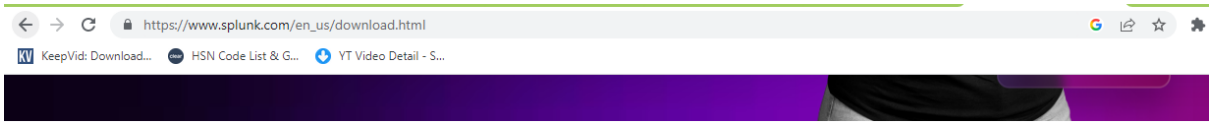
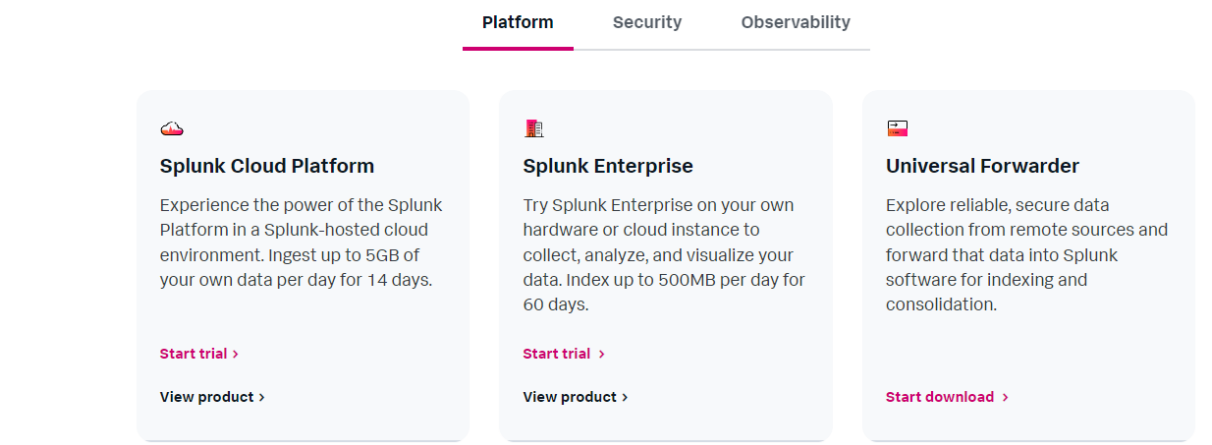
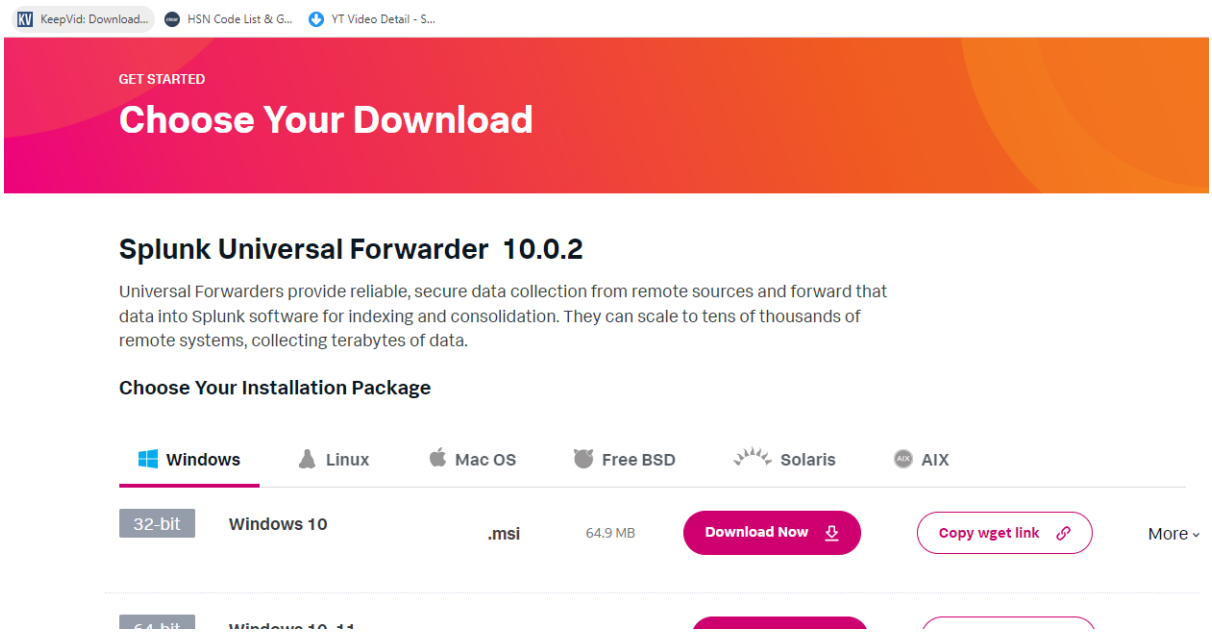
Adding Windows Server to Splunk Enterprise through Universal_Forwarder

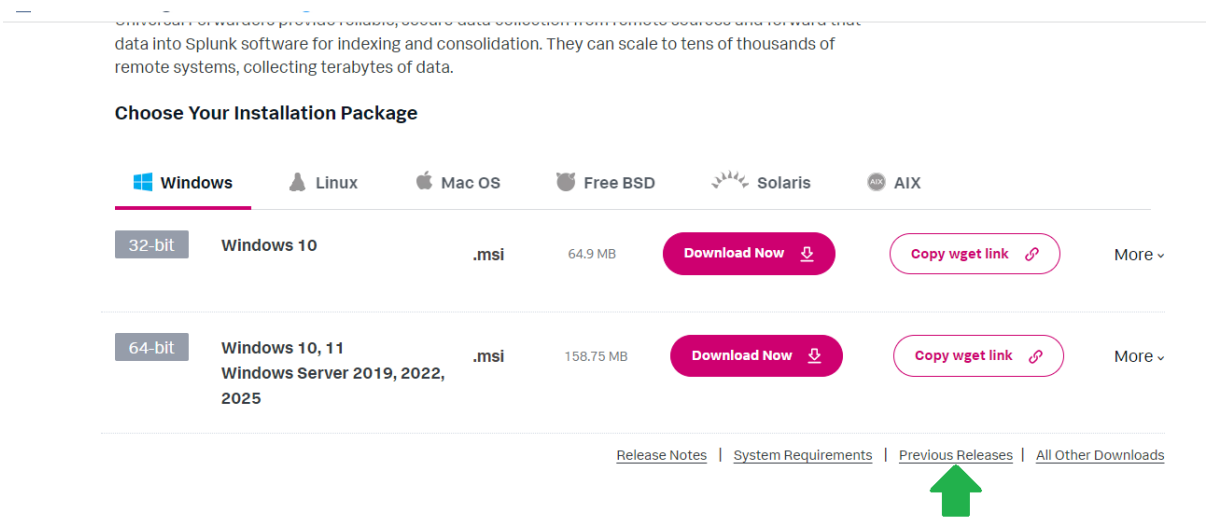
Download Splunk Universal Forwarder (Windows)

1. Go to **splunk.com → Downloads → Universal Forwarder**

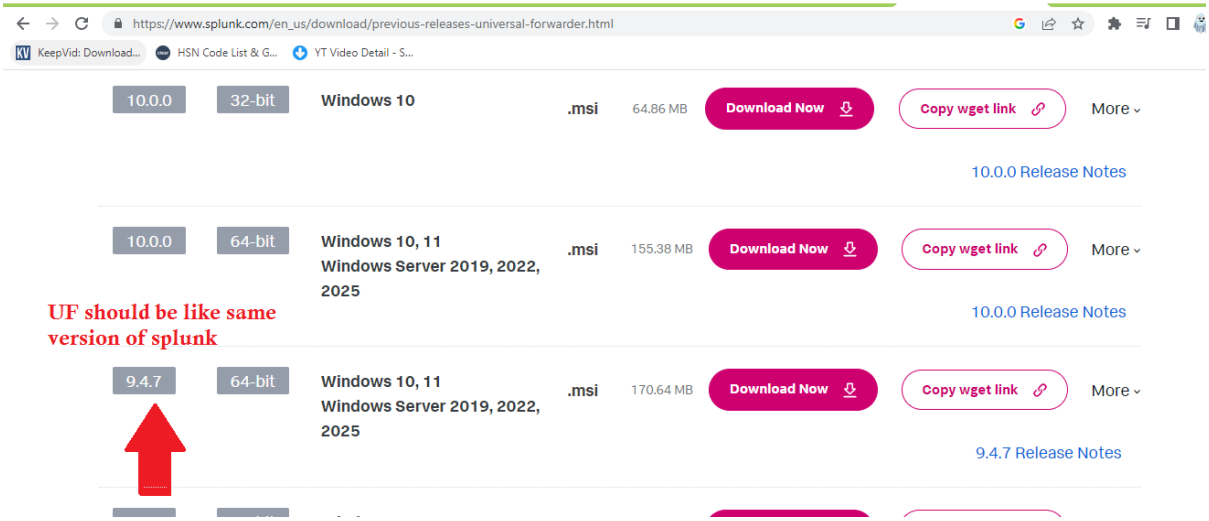




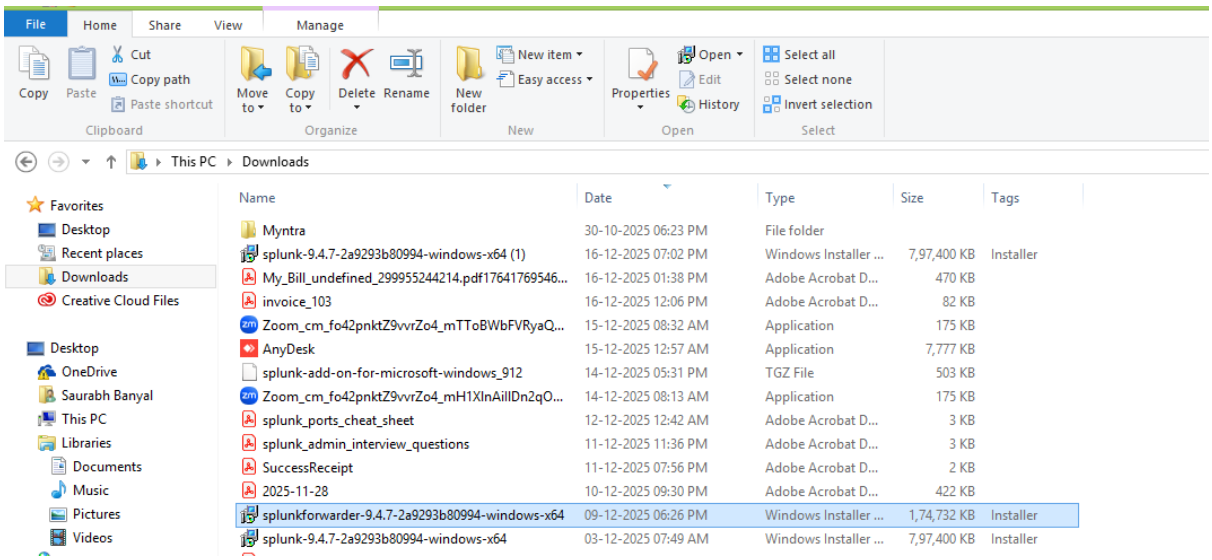




2. Download **Windows (64-bit)** version matching your Splunk Enterprise version



3. Copy installer to the Windows server

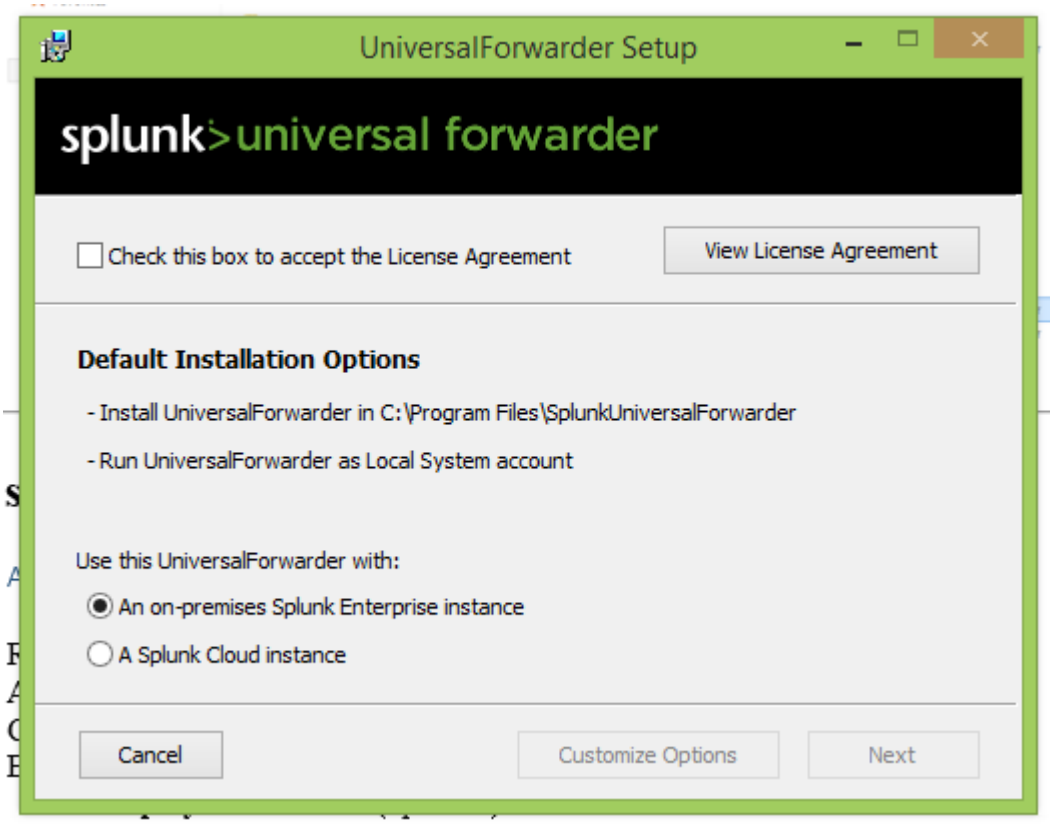
4. 

---

3. Install Universal Forwarder on Windows

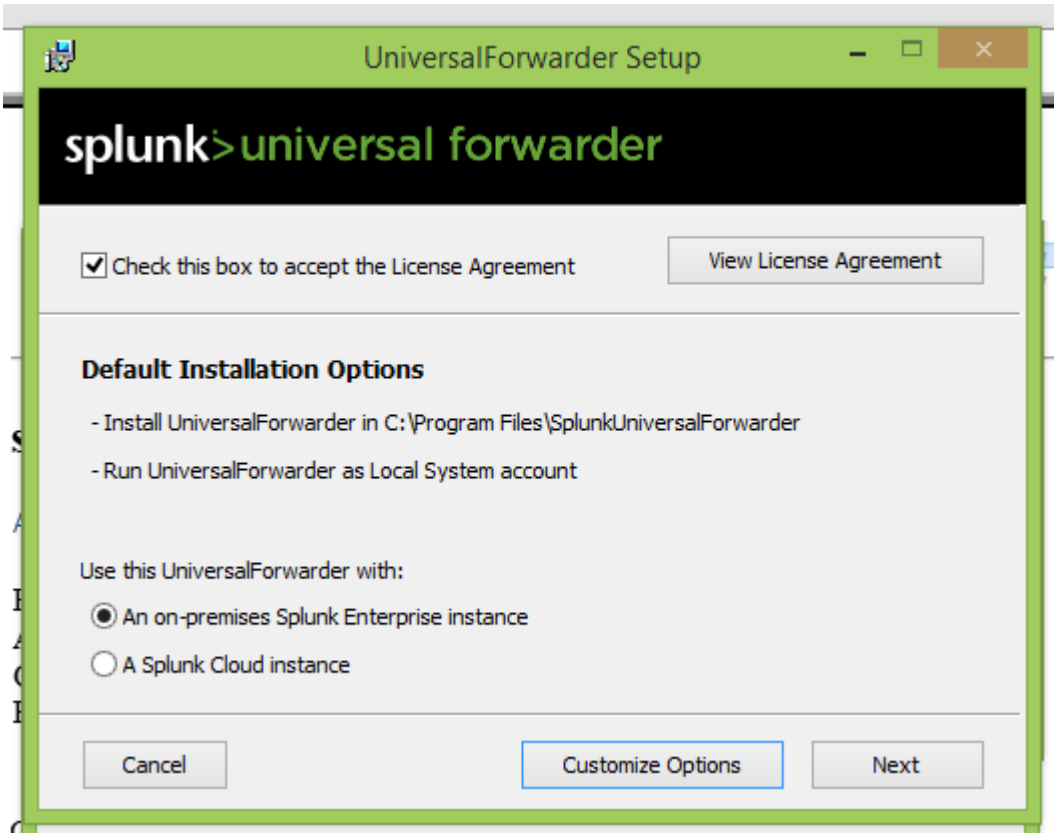
Option A: GUI Installation (Recommended)

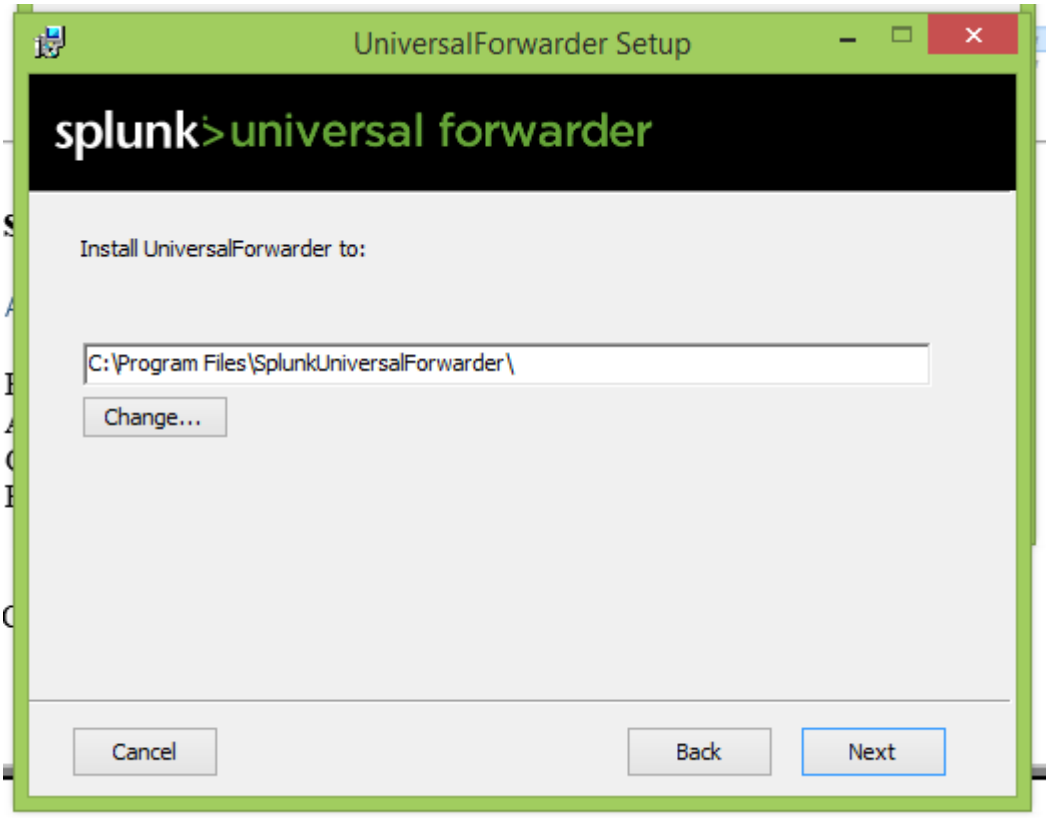
1. Run `splunkforwarder-<version>-x64-release.msi`
2. Accept license

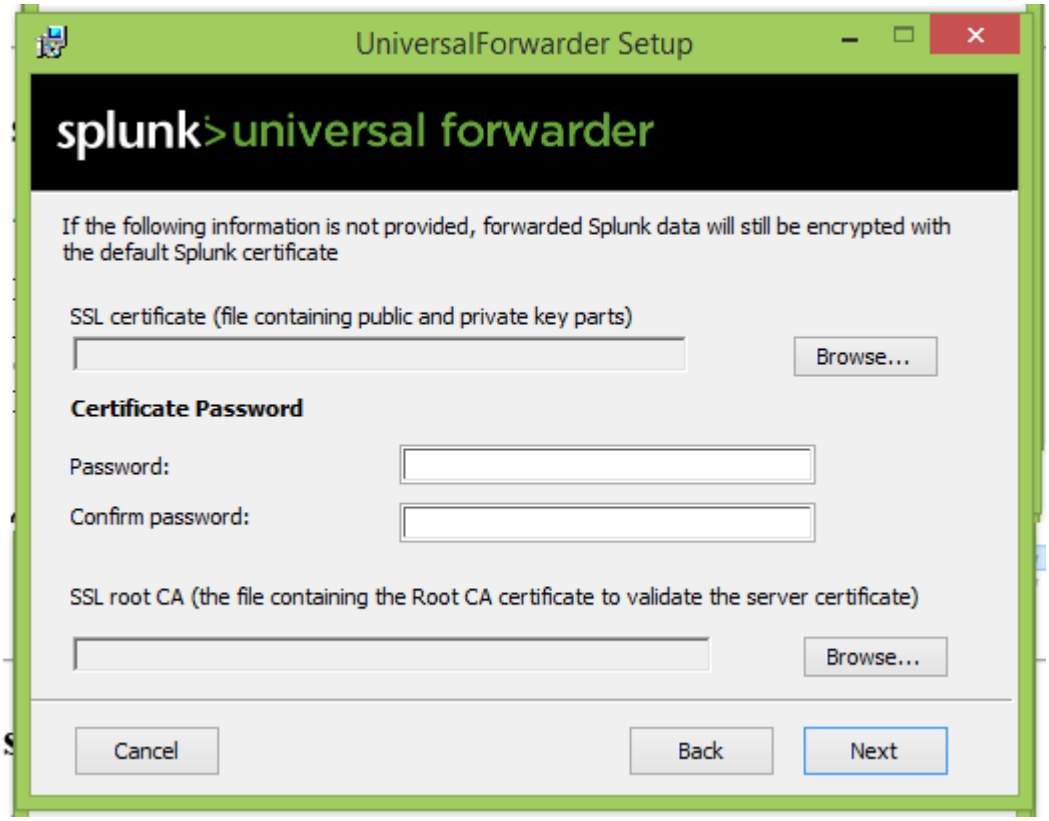


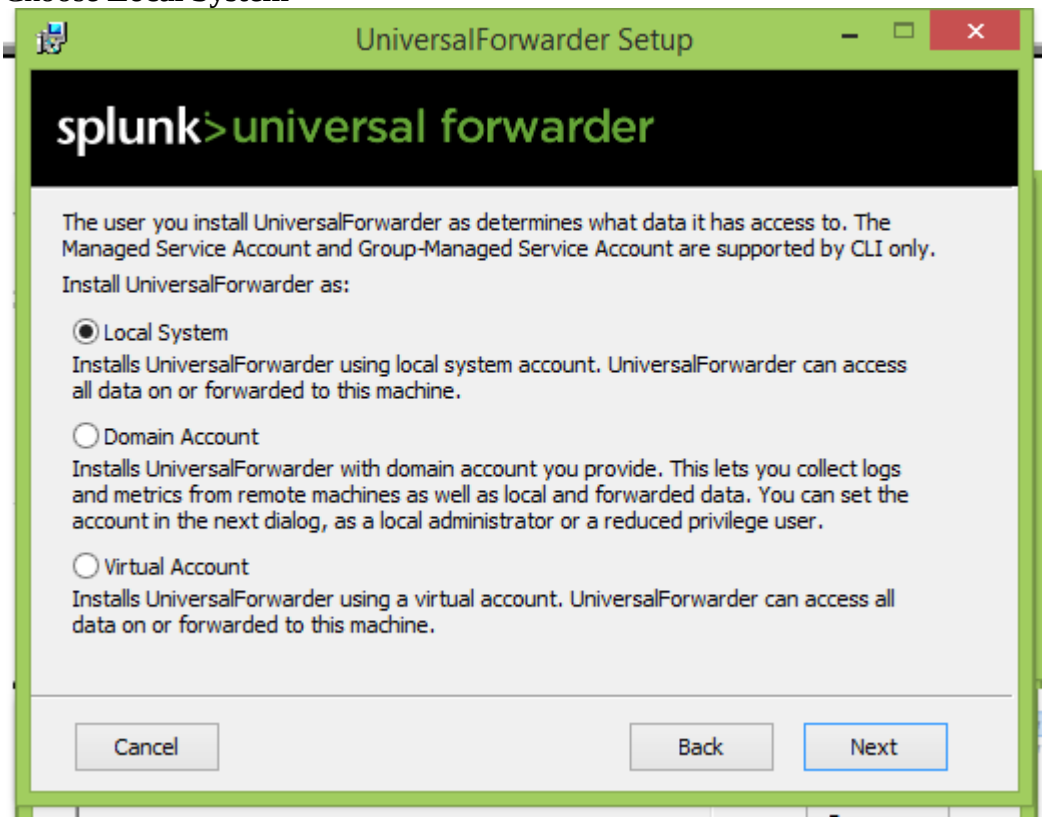
3. Click on Customize Options

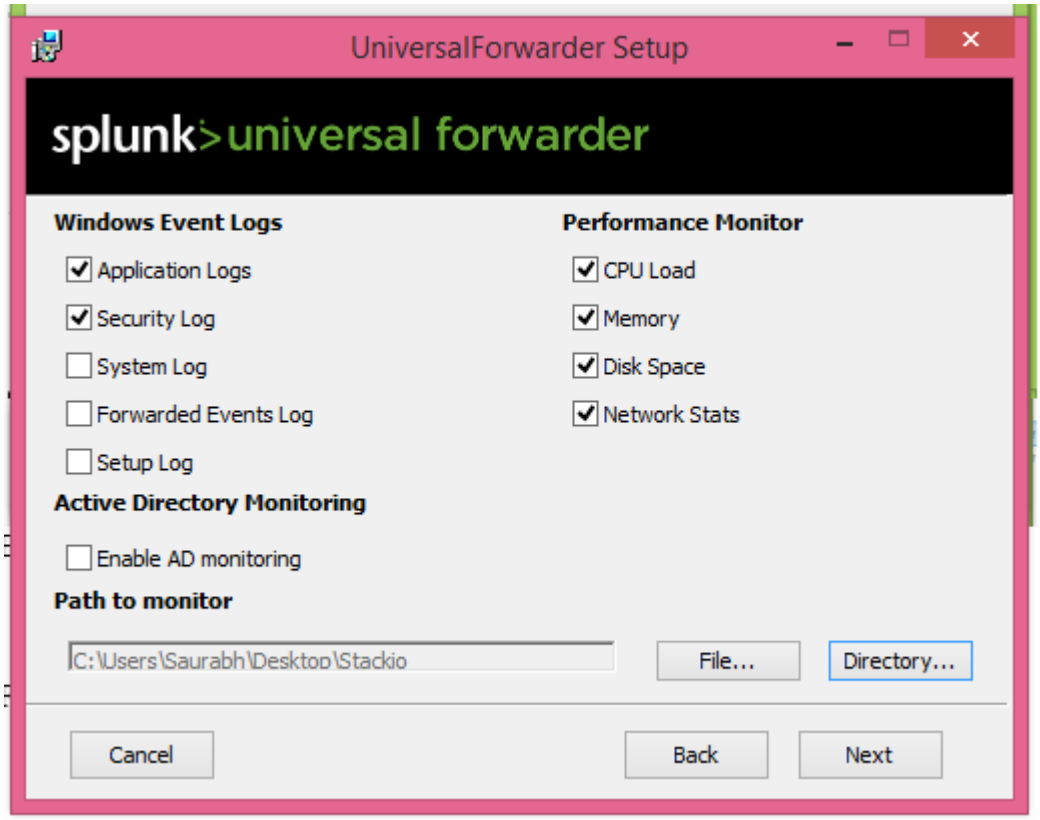
4.

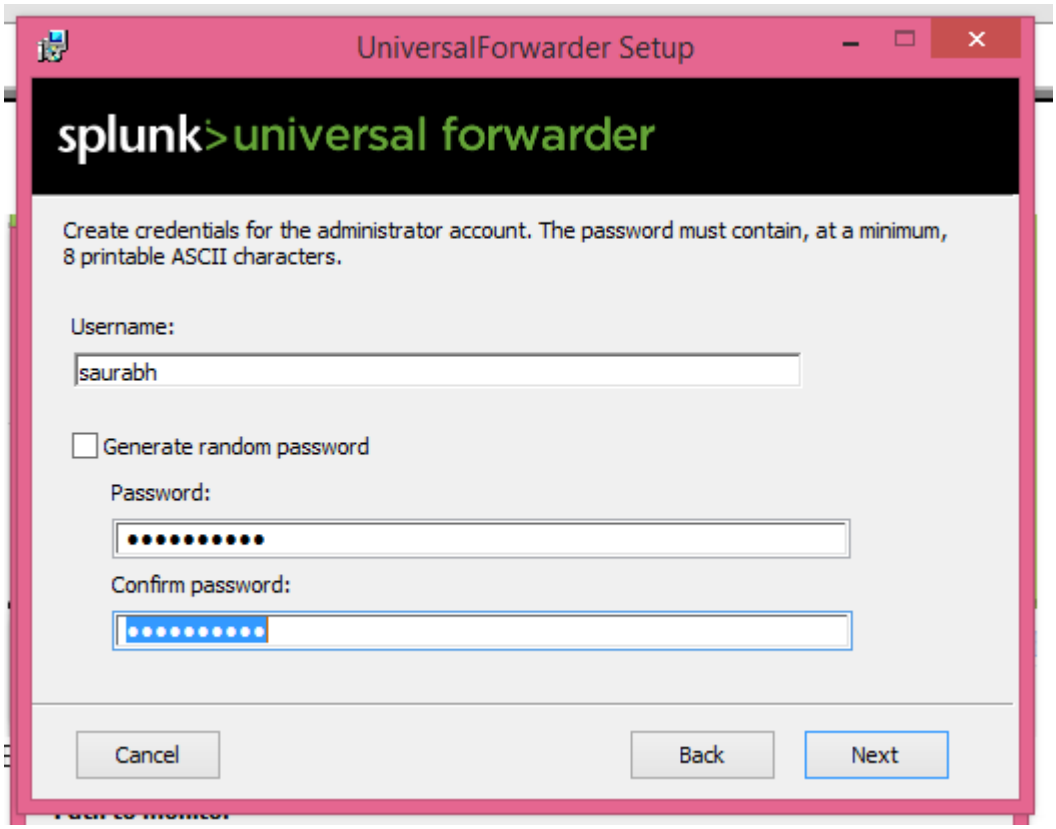

UniversalForwarder Setup
splunk>universal forwarder
Check this box to accept the License Agreement
View License Agreement
Default Installation Options
- Install UniversalForwarder in C:\Program Files\SplunkUniversalForwarder
- Run UniversalForwarder as Local System account
Use this UniversalForwarder with:
An on-premises Splunk Enterprise instance
A Splunk Cloud instance
Cancel
Customize Options
Next


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

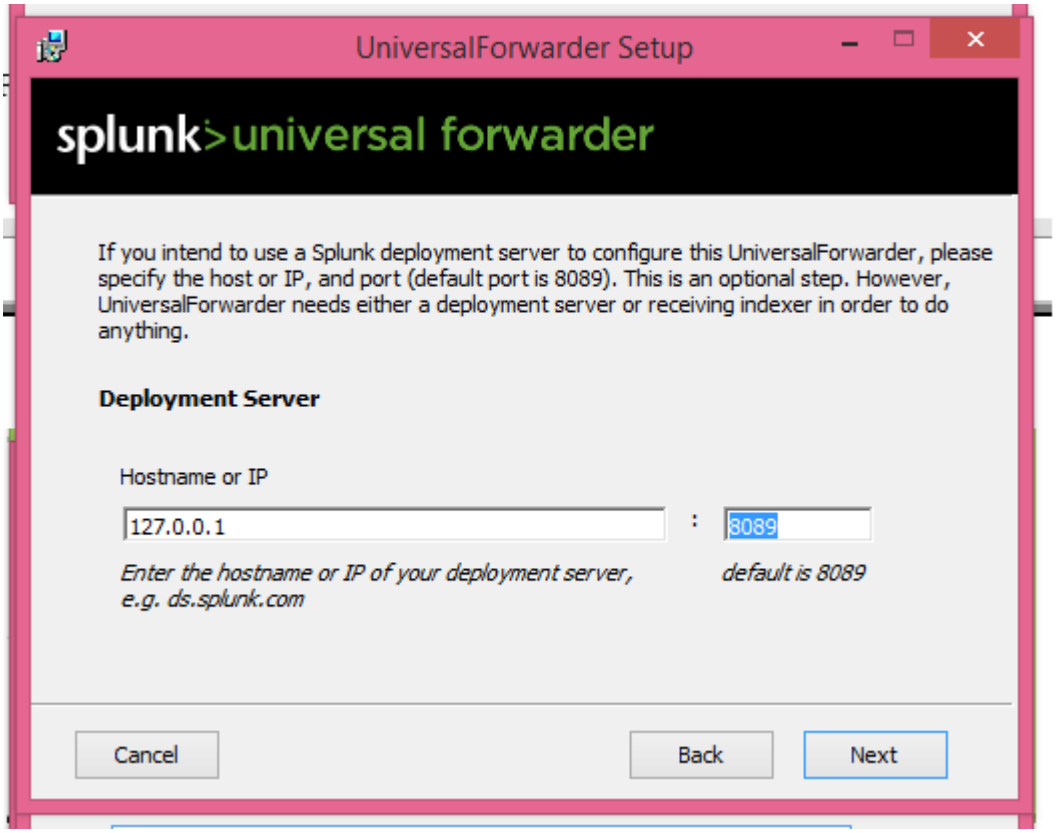
5. 

6. Choose **Local System**
7. 

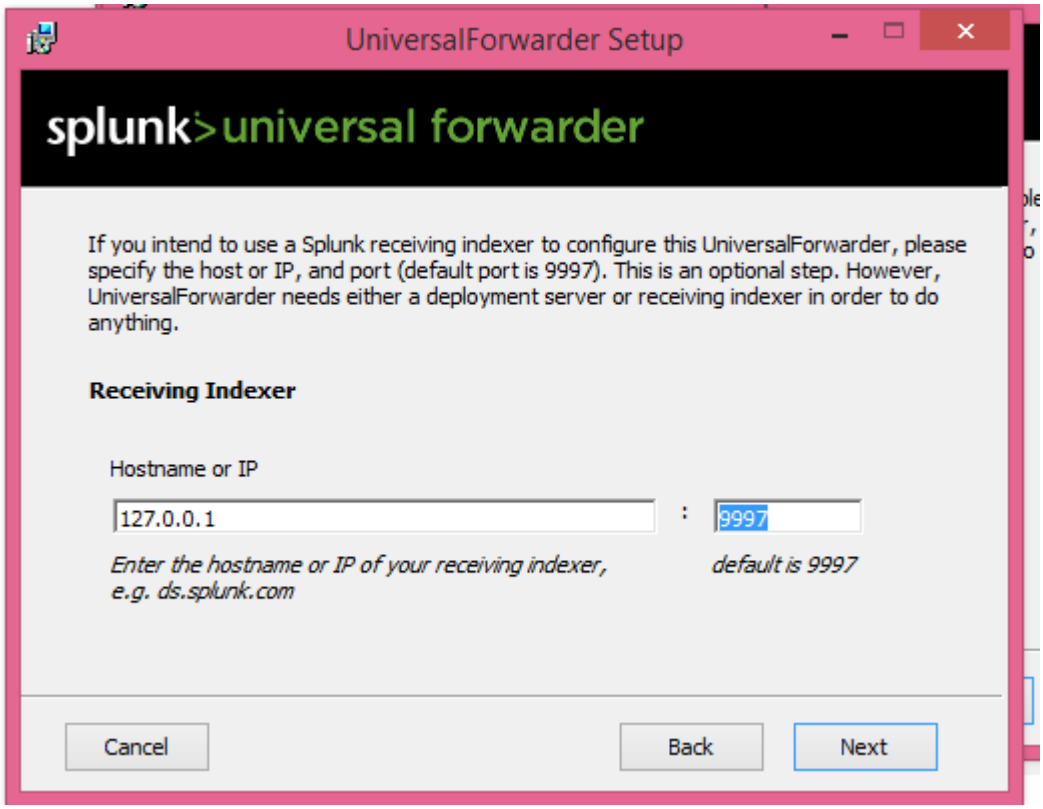
8. 

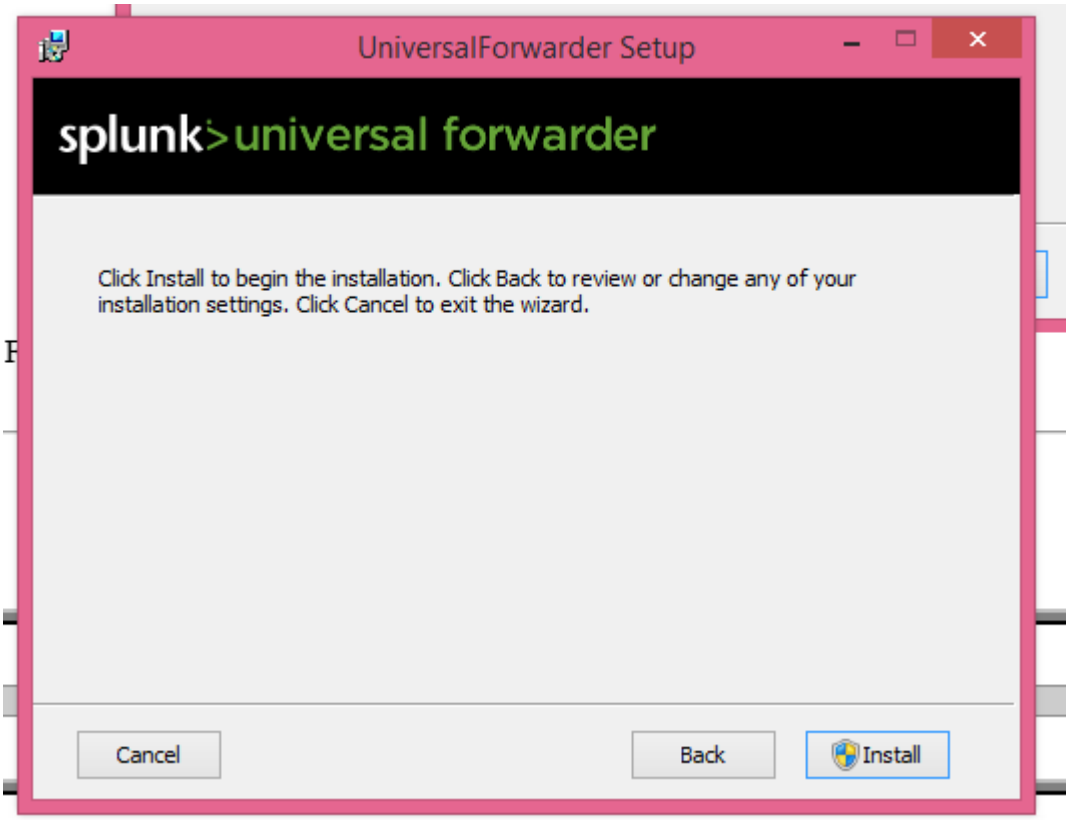
9. 

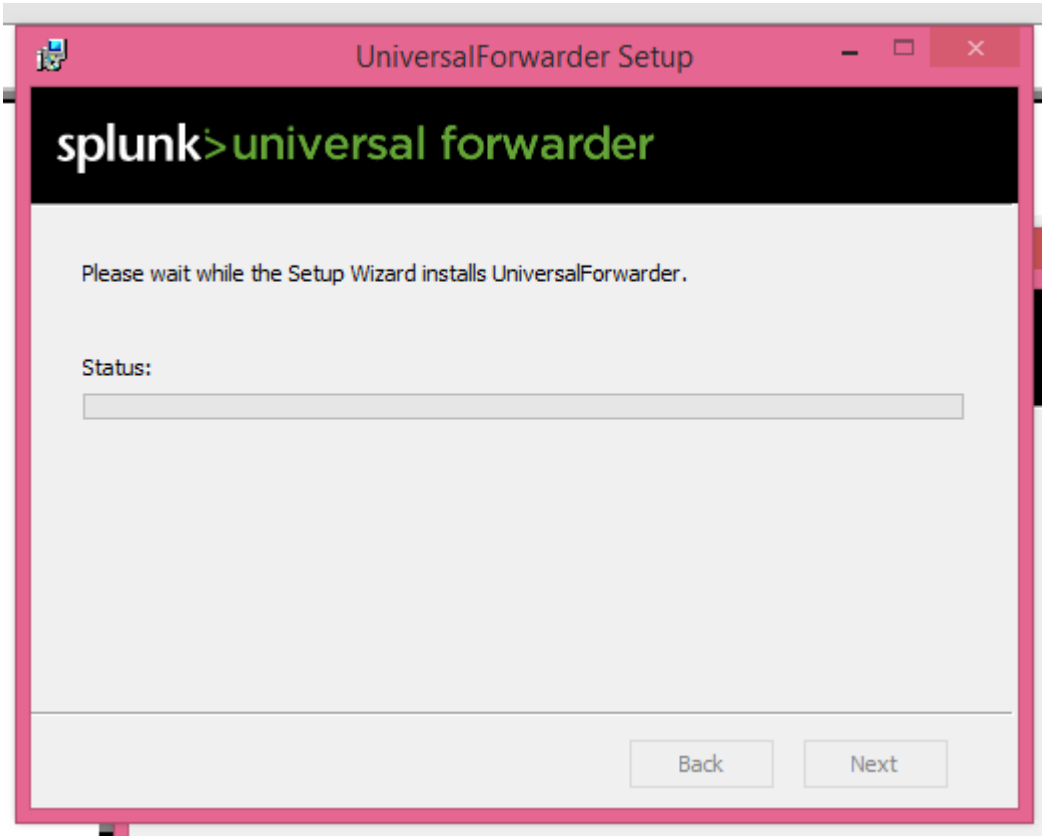
10. Enter:
    - **Deployment Server** (optional)

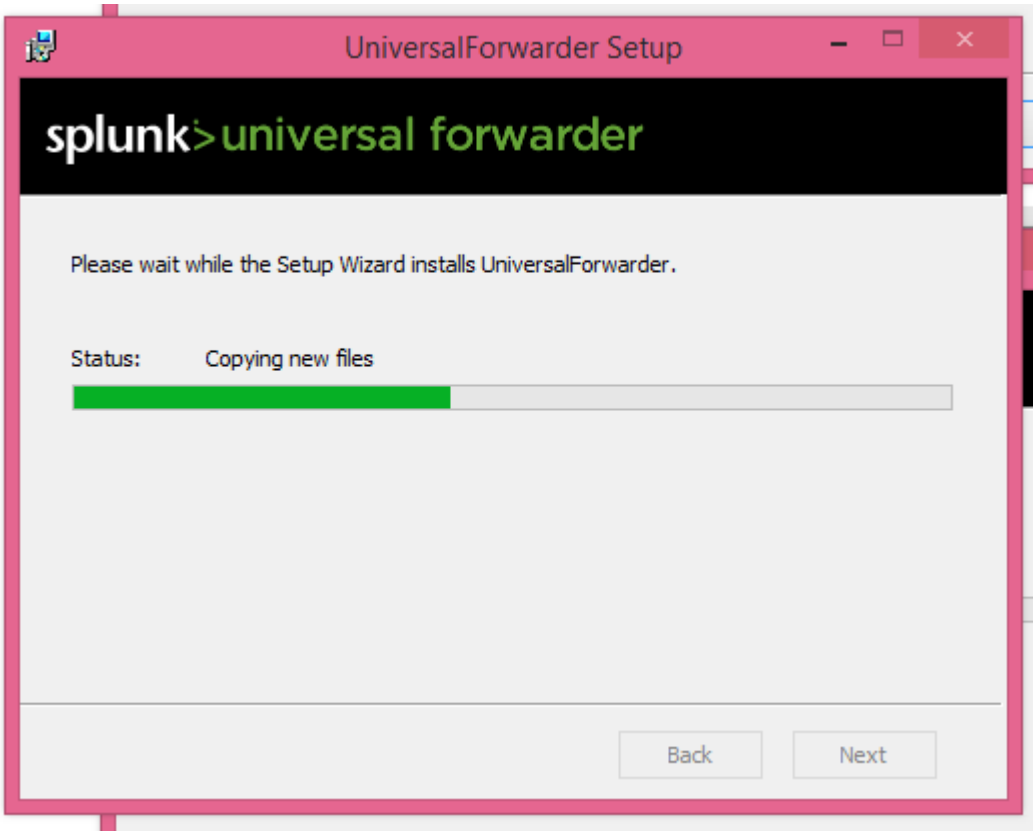


- **Receiving Indexer Hostname/IP or Port Number**
- **Port:** `9997`

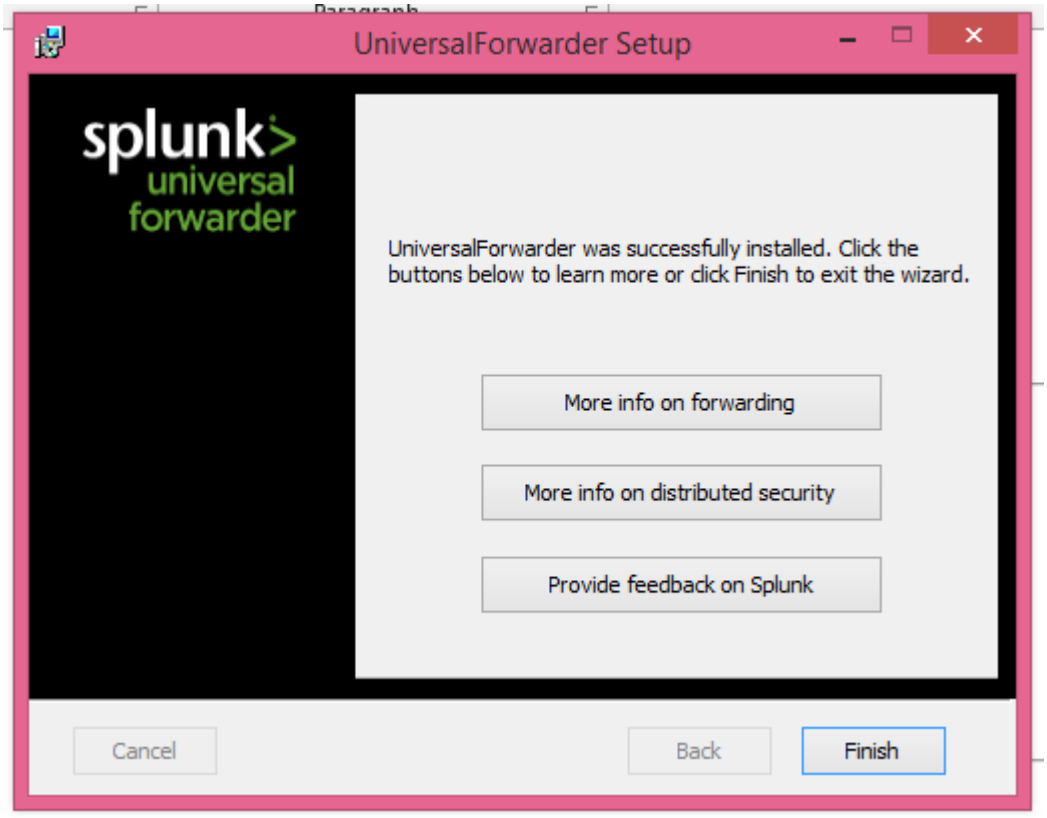



UniversalForwarder Setup
splunk>universal forwarder
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Cancel
Back
Install


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

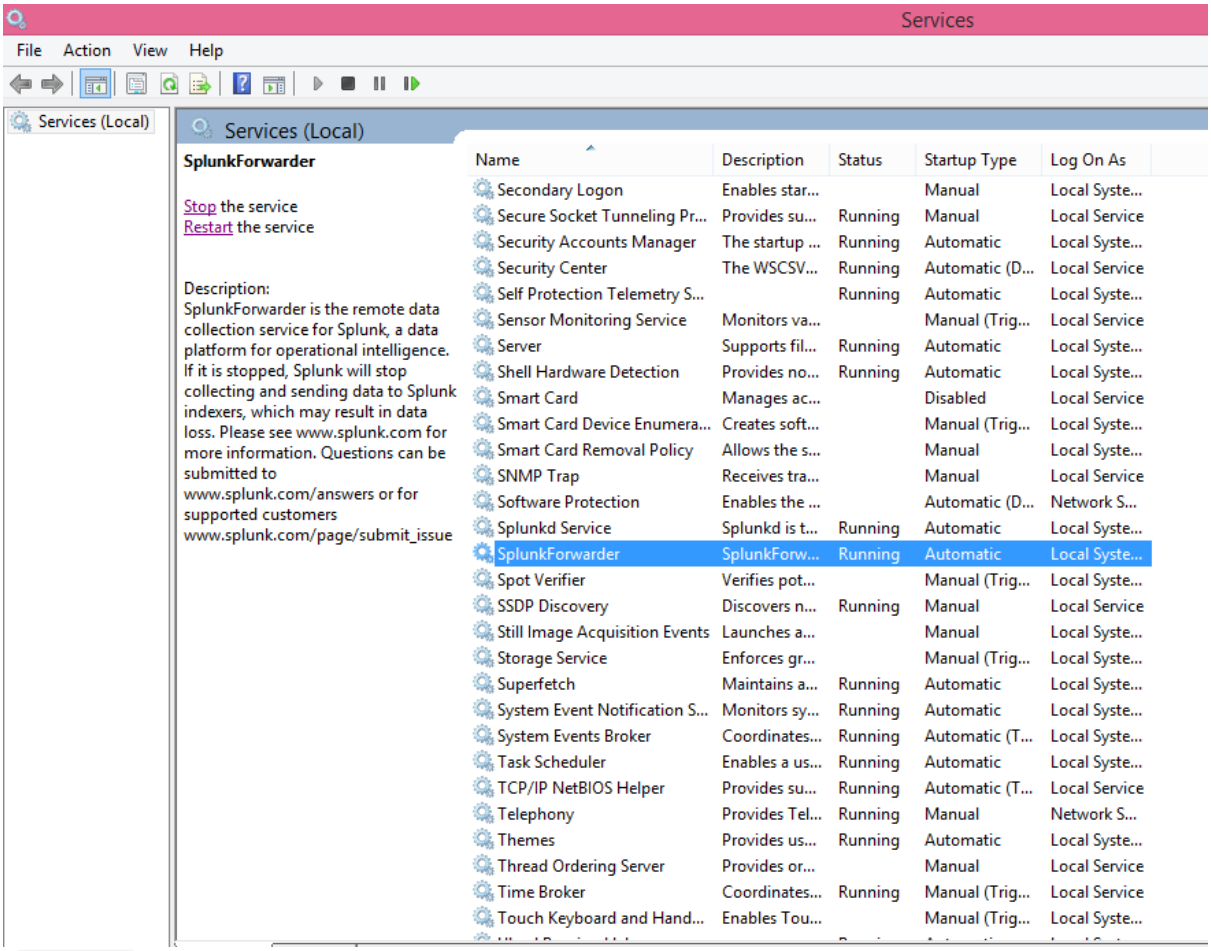


11. Finish installation

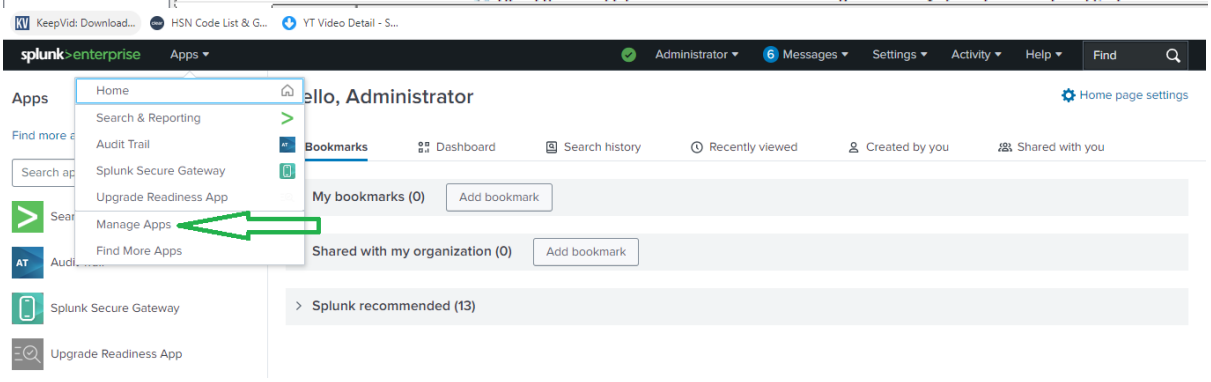


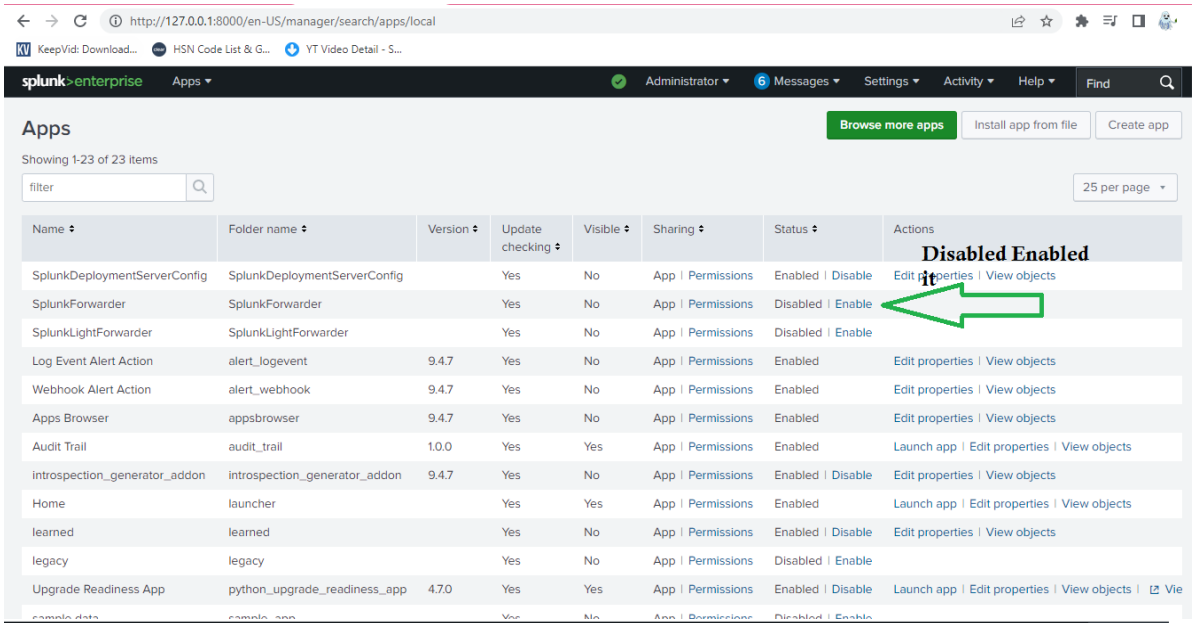
12.

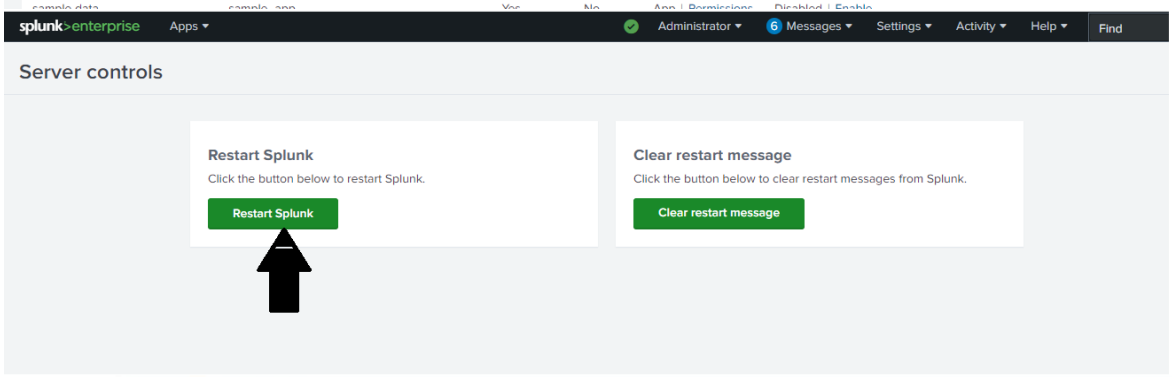
13.

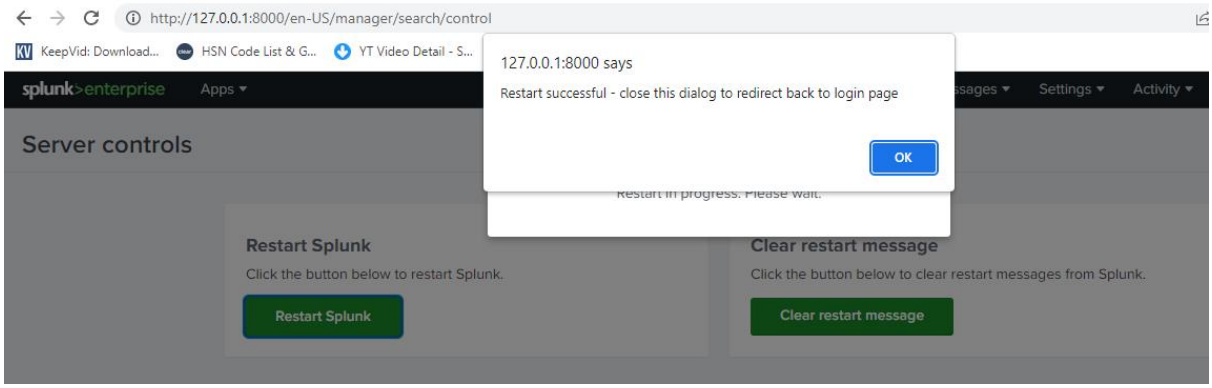

Services
File Action View Help
Services (Local)
Services (Local)
SplunkForwarder
Stop the service
Restart the service
Description:
SplunkForwarder is the remote data collection service for Splunk, a data platform for operational intelligence. If it is stopped, Splunk will stop collecting and sending data to Splunk indexers, which may result in data loss. Please see www.splunk.com for more information. Questions can be submitted to www.splunk.com/answers or for supported customers www.splunk.com/page/submit_issue
Name | Description | Status | Startup Type | Log On As
Secondary Logon | Enables star... | | Manual | Local Syste...
Secure Socket Tunneling Pr... | Provides su... | Running | Manual | Local Service
Security Accounts Manager | The startup ... | Running | Automatic | Local Syste...
Security Center | The WSCSV... | Running | Automatic (D... | Local Service
Self Protection Telemetry S... | | Running | Automatic | Local Syste...
Sensor Monitoring Service | Monitors va... | | Manual (Trig... | Local Service
Server | Supports fil... | Running | Automatic | Local Syste...
Shell Hardware Detection | Provides no... | Running | Automatic | Local Syste...
Smart Card | Manages ac... | | Disabled | Local Service
Smart Card Device Enumera... | Creates soft... | | Manual (Trig... | Local Syste...
Smart Card Removal Policy | Allows the s... | | Manual | Local Syste...
SNMP Trap | Receives tra... | | Manual | Local Service
Software Protection | Enables the ... | | Automatic (D... | Network S...
Splunkd Service | Splunkd is t... | Running | Automatic | Local Syste...
SplunkForwarder | SplunkForw... | Running | Automatic | Local Syste...
Spot Verifier | Verifies pot... | | Manual (Trig... | Local Syste...
SSDP Discovery | Discovers n... | Running | Manual | Local Service
Still Image Acquisition Events | Launches a... | | Manual | Local Syste...
Storage Service | Enforces gr... | | Manual (Trig... | Local Syste...
Superfetch | Maintains a... | Running | Automatic | Local Syste...
System Event Notification S... | Monitors sy... | Running | Automatic | Local Syste...
System Events Broker | Coordinates... | Running | Automatic (T... | Local Syste...
Task Scheduler | Enables a us... | Running | Automatic | Local Syste...
TCP/IP NetBIOS Helper | Provides su... | Running | Automatic (T... | Local Service
Telephony | Provides Tel... | Running | Manual | Network S...
Themes | Provides us... | Running | Automatic | Local Syste...
Thread Ordering Server | Provides or... | | Manual | Local Service
Time Broker | Coordinates... | Running | Manual (Trig... | Local Service
Touch Keyboard and Hand... | Enables Tou... | | Manual (Trig... | Local Syste...

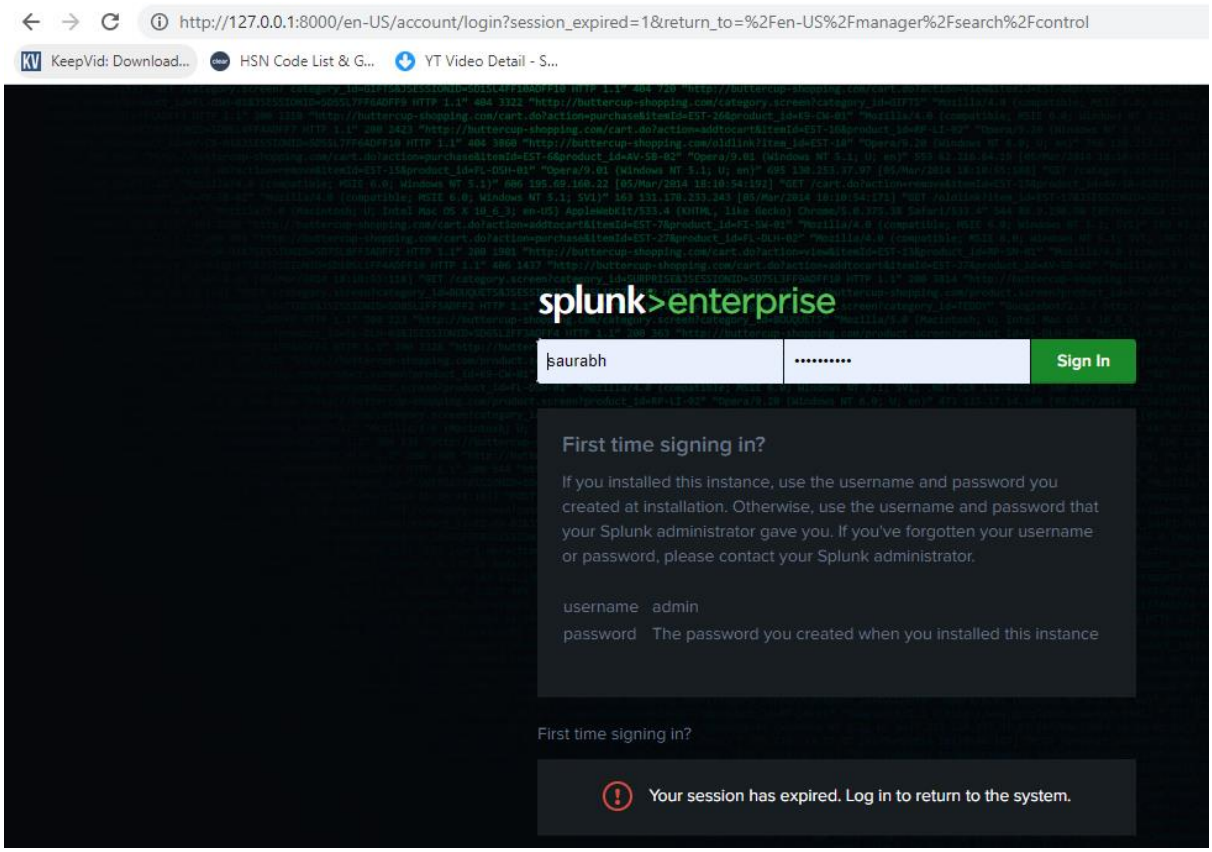
14.

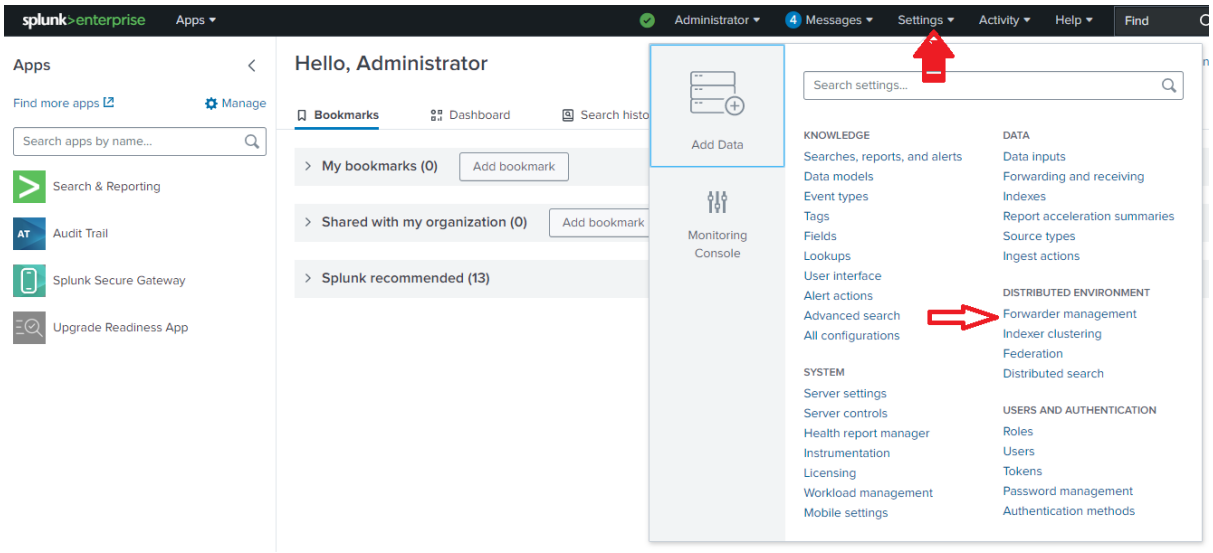

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Apps
Home
Search & Reporting
Audit Trail
Splunk Secure Gateway
Upgrade Readiness App
Manage Apps
Find More Apps
Hello, Administrator
Home page settings
Bookmarks
Dashboard
Search history
Recently viewed
Created by you
Shared with you
My bookmarks (0)
Add bookmark
Shared with my organization (0)
Add bookmark
Splunk recommended (13)
Splunk Secure Gateway
Upgrade Readiness App

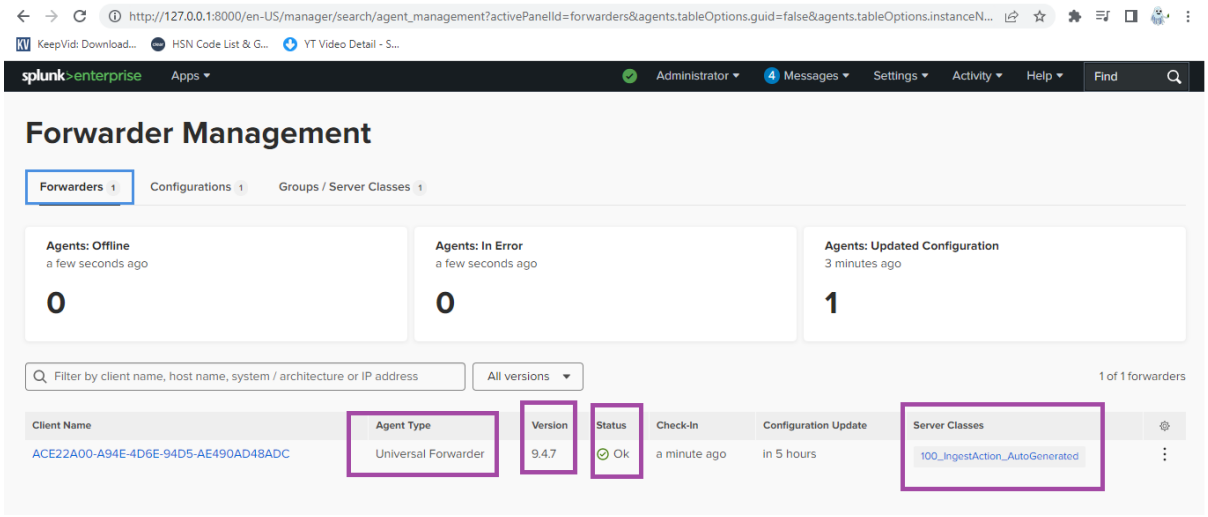
15. 
http://127.0.0.1:8000/en-US/manager/search/apps/local
splunk>enterprise
Apps
Administrator
6 Messages
Settings
Activity
Help
Find
Apps
Browse more apps
Install app from file
Create app
Showing 1-23 of 23 items
filter
25 per page
Name
Folder name
Version
Update checking
Visible
Sharing
Status
Actions
Disabled Enabled it
SplunkDeploymentServerConfig | SplunkDeploymentServerConfig | Yes | No | App | Permissions | Enabled | Disable | Edit properties | View objects
SplunkForwarder | SplunkForwarder | Yes | No | App | Permissions | Disabled | Enable
SplunkLightForwarder | SplunkLightForwarder | Yes | No | App | Permissions | Disabled | Enable
Log Event Alert Action | alert_logevent | 9.4.7 | Yes | No | App | Permissions | Enabled | Edit properties | View objects
Webhook Alert Action | alert_webhook | 9.4.7 | Yes | No | App | Permissions | Enabled | Edit properties | View objects
Apps Browser | appsbrowser | 9.4.7 | Yes | No | App | Permissions | Enabled | Edit properties | View objects
Audit Trail | audit_trail | 1.0.0 | Yes | Yes | App | Permissions | Enabled | Launch app | Edit properties | View objects
introspection_generator_addon | introspection_generator_addon | 9.4.7 | Yes | No | App | Permissions | Enabled | Disable | Edit properties | View objects
Home | launcher | Yes | Yes | App | Permissions | Enabled | Launch app | Edit properties | View objects
learned | learned | Yes | No | App | Permissions | Enabled | Disable | Edit properties | View objects
legacy | legacy | Yes | No | App | Permissions | Disabled | Enable
Upgrade Readiness App | python_upgrade_readiness_app | 4.7.0 | Yes | Yes | App | Permissions | Enabled | Disable | Launch app | Edit properties | View objects

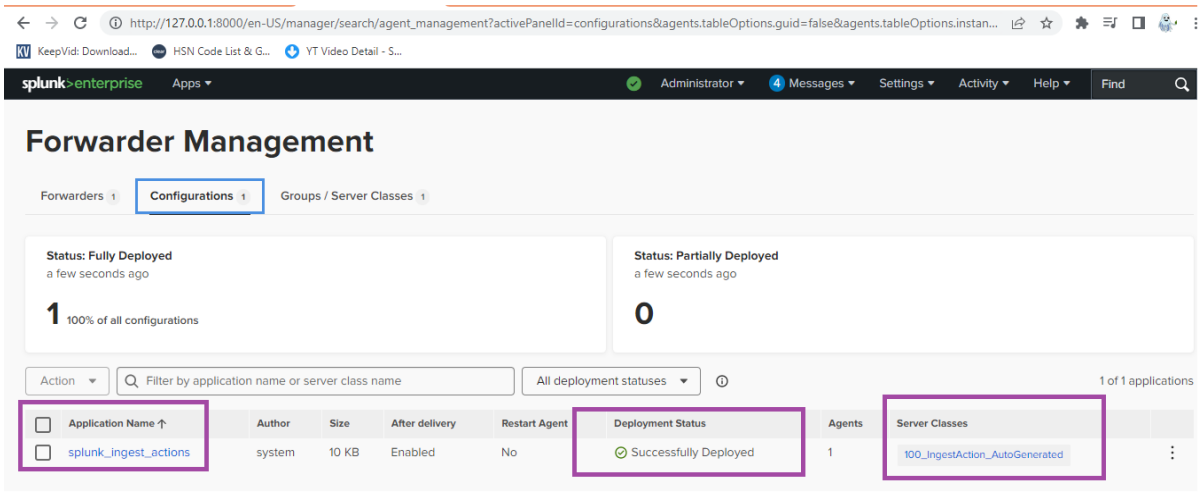
16. 
splunk>enterprise
Apps
Administrator
6 Messages
Settings
Activity
Help
Find
Server controls
Restart Splunk
Click the button below to restart Splunk.
Restart Splunk
Clear restart message
Click the button below to clear restart messages from Splunk.
Clear restart message

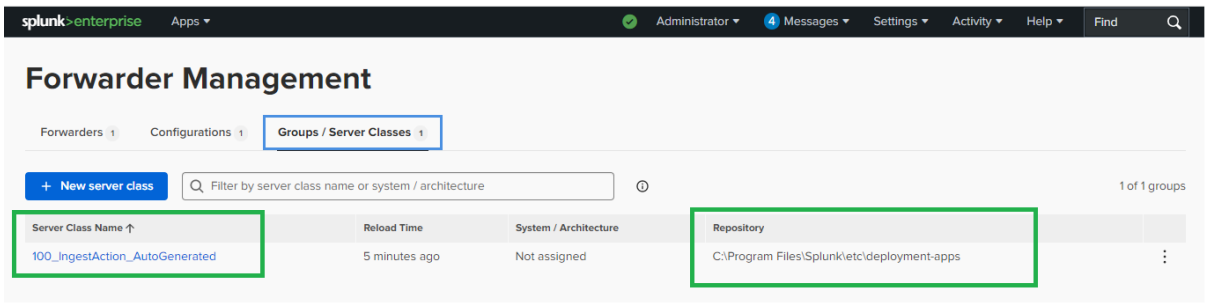
17. 
http://127.0.0.1:8000/en-US/manager/search/control
127.0.0.1:8000 says
Restart successful - close this dialog to redirect back to login page
OK
splunk>enterprise
Apps
Settings
Activity
Server controls
Restart Splunk
Click the button below to restart Splunk.
Restart Splunk
Clear restart message
Click the button below to clear restart messages from Splunk.
Clear restart message

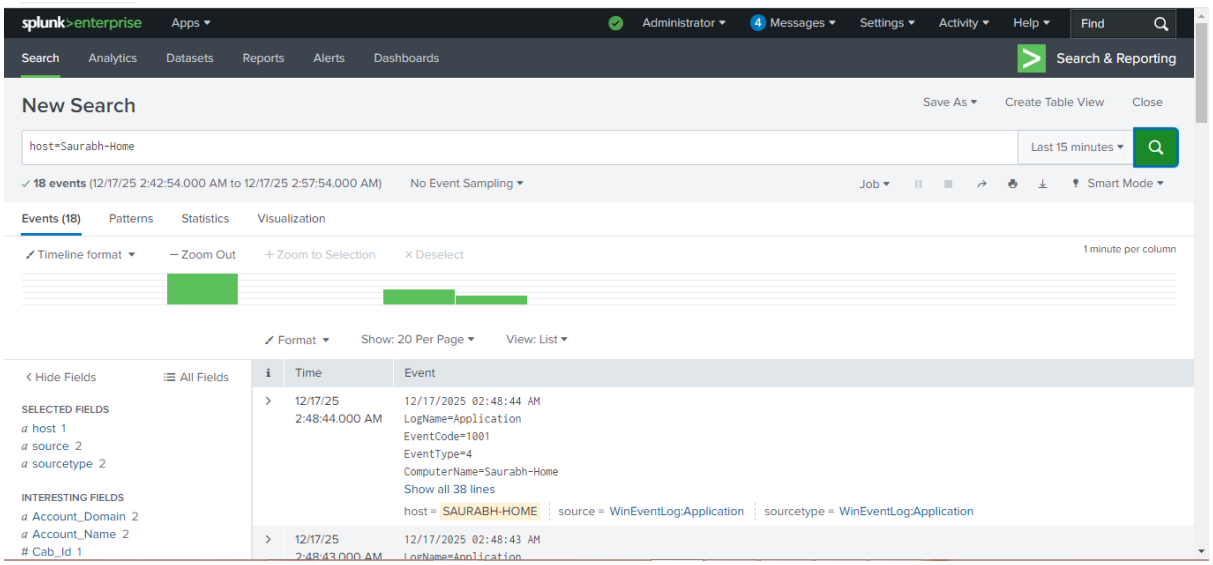
18. 
http://127.0.0.1:8000/en-US/account/login?session_expired=1&return_to=%2Fen-US%2Fmanager%2Fsearch%2Fcontrol
KeepVid: Download...
HSN Code List & G...
YT Video Detail - S...
splunk>enterprise
saurabh
Sign In
First time signing in?
If you installed this instance, use the username and password you created at installation. Otherwise, use the username and password that your Splunk administrator gave you. If you've forgotten your username or password, please contact your Splunk administrator.
username admin
password The password you created when you installed this instance
First time signing in?
Your session has expired. Log in to return to the system.

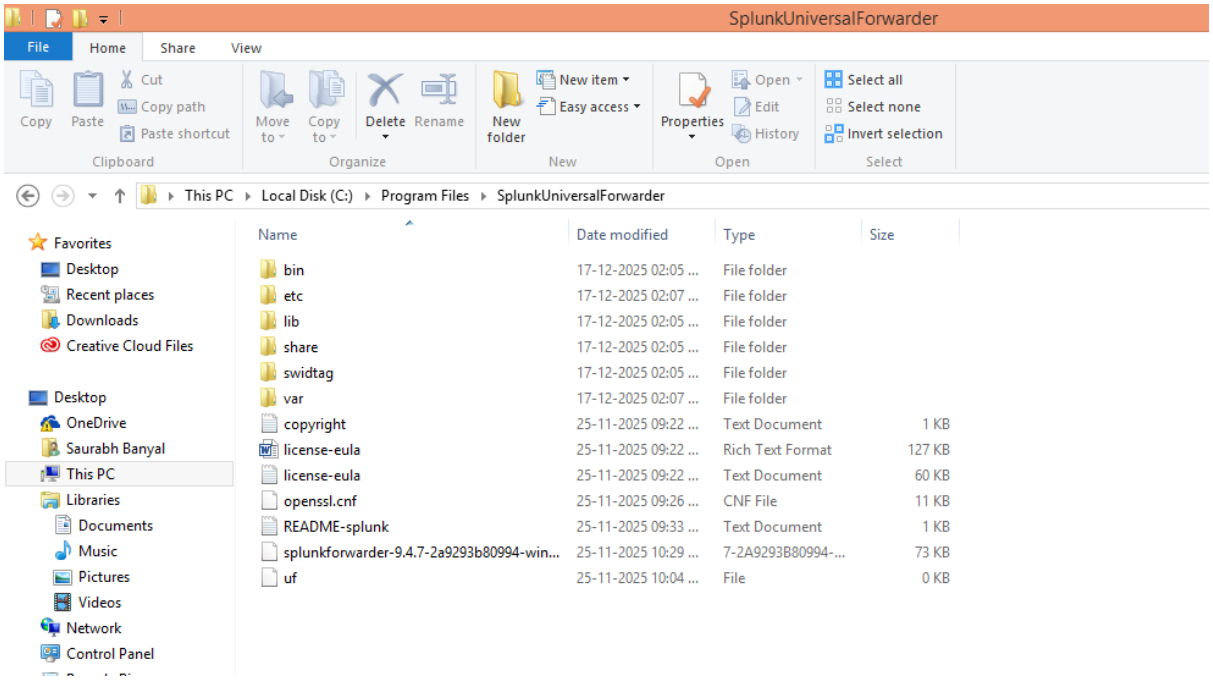

splunk>enterprise
Apps
Administrator
4 Messages
Settings
Activity
Help
Find
Apps
Find more apps
Manage
Search apps by name...
Search & Reporting
Audit Trail
Splunk Secure Gateway
Upgrade Readiness App
Hello, Administrator
Bookmarks
Dashboard
My bookmarks (0)
Add bookmark
Shared with my organization (0)
Add bookmark
Splunk recommended (13)
Add Data
Monitoring Console
Search settings...
KNOWLEDGE
Searches, reports, and alerts
Data models
Event types
Tags
Fields
Lookups
User interface
Alert actions
Advanced search
All configurations
DATA
Data inputs
Forwarding and receiving
Indexes
Report acceleration summaries
Source types
Ingest actions
DISTRIBUTED ENVIRONMENT
Forwarder management
Indexer clustering
Federation
Distributed search
SYSTEM
Server settings
Server controls
Health report manager
Instrumentation
Licensing
Workload management
Mobile settings
USERS AND AUTHENTICATION
Roles
Users
Tokens
Password management
Authentication methods


http://127.0.0.1:8000/en-US/manager/search/agent_management?activePanelId=forwarders&agents.tableOptions.guid=false&agents.tableOptions.instanceN...
splunk>enterprise
Apps
Administrator
4 Messages
Settings
Activity
Help
Find
Forwarder Management
Forwarders 1
Configurations 1
Groups / Server Classes 1
Agents: Offline
a few seconds ago
0
Agents: In Error
a few seconds ago
0
Agents: Updated Configuration
3 minutes ago
1
Filter by client name, host name, system / architecture or IP address
All versions
1 of 1 forwarders
Client Name
Agent Type
Version
Status
Check-In
Configuration Update
Server Classes
ACE22A00-A94E-4D6E-94D5-AE490AD48ADC
Universal Forwarder
9.4.7
Ok
a minute ago
in 5 hours
100_IngestAction_AutoGenerated


http://127.0.0.1:8000/en-US/manager/search/agent_management?activePanelId=configurations&agents.tableOptions.guid=false&agents.tableOptions.instan...
splunk>enterprise
Apps
Administrator
4 Messages
Settings
Activity
Help
Find
Forwarder Management
Forwarders 1
Configurations 1
Groups / Server Classes 1
Status: Fully Deployed
a few seconds ago
1 100% of all configurations
Status: Partially Deployed
a few seconds ago
0
Action
Filter by application name or server class name
All deployment statuses
1 of 1 applications
Application Name
Author
Size
After delivery
Restart Agent
Deployment Status
Agents
Server Classes
splunk_ingest_actions
system
10 KB
Enabled
No
Successfully Deployed
1
100_IngestAction_AutoGenerated


splunk>enterprise
Apps
Administrator
4 Messages
Settings
Activity
Help
Find
Forwarder Management
Forwarders 1
Configurations 1
Groups / Server Classes 1
+ New server class
Filter by server class name or system / architecture
1 of 1 groups
Server Class Name
Reload Time
System / Architecture
Repository
100_IngestAction_AutoGenerated
5 minutes ago
Not assigned
C:\Program Files\Splunk\etc\deployment-apps


splunk>enterprise
Apps
Administrator
4 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
host=Saurabh-Home
Last 15 minutes
18 events (12/17/25 2:42:54.000 AM to 12/17/25 2:57:54.000 AM)
No Event Sampling
Job
Smart Mode
Events (18)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 minute per column
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 2
a sourcetype 2
INTERESTING FIELDS
a Account_Domain 2
a Account_Name 2
Cab_Id 1
Time
Event
12/17/25 2:48:44.000 AM
12/17/2025 02:48:44 AM
LogName=Application
EventCode=1001
EventType=4
ComputerName=Saurabh-Home
Show all 38 lines
host = SAURABH-HOME
source = WinEventLog:Application
sourcetype = WinEventLog:Application
12/17/25 2:48:43.000 AM
12/17/2025 02:48:43 AM


SplunkUniversalForwarder
File
Home
Share
View
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
This PC
Local Disk (C:)
Program Files
SplunkUniversalForwarder
Favorites
Desktop
Recent places
Downloads
Creative Cloud Files
Desktop
OneDrive
Saurabh Banyal
This PC
Libraries
Documents
Music
Pictures
Videos
Network
Control Panel
Name
Date modified
Type
Size
bin 17-12-2025 02:05 ... File folder
etc 17-12-2025 02:07 ... File folder
lib 17-12-2025 02:05 ... File folder
share 17-12-2025 02:05 ... File folder
swidtag 17-12-2025 02:05 ... File folder
var 17-12-2025 02:07 ... File folder
copyright 25-11-2025 09:22 ... Text Document 1 KB
license-eula 25-11-2025 09:22 ... Rich Text Format 127 KB
license-eula 25-11-2025 09:22 ... Text Document 60 KB
openssl.cnf 25-11-2025 09:26 ... CNF File 11 KB
README-splunk 25-11-2025 09:33 ... Text Document 1 KB
splunkforwarder-9.4.7-2a9293b80994-win... 25-11-2025 10:29 ... 7-2A9293B80994-... 73 KB
uf 25-11-2025 10:04 ... File 0 KB