



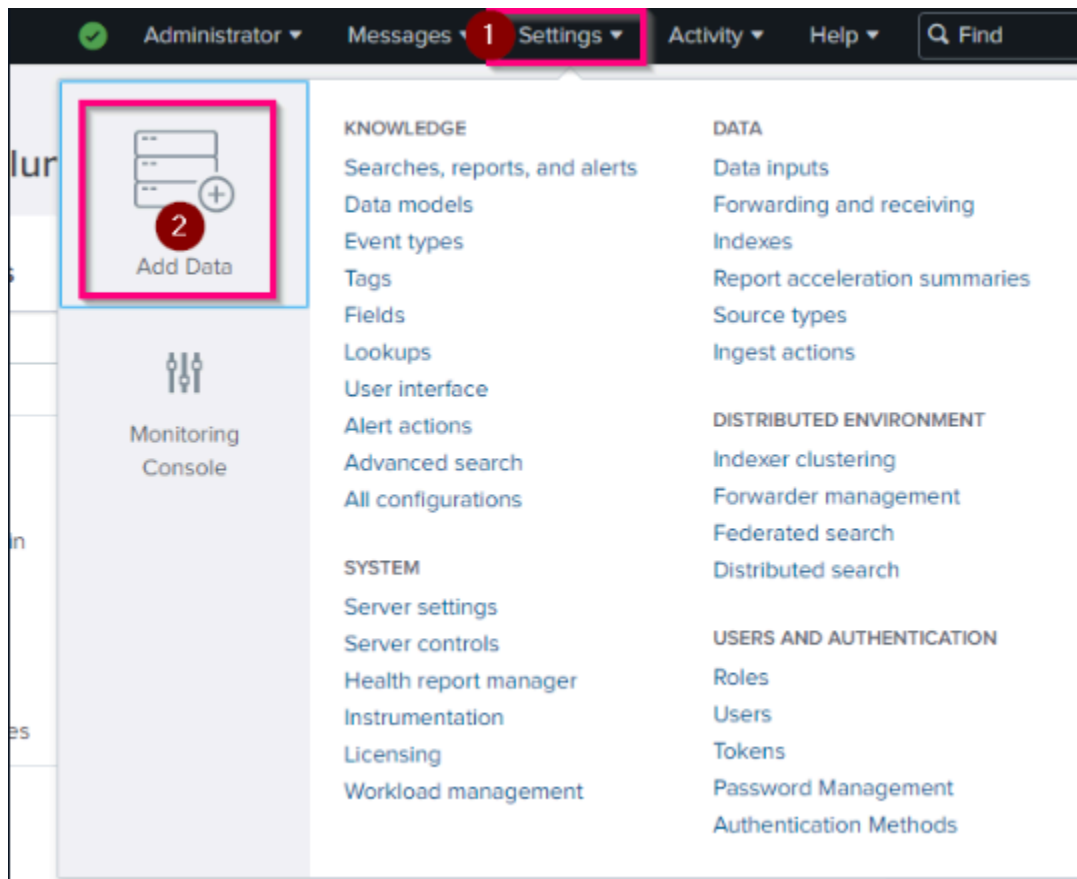
Add Data to Splunk

By: Ryan Stewart

In Splunk, there are various ways to add data. Here, I'll explore adding data using the forwarder installed on a Win10 computer and uploading a log file.

Add Data from Forwarder:

1. Go to ****Settings > Add Data.****



2. Select "Forward" at the bottom.

What data do you want to send to the Splunk platform?

Follow guides for onboarding popular data sources

Cloud computing
Get your cloud computing data in to the Splunk platform.
10 data sources

Networking
Get your networking data in to the Splunk platform.
2 data sources

Operating System
Get your operating system data in to the Splunk platform.
1 data source

Security
Get your security data in to the Splunk platform.
3 data sources

4 data sources in total

Or get data in with the following methods

Upload
files from my computer
Local log files
Local structured files (e.g. CSV)
[Tutorial for adding data](#)

Monitor
files and ports on this Splunk platform instance
Files - HTTP - WMI - TCP/UDP - Scripts
Modular inputs for external data sources

Forward
data from a Splunk forwarder
Files - TCP/UDP - Scripts

3. Add the computer to the selected host and assign a Server Class Name.

4. Click "Next."

splunk>enterprise Apps Administrator Messages Settings Activity

Add Data Select Forwarders Select Source Input Settings Review Done < Back Next > 3

Select Forwarders

Create or select a server class for data inputs. Use this page only in a single-instance Splunk environment.

