SPLUNK INSTALLATION

By: SAMEER HASSAN

GitHub-link: GitHub - sameerhassancode/Wazuh-labs

LinkedIn: https://www.linkedin.com/in/sameer-hassan-15a428255/

What is Splunk?

Splunk is a powerful log management and SIEM tool used for:

Collecting machine data from servers, apps, network devices

Indexing, searching, and analyzing logs in real time

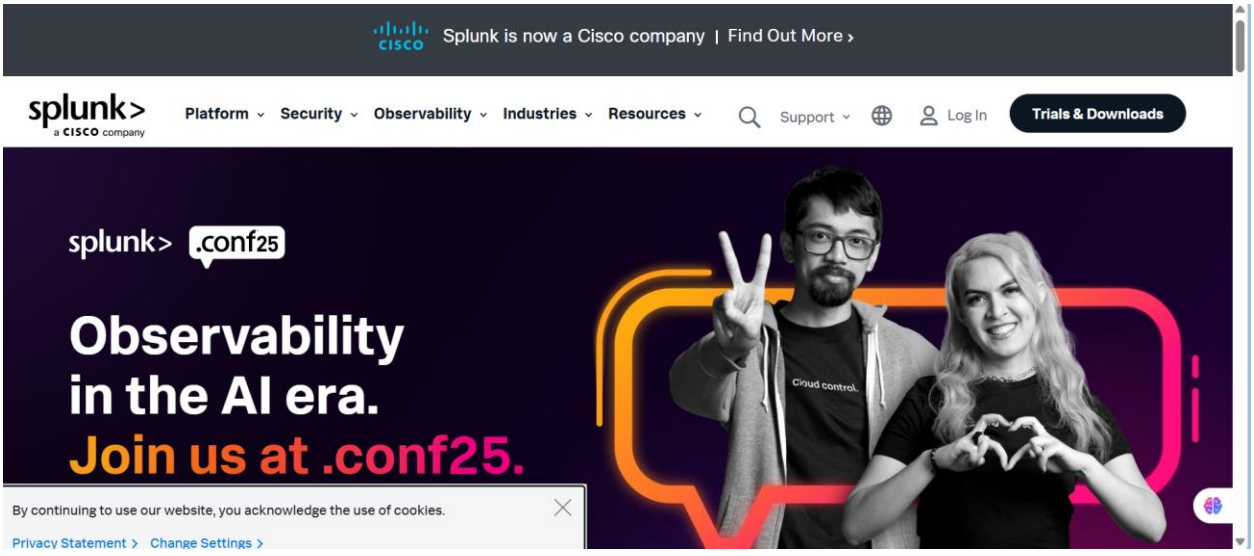
Creating dashboards, alerts, and reports for monitoring and security

Splunk is very flexible, user-friendly, and is often used by:

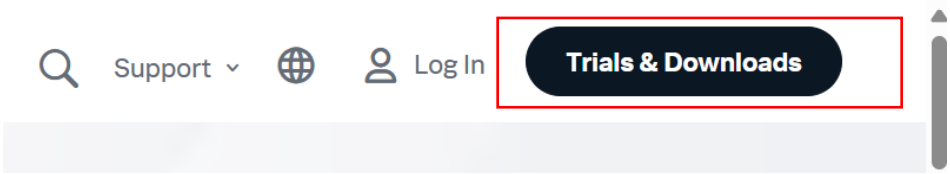
- SOC teams
- IT operations
- DevOps and SREs
- Security analysts

Installation:

Go to the official Splunk website:

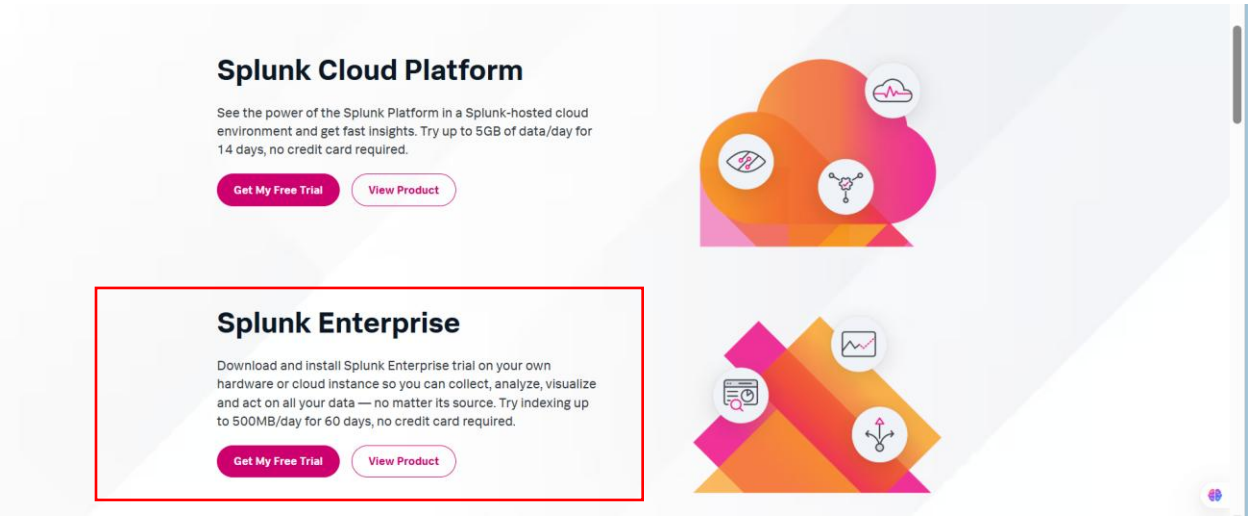


Click on Trail and Download:

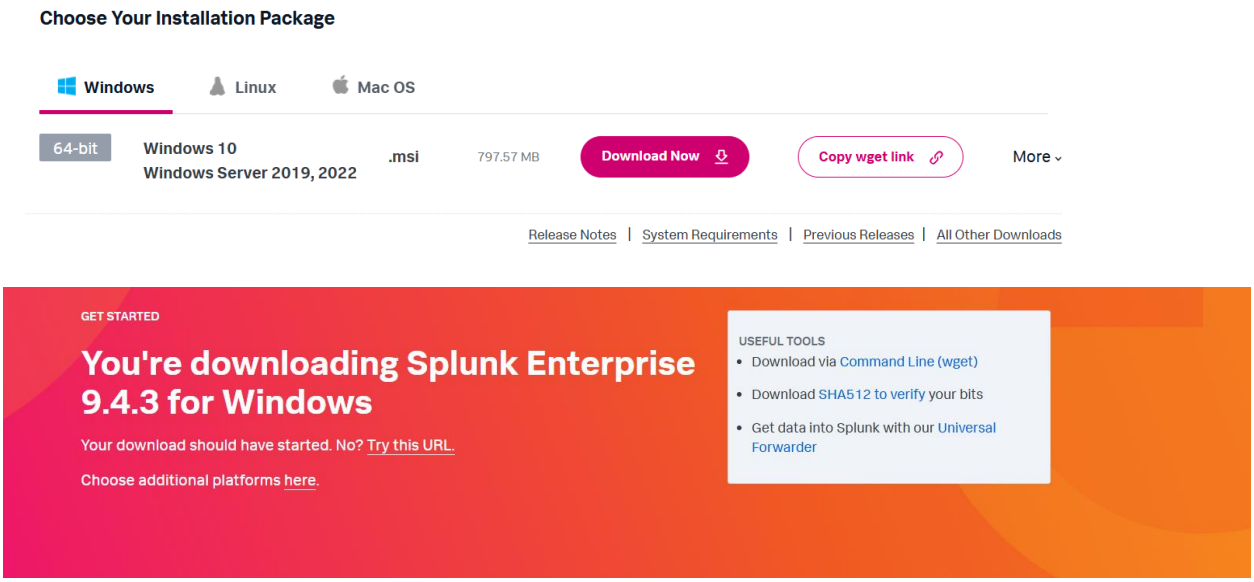


Here you have 2 options Splunk cloud or download on your pc (Splunk Enterprise)

