Forcepoint ONE and Splunk Integrated Configuration Guide

Forcepoint

Overview

Forcepoint ONE traffic, status and access logs provide a rich source of data for ingesting into the Splunk platform. This information enriches other data sources and generates interesting events related to cybersecurity, business services and technology operations. To learn more, refere to Splunk's website.

Audience

This guide is designed for network administrators, endpoint and IT administrators, along with security analysts responsible for deploying, monitoring and managing enterprise security systems. This document is targeted to those interested in learning details of how Forcepoint ONE and Splunk interact as well as guidance for their integration. This can consist of:

- Enterprise, solution and security architects
- SOC and NOC designers and managers
- Splunk designers, implementors, administrators and operators
- Anyone with general interest in Forcepoint ONE SIEM integration and reference materials

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

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

This document was authored using the latest version of Forcepoint ONE and Splunk Enterprise.

Forcepoint ONE and Splunk Introduction

In order to ease integration of Forcepoint ONE capabilities into environments using Splunk, Forcepoint has developed a "Splunk App" which simplifies the ingestion of Forcepoint ONE-generated data into the Splunk platform. This Splunk App makes the overall integration process between our technologies more accessible for our joint customers.

Forcepoint ONE Overview

Forcepoint ONE is an all-in-one cloud service that makes security simple for distributed businesses and government agencies that need to adapt quickly to changing remote and hybrid workforces. It gives employees, contractors and other users safe, controlled access to business information on the web, in the cloud (SaaS and IaaS) and in private applications, while keeping attackers out and sensitive data in. As a result, Forcepoint ONE makes users more productive, whether remote or in the office, and businesses more efficient.

Forcepoint ONE Resources
The following table contains links to Forcepoint resources based on general topic areas.

Name and Link	Description
Forcepoint ONE Help Portal	Help articles for Forcepoint ONE
Forcepoint ONE REST API	Log export rest API guide
Forcepoint ONE Customer Hub	Forcepoint support portal for submitting requests and issues

Splunk Overview
The Splunk platform provides a suite of self-service capabilities for ingesting and analyzing security and event data. The Splunk platform collects, searches, monitors, reports and analyzes real-time and historical event logs. In addition, you can use the Splunk Monitoring Console to holistically monitor the data ingestion and health of your Splunk platform.

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 Common Information Model (CIM)	Description of Splunk's CIM

Application Architecture

Forcepoint's integration with Splunk follows Splunk's well-defined framework. The Forcepoint Splunk App is designed specifically to be installed and run in a Splunk environment. The app is separated into two discrete parts: the Technical Add-on and the Forcepoint Splunk App.

The app takes advantage of several technologies in order to ingest data from Forcepoint ONE, which consists of log streams generated from customer environments, and can also retrieve data using

Forcepoint ONE APIs. The following diagram shows these various interfaces.

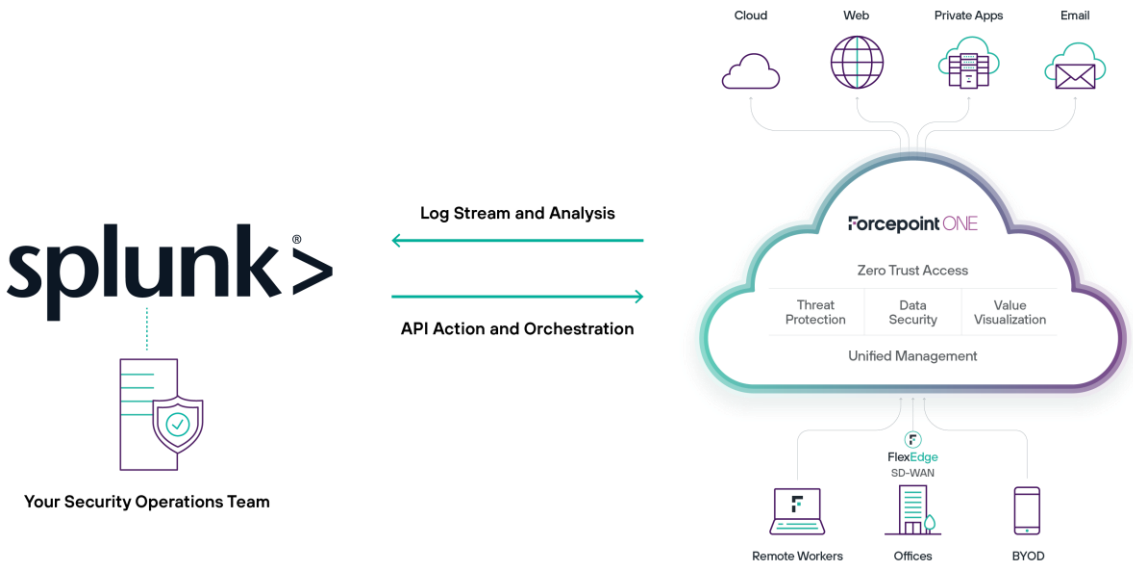


Figure 1. Application architecture

The interfaces are detailed in the following sections.

