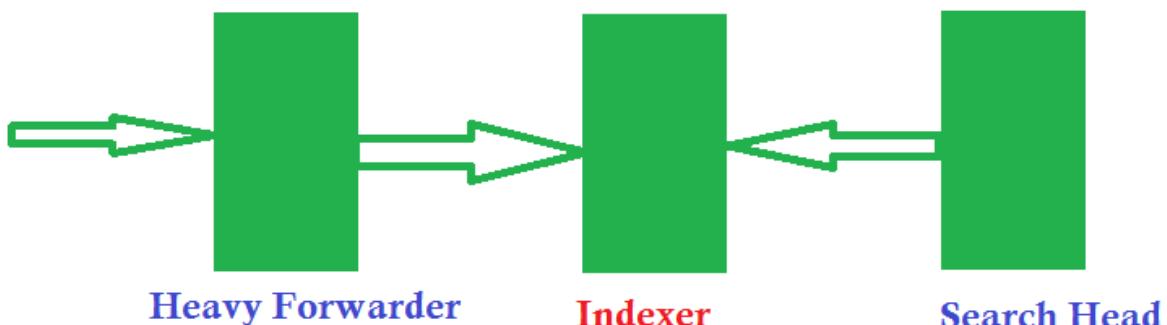


Adding Windows Server to Splunk Enterprise through WMI



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

S

File Action View Help

Services (Local)

Windows Management Instrumentation

[Stop the service](#) [Pause the service](#) [Restart the service](#)

Description:
Provides a common interface and object model to access management information about operating system, devices, applications and services. If this service is stopped, most Windows-based software will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start.

Name	Description	Status	Startup Type	Log On As
Windows Connection Mana...	Makes auto...	Running	Automatic (T...	Local Service
Windows Defender Networ...	Helps guard...	Manual	Local Service	Local Syste...
Windows Defender Service	Helps prote...	Manual	Local Syste...	Local Syste...
Windows Driver Foundation...	Creates and...	Manual (Trig...	Local Syste...	Local Syste...
Windows Encryption Provid...	Windows E...	Manual (Trig...	Local Service	Local Syste...
Windows Error Reporting Se...	Allows error...	Manual (Trig...	Local Syste...	Local Syste...
Windows Event Collector	This service ...	Manual	Network S...	Network S...
Windows Event Log	This service ...	Running	Automatic	Local Service
Windows Firewall	Windows Fi...	Running	Automatic	Local Service
Windows Font Cache Service	Optimizes p...	Running	Automatic	Local Service
Windows Image Acquisitio...	Provides im...	Running	Automatic	Local Service
Windows Installer	Adds, modifi...	Manual	Local Syste...	Local Syste...
Windows Location Framew...	This service...	Manual (Trig...	Local Syste...	Local Syste...
Windows Management Inst...	Provides a c...	Running	Automatic	Local Syste...
Windows Media Player Net...	Shares Win...	Manual	Network S...	Network S...
Windows Modules Installer	Enables inst...	Manual	Local Syste...	Local Syste...
Windows Presentation Fou...	Optimizes p...	Running	Manual	Local Service
Windows Remote Manage...	Windows R...	Manual	Network S...	Network S...
Windows Search	Provides co...	Running	Automatic (D...	Local Syste...
Windows Store Service (WS...	Provides inf...	Manual (Trig...	Local Syste...	Local Syste...
Windows Time	Maintains d...	Manual (Trig...	Local Service	Local Service
Windows Update	Enables the ...	Manual (Trig...	Local Syste...	Local Syste...
WinHTTP Web Proxy Auto...	WinHTTP i...	Manual	Local Service	Local Service
Wired AutoConfig	The Wired ...	Manual	Local Syste...	Local Syste...
WLAN AutoConfig	The WLANS...	Running	Automatic	Local Syste...
WMI Performance Adapter	Provides pe...	Manual	Local Syste...	Local Syste...
Work Folders	This service ...	Manual	Local Service	Local Service
Workstation	Creates and...	Running	Automatic	Network S...
WWAN AutoConfig	This service ...	Running	Automatic	Local Service

Extended Standard

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>

← → ⓘ http://127.0.0.1:8000/en-US/app/launcher/home

KeepVid: Download... HSN Code List & G... YT Video Detail - S...

splunk>enterprise Apps

Hello, Administrator

Home page setti

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)

Search apps by name...

