LetsDefend

Splunk Installation on Windows

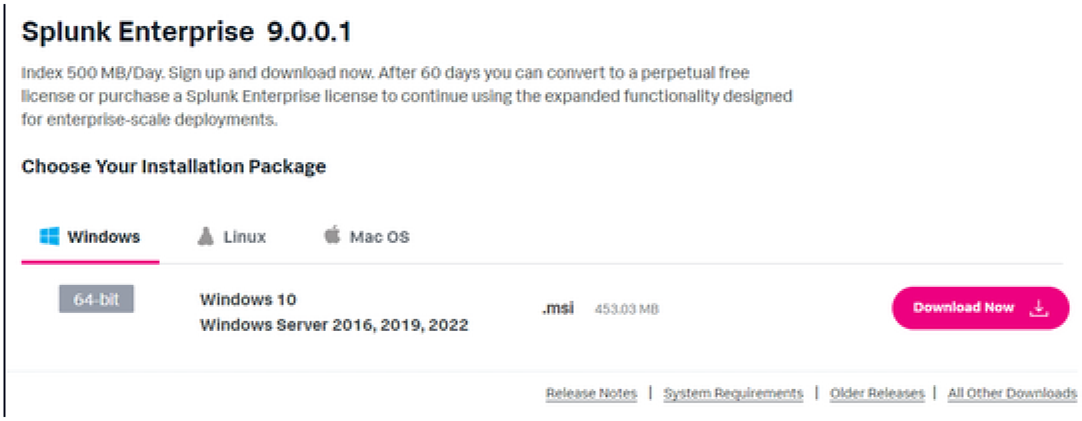
By: Ryan Stewart

For this training session, I'll guide you through the installation of Splunk on a virtual machine running Windows Server 2022.

1. Visit the Splunk official website.

2. Create a Splunk account.

3. Download the MSI installer.



Splunk Enterprise 9.0.0.1

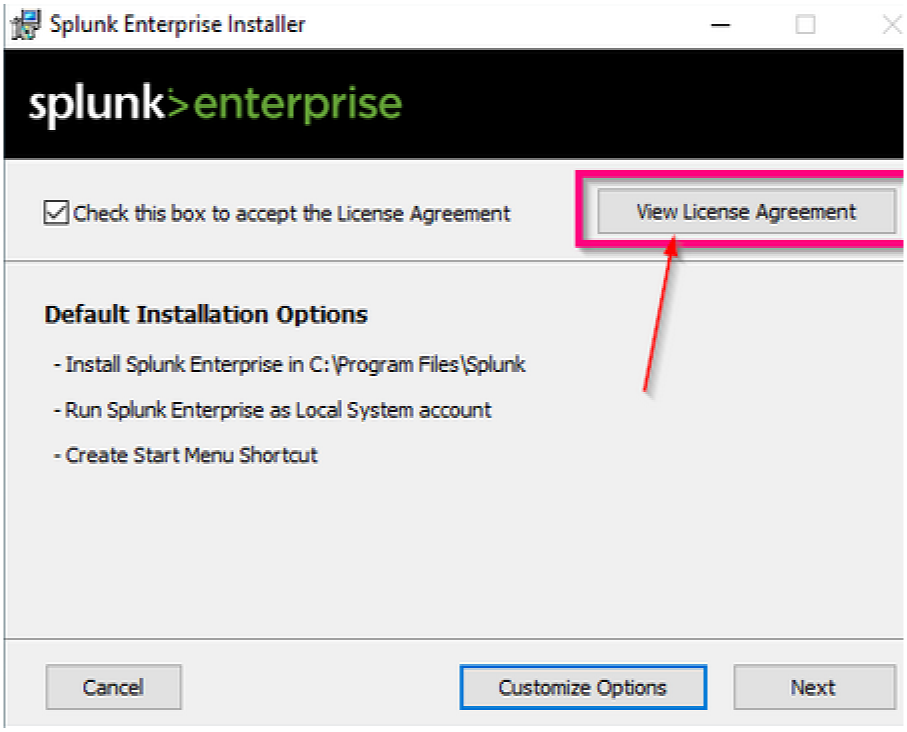
Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

Choose Your Installation Package

Windows
Linux
Mac OS
Download Now
Release Notes | System Requirements | Older Releases | All Other Downloads

64-bit	Windows 10 Windows Server 2016, 2019, 2022	.msi	453.03 MB

4. Carefully Read the License Agreement:
   - Although it may seem routine, it is crucial to read and comprehend the License Agreement as it contains vital enterprise information. Understanding the terms is essential for handling your data responsibly.

