Splunk® Supported Add-ons
Splunk Add-on for Sysmon released

Generated: 11/05/2022 11:54 am

Table of Contents

Overview

Splunk Add-on for Sysmon

Version	3.0.0
Vendor Products	Microsoft Sysmon v13.33
Add-on has a web UI	No. This add-on does not contain any views.

The Splunk Add-on for Sysmon allows a Splunk software administrator to create a Splunk software data input and **CIM**-compliant field extractions for Microsoft Sysmon.

> The Splunk Add-on for Sysmon is not the same as the Splunk Add-on for Microsoft Sysmon, which is a community-supported add-on. The community-supported add-on will remain available, but since the Splunk Add-on for Sysmon contains enhancements to events field mappings and Common Information Model (CIM) changes, you should migrate your Microsoft Sysmon data ingestion from the Splunk Add-on for Microsoft Sysmon to the Splunk Add-on for Sysmon. For information on the differences in the technical support for different Splunkbase app or add-ons, see the Support content topic in the Splunk Developer Guide.

Download the Splunk Add-On for Sysmon from Splunkbase.

For a summary of new features, fixed issues, and known issues, see Release Notes for the Splunk Add-on for Sysmon.

For information about installing and configuring the Splunk Add-on for Sysmon, see Installation and configuration overview for the Splunk Add-on for Sysmon.

See the Splunk Community page for questions related to Splunk Add-on for Sysmon.

Hardware and software requirements for the Splunk Add-on for Sysmon

To install and configure the Splunk Add-on for Sysmon, you must be a member of the admin or sc_admin role.

Microsoft Sysmon setup requirements

To install or uninstall the Sysmon service, you must have local administrator rights on the monitored Windows endpoint platform. There is no dedicated installer or uninstaller for Sysmon. System service and driver installation or removal are performed by a standalone executable with command line switches.

You must prepare and run Sysmon with a customized configuration file that enables proper event capture and filtering. If you do not do this, the expected events are not captured and ingested by the Splunk component, or an overwhelming volume of noisy events may impact Splunk's performance. See Configure your Microsoft Sysmon deployment to collect data for more information.

Splunk platform requirements

Because this add-on runs on the Splunk platform, all of the system requirements apply for the Splunk software that you use to run this add-on.

- For Splunk Enterprise system requirements, see System Requirements in the Splunk Enterprise *Installation Manual*.
- If you are managing on-premises forwarders to get data into Splunk Cloud, see System Requirements in the Splunk Enterprise *Installation Manual*, which includes information about forwarders.

Installation and configuration overview for the Splunk Add-on for Sysmon

Complete the following steps to install and configure this add-on:

1. Configure your Microsoft Sysmon deployment to collect data

   Optionally, configure WEF/WEC support to forward and collect Sysmon events

2. Install your add-on:
   - Install the Splunk Add-on for Sysmon on to your Splunk platform deployment
3. Configure your inputs:
   - Configure inputs for the Splunk Add-on for Sysmon.

> The Splunk Add-on for Microsoft Windows and the Splunk App for Windows Infrastructure are not required for the Splunk Add-on for Sysmon to function.

Installation and Configuration

Configure your Microsoft Sysmon deployment to collect data

Sysmon events are stored in `Applications and Services Logs/Microsoft/Windows/Sysmon/Operational` or on the WEC server, if using WEC, and collected by the Splunk software.

Prepare your Sysmon configuration file based on your security team or SOC needs. The best practice is to start preparing the configuration with the template SwiftOnSecurity/sysmon-config and adjust filtering rules of each event type according to your environment needs, instead of running Sysmon without a custom configuration file. Otherwise, Sysmon will monitor a predefined small subset of events and event types or flood the eventlog and your Splunk platform deployment with unnecessary events.

To learn more about configuration file preparation and adjustment, see:

- Microsoft documentation on Sysmon
- TrustedSec Sysmon Community Guide
- Olaf Hartong's sysmon-modular
- SwiftOnSecurity sysmon-config

WEF/WEC support

Splunk Add-on for Sysmon can be used for Sysmon events forwarded and collected with use of Windows Event Forwarding (https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection and Windows Event Collector (https://docs.microsoft.com/en-us/windows/win32/wec/windows-event-collector) or WEF/WEC for short. WEF/WEC architecture requires careful tuning to work reliably. Use a dedicated collector channel for Sysmon events and name the channel is WEC-Sysmon or something similar.

Hashes generation configuration

Choose one hashing algorithm in Sysmon's general configuration for process and file hash generation. Select the hash type used by your threat intelligence solution, so that processing cycles aren't wasted by checking for the presence of a specific MD5 hash in a field containing a SHA256 hash.