Find more apps Manage

Search & Reporting Audit Trail Splunk Secure Gateway Upgrade Readiness App

2. Go to:

Settings → Data Inputs → WMI

The screenshot shows the Splunk Enterprise interface. In the top navigation bar, 'Administrator' is selected. A large orange arrow points upwards from the 'Data inputs' section in the sidebar towards the 'Settings' dropdown. Another orange arrow points to the 'Forwarding and receiving' link under the 'DATA' category in the sidebar.

splunk>enterprise Apps ▾

Hello, Administrator

Bookmarks Dashboard Search history

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

SYSTEM

- Server settings
- Server controls
- Health report manager
- Instrumentation
- Licensing
- Workload management
- Mobile settings

DATA

- Data inputs (highlighted by orange arrow)
- Forwarding and receiving (highlighted by purple arrow)
- Indexes
- Report acceleration summaries
- Source types
- Ingest actions

DISTRIBUTED ENVIRONMENT

- Forwarder management
- Indexer clustering
- Federation
- Distributed search

USERS AND AUTHENTICATION

- Roles
- Users
- Tokens
- Password management
- Authentication methods

3. Click New Local WMI

http://127.0.0.1:8000/en-US/manager/launcher/datainputstats

The screenshot shows the 'Data inputs' page. A purple box highlights the 'Remote event log collections' row in the 'Local inputs' table. A purple rectangle surrounds the entire table area. A purple box also highlights the '+ Add new' button next to the 'Remote event log collections' row.

Data inputs

Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to Forwarding and receiving.

Local inputs

Type	Inputs	Actions
Local event log collection Collect event logs from this machine.	-	Edit
Remote event log collections Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.	1	+ Add new (highlighted by purple box)
Files & Directories Index a local file or monitor an entire directory.	19	+ Add new
Local performance monitoring Collect performance data from local machine.	0	+ Add new
Remote performance monitoring Collect performance and event information from remote hosts. Requires domain credentials.	0	+ Add new
HTTP Event Collector Receive data over HTTP or HTTPS.	0	+ Add new

← → ⌂ ⓘ http://127.0.0.1:8000/en-US/manager/launcher/adddatamethods/selectsource?input_type=evt_logs_remote&input_mode=1

KV 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

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.

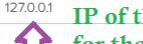
HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

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.

Event Log collection name ? Security_Logs 

Choose logs from this host ? 127.0.0.1  Find logs

Select Event Log Type Available Item(s) Selected item(s) * remove all

Application
Security
System
HardwareEvents
Internet Explorer
Select the Windows Event Logs you want to index from this list

Types of Logs 

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

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 destination if you have problems determining a source type for

Index Default ▾ Create a new index

splunk>enterprise Apps ▾

Administrator ▾ 6 Messages ▾ Settings ▾ Activity ▾ H

Add Data

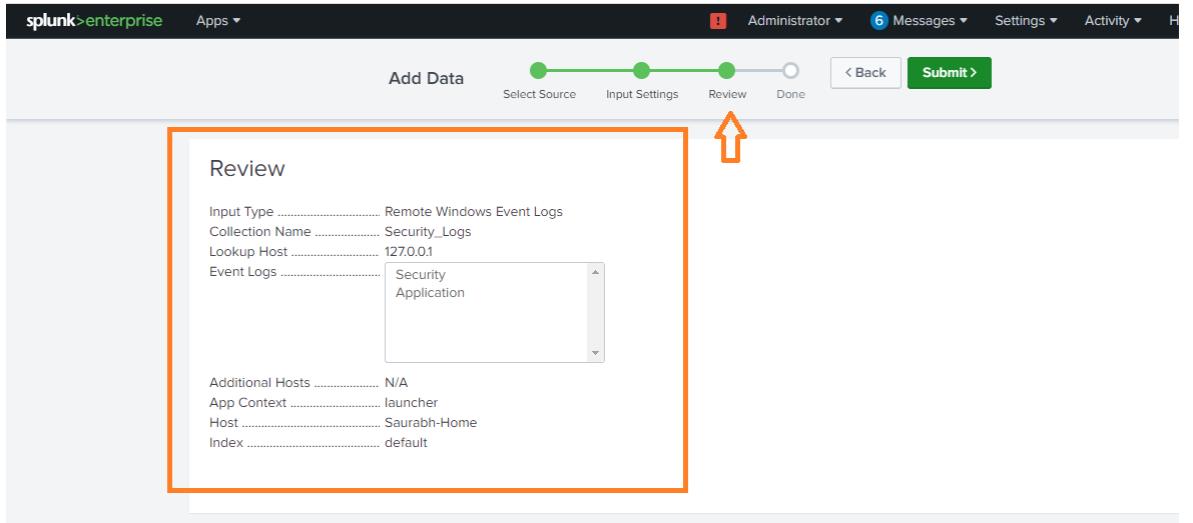
Review

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

Done

< Back Submit >



← → ⌂ ⓘ http://127.0.0.1:8000/en-US/manager/launcher/adddatamethods/success

KV KeepVid: Download... HSN Code List & G... YT Video Detail - S...

splunk>enterprise Apps ▾

Administrator ▾ 6 Messages ▾ Set

Add Data

Review ✓ Done

✓ Remote event logs input has been created successfully.