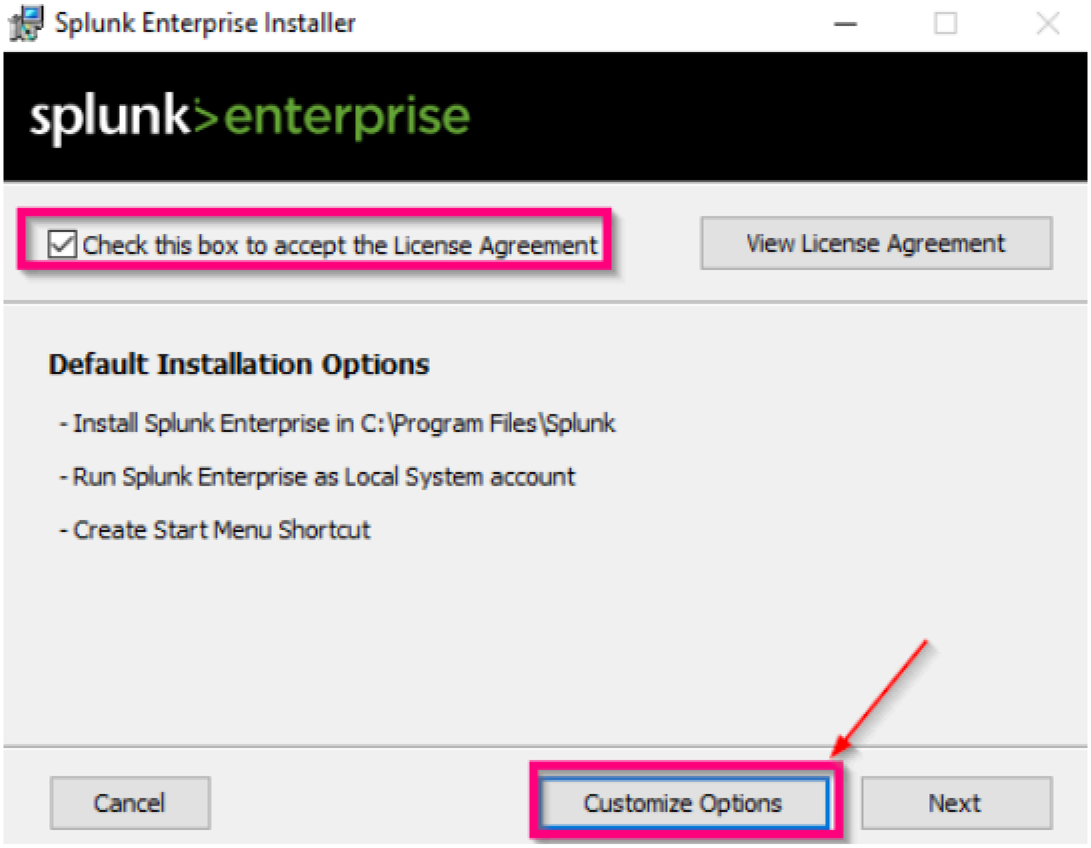


☑ Check this box to accept the License Agreement

Default Installation Options

- Install Splunk Enterprise in C:\Program Files\Splunk
- Run Splunk Enterprise as Local System account
- Create Start Menu Shortcut

5. Accept the License Agreement:
 - Choose to customize options even if default configurations are maintained for training purposes.