Using `*` or multiple types of hashes in the hash declaration is not recommended due to performance implications and the possibility of false negatives caused by labels in the hash field.

Install the Splunk Add-on for Sysmon

1. Get the Splunk Add-On for Sysmon by downloading it from https://splunkbase.splunk.com/app/5709/ or by browsing to it using the app browser within Splunk Web.
2. Determine where and how to install this add-on in your deployment, using the tables on this page.
3. Perform any prerequisite steps before installing, if required and specified in the tables below.

4. Complete your installation.

If you need step-by-step instructions on how to install an add-on in your specific deployment environment, see the installation walkthroughs section at the bottom of this page for links to installation instructions specific to a single-instance deployment, distributed deployment, or Splunk Cloud.

Distributed deployments

Use the tables below to determine where and how to install this add-on in a distributed deployment of Splunk Enterprise or any deployment for which you are using forwarders to get your data in. Depending on your environment, your preferences, and the requirements of the add-on, you may need to install the add-on in multiple places.

Where to install this add-on

Unless otherwise noted, all supported add-ons can be safely installed to all tiers of a distributed Splunk platform deployment. See Where to install Splunk add-ons in *Splunk Add-ons* for more information.

Install the Splunk Add-on for Sysmon on Windows endpoints where the data should be collected from regardless of the Splunk role the machine possesses.

This table provides a reference for installing this specific add-on to a distributed deployment of the Splunk platform.

Splunk platform instance type	Supported	Required	Actions required / Comments
Search Heads	Yes	Yes	Install this add-on to all search heads where Sysmon knowledge management is required.
Indexers	Yes	Yes	
Heavy Forwarders	Yes	See Comments	This add-on supports forwarders of any type for data collection. The forwarder needs to be installed directly on the monitored Microsoft Windows endpoint or Windows Event Collector for WEF/WEC architecture.
Universal Forwarders	Yes	See Comments	This add-on supports forwarders of any type for data collection. The forwarder needs to be installed directly on the monitored Microsoft Windows endpoint or Windows Event Collector for WEF/WEC architecture.
Splunk Cloud	Yes	See Comments	This product is compatible with Self Service App Install (SSAI). See your Splunk Cloud administrator for more information.

Distributed deployment feature compatibility

This table describes the compatibility of this add-on with Splunk distributed deployment features.

Distributed deployment feature	Supported	Actions required / Comments
Search Head Clusters	Yes	
Indexer Clusters	Yes	

Distributed deployment feature	Supported	Actions required / Comments
Deployment Server	Yes	Supported for deploying the configured add-on to multiple forwarders for local data collection using Windows Event Monitoring.

Installation walkthroughs

The *Splunk Add-Ons* manual includes an Installing add-ons guide that helps you successfully install any Splunk-supported add-on to your Splunk platform.

For a walkthrough of the installation procedure, follow the link that matches your deployment scenario:

- Single-instance Splunk Enterprise
- Distributed Splunk Enterprise
- Splunk Cloud

Configure inputs for the Splunk Add-on for Sysmon

The Splunk Add-on for Sysmon contains:

- WinEventLog://Microsoft-Windows-Sysmon/Operational input, which is enabled by default
- WinEventLog://WEC-Sysmon, which requires enablement for the add-on to work in a WEF/WEC architecture.

- To collect data, install your forwarders directly onto your Microsoft Windows endpoints or Windows Event Collector.
- If you install Splunk forwarders directly on the endpoints, no additional action is required.
- If you install the forwarders on Windows Event Collector:
    1. Go to Settings > Data Inputs > Remote event log collections
    2. Find and enable 'WEC-Sysmon' Event log collection
- Make sure you collect Sysmon events in the WEC-Sysmon log or adjust the stanza name in inputs.conf
- If you forward events from WEC server to its own sysmon channel, disable the WinEventLog://Microsoft-Windows-Sysmon/Operational input to avoid forwarding duplicate logs to Splunk.

.

For more information, see https://docs.splunk.com/Documentation/Splunk/latest/Admin/Inputsconf.

Troubleshooting

Troubleshoot the Splunk Add-on for Sysmon

Troubleshoot the Splunk Add-on for Sysmon with the following troubleshooting tips and best practices.

If your Sysmon service is stopped, Microsoft-Windows-Sysmon/Operational EventLog becomes unavailable. After starting Sysmon again, restart your Splunk forwarders before any new events are fed into Splunk.

