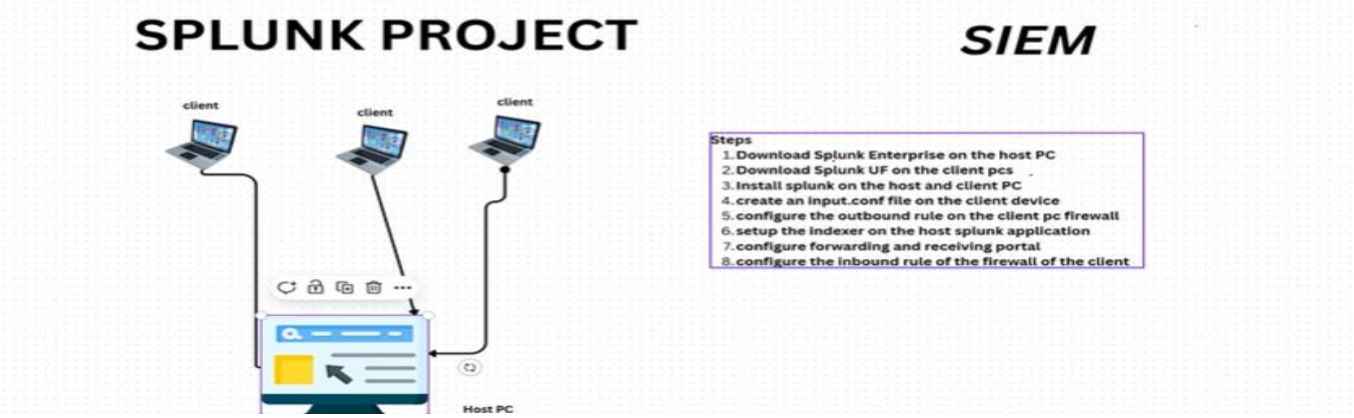


Splunk Alert Project: Detecting Failed Logins on Windows Server

Completed by Kifayah Oladejo

15/11/2025

1. Project Overview

This project demonstrates how to create and trigger a security alert in Splunk Enterprise using data collected from a Windows Server via the Splunk Universal Forwarder. The alert identifies multiple failed login attempts (Event ID 4625), which can be indicative of brute-force attacks or unauthorized access attempts.

2. Architecture & Setup

• Splunk Universal Forwarder installed on Windows Server.
• Splunk Enterprise installed on Host PC.
• Forwarder configured to send Windows Security logs to Splunk Enterprise.
• Data indexed under 'main' index with sourcetype 'WinEventLog:Security'.

3. Objective

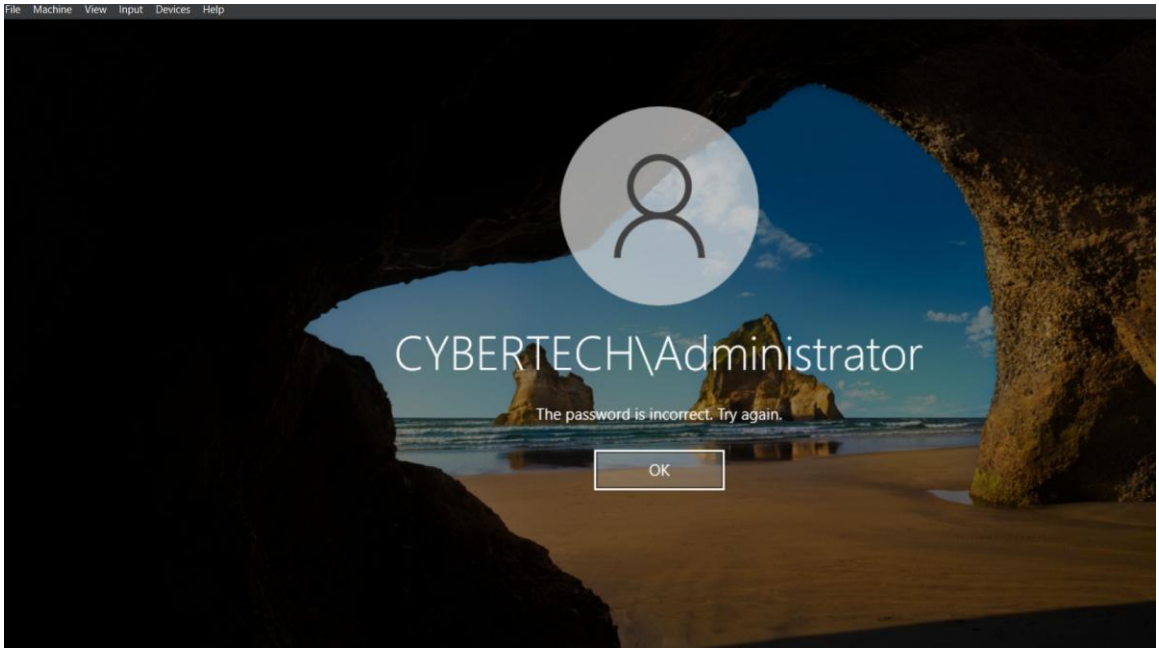
Trigger an alert when more than 5 failed login attempts (EventCode 4625) occur within a 10-minute window.

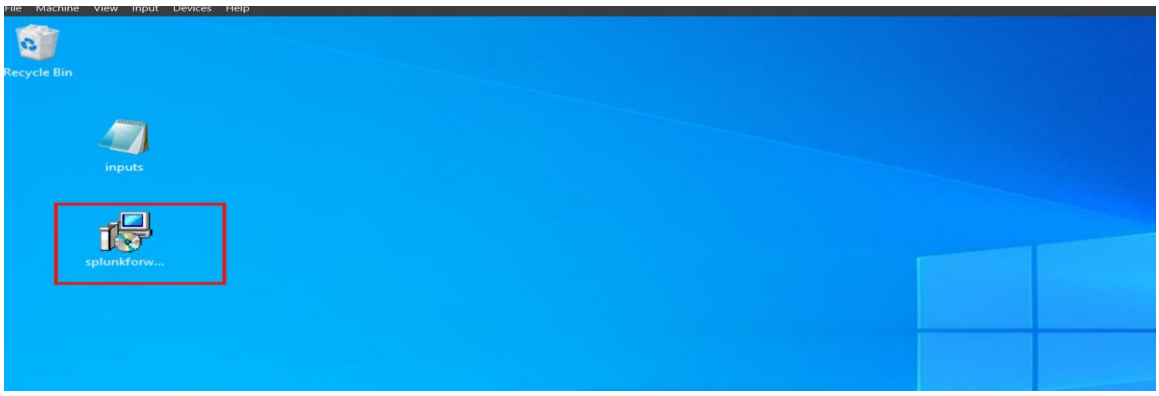
Windows logs authentication events in the Security log:

- Event ID 4625 → Failed login attempt.

- Event ID 4624 → Successful login.

For the sake of this documentation, I tried inputting the wrong password three times and then entered the correct password in the fourth attempt.



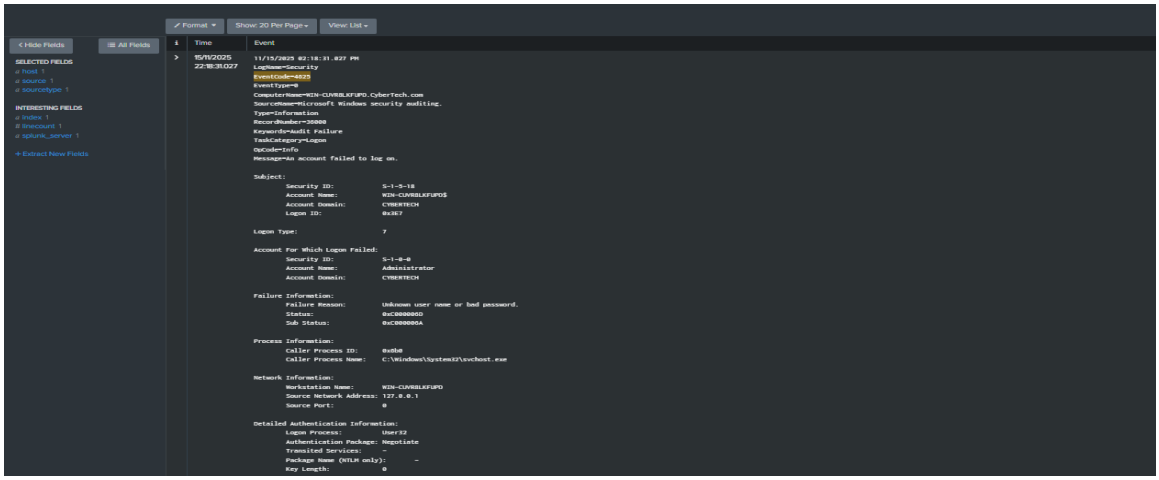


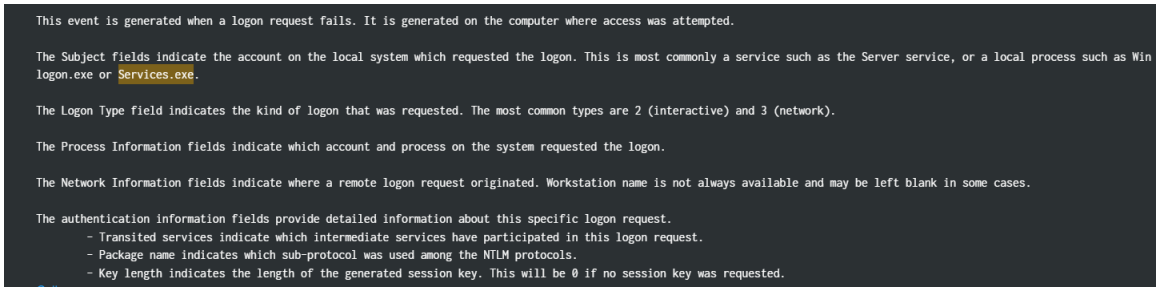
4. Splunk Search Query

The following SPL query was used to detect failed login attempts:

index=main sourcetype=WinEventLog:Security EventCode=4625
| stats count by Account_Name, host
| where count > 5

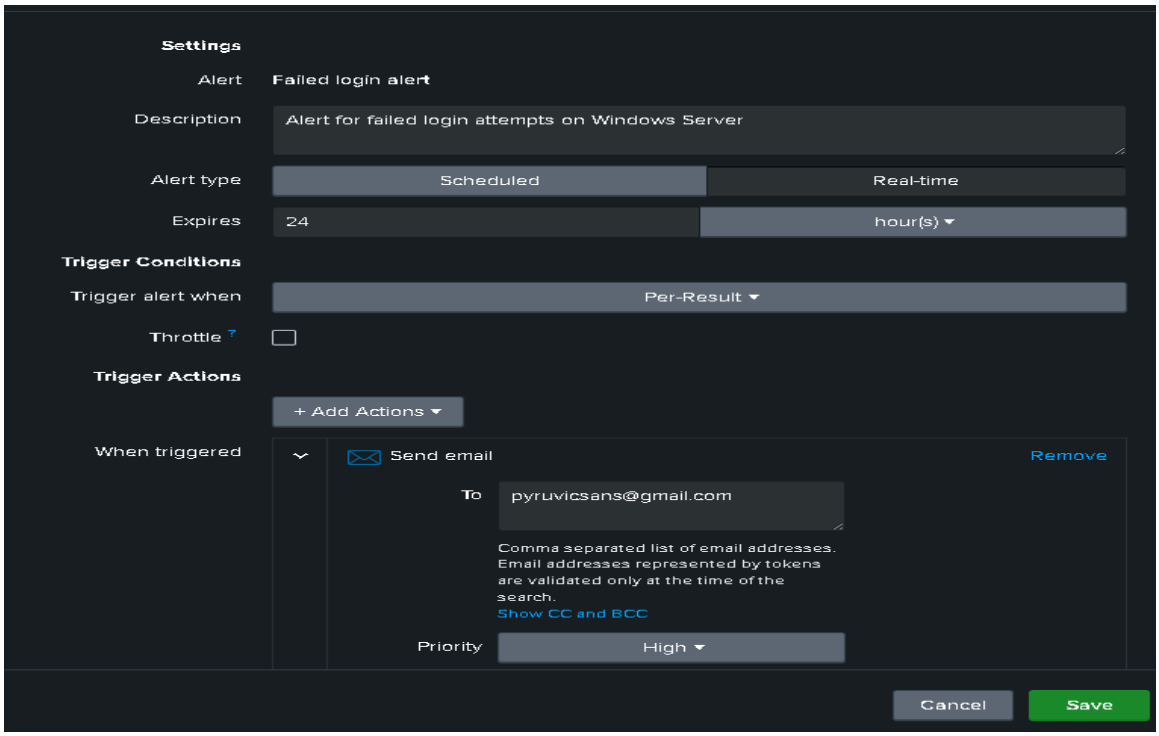
Host=computer_name LogName="Security" EventCode=4625





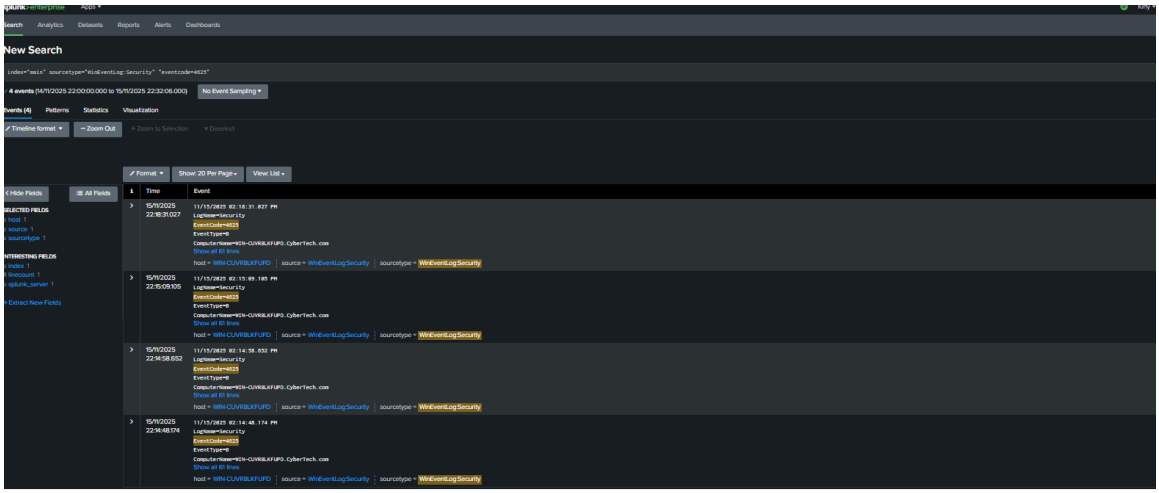
5. Alert Configuration

• Title: Failed Logins Alert
• Type: Scheduled Alert (Every 10 minutes)
• Time Range: Last 10 minutes
• Trigger Condition: Number of results > 4
• Trigger Actions: Send Email (Configured via SMTP in Splunk Settings)



6. Simulating the Alert

To simulate real-world conditions, failed login attempts were manually triggered on the Windows Server using the `runas` command with incorrect credentials. This ensured multiple Event ID 4625 logs were generated and forwarded to Splunk for processing.



7. Validation & Output

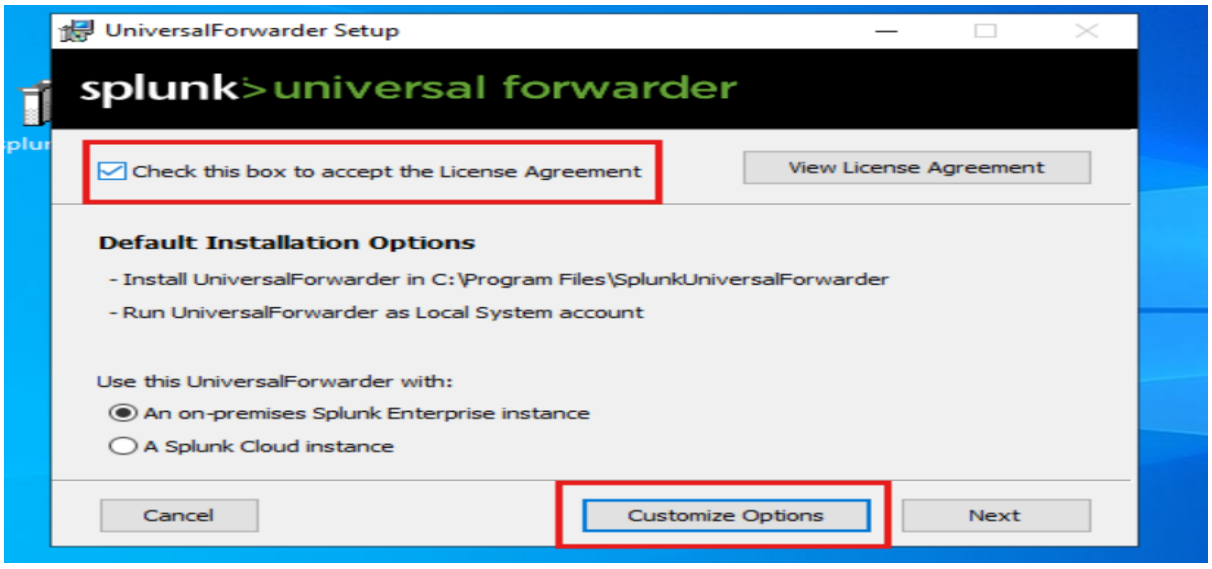
The alert was successfully triggered after 6 failed login attempts. It appeared in the 'Triggered Alerts' section of Splunk and an email notification was received, confirming successful detection and response.

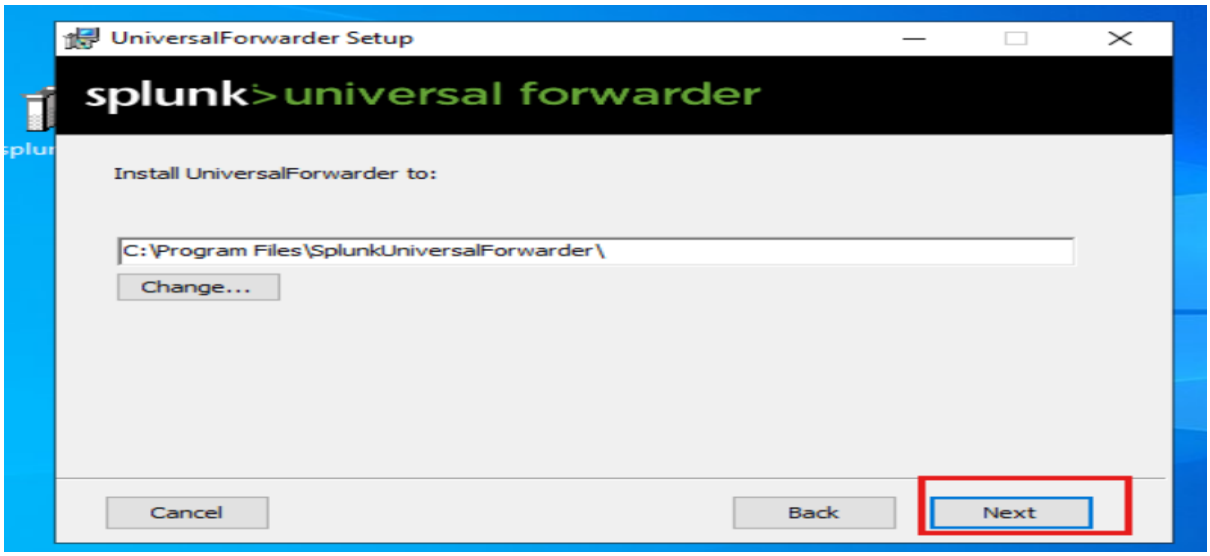
8. Conclusion

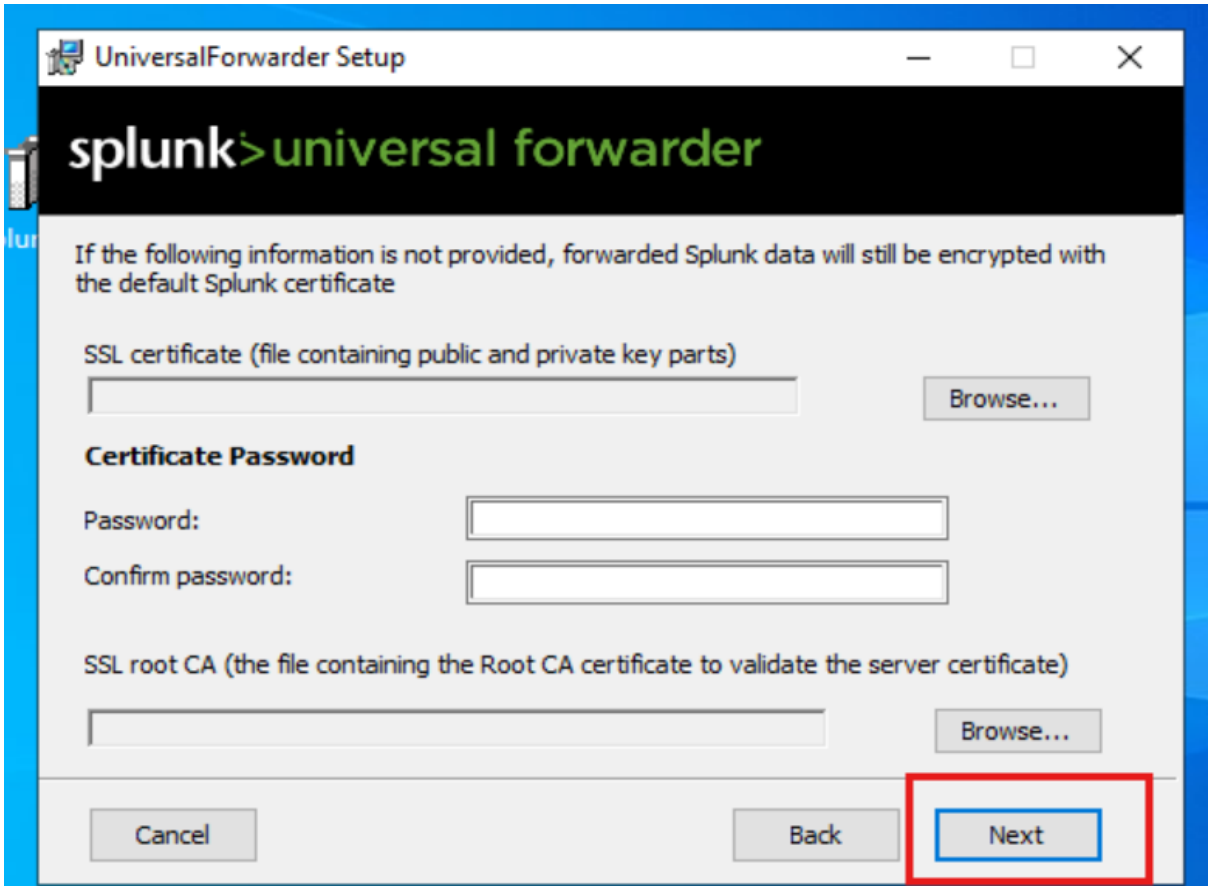
This project demonstrates the practical use of Splunk for real-time log monitoring and alerting.

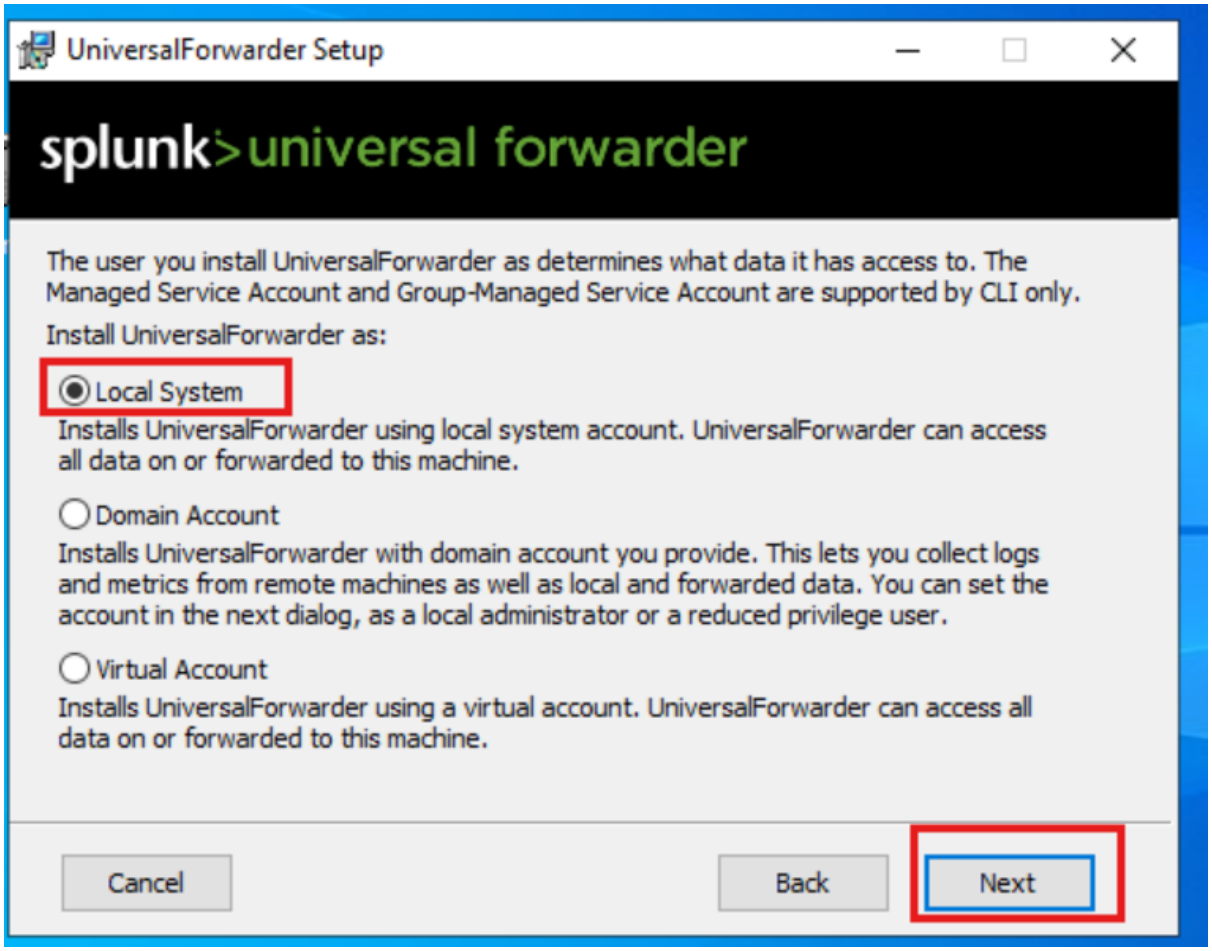
Screenshots downloading splunk>universal forwarder:

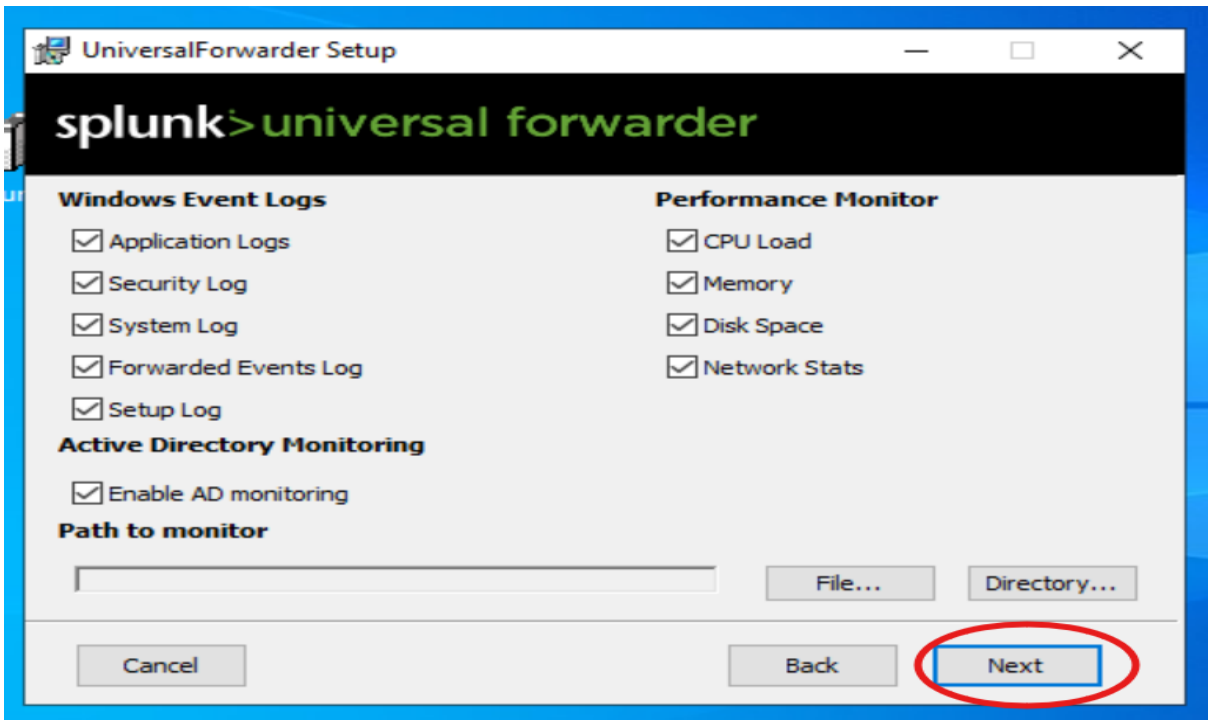
https://www.splunk.com/en_us/download/universal-forwarder.html

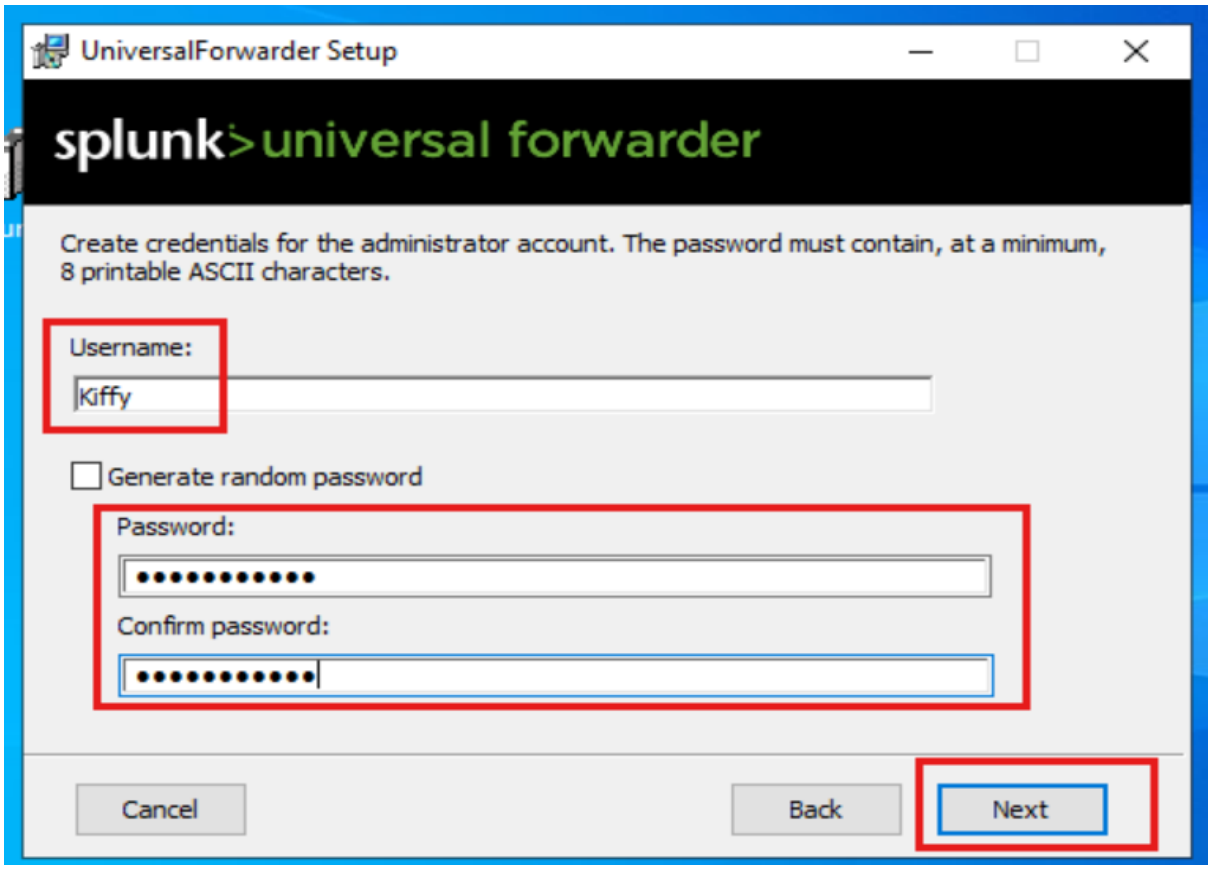


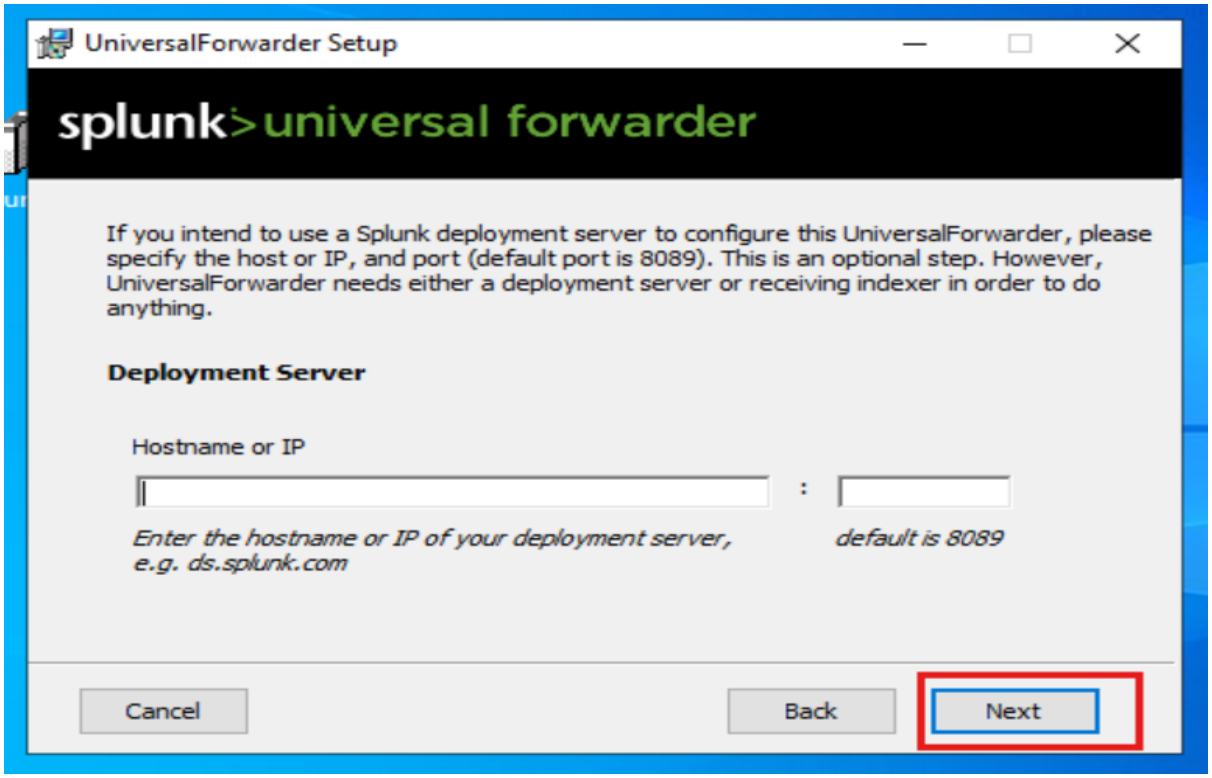

UniversalForwarder Setup
splunk>universal forwarder
Install UniversalForwarder to:
C:\Program Files\SplunkUniversalForwarder\
Change...
Cancel
Back
Next

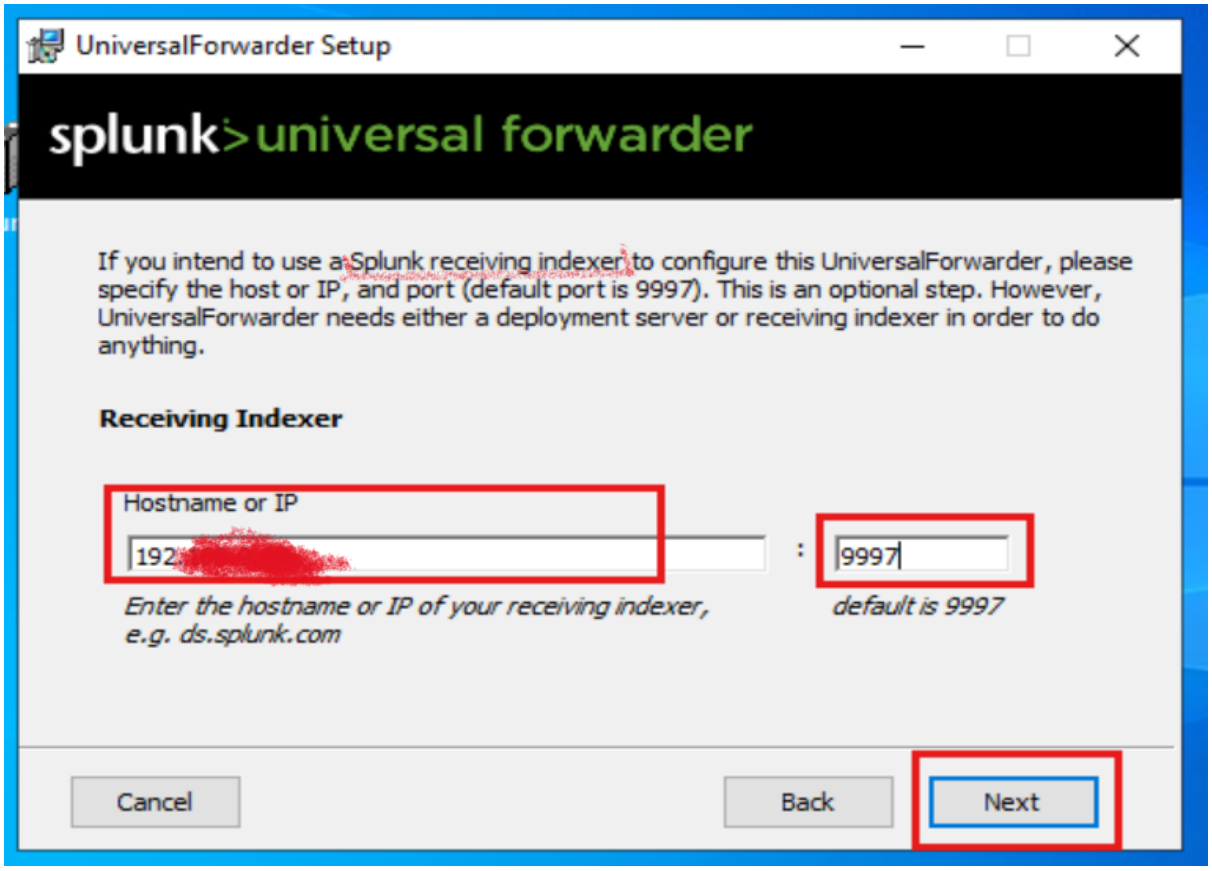

UniversalForwarder Setup
splunk>universal forwarder
If the following information is not provided, forwarded Splunk data will still be encrypted with the default Splunk certificate
SSL certificate (file containing public and private key parts)
Browse...
Certificate Password
Password:
Confirm password:
SSL root CA (the file containing the Root CA certificate to validate the server certificate)
Browse...
Cancel
Back
Next

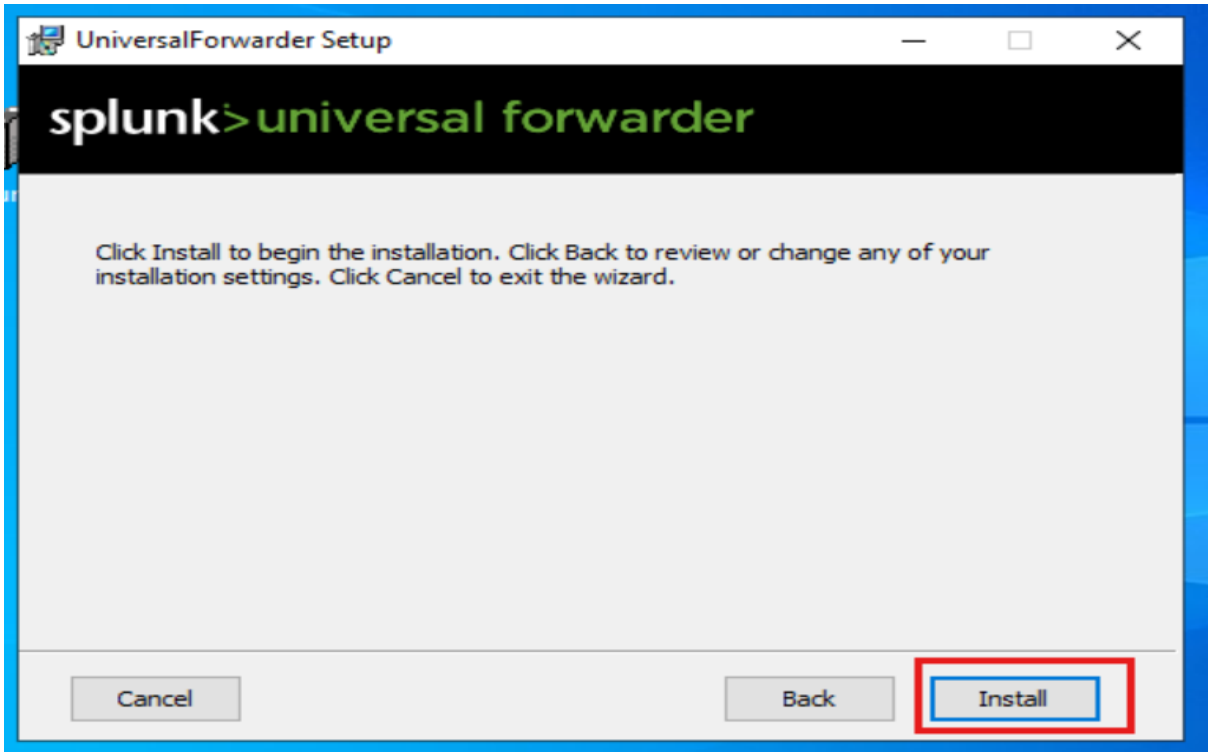

UniversalForwarder Setup
splunk>universal forwarder
The user you install UniversalForwarder as determines what data it has access to. The Managed Service Account and Group-Managed Service Account are supported by CLI only.
Install UniversalForwarder as:
Local System
Installs UniversalForwarder using local system account. UniversalForwarder can access all data on or forwarded to this machine.
Domain Account
Installs UniversalForwarder with domain account you provide. This lets you collect logs and metrics from remote machines as well as local and forwarded data. You can set the account in the next dialog, as a local administrator or a reduced privilege user.
Virtual Account
Installs UniversalForwarder using a virtual account. UniversalForwarder can access all data on or forwarded to this machine.
Cancel
Back
Next

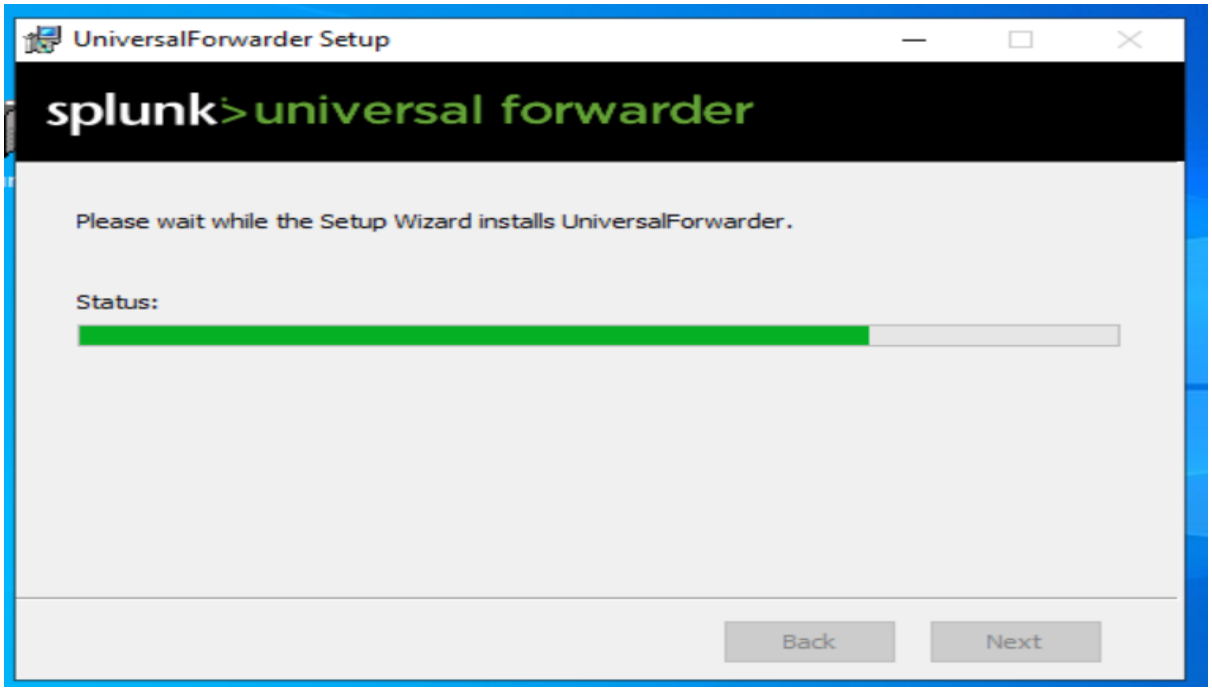

UniversalForwarder Setup
splunk>universal forwarder
Windows Event Logs
Application Logs
Security Log
System Log
Forwarded Events Log
Setup Log
Performance Monitor
CPU Load
Memory
Disk Space
Network Stats
Active Directory Monitoring
Enable AD monitoring
Path to monitor
File...
Directory...
Cancel
Back
Next

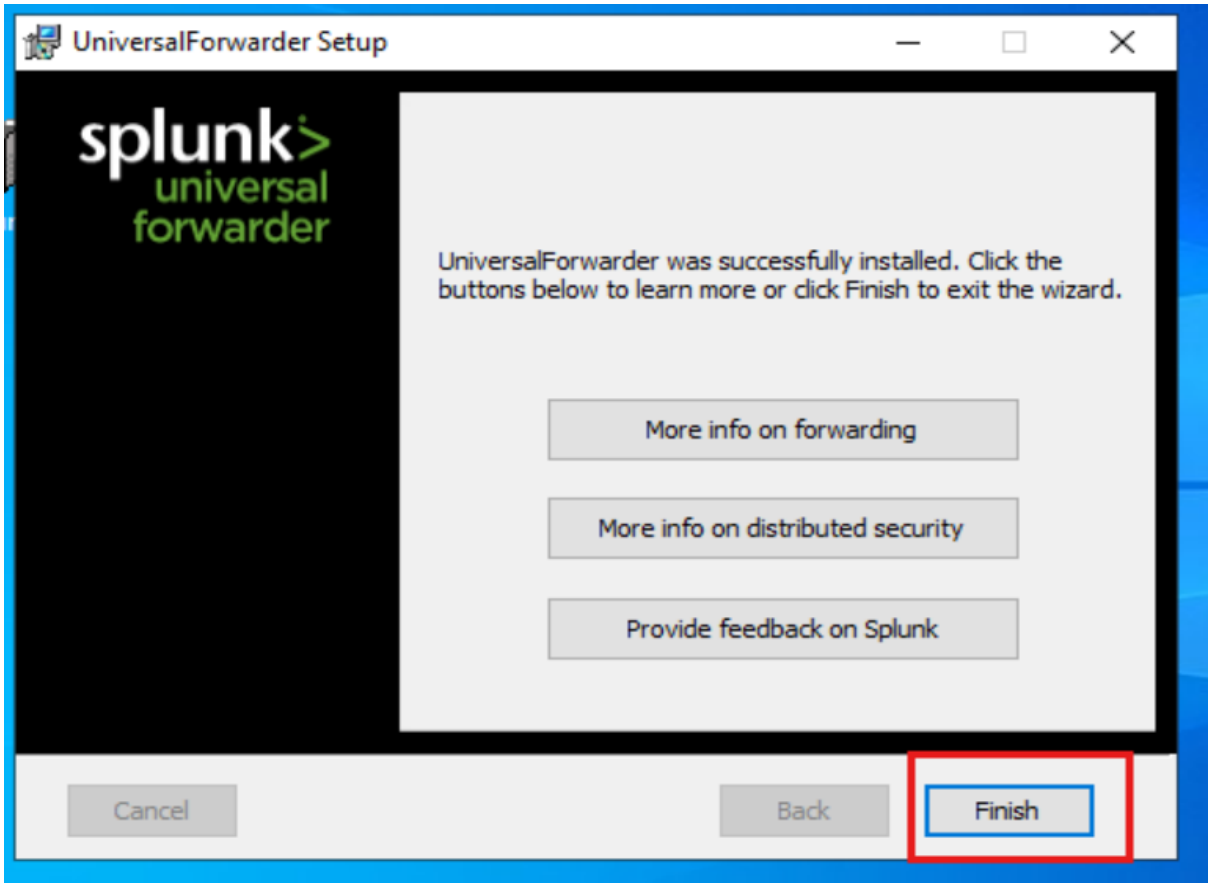

UniversalForwarder Setup
splunk>universal forwarder
Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.
Username:
Kiffy
Generate random password
Password:
Confirm password:
Cancel
Back
Next


UniversalForwarder Setup
splunk>universal forwarder
If you intend to use a Splunk deployment server to configure this UniversalForwarder, please specify the host or IP, and port (default port is 8089). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.
Deployment Server
Hostname or IP
:
Enter the hostname or IP of your deployment server, e.g. ds.splunk.com
default is 8089
Cancel
Back
Next


UniversalForwarder Setup
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
192
9997
Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com
default is 9997
Cancel
Back
Next


UniversalForwarder Setup
splunk>universal forwarder
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Cancel
Back
Install


UniversalForwarder Setup
splunk>universal forwarder
Please wait while the Setup Wizard installs UniversalForwarder.
Status:
Back
Next


UniversalForwarder Setup
splunk>
universal
forwarder
UniversalForwarder was successfully installed. Click the buttons below to learn more or click Finish to exit the wizard.
More info on forwarding
More info on distributed security
Provide feedback on Splunk
Cancel
Back
Finish