☑ Check this box to accept the License Agreement

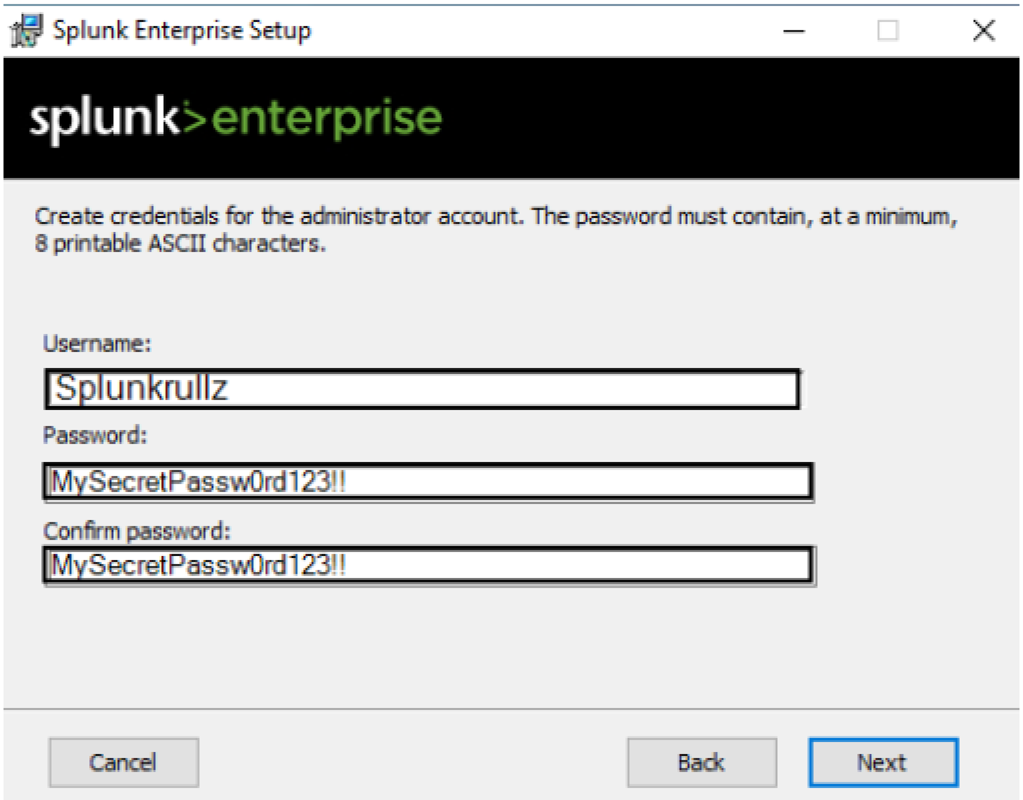
Default Installation Options

- Install Splunk Enterprise in C:\Program Files\Splunk
- Run Splunk Enterprise as Local System account
- Create Start Menu Shortcut

6. Select Installation Location:
   - Specify the preferred installation directory for Splunk.

7. Install Splunk as a Local System:
   - Opt to install Splunk with local system permissions.

8. Set Credentials:
   - Configure login credentials for accessing Splunk.



Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.