Configure your inputs by going to Settings > Data Inputs

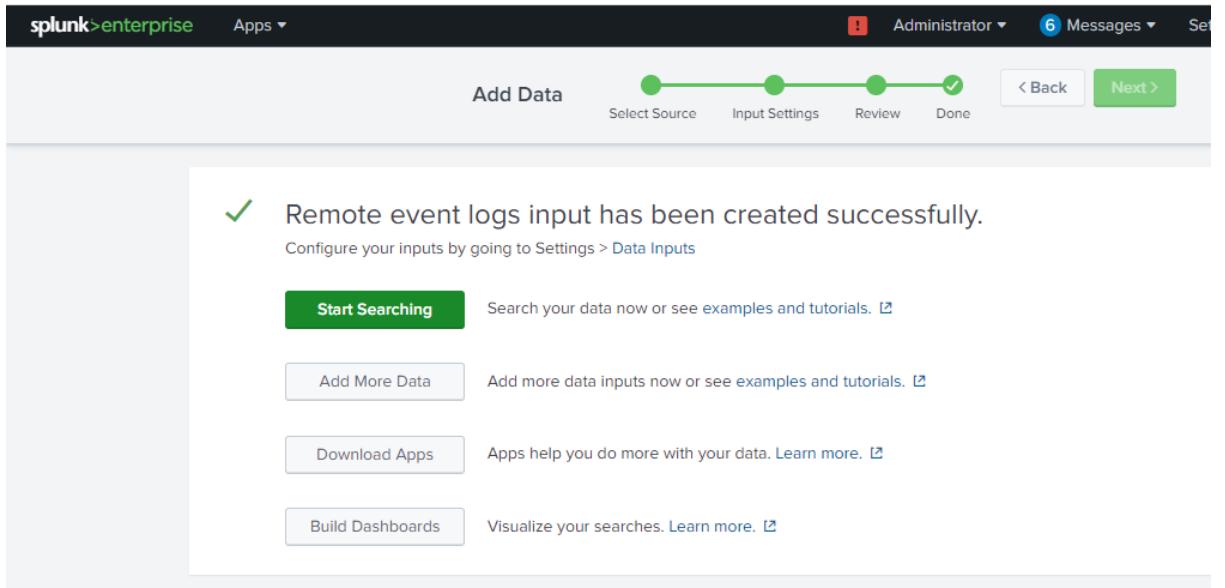
[Start Searching](#) Search your data now or see examples and tutorials. ↗

[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. ↗

< Back Next >



Splunk > enterprise Apps ▾

Administrator ▾ 5 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

4 events (12/17/25 1:20:14.000 AM to 12/17/25 1:35:14.000 AM) No Event Sampling ▾

Events (4) Patterns Statistics Visualization

✓ Timeline format - Zoom Out + Zoom to Selection × Deselect

1 minute per column

Last 15 minutes ▾

0 events at 1:33 AM Wednesday, December 17, 2025

Format Show: 20 Per Page ▾ View: List ▾

Time	Event
12/17/25 1:26:18.000 AM	20251217012618.00000 Category=12544 CategoryString=Logon EventCode=4624 EventIdentifier=4624 Show all 67 lines host = Saurabh-Home source = WMI:WinEventLog:Security sourcetype = WMI:WinEventLog:Security
12/17/25 1:26:18.000 AM	20251217012618.00000 Category=12544 CategoryString=Logon EventCode=4624 EventIdentifier=4624 Show all 67 lines host = Saurabh-Home source = WMI:WinEventLog:Security sourcetype = WMI:WinEventLog:Security
12/17/25 1:26:18.000 AM	20251217012618.00000 Category=12544 CategoryString=Logon EventCode=4624 EventIdentifier=4624 Show all 67 lines host = Saurabh-Home source = WMI:WinEventLog:Security sourcetype = WMI:WinEventLog:Security
12/17/25 1:26:18.000 AM	20251217012618.00000 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 ▾

Time	Event
12/17/25 1:26:18.000 AM	20251217012618.00000 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=WMI:WinEventLog:Security Message=An account was successfully logged on.
	Subject:
	Security ID: S-1-5-18

Raw+Parse Logs