Update your running Sysmon configurations with the `-c` command line parameter and updated xml file instead of restarting the service with the `-u` and `-i` parameters. For example, `sysmon -c c:\windows\config.xml`

Troubleshoot your version of Sysmon

On 64-bit platforms, you can use both 32-bit and 64-bit versions of the Sysmon executable. Depending on the version you choose, the `sysmon` or `sysmon64` service name that is created, and `sysmon` or `sysmon64` executable must be referred to in the command line.

Multiple Sysmon executables

More than one Sysmon executable might be present on the system/user `PATH`. When stopping or updating the service, make sure to use the same executable as was used for to start (installing) the Sysmon service or reference the full path to the same executable binary.

Extending the capability of new event types capture

The Sysmon upgrades' configuration file schema may change, extending the capability of new event types capture. Updating the xml configuration file used with previous Sysmon versions with new rules may not allow new event types capture. Review the new file schema when upgrading your Sysmon binary and rebuild your current configuration if necessary.

```
{new_sysmon.exe} -s
```

Reference

Lookups for the Splunk Add-on for Sysmon

The Splunk Add-on for Sysmon has the following lookups that map fields from Sysmon to Common Information Model (CIM)-compliant values in the Splunk software. The lookup files are located in `$SPLUNK_HOME\etc\apps\Splunk_TA_microsoft-sysmon/lookups`

Filename	Description
`microsoft_sysmon_eventcode.csv`	Maps `EventCode` to `EventDescription`. For more information, see the Microsoft Sysmon documentation.
`microsoft_sysmon_record_type.csv`	Maps `record_type` to `record_type_name` (DNS resource record type [RFC6895] [RFC1035]).

Sysmon product comparisons

The following sections describe the differences between versions 10.6.2 of the Splunk Add-on for Microsoft Sysmon and 1.0.1 of the Splunk Add-on for Sysmon:

Field mapping comparison for versions 10.6.2 of the Splunk Add-on for Microsoft Sysmon and 1.0.1 of the Splunk Add-on for Sysmon

Version 1.0.1 of the Splunk Add-on for Sysmon introduces field mapping changes to the XmlWinEventLog sourcetype. See the following table for information in field changes between version 10.6.2 of the Splunk Add-on for Microsoft Sysmon and 1.0.1 of the Splunk Add-on for Sysmon

Source type	EventCode	Fields added	Fields modified	Fields removed	10.6

`XmlWinEventLog`	1	`original_file_name`
		`os`
			`signature`
			`EventDescription`
				`app`
				`cmdline direction dvc hashes session_id user_id`
					Process Create,

`XmlWinEventLog`	2	`action`
		`dest file_modify_time`
			`signature`
			`EventDescription tag::eventtype tag`
				`app`
				`direction dvc session_id user_id`
					File Create Time endpoint filesyste filesystem

`XmlWinEventLog`	3	`action`
		`dvc_ip protocol_version transport_dest_port`
			`signature`
			`protocol dest state EventDescription tag tag::eventtype`
				`dest_host`
				`process_path session_id user_id`
					Network Connec Connect, listenin network, listening

`XmlWinEventLog`	4	`description`
		`dest eventtype service service_name status tag tag::eventtype`
			`signature`
			`EventDescription`
				`direction`
				`dvc parent_process_exec parent_process_name`
					Sysmon Start, Sy

Source type	EventCode	Fields added	Fields modified	Fields removed	10.6
				process_exec process_name user_id	
XmlWinEventLog	5	action dest os process	signature EventDescription	app direction dvc session_id user_id	Process Termina
XmlWinEventLog	6	action dest os process_path service_signature_exists service_signature_verified	signature	direction dvc hashes parent_process_exec parent_process_name process_exec process_name user_id	Driver Load
XmlWinEventLog	7	action dest eventtype os parent_process_exec parent_process_guid parent_process_id parent_process_name parent_process_path service_dll_signature_exists service_dll_signature_verified tag tag::action tag::eventtype	signature process_exec EventDescription process_path process_name	app direction dvc hashes process_guid process_id session_id user_id	Image Load, uns C:\Windows\Sys unsecapp.exe
XmlWinEventLog	8	action dest os parent_process_guid parent_process_id parent_process_path process_guid process_id process_path src_address src_function src_module	signature process_name parent_process_name EventDescription parent_process_exec process_exec	direction dvc user_id	Create Remote T Remote Thread,
XmlWinEventLog	9	action dest os	signature EventDescription	app direction dvc session_id user_id	Raw Access Rea
XmlWinEventLog	10	action dest granted_access os parent_process_guid parent_process_id parent_process_path process_guid process_id process_path	process_exec parent_process_exec EventDescription parent_process_name process_name signature	direction user_id	svchost.exe,, Pro Process Access