To enable forwarding of data from deployment clients to this instance, set the output configurations on your forwarders. [Learn More](#)

Select Server Class New Existing

Available host(s) add all Selected host(s) remove all

DESKTOP-4L9QKFS WINDOWS 1 DESKTOP-4L9QKFS WINDOWS

New Server Class Name 2 Windows10_client

- Select the data you want to monitor, e.g., local event logs from the computer.
- Choose the specific log.

- Click "Next."

Add Data

Progress: Select Forwarders, Select Source, Input Settings, Review, Done

Local Event Logs (1) [Collect event logs from this machine.](#)

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Local Performance Monitoring
Collect performance data from this machine.

Scripts
Get data from any API, service, or database with a script.

Splunk Assist Instance Identifier
Assigns a random identifier to each Beam node

Powershell v3 Modular Input
Execute PowerShell scripts v3 with parameters as inputs.

Configure selected Splunk Universal Forwarders to monitor local Windows event log channels, which contain log data published by installed applications, services, and system processes. The event log monitor runs once for every event log input defined in the Splunk platform. [Learn More](#)

Select Event Logs	Available Item(s)	add all >	Selected item
	Application		Application
	ForwardedEvents		Security
	Security		Setup
	Setup		System
	System		

Select the Windows Event Logs you want to index from the list.

FAQ

- > What event logs does this Splunk platform instance have access to?
- > What is the best method for monitoring event logs of remote Windows machines?

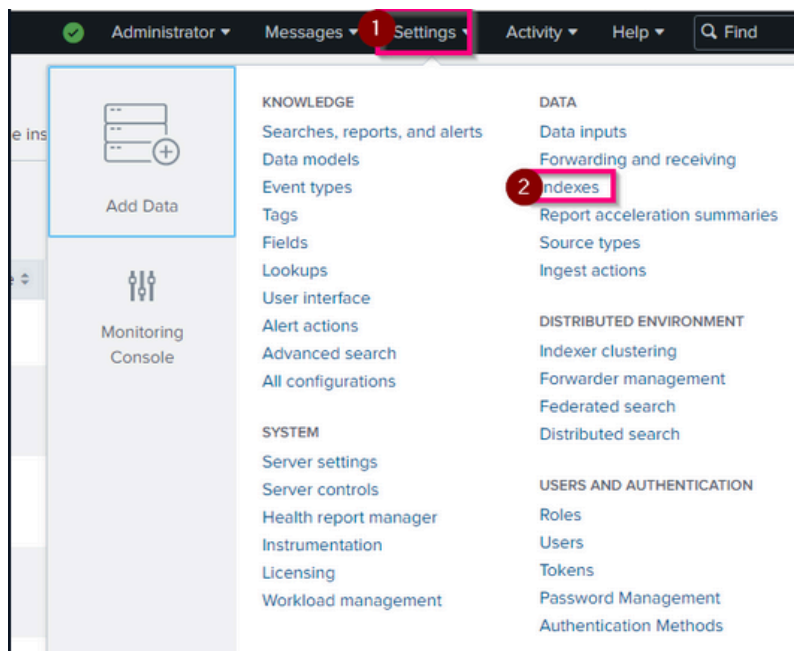
- Select the index for the logs. Create a new index, e.g., "WinLog_clients."

- Click "Review" to verify and then submit.

6. Click "Start Searching" to find the recent connection on the client's computer.

Check Your Indexes:

1. Go to Settings > Indexes.



2. Search for the index you created.

- If no events are incoming, proceed to configure.

Indexes

A repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexer. [Learn more](#)

13 Indexes 20 per page

Name	Actions	Type	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Home Path	Frozen Path
_audit	Edit Delete Disable	Events	system	3 MB	488.28 GB	13.8K	2 hours ago	a few seconds ago	\$SPLUNK_HOME\$/data/_audit	N/A
_configtrack	Edit Delete Disable	Events	system	3 MB	488.28 GB	170	2 hours ago	9 minutes ago	\$SPLUNK_HOME\$/data/_configtrack	N/A
_internal	Edit Delete Disable	Events	system	7 MB	488.28 GB	60.1K	2 hours ago	a few seconds ago	\$SPLUNK_HOME\$/data/_internal	N/A
_introspecti	Edit Delete Disable	Events	system	16 MB	488.28 GB	6.8K	2 hours ago	a few seconds ago	\$SPLUNK_HOME\$/data/_introspecti	N/A
_metrics	Edit Delete Disable	Metrics	system	7 MB	488.28 GB	46K	2 hours ago	a few seconds ago	\$SPLUNK_HOME\$/data/_metrics	N/A
_metrics_roll	Edit Delete Disable	Metrics	system	1 MB	488.28 GB	0			\$SPLUNK_HOME\$/data/_metrics_roll	N/A
_telemetry	Edit Delete Disable	Events	system	1 MB	488.28 GB	1	an hour ago	an hour ago	\$SPLUNK_HOME\$/data/_telemetry	N/A
_thefishbuck	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_HOME\$/data/_thefishbuck	N/A
history	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_HOME\$/data/history	N/A
main	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_HOME\$/data/default	N/A
splunklogge	Edit Delete Enable	Events	system	0 B	488.28 GB	0			\$SPLUNK_HOME\$/data/splunklogge	N/A
summary	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_HOME\$/data/summary	N/A
winlog_clie	Edit Delete Disable	Events	alert_logeve	1 MB	500 GB	0			\$SPLUNK_HOME\$/data/winlog_clie	N/A