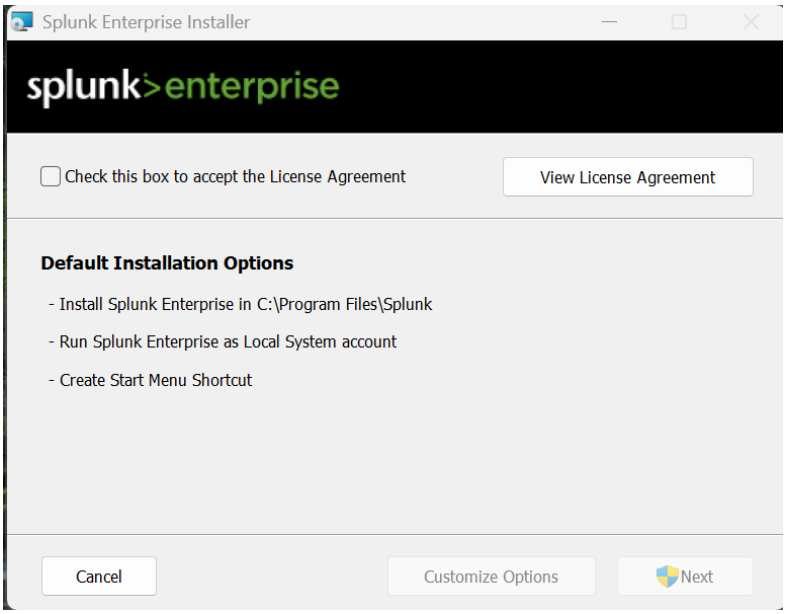
I will go with Splunk enterprise. (60 day free Trail**)**



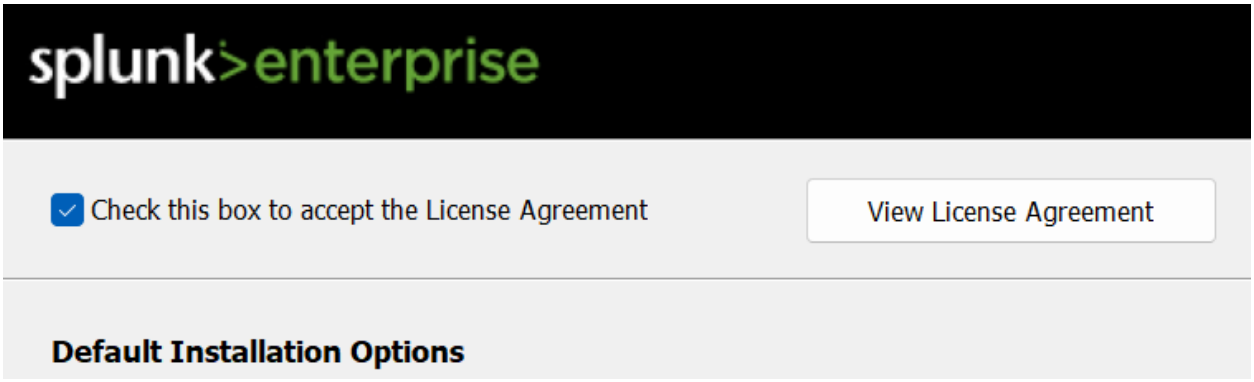
It will redirect you to registration page. Complete the registration and click download Splunk.



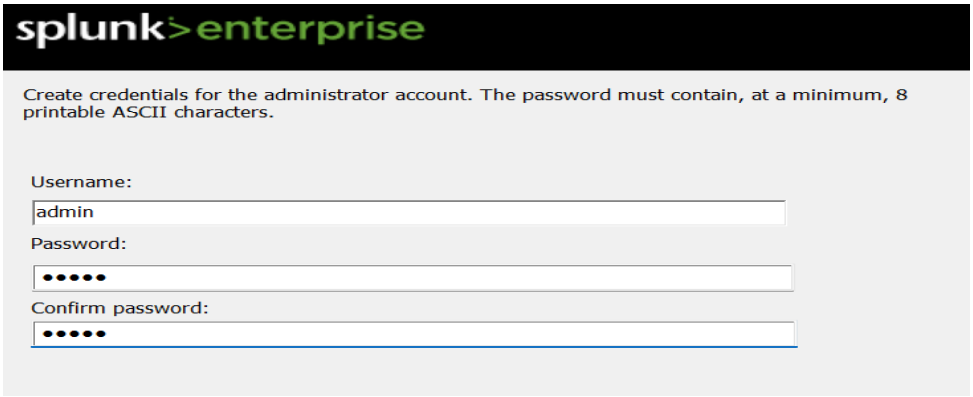
Now open the exe file:



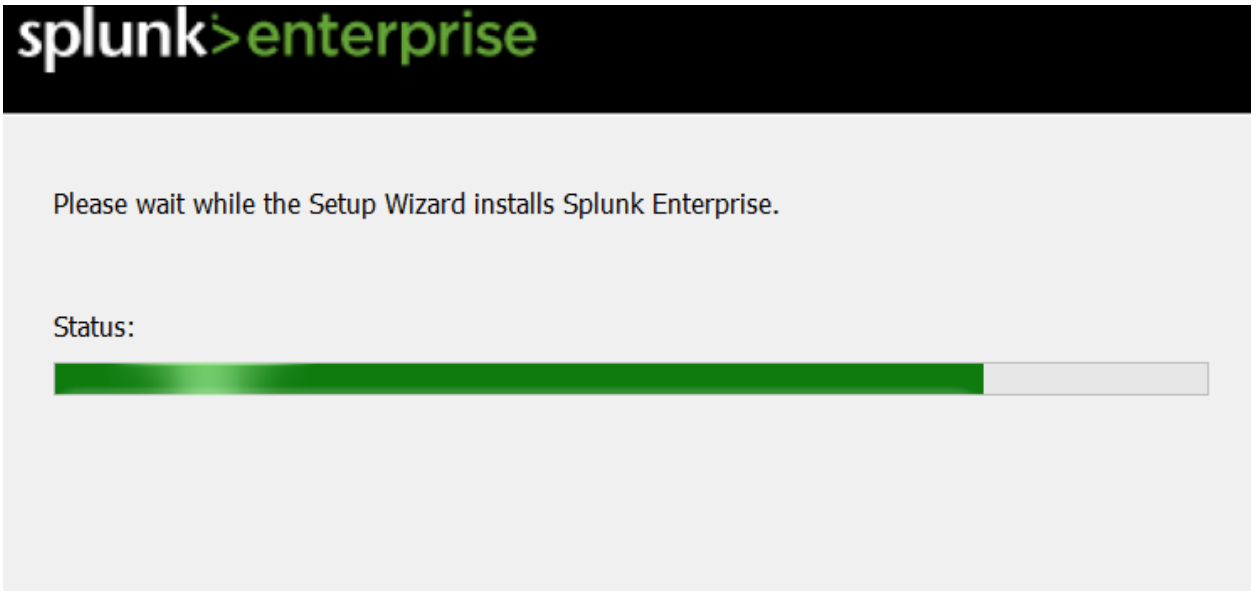
Click on License agreement check box and click next



