

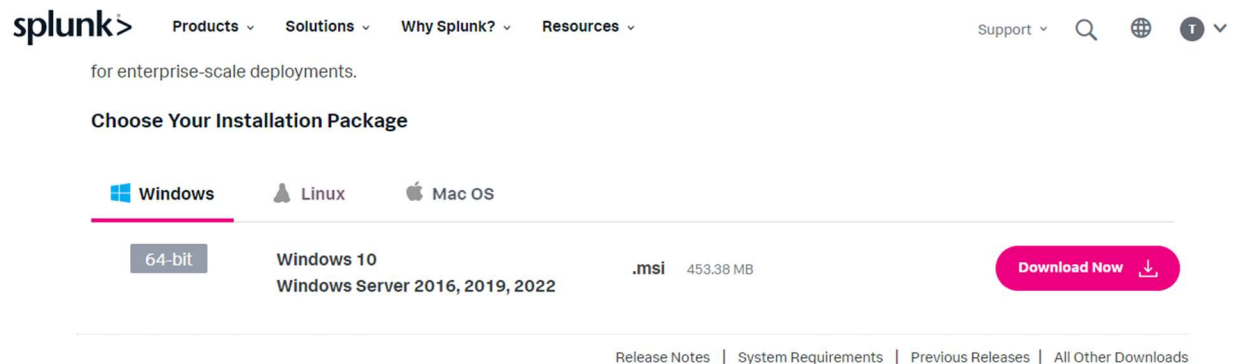
Installing Splunk Enterprise & Setting up Universal Forwarder

Hosting Splunk on Windows

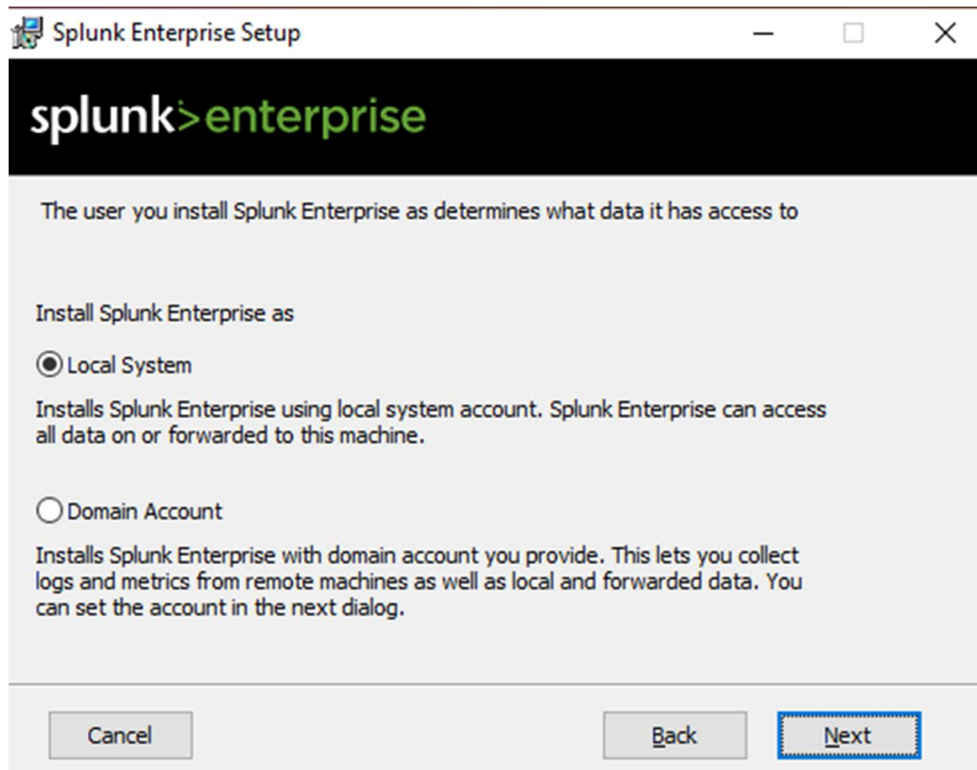
First to download Splunk, Go to:

https://www.splunk.com/en_us/download/splunk-enterprise.html

Then Download the version according to your installed OS. I am downloading a free version for windows.



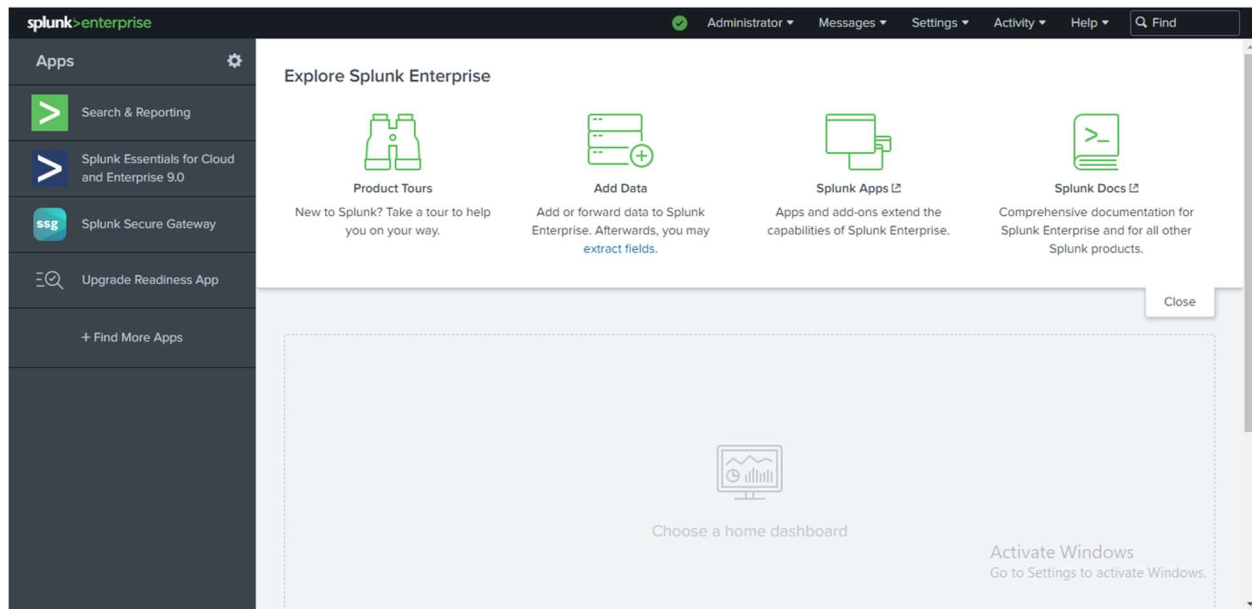
Then after downloading the “.msi” file open the Microsoft Software Installation file. Then after some processing, a UI prompt to chose account for setting up splunk is displayed. Chose the appropriate account. In this case I have chose local account.



Then we need to configure credentials for accessing Splunk. After providing credentials, hit the next button to start the installation process.

The screenshot shows the 'Splunk Enterprise Setup' window at the credential configuration step. It contains three input fields: 'Username:' with the text 'User' entered, 'Password:' with masked characters (dots), and 'Confirm password:' also with masked characters. At the bottom of the window are three buttons: 'Cancel', 'Back', and 'Next'. The 'Next' button is highlighted with a blue border.

After installation completes a prompt to open Splunk in a browser is displayed. By clicking the button, we are redirected to the login page. Then entering the credential that we created during setup allows us to get access to SIEM UI.



By logging in, we are provided with the above interface. By going to Search & Reporting we can search for logs. To do that we must first configure the auditing policy in our system and set up a log forwarder to Splunk enterprise. For the sake of forwarding logs, we are only going to enable Process Creation Log.

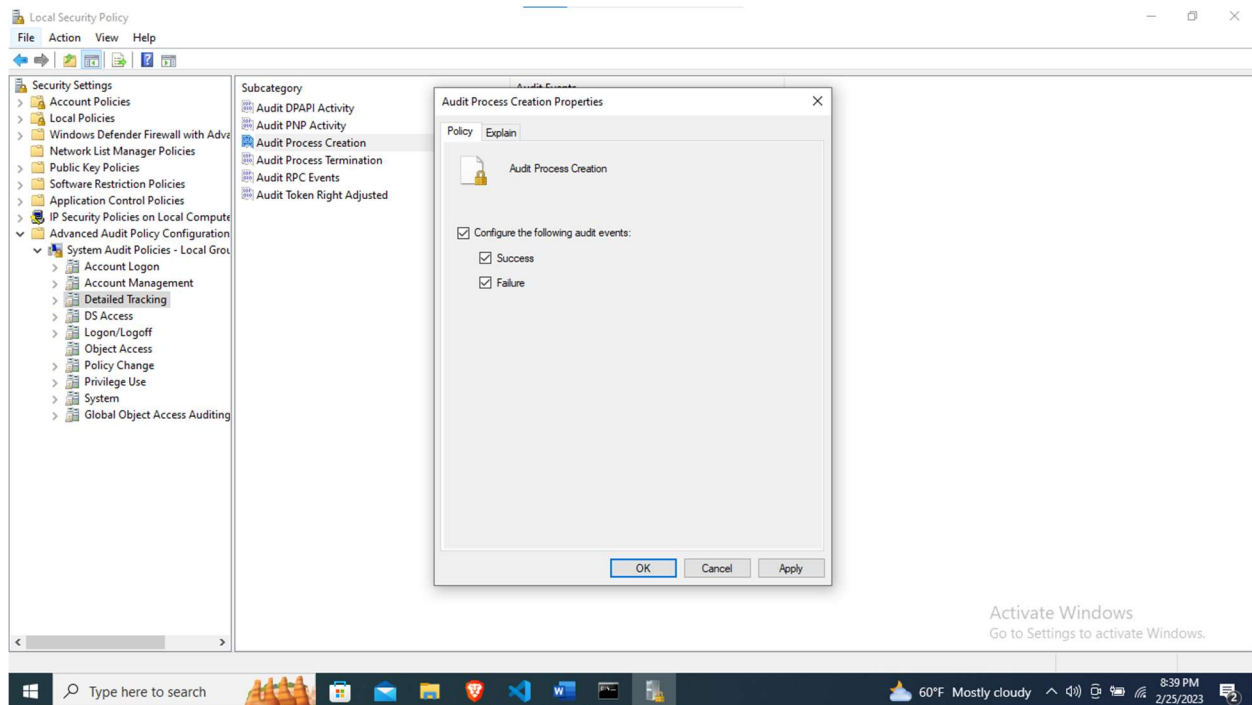
Enabling Auditing

I am currently using Windows 10 Pro. By going to the **Local Security Policy** we can configure the auditing policy.

After opening the **Local Security Policy**:

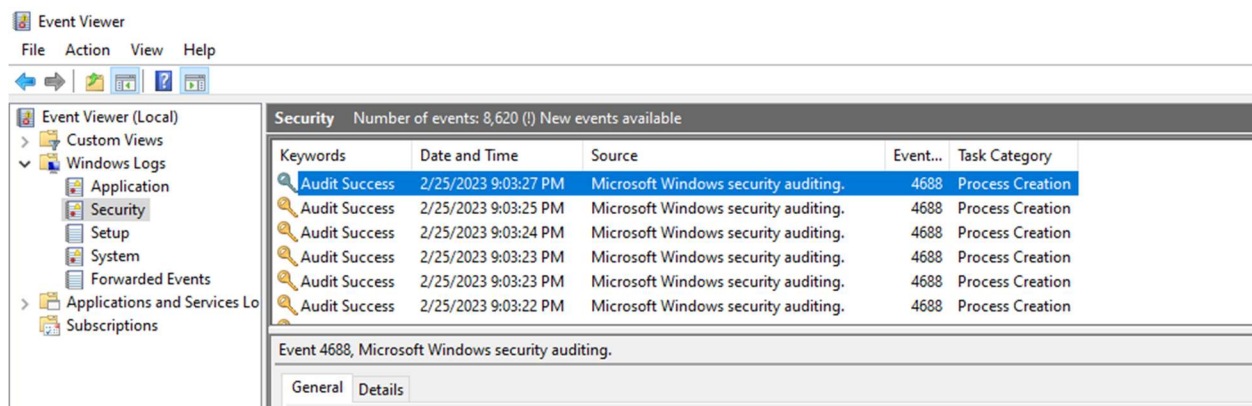
Go to “**Security Settings**” -> “**Advanced Audit Policy Configuration**” -> “**System Audit Policies – Local Group Policy Object**” -> “**Detailed Tracking**”.

Under Detailed Tracking click on “**Audit Process Creation**”. Only the “**Success**” event category will be enough for our purpose as it generates a log for every successful process creation event.



To verify if auditing is successful or not.

1. Go to event viewer.
2. Then go to "Windows Logs" -> "**Security**"
3. There we will be able to Event ID 4688 with the task category "Process Creation"



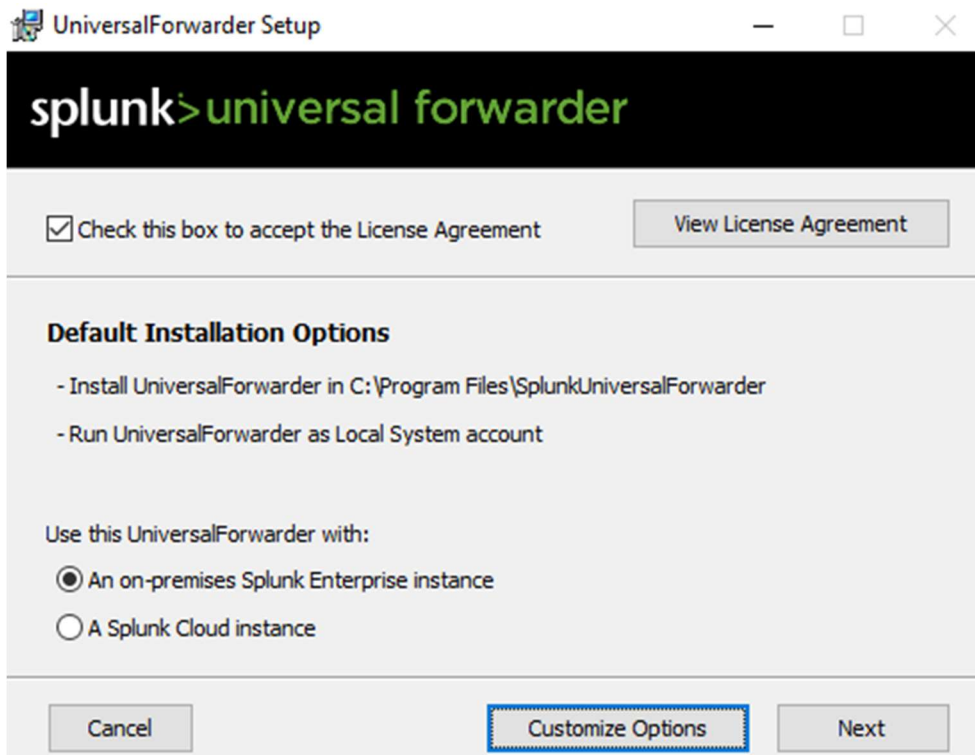
If you were to view similar events as shown above then you were successful in generating process creation logs.

Installing Universal Forwarder

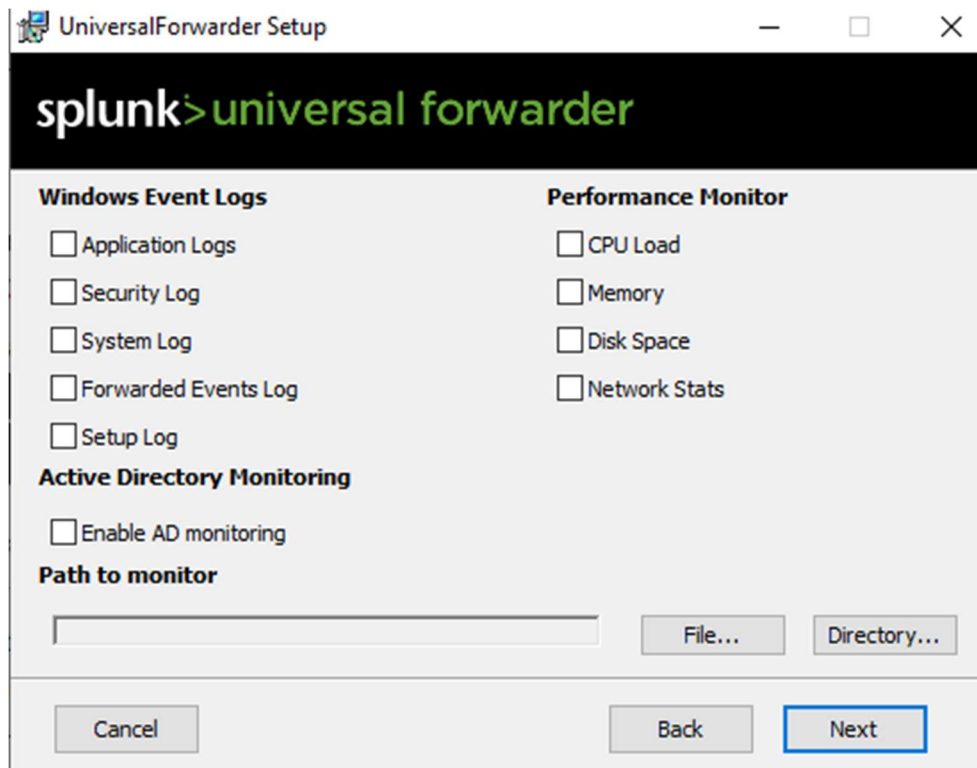
On the Splunk download page, we will be provided with options to install Universal Forwarder.