Data Models

Joint customers of Forcepoint ONE and Splunk require Forcepoint ONE logging data to be in a format that is compatible with Splunk's CIM data model. The Forcepoint ONE Technical Add-on maps all Forcepoint ONE log fields into CIM-compatible syntax, as well as tagging all events that are relevant to specific CIM data models.

Forcepoint ONE Log Streams

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

These virtual machines attach to Forcepoint ONE via REST API connections and receive logs to stream into customer log collection and SIEM platforms. The following table describes the various log streams.

Log Type	Streaming Technology	Platforms
Web Proxy	REST API (Python Script)	VMware, AWS and Azure
Web DLP Proxy	REST API (Python Script)	VMware, AWS and Azure

Web Logs

A decidated Forcepoint VA server delivers Forcepoint ONE Web and DLP logs. Event streams are generated for the following log types:

- Proxy logs: all-access logs processed by Forcepoint ONE proxy
- Proxy DLP logs: DLP Incident logs processed by Forcepoint ONE proxy

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

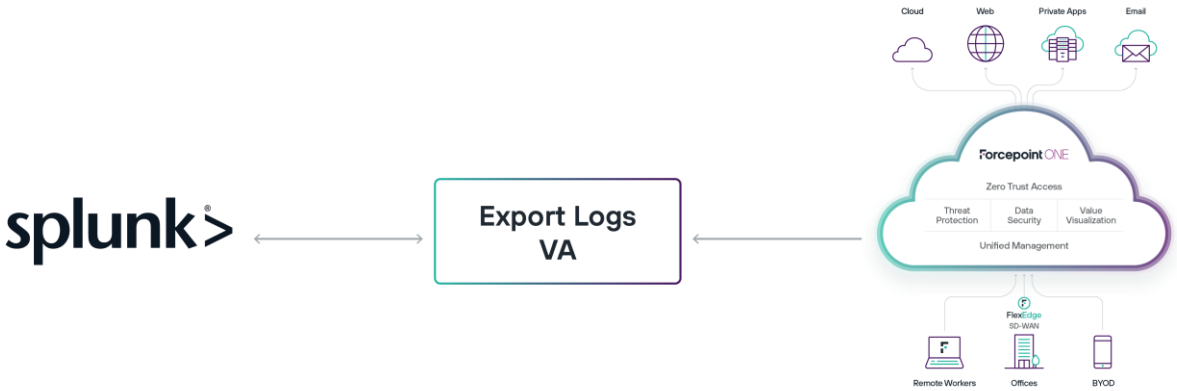


Figure 2. Forcepoint ONE data in Splunk

Forcepoint ONE APIs

Forcepoint ONE runs multiple open APIs for customer use, which include read and write functions. The current Splunk integration focuses on the read function for Forcepoint ONE logs. Full specifications for the Forcepoint ONE API are found in the API Reference.

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

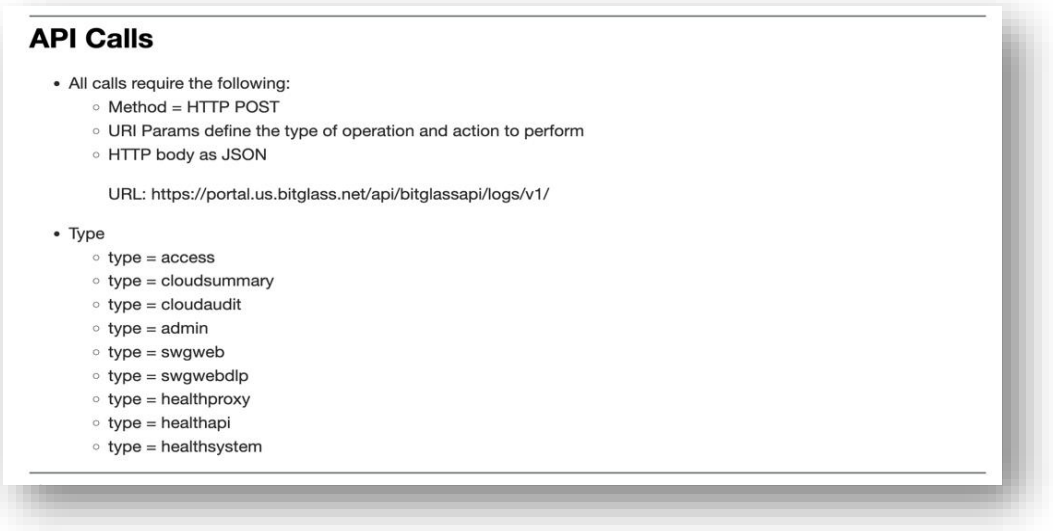


Figure 3. Forcepoint ONE APIs used by Splunk modular inputs

Python SDK

The Splunk App contains several scripts that interface with Forcepoint ONE API.

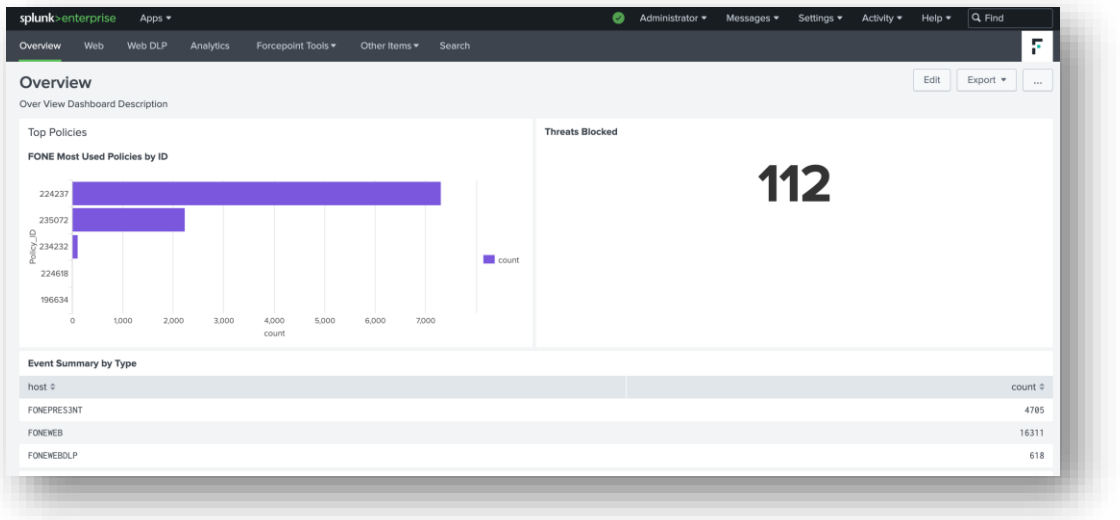


Figure 4. Forcepoint ONE log analytics in Splunk

Forcepoint ONE VA Add-on

The Forcepoint ONE VA Add-on does all the hard work in accessing and processing Forcepoint ONE event information. This includes:

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

The add-on is a requirement for the Forcepoint ONE Splunk App because the app takes advantage of many configurations and components defined in the add-on.

Source Types

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

Source Type	Function	Stream Format
Forcepoint ONE Web	Forcepoint ONE Proxy Logs	Splunk CIM
Forcepoint ONE Web DLP	Forcepoint ONE DLP Proxy Logs	Splunk CIM

Forcepoint ONE Splunk App

The Forcepoint ONE Splunk App front-ends all the Forcepoint ONE data ingested into Splunk. This includes a large volume of saved searches and dashboards. The app's menu is laid out similar to core Forcepoint ONE capabilities of Access Control, Threat Prevention, Private Access, and Data Protection. You can drill down into each area.

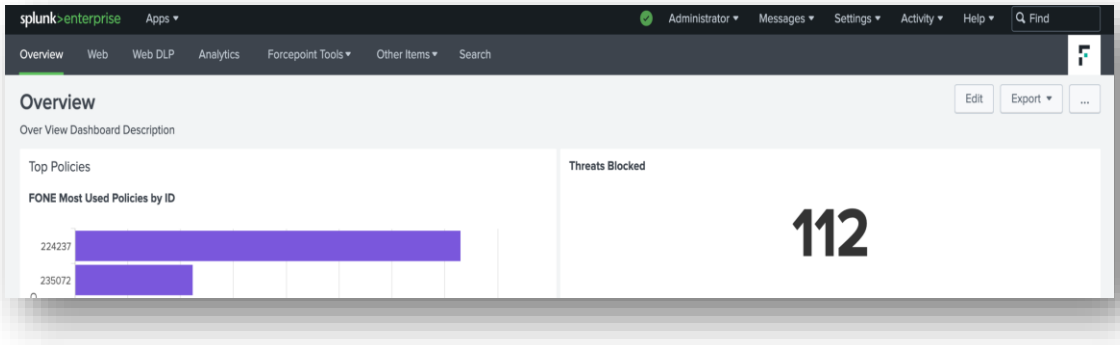


Figure 5. Splunk App menu

Dependencies

The Forcepoint ONE Splunk App is dependent on the Forcepoint ONE VA Add-on.

