Tenable Web App Scanning Add-on for Splunk Integration Guide

Last Revised: July 10, 2023

Table of Contents

Welcome to Tenable for Splunk

The Tenable for Splunk application performs data collection, normalization, and visualization. The application is divided into two parts:

- Tenable Web App Scanning Add-on for Splunk provides all data collection and normalization functionality.
- Tenable App for Splunk provides a dashboard to view the Tenable data in Splunk.

The Tenable Web App Scanning Add-On for Splunk pulls data from Tenable platforms and normalizes it in Splunk. The current Tenable Web App Scanning Add-on uses the following pyTenable SDK to retrieve all data.

Components

The Tenable Add-on has specific purposes for each Splunk component. The available components are in the following list:

Indexer

The **Indexer** ensures Tenable data is properly indexed.

Note: Use a default index or create and set a custom index. (Required)

Tenable Tenable Web App Scanning Add-on

The Tenable Tenable Web App Scanning Add-On for Splunk pulls data from Tenable platforms and normalizes it in Splunk.

The current Tenable Web App Scanning Add-on uses the following pyTenable SDK to retrieve all data:

Vulnerability Export

The Splunk Add-on uses the export method to export the vulnerability data. You can initiate the method in the following ways:

- Create an object for a tenable IO -> **self._tio = TenableIO()**
- Call export methods -> **self._tio.was.export(filters)**

Source and Source Types

The Tenable Add-on for Splunk stores data with the following sources and source types.

Tenable Web App Scanning

Source	Source type	Description
<username>|<address>	tenable:io:vuln:was	This collects all vulnerability data.

Installation Workflow

Use the following workflow to complete the installation and configuration of the Tenable applications for Splunk.

Before you begin:

To install and configure Tenable applications for Splunk:

1. Install the Tenable application.
2. Create an input for the configured Tenable application for Splunk.

Splunk Environments

The installation process for the Tenable Web App Scanning Add-on for Splunk varies based on your Splunk environment.

Deployment Types

Single-server, distributed deployment, and cloud instance options are available.

Single-Server Deployment

In a single-server deployment, a single instance of Splunk Enterprise works as a data collection node, indexer, and search head. Use this instance to install the Tenable Web App Scanning Add-On. Complete the setup to start data collection.

Distributed Deployment

In a distributed deployment, install Splunk on at least two instances. One node works as a search head, while the other node works as an indexer for data collection.

Cloud Instance

In Splunk Cloud, the data indexing takes place in a cloud instance.

You can install the application via a command line or from the Splunk user interface.

Installation

Complete the installation and configuration of the Tenable applications for Splunk according to the following workflow.

Before you begin:

- You must have Splunk downloaded on your system with a Splunk basic login.

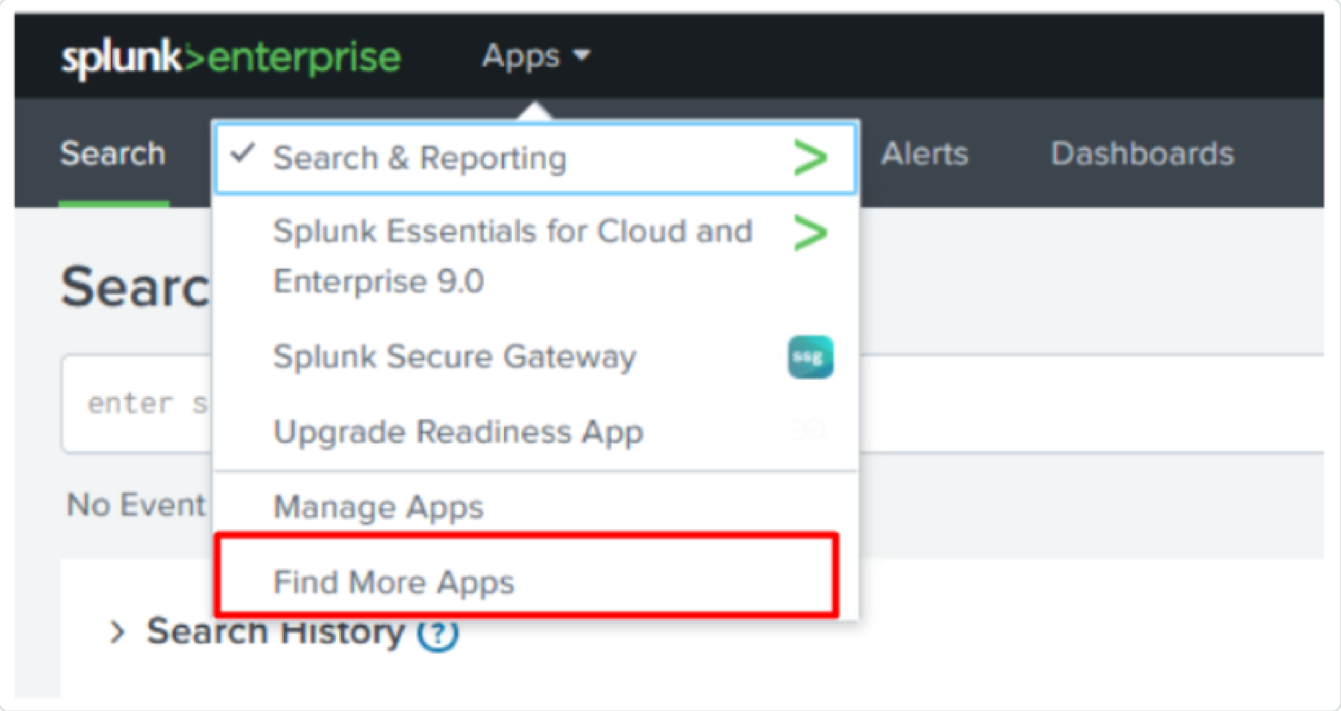
> **Note:** See the Splunk Environments section for additional information about the different types of Splunk deployments and their requirements.