Link - https://www.splunk.com/en_us/download/universal-forwarder.html

Download the forwarder and install it to forward the log. Click on customize options to select the location to install the forwarder. Then hit next to continue. Also, you don't need to enter the password to continue.



Then choose the appropriate logs to forward and hit next to continue. As we have only enabled process creation logs so selecting **Security Log**, for now, will be sufficient.



As we are forwarding it to the Splunk instance hosted on our local system, so use the localhost IP address and leave the port as default. In case of other services are running on the port then change it to other available ports. For now, we are leaving the deployment server IP blank and setting up receiving indexer IP only.

splunk>universal forwarder

If you intend to use a Splunk receiving indexer to configure this UniversalForwarder, please specify the host or IP, and port (default port is 9997). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

Receiving Indexer

Hostname or IP

:

Enter the hostname or IP of your receiving indexer,
e.g. ds.splunk.com

default is 9997

Then after completing the installation go back to the web page where Splunk is running.

Then go to Search & Reporting.

Search **EventCode=4688** to view process creation logs (Splunk search engine is case sensitive unlike LogPoint)

The screenshot shows the Splunk Search interface. At the top, the search bar contains "EventCode=4688". Below the search bar, it indicates "34,638 events" and shows a timeline visualization. The main results table has two columns: "Time" and "Event". The first event is from 2/26/23 at 3:09:40.000 PM, with LogName=Security, EventCode=4688, EventType=0, and ComputerName=DESKTOP-40R005V. The second event is from 2/26/23 at 3:09:40.000 PM, with LogName=Security, EventCode=4688, EventType=0, and ComputerName=DESKTOP-40R005V. The interface also includes a sidebar with "SELECTED FIELDS" and "INTERESTING FIELDS", and a "Format" dropdown set to "List".

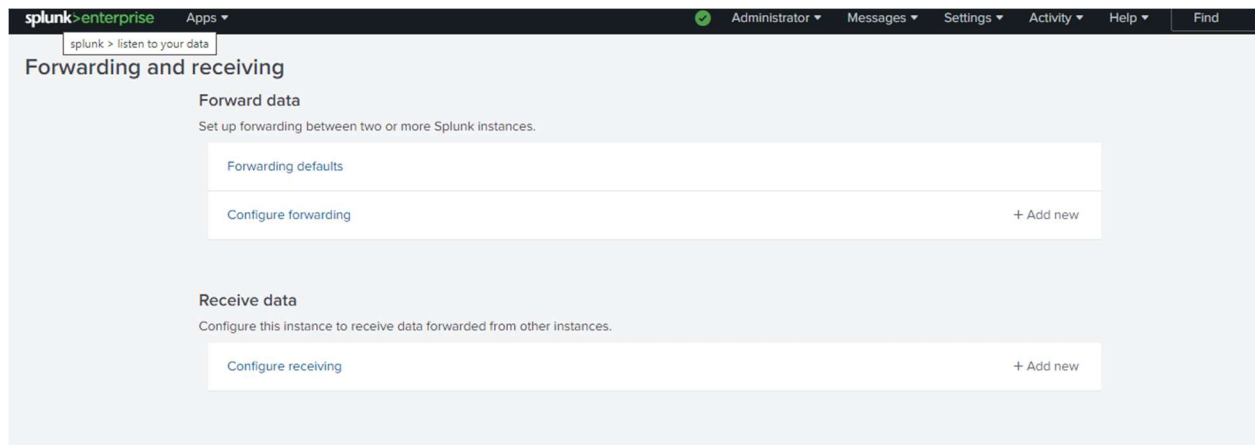
Time	Event
2/26/23 3:09:40.000 PM	LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-40R005V Show all 41 lines host = DESKTOP-40R005V source = WinEventLog:Security sourcetype = WinEventLog:Security
2/26/23 3:09:40.000 PM	LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-40R005V Show all 41 lines host = DESKTOP-40R005V source = WinEventLog:Security sourcetype = WinEventLog:Security

Log Not Forwarded Case

In case any logs are not forwarded then,

Go to **Settings -> Forwarding and Receiving**

Then go to Configure Receiving which is under Receive data.



Then by going to New Receiving Port configure the receiving port or leave it to default in case if you haven't changed it.

Configure receiving

Set up this Splunk instance to receive data from forwarder(s).

Listen on this port *

For example, 9997 will receive data on TCP port 9997.

Cancel

Save