ZSCALER AND SPLUNK DEPLOYMENT GUIDE

JULY 2023, VERSION 1.4

BUSINESS DEVELOPMENT GUIDE

Contents

Terms and Acronyms 6

About This Document 7

- Zscaler Overview 7
- Splunk Overview 7
- Audience 7
- Software Versions 7
- Request for Comments 8

Zscaler and Splunk Introduction 9

- ZIA Overview 9
- ZPA Overview 9
- Zscaler Resources 10
- Splunk Cloud Overview 10
- Splunk SOAR Overview 10
- Splunk Resources 11

Application Architecture 12

- Data Models 12
- Zscaler Log Streams 13
  - Web and Tunnel Logs 13
  - Firewall and DNS Logs 14
  - Private Access Logs 14
- Zscaler APIs 15
  - Python SDK 15
  - Sandbox 16
  - Audit Logs 17

Zscaler Technical Add-on 18

- Source Types 18
- Macros 19
  - Splunk CIM 19
- Modular Inputs 19

Zscaler Splunk App 20
Dependencies 20
User Interface 20
Overview and Connections 20
Access Control 21
Threat Prevention 22
Private Access Overview 23
Private Access Health 23
Installation and Configuration 24
Zscaler Configuration 24
Output Strings 24
Splunk Configuration 26
Search Head 26
Forwarders (or Indexers) 26
Network Inputs 26
Modular Inputs 28
Macro Modification 29
Custom Field Mapping 29
Appendix A: Splunk Configs 30
Event Types, Tags, and Aliases 30
Appendix B: Splunk Essential Configuration (Using NSS VM—Stream Syslog Over TCP) 39
Configure Zscaler NSS 39
Add or Create Index 39
Log In to the Splunk Instance 39
Configure New Index in Splunk 40
Add Zscaler Index in Splunk 41
Create Data Inputs 42
Splunk Connect for Syslog 42
TCP Data Input 42
Select the Desired Zscaler Source Type 42
Change Default App Context and Default index 43
Verify Incoming Logs 44
Inspect Log Fields 44
Extracted Log Fields 45
Verify Splunk's Zscaler App 45

Appendix C: Splunk Essential Configuration (Using Cloud-to-Cloud Logging—HTTPS POST) 47

Configure Splunk Cloud to Ingest ZIA Logs Over HEC Input 47

Log In to Splunk Cloud Tenant 48
Install Zscaler App and Zscaler Technical Add-On in Your Cloud Tenant 48
Create Zscaler Index in Splunk 49
Add Zscaler Index in Splunk 49
Create a new Data Input and HEC token 50
Configure Data Input and HEC token 51
Copy the HEC Token Value 54
Determine the Splunk Cloud API Endpoint to Send Logs To 55

Configure Splunk Cloud to Fetch Zscaler Audit Logs and Sandbox Events 56

Log In to Splunk IDM Instance 56
Install Zscaler Splunk Technical Add-On on Splunk IDM Instance 57
Configure Zscaler Index on Splunk IDM Instance 58
Add Zscaler Account Used by Splunk IDM to Make API Calls to ZIA 58
Configure Input for Audit Logs 59
Fill in the Settings for Fetching ZIA Audit Logs 60
Configure Input for Sandbox Events 60
Fill in the Settings for Fetching ZIA Sandbox Events 61
Confirm that Both Input Settings are Saved and Enabled 61
Configure Zscaler for Cloud-to-Cloud Logging 61
Go to Cloud-to-Cloud Logging Section in ZIA Portal 62
Set Up the Cloud NSS Log Feed (Web) 62
Set Up the Cloud NSS Log Feed (Firewall) 65
Add Other Log Source Types 66
Validate NSS Cloud Configuration 67
Verify Zscaler Splunk App 68

Appendix D: Using SOAR with Zscaler and Splunk 69

SOAR Components 69

A Sample Playbook to Showcase Zscaler and SOAR Integration 69

Configuring SOAR 71

Create New Event Label in SOAR 71
Create Automation User in SOAR 72
Installing Zscaler App on SOAR 73
Search for Zscaler App 73
Configure Zscaler App 74

Test Connectivity Between SOAR and Zscaler 75
Installing Splunk App on SOAR 76
Search for Splunk App 76
Configure Splunk App 77
Test Connectivity Between SOAR and Splunk 79
Download Zscaler Playbook 79
Edit the Playbook Settings 80
Configuring Splunk 81
Install Splunk ES App 81
Manage Threat Intelligence Within ES App 82
Notable Events and Forwarding to SOAR 84
Install SOAR App 86
Configure Automation User 87
Verify Events in SOAR 88
Inspect Actions Taken by SOAR 89
Appendix E: Posture Control and Splunk 90
Create AWS S3 Bucket 90
Configuring ZPC to Send Alerts to AWS S3 91
Configuring AWS 93
Configuring Splunk 96
Appendix F: Requesting Zscaler Support 99

Terms and Acronyms

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

Acronym	Definition
API	Application Programming Interface
CA	Central Authority (Zscaler)
CIM	Common Information Model (Splunk-defined data model)
CSV	Comma-Separated Values
DLP	Data Loss Prevention
DNS	Domain Name Service
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
LSS	Log Streaming Service
NSS	Nanolog Streaming Service
NOC	Network Operations Centre
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SaaS	Software as a Service
SDK	Software Development Kit
SIEM	Security Incident and Event Management
SOAR	Security Orchestration and Automation
SOC	Security Operations Centre
SSL	Secure Socket Layer (RFC6101)
TCP Input	Method of ingesting data in Splunk via TCP datagrams
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
XFF	X-Forwarded-For (RFC7239)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

About This Document

The following sections describe the organizations and requirements for the integration covered by this deployment guide.

Zscaler Overview

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

Splunk Overview

Splunk (NASDAQ: 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. You can then use this information to enrich other data sources and generate interesting events related to business services and technology operations. To learn more, refer to Splunk's website.

Audience

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

Notice that appendices are provided for those needing a foundational exposure to Splunk and NSS as it relates to this integration. For additional product and company resources, see:

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

Software Versions

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

Request for Comments

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

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

- Email: splunk-support@zscaler.com
- From the ZIA Admin Portal, go to Zscaler Community Products and email Cloud Reporting and Management.

Zscaler and Splunk Introduction

The Zscaler and Splunk applications are described in this section. Zscaler and Splunk share a large joint customer base where the two technologies interact, and our companies have a mutual partnership. In order to ease integration of Zscaler capabilities into your environments, Zscaler has developed a *Splunk App*, which simplifies the ingestion of Zscaler-generated data into the Splunk platform. This Splunk App makes the overall integration process between our technologies more accessible for our joint customers.

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

ZIA Overview

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of 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, and Isolation, allowing you start with the services you need now and activate others as your needs grow.

ZPA Overview

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

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

Zscaler Resources

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

Name and Link	Description
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
ZPA Access Policies	Help link for how to configure ZPA access policies with a set of configuration examples.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

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

Name and Link	Description
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
ZPA Access Policies	Help link for how to configure ZPA access policies with a set of configuration examples.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

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 allowlist 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 cloud customer base. 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, you can ensure your Operational Contacts are kept up-to-date.

Splunk SOAR Overview

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

Splunk Resources

The following table contains links to Splunk support resources.

Name and Link	Description
Splunk Documentation	Splunk platform online documentation.
Splunk Cloud help	Splunk Cloud online help articles.
Splunk SOAR help	Splunk SOAR online help articles.
Splunk Common Information Model (CIM)	Description of Splunk's CIM.
SOAR Demonstration	Video demonstration of Splunk's SOAR capabilities and uses.
Splunk and Zscaler partner page	Splunk's Zscaler partner page.

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 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 consists of log streams generated from customer environments, and can also retrieve data using Zscaler APIs. The following diagram shows these various interfaces.

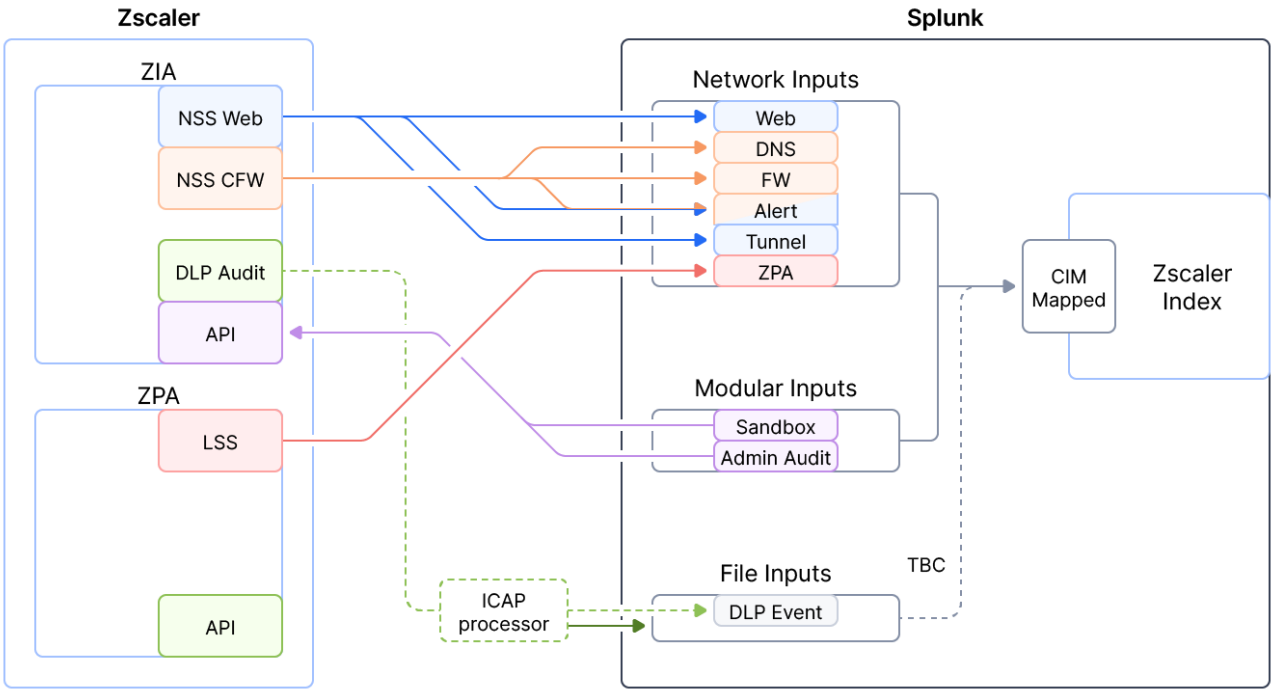

Figure 1. Application architecture

The interfaces are detailed in the following sections.

Data Models

Zscaler and Splunk joint customers require Zscaler logging data to be in a format that is 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 that are relevant to specific CIM data models.

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 following table describes the various log streams.

Log Type	Streaming Technology	Platforms
Proxy	NSS - Web	VMware, AWS, and Azure
Tunnel	NSS - Web	VMware, AWS, and Azure
Firewall	NSS - CWF	VMware, AWS, and Azure
DNS	NSS - CWF	VMware, AWS, and Azure
Alert	NSS – CWF/Web	VMware, AWS, and Azure
App Auth	LSS	RedHat-compatible
App Access	LSS	RedHat-compatible
Browser Access	LSS	RedHat-compatible
Proxy	NSS - Web	VMware, AWS, and Azure

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

For more information, see the following:

- NSS Feed Output Format: Web Logs (government agencies, see NSS Feed Output Format: Web Logs).
- Adding NSS Feeds for Tunnel Logs (government agencies, see Adding NSS Feeds for Tunnel Logs).
- Adding NSS Feeds for Alerts (government agencies, see Adding NSS Feeds for Alerts).

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

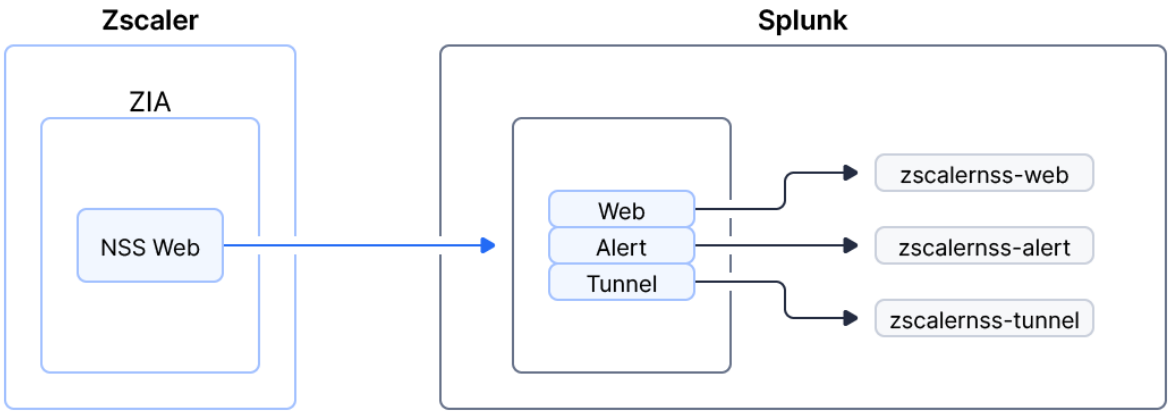

Figure 2. Zscaler NSS web and tunnel data in Splunk

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, see:

- NSS Feed Output Format: Firewall Logs (government agencies, see NSS Feed Output Format: Firewall Logs).
- NSS Feed Output Format: DNS Logs (government agencies, see NSS Feed Output Format: DNS Logs).
- Adding NSS Feeds for Alerts (government agencies, see Adding NSS Feeds for Alerts).

These log streams have a dedicated Splunk event type, detailed in the Source Types section.

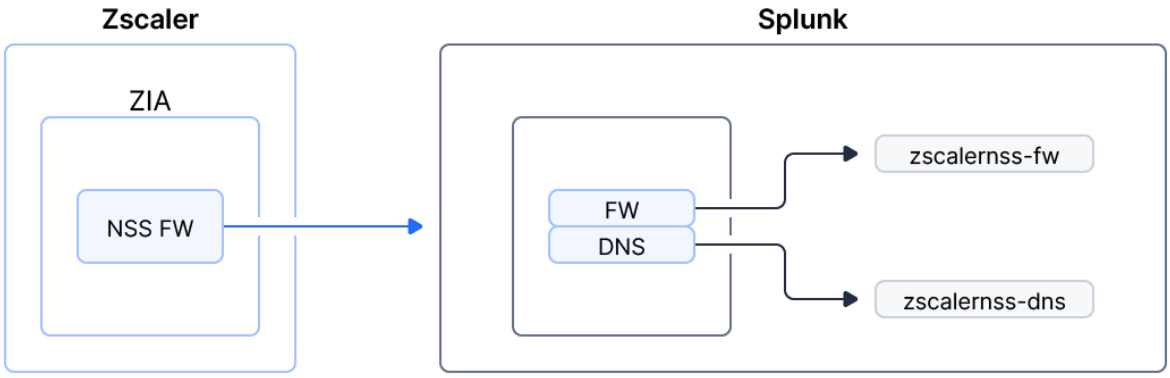

Figure 3. Zscaler NSS firewall and DNS data in Splunk

Private Access Logs

Log formats expected by Splunk are JSON. You can find the default log string format from the drop-down menu in the Logging section of the ZPA Admin Portal. ZPA has the following log types:

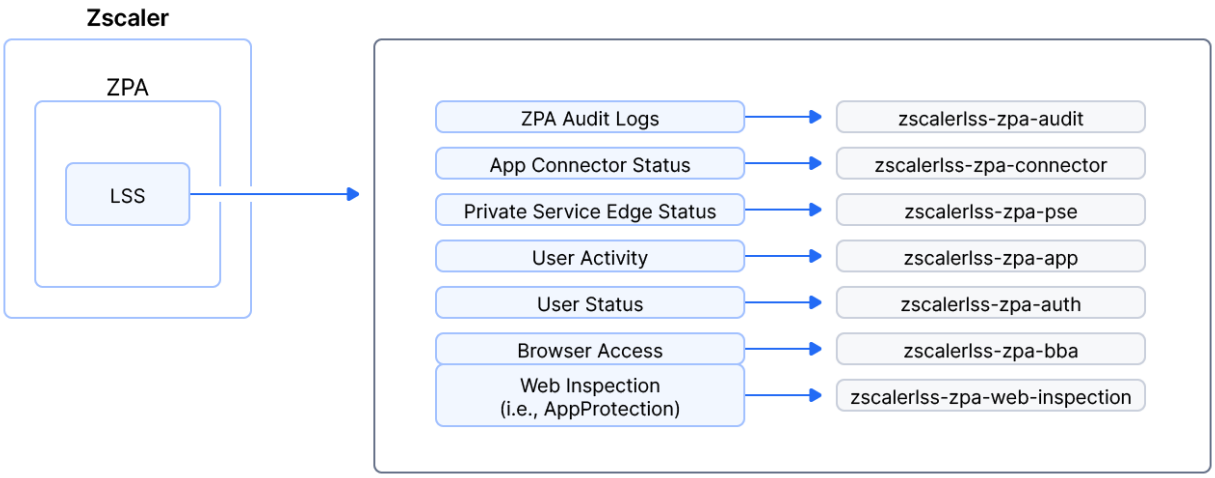

Figure 4. Zscaler LSS ZPA data in Splunk

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 ZIA Admin audit logs. Full specifications for the Zscaler API are found in the API Reference (government agencies, see API Reference).

Splunk makes use of these APIs via Splunk modular inputs. Both Sandbox and audit logs have dedicated Splunk event types and are detailed in the Source Types section.

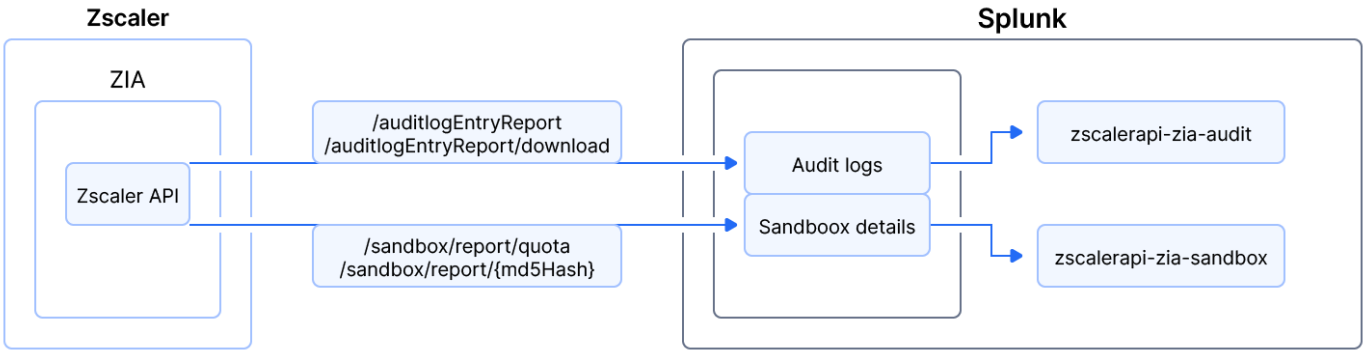

Figure 5. Zscaler APIs used by Splunk modular inputs

SOAR 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 is located at the Zscaler Python SDK GitHub repository.

The raw scripts and SDK are 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 are found in Configuring the Sandbox Policy (government agencies, see Configuring the Sandbox Policy).

Sandbox detonation results are significant to customers because a malicious verdict indicates a possibly compromised user or risky user behavior that could jeopardize business. As such, Zscaler offers full Sandbox reporting as 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.

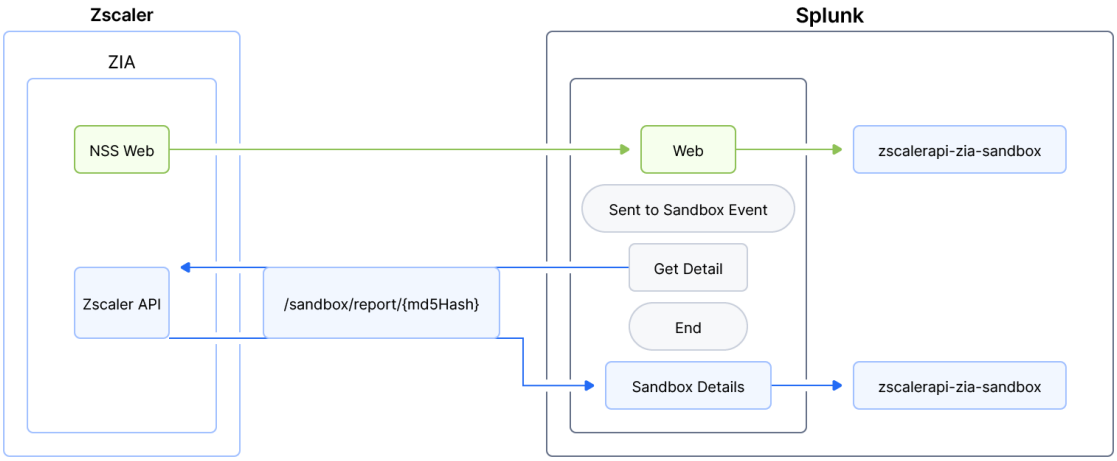

Figure 6. How Sandbox modular input works

The following image sows the Zscaler sandbox.

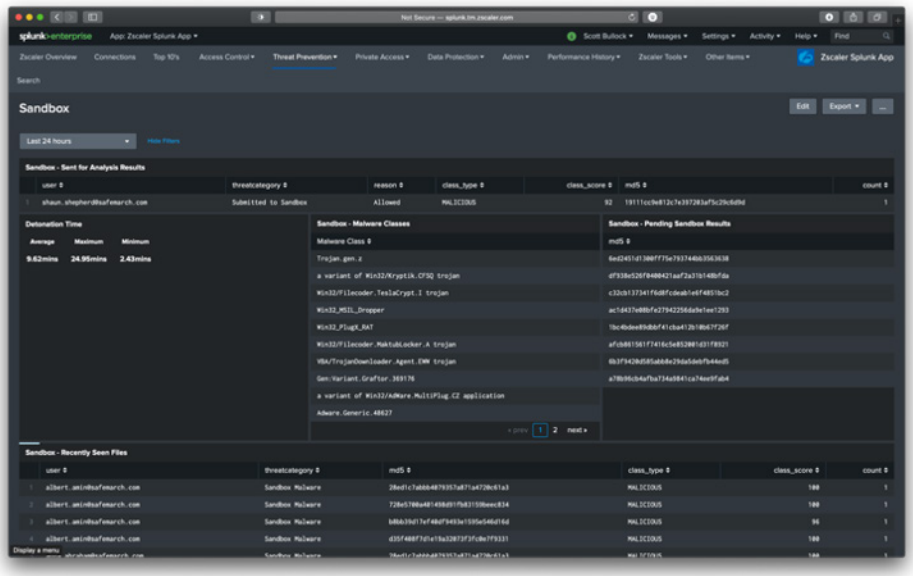

Figure 7. Zscaler Sandbox data in Splunk

It's possible that Splunk ES can find a notable event and generate a response action and engage a SOAR platform such as Splunk > SOAR via correlation. Note that SOAR has existing read and write integrations to Zscaler API, however, details of these integrations are not in scope for this document.

Audit Logs

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

When 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.

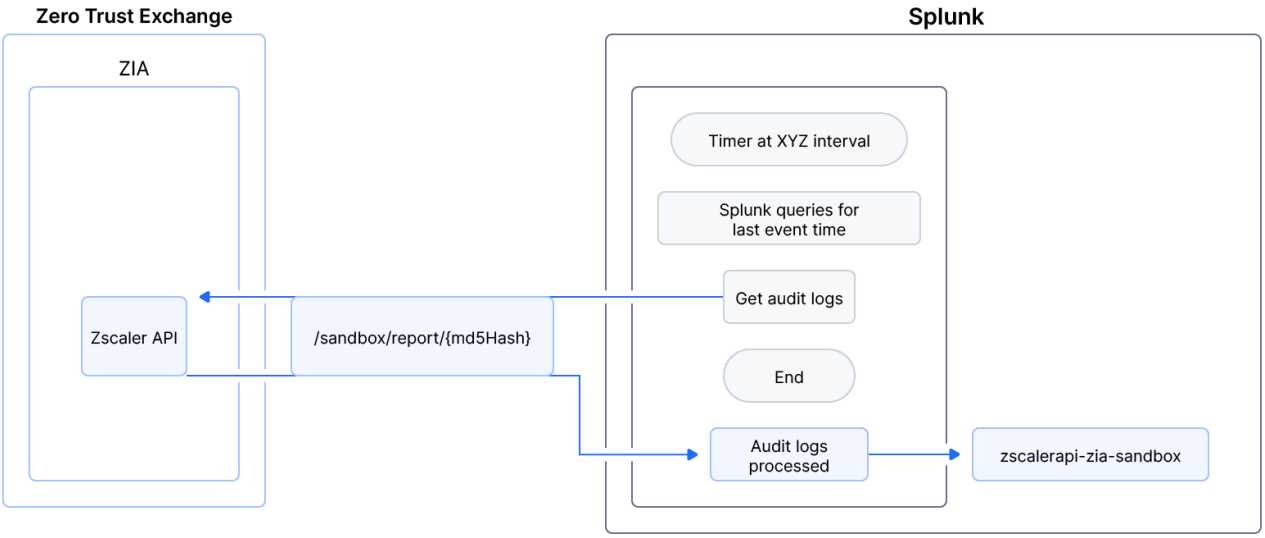

Figure 8. How audit logs modular input works

The following image shows the Zscaler audit logs.

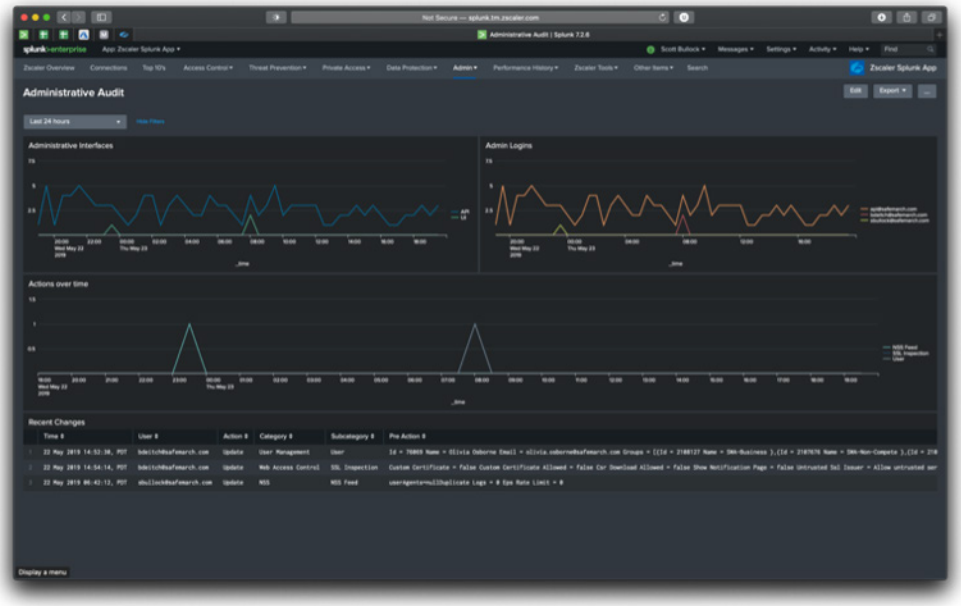

Figure 9. Zscaler audit logs in Splunk

Zscaler Technical Add-on

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

You can download the Zscaler Technical Add-On from the Splunk Base.

Source Types

The following source types are defined in the Zscaler Technical Add-On, and cover the current possible inputs. Actual use of the source types might vary depending on the bundle and features to which the Zscaler customer subscribed.

There are no preconfigured data inputs. The Splunk Admin must configure data inputs according to the Network Inputs and Modular Inputs sections. Splunk's best practice is to not permit the definition of network inputs in a Splunk app.

Source Type	Function	Stream Format
zscalernss-web	ZIA Proxy Logs	Splunk CIM
zscalernss-tunnel	ZIA Tunnel Logs–up or down events and aggregate traffic stats	Name Value Pairs
zscalernss-fw	ZIA Firewall Logs	Name Value Pairs
zscalernss-dns	ZIA DNS Logs	Name Value Pairs
zscalernss-alerts	VM-related Alerts from Zscaler NSS VM	(not applicable)
zscalerlss-zpa-audit	ZPA Audit Logs	JSON
zscalerlss-zpa-connector	App Connector Status Logs	JSON
zscalerlss-zpa-pse	Private Service Edge Status Logs	JSON
zscalerlss-zpa-app	User Activity Log	JSON
zscalerlss-zpa-auth	User Status Log	JSON
zscalerlss-zpa-bba	Browser Access Logs	JSON
zscalerlss-zpa-web-inspection	Web Inspection (i.e., AppProtection logs)	JSON
zscalerapi-zia-audit	ZIA Administrative Audit Logs	API
zscalerapi-zia-sandbox	ZIA detailed Sandbox Logs (detonation)	API
zscalernss-audit	Zscaler NSS Admin Logs via streaming (not API)	JSON

Macros

Splunk macros are used to shortcut frequently used sets of search commands. The Technical Add-On defines several search macros to:

- Ease dashboard creation and the underlying reports.
- Create a simple configuration point to a customer's specific Zscaler data index.

The search macros are defined in the Zscaler Technical Add-On, and are used extensively throughout the Zscaler Technical 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
- DLP and Incident

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 are called if there is a need to ingest logs from multiple Zscaler tenants.

The modular inputs are written in Python and are engineered for compatibility 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 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.

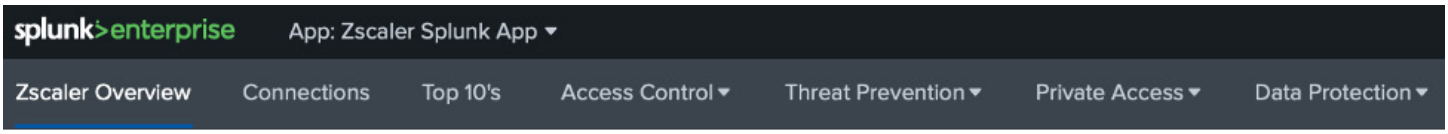

Figure 10. Splunk app menu

You can download the app from the Splunk Base.

Dependencies

The Zscaler Splunk App is dependent on Zscaler's Technical Add-On (mandatory).

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. The following is 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

The following image shows the Zscaler overview in Splunk.

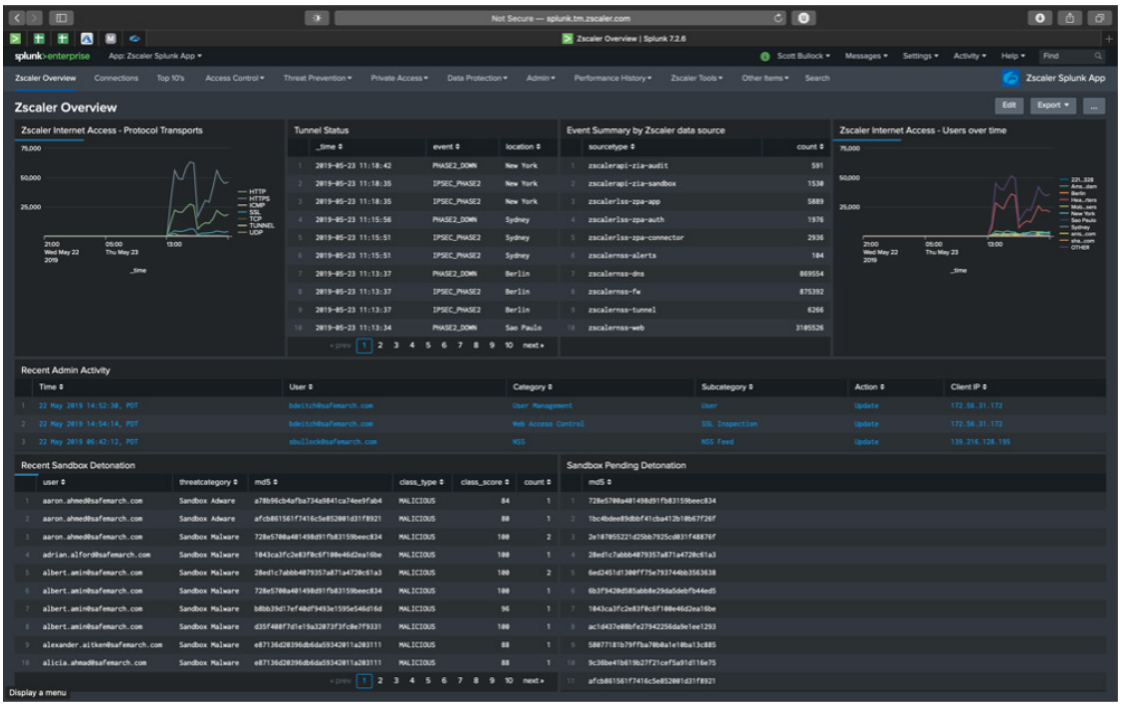

Figure 11. Zscaler overview in Splunk

Access Control

The following image shows the Zscaler Bandwidth report.

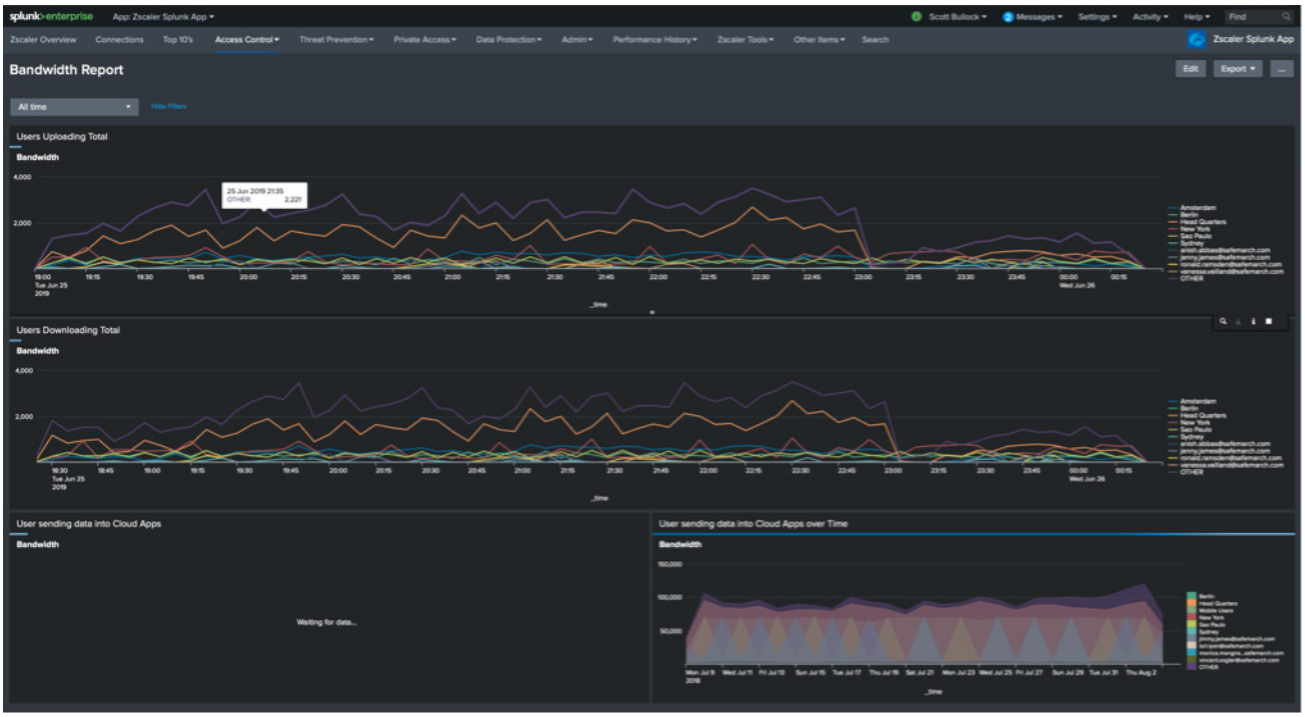

Figure 12. Bandwidth Report

The following image shows the Zscaler Web Access controls.

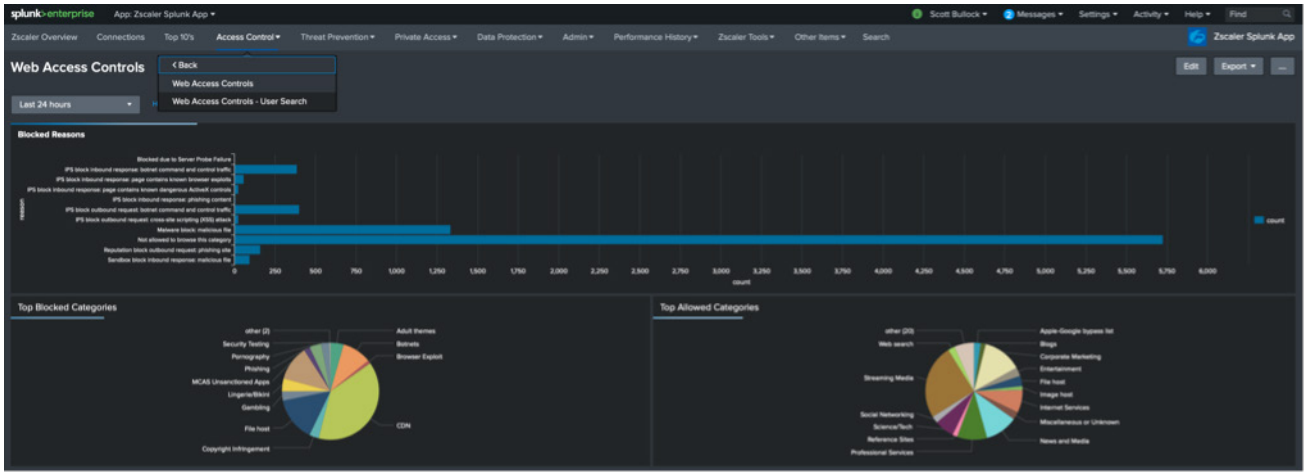

Figure 13. Web Access Controls

Threat Prevention

The following image shows the Threat Prevention overview.