> **Note:** If you install the Tenable App for Splunk on the search head, you must also install the Tenable Add-on.

To install Tenable Web App Scanning Add-on for Splunk for the first time:

1. Log in to Splunk.
2. Go to **Apps** at the top of the screen.

   A drop-down menu appears:



3. Click **Find More Apps**.

4. On the **Browse More Apps** page, type Tenable in the search bar.

5. Click the **Install** button next to **Tenable Tenable Web App Scanning Add-on for Splunk**.

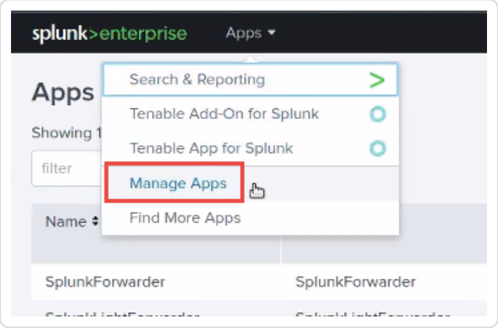
6. Restart Splunk if a **Restart Required** prompt displays.

To upgrade Tenable Web App ScanningAdd-on for Splunk:

1. Log in to Splunk.

2. Go to **Apps** at the top of the screen.

   A drop-down menu appears:

3. Click **Manage Apps**.

4. In the search bar, type Tenable.

5. In the **Version** column, click **Update to** x.y.z version link for Tenable Web App Scanning Add-On for Splunk:

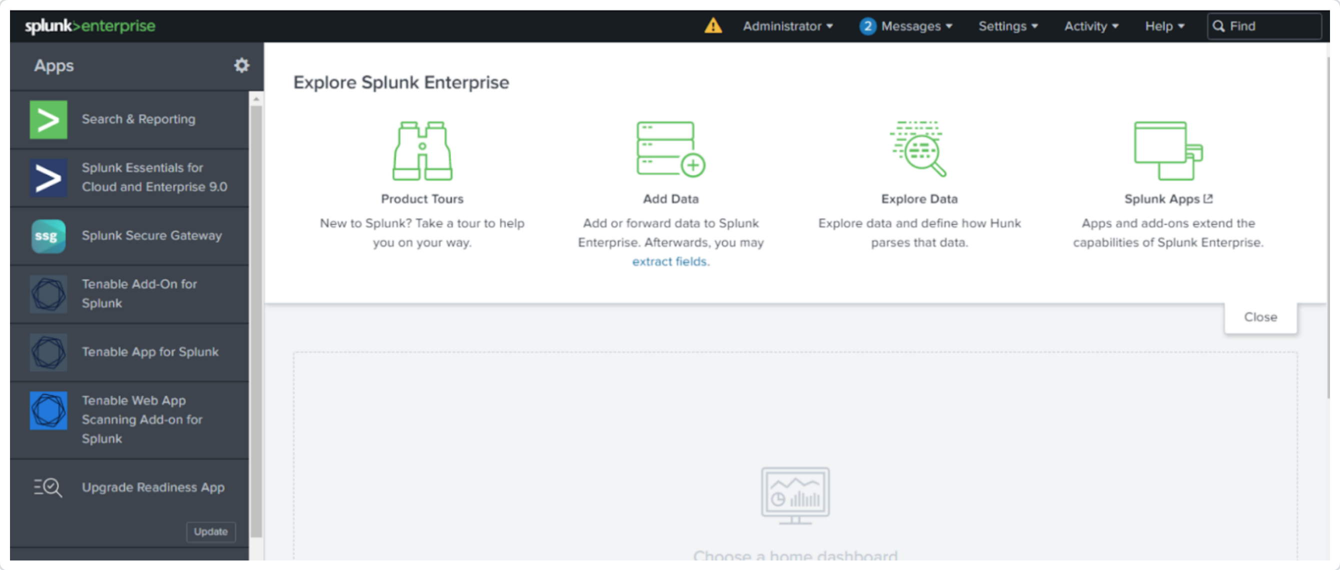
6. Restart Splunk if a **Restart Required** prompt appears.