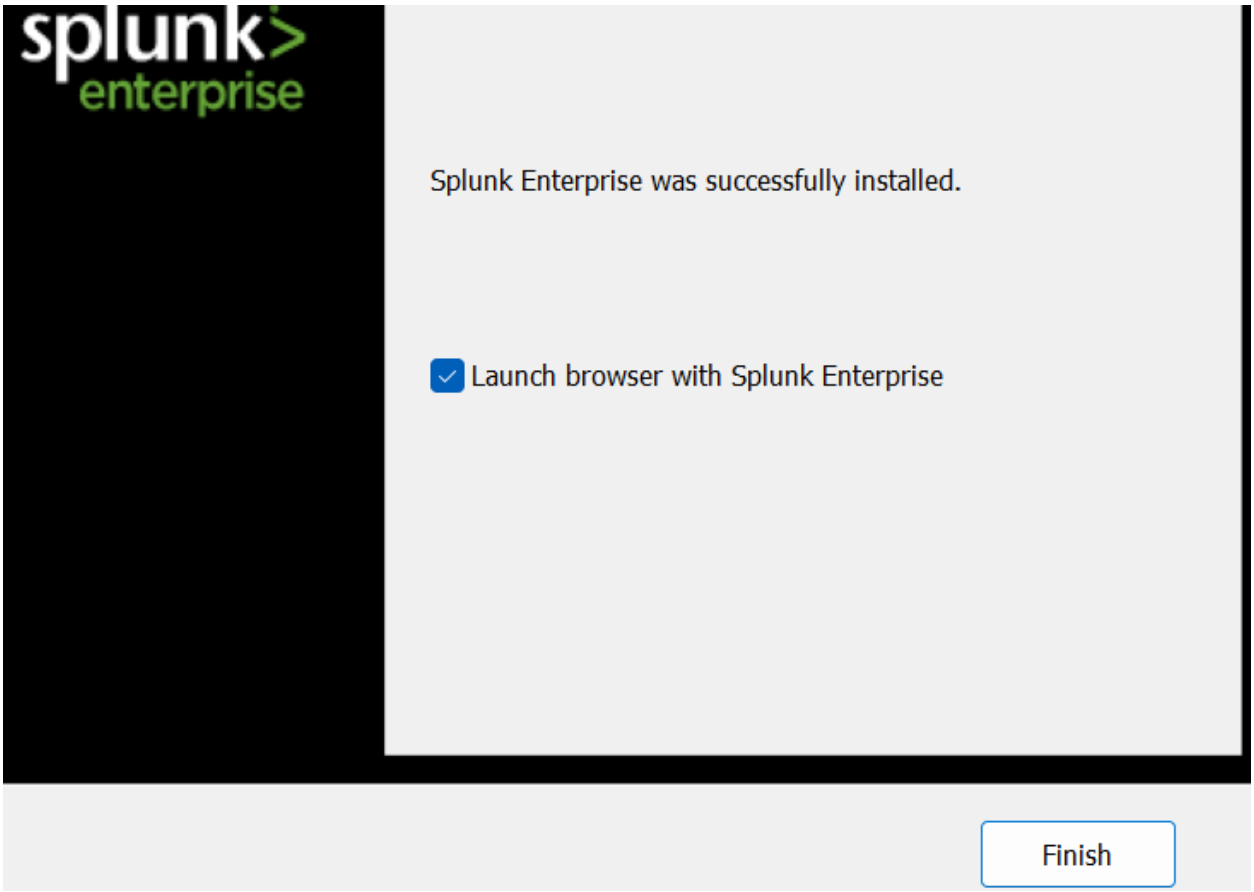
Now create username and password for login!



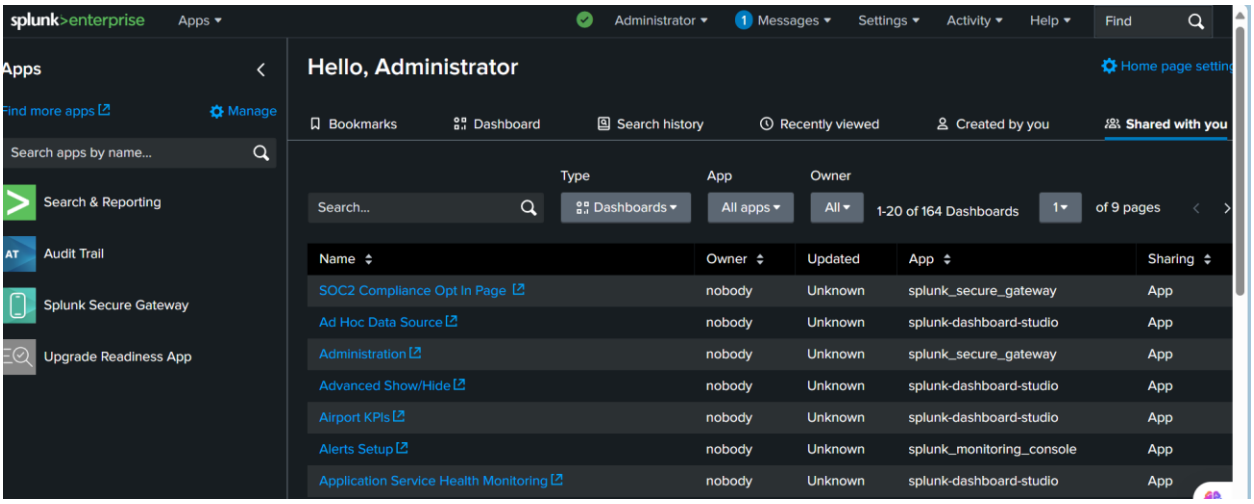
After that click install button and wait for the process to complete!



Click finish and Splunk will automatically open in your browser!



Here’s view of admin SIEM



Summary:

Splunk installation involves downloading the installer from the official Splunk website based on your operating system. After running the installer, follow the setup wizard or use CLI commands to complete the installation. Once installed, access the Splunk web interface on port 8000. From there, you can start indexing data and configuring your Splunk environment.