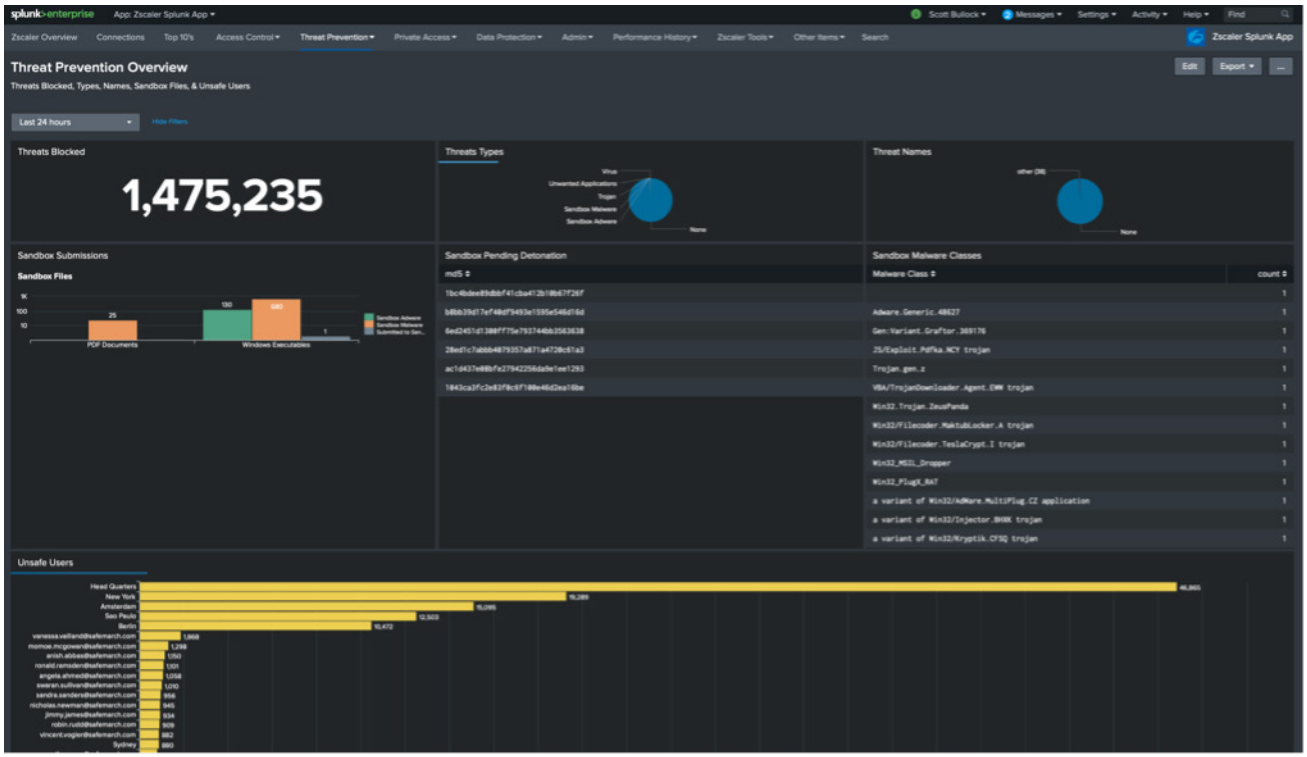

Figure 14. Threat Prevention overview

The following image shows the Zscaler sandbox.

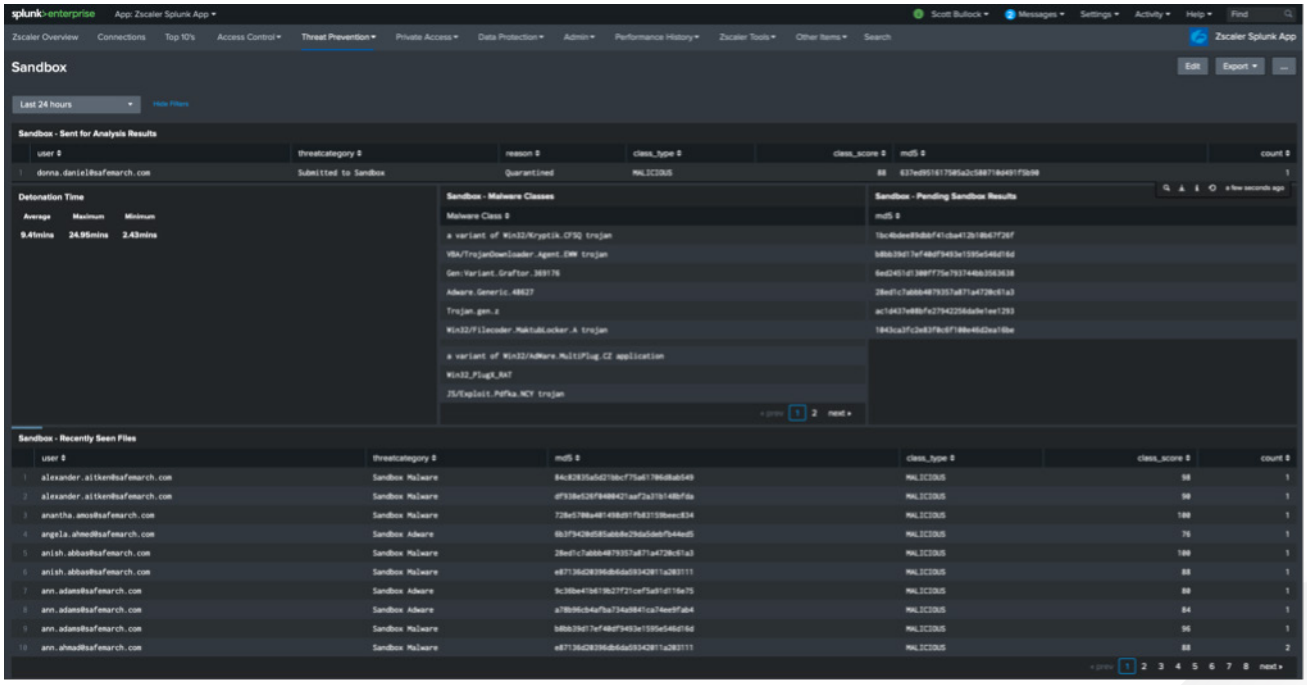

Figure 15. Sandbox

Private Access Overview

The following image shows the Private Access overview.

Figure 16. Private Access overview

Private Access Health

The following image shows the Private Access health.

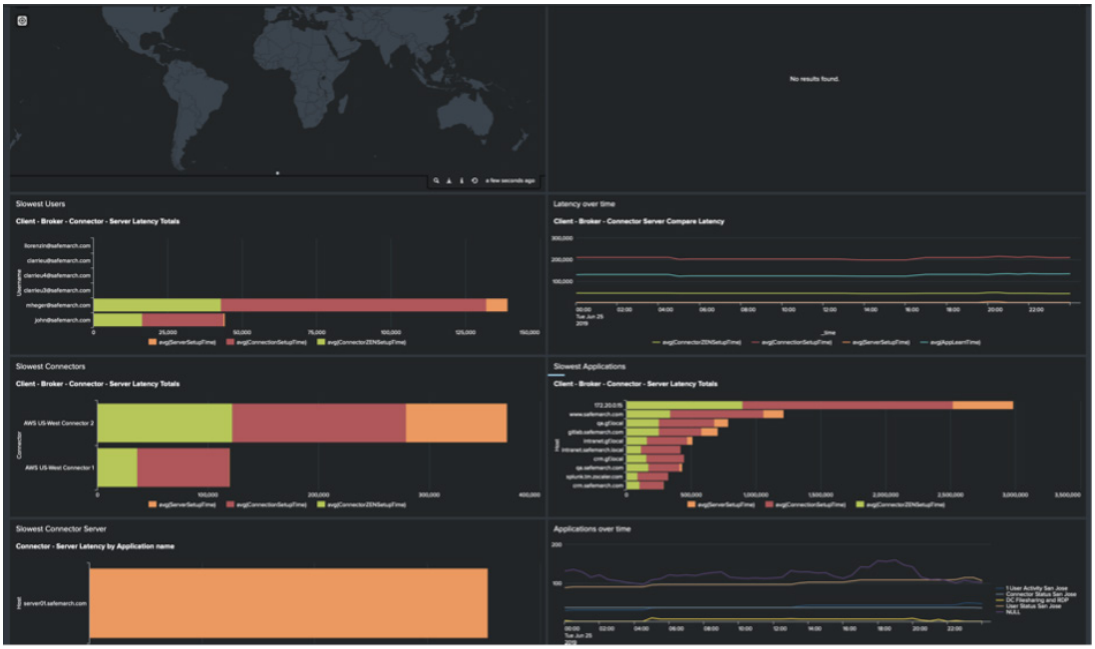

Figure 17. Private Access health

Installation and Configuration

The following sections describe how to configure the Zscaler and Splunk integration.

Zscaler Configuration

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

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

Output Strings

If you copy and paste the following outputs, remove any spaces between the fields when configuring an NSS feed in the ZIA Admin Portal. Removing all spaces allows you to save your NSS feed configuration successfully.

The Splunk App uses fields not included in the base output fields. Configure each of your LSS and NSS feeds as follows:

NSS Web

```
%d{yy}-%02d{mth}-%02d{dd}-%02d{hh}:%02d{mm}:%02d{ss}\treason=%s{reason}\
tevent_id=%d{recordid}\tmd5=%s{bamd5}\tprotocol=%s{proto}\taction=%s{action}\
ttransactionsize=%d{totalsize}\tresponsesize=%d{respsize}\trequestsize=%d{reqsize}\
turlcategory=%s{urlcat}\tserverip=%s{sip}\tclienttranstime=%d{ctime}\
trequestmethod=%s{reqmethod}\trefererURL=%s{ereferer}\tuseragent=%s{ua}\tproduct=NSS\
tlocation=%s{location}\tClientIP=%s{cip}\tstatus=%s{respcode}\tuser=%s{login}\
turl=%s{eurl}\tvendor=Zscaler\thostname=%s{ehost}\tclientpublicIP=%s{cintip}\
tthreatcategory=%s{malwarecat}\tthreatname=%s{threatname}\tfiletype=%s{filetype}\
tappname=%s{appname}\tpagerisk=%d{riskscore}\tdepartment=%s{dept}\turlsup
ercategory=%s{urlsupercat}\tappclass=%s{appclass}\tdlpengine=%s{dlpeng}\
tssldecrypted=%s{ssldecrypted}\turlclass=%s{urlclass}\tthreatclass=%s{malwareclass}\
tdlpdictionaries=%s{dlpdict}\tfileclass=%s{fileclass}\tbwthrottle=%s{bwthrottle}\
tservertranstime=%d{stime}\tcontenttype=%s{contenttype}\tunscannabletype=%s{unscannabl
etype}\tdevicehostname=%s{devicehostname}\tdeviceowner=%s{deviceowner}\n
```

NSS Tunnel Sample

```
%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}\recordid=%d{recordid}\n
```

IKE Phase 1

```
%s{datetime}\tRecordtype=%s{tunnelactionname}\ttunneltype=IPSEC_IKEV %d{ikeversion}\
tuser=%s{vpncredentialname}\tlocation=%s{locationname}\tsourceip=%s{sourceip}\
tdestinationip=%s{destvip}\tsourceport=%d{srcport}\tdestinationport=%d{dstport}\
tlifetime=%d{lifetime}\tikeversion=%d{ikeversion}\tspi_in=%lu{spi_in}\tspi_out=%lu{spi_
out}\talgo=%s{algo}\tauthentication=%s{authentication}\tauthtype=%s{authtype}\
recordid=%d{recordid}\n
```


IKE Phase 2

```
%s{datetime}\tRecordtype=%s{tunnelactionname}\ttunneltype=IPSEC_IKEV
%d{ikeversion}\tuser=%s{vpncredentialname}\tlocation=%s{locationname}\
tsourceip=%s{sourceip}\tdestinationip=%s{destvip}\tsourceport=%d{srcport}\
tsourceportstart=%d{srcportstart}\tdestinationportstart=%d{destportstart}\
tsrcipstart=%s{srcipstart}\tsrcipend=%s{srcipend}\tdestinationipstart=%s{destipstart}\
tdestinationipend=%s{destipend}\tlifetime=%d{lifetime}\tikeversion=%d{ikeversion}\
tlifebytes=%d{lifebytes}\tspi=%d{spi}\talgo=%s{algo}\tauthentication=%s{authentic
ation}\tauthtype=%s{authtype}\tprotocol=%s{protocol}\ttunnelprotocol=%s{tunnelpro
tocol}\tpolicydirection=%s{policydirection}\recordid=%d{recordid}\n
```

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}\recordid=%d{recordid}\n
```

NSS CFW

```
datetime=%s{time}\tuser=%s{login}\tdepartment=%s{dept}\tlocationname=%s{location}\
tcdport=%d{cdport}\tcsport=%d{csport}\tsdport=%d{sdport}\tssport=%d{ssport}\
tcsip=%s{csip}\tcdip=%s{cdip}\tssip=%s{ssip}\tsdip=%s{sdip}\ttsip=%s{tsip}\
ttunsport=%d{tsport}\ttuntype=%s{ttype}\taction=%s{action}\tdnat=%s{dnat}\
tstateful=%s{stateful}\taggregate=%s{aggregate}\tnwsvc=%s{nwsvc}\tnwapp=%s{nwapp}\
tproto=%s{ipproto}\tipcat=%s{ipcat}\tdestcountry=%s{destcountry}\
tavgduration=%d{avgduration}\trulelabel=%s{rulelabel}\tinbytes=%ld{inbytes}\
toutbytes=%ld{outbytes}\tduration=%d{duration}\tdurationms=%d{durationms}\
tnumsessions=%d{numsessions}\tipsrulelabel=%s{ipsrulelabel}\tthreatcat=%s{threatcat}\
tthreatname=%s{threatname}\tdeviceowner=%s{deviceowner}\tdevicehostname=%s{devicehostna
me}\n
```

NSS DNS

```
datetime=%s{time}\tuser=%s{login}\tdepartment=%s{dept}\tlocation=%s{location}\
treqaction=%s{reqaction}\tresaction=%s{resaction}\treqrulelabel=%s{reqrulelabel}\
tresrulelabel=%s{resrulelabel}\tdns_reqtype=%s{reqtype}\tdns_req=%s{req}\tdns_
resp=%s{res}\tsrv_dport=%d{sport}\tdurationms=%d{durationms}\tclt_sip=%s{cip}\tsrv_
dip=%s{sip}\tcategory=%s{domcat}\tdeviceowner=%s{deviceowner}\tdevicehostname=%s{device
hostname}\nNSS Alert
```

Admin Audit

```
\{ "sourcetype" : "zscalernss-audit", "event" :\{"time":"%s{time}","recordid":"%d{re
cordid}","action":"%s{action}","category":"%s{category}","subcategory":"%s{subcatego
ry}","resource":"%s{resource}","interface":"%s{interface}","adminid":"%s{adminid}","
clientip":"%s{clientip}","result":"%s{result}","errorcode":"%s{errorcode}","auditlo
gtype":"%s{auditlogtype}","preaction":%s{preaction},"postaction":%s{postaction}\}\}
```

All ZPA (LSS) logs

All ZPA log types use default JSON drop-down log format available in the Logging section of the ZPA Admin Portal.

Splunk Configuration

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

Search Head

You can install the Zscaler Splunk App 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, install the Zscaler Technical Add-On on a search head because 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 source types (the receivers of NSS and LSS streams).

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

- You can download the App and Technical Add-On 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. Splunk typically uses TCP inputs and, if using cloud NSS, can be an HTTP Event Collector (HEC).

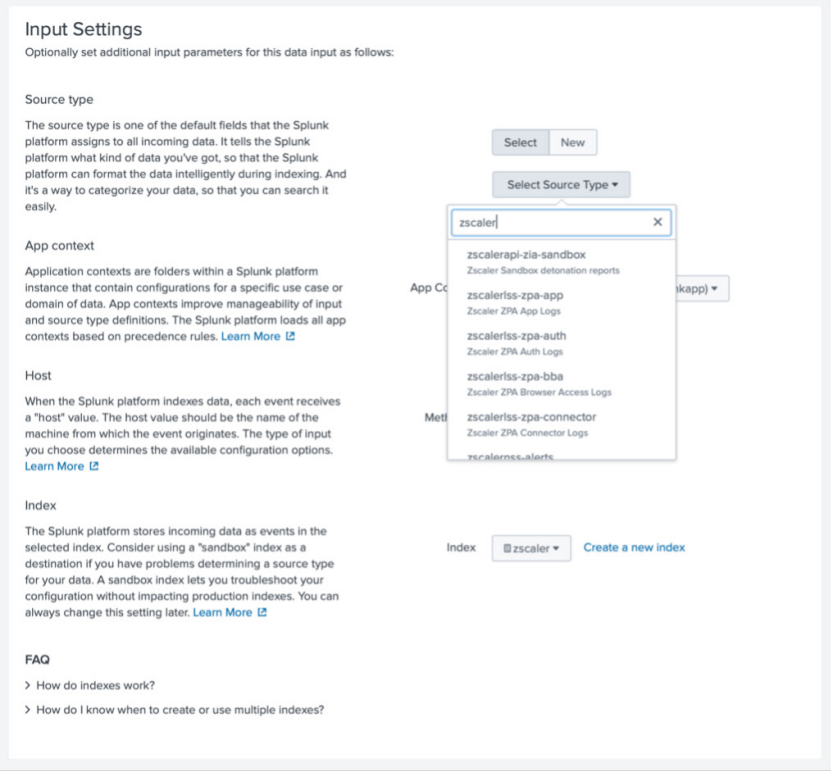

Figure 18. Example Splunk TCP inputs

Example Configuration

The following image shows the Splunk TCP inputs example.

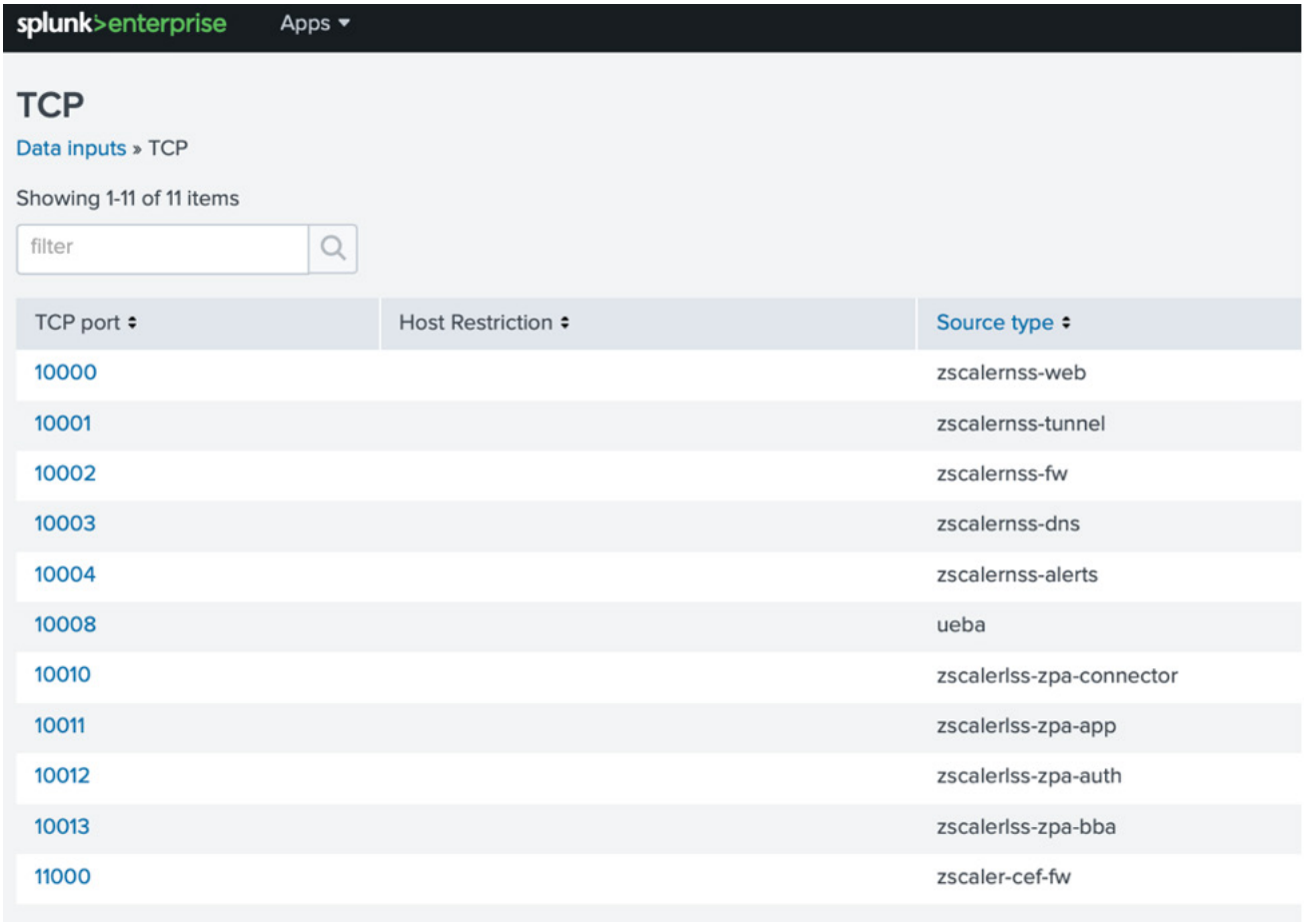

Figure 19. Example Splunk TCP inputs

Note the UEBA 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 Technical Add-On's setup page, and there is a specific configuration for each input type. Splunk best practice uses a Global Account for the API user, password, and key, and a setup screen when adding each input.

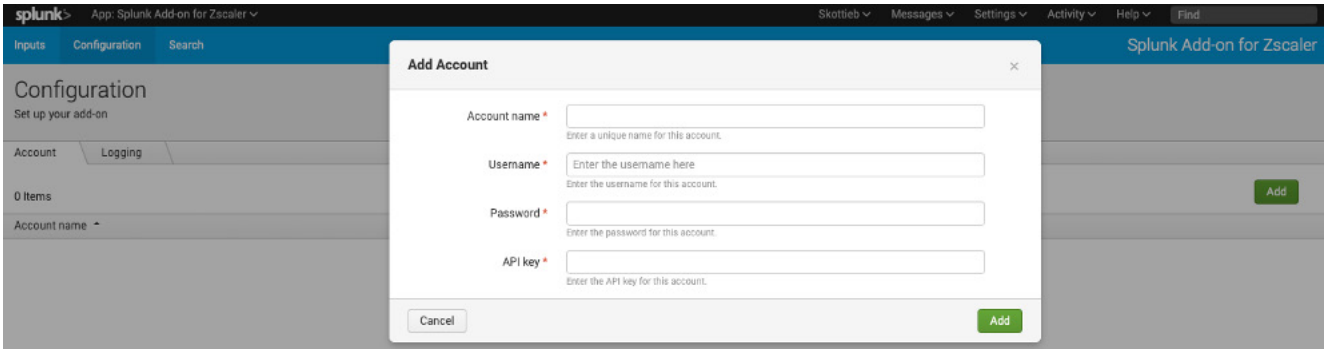

Figure 20. Adding a global account

The following image shows a modular input configuration example.

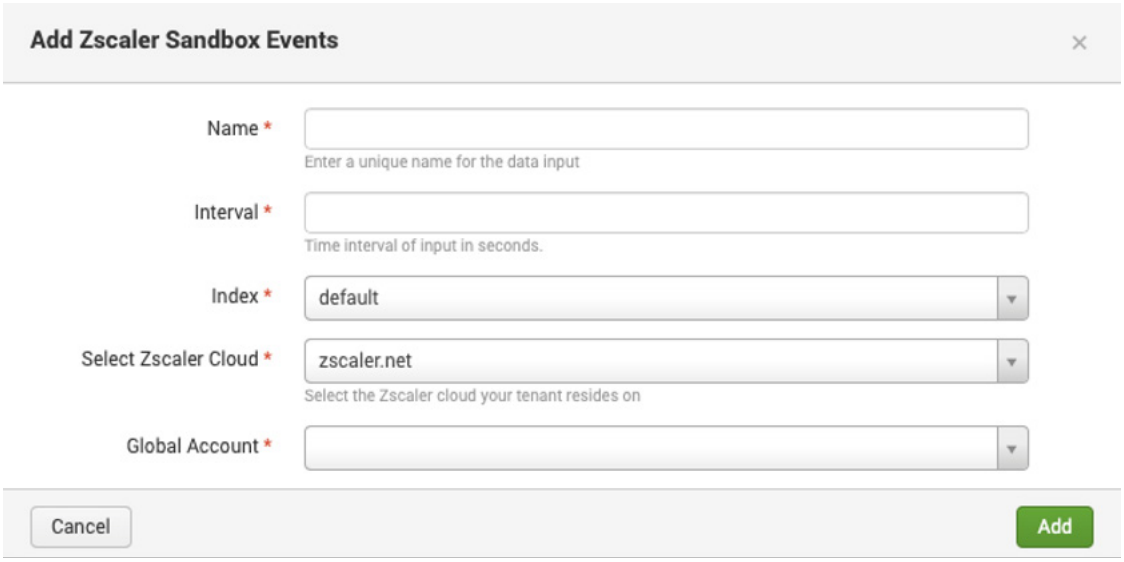

Figure 21. Modular input configuration example (Sandbox)

Take care when defining the interval that you stay within your API rate limits. For more information, see API Rate Limit Summary (government agencies, see API Rate Limit Summary)

Macro Modification

Your pre-existing Splunk environment might use an index name different to what Zscaler's Splunk App and Technical Add-On expect. In this case, modify `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="zscalernss-dns"
```

Figure 22. Macro modification example

Custom Field Mapping

The Zscaler Splunk App and Technical Add-On look for field names as shown in Output Strings. If you use different field names, you or the Splunk admin must:

1. Change your Zscaler log stream configurations to match what the app is expecting.
2. Define local field aliases to align to what the app is expecting.

Appendix A: Splunk Configs

Event Types, Tags, and Aliases

The following image shows the `eventtypes.conf` file.

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

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

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

[Zscaler_Proxy_DLP]
search = (sourcetype=zscalernss-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="zscalernss-web" threatname!="None")

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

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

Figure 23. eventtypes.conf

The following image shows the `tags.conf` file.

```
dns = enabled
network = enabled
resolution = enabled

[eventtype=Zscaler_CFW]
communicate = enabled
network = enabled
[eventtype=Zscaler_Proxy_General]
communicate = enabled
end = 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]
dlp = enabled
incident = enabled

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

Figure 24. tags.conf

The following image shows the `props.conf` file.

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

[zscalernss-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

[zscalernss-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-refererURL_as_http_referrer = refererURL AS http_referrer
FIELDALIAS-requestmethod_as_http_method = requestmethod AS http_method
FIELDALIAS-requestsize_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_zscalerlss_zpa_connector_alias_4 = Host AS dest
SHOULD_LINEMERGE = 0
category = Network & Security
description = Zscaler ZPA Connector Logs
pulldown_type = 1

[zscalernss-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_cert = "Full Details.FileProperties.DigitalCerificate" AS file_cert
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 25. props.conf

The following image shows the `moacros.conf` file.

```
[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="zscalerapi-zia-sandbox"
iseval = 0

[z-audit]
definition = index=zscaler sourcetype="zscalerapi-zia-audit"
iseval = 0

[z-index]
```



```
definition = index=zscaler
iseval = 0

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

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

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

[z-zpa-con]
definition = index=zscaler sourcetype="zscalerlss-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 26. 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 plain text TCP.

Configure Zscaler NSS

Zscaler configuration guides are available at the following links. For more information, see Understanding Nanolog Streaming Service (government agencies, see Understanding Nanolog Streaming Service).

Deploy NSS

- NSS Deployment Guide for Microsoft Azure (government agencies, see NSS Deployment Guide for Microsoft Azure).
- NSS Deployment Guide for Amazon Web Services (government agencies, see NSS Deployment Guide for Amazon Web Services).
- NSS Deployment Guide for VMWare vSphere (government agencies, see NSS Deployment Guide for VMWare vSphere).
- Configuring Advanced NSS Settings (government agencies, see Configuring Advanced NSS Settings).
- Troubleshooting Deployed NSS Servers (government agencies, see Troubleshooting Deployed NSS Servers).

Add NSS Feeds

- Adding NSS Feeds (government agencies, see Adding NSS Feeds).

Add or Create Index

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

Log In to the Splunk Instance

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

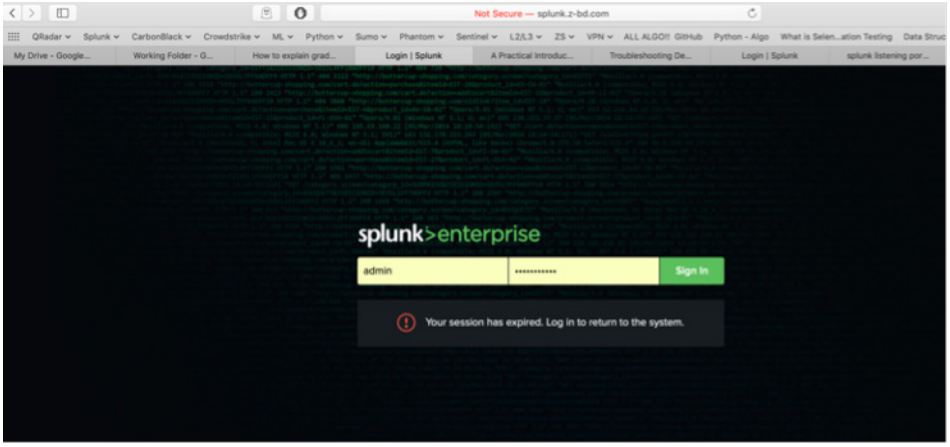

Figure 27. Log in to Splunk

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.

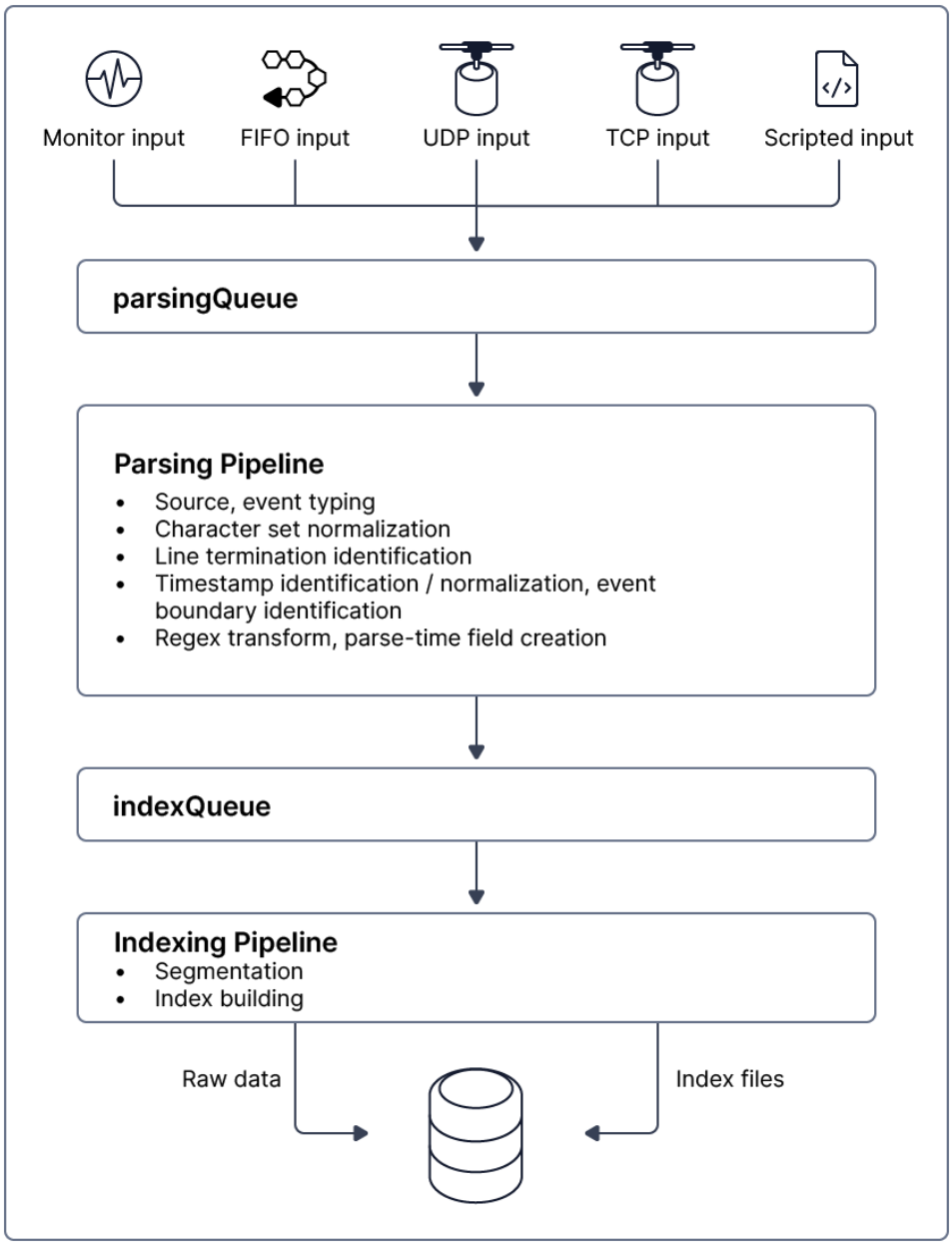

Figure 28. Log flow pipeline

After logging in to Splunk, go to **Settings** > **Indexes** > **New Index**.

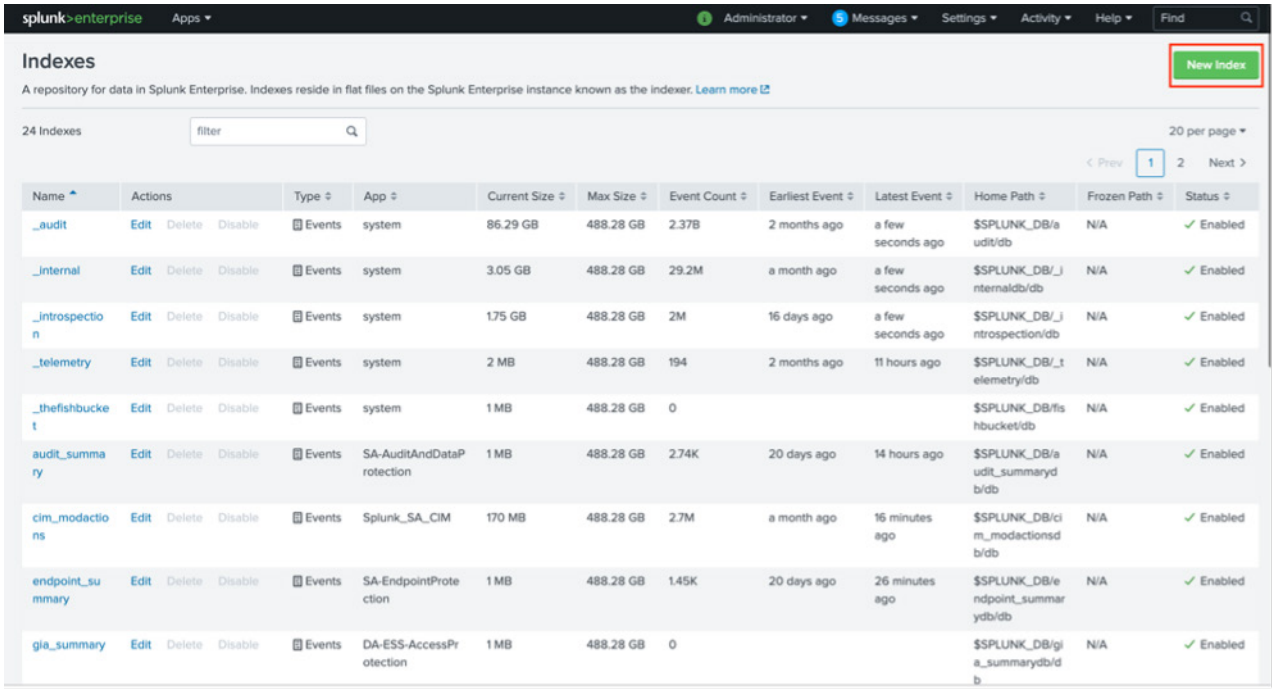

Figure 29. View indexes

Add Zscaler Index in Splunk

Zscaler creates an index titled *zscaler*. Because the Splunk App for Zscaler looks for data written at index *zscaler* by default, setting *index=zscaler* allows you to use the Splunk App for Zscaler out-of-the-box.

In the **New Index** dialog, enter `zscaler` without quotes (case sensitive) and click **Save**.