User Interface

The Splunk App is a visual component of Forcepoint ONE's Splunk integration. The Forcepoint ONE Splunk App can serve as a useful base for you to create your own Forcepoint ONE oriented searches, reports, and dashboards.

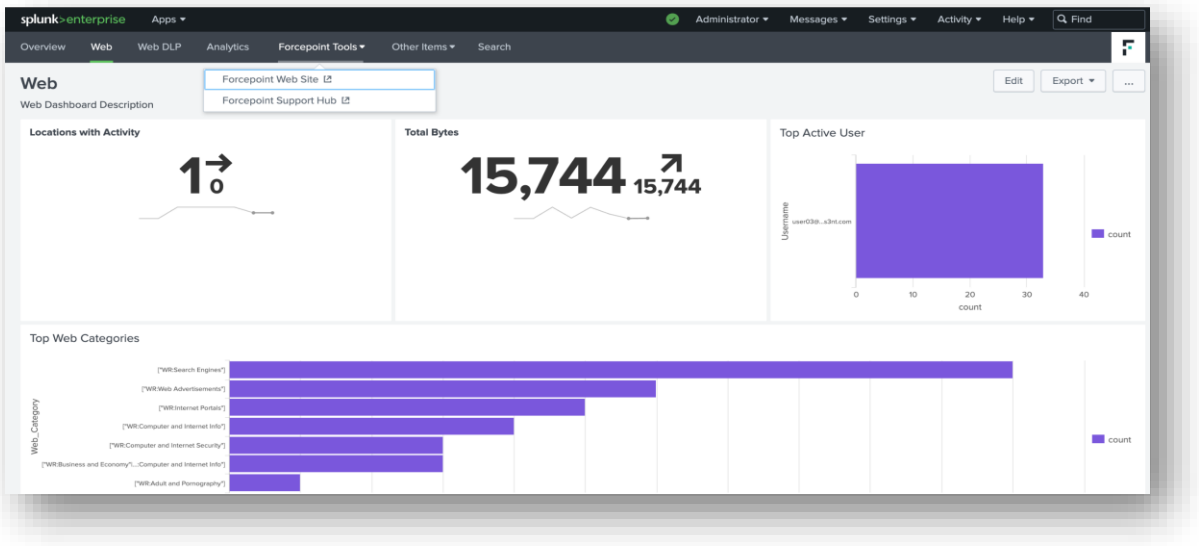


Figure 6. Forcepoint ONE overview in Splunk

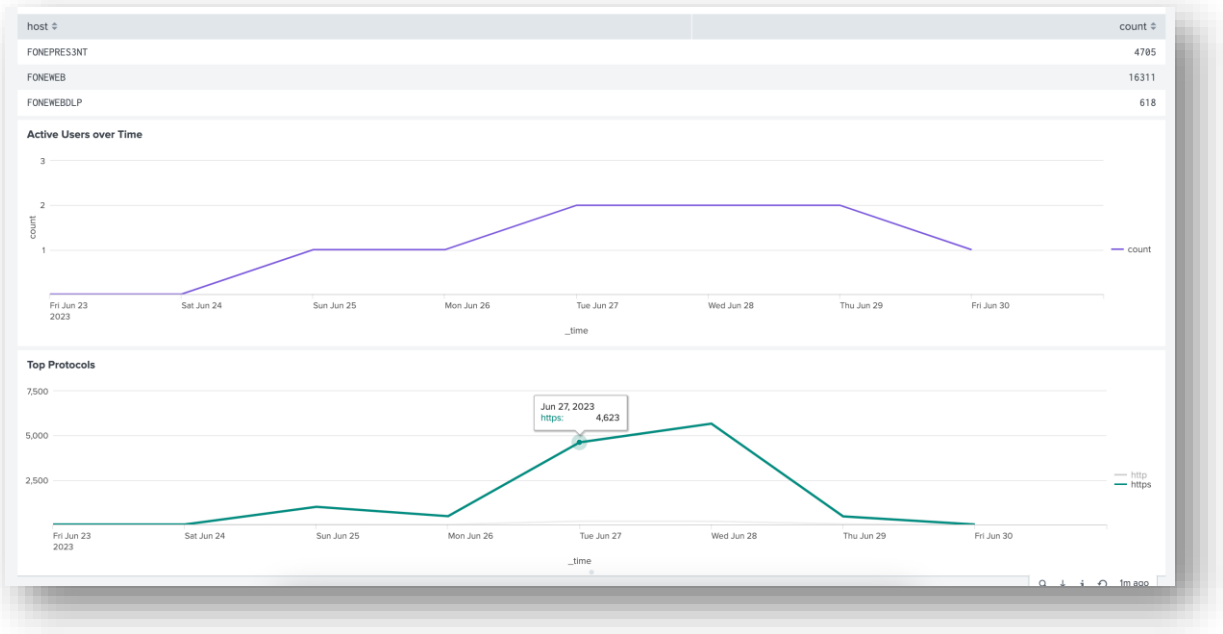


Figure 7. Forcepoint ONE overview

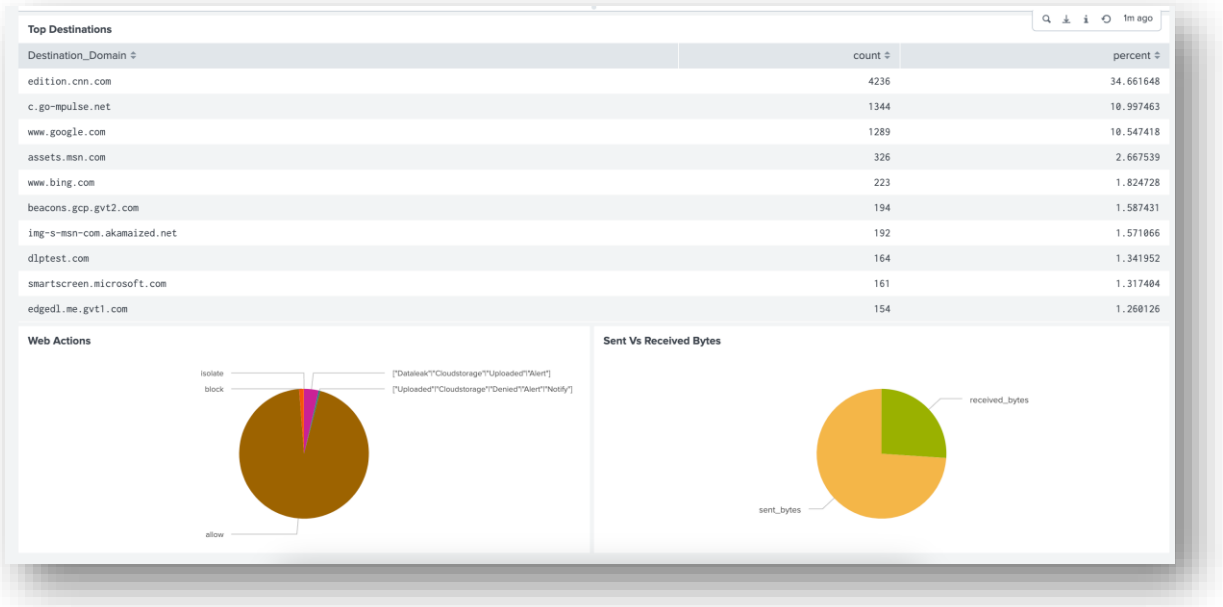


Figure 8. Forcepoint ONE Web Analytics

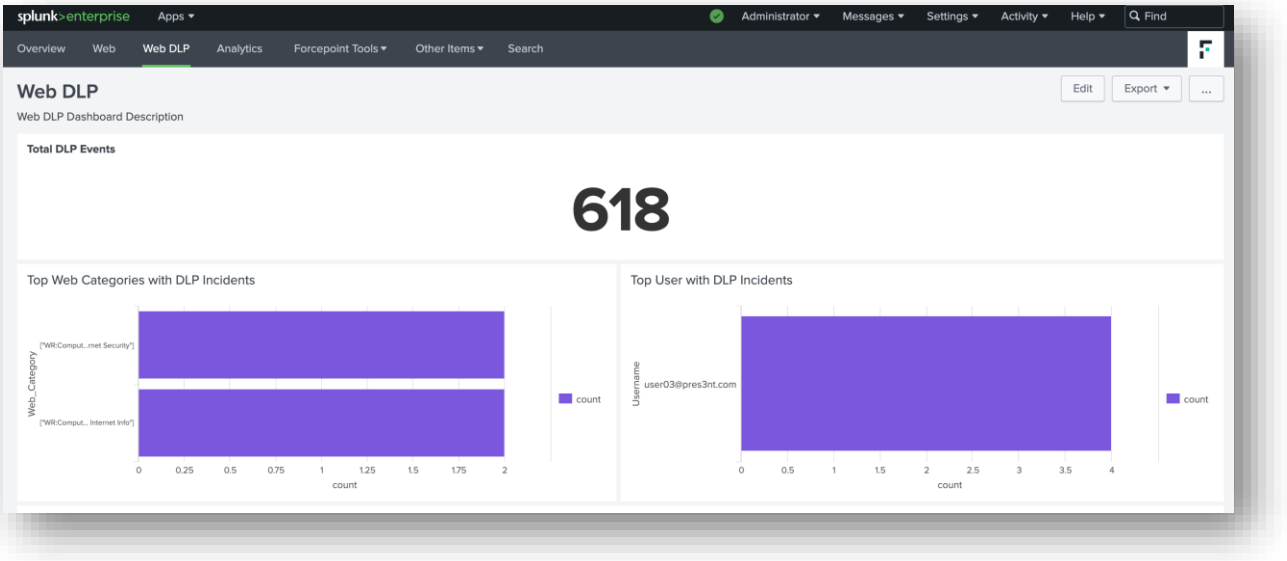


Figure 9. Forcepoint ONE DLP Analytics

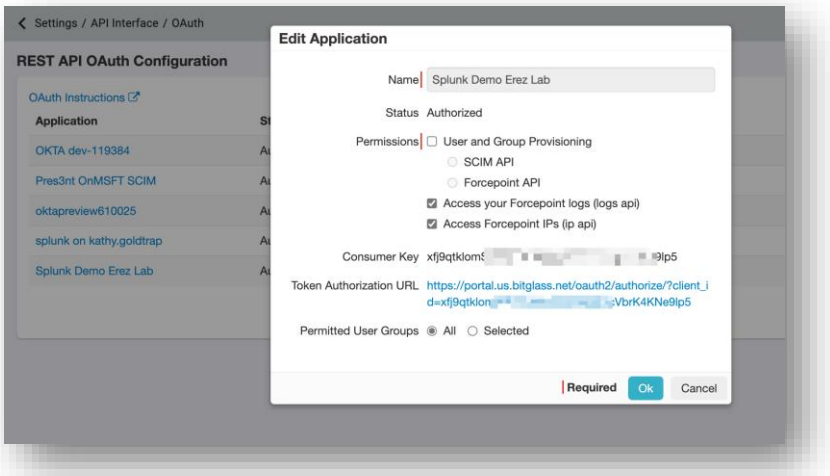
Installation and Configuration

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

Forcepoint ONE Configuration

You must configure Forcepoint ONE to send data into Splunk. Follow Forcepoint ONE's existing documentation to set up the base configuration of REST API access. The relevant reference links are:

- Creating OAUTH Token
    - Creating new API Token per the screenshot so Forcepoint ONE VA Add-on can use it to export log data via API



- Log Export API

Forcepoint ONE VA Add-on

You must import Forcepoint ONE VA Add-on to your choice of VM in order to send data into Splunk. Once it has been imported, please configure the token to be used when retrieving logs via REST API.

- Web Logs

  [root@centos fone] #

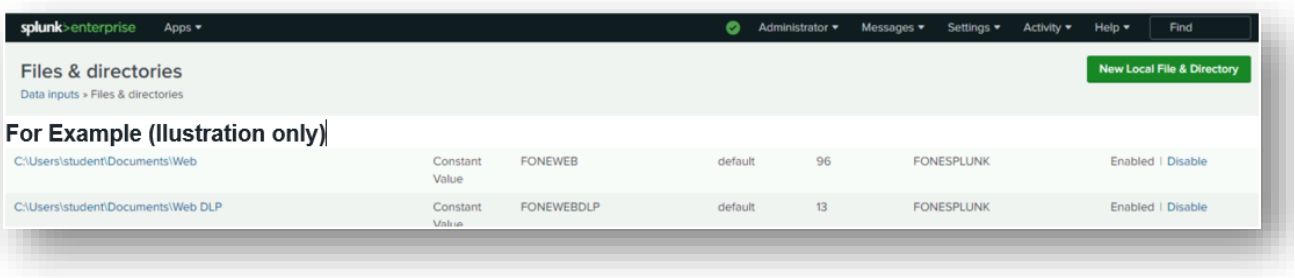
  [root@centos fone] # python3 log_export_example.py -a start -d 2023-06-28 swgweb -p portal.us.bitglass.net -f csv -o GDjYz19As9ZY2fuF6zYlhgAD1vMkhx

- Web DLP Logs

  [root@centos fone] # python3 log_export_example.py -a start -d 2023-06-28 -1 swgwebdlp -p

  portal.us.bitglass.net -f csv -o GDjYz19As9ZY2fuF6zY11

The above will download logs to a directory on the Forcepoint ONE Log Exporter VA. The logs will have to be imported to Splunk via File & Directory Input. (Please consult Splunk configuration and architect to configure this per your environment.)