Create an Input

After you complete the configuration for your Tenable Add-On for Splunk, you must create the input. The following process outlines input creation if you have a deployment with Tenable Web App Scanning Add-on for Splunk.

To create an input:

1. In the left navigation bar, click or **Tenable Web App Scanning Add-on for Splunk**.



Explore Splunk Enterprise

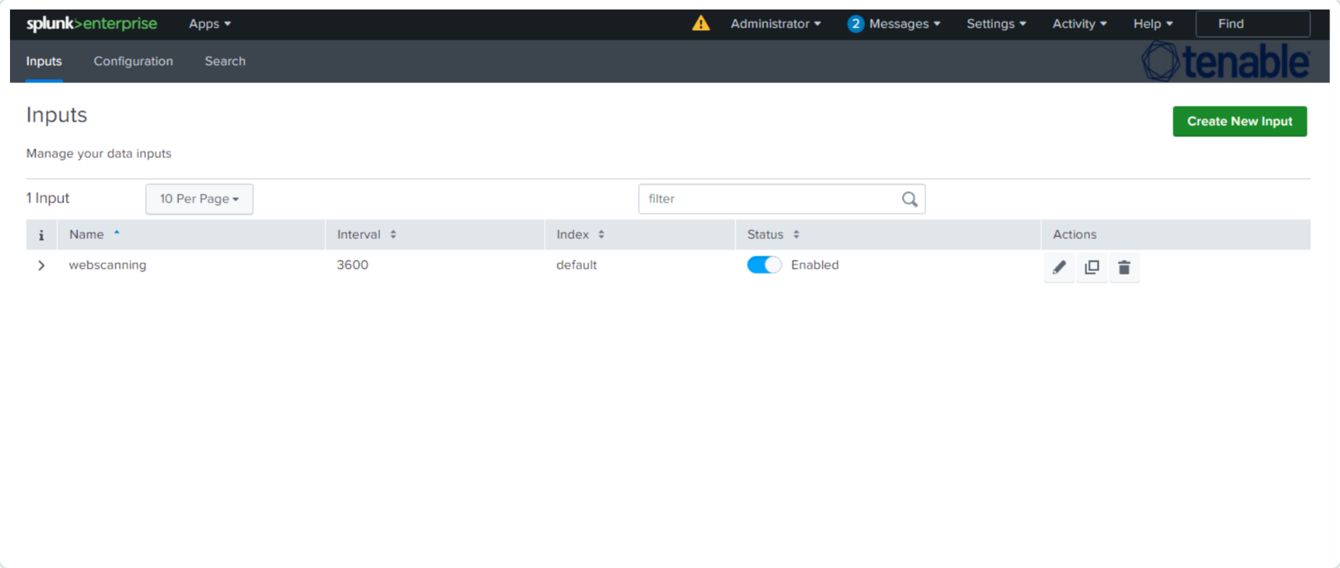
New to Splunk? Take a tour to help you on your way.

Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Explore data and define how Hunk parses that data.

Apps and add-ons extend the capabilities of Splunk Enterprise.

