

Tenable Attack Surface Management Add-on for Splunk Integration Guide

Last Revised: August 14, 2023

Table of Contents

Welcome to Tenable for Splunk	3
Components	4
Tenable Attack Surface Management Add-on	5
Source and Source Types	6
Installation and Configuration Workflow	7
Splunk Environments	8
Installation	9
Create an Input	11

- Ø

Welcome to Tenable for Splunk

Tenable Attack Surface Management (formerly known as Tenable.asm) is a web-based inventory tool that you can use to identify internet-accessible assets that your organization may or may not know about. Tenable Attack Surface Management identifies assets using DNS records, IP addresses, and ASN, and includes more than 180 columns of metadata to help you organize and inventorize your assets. The Tenable Attack Surface Management Add-on for Splunk performs data collection and normalization.

O

Components

- Ø -

Tenable Attack Surface Management Add-on

The Tenable Attack Surface Management Add-On for Splunk pulls data from Tenable platforms and normalizes it in Splunk.

 \bigcirc

The current Tenable Attack Surface Management Add-On uses the following API endpoints:

Subscriptions

Get subscriptions from store.

• GET /smartfolder

Inventory

List the assets in your inventory.

• POST /inventory

Source and Source Types

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

The Tenable Attack Surface Management Add-on for Splunk stores data with the following source and source type.

O

Source	Source type	Description
<username> <address></address></username>	tenable:asm:domains	This collects all assets data.

Installation and Configuration Workflow

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

Before you begin:

 Generate an API key in Tenable Attack Surface Management to complete the configuration. See the <u>Tenable Attack Surface Management User Guide</u> for instructions on how to generate an API key. Do not use this API key for any other third-party or custom-built application or integration. It must be unique for each installed instance of the integration.

To install and configure Tenable applications for Splunk:

- 1. Install the Tenable application.
- 2. Configure the required Tenable application for Splunk: Tenable Attack Surface Management.

Note: You need unique credentials for each Splunk environment.

3. <u>Create an input</u> for the configured Tenable application for Splunk.

Splunk Environments

The installation process for the Tenable Attack Surface Management 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 . Complete the setup to start data collection.

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 Attack Surface Management Add-On. Complete the setup for the Tenable Attack Surface Management Add-On 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

Before you begin:

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

Note: See the <u>Splunk Environments</u> 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 Attack Surface Management 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:

splunk >er	nterprise Apps -			
Search	Search & Reporting	>	Alerts	Dashboards
Searc	Splunk Essentials for Cloud and Enterprise 9.0	>		
enter s	Splunk Secure Gateway	ssg	-	
encer s	Upgrade Readiness App	30,		
No Event	Manage Apps	_		
	Find More Apps			
> Searc	ch History (?)			

- 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.asm Add-on for Splunk.
- 6. Restart Splunk if a **Restart Required** prompt displays.

Note: Follow steps 1 to 6 to install the Tenable Attack Surface Management App for Splunk.

To upgrade Tenable Attack Surface Management Add-on for Splunk:

- 1. Log in to Splunk.
- 2. Go to **Apps** at the top of the screen.
 - A drop-down menu appears:

splunk >e	nterprise Apps -	
Anne	Search & Reporting	>
Apps	Tenable Add-On for Splunk	0
Showing 1	Tenable App for Splunk	0
filter	Manage Apps	
Name \$	Find More Apps	
SplunkFo	rwarder Splu	inkForwarder
Colorada	hitaanaalaa Cali	

- 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 Attack Surface Management 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 Attack Surface Management.

O

To create an input:

1. In the left navigation bar, click **Tenable Attack Surface Management**.

splunk	>enterprise			🥏 Administrator 🔻 Messages 🔻	Settings ▼ Activity ▼ Help ▼	Q Find
Apps	¢	Explore Splunk Enterprise				Î
>	Search & Reporting	Г.			>_	
>	Splunk Essentials for Cloud and Enterprise 9.0	Product Tours	Add Data	Splunk Apps 🖄	Splunk Docs 🖄	
ssg	Splunk Secure Gateway	New to Splunk? Take a tour to help you on your way.	Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.	Apps and add-ons extend the capabilities of Splunk Enterprise.	Comprehensive documentation for Splunk Enterprise and for all other Splunk products.	
\bigcirc	Tenable.asm for Splunk				optime products.	Close
ΞQ	Upgrade Readiness App					
	Update					
	+ Find More Apps					
				ne dashboard		

2. Click the **Inputs** tab.

nputs Configuration Search				Administrato	r ▼ Messages ▼ S	Settings ▼ 4	Activity 🔻 He	Find
nputs Ianage your data inputs								Create New Input
Input 10 Per Page 🕶			filter		Q			
i Name *	Interval ¢	Index ¢		Status ¢		Actions		
				C Enabled		/ []	Î	

3. Click Create New Input.

The Add Tenable Attack Surface Management window opens.

splunk >enterprise Apps *		Adminis	strator 🔻 Messages 🔻 Se	ttings 👻 Activity 🔻	Help • Find
Inputs Configuration Search	Add Tenable.asm		\times		
Inputs					Create New Input
Manage your data inputs	Name	Enter a unique name for the data input			
1 Input 10 Per Page 🕶	Interval				
Name * Interval asm_one 3600		Time interval of input in seconds.		Actions	
	Index	default			
	Tenable.asm Domain	bitdiscovery.com			
	Tenable.asm API Key				
			Cancel Add		

 \bigcirc

4. Provide the following information.

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

Tenable Attack Surface Management

Input Parameters	Description	Required
Name	The unique name for each Ten- able data input.	Yes
Interval	The interval parameter specifies when the input restarts to per- form the task again (in seconds). The interval amount must be between 3600 and 86400.	Yes
Index	The index in which to store Ten- able Vulnerability Management data.	Yes

	- Ø	
Tenable Attack Surface Management Domain	Splunk pulls data from this Ten- able account.	Yes
Tenable Attack Surface Management API Key	Tenable Attack Surface Man- agement API Key.	Yes

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