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 Forcepoint ONE Logs and APIs into Splunk.

Search Head

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

Appendix B: Splunk Essential Configuration Using Forcepoint ONE VM

This appendix details how to perform the initial integration between Splunk and Forcepoint ONE for logs that are streamed to a Splunk instance.

Add or Create Index

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

Log Into Splunk Instance

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

Configure New Index in Splunk

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

After logging into Splunk, navigate to **Settings** > **Indexes** > **New Index**.

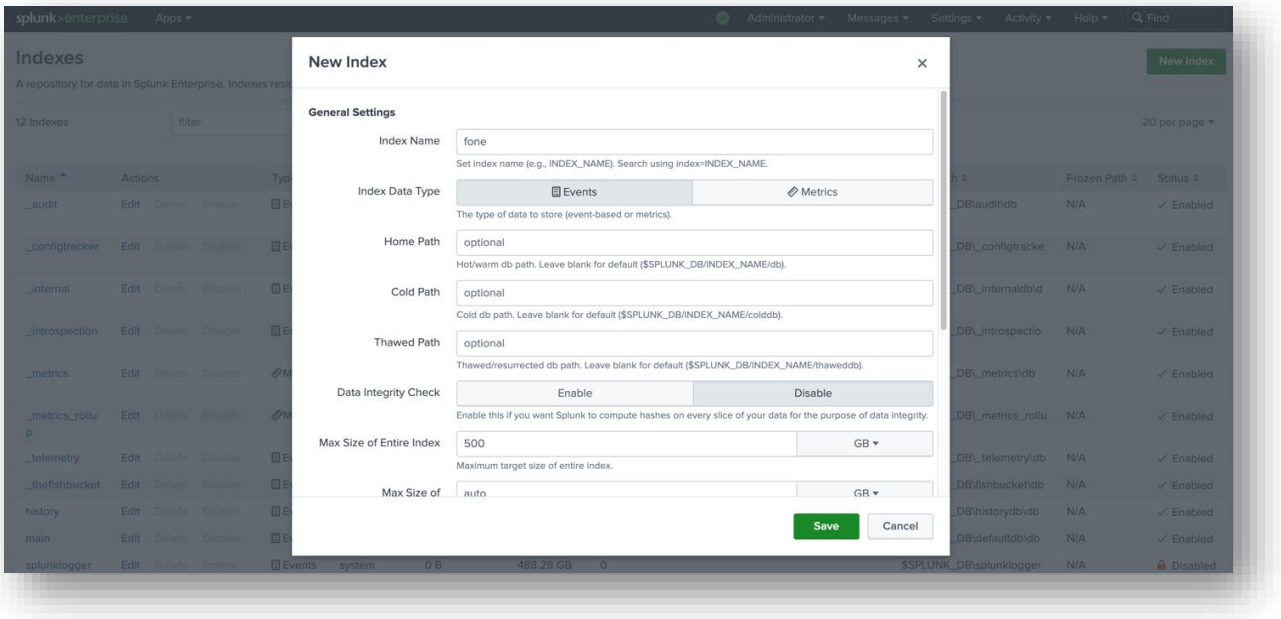


Figure 10. Forcepoint ONE index in Splunk

Forcepoint ONE creates an index titled **FONE** because the Splunk App for Forcepoint ONE looks for data written at index **FONE** by default; setting **index=FONE** allows us to use the Splunk App for Forcepoint ONE out of the box.

In the **New Index** dialog, type **fone** (case sensitive) and click **Save**.

Verify Splunk Forcepoint ONE App

Then navigate to **Apps** > **Forcepoint ONE App** > **Dashboard** > **Web**.

The window is populated with incoming Forcepoint ONE data.