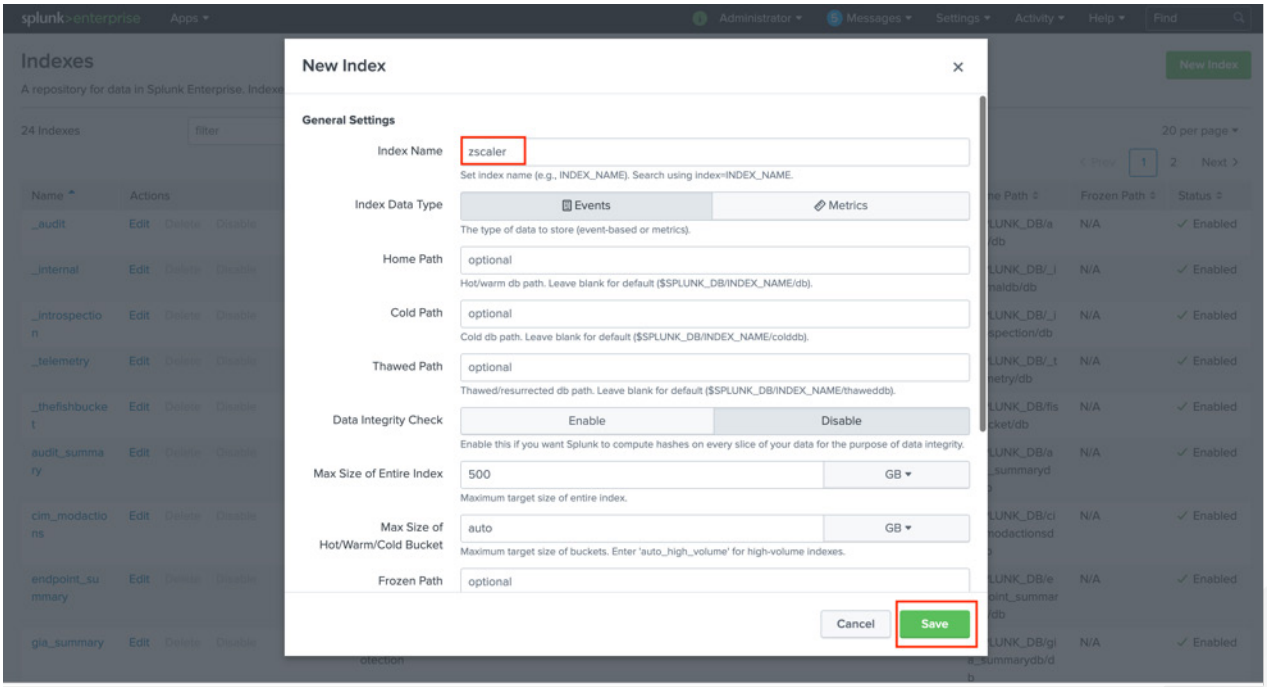

Figure 30. Add Zscaler index in Splunk

Create Data Inputs

Splunk Connect for Syslog

Syslog is Splunk's preferred method of ingesting high volumes of data. For more information, refer to Splunk Connect for Syslog!

TCP Data Input

1. Go to **Settings** > **Data Inputs** > **TCP (Add new)**.

   The Add Data wizard is displayed. This step configures Splunk to listen on TCP using port 514. NSS supports only TCP, but you can configure the destination port. Most administrators use port 514 as it is the default port for UDP-based syslog.

2. Configure the SIEM port, then click **Next**.

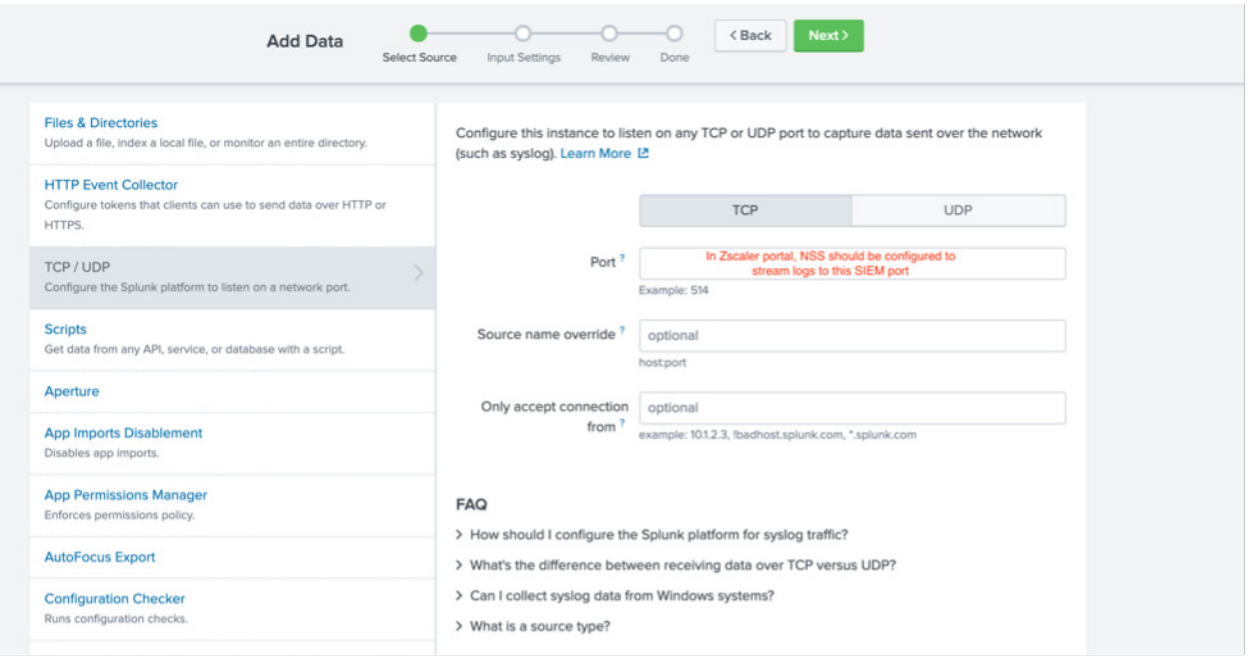

Figure 31. Configure new TCP input

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 is 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 because you can use Splunk search to display all data of a certain source type.

For example, Windows event logs, NSS web logs, and NSS Firewall logs are all source types.

If multiple web NSS servers send logs to the same Splunk instance, the servers all belong to the same source type, but each one of these servers constitute an independent source.

Splunk apps use sources and source types to extract knowledge from the data they index. Enter `zscaler` to display all possible Zscaler-specific source types. Select the option based on the kind of Zscaler logs sent to Splunk.

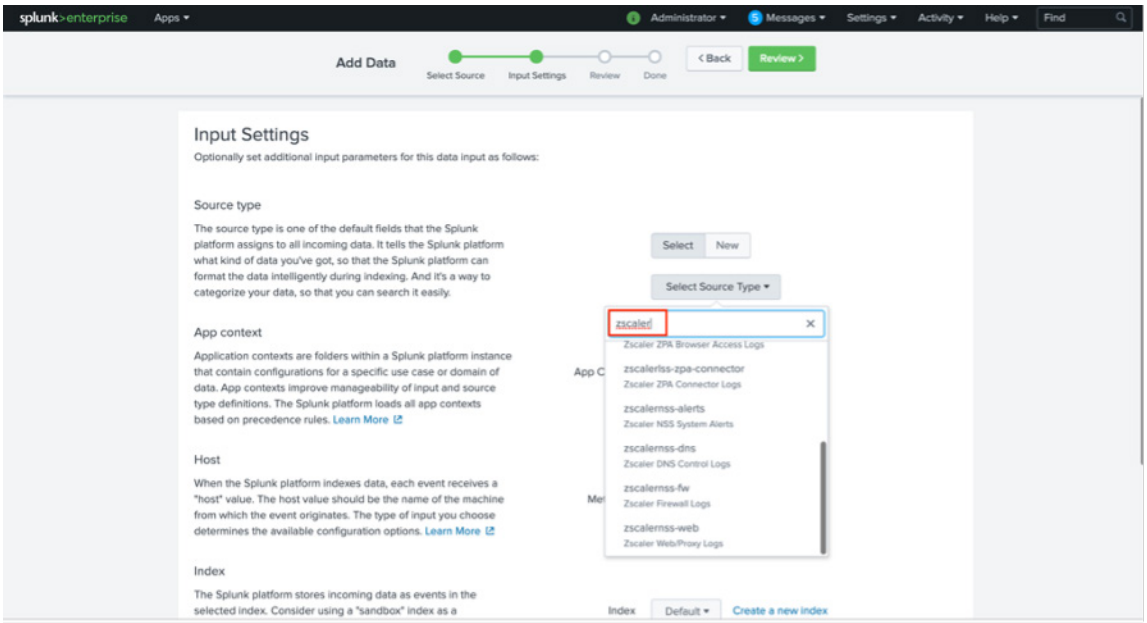

Figure 32. Select desired Zscaler source type

Change Default App Context and Default index

On the same page:

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**.

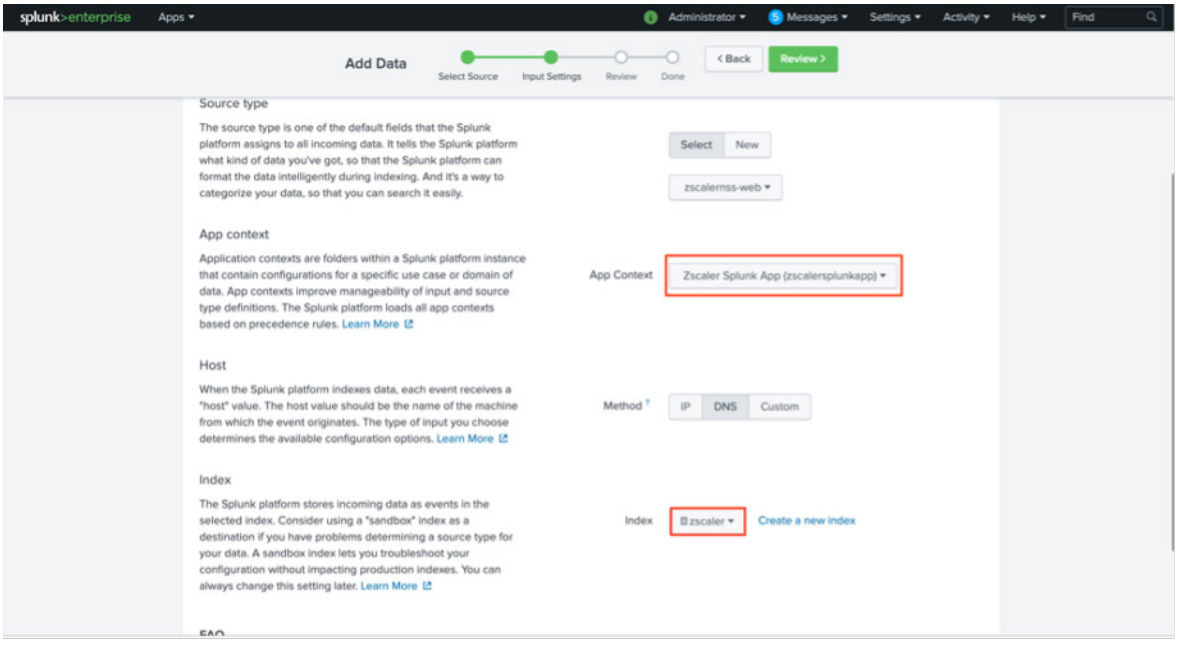

Figure 33. Change default app context

Verify Incoming Logs

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

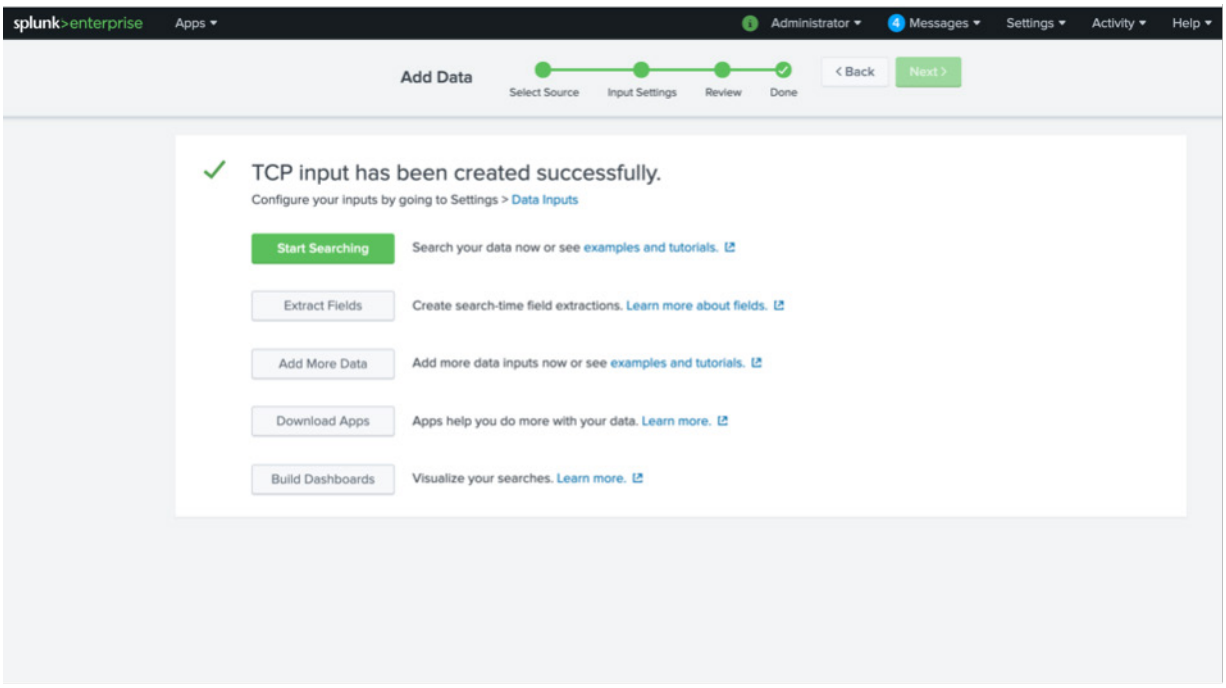

Figure 34. Verify incoming logs

Inspect Log Fields

This displays only the logs that are from Zscaler.

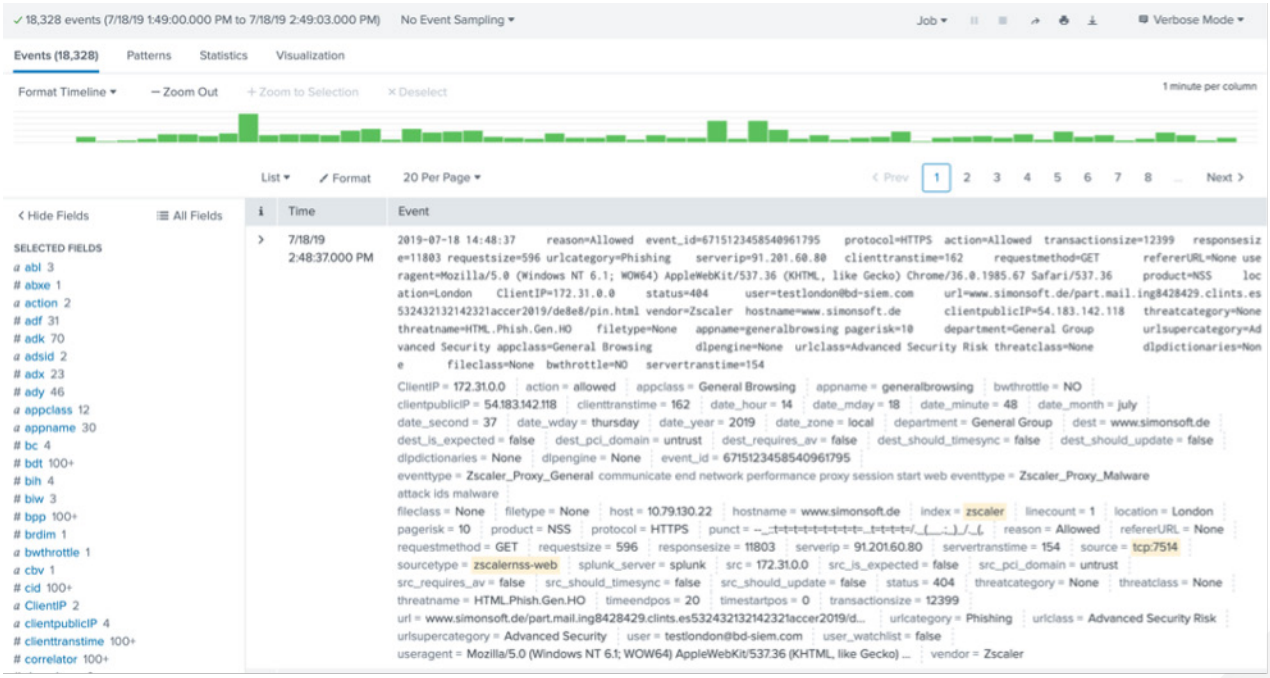

Figure 35. Inspect log fields

Extracted Log Fields

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

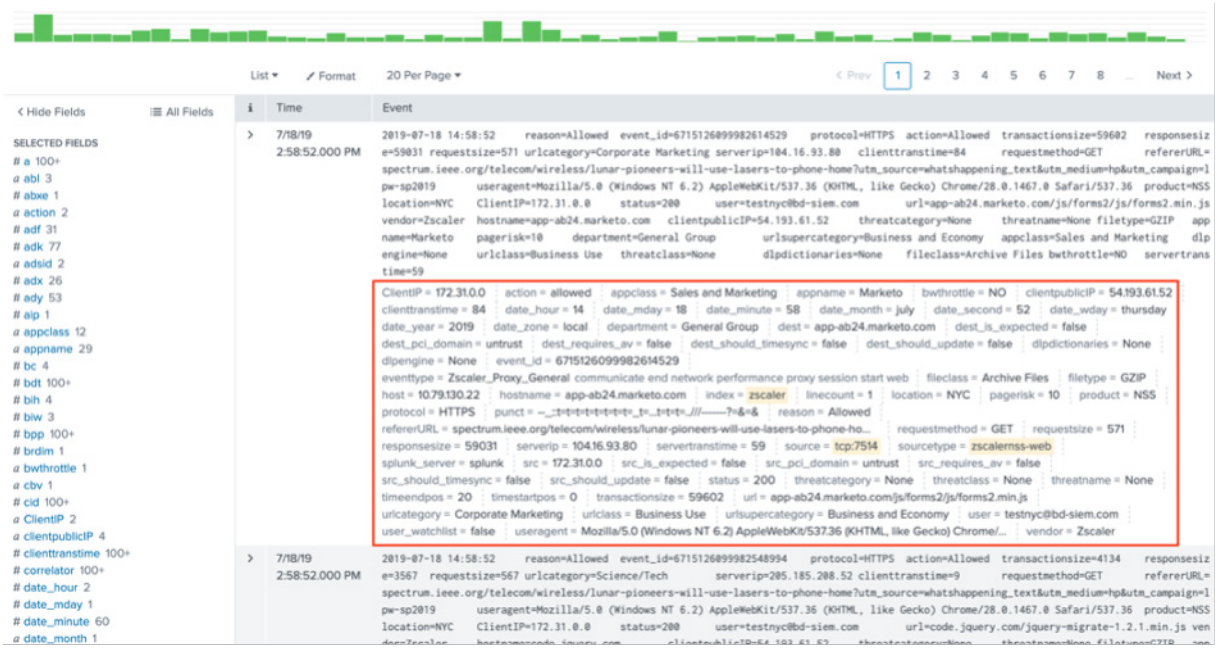

Figure 36. View extracted log fields

Verify Splunk's Zscaler App

Go to **Apps** > **Zscaler Splunk App.**

The window is populated with incoming Zscaler data.

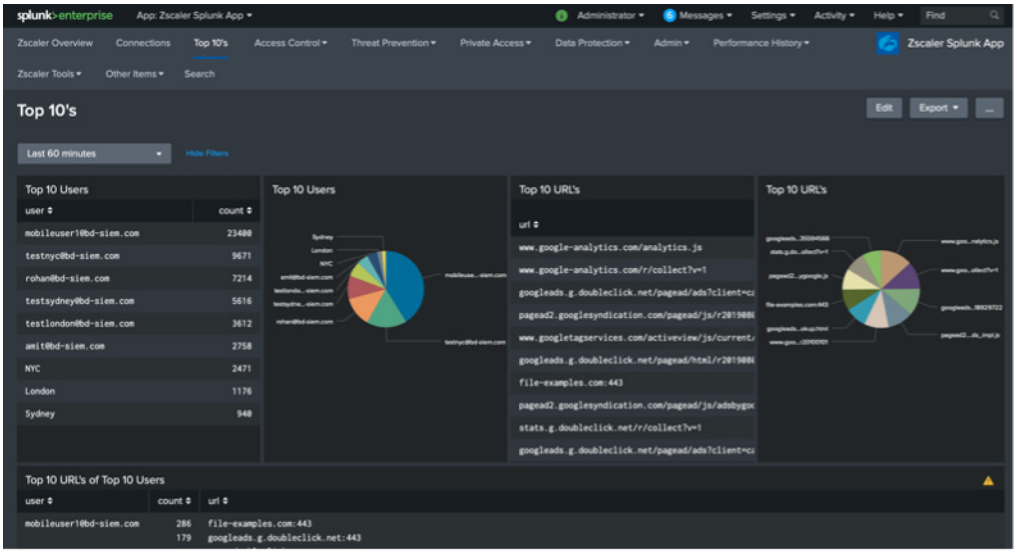

Figure 37. Verify Splunk Zscaler app

If a particular panel is not populated, click the **Search** icon next to it. This shows the query that the panel is running behind the scenes to help with troubleshooting.

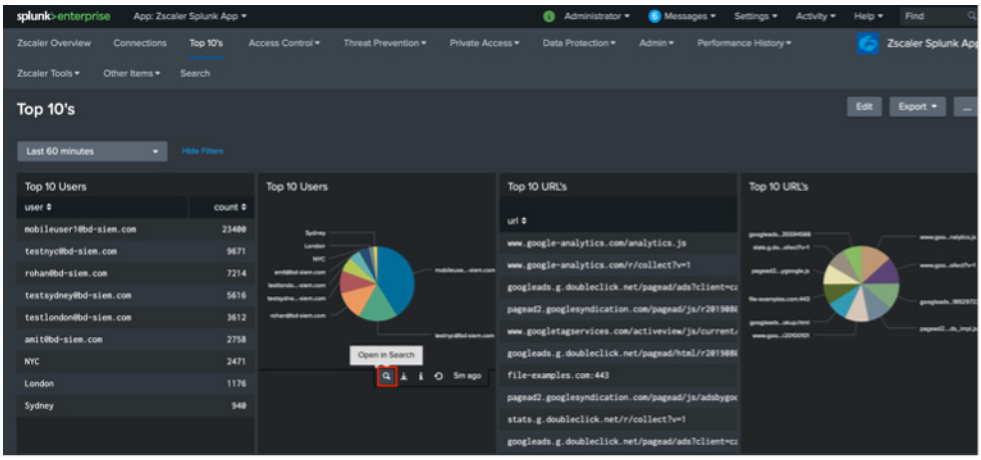

Figure 38. Verify Splunk Zscaler app

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 HTTP Event Collector (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, you 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.

Contact Zscaler Support to request access to this service.

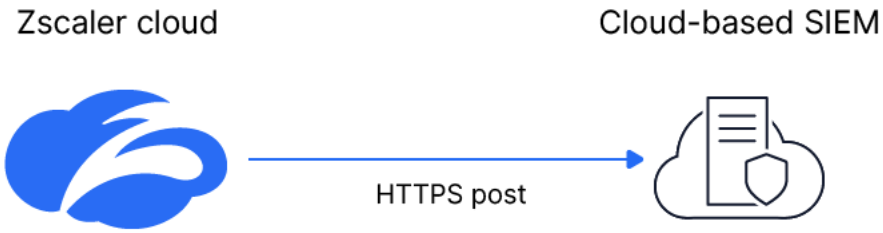

Figure 39. High-level overview of cloud-to-cloud logging

You 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:

- Understanding Nanolog Streaming Service (government agencies, see Understanding Nanolog Streaming Service).
- About Cloud NSS Feeds (government agencies, see About Cloud NSS Feeds).
- Add NSS Feeds (government agencies, see Add NSS Feeds).
- Adding Cloud NSS Feeds for Web Logs (government agencies, see Adding Cloud NSS Feeds for Web Logs).

Configure Splunk Cloud to Ingest ZIA Logs Over HEC Input

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

The Splunk HEC sends data and application events to a Splunk deployment over 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. You must later paste the HEC token that is created from the following steps into the ZIA Admin Portal. While the HEC token is required in this deployment, in addition, you can optionally restrict the public source IPs that are allowed to send logs to their Splunk cloud stack. Contact Splunk support to employ any IP-level allowlists.

Log In to Splunk Cloud Tenant

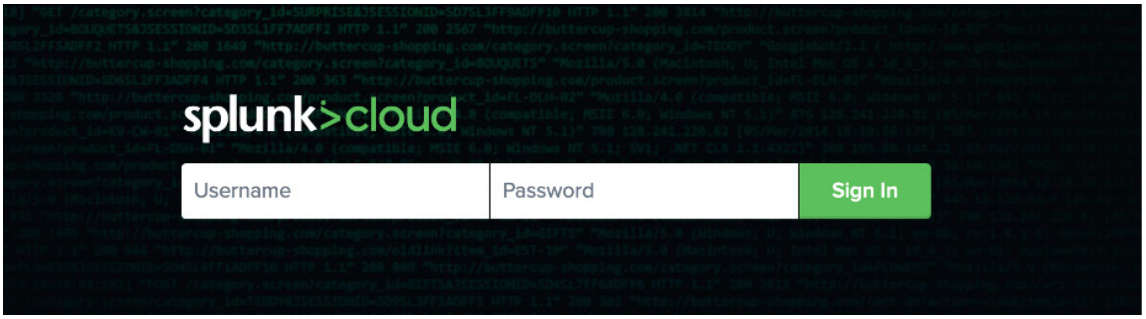

Figure 40. Log in to Splunk Cloud tenant

Install Zscaler App and Zscaler Technical Add-On in Your Cloud Tenant

After logging in, go to **Apps** > **Browse More Apps** and search for `zscaler`.

You can install Zscaler Splunk App on your Splunk cloud tenant.

Contact the Splunk cloud support team to get *Zscaler Technical Add-On* installed in your Splunk cloud tenant.

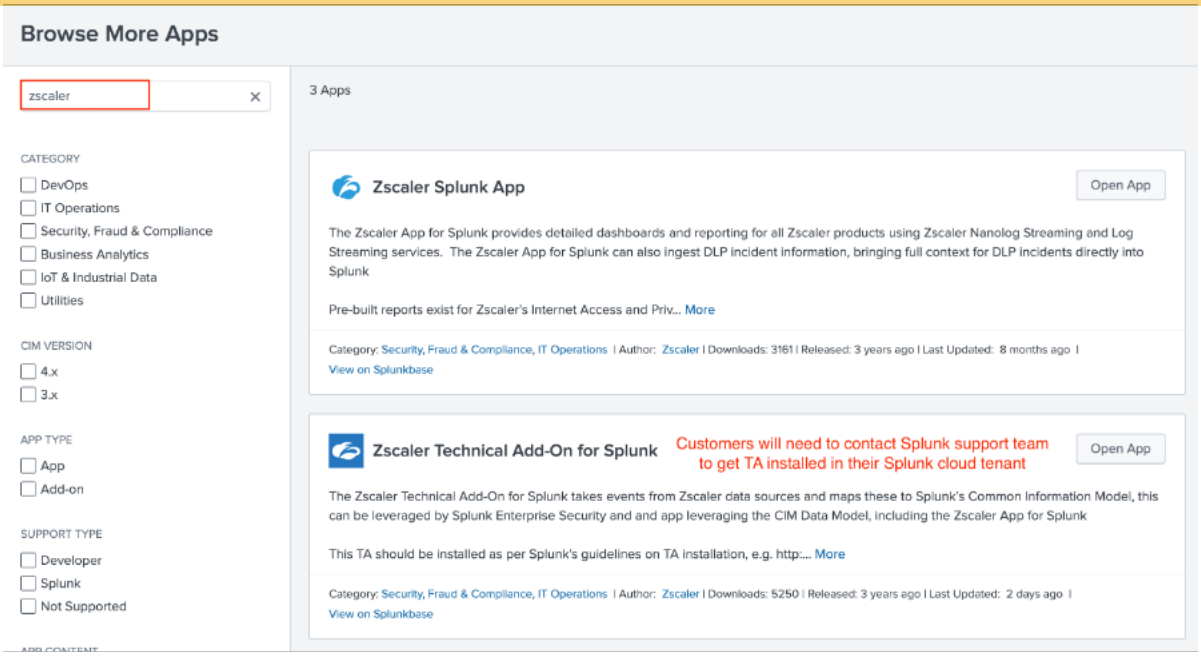

Figure 41. Install Zscaler App and Technical Add-On

Create Zscaler Index in Splunk

After installing Zscaler App and Technical Add-On, go to **Settings** > **Indexes** > **New Index**.

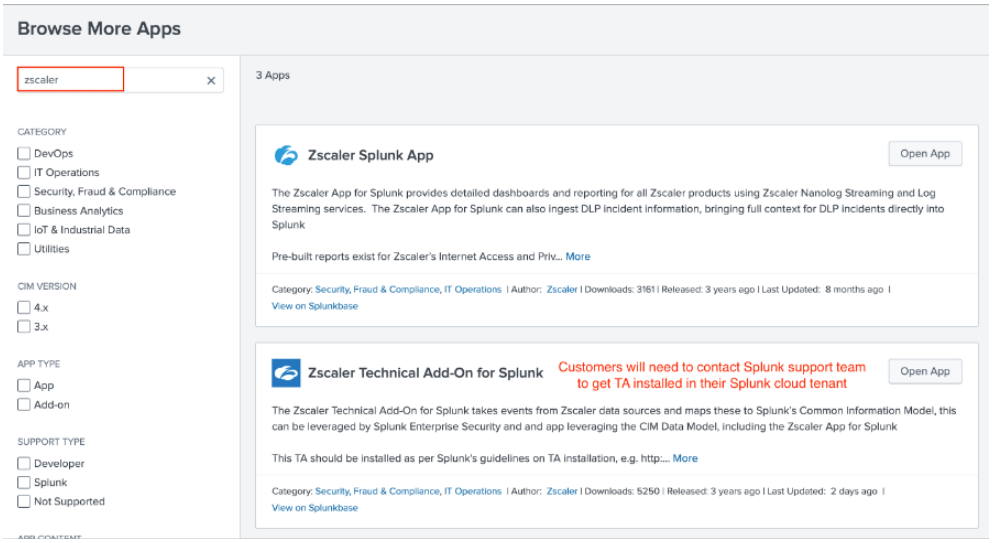

Figure 42. Add new index

Add Zscaler Index in Splunk

In the **New Index** dialog, enter `zscaler` (case sensitive) and click Save.

Because the Splunk App for Zscaler looks for data written at index *zscaler* by default, setting *index=zscaler* allows you 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 your setup, amount of logs, cost associated with storage in Splunk cloud, etc., and vary from customer to customer. For more information regarding these settings, refer to the Splunk documentation.

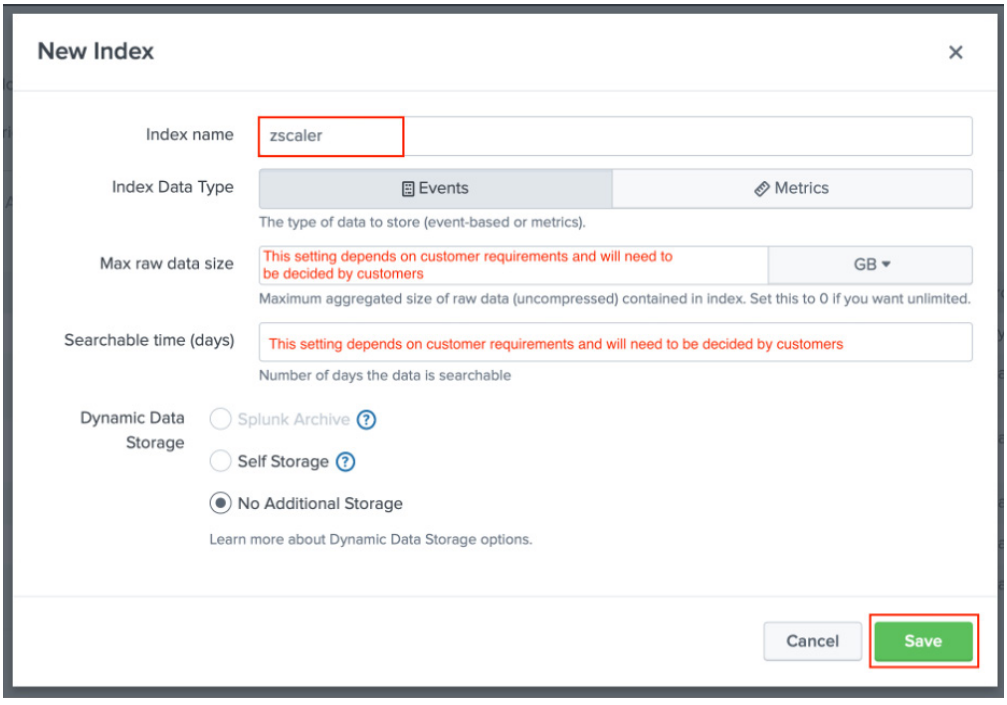

Figure 43. Add Zscaler index in Splunk

Create a new Data Input and HEC token

After creating an index, go to **Settings** > **Data inputs**.

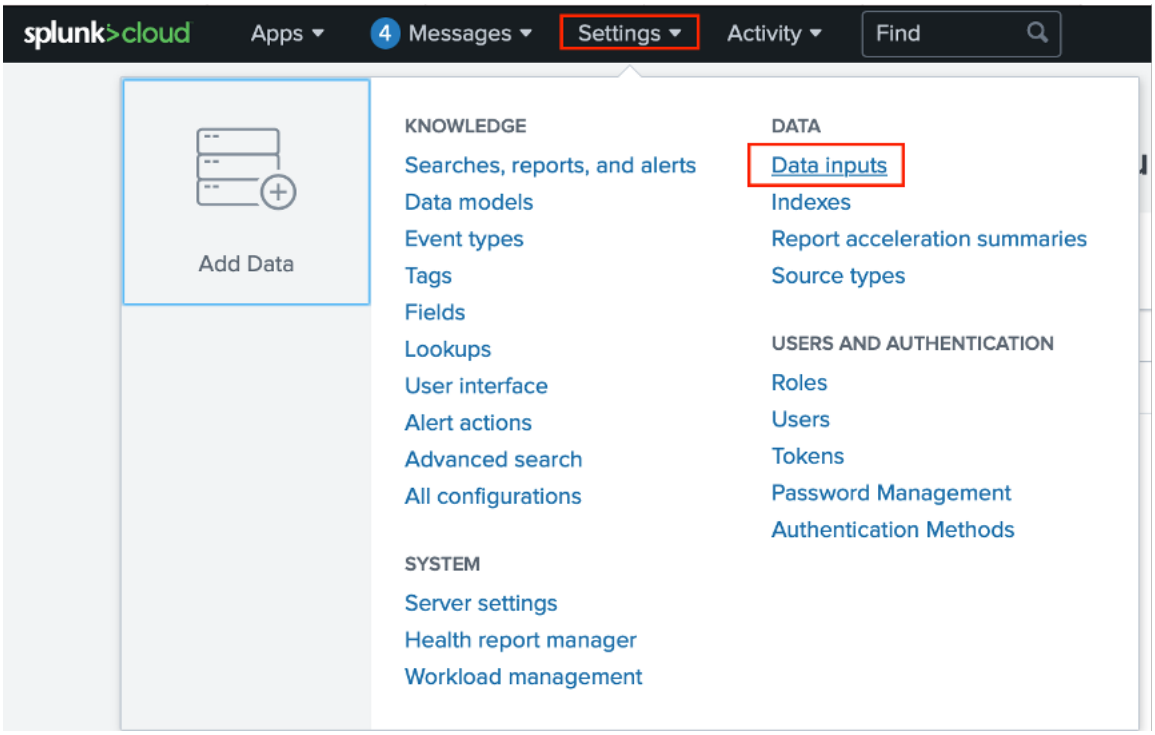

Figure 44. Go to Data Inputs

The **Data inputs** dialog is displayed. Click the option to **Add new** input.

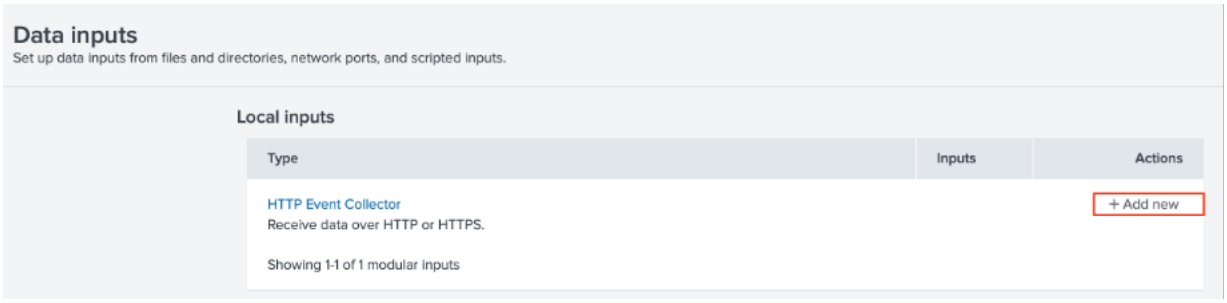

Figure 45. Create new input

Configure Data Input and HEC token

Create an HEC token. This is a 32-character 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.

Do not enable indexer acknowledgment. Enter a token name. Leave the rest of options at default settings and click **Next**.

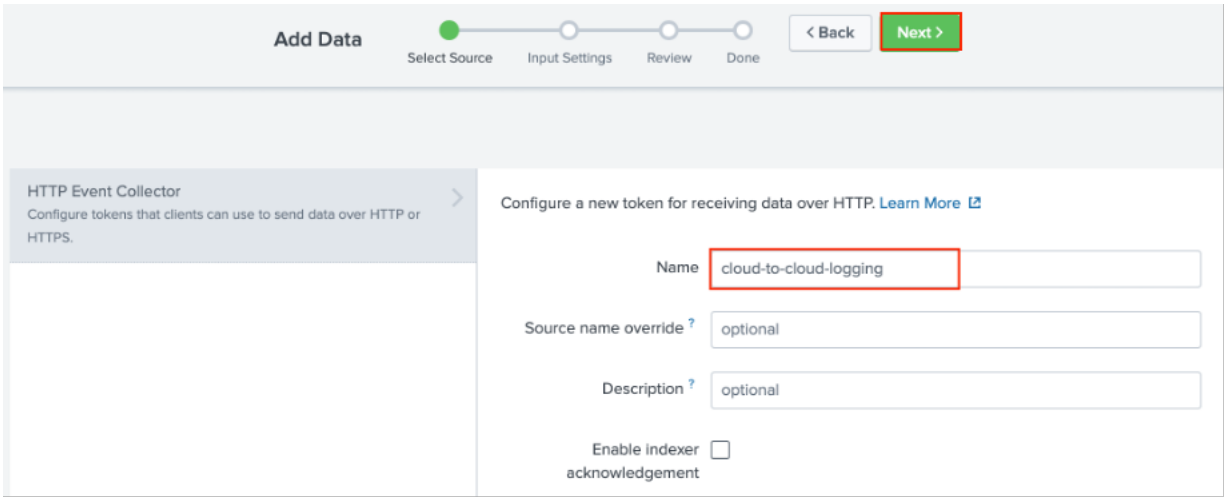

Figure 46. Configuring HEC token and input

The following example sends ZIA Web logs to the Splunk cloud. Thus, the source type selected in this example is zscalernss-web. Change the source type to match the log type that you want to ingest (for example, zscalernss-fw, zscalernss-dns, etc.).

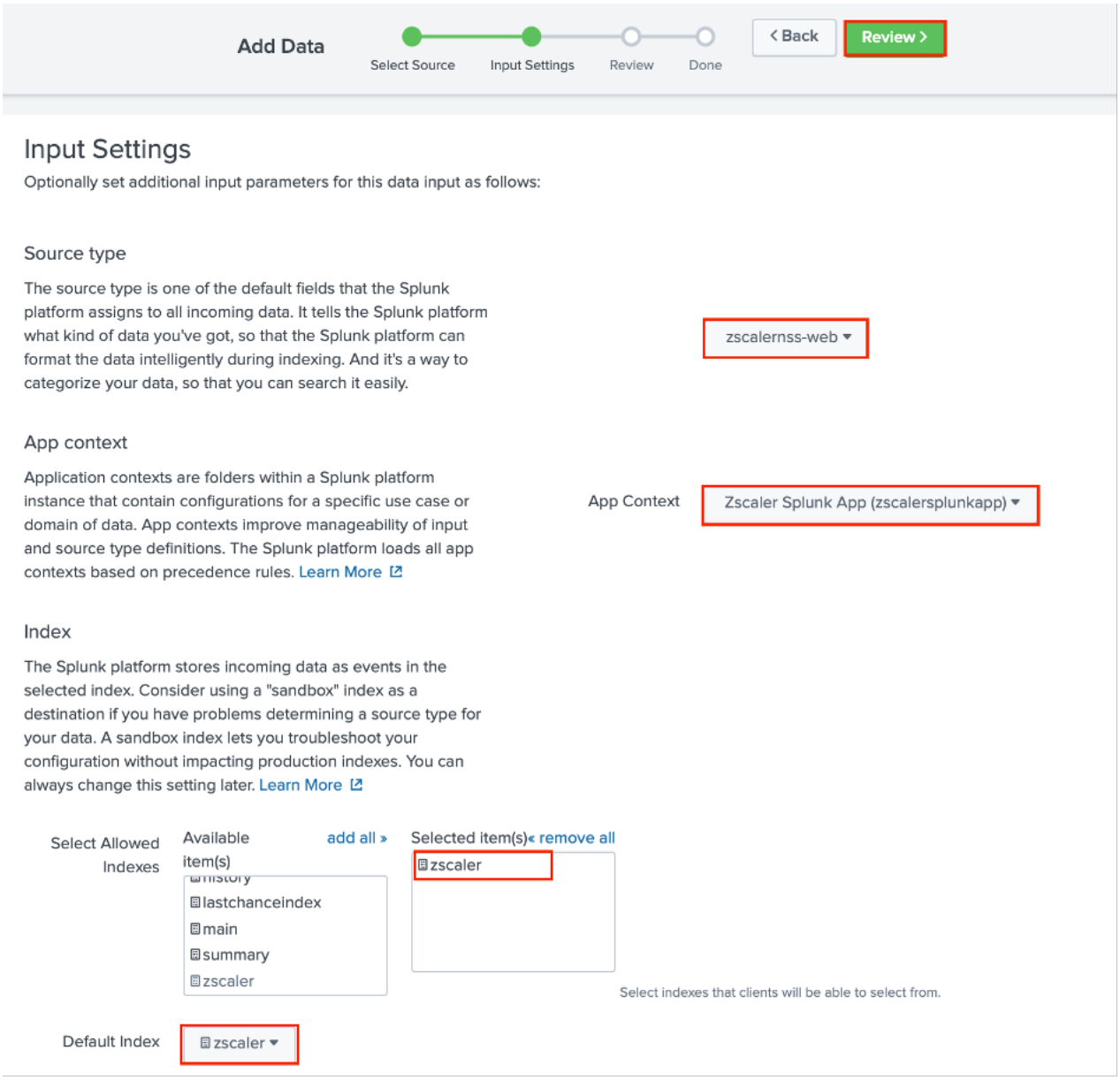

Figure 47. Configuring HEC token and input (cont.)

From the Review dialog, confirm the settings and click **Submit**.

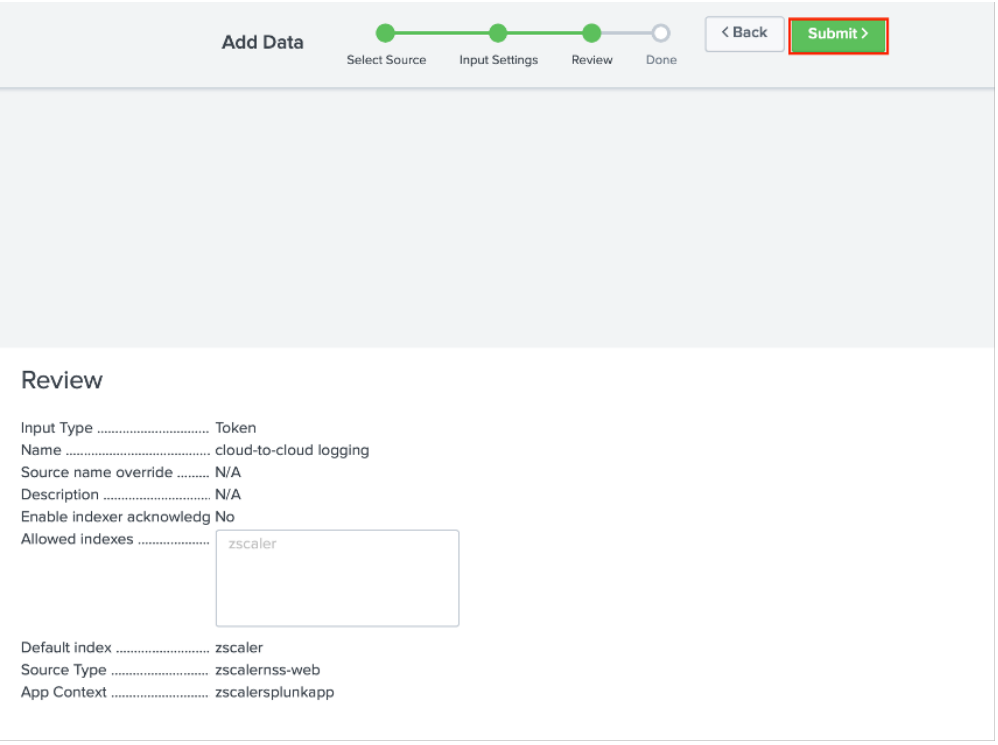

Figure 48. Review the setup

The Token is being deployed. The token might take a few minutes to deploy in the Splunk cloud.

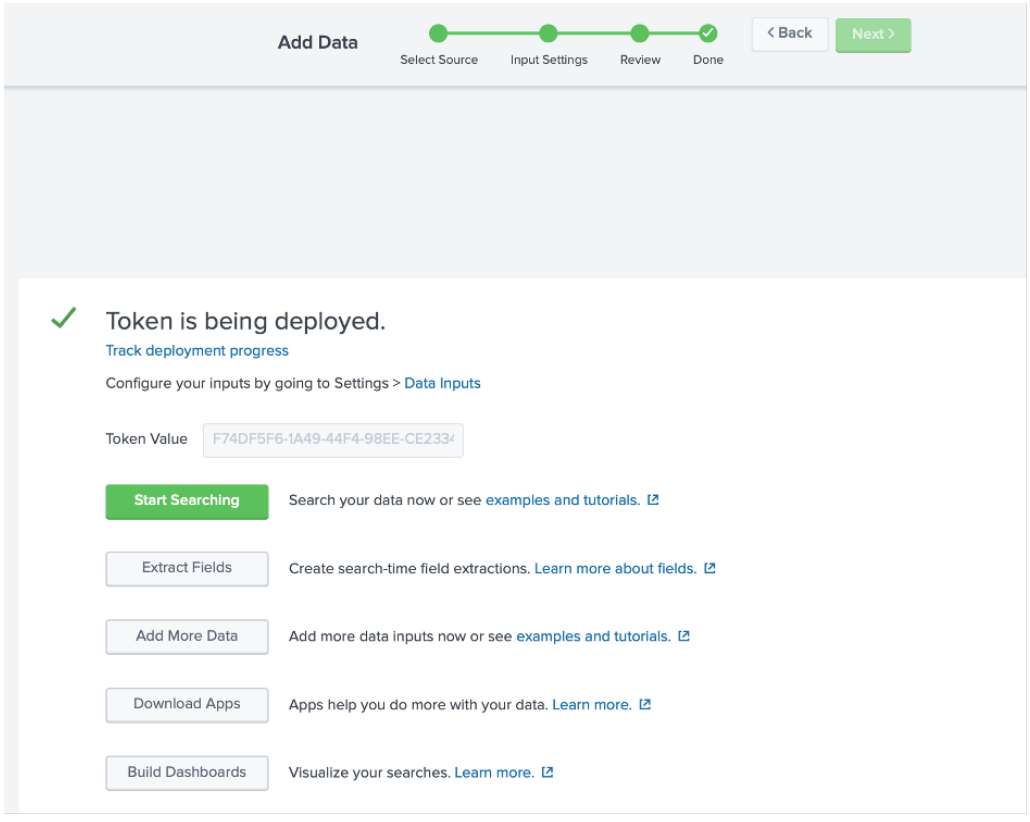

Figure 49. Wait for token to be deployed

Copy the HEC Token Value

After the token is deployed, go to **Setting** > **Data inputs** > **HTTP Event Collector**.

The 32-character HEC token is shown in this window. Make a note of this token for use in the ZIA Admin Portal later. In Splunk, HEC tokens are tied to different source types (Zscaler's source types: web, Firewall, DNS, etc.).

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

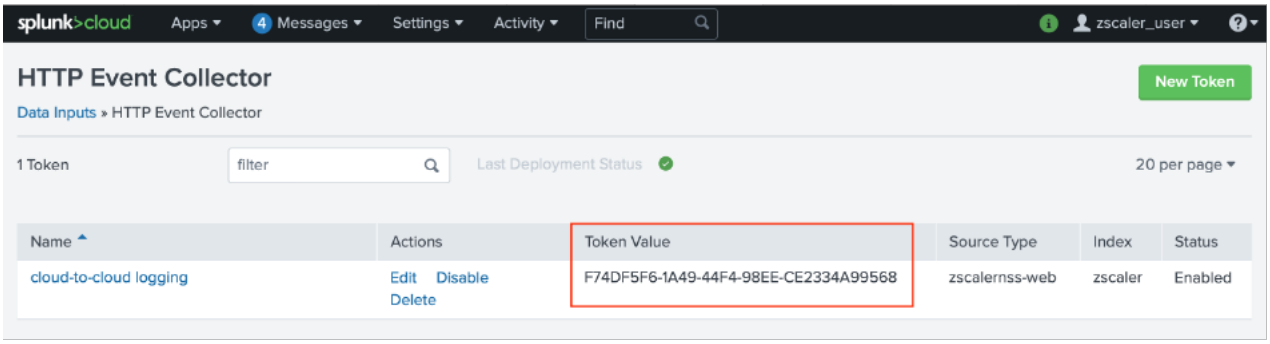

Figure 50. Note the HEC token

Determine the Splunk Cloud API Endpoint to Send Logs To

The host of the Splunk API endpoint that you specify to send logs to depends on your Splunk cloud deployment. Refer to Set up and use HTTP Event Collector in Splunk Web to determine the *host* portion. Use JSON-formatted log messages.

The *endpoint* portion is always */services/collector*, and endpoint */services/collector/raw* does not come into play. Note 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-`

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

Figure 51. Determine the Splunk Cloud API endpoint to send logs to

Configure Splunk Cloud to Fetch Zscaler Audit Logs and Sandbox Events

Previously, the Zscaler Splunk Technical Add-On needed to be installed on Splunk Inputs Data Manager (IDM). IDM was a Splunk instance within a Splunk Cloud Stack that set up and configured 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. To use IDM, contact Splunk support.

Now, Splunk cloud prefers using Victoria, which removes the necessity of IDM. You can install most apps on Splunk cloud directly as opposed to contacting Splunk support.

If using IDM, a Zscaler username, password, and API credentials are configured on the Splunk Technical Add-On installed on IDM. This initiates API calls from the Splunk cloud to Zscaler to fetch audit logs and Sandbox reports.

If using the newer Victoria stack, complete the following steps on the same Splunk cloud instance on which the Zscaler Splunk app is installed (instead of IDM).

You must also request the Splunk cloud support team to enable *Scheduled search* capabilities on their IDM. This setting is disabled in Splunk cloud by default. You must peer the IDM to the indexing tier so that indexed data can be searched.

Second, the account running the Zscaler Technical Add-On (likely sc_admin or splunk-system-user) must have Splunk capabilities to:

- Run saved searches.
- Output a lookup.

Finally, the equivalent saved search on the IDM must be enabled and scheduled to run.

For more information, refer to the Splunk documentation.

Log In to Splunk IDM Instance

The following image shows the Splunk IDM log in dialog.

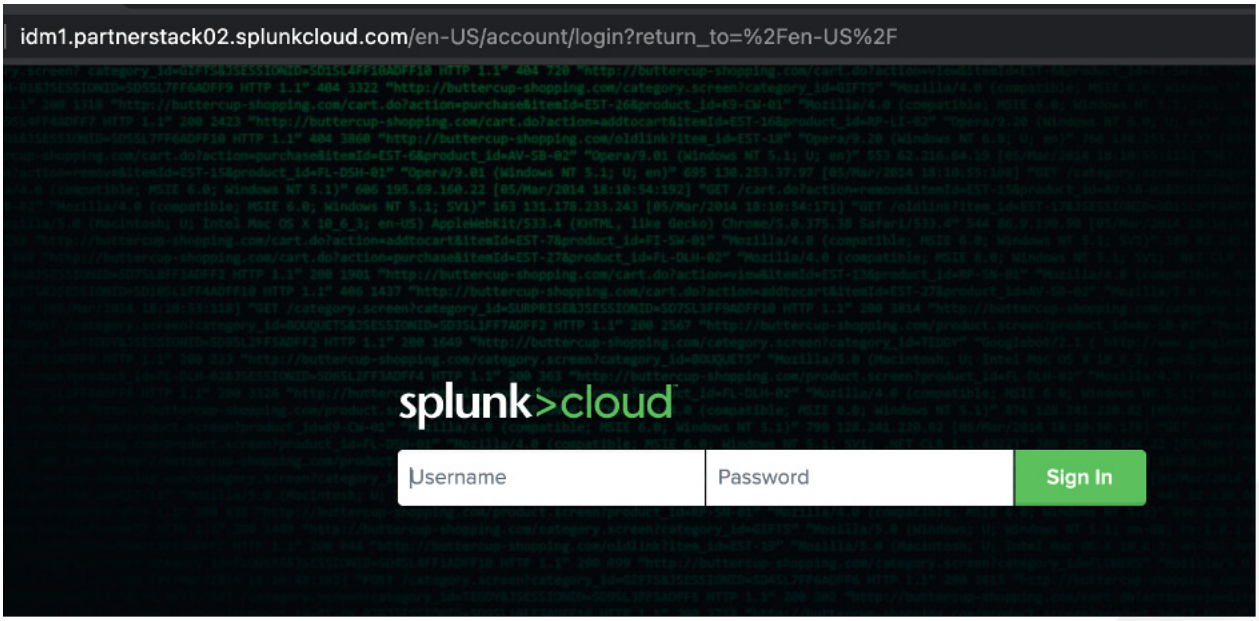

Figure 52. Log in to Splunk cloud IDM

Install Zscaler Splunk Technical Add-On on Splunk IDM Instance

After logging in, go to **Apps** > **Find more Apps** and search for `zscaler`.

You must contact Splunk cloud support team to get the Zscaler Technical Add-On installed in your Splunk cloud tenant. Zscaler Splunk App doesn't need to be installed on IDM.

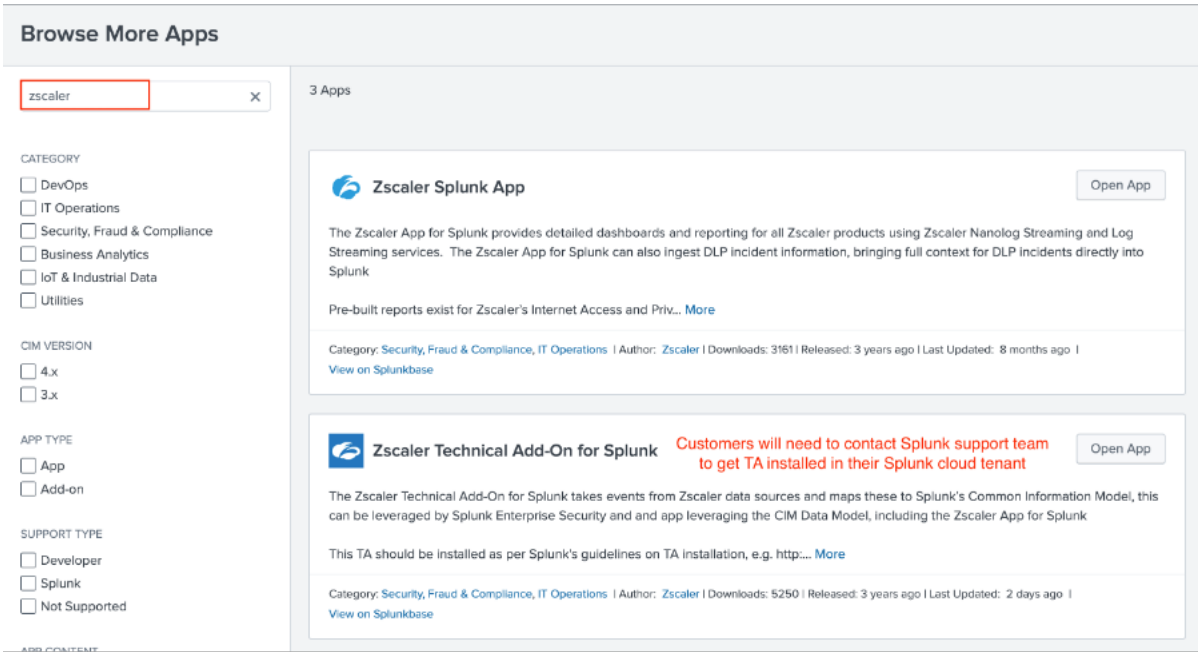

Figure 53. Install Zscaler Splunk App and Technical Add-On

Configure Zscaler Index on Splunk IDM Instance

After Zscaler Splunk Technical Add-On is installed on Splunk IDM, go to **Settings** > **Indexes** and create a new *zscaler* index.

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

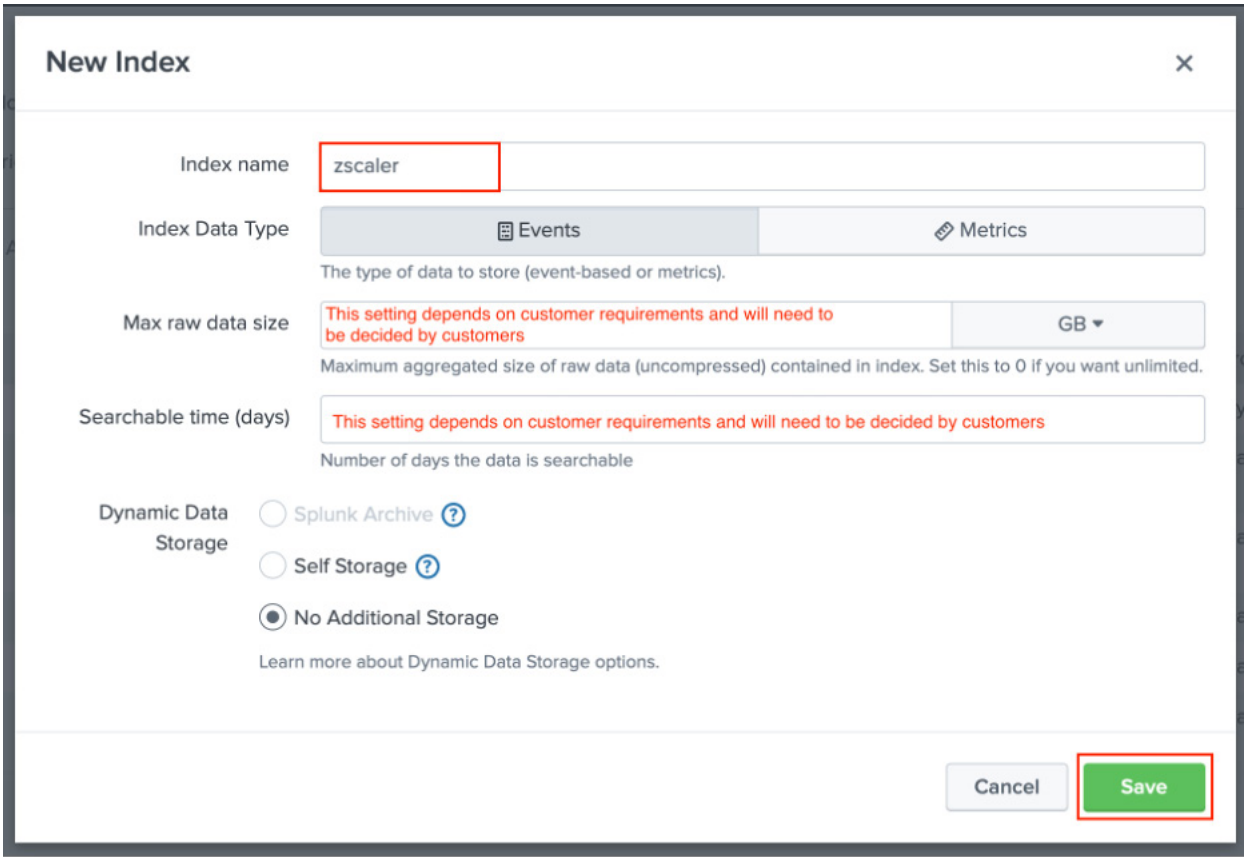

Figure 54. Add Zscaler Index in Splunk IDM

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

Go to **Configuration** > **Account** > **Add**.

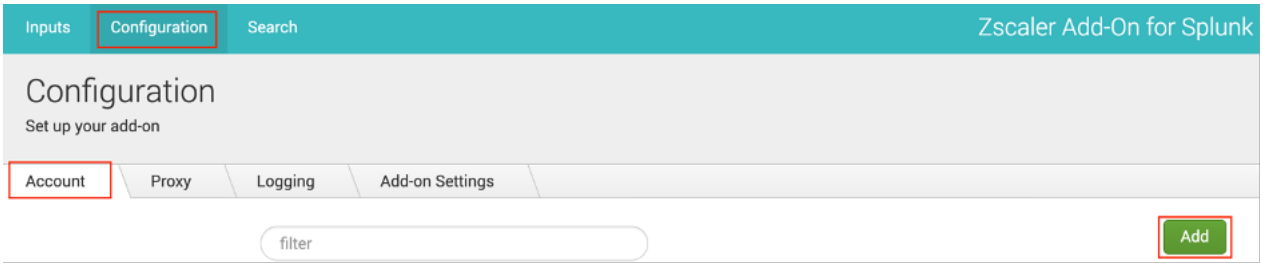

Figure 55. Create new account in Splunk IDM

Fill in the Zscaler credentials pertinent to your ZIA tenant and save the settings by clicking **Add**.

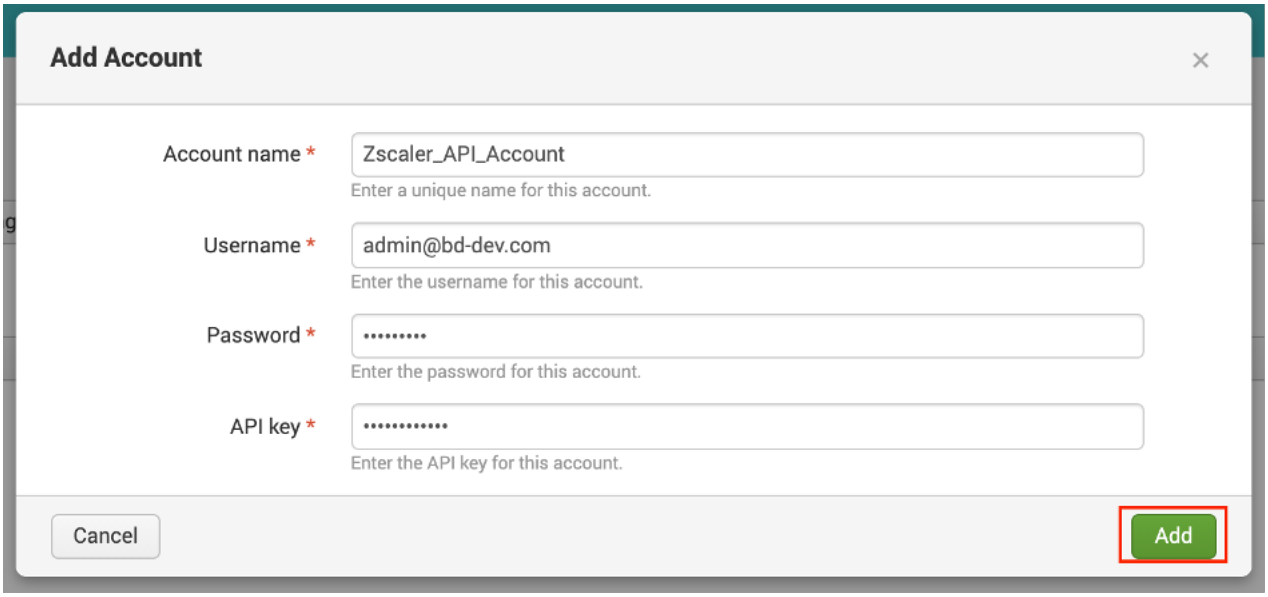

Figure 56. Fill in ZIA credentials in Splunk IDM

Configure Input for Audit Logs

In IDM, go to **Inputs** > **Create New Input**. First, configure input for fetching **Zscaler Audit Logs**.

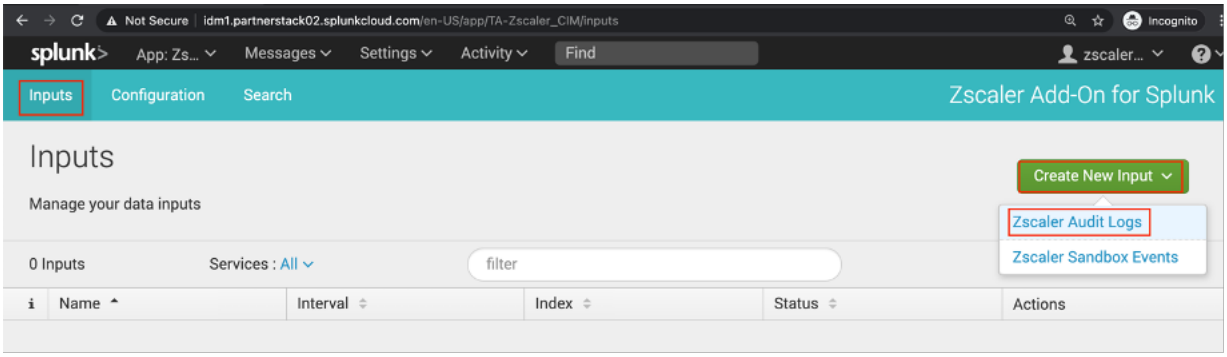

Figure 57. Add audit logs input in Splunk IDM

Fill in the Settings for Fetching ZIA Audit Logs

After filling in the details, click **Add**. Settings might take a few minutes to take effect.

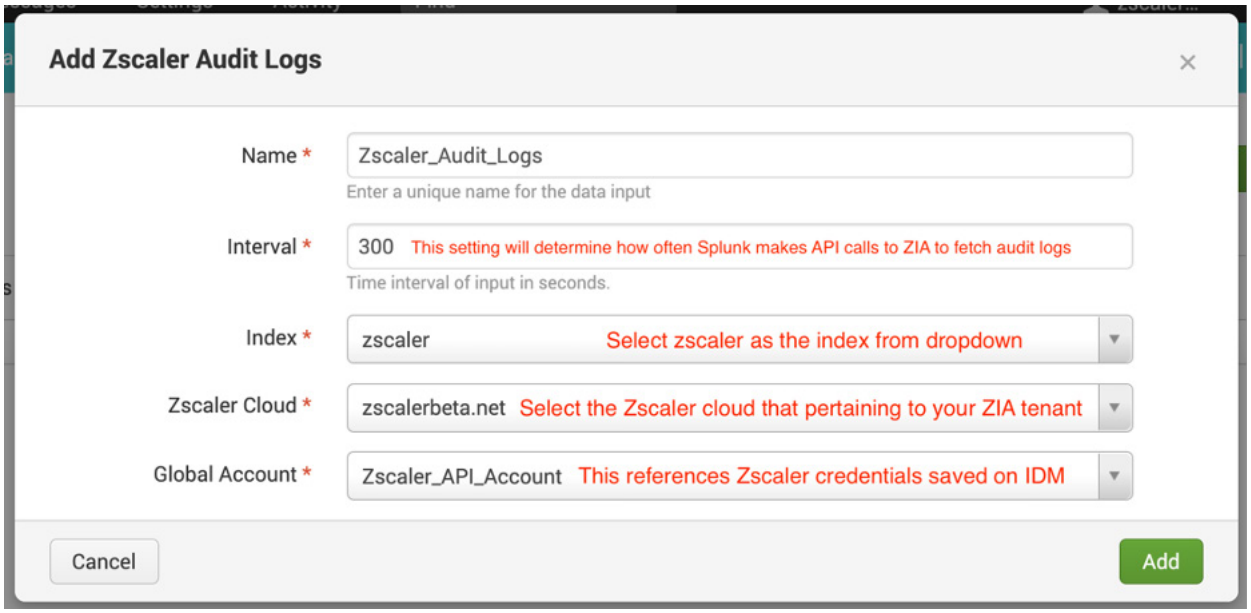

Figure 58. Save Audit Logs input in Splunk IDM

Configure Input for Sandbox Events

In IDM, go to **Inputs** > **Create New Input**. Then, select **Zscaler Sandbox Events**.

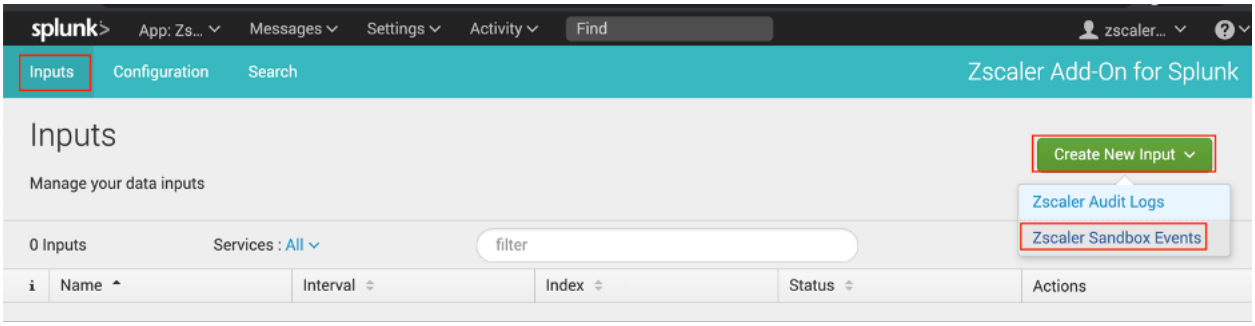

Figure 59. Add Sandbox events input in Splunk IDM

Fill in the Settings for Fetching ZIA Sandbox Events

After filling in the details, click **Add**. Settings might take a few minutes to take effect.

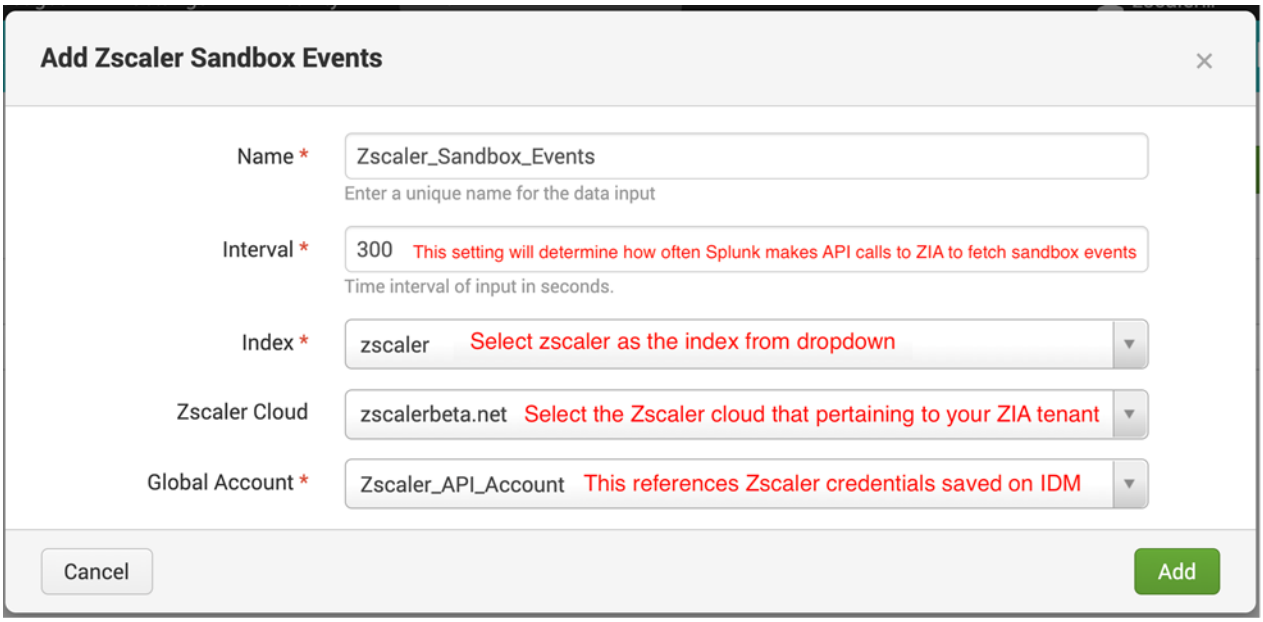

Figure 60. Save Sandbox events input in Splunk IDM

Confirm that Both Input Settings are Saved and Enabled

On the Inputs section of IDM, view the Zscaler Audit Logs and Zscaler Sandbox Events. Confirm that the **Status** for each input is **Enabled**.

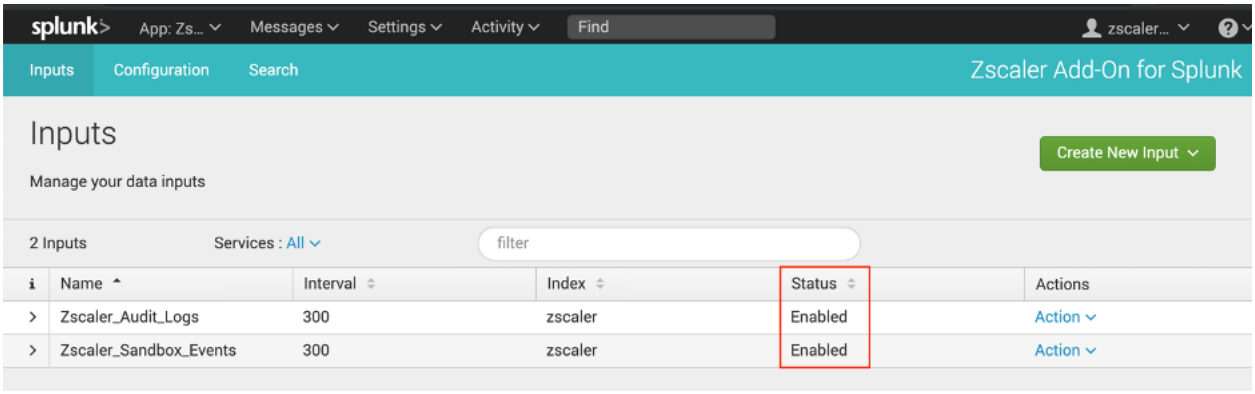

Figure 61. Confirm that both Inputs are enabled in Splunk IDM

Configure Zscaler for Cloud-to-Cloud Logging

You 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, you can configure an HTTP or HTTPS API feed that pushes logs from the Zscaler cloud service into an HTTPS API endpoint on the SIEM (i.e., the HEC input for the Splunk cloud). The following steps show how to set up the log feed for web logs. You must repeat these steps to set up other Zscaler log types (e.g., Firewall or DNS logs).

Go to Cloud-to-Cloud Logging Section in ZIA Portal

After logging in to ZIA Admin Portal, go to **Administration** > **Nanolog Streaming Service** > **Cloud NSS Feeds** > **Add Cloud NSS Feed**.

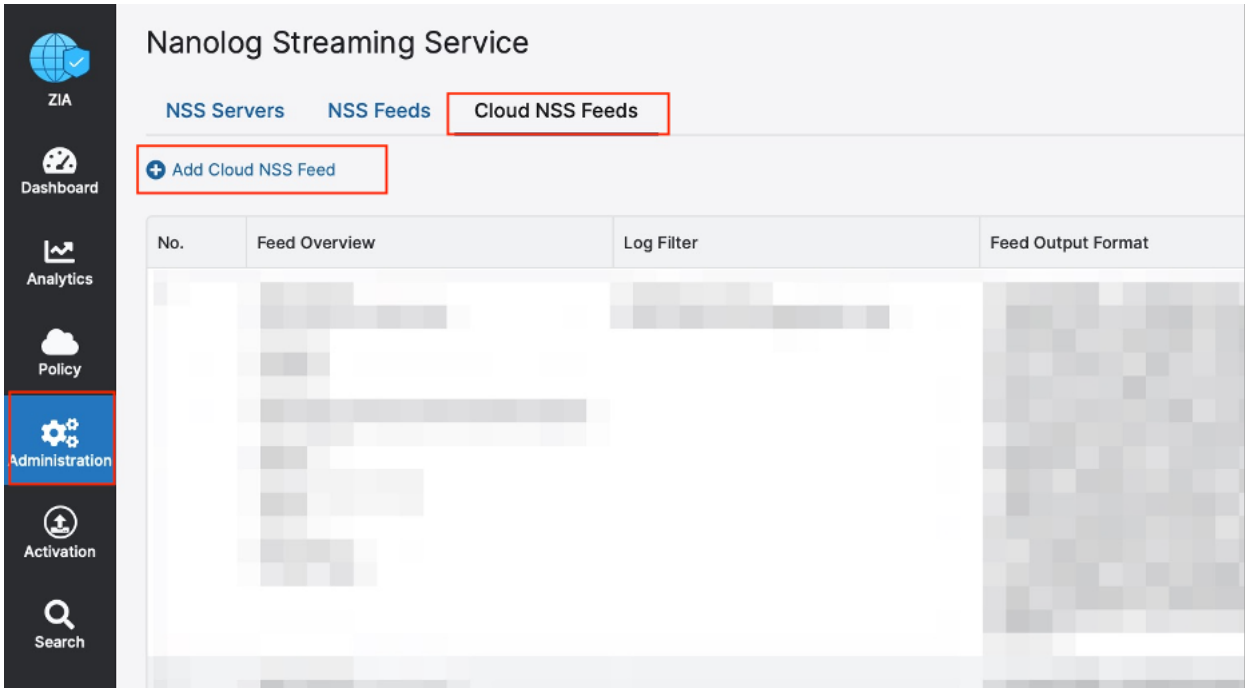

Figure 62. Go to cloud-to-cloud logging section in ZIA

Set Up the Cloud NSS Log Feed (Web)

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

The API URL is a Splunk URL dependent on your Splunk cloud stack.

Enter `?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, in the ZIA Admin Portal, configure it as:

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

The 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 menu. After filling in required parameters, click **Save**. Enter **,** \" (comma, backslash, double quotes) to the **Feed Escape Character** list.

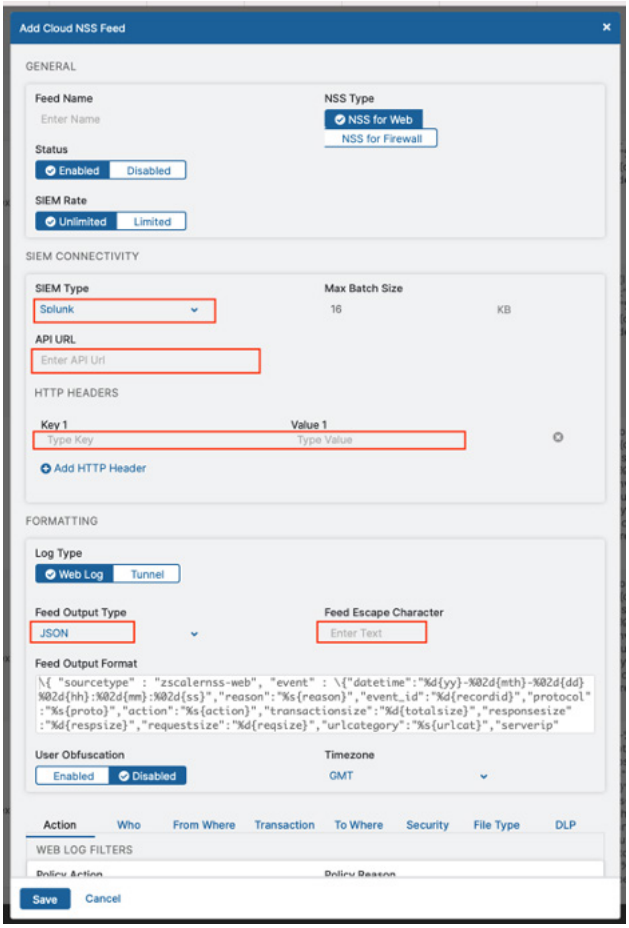

Figure 63. Configure cloud NSS feed

When you create a web feed, you must set the Feed Output Type to Custom and then paste the following code text into the Feed Output Format:

```
\{ "sourcetype" : "zscalernss-web", "event" : \{"datetime":"%d{yy}-%02d{mth}-%02d{dd}
%02d{hh}:%02d{mm}:%02d{ss}","reason":"%s{reason}","event_id":"%d{recordid}","protocol
":"%s{proto}","action":"%s{action}","transactionsize":"%d{totalsize}","responsesize":
"%d{respsize}","requestsize":"%d{reqsize}","urlcategory":"%s{urlcat}","serverip":"%s{
sip}","clienttranstime":"%d{ctime}","requestmethod":"%s{reqmethod}","refererURL":"%s{
ereferer}","useragent":"%s{eua}","product":"NSS","location":"%s{elocation}","ClientIP
":"%s{cip}","status":"%s{respcode}","user":"%s{elogin}","url":"%s{eurl}","vendor":"Zs
caler","hostname":"%s{ehost}","clientpublicIP":"%s{cintip}","threatcategory":"%s{malw
arecat}","threatname":"%s{threatname}","filetype":"%s{filetype}","appname":"%s{appname}
","pagerisk":"%d{riskscore}","department":"%s{edepartment}","urlsupercategory":"%s{ur
lsupercat}","appclass":"%s{appclass}","dlpengine":"%s{dlpeng}","urlclass":"%s{urlclas
s}","threatclass":"%s{malwareclass}","dlpdictionaries":"%s{dlpdict}","fileclass":"%s{fi
leclass}","bwthrottle":"%s{bwthrottle}","servertranstime":"%d{stime}","contenttype":"
%s{contenttype}","ssldecrypted":"%s{ssldecrypted}","unscannabletype":"%s{unscannablet
ype}","md5":"%s{bamd5}","deviceowner":"%s{deviceowner}","devicehostname":"%s{deviceho
stname}"\}\}
```


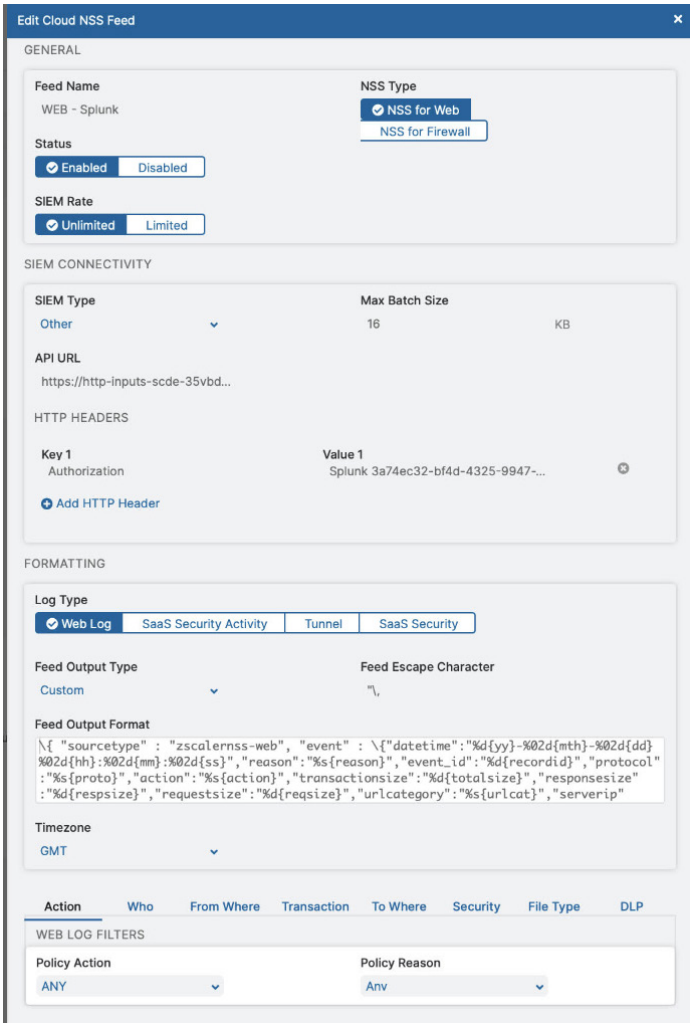

Figure 64. Example with all fields populated (web)

Set Up the Cloud NSS Log Feed (Firewall)

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

The API URL is a Splunk URL, dependent on your Splunk cloud stack.

Enter `?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, in the ZIA Admin Portal, configure it as:

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

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

1. 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).
2. Select the **Feed Output Type** of **JSON** from the drop-down menu. Enter **,** `\"` (comma, backslash, double quotes) to the **Feed Escape Character** list. In the **Feed Output Format**, change the `sourcetype` to `zscalernss-fw`.
3. After filling in required parameters, click **Save**.

Figure 65. Configure cloud NSS feed

The following image is an example with all fields populated.

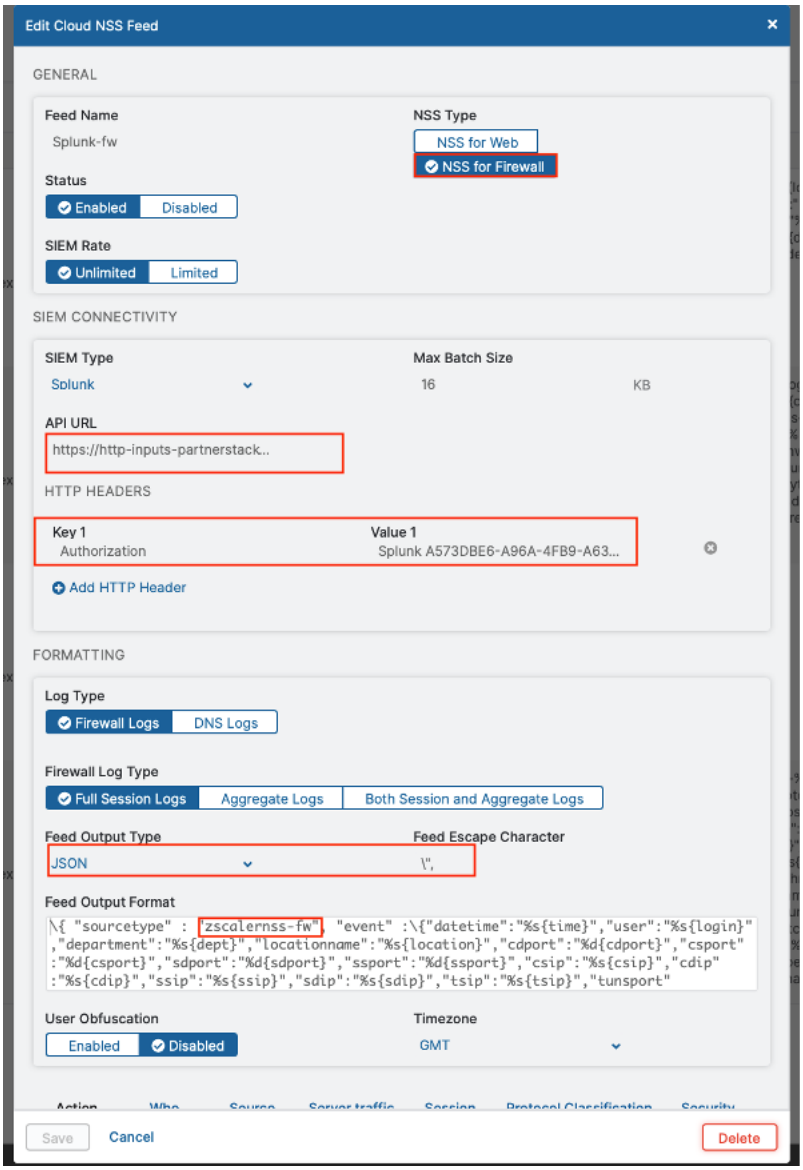

Figure 66. Example with all fields populated (firewall)

Add Other Log Source Types

Repeat the preceding steps to add other log source types (for example, DNS logs, tunnel logs, etc.).

Make sure to edit the feed output format to `zscalernss-dns`, `zscalernss-tunnel`, etc. See the table in the Source Types section for a list of source types.

Validate NSS Cloud Configuration

After the config is saved, click the **Zscaler** icon 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 when Splunk sends the expected response.

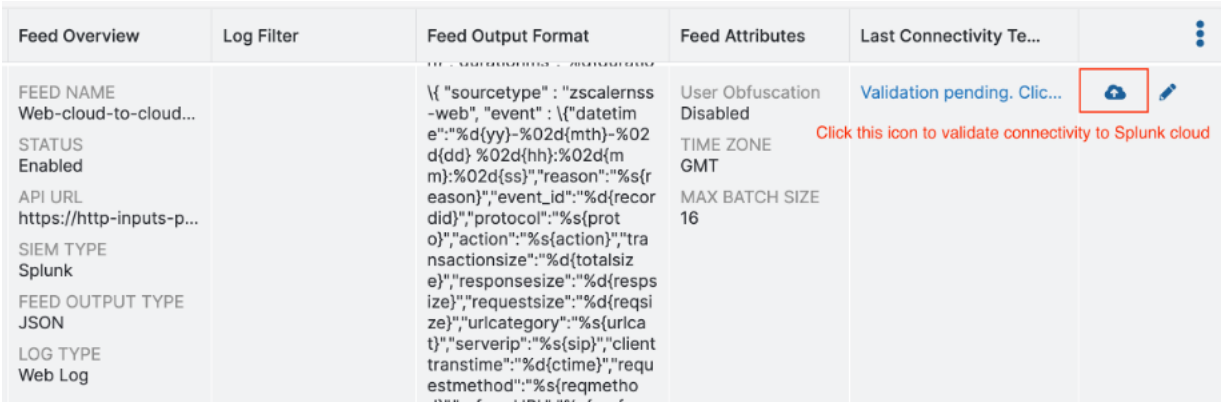

Figure 67. Verify connectivity to Splunk cloud

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

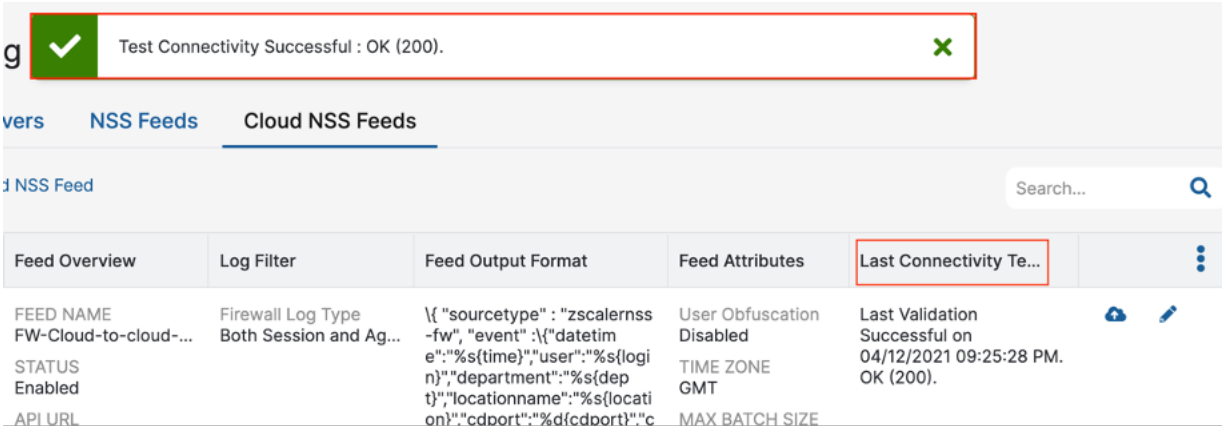

Figure 68. Splunk cloud connectivity verified

Verify Zscaler Splunk App

Log back in to your Splunk cloud tenant and go to **Apps** > **Zscaler Splunk App**.

It is populated with incoming Zscaler log data.

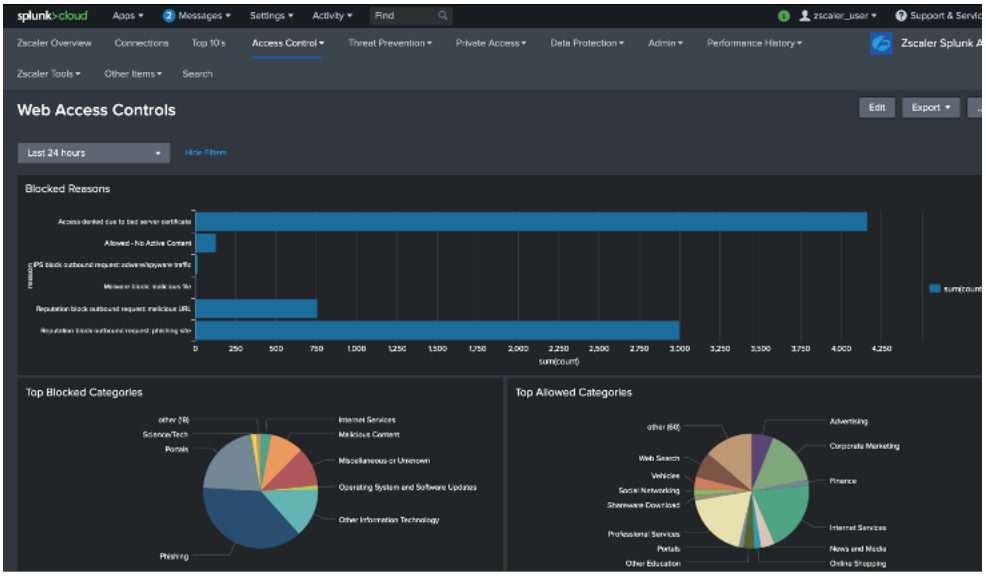

Figure 69. Verify Zscaler Splunk App

If you see a particular panel unpopulated, click the magnifying glass next to it. This shows you the query that the panel is running behind the scenes, which helps with troubleshooting.

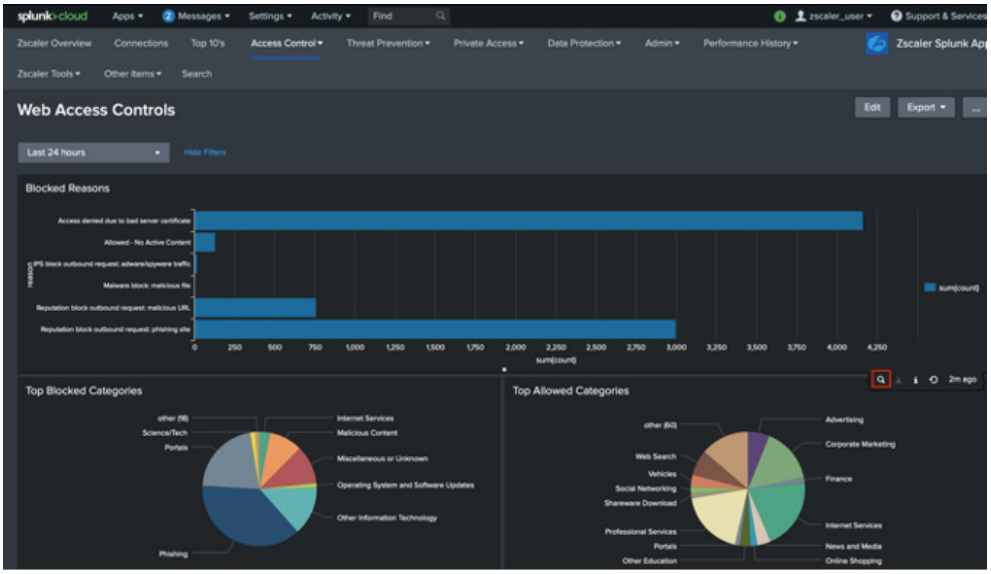

Figure 70. Access individual searches within Zscaler Splunk App

Appendix D: Using SOAR with Zscaler and Splunk

Splunk SOAR (formerly Phantom) is a security orchestration, automation, and response (SOAR) system. The Splunk SOAR 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.

You can watch a video demonstrating Splunk SOAR.

SOAR Components

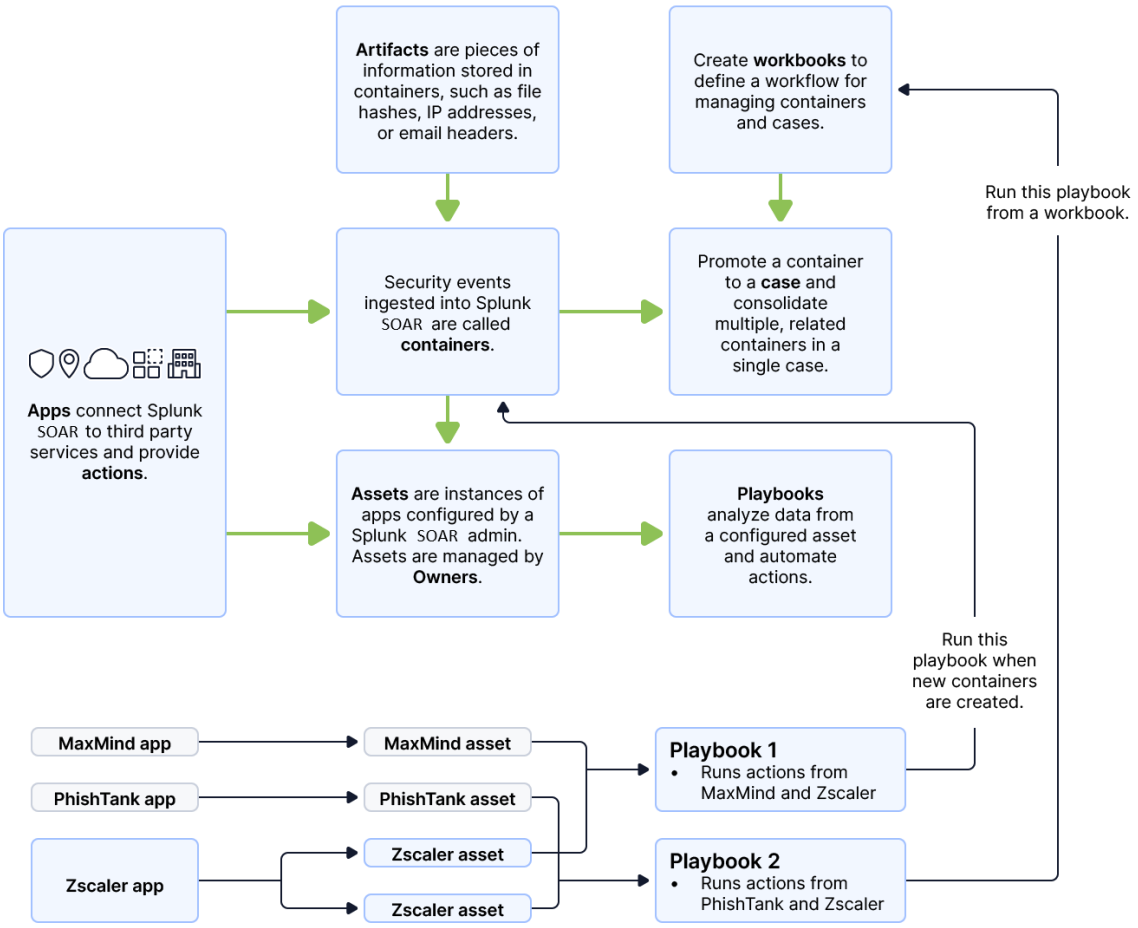

Figure 71. SOAR components

A Sample Playbook to Showcase Zscaler and SOAR Integration

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

In the example, ZIA NSS logs are streamed to Splunk (SIEM). SOAR 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 SOAR.

SOAR then checks to see if Zscaler currently classifies this domain as malicious. If Zscaler classifies this domain as malicious, SOAR triggers a search in NSS logs that were consumed by Splunk to look at historical data.

If Zscaler doesn't classify them as malicious, SOAR adds the domain to your ZIA denylist and then looks at historical data (with an adjustable time range) to find which users have accessed those domains by triggering a search over NSS logs that were consumed by Splunk.

SOAR then sends an email to the network admin detailing which users were exposed to these domains, along with relevant timestamps.

The following steps enable a SOAR instance to communicate with Splunk and Zscaler. Configure a sample playbook which is used to automate threat hunting. This sample playbook is just an example of what is achievable by leveraging SOAR abilities with Zscaler APIs. You can build your own playbooks to implement your custom use cases.

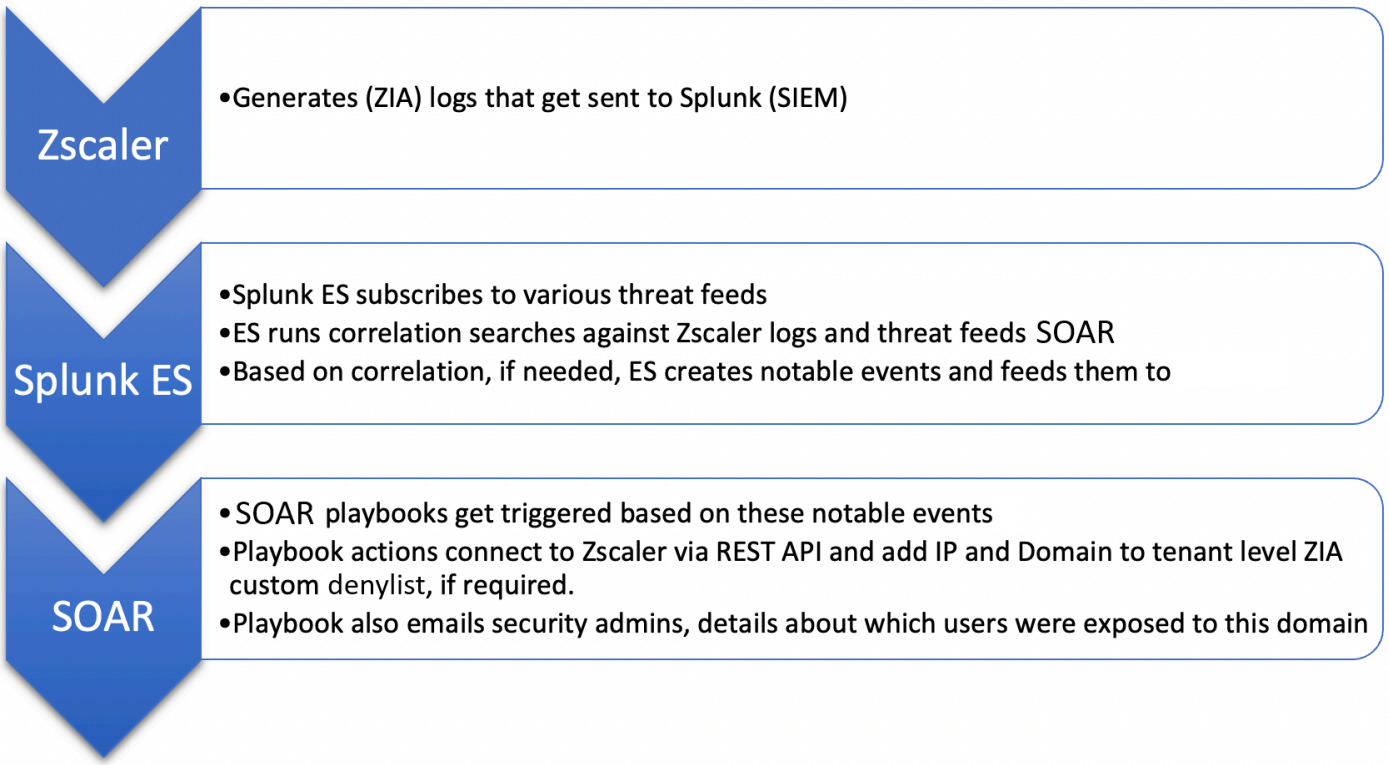

Figure 72. Zscaler and Splunk ES SOAR

Configuring SOAR

The following steps assume that you have admin access to the SOAR instance.

Create New Event Label in SOAR

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

Triggered events is a way to limit a playbook, specifying actions only on specific kinds of events.

1. Go to **Administration** > **Event Settings** > **Label Settings** and then **+ Label**.

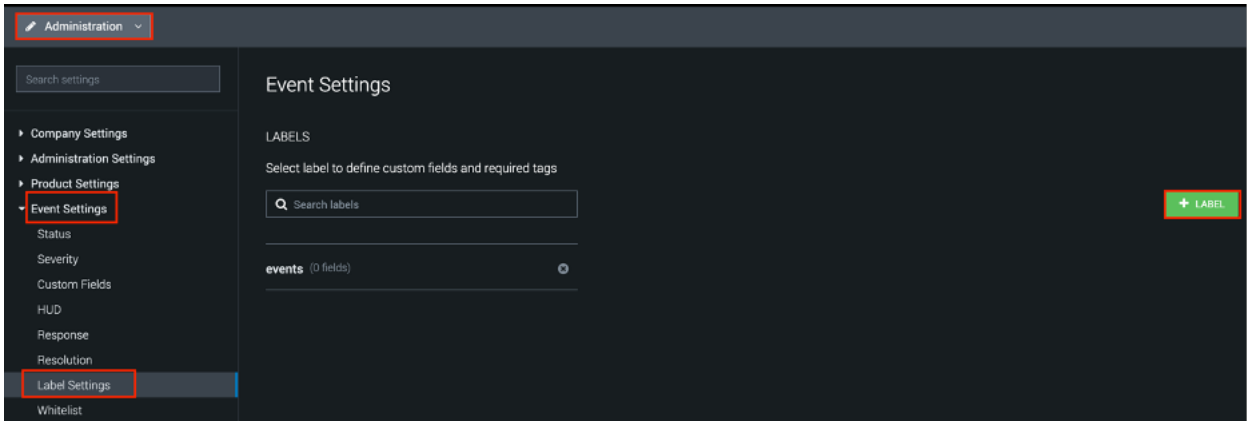

Figure 73. Create event label in SOAR

2. Enter `from_correlation_splunk_search`.

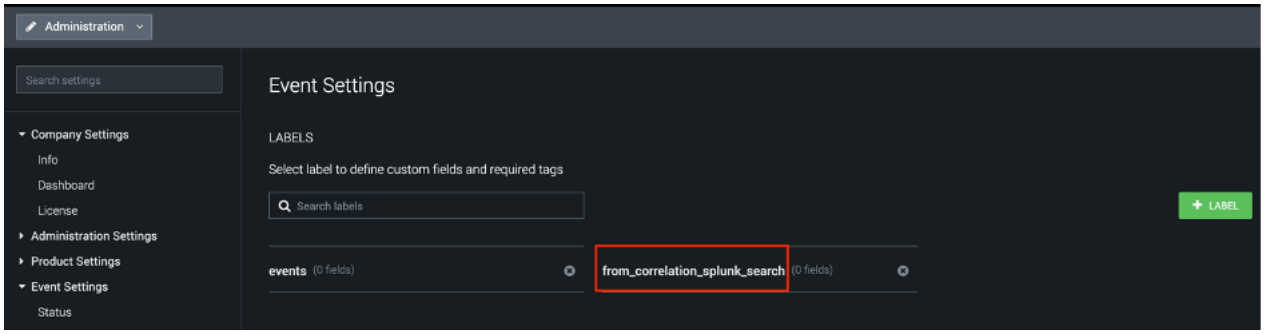

Figure 74. Create event label in SOAR

Create Automation User in SOAR

This username is used by Splunk to communicate with SOAR.

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

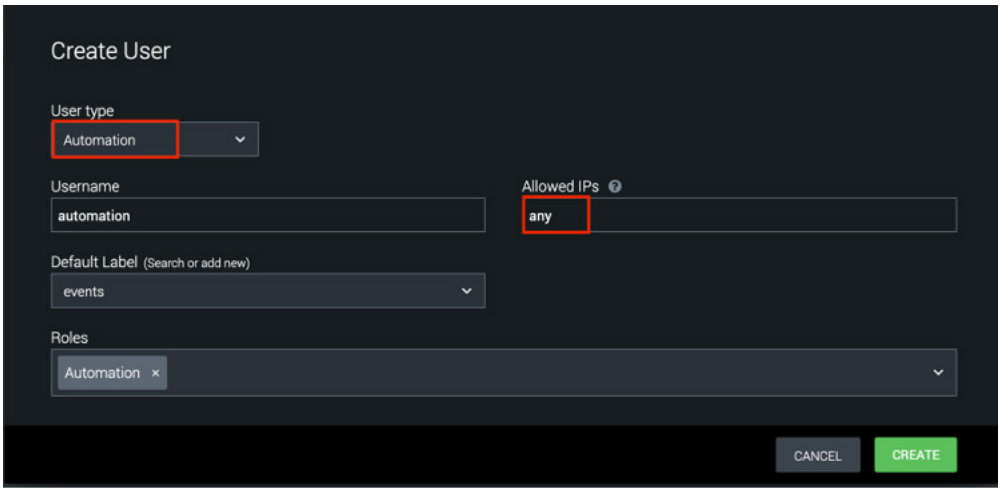

Figure 75. Create automation user in SOAR

2. Click the username created.
3. Copy the following section for your record. The Authorization Configuration for REST API is used by Splunk to authenticate with SOAR.

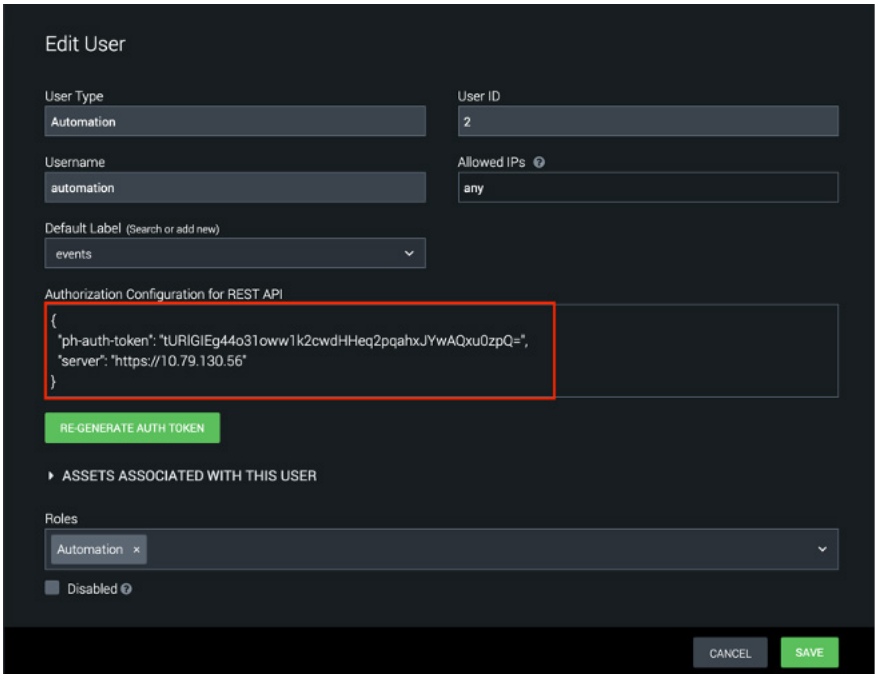

Figure 76. Copy code in Authorization Configuration for REST API

Installing Zscaler App on SOAR

Log in to SOAR and go to **Apps**.

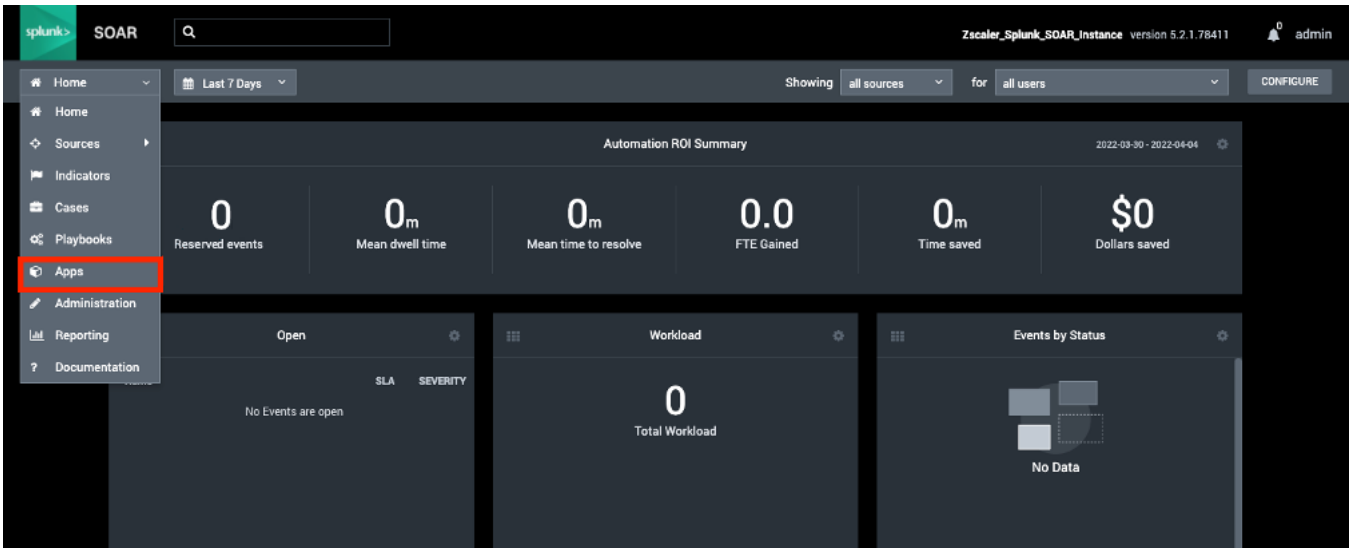

Figure 77. Go to Apps section in SOAR

Search for Zscaler App

Search for `zscaler`. Go to **Unconfigured Apps** > **Configure new Asset**.

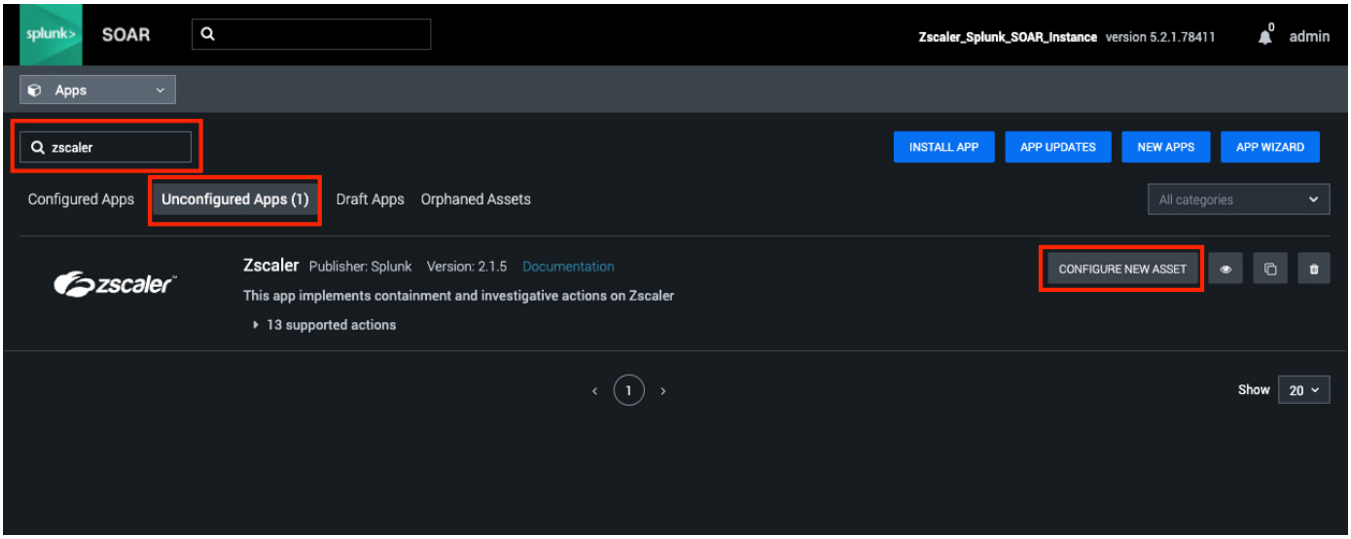

Figure 78. Search for Zscaler App in SOAR

Configure Zscaler App

The **Asset Info** tab allows free-form text input. Enter an asset **Name** according to your organization's naming conventions.

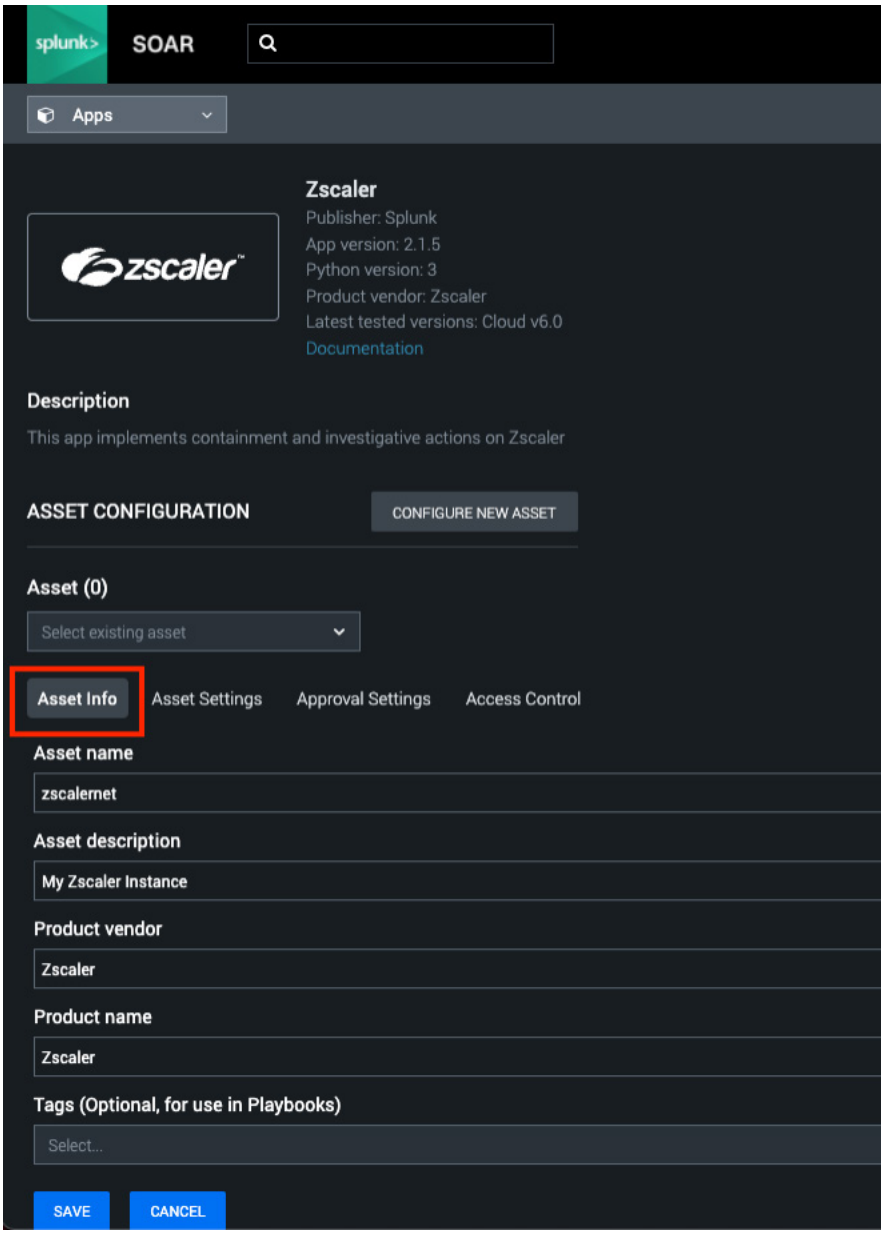

Figure 79. Configure Zscaler app in SOAR

Fill out **Asset Settings** with your pertinent ZIA tenant details.

After filling all the details, click **Save**, and then click **Test Connectivity**.

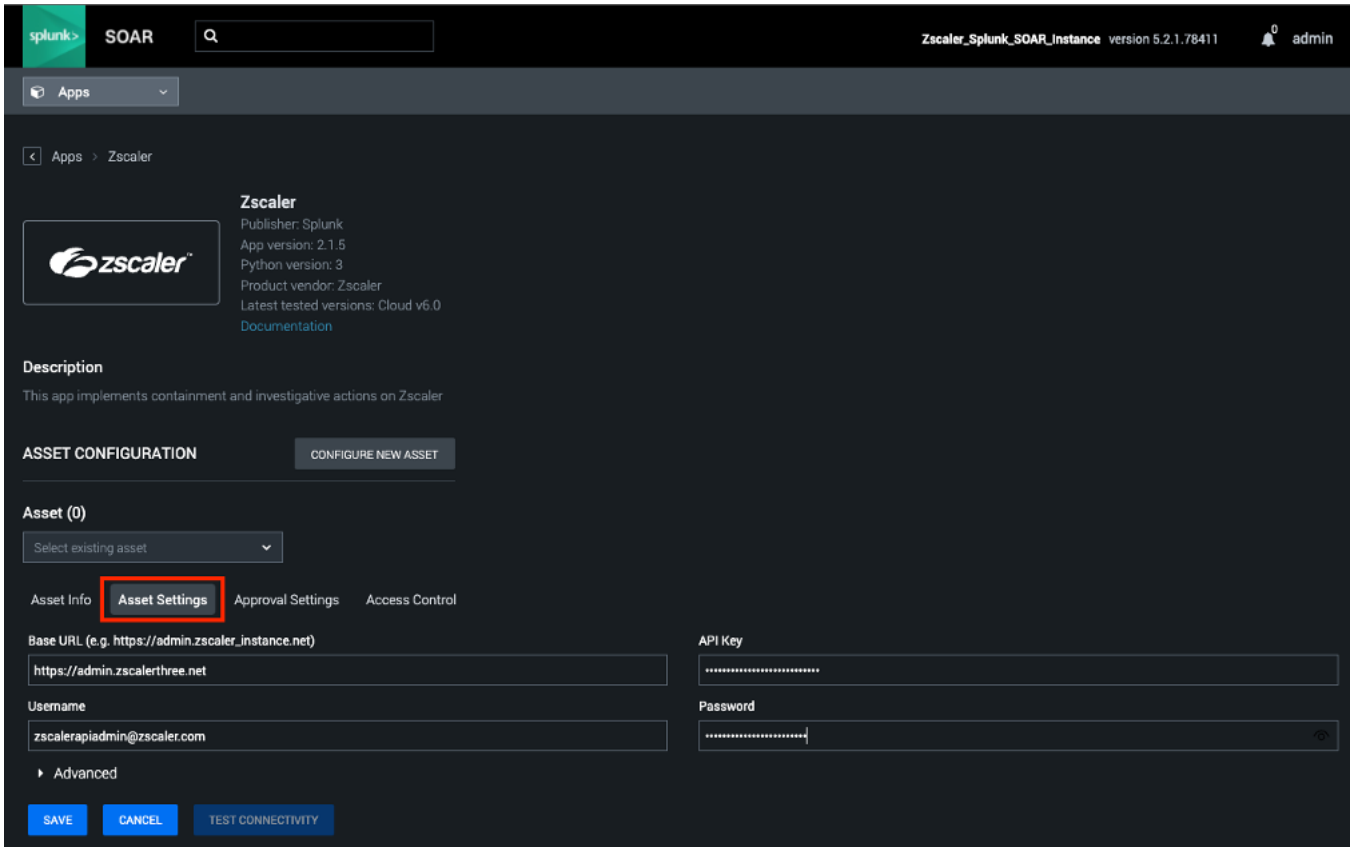

Figure 80. Configure Zscaler App in SOAR

Test Connectivity Between SOAR and Zscaler

When all the information is filled in correctly, the connectivity test passes and your result looks similar to the following example.

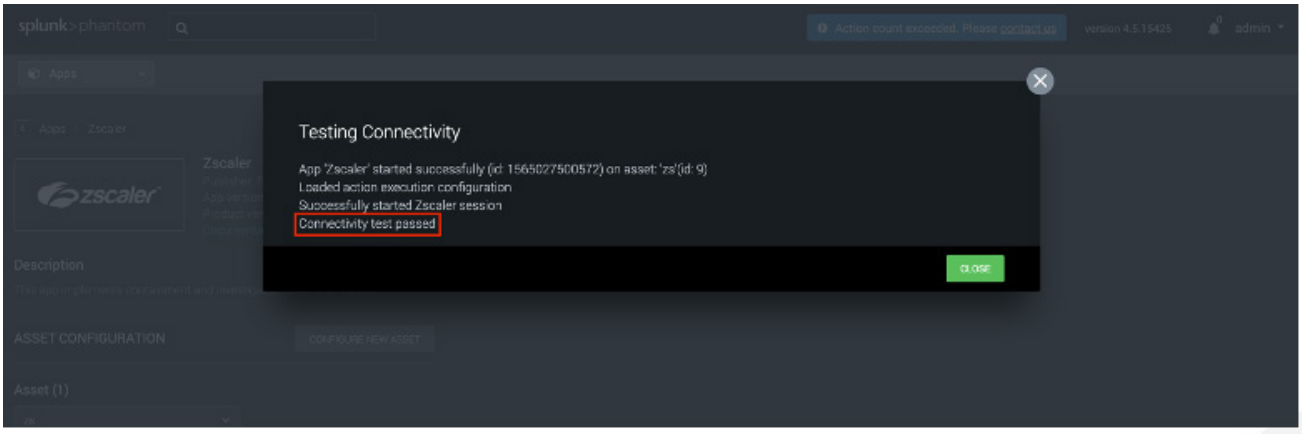

Figure 81. Test connectivity between SOAR and Zscaler

Installing Splunk App on SOAR

Click **Apps** to display the available apps in Splunk SOAR.

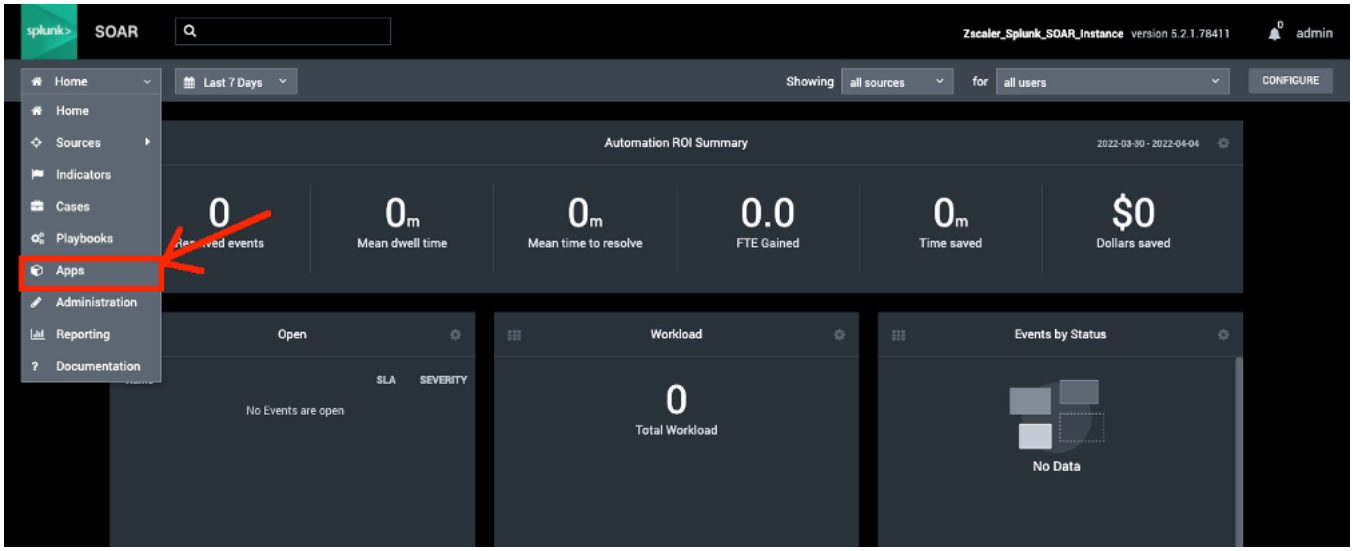

Figure 82. Install Splunk app

Search for Splunk App

Search for `splunk`.

Go to **Unconfigured Apps** > **Configure New Asset**.

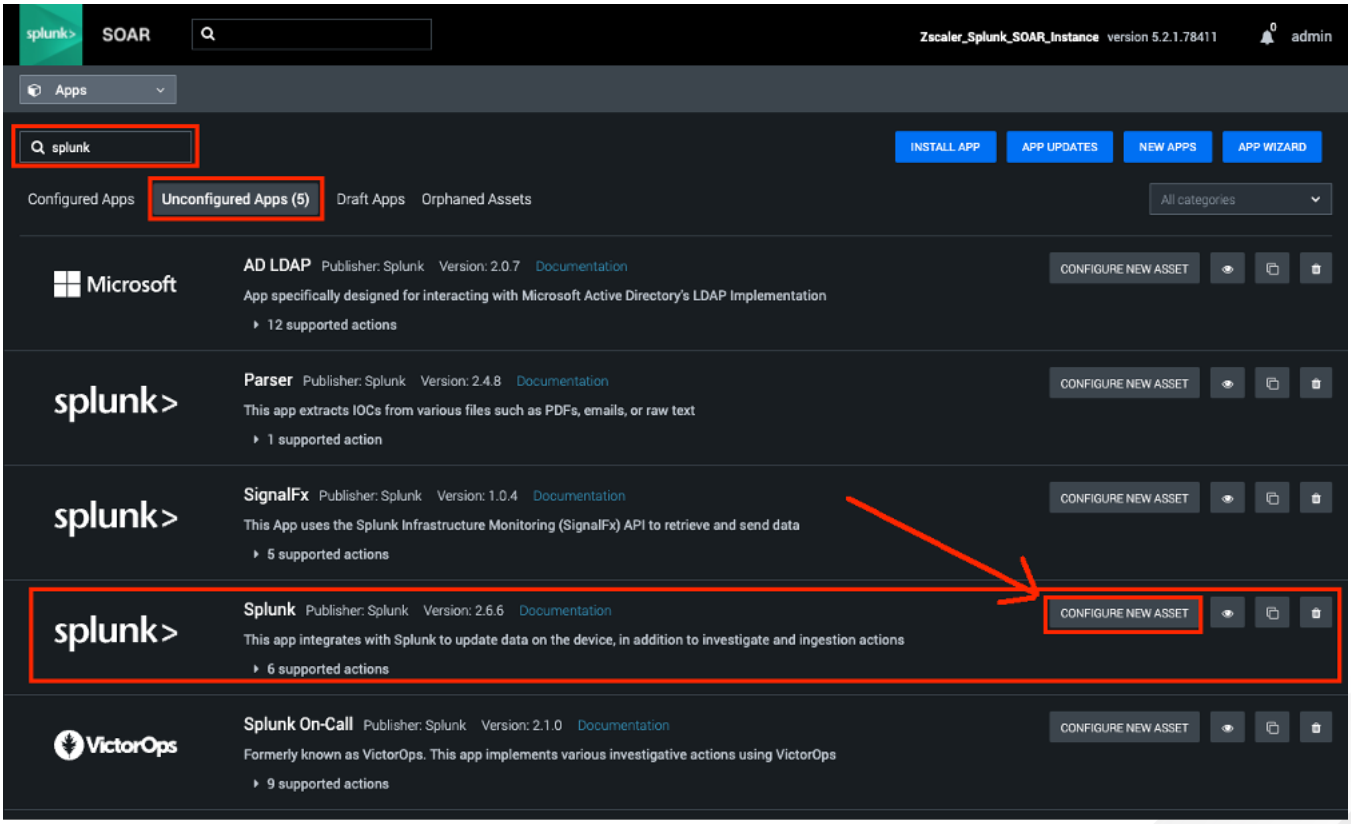

Figure 83. Configure new asset

Configure Splunk App

The **Asset Info** tab allows free-form text input. Enter an **Asset name** using your organization's naming conventions..

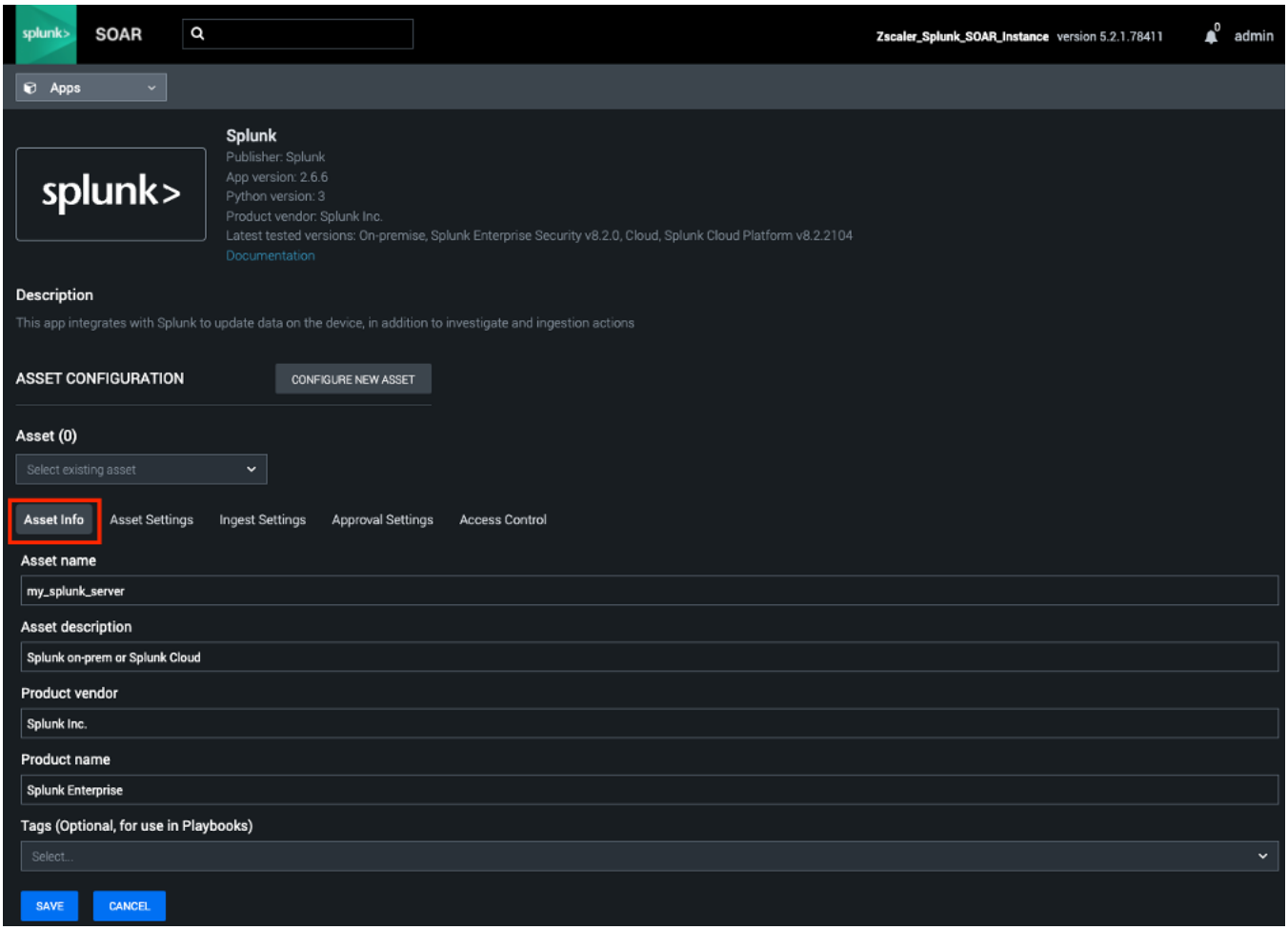

Figure 84. Configure asset info

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

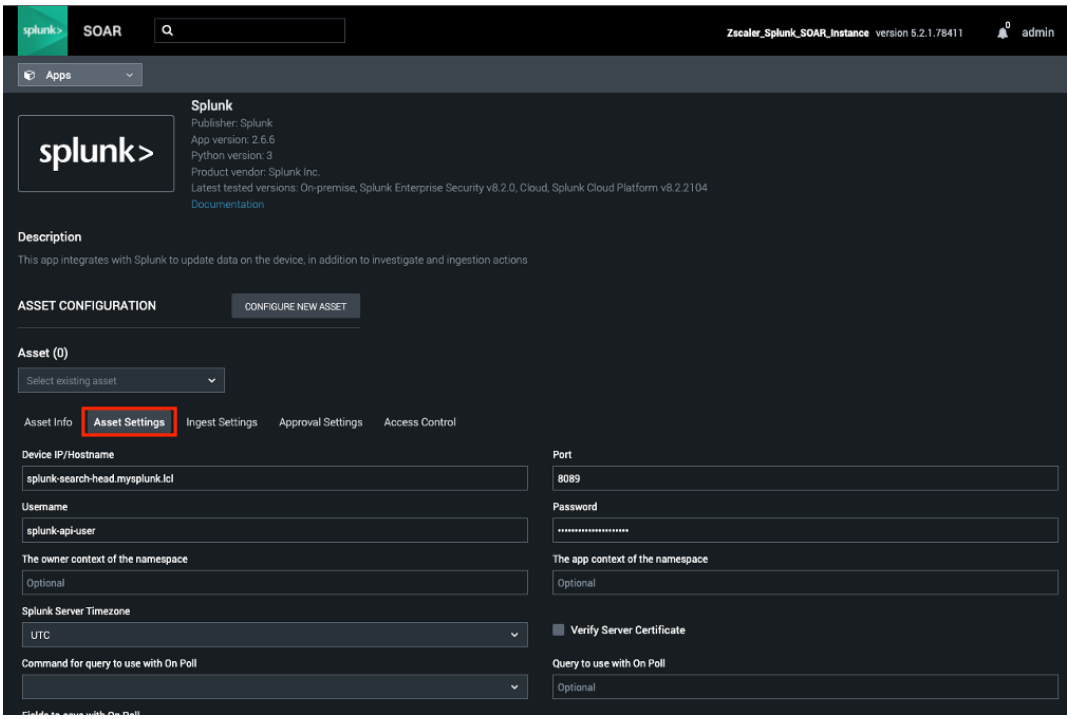

Figure 85. Configure Splunk app in SOAR

Under **Ingest Settings**, set the **Polling Interval** per your operational needs. In the following figure, the **Polling Interval** is set to 5 minutes.

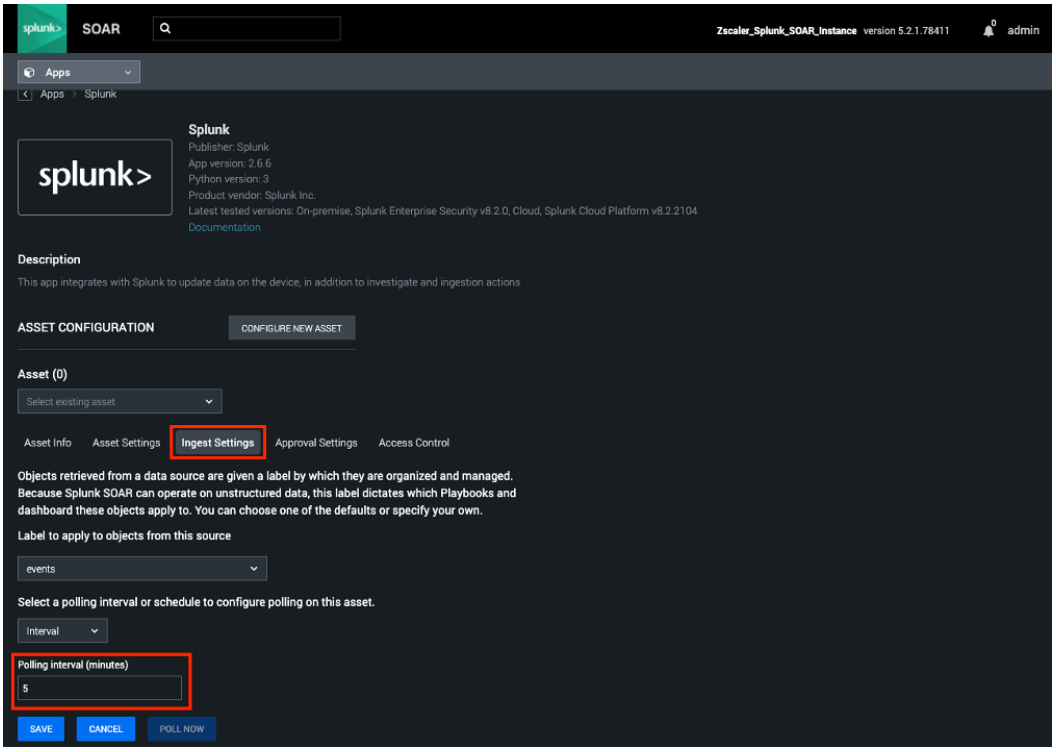

Figure 86. Configure polling interval

Test Connectivity Between SOAR and Splunk

When all the information is filled in correctly, the connectivity test passes and your result looks similar to the following example.

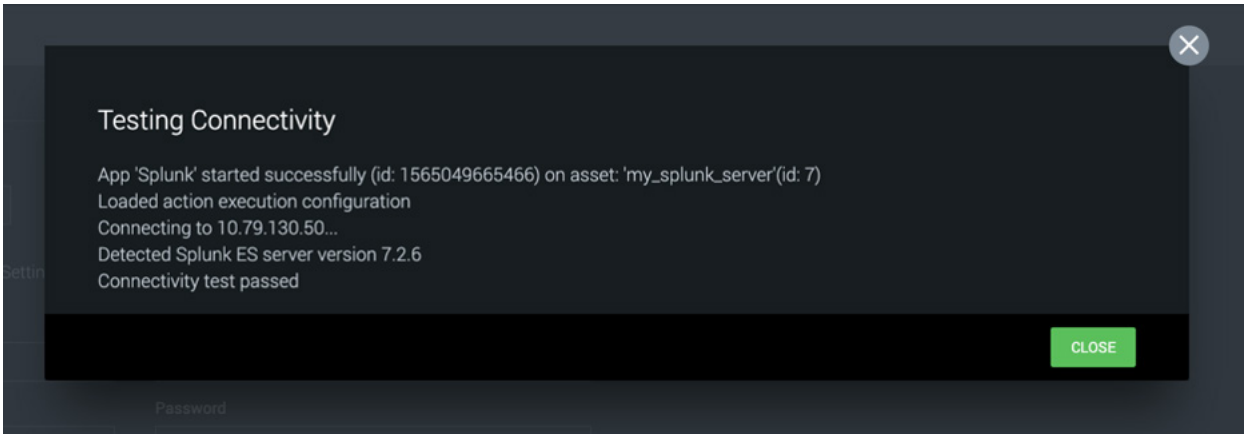

Figure 87. Test connectivity between SOAR and Splunk

Download Zscaler Playbook

Download the Zscaler playbook (as a .tar file) using this link and import it into your SOAR instance.

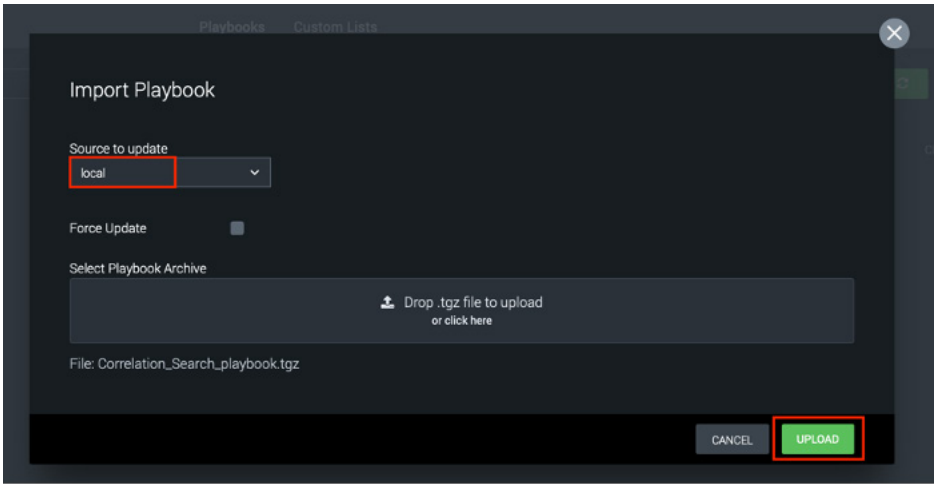

Figure 88. Upload sample playbook to SOAR

This playbook does a correlation search against known malicious IPs and domains and your 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 denylist.

If it is, then no action is taken.

If it is not on the denylist, SOAR checks how Zscaler classifies this IP and domain. If Zscaler classifies it as *Unknown*, SOAR updates Zscaler's denylist via an API call..

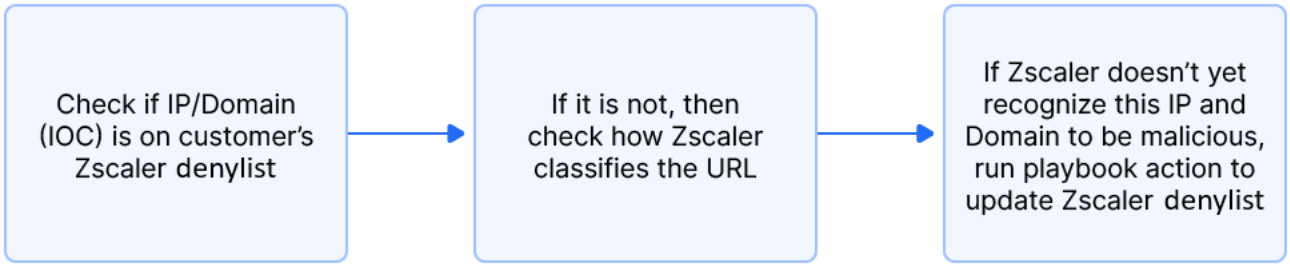

Figure 89. Playbook process

Edit the Playbook Settings

Go to Playbooks and open the one that was imported. Edit the Playbook Properties and mark it as **Active**.

Also change **Operates on** to the label that was created earlier in the drop-down menu and click **Save**.

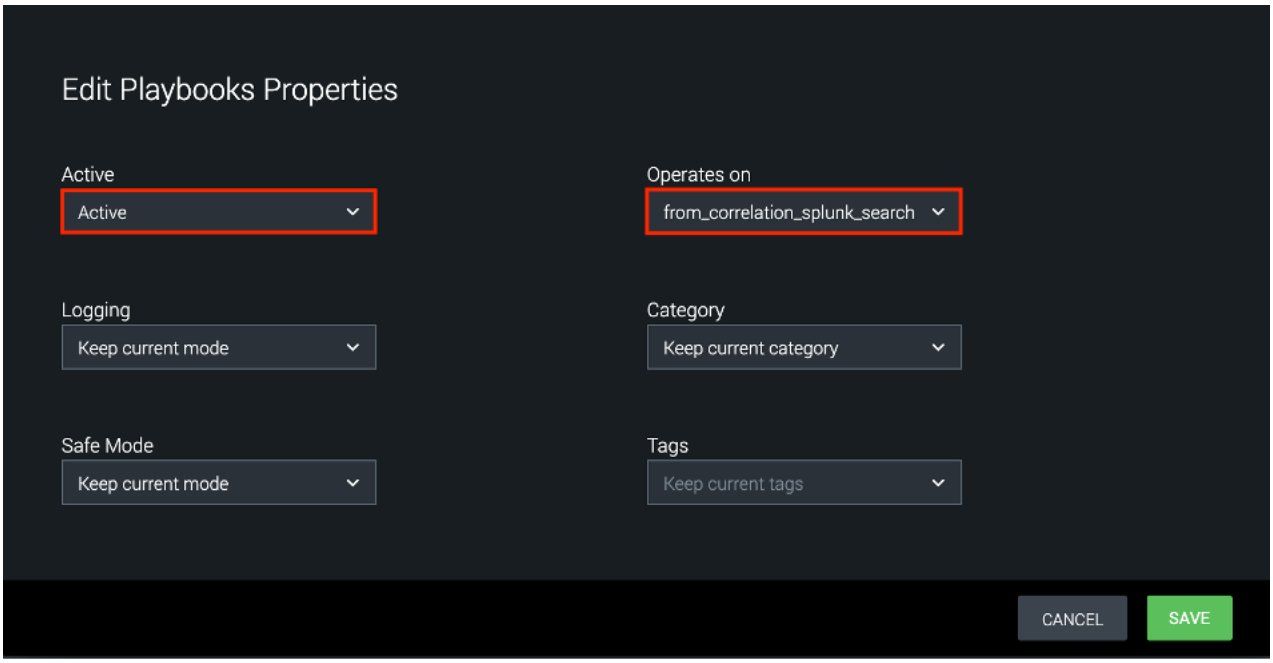

Figure 90. Change playbook status to active

Configuring Splunk

The following sections describe how to configure Splunk.

Install Splunk ES App

After logging in to your Splunk instance, click **Splunk Apps** and search for `enterprise security`.

Install the Splunk ES app.