Add Receiver:

1. Go to ****Settings > Forwarding and Receiving.****
2. Click to add a new receiving.

Forwarding and receiving

Forward data

Set up forwarding between two or more Splunk instances.

[Forwarding defaults](#)

[Configure forwarding](#)

[+ Add new](#)

Receive data

Configure this instance to receive data forwarded from other instances.

[Configure receiving](#)

[1 + Add new](#)

- Add the 9997 port (default).
- Wait a few minutes, then check indexes for new values.

Indexes											New Index
A repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexer. Learn more											
13 Indexes											20 per page
filter											
Name	Actions	Type	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Home Path	Frozen Path	
._audit	Edit Delete Disable	Events	system	3 MB	488.28 GB	15.7K	2 hours ago	a few seconds ago	\$SPLUNK_DB/auditdb	N/A	
._configtrack	Edit Delete Disable	Events	system	3 MB	488.28 GB	201	2 hours ago	a minute ago	\$SPLUNK_DB/_configtrack/db	N/A	
._internal	Edit Delete Disable	Events	system	7 MB	488.28 GB	73.8K	2 hours ago	a few seconds ago	\$SPLUNK_DB/_internal/db	N/A	
._introspection	Edit Delete Disable	Events	system	15 MB	488.28 GB	7.04K	2 hours ago	a few seconds ago	\$SPLUNK_DB/_introspection/db	N/A	
._metrics	Edit Delete Disable	Metrics	system	8 MB	488.28 GB	55.5K	2 hours ago	a few seconds ago	\$SPLUNK_DB/_metrics/db	N/A	
._metrics_rollup	Edit Delete Disable	Metrics	system	1 MB	488.28 GB	0			\$SPLUNK_DB/_metrics_rollup/db	N/A	
._telemetry	Edit Delete Disable	Events	system	1 MB	488.28 GB	1	2 hours ago	2 hours ago	\$SPLUNK_DB/_telemetry/db	N/A	
._thefishbucket	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB/_fishbucket/db	N/A	
history	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB/historydb	N/A	
main	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB/defaultdb	N/A	
splunklog	Edit Delete Enable	Events	system	0 B	488.28 GB	0			\$SPLUNK_DB/splunkloger/db	N/A	
summary	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB/summarydb	N/A	
winlog_clients	Edit Delete Disable	Events	alert_logevent	1 MB	500 GB	2.53K	an hour ago	a minute ago	\$SPLUNK_DB/winlog_clients/db	N/A	

3. Check your indexes again to confirm the data reception.

Try a Quick Search.

New Search Save As Create Table View Close

index="winlog_clients" Last 24 hours Q

✓ 2,709 events (9/1/22 1:00:00.000 AM to 9/2/22 1:38:10.000 AM) No Event Sampling Job || ↗ ⬇ Smart Mode