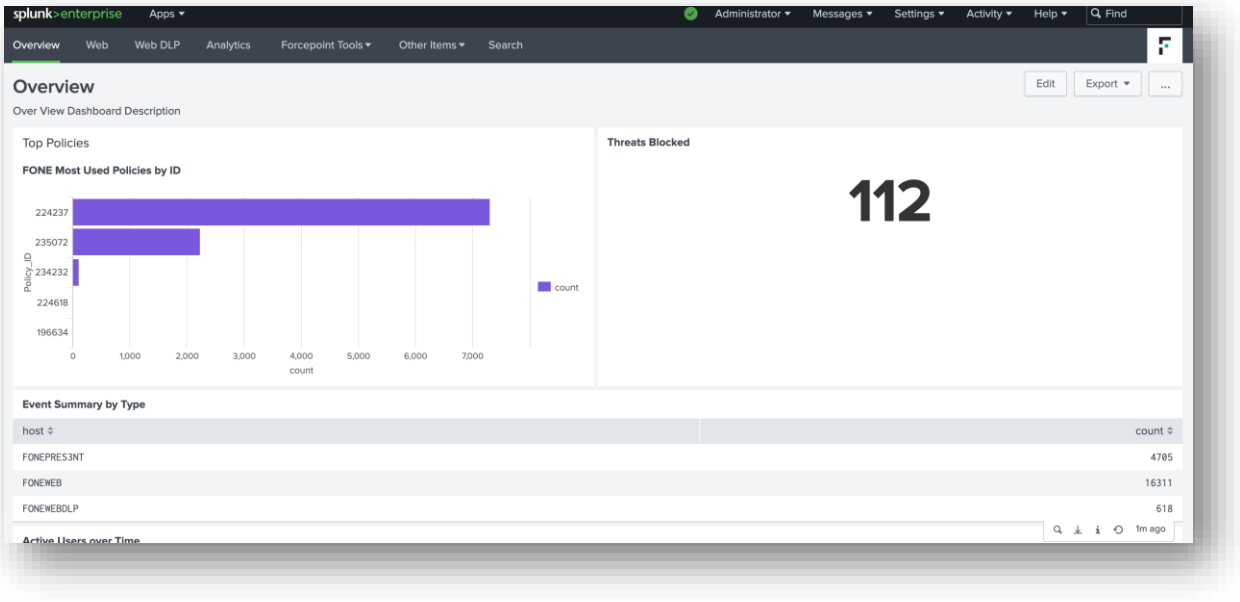
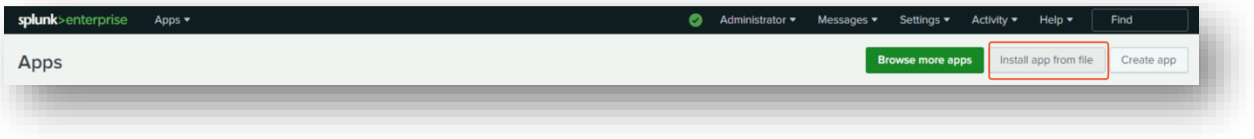


Figure 11. Verfify Splunk Forcepoint ONE Data Ingestion

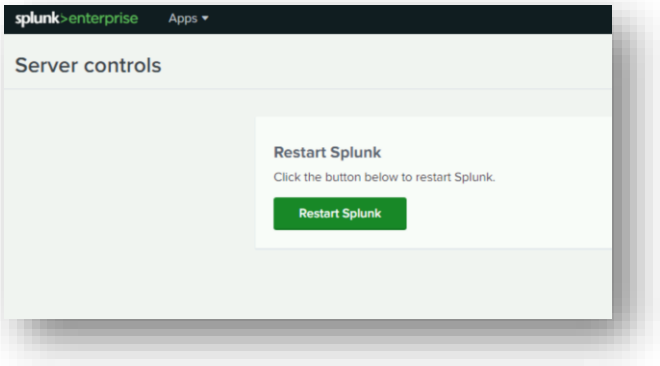
If a particular panel is not populated, click the **Search** icon next to it. This shows the query that the panel is running behind the scenes to help with troubleshooting.

Appendix C: Splunk Essential Configuration

Install Forcepoint ONE App in Your Splunk Enterprise
After logging in, navigate to **Apps** > **Manage Apps** > **Install App from File** and choose the Forcepoint ONE App spl file.



You will need to restart Splunk for the app to work via **Settings** > **Server Controls** > **Restart Splunk**.



Appendix F: Requesting Forcepoint ONE

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

To contact Forcepoint Support, visit the Forcepoint Customer Hub.

Terms and Acronyms

This table defines abbreviations used in the deployment guide.

Acronym	Definition
API	Application Programming Interface
CIM	Common Information Model (Splunk-defined data model)
CSV	Comma-Separated Values
DLP	Data Loss Prevention
DNS	Domain Name Service
SaaS	Software as a Service
SIEM	Security Incident and Event Management
SOAR	Security Orchestration and Automation
SOC	Security Operations Centre
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security
XFF	X-Forwarded-For (RFC7239)

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

[FP ONE and Splunk Integrated Configuration Guide] 20Sept2023