshot](image)

**Figure 91. Search and install Splunk Enterprise Security**
**Manage Threat Intelligence within ES App**

Navigate to the newly installed **Enterprise Security** Splunk app and then click the **App Configuration** section as shown below.

*Figure 92. Splunk enterprise security*

*Figure 93. Splunk enterprise security app configuration*

Click on **Content Management**.

*Figure 94. Content management in Splunk ES*
Type “Threat” in the search box and select the **Type** as **Correlation Search**.

Enable the **Threat Activity Detected** correlation search as shown below.

**Figure 95. Threat activity search**

After enabling, click on “Threat Activity Detected” correlation search.

**Figure 96. Enable “Threat Activity Detected” correlation**

This brings you to following page.

**Figure 97. Correlation search**
**Notable Events and Forwarding to Phantom**

Once you scroll down to the bottom of this page, you will see the Notable and Risk Analysis option checked by default. Select the **Add New Response Action** button and add **Send to Phantom**.

*Figure 98. Add adaptive response action in Phantom*
Notable events are automatically created by Splunk ES based on correlation searches. Below, we add action to forward artifacts related to such events to your Phantom setup.

**Figure 99. Forward notable events to Phantom**

**Install Phantom App**

We need to install Phantom App on Splunk. Phantom IP is defined here and Splunk forwards artifacts to this Phantom instance.

**Install the Phantom App for Splunk.**
**Configure Automation User**

Configure username and authentication settings to establish communication between Splunk and Phantom.

Navigate to the newly installed Phantom Splunk App and then click **Create Server** section as shown below.

![Phantom Server Configuration](image)

**Figure 101. Phantom server configuration**

Populate the **Authorization Configuration** by pasting the **Authorization token** content we copied in earlier steps and click **Save**.

![New Phantom server credentials](image)

**Figure 102. New Phantom server credentials**
You should receive confirmation as shown below.

New Server Configuration

Splunk has added the server configuration.

Figure 103. Phantom server verification

Verify Events in Phantom

Log back into Phantom. You should start seeing events getting populated as shown below. It may take up to 30 min for events to show up. These events trigger the Phantom playbook.

Figure 104. Verify that the notable events are being forwarded by Splunk to Phantom
**Inspect Actions Taken by Phantom**

Clicking on any of these events brings up pertinent playbook runs. Playbook lists all the actions invoked with the success or failure status.

*Figure 105. Verify playbook runs and actions taken*
Appendix E: Requesting Zscaler Support

Gather Support Information

You might sometimes 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 > and then click Company profile.

![Company Profile](image)

*Figure 106. Collecting details to open support case with Zscaler TAC*

**Save Company ID**

Copy the Company ID, as shown below.
Figure 107. Company ID

**Enter Support Section**

Now that you have our company ID, you can open a support ticket. Navigate to Dashboard > Support > Submit a Ticket.
**Figure 108.** Submit ticket
## Appendix F: Revision History

<table>
<thead>
<tr>
<th>Name</th>
<th>Date</th>
<th>Status</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scott Bullock</td>
<td>20190609</td>
<td>Initial draft</td>
<td></td>
</tr>
<tr>
<td>Scott Bullock</td>
<td>20190701</td>
<td>Draft in Review</td>
<td></td>
</tr>
<tr>
<td>Scott Bullock</td>
<td>20190725</td>
<td>Released</td>
<td></td>
</tr>
<tr>
<td>Scott Bullock</td>
<td>20190910</td>
<td>Released</td>
<td>Cosmetic changes</td>
</tr>
<tr>
<td>BD Team</td>
<td>20191106</td>
<td>In review</td>
<td>Added Appendix A</td>
</tr>
<tr>
<td>Scott Bullock</td>
<td>20191114</td>
<td>In review</td>
<td>Added SC4S guidance</td>
</tr>
<tr>
<td>BD Team</td>
<td>20210418</td>
<td>In review</td>
<td>Added Appendix B</td>
</tr>
<tr>
<td>BD Team</td>
<td>20210628</td>
<td>In review</td>
<td>Added Appendix C</td>
</tr>
</tbody>
</table>