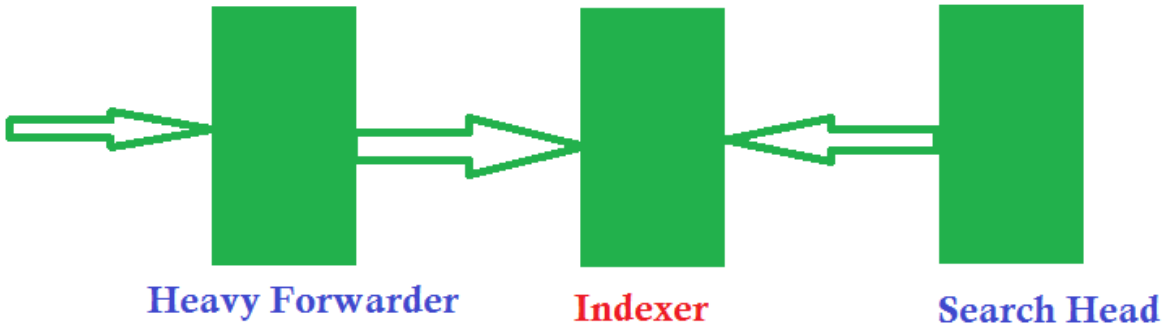
Adding Windows Server to Splunk Enterprise through WMI



Architecture Overview (WMI)

```
Windows Server (no agent)
        ↓  WMI
Splunk Enterprise / Heavy Forwarder
        ↓
Indexer
```

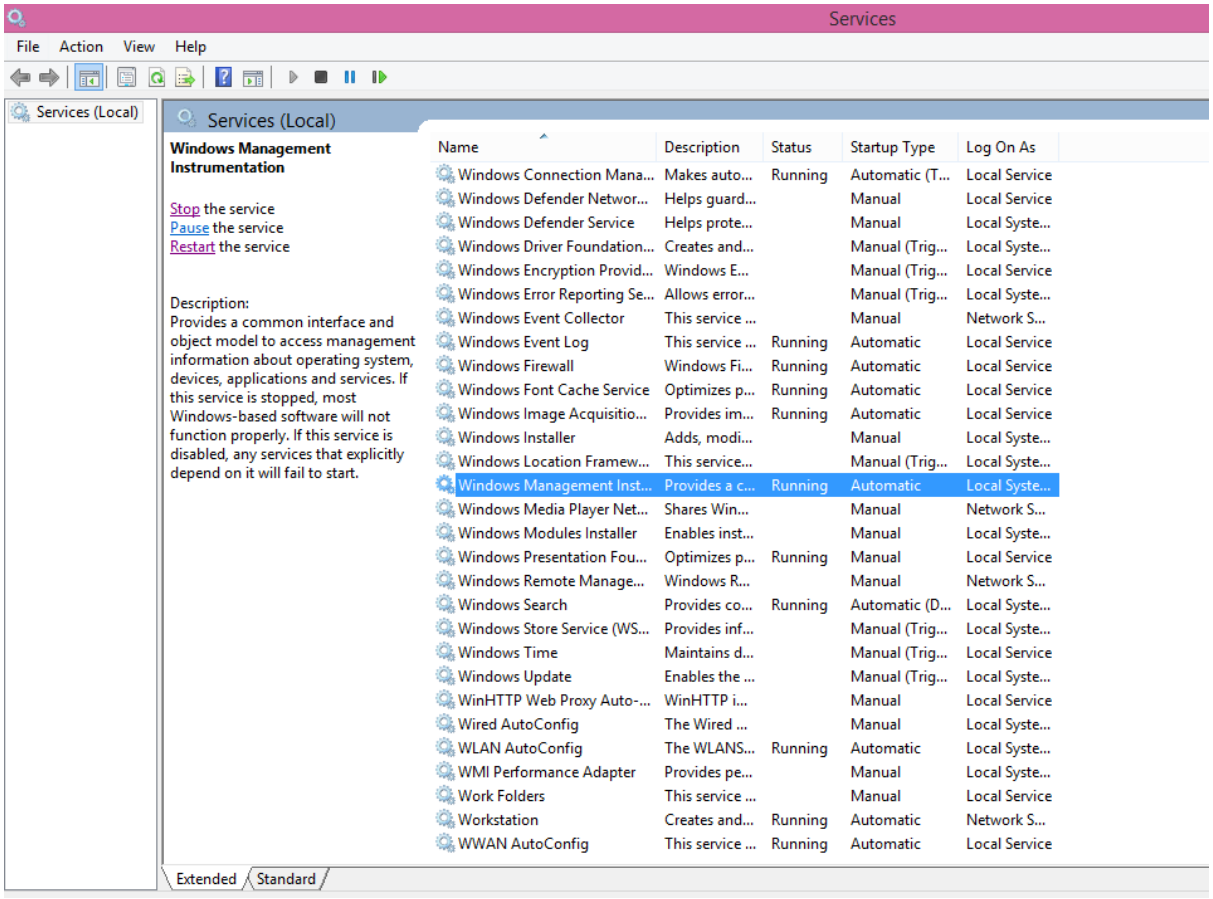
☞ **WMI input runs on a Heavy Forwarder or Indexer**,
☞ **NOT on a Search Head**.

---

1. Prerequisites (Windows Server Target)

On the target Windows Server

✓ WMI service running
✓ RPC & DCOM enabled Port 135
✓ Windows Firewall open 135



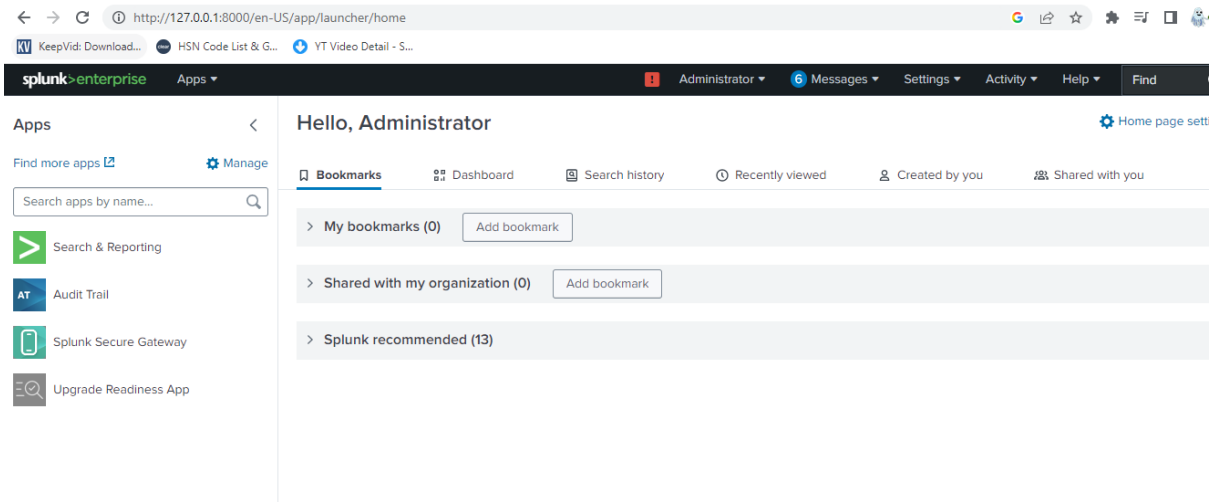
Configure Splunk WMI Input (Splunk Side)

Option A: Using Splunk Web (Recommended)

On Heavy Forwarder / Indexer

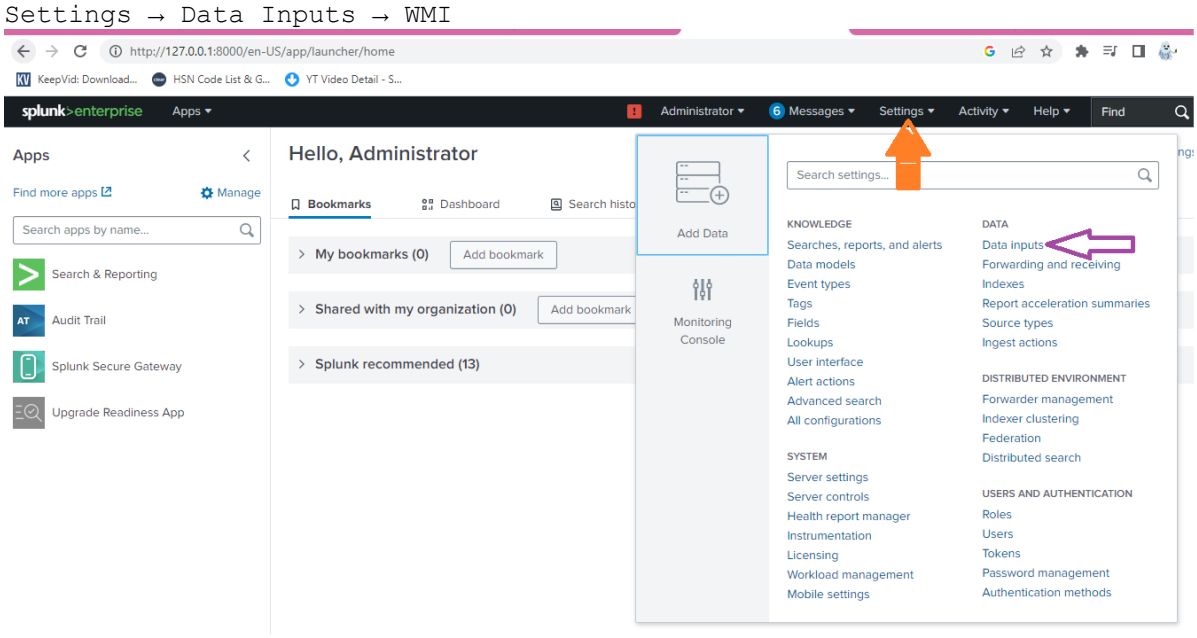
1. Login to Splunk Web:

http://<127.0.0.1>:8000

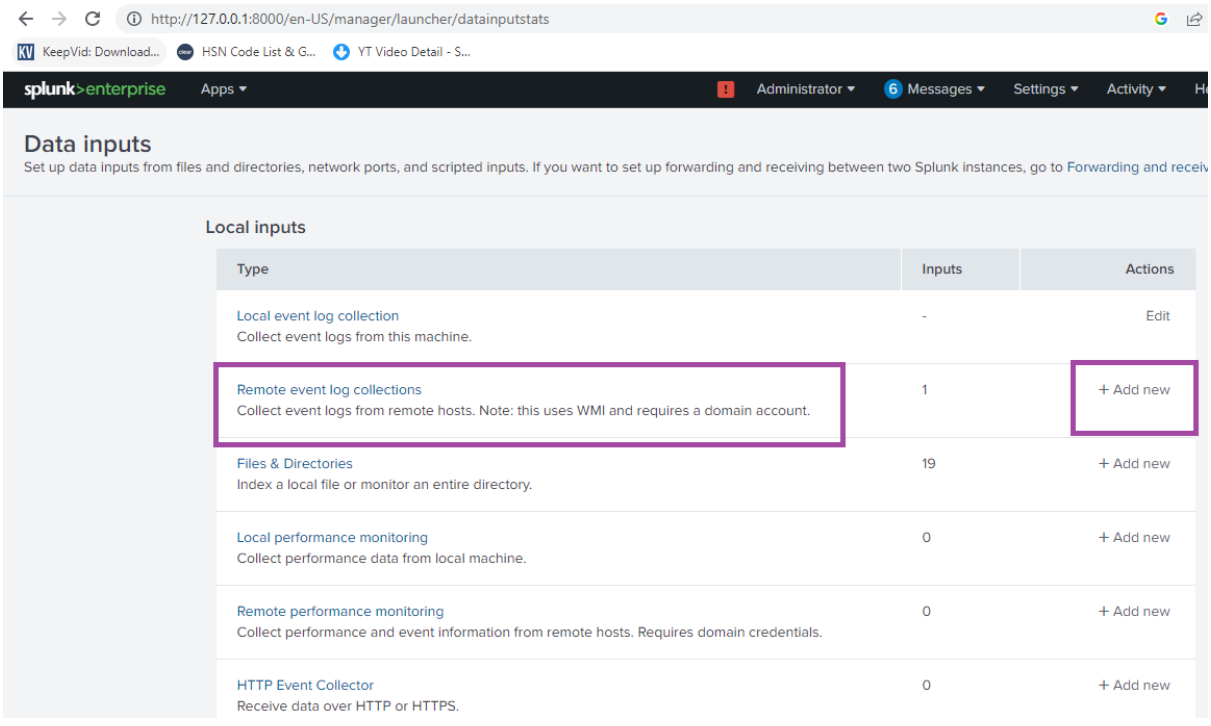


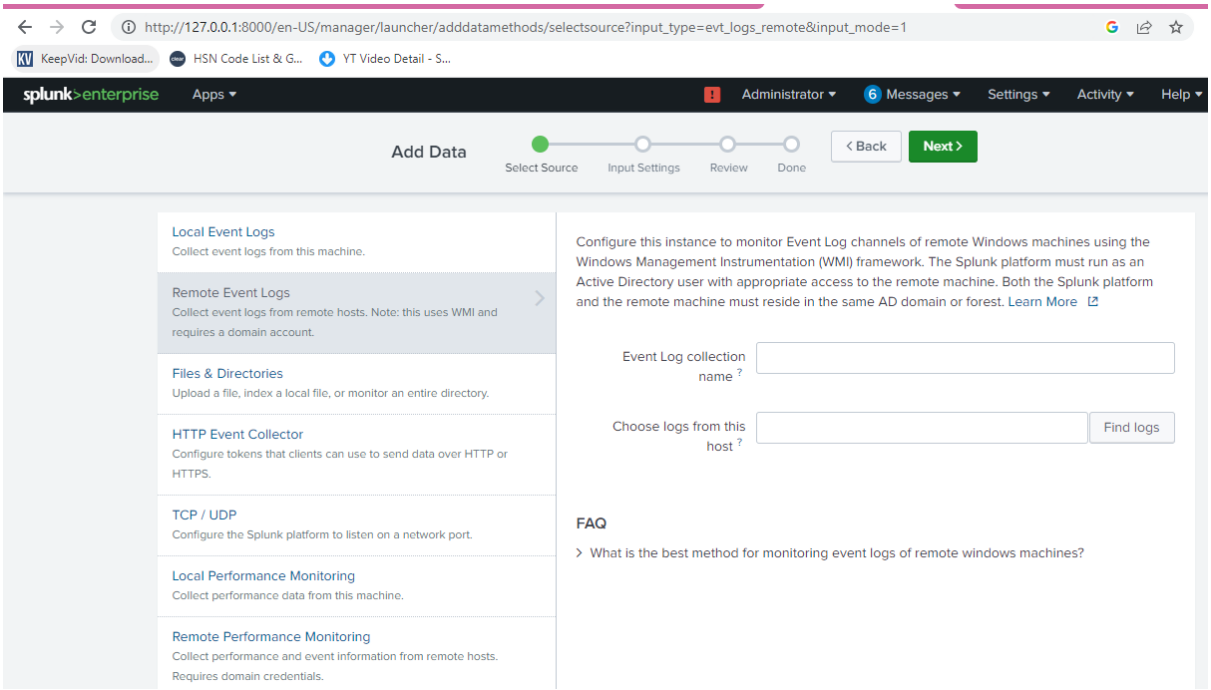
2. Go to:

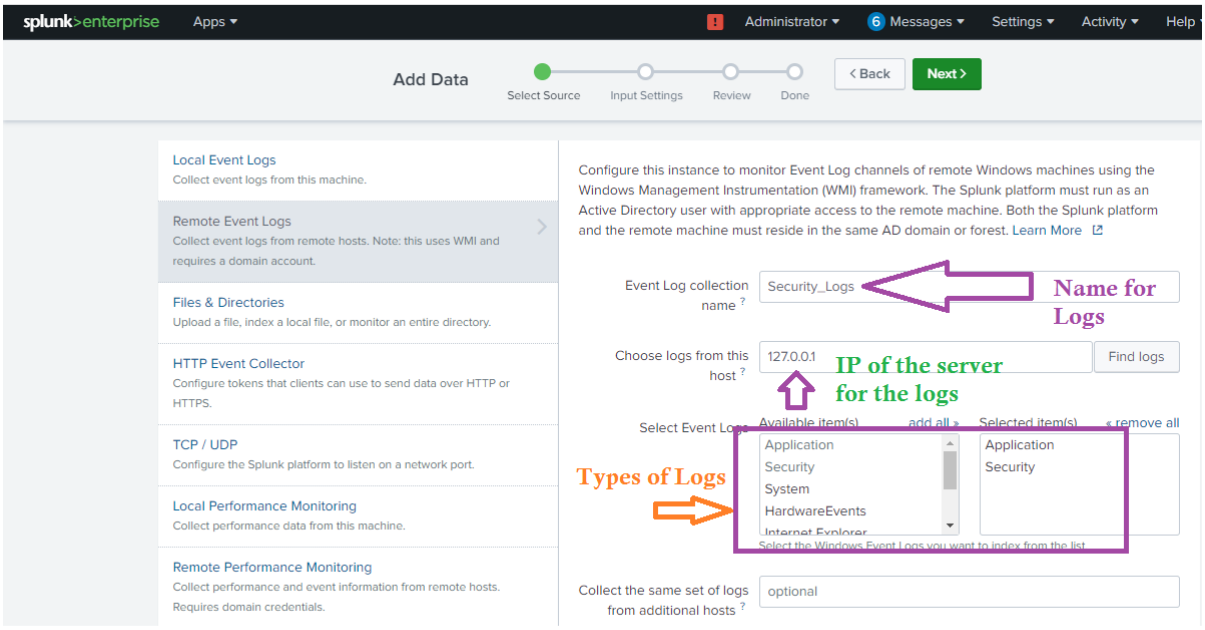
`Settings → Data Inputs → WMI`

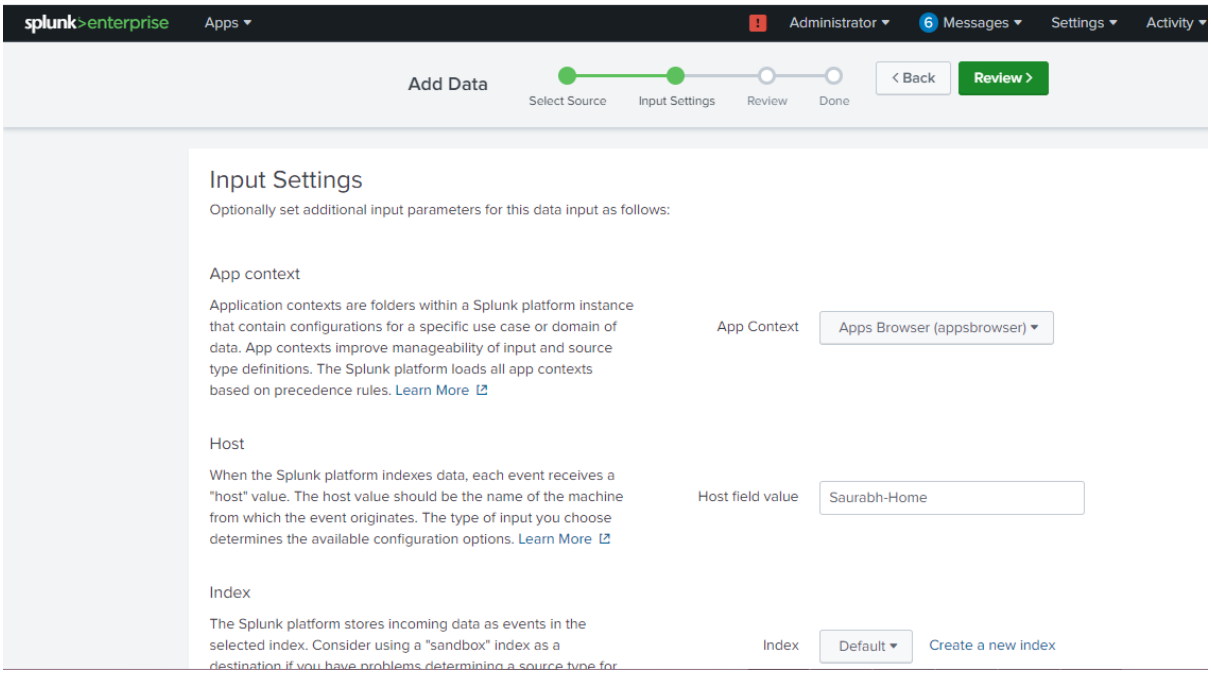


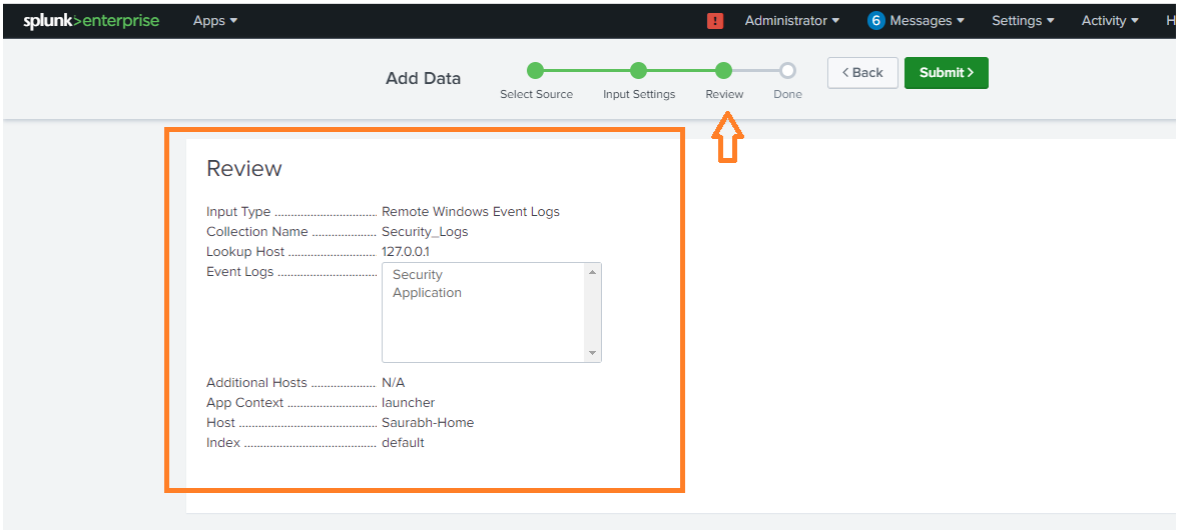
3. Click **New Local WMI**

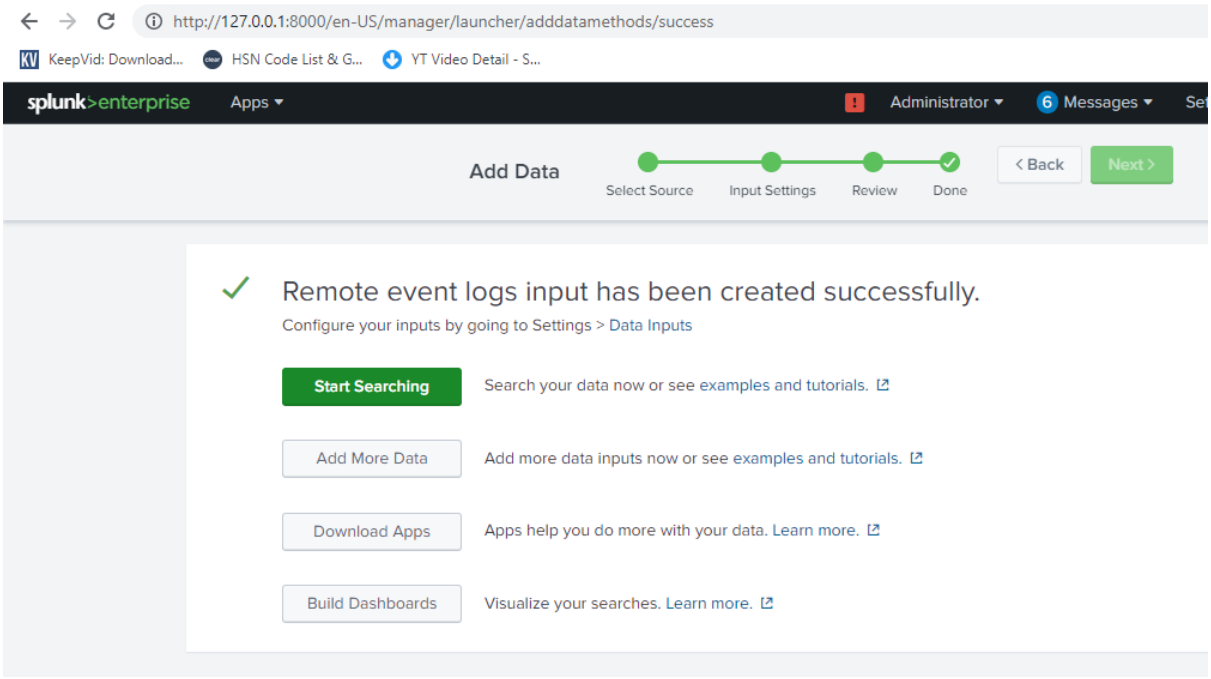


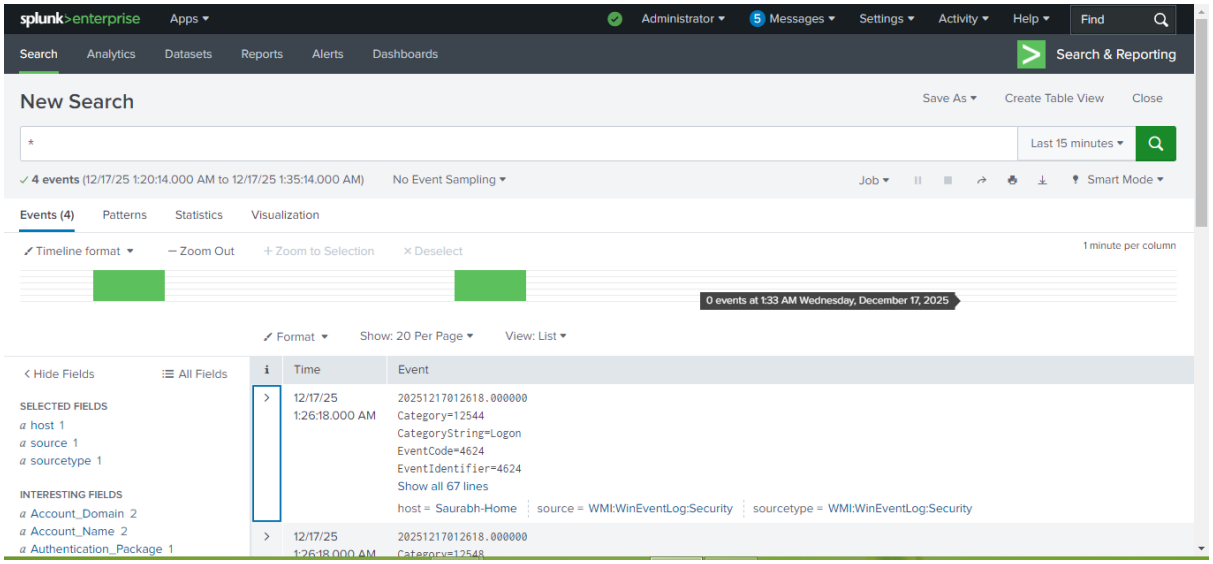

http://127.0.0.1:8000/en-US/manager/launcher/adddatamethods/selectsource?input_type=evt_logs_remote&input_mode=1
KeepVid: Download...
HSN Code List & G...
YT Video Detail - S...
splunk>enterprise
Apps
Administrator
6 Messages
Settings
Activity
Help
Add Data
Select Source
Input Settings
Review
Done
< Back
Next >
Local Event Logs
Collect event logs from this machine.
Remote Event Logs
Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.
Files & Directories
Upload a file, index a local file, or monitor an entire directory.
HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.
TCP / UDP
Configure the Splunk platform to listen on a network port.
Local Performance Monitoring
Collect performance data from this machine.
Remote Performance Monitoring
Collect performance and event information from remote hosts. Requires domain credentials.
Configure this instance to monitor Event Log channels of remote Windows machines using the Windows Management Instrumentation (WMI) framework. The Splunk platform must run as an Active Directory user with appropriate access to the remote machine. Both the Splunk platform and the remote machine must reside in the same AD domain or forest. Learn More
Event Log collection name ?
Choose logs from this host ?
Find logs
FAQ
What is the best method for monitoring event logs of remote windows machines?

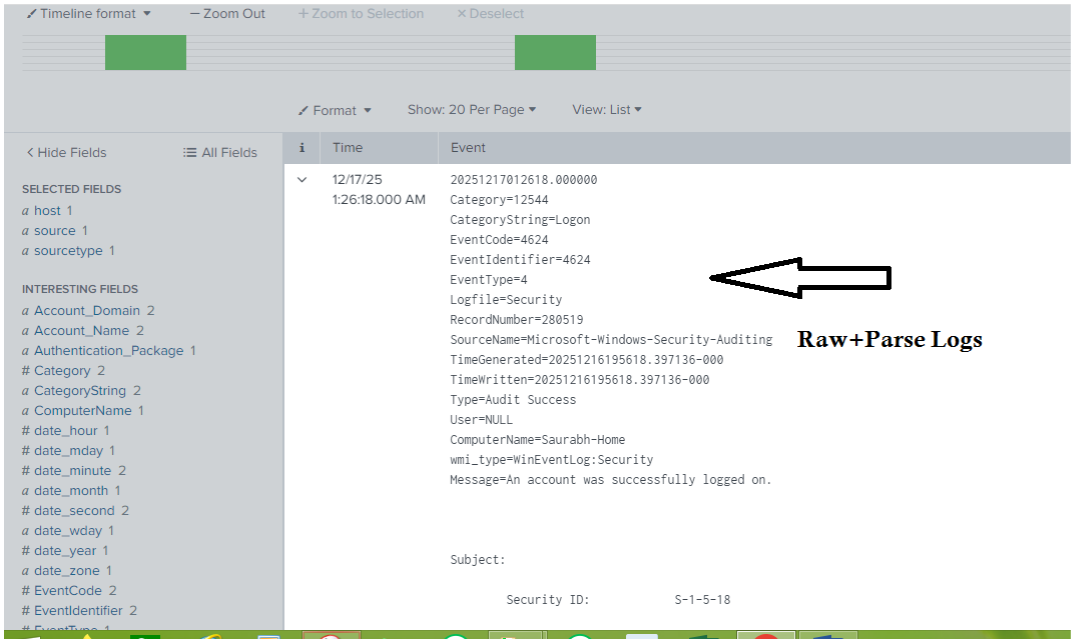

splunk>enterprise
Apps
Administrator
6 Messages
Settings
Activity
Help
Add Data
Select Source
Input Settings
Review
Done
< Back
Next >
Local Event Logs
Collect event logs from this machine.
Remote Event Logs
Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.
Files & Directories
Upload a file, index a local file, or monitor an entire directory.
HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.
TCP / UDP
Configure the Splunk platform to listen on a network port.
Local Performance Monitoring
Collect performance data from this machine.
Remote Performance Monitoring
Collect performance and event information from remote hosts. Requires domain credentials.
Configure this instance to monitor Event Log channels of remote Windows machines using the Windows Management Instrumentation (WMI) framework. The Splunk platform must run as an Active Directory user with appropriate access to the remote machine. Both the Splunk platform and the remote machine must reside in the same AD domain or forest. Learn More
Event Log collection name
Security_Logs
Name for Logs
Choose logs from this host
127.0.0.1
IP of the server for the logs
Find logs
Select Event Logs
Available item(s)
add all »
Selected item(s)
« remove all
Types of Logs
Application
Security
System
HardwareEvents
Internet Explorer
Application
Security
Select the Windows Event Logs you want to index from the list.
Collect the same set of logs from additional hosts
optional


splunk>enterprise
Apps
Administrator
6 Messages
Settings
Activity
Add Data
Select Source
Input Settings
Review
Done
< Back
Review >
Input Settings
Optionally set additional input parameters for this data input as follows:
App context
Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. Learn More
App Context
Apps Browser (appsbrowser)
Host
When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More
Host field value
Saurabh-Home
Index
The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a
Index
Default
Create a new index


splunk>enterprise
Apps
Administrator
6 Messages
Settings
Activity
Add Data
Select Source
Input Settings
Review
Done
< Back
Submit >
Review
Input Type ..... Remote Windows Event Logs
Collection Name ..... Security_Logs
Lookup Host 127.0.0.1
Event Logs ..... Security
Application
Additional Hosts ..... N/A
App Context ..... launcher
Host ..... Saurabh-Home
Index ..... default


http://127.0.0.1:8000/en-US/manager/launcher/adddatamethods/success
KeepVid: Download...
HSN Code List & G...
YT Video Detail - S...
splunk>enterprise
Apps
Administrator
6 Messages
Add Data
Select Source
Input Settings
Review
Done
< Back
Next >
Remote event logs input has been created successfully.
Configure your inputs by going to Settings > Data Inputs
Start Searching
Search your data now or see examples and tutorials.
Add More Data
Add more data inputs now or see examples and tutorials.
Download Apps
Apps help you do more with your data. Learn more.
Build Dashboards
Visualize your searches. Learn more.


splunk>enterprise
Apps
Administrator
5 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
*
Last 15 minutes
4 events (12/17/25 1:20:14.000 AM to 12/17/25 1:35:14.000 AM)
No Event Sampling
Job
Smart Mode
Events (4)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 minute per column
0 events at 1:33 AM Wednesday, December 17, 2025
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
Time
Event
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a Account_Domain 2
a Account_Name 2
a Authentication_Package 1
12/17/25
1:26:18.000 AM
20251217012618.000000
Category=12544
CategoryString=Logon
EventCode=4624
EventIdentifier=4624
Show all 67 lines
host = Saurabh-Home
source = WMI:WinEventLog:Security
sourcetype = WMI:WinEventLog:Security


Timeline format
Zoom Out
Zoom to Selection
Deselect
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
Time
Event
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a Account_Domain 2
a Account_Name 2
a Authentication_Package 1
Category 2
a CategoryString 2
a ComputerName 1
date_hour 1
date_mday 1
date_minute 2
a date_month 1
date_second 2
a date_wday 1
date_year 1
a date_zone 1
EventCode 2
EventIdentifier 2
12/17/25
1:26:18.000 AM
20251217012618.000000
Category=12544
CategoryString=Logon
EventCode=4624
EventIdentifier=4624
EventType=4
Logfile=Security
RecordNumber=280519
SourceName=Microsoft-Windows-Security-Auditing
TimeGenerated=20251216195618.397136-000
TimeWritten=20251216195618.397136-000
Type=Audit Success
User=NULL
ComputerName=Saurabh-Home
wmi_type=WinEventLog:Security
Message=An account was successfully logged on.
Subject:
Security ID: S-1-5-18
Raw+Parse Logs