2. Click the **Inputs** tab.



Inputs

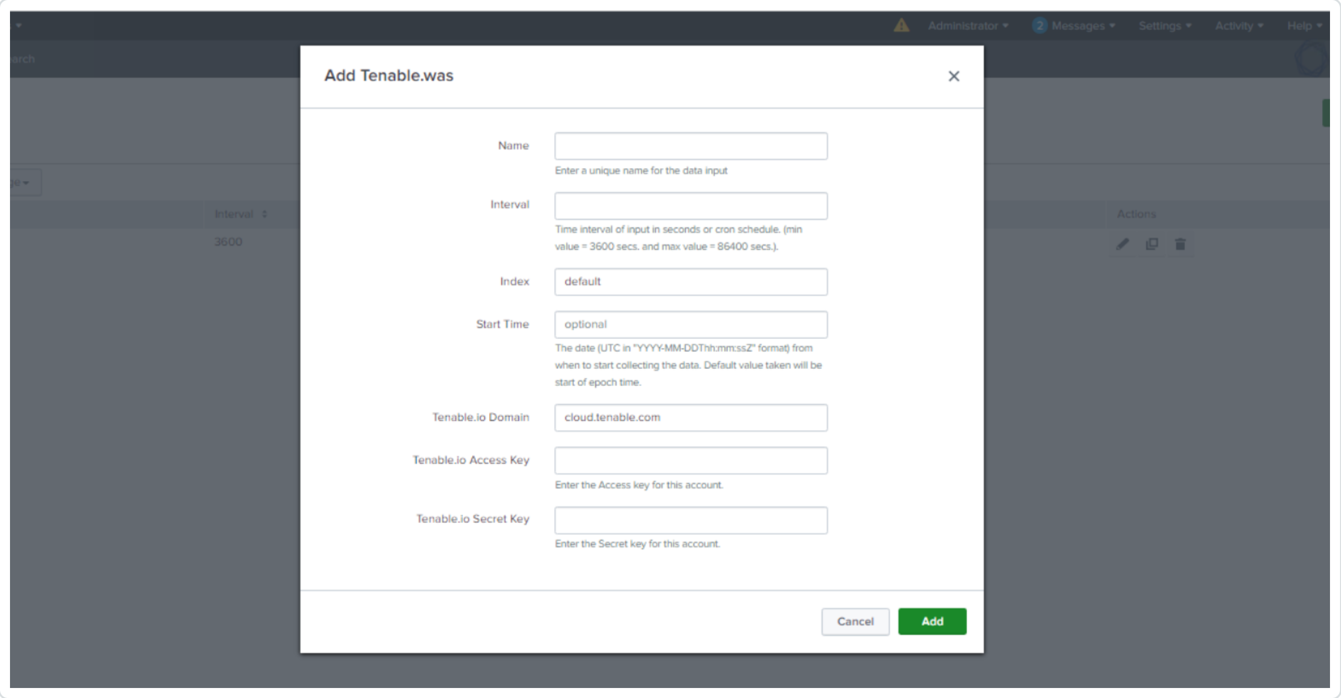
Manage your data inputs

1 Input

i	Name	Interval	Index	Status	Actions
›	webscanning	3600	default	Enabled	

3. Click **Create New Input**.

   The **Add Tenable Web App Scanning Add-on for Splunk** window appears:



Add Tenable.was

Name:
Enter a unique name for the data input

Interval:
Time interval of input in seconds or cron schedule. (min value = 3600 secs. and max value = 86400 secs.).

Index: default

Start Time: optional
The date (UTC in "YYYY-MM-DDThh:mm:ssZ" format) from when to start collecting the data. Default value taken will be start of epoch time.

Tenable.io Domain: cloud.tenable.com

Tenable.io Access Key:
Enter the Access key for this account.

Tenable.io Secret Key:
Enter the Secret key for this account.

4. Provide the following information.

   Note: If you don't use the default index, you must update the Tenable Macro.

   Tenable Web App Scanning

Input Parameters	Description	Required
Name	The unique name for each Tenable data input.	Yes
Interval	The interval parameter specifies when the input restarts to perform the task again (in seconds). The interval amount must be between 300 and 86400.	Yes
Index	The index in which to store Tenable Vulnerability Management data.	Yes

Start Time	The date and time to start collecting data. If you leave this field blank, the integration collects all historical data. **Note:** Uses the *YYYY-MM-DD hh:mm:ss* format.	No
Tenable Vulnerability Management Domain	Splunk pulls data from this Tenable account.	Yes
Tenable Vulnerability Management Access Key	Tenable Vulnerability Management API access key.	Yes
Tenable Vulnerability Management Secret Key	Your Tenable Vulnerability Management API secret key	Yes

5. Click **Add** to create the input.