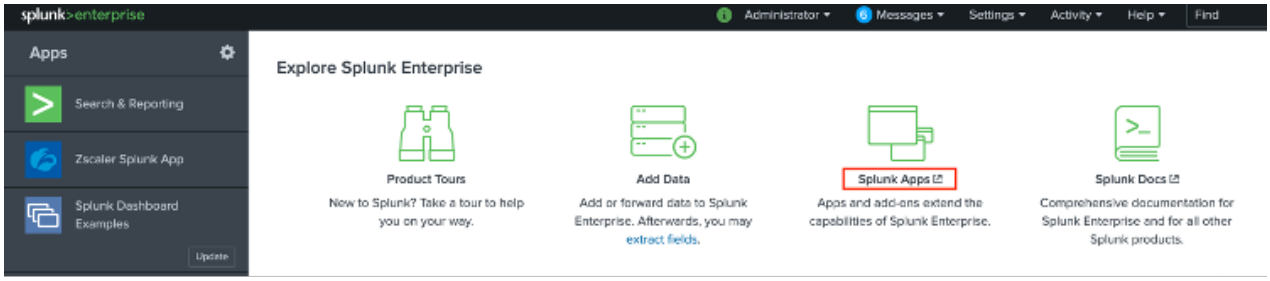

Figure 91. Splunk ES app

The following image shows a search and install for Splunk Enterprise Security.

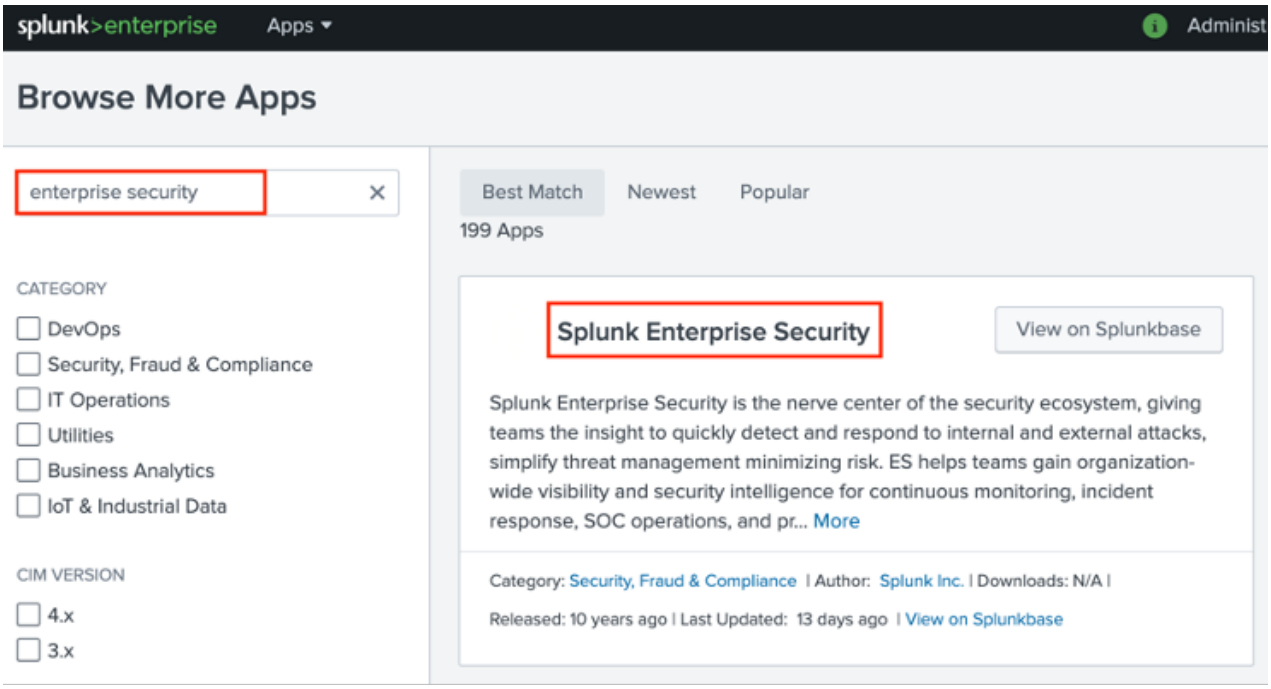

Figure 92. Search and install Splunk Enterprise Security

Manage Threat Intelligence Within ES App

Go to the newly installed **Enterprise Security** Splunk app and then click **App Configuration**.

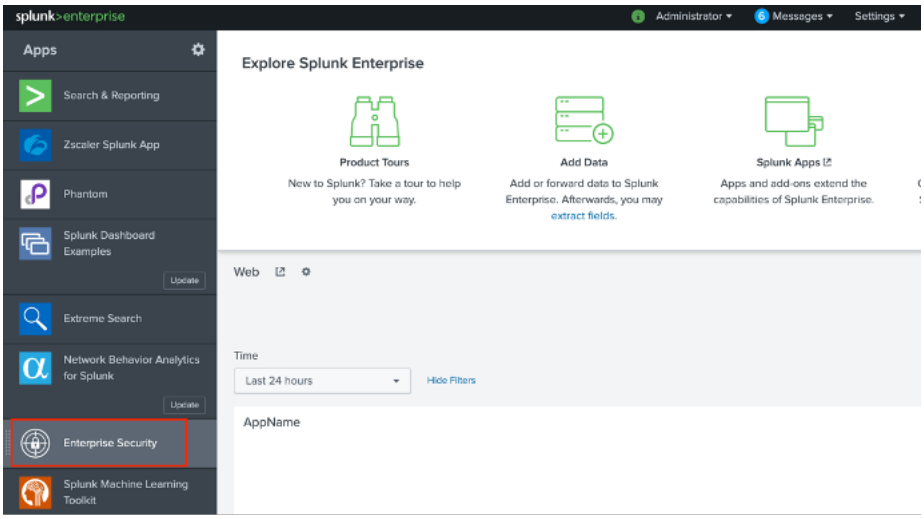

Figure 93. Splunk enterprise security

The following image shows the Splunk enterprise security app configuration.

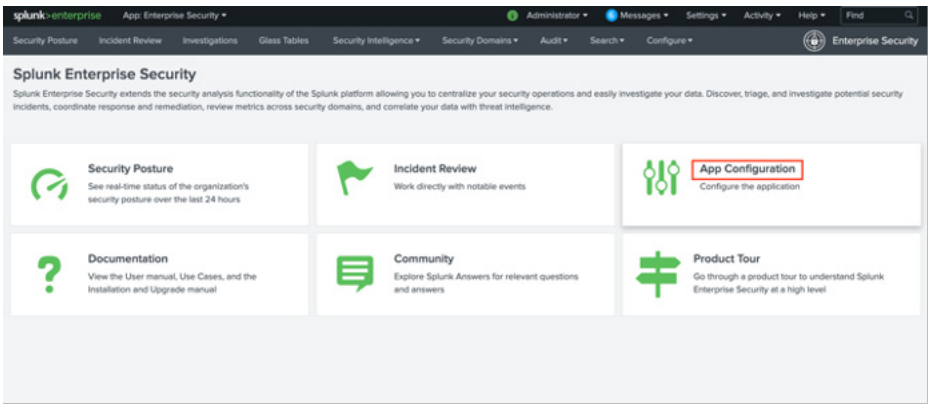

Figure 94. Splunk enterprise security app configuration

Click **Content Management**.

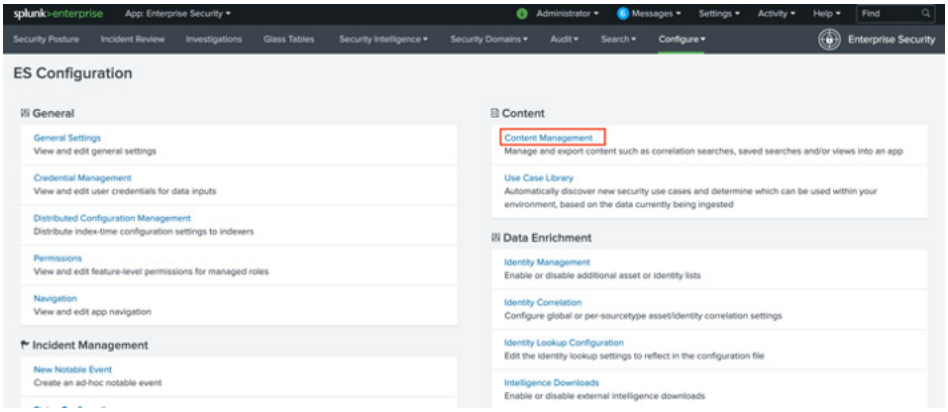

Figure 95. Content management in Splunk ES

Enter `Threat` in the search box and select the **Type** as **Correlation Search**.

Enable the **Threat Activity Detected** correlation search.

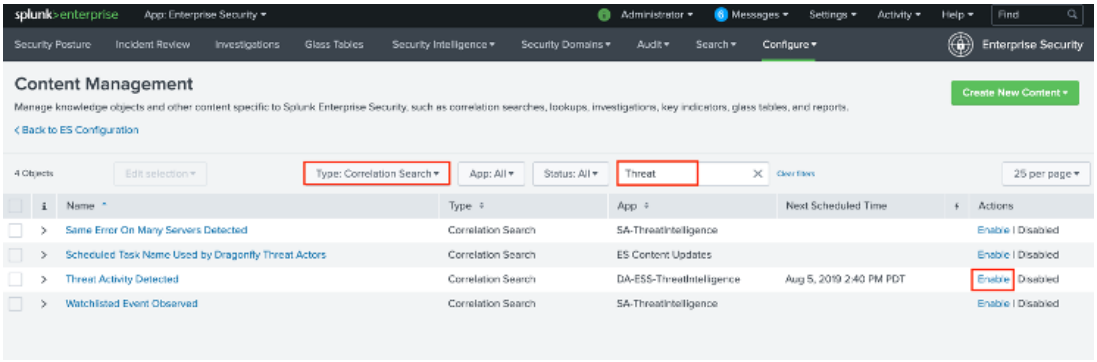

Figure 96. Threat activity search

After enabling, click **Threat Activity Detected**.

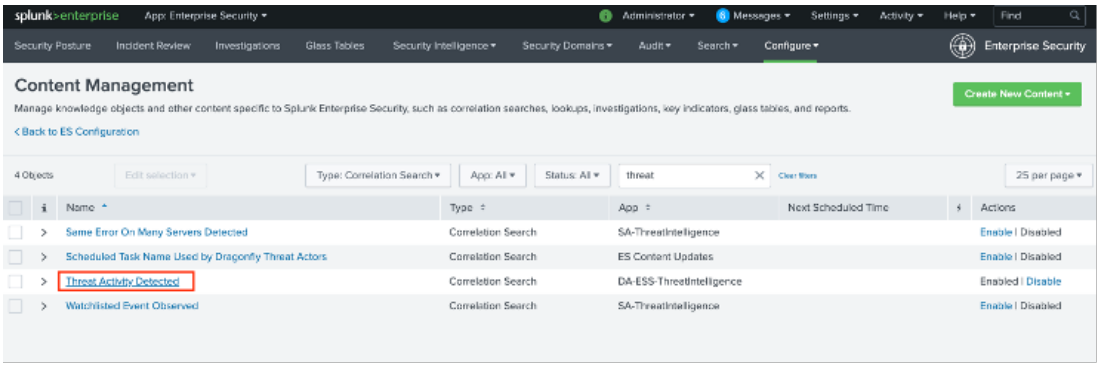

Figure 97. Enable Threat Activity Detected correlation

The following window is displayed.

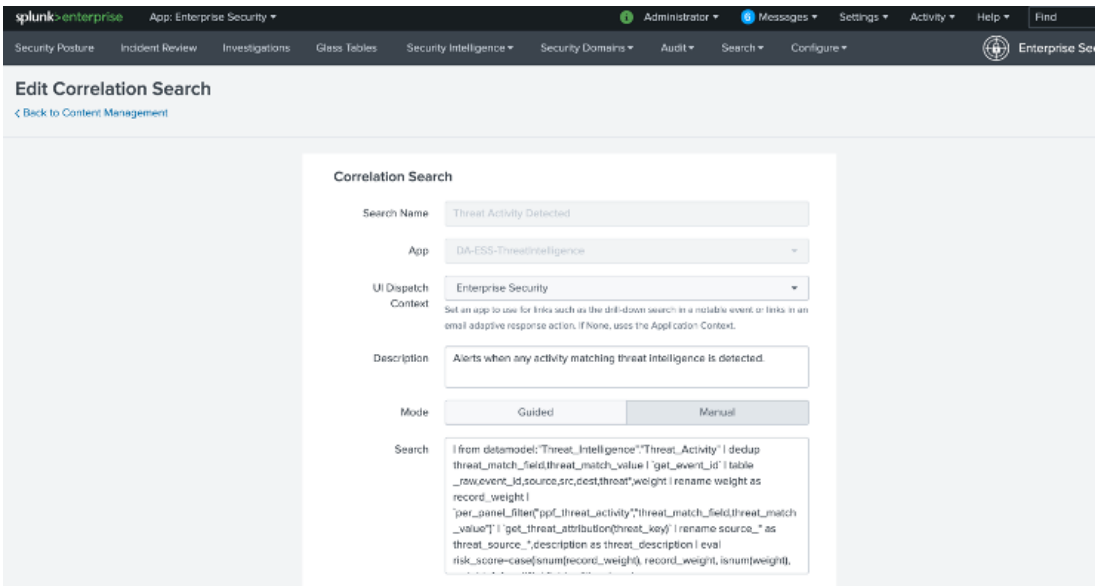

Figure 98. Correlation search

Notable Events and Forwarding to SOAR

When you scroll to the bottom of this page, the **Notable** and **Risk Analysis** actions are selected by default. Click **Add New Response Action** and add **Send to SOAR**.

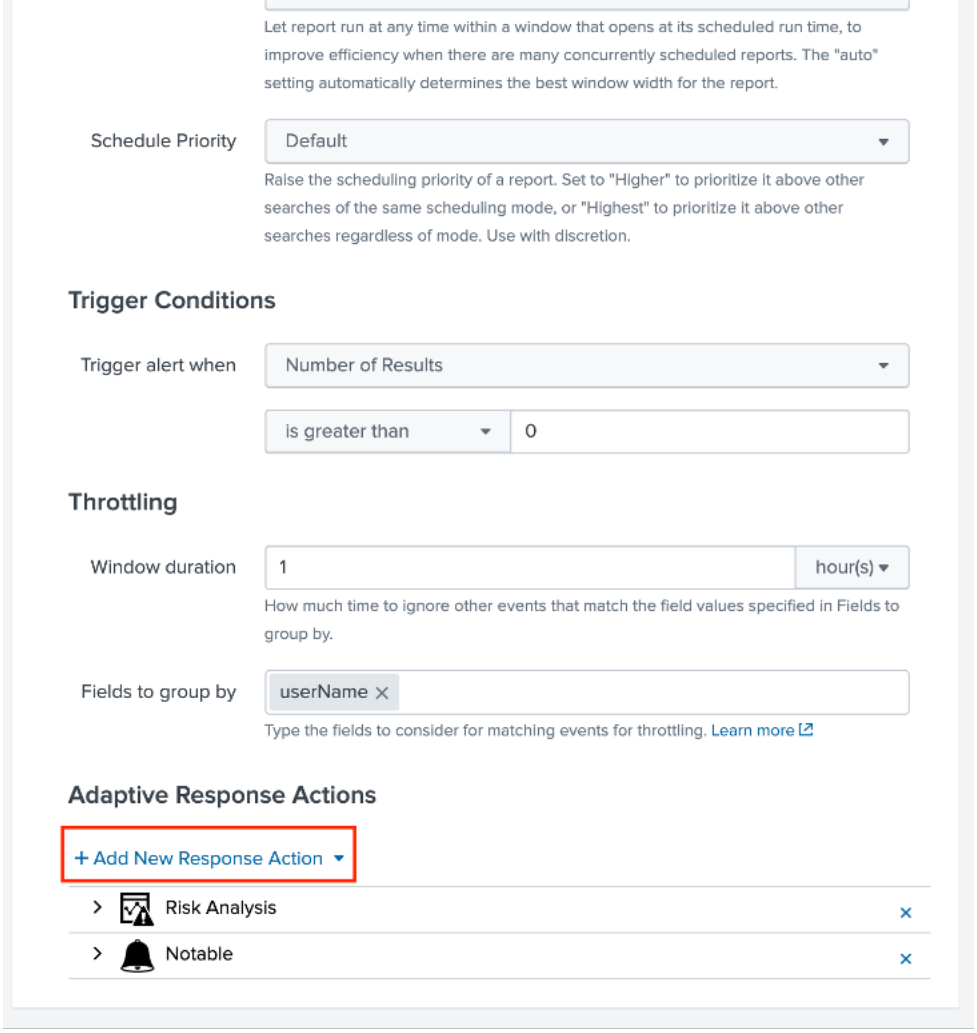

Figure 99. Add adaptive response action in SOAR

Notable events are automatically created by Splunk ES based on correlation searches. Add an action to forward artifacts related to such events to your SOAR setup.

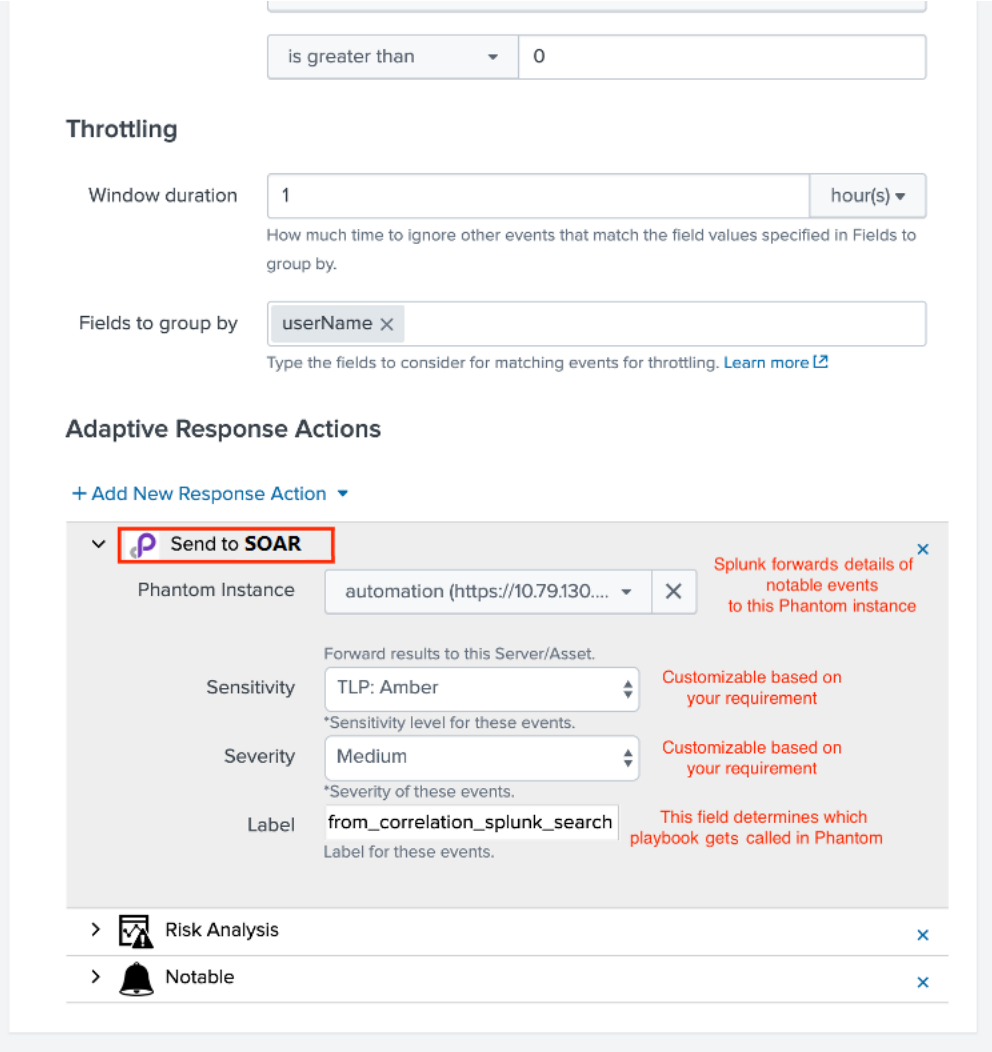

Figure 100. Forward notable events to SOAR

Install SOAR App

Install the SOAR App on Splunk. SOAR IP is defined here and Splunk forwards artifacts to this SOAR instance.

Click **Splunk Apps**.

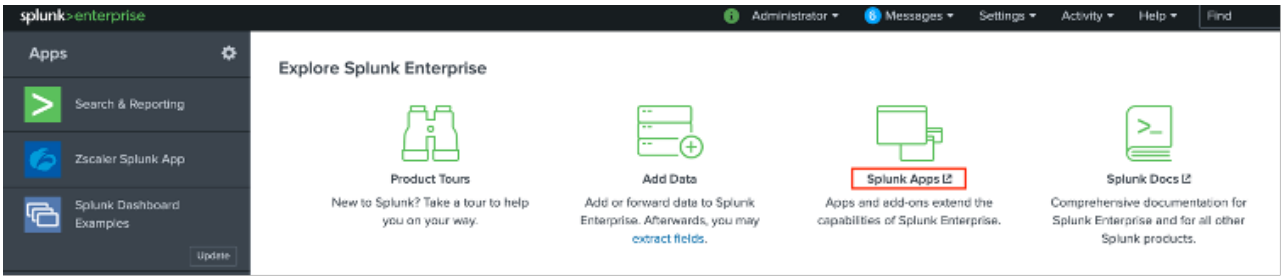

Figure 101. SOAR App for Splunk

The following image shows SOAR app in Splunk.

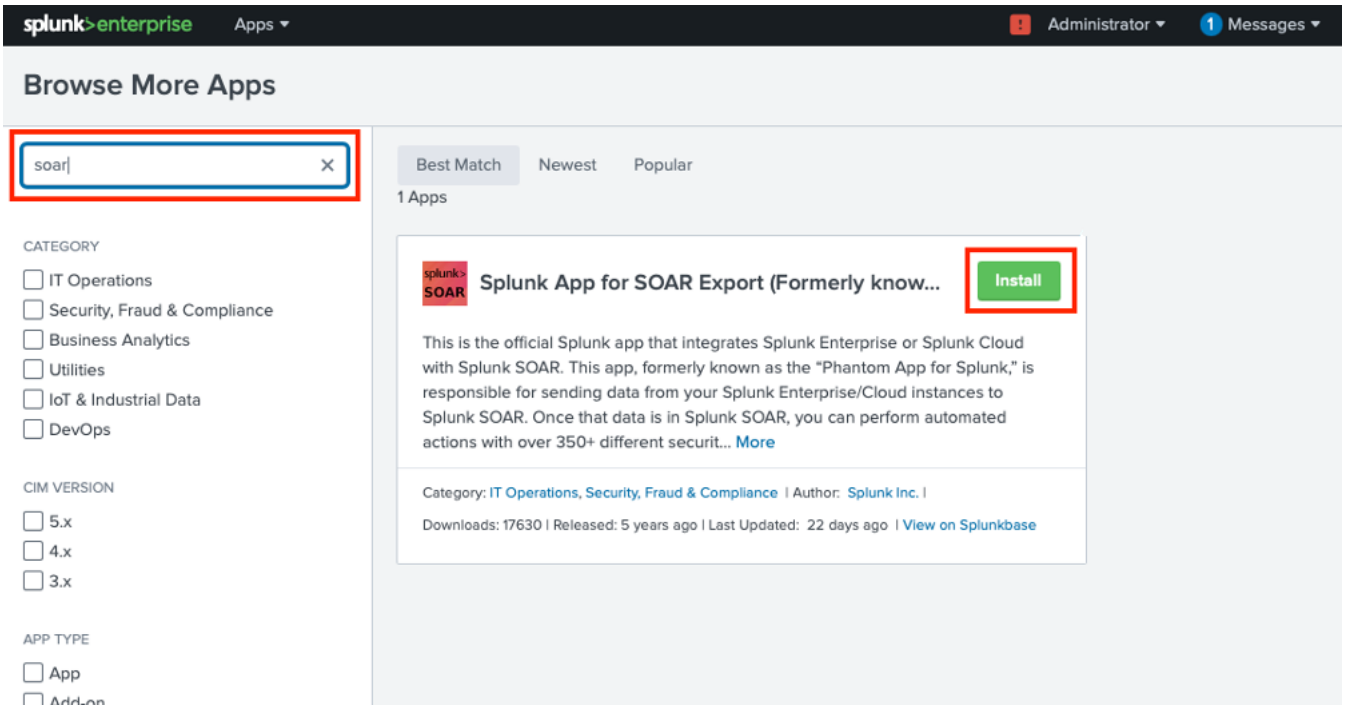

Figure 102. Install SOAR app in Splunk

Configure Automation User

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

Go to the newly installed SOAR Splunk App and then click **Create Server**.

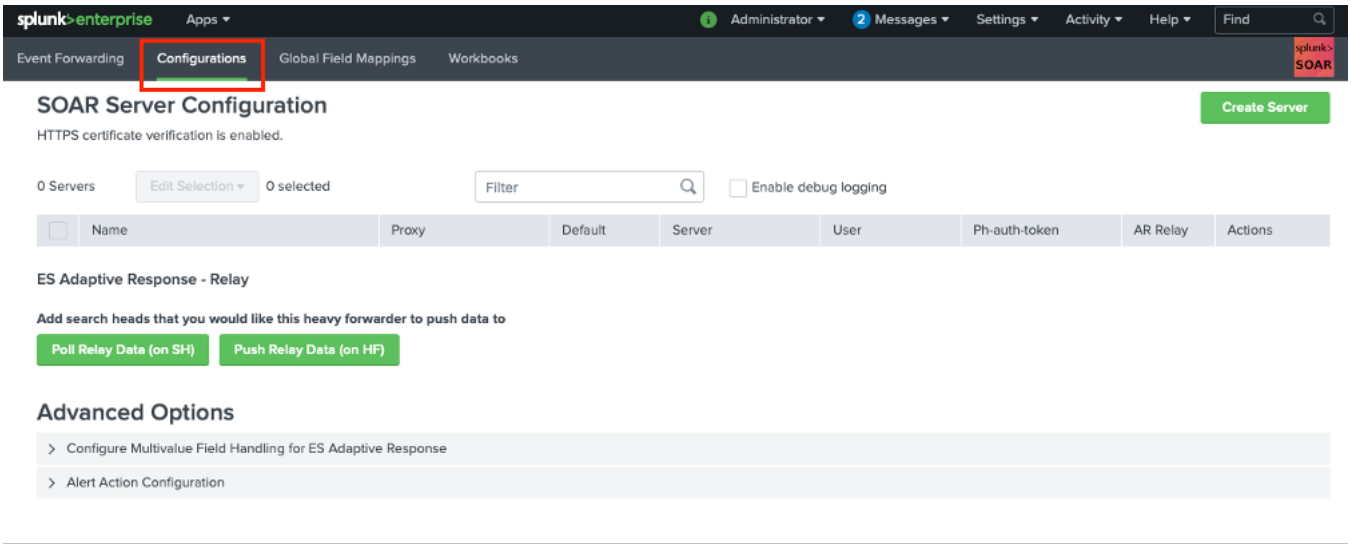

Figure 103. SOAR server configuration

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

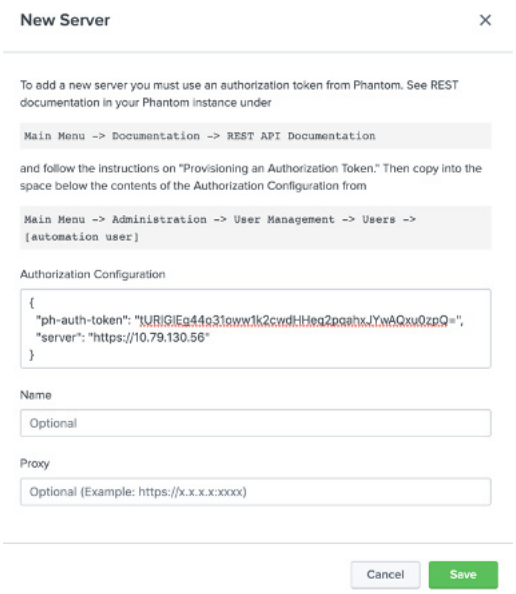

Figure 104. New SOAR server credentials

You see a confirmation dialog.

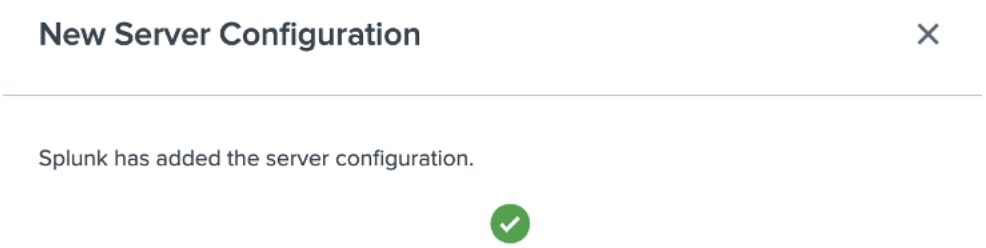

Figure 105. SOAR server verification

Verify Events in SOAR

Log back in to SOAR. You start seeing events being populated. It might take up to 30 minutes for events to display. These events trigger the SOAR playbook.

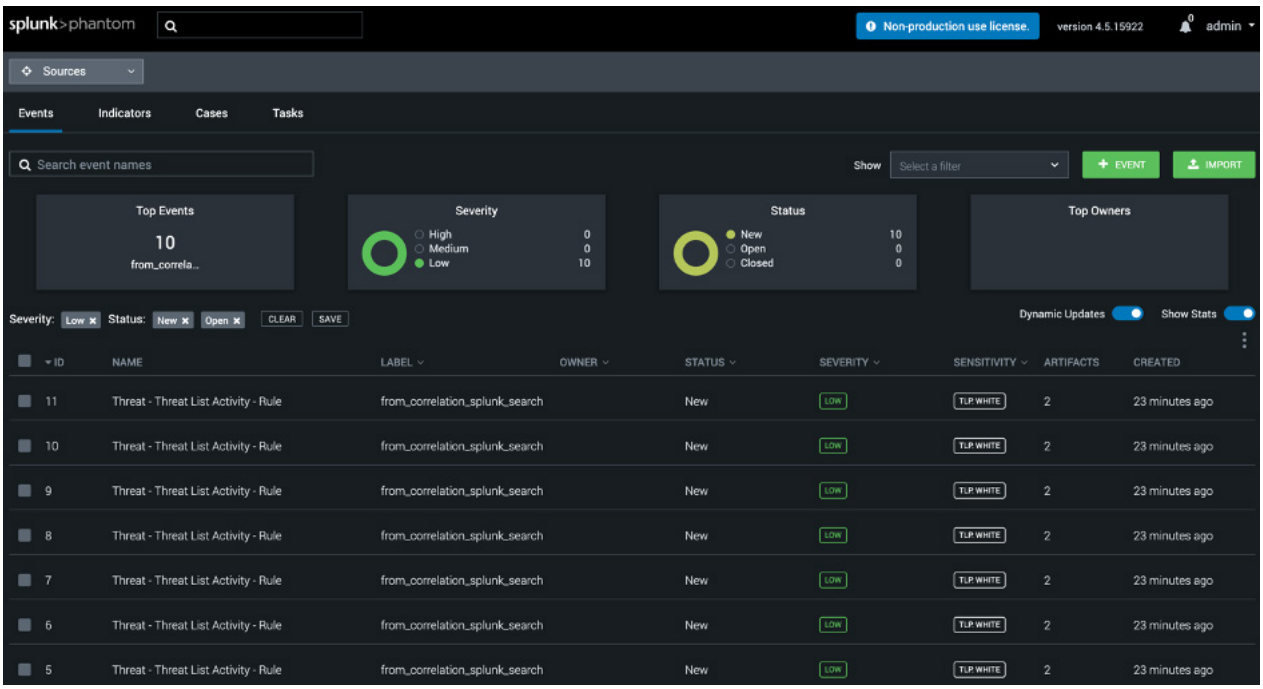

Figure 106. Verify that the notable events are being forwarded by Splunk to SOAR

Inspect Actions Taken by SOAR

Clicking any of these events displays pertinent playbook runs. A playbook lists all the actions invoked with the success or failure status.

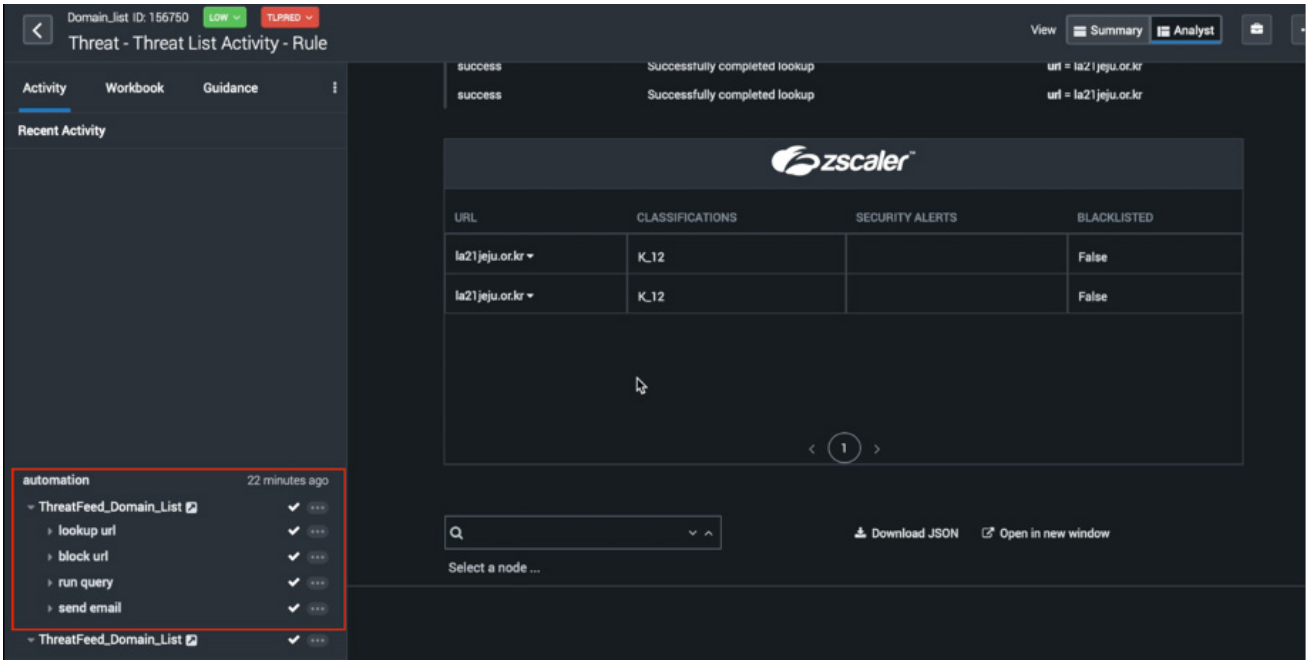

Figure 107. Verify playbook runs and actions taken

Appendix E: Posture Control and Splunk

Posture Control is a Cloud-Native Application Protection Platform (CNAPP) that takes a radically new approach to cloud native application security with a 100% agentless solution that correlates across multiple security engines to prioritize hidden risks caused by misconfigurations, threats, and vulnerabilities across the entire cloud stack, reducing cost, complexity, and cross-team friction.

Posture Control is part of Zscaler for Workloads, a comprehensive cloud security solution for any application running on any service in any cloud.

Figure 108. ZPC and Splunk integration

Create AWS S3 Bucket

Zscaler Posture Control (ZPC) exports its alerts to an S3 bucket. These alerts are then ingested into Splunk by Splunk reading the contents of that S3 bucket via a generic Splunk S3 input. The first step is to log in to AWS console and create an S3 bucket to which ZPC exports the alerts.