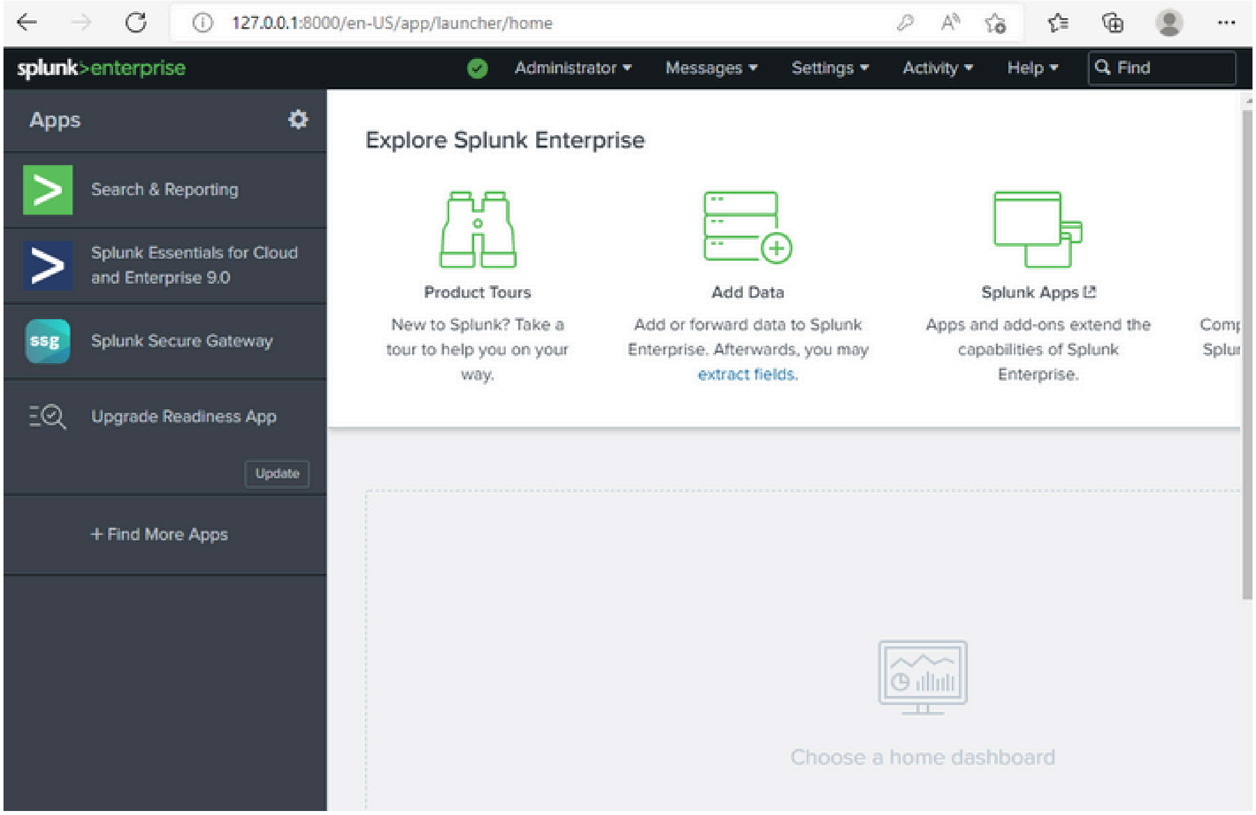
Username: Splunkrullz

Password: MySecretPassw0rd123!!

Confirm password: MySecretPassw0rd123!!

9. Initiate Installation:
   - Launch the installation process and patiently wait for its completion.

10. Verify Splunk Installation:
   - After the installation is complete, attempt to connect to:
https://127.0.0.1:8000



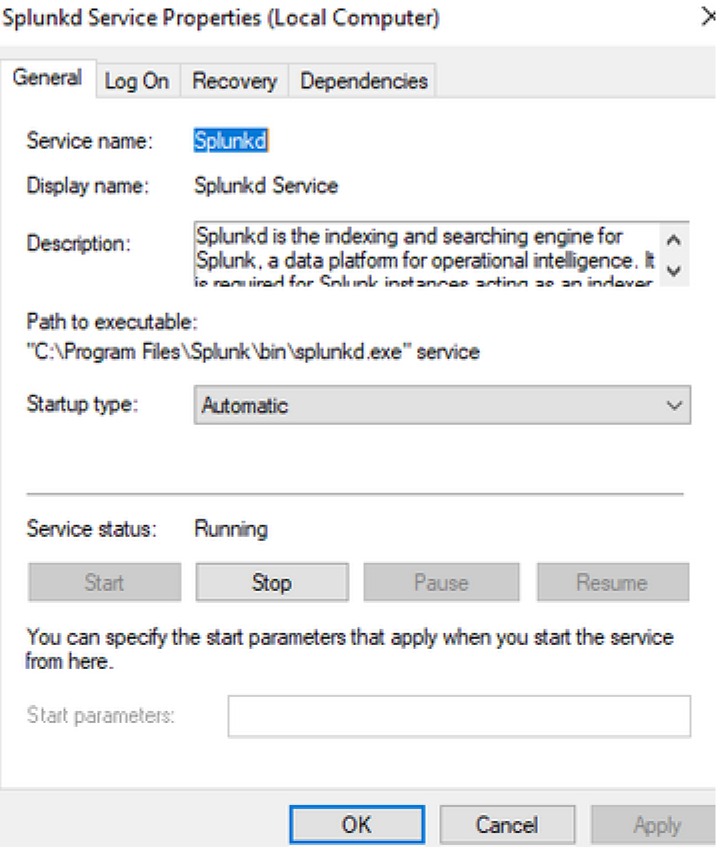
New to Splunk? Take a tour to help you on your way.

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

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

Congratulations! You have successfully installed Splunk!

Supervision:
- Check the "Splunkd Service" in services.msc, ensuring its startup type is set to "**automatic**" and it is in a running status. Monitoring this service and its status provides insights into the operational state of your Splunk installation.



Splunkd Service Properties (Local Computer)

Service name: Splunkd

Display name: Splunkd Service

Description: Splunkd is the indexing and searching engine for Splunk, a data platform for operational intelligence. It is required for Splunk instances acting as an indexer

Path to executable:
"C:\Program Files\Splunk\bin\splunkd.exe" service

Startup type: Automatic

Service status: Running

You can specify the start parameters that apply when you start the service from here.

Start parameters: