# Table of Contents

**Welcome to Tenable for Splunk** ................................................................. 3

Components .................................................................................................. 4

Tenable Tenable Web App Scanning Add-on .............................................. 5

Source and Source Types ........................................................................... 6

**Installation Workflow** ............................................................................. 7

Splunk Environments .................................................................................. 8

Installation .................................................................................................. 9

Configure Tenable Web App Scanning ....................................................... 11

**Create an Input** ...................................................................................... 14
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

<table>
<thead>
<tr>
<th>Source</th>
<th>Source type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;username&gt;</td>
<td>&lt;address&gt;</td>
<td>tenable:io:vuln:was</td>
</tr>
</tbody>
</table>
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 Scanning Add-on for Splunk:

1. Log in to Splunk.

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

   A drop-down menu appears:

   ![App menu](image)

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.
Configure Tenable Web App Scanning

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

**Required User Role:** Administrator

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

1. Log in to Splunk.
2. Click Apps at the top-left of the screen.

A drop-down menu appears:
3. Click the **Find More Apps**.

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

   Tenable-related options appear.

5. Enter the necessary information for each field. The following table describes the available options.

<table>
<thead>
<tr>
<th>Input Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Name</td>
<td>(Required) The unique name for each Tenable data input.</td>
</tr>
<tr>
<td>Tenable Account Type</td>
<td>(Required) The type of Tenable account – Tenable Web App Scanning, Tenable Vulnerability Management, Tenable.sc API Keys, or Tenable.sc Certificate</td>
</tr>
<tr>
<td>Address</td>
<td>(Required) The hostname or IP address for Tenable Vulnerability Management.</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>If enabled, Splunk verifies the SSL certificate in Tenable Vulnerability Management.</td>
</tr>
<tr>
<td>Tenable.io Domain</td>
<td>(Required) URL of Tenable server.</td>
</tr>
<tr>
<td>Tenable.io Access Key</td>
<td>(Required) Your Tenable account API access key.</td>
</tr>
<tr>
<td>Tenable.io Secret Key</td>
<td>(Required) Your Tenable account API secret key.</td>
</tr>
<tr>
<td>Proxy Enable</td>
<td>Enables the plugin to collect Tenable Vulnerability Management data via a proxy server. If you select this option, the plugin prompts you to enter the following:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Proxy Type</strong> – the type of proxy used.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Proxy Host</strong> – the hostname or IP address of the proxy server.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Proxy Port</strong> – the port number of the proxy server.</td>
</tr>
</tbody>
</table>
server.

- **Proxy Username** - the username for an account that has permissions to access and use the proxy server.

- **Proxy Password** - the password associated with the username you provided.

6. Click **Add** to complete the configuration.

**Next steps**

- [Create an Input](#) for the Tenable Tenable Web App Scanning Add-On for Splunk.
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**.

2. Click the **Inputs** tab.
3. Click **Create New Input**.

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

![Add Tenable Web App Scanning Add-on for Splunk window]

4. Provide the following information.

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

**Tenable Web App Scanning**

<table>
<thead>
<tr>
<th>Input Parameters</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The unique name for each Tenable data input.</td>
<td>Yes</td>
</tr>
<tr>
<td>Interval</td>
<td>The interval parameter specifies when the input restarts to perform the task again (in seconds). The interval amount must be between 300 and 86400.</td>
<td>Yes</td>
</tr>
<tr>
<td>Index</td>
<td>The index in which to store Tenable Vulnerability Management data.</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Start Time</strong></td>
<td>The date and time to start collecting data. If you leave this field blank, the integration collects all historical data.</td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>Uses the <code>YYYY-MM-DD hh:mm:ss</code> format.</td>
<td></td>
</tr>
<tr>
<td><strong>Tenable Vulnerability Management Domain</strong></td>
<td>Splunk pulls data from this Tenable account.</td>
<td></td>
</tr>
<tr>
<td><strong>Tenable Vulnerability Management Access Key</strong></td>
<td>Tenable Vulnerability Management API access key.</td>
<td></td>
</tr>
<tr>
<td><strong>Tenable Vulnerability Management Secret Key</strong></td>
<td>Your Tenable Vulnerability Management API secret key</td>
<td></td>
</tr>
</tbody>
</table>

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