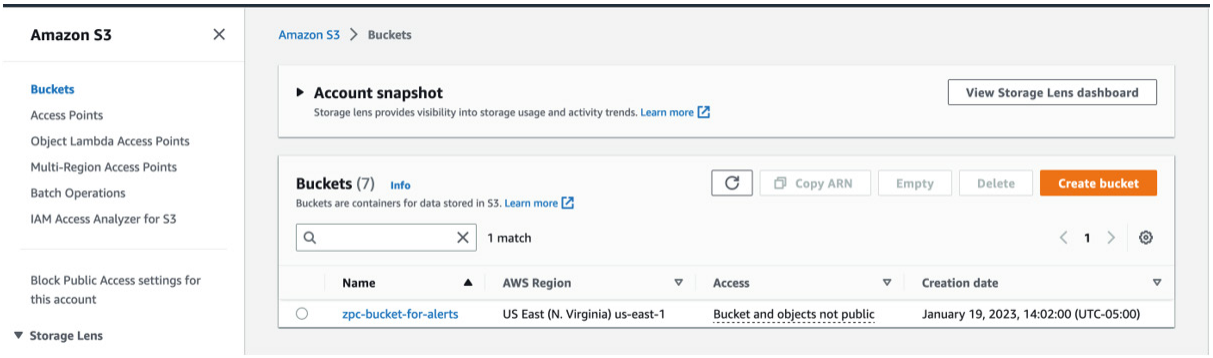

Figure 109. Amazon S3 Buckets

Configuring ZPC to Send Alerts to AWS S3

To configure ZPC to sent alerts to AWS S3 buckets:

1. Log in to the ZPC Admin Portal. Go to **Administration** > **Integrations**.

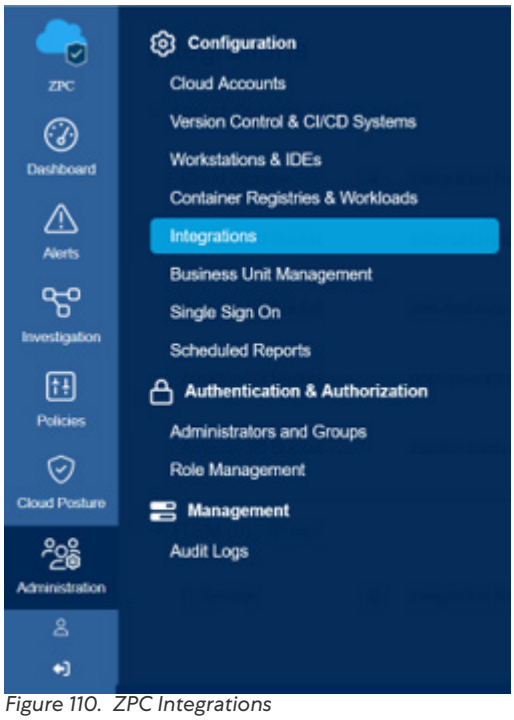

Figure 110. ZPC Integrations

2. Click **Add** to enter a new cloud storage integration, which is used as a location to store alerts.

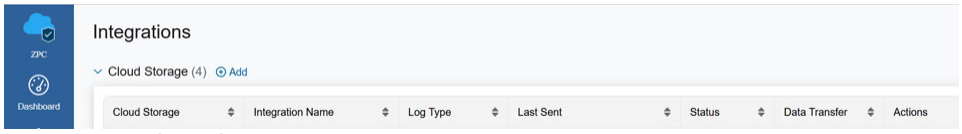

Figure 111. Add Cloud Storage

3. Enter the integration **Name** and select **Amazon S3 Bucket** as the **Cloud Storage**.

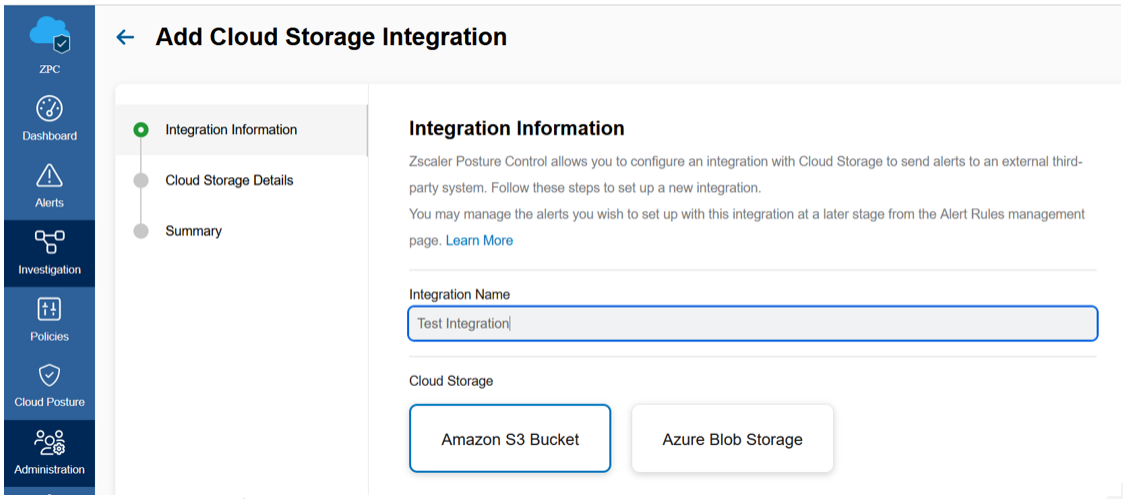

Figure 112. Integration Information

4. Enter the **AWS S3 Bucket Name** to which ZPC should push alerts.

5. Click **Copy the S3 Bucket policy** and log in to the AWS S3 portal.

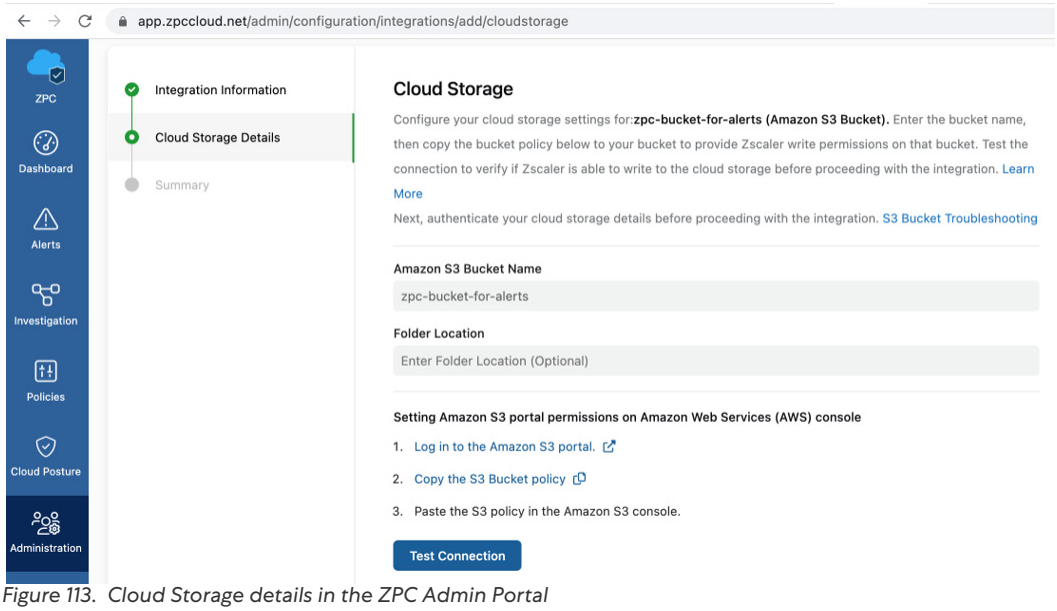

Figure 113. Cloud Storage details in the ZPC Admin Portal

6. Paste the bucket policy in to the permissions of the bucket. The bucket policy looks similar to the following example.

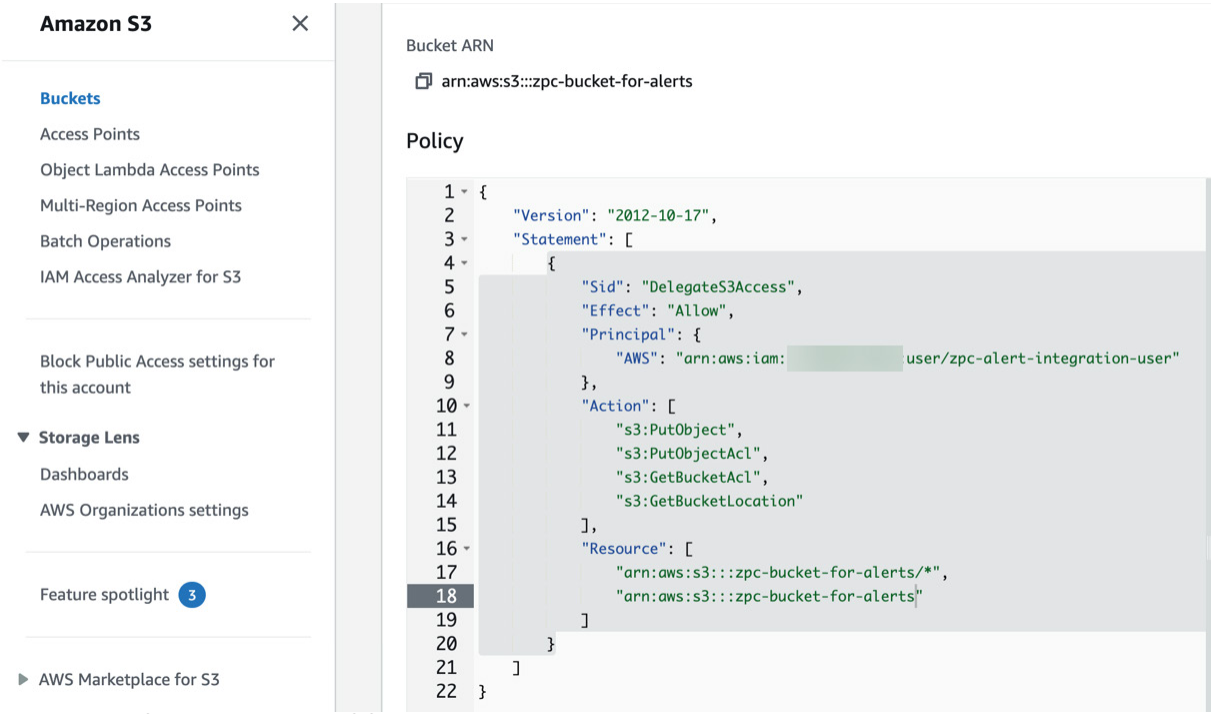

Figure 114. AWS Bucket Policy in AWS S3 portal

7. Return to the ZPC Admin Portal and click **Test Connection**. The connection test must succeed before moving to the next step.

Configuring AWS

ZPC writes alerts to this S3 bucket in AWS, and Splunk reaches out to this S3 bucket to pull down the alerts written to this bucket.

To create an Identity and Access Management (IAM) user and assign permissions to that user in AWS to allow listing of S3 buckets:

1. Click **Add Users**.

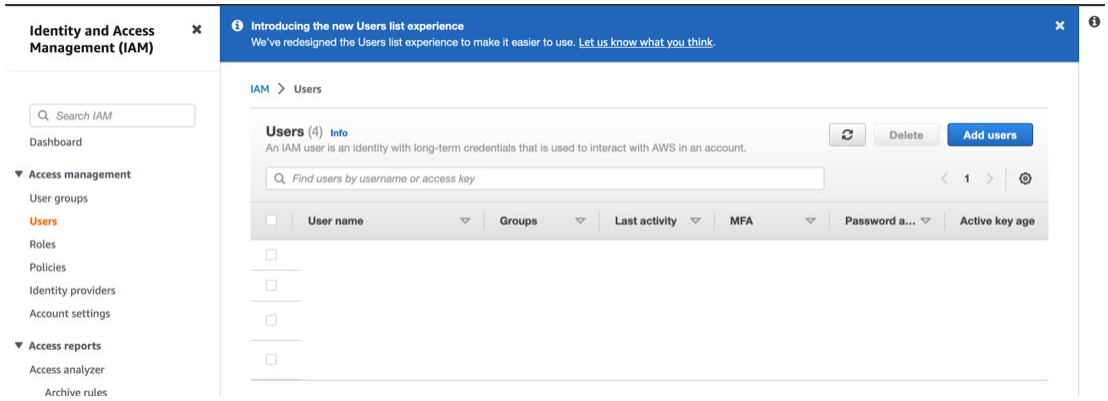

Figure 115. AWS Add Users

2. Enter a username and select **Access Key**. You can download the access key, which is used later by Splunk to pull contents of this S3 bucket into Splunk.

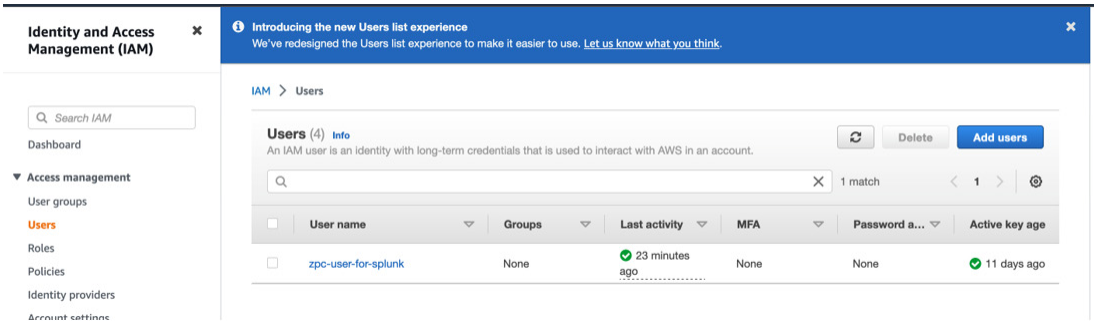

Figure 116. IAM Users

3. Create and attach an IAM policy to the user. This policy allows the Splunk user account to see all the buckets available when configuring Splunk. In the following example, a similar policy must be created in AWS and attached to the user.
4. Click **Next**.

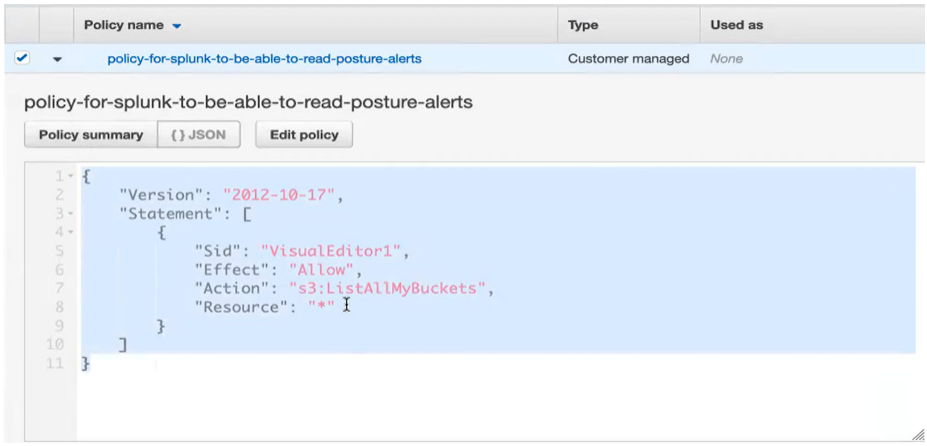

Figure 117. IAM Policy

5. After the user is created, create Access Keys to enable programmatic access using those credentials. Splunk uses the credentials to contact S3. Create and download an **Access key** and corresponding **Secret access key** for this user.

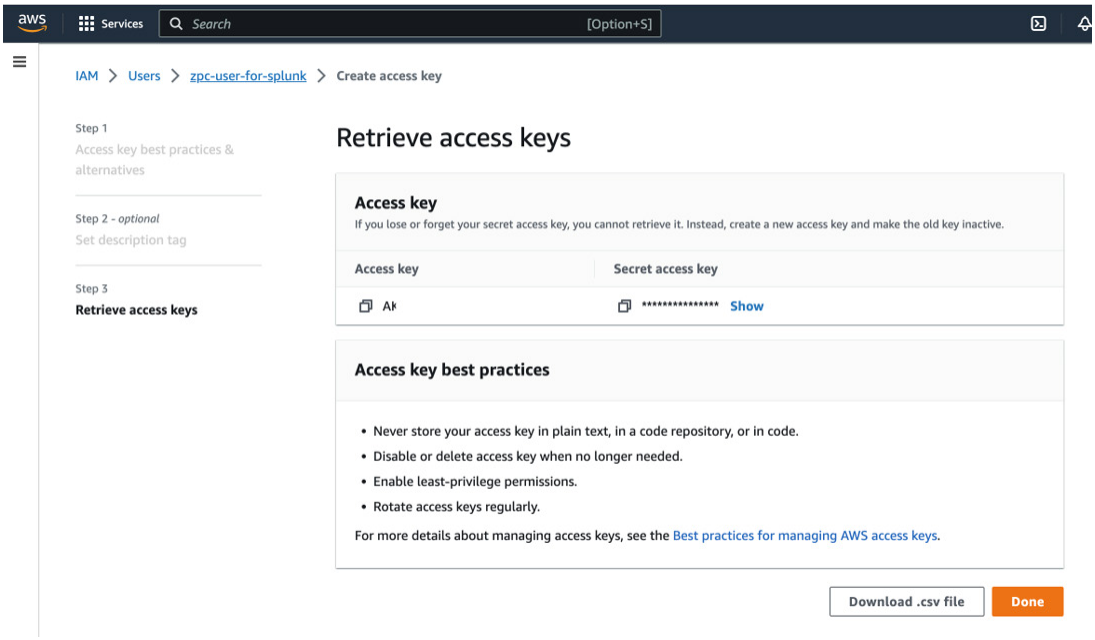

Figure 118. Access keys

6. Edit the permissions of the bucket so that the user can read from that bucket. You must make changes to the **Principal** and **Resource** sections to match your accounts and usernames. The end result is an addition of a stanza in the bucket permissions pertaining to the username that is used by Splunk to pull down the alerts from S3 bucket.

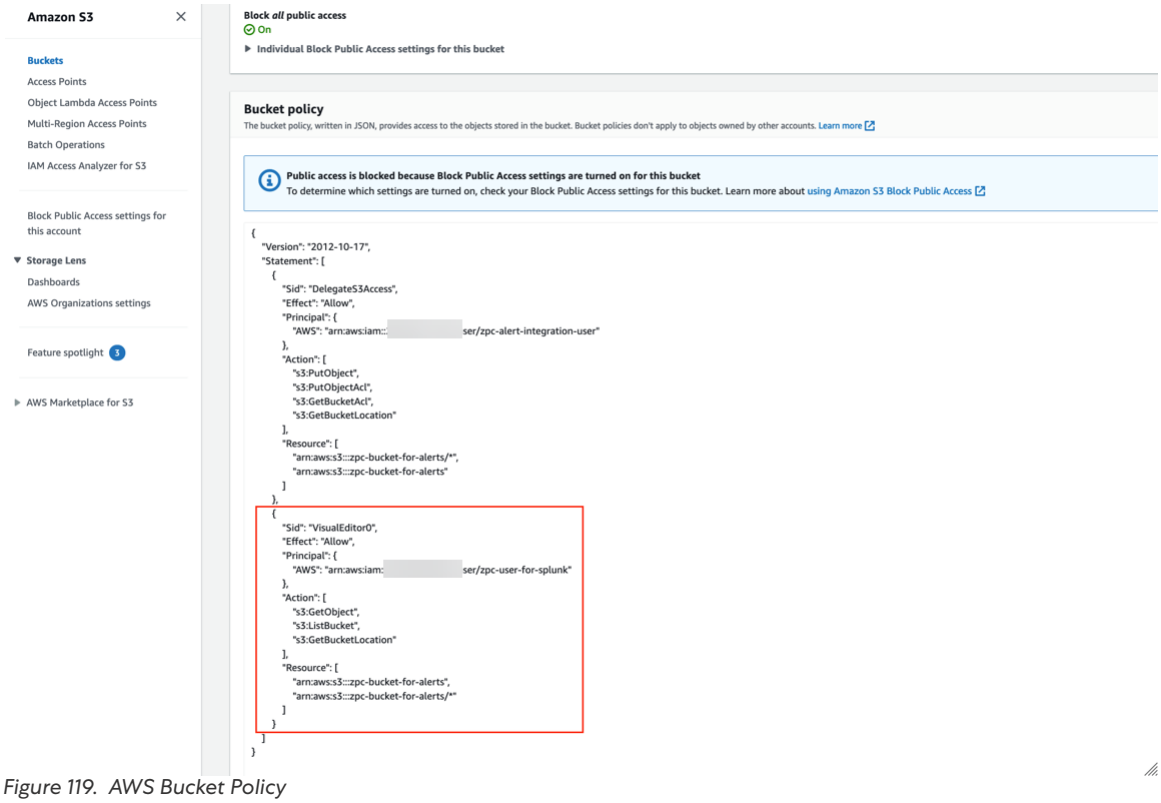

Figure 119. AWS Bucket Policy

Configuring Splunk

To configure Splunk to read from the S3 bucket:

1. On your Splunk instance, install the Splunk Add-on for AWS. This allows you to configure Splunk to ingest the alerts from S3.
2. Select the **Splunk Add-on for AWS** and then **Account** under the **Configuration** tab.

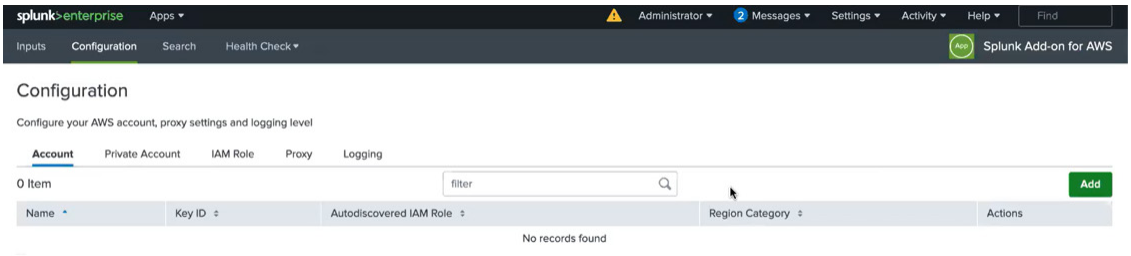

Figure 120. Splunk Account Configuration

3. Click **Add**.
4. Add the user created earlier.
5. Enter the **Username**, **Key ID**, and **Secret Key**.

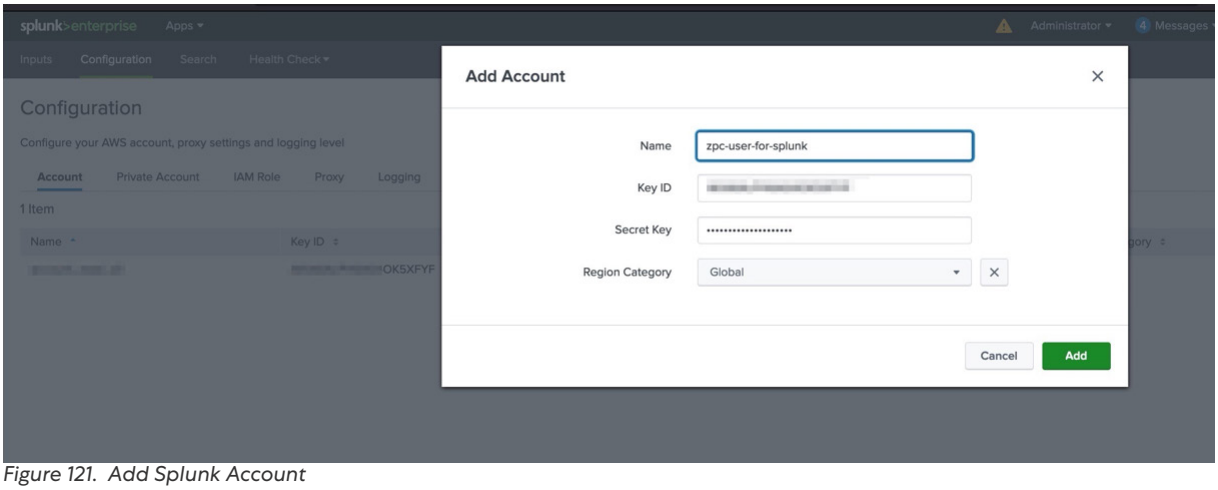

Figure 121. Add Splunk Account

6. Create a generic S3 input from the Splunk App by going to **Inputs** > **Create New Input** > **Custom Data Type** > **Generic S3**.

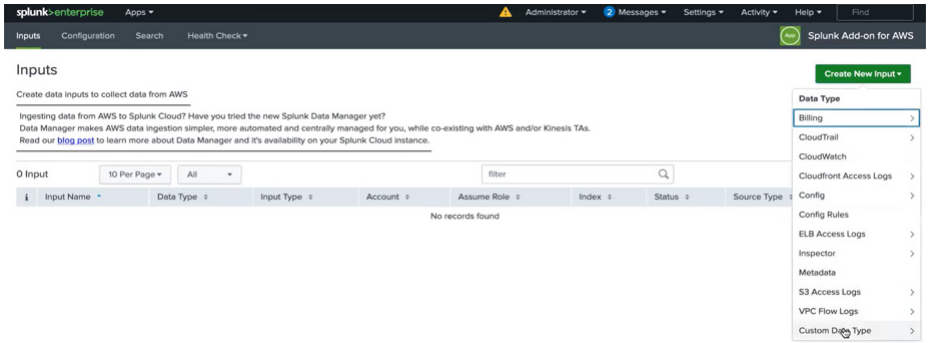

Figure 122. Splunk S3 Inputs

7. Enter a **Name**.
8. Select the AWS username created earlier.
9. Select the name of the bucket used in the previous sections.
10. In **Source Type**, enter `zscaler-posturecontrol-alerts` and for index, enter `zscaler`.
11. Click **Add**.

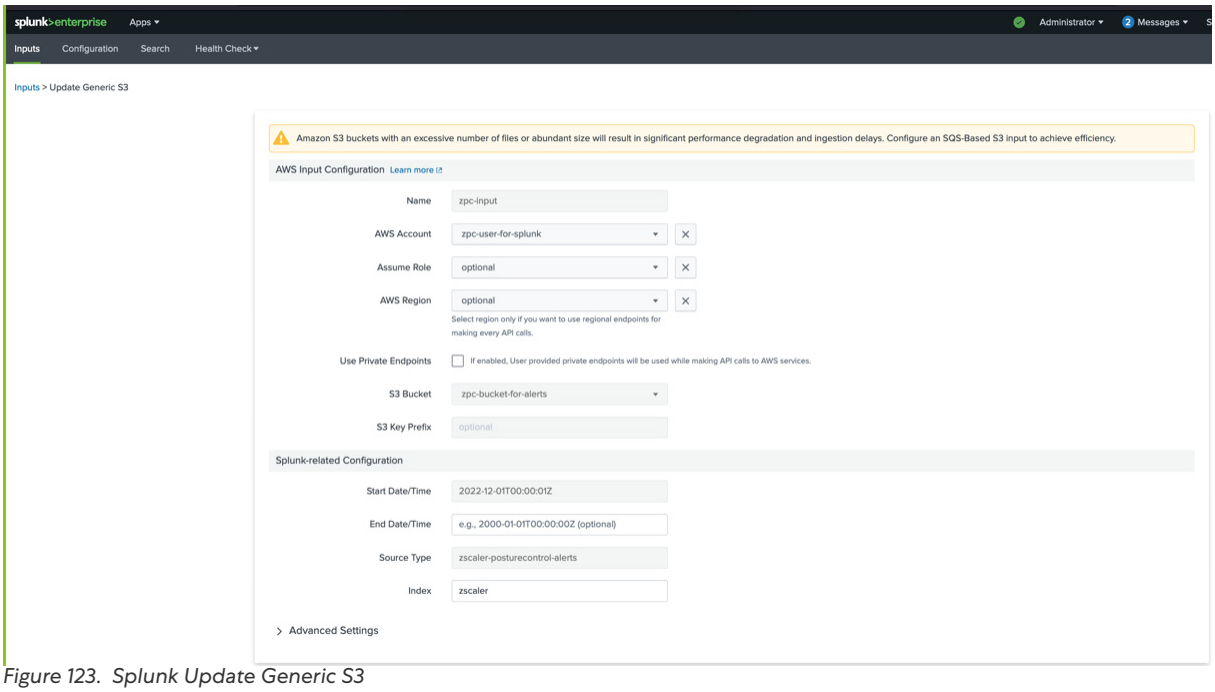

Figure 123. Splunk Update Generic S3

12. Return to the Zscaler Splunk app and select the **Posture Control** tab. As alerts get pushed out by ZPC, the corresponding Splunk dashboards are populated.

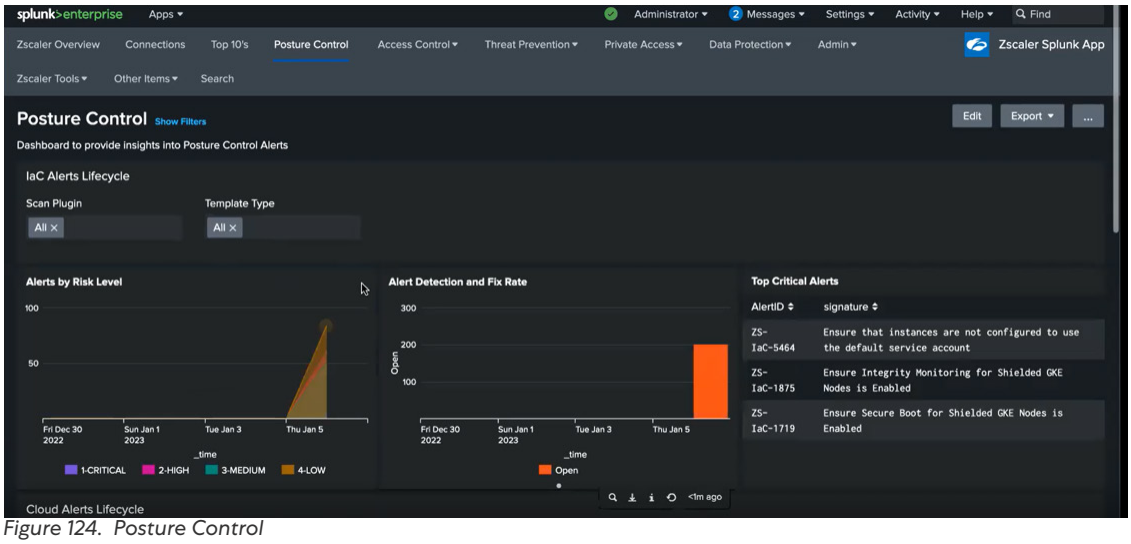

Figure 124. Posture Control

The following image shows open alerts by risk level.

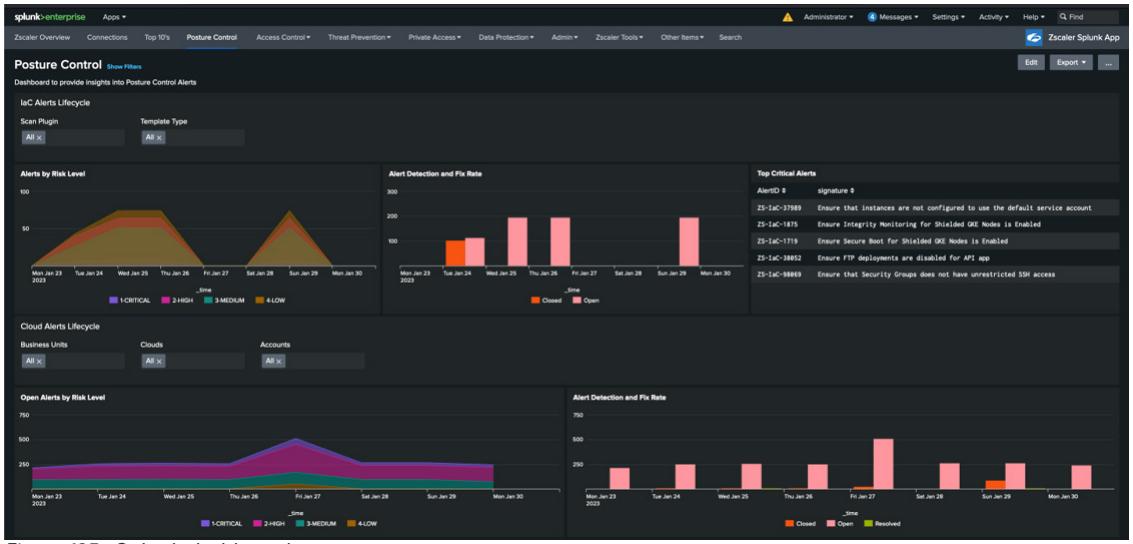

Figure 125. Splunk dashboards

Appendix F: Requesting Zscaler Support

You might sometimes need Zscaler Support for provisioning certain services, or to help troubleshoot configuration and service issues. Zscaler Support is available 24/7/365.

To contact Zscaler Support:

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

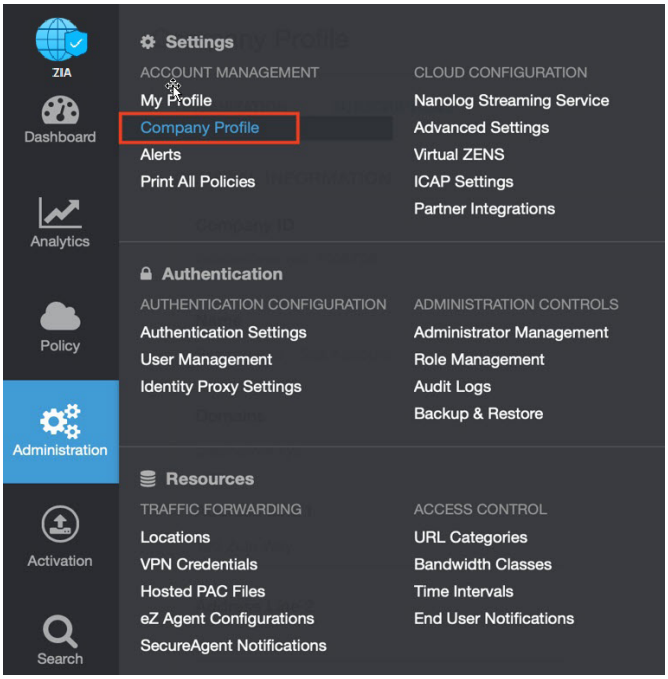

Figure 126. Collecting details to open support case with Zscaler TAC

2. Copy the Company ID.

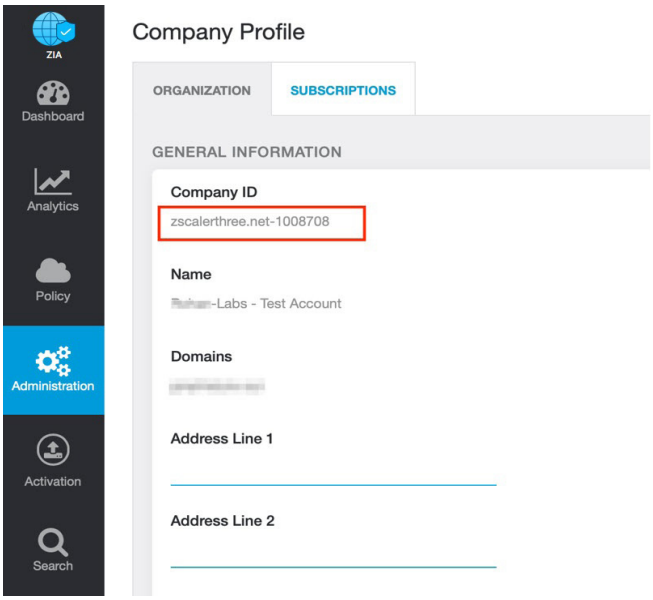

Figure 127. Company ID

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

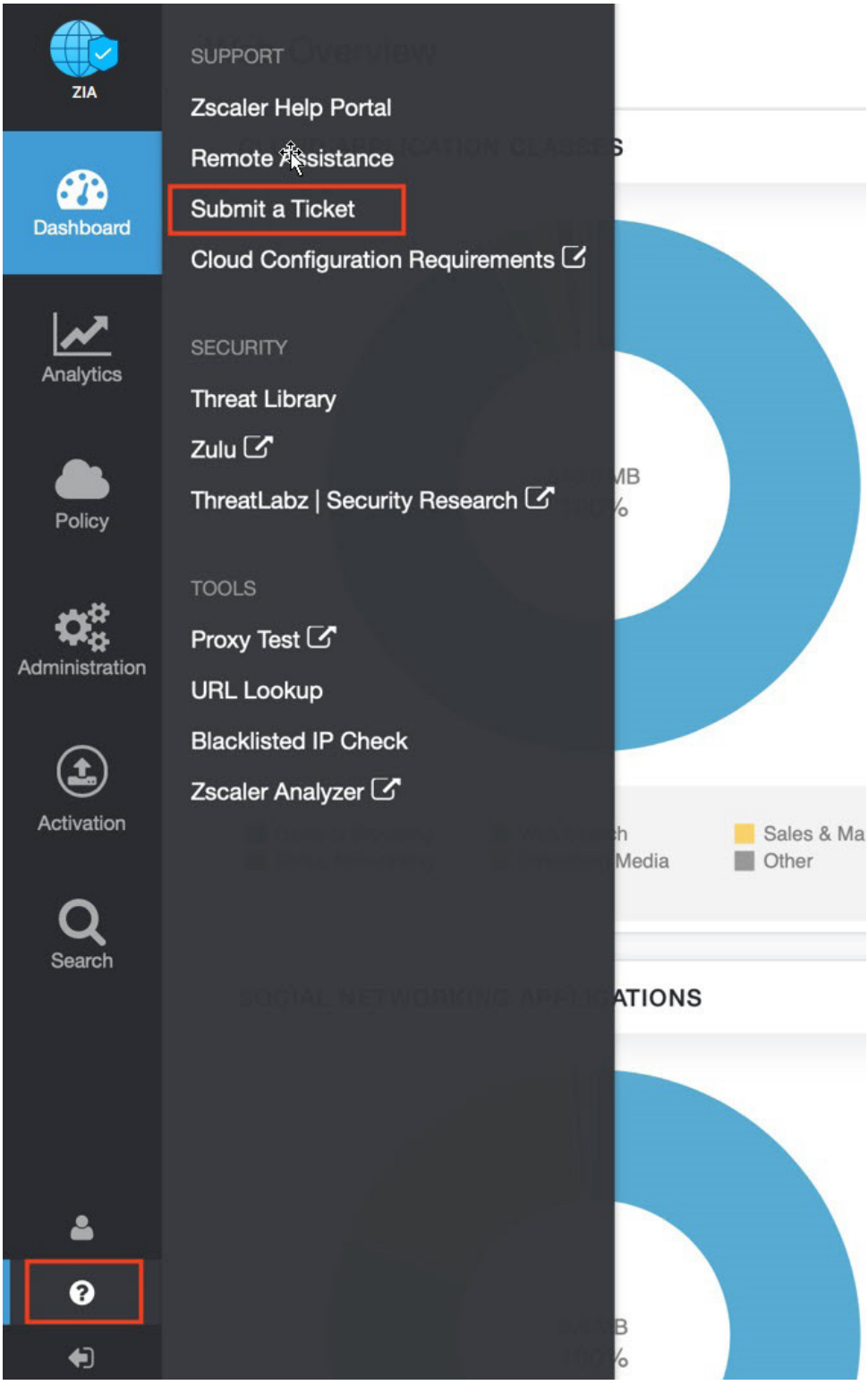

Figure 128. Submit a ticket