Events (2,709) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

List Format 20 Per Page < Prev 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields	All Fields	i	Time	Event
SELECTED FIELDS a host 1 a source 3 a sourcetype 3				
INTERESTING FIELDS a ComputerName 2 a Domaine_du_compte 8 # EventCode 100+ # EventType 4 a ID de sécurité 38 a ID d'ouverture de session 43 a Index 1 a Keywords 9 # linecount 30 a LogName 3 a Message 100+ a Nom_du_compte 32 a OpCode 11 a punct 100+ # RecordNumber 100+ a Sid 5 # SidType 1 a SourceName 40 a splunk_server 1 a TaskCategory 35 a Type 3 a User 1 140 more fields + Extract New Fields				
		>	9/2/22 1:37:40.000 AM	09/02/2022 10:37:40 AM LogName=Security EventCode=4634 EventType=0 ComputerName=DESKTOP-4L9QKFS Show all 22 lines host = DESKTOP-4L9QKFS source = WinEventLog:Security sourcetype = WinEventLog:Security
		>	9/2/22 1:37:40.000 AM	09/02/2022 10:37:40 AM LogName=Security EventCode=4634 EventType=0 ComputerName=DESKTOP-4L9QKFS Show all 22 lines host = DESKTOP-4L9QKFS source = WinEventLog:Security sourcetype = WinEventLog:Security
		>	9/2/22 1:37:40.000 AM	09/02/2022 10:37:40 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-4L9QKFS Show all 28 lines host = DESKTOP-4L9QKFS source = WinEventLog:Security sourcetype = WinEventLog:Security
		>	9/2/22 1:37:40.000 AM	09/02/2022 10:37:40 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-4L9QKFS Show all 70 lines host = DESKTOP-4L9QKFS source = WinEventLog:Security sourcetype = WinEventLog:Security
		>	9/2/22 1:37:40.000 AM	09/02/2022 10:37:40 AM LogName=Security EventCode=4624 EventType=0

Add Data From Uploaded Logs:

1. Go to Settings > Add Data.

Administrator Messages 1 Settings Activity Help Q Find

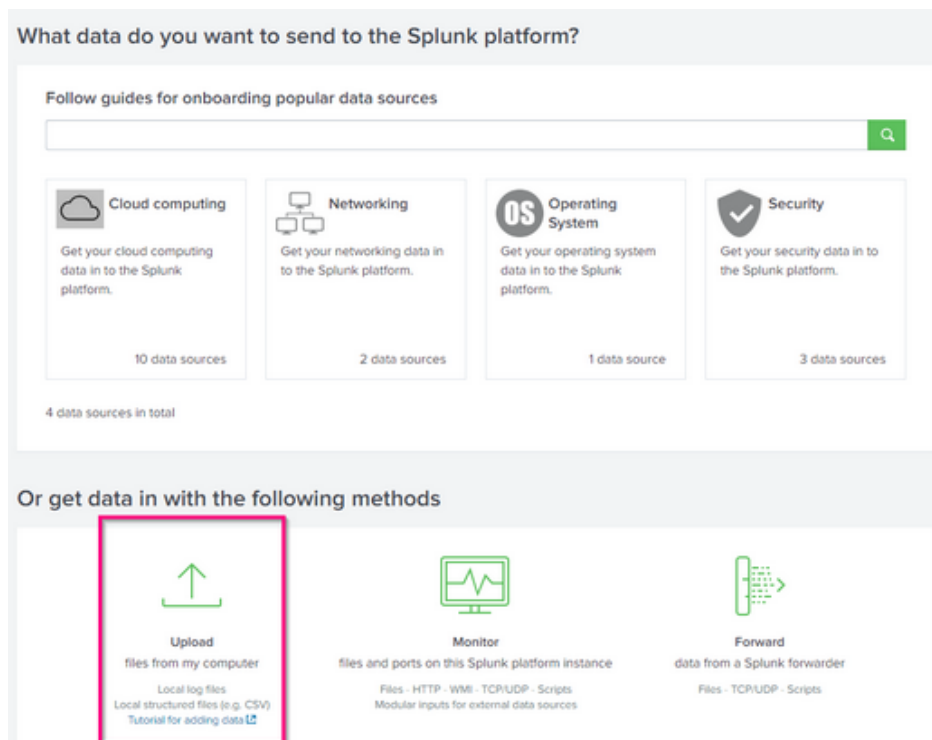
ur

2 Add Data

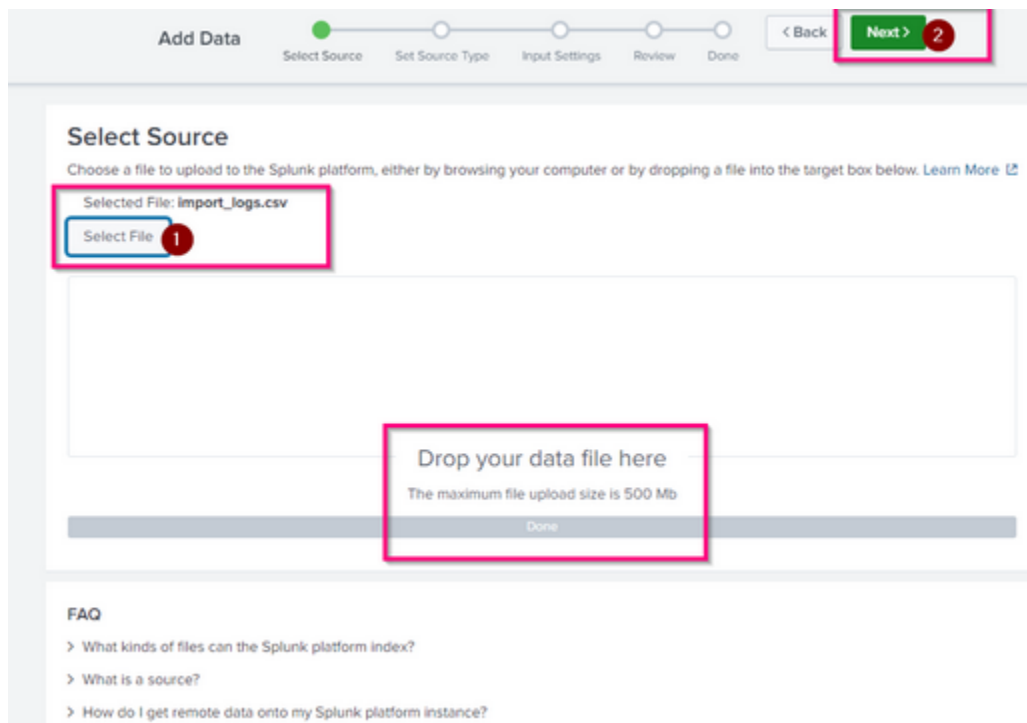
Monitoring Console

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
SYSTEM Server settings Server controls Health report manager Instrumentation Licensing Workload management	DISTRIBUTED ENVIRONMENT Indexer clustering Forwarder management Federated search Distributed search
	USERS AND AUTHENTICATION Roles Users Tokens Password Management Authentication Methods

2. Select "Upload" in the bottom left corner.



3. Upload the desired file, then click "Next."



- Check how Splunk will read the file, and press "Next" if everything is correct.

4. Select a host field value if needed and choose the index (use default for the exercise).

5. Continue to the end and start searching on the uploaded data.

The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with 'splunk>enterprise' and various menu items like 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a search bar. Below this is a secondary navigation bar with 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The main content area is titled 'New Search' and shows a search query: `source="import_logs.csv" host="WIN-D9CJUS3F2RK" sourcetype="csv"`. It indicates that 938 events were found. The interface includes a timeline view and a list view. The list view is currently selected, showing a table of search results. The table has columns for 'Time' and 'Event'. The first event is an 'Audit Success' log from 2/9/22 at 9:37:03.000 AM, detailing a successful login for a user named 'An account was successfully log ged on.' The event details include 'Security ID: SYSTEM' and 'Account Name: WIN-D9CJUS3F2RK\$'. The source is identified as 'import_logs.csv' and the sourcetype as 'csv'. The interface also includes a sidebar on the left with 'SELECTED FIELDS' and 'INTERESTING FIELDS' sections, and a 'Format' dropdown set to 'List'.

Time	Event
2/9/22 9:37:03.000 AM	Audit Success,02/09/2022 09:37:03,Microsoft-Windows-Security-Auditing,4624,Logon,"An account was successfully log ged on." Subject: Security ID: SYSTEM Account Name: WIN-D9CJUS3F2RK\$ Show all 59 lines host = WIN-D9CJUS3F2RK source = import_logs.csv sourcetype = csv
2/9/22 9:37:03.000 AM	Audit Success,02/09/2022 09:37:03,Microsoft-Windows-Security-Auditing,4672,Special Logon,"Special privileges assi gned to new logon." Subject: Security ID: SYSTEM Account Name: SYSTEM Show all 20 lines host = WIN-D9CJUS3F2RK source = import_logs.csv sourcetype = csv
2/9/22 9:37:03.000 AM	Audit Success,02/09/2022 09:37:03,Microsoft-Windows-Security-Auditing,4624,Logon,"An account was successfully log ged on." Subject: Security ID: SYSTEM Account Name: WIN-D9CJUS3F2RK\$ Show all 59 lines host = WIN-D9CJUS3F2RK source = import_logs.csv sourcetype = csv
2/9/22 9:37:03.000 AM	Audit Success,02/09/2022 09:37:03,Microsoft-Windows-Security-Auditing,4672,Special Logon,"Special privileges assi gned to new logon." Subject: Security ID: SYSTEM Account Name: SYSTEM Show all 20 lines host = WIN-D9CJUS3F2RK source = import_logs.csv sourcetype = csv
2/9/22 9:37:03.000 AM	Audit Success,02/09/2022 09:37:03,Microsoft-Windows-Security-Auditing,4624,Logon,"An account was successfully log ged on."

By following these steps, you can effectively add and monitor data in Splunk, whether through the forwarder on a Windows computer or by uploading log files directly.