Source type	EventCode	Fields added	Fields modified	Fields removed	10.6
XmlWinEventLog	11	action	tag::eventtype tag EventDescription signature	app direction dvc session_id user_id	change endpoint filesystem, File C
XmlWinEventLog	12	registry_hive status	tag::eventtype tag,registry_key_name EventDescription signature	app direction dvc object session_id user_id	change endpoint registry, Paramet or deleted, Regis
XmlWinEventLog	13	RegistryValueData registry_hive registry_value_data registry_value_type status	tag::eventtype tag registry_key_name EventDescription registry_value_name signature	app direction object session_id user_id	change endpoint registry, SecureT QWORD (0x01d Registry value se
XmlWinEventLog	14	action registry_hive status	tag::eventtype tag registry_key_name EventDescription signature	app direction dvc object session_id user_id	change endpoint registry, test1, R Registry object r
XmlWinEventLog	15	action dest file_hash http_referrer http_referrer_domain os uri_path url url_domain	file_path EventDescription file_name signature	app direction dvc session_id user_id	C:\Users\splunke Build 3211 x64 S File stream creat x64 Setup.exe:Z created
XmlWinEventLog	16	description dest eventtype process_id service service_name status tag tag::eventtype	EventDescription signature	direction dvc parent_process_exec parent_process_name process_exec process_name user_id	Sysmon Configu Configuration Ch
XmlWinEventLog	17	action dest os pipe_name	EventDescription signature	app direction dvc session_id user_id	Pipe Created, Pi
XmlWinEventLog	18	action dest os pipe_name	EventDescription signature	app direction dvc session_id user_id	Pipe Connected,
XmlWinEventLog	19	action change_type dest result src status user_name	EventDescription signature	direction parent_process_exec parent_process_name process_exec	WmiEventFilter a WmiEventFilter a

Source type	EventCode	Fields added	Fields modified	Fields removed	10.6
				process_name user_id	
XmlWinEventLog	20	action change_type dest object object_path src status user_name	EventDescription signature	direction parent_process_exec parent_process_name process_exec process_name user_id	WmiEventConsu WmiEventConsu
XmlWinEventLog	21	action change_type dest object object_attrs object_path result src status user_name	EventDescription signature	direction parent_process_exec parent_process_name process_exec process_name user_id	WmiEventConsu detected, WmiEv activity detected
XmlWinEventLog	22	answer_count query_count src	EventDescription signature	app direction dvc parent_process_exec parent_process_name process_id process_path record session_id user_id	DNS Query, DNS
XmlWinEventLog	23	action dest eventtype file_hash file_modify_time object_category tag tag::eventtype tag::object_category	process_exec EventDescription process_name signature	app direction dvc hashes parent_process_exec parent_process_name process_hash session_id user_id	,Unknown,, Unkn
XmlWinEventLog	24	SrcHost action dest eventtype os src_host tag tag::eventtype user	process_exec EventDescription process_name signature	app direction hashes parent_process_exec parent_process_name session_id user_id	,Unknown,, Unkn
XmlWinEventLog	25	action dest eventtype os result tag tag::eventtype	EventDescription signature	app direction dvc parent_process_exec parent_process_name process_exec process_name session_id user_id	Unknown, Unkno

Source type	EventCode	Fields added	Fields modified	Fields removed	10.6
XmlWinEventLog	26	action dest eventtype file_access_time file_hash file_modify_time object_category tag tag::eventtype tag::object_category	process_exec EventDescription process_name signature	app direction hashes parent_process_exec parent_process_name process_hash session_id user_id	, Unknown,, Unk
XmlWinEventLog	255	description dest process_id result service service_name status	tag::eventtype eventtype tag	direction parent_process_exec parent_process_name process_exec process_name user_id	

CIM model comparison for versions 10.6.2 of the Splunk Add-on for Microsoft Sysmon and 1.0.1 of the Splunk Add-on for Sysmon

Source	EventID	Previous CIM model	New CIM model
XmlWinEventLog	1, 10, 15, 17, 18, 19, 20, 21, 22, 5, 6, 8, 9		
XmlWinEventLog	11, 12, 13, 14, 2	Change	
XmlWinEventLog	3	Endpoint	
XmlWinEventLog	16, 255, 4		Endpoint
XmlWinEventLog	23, 26		Endpoint
XmlWinEventLog	24, 25, 7		Endpoint

Source types for the Splunk Add-on for Sysmon

The Splunk Add-on for Sysmon collects data from Sysmon's dedicated Windows Event log.

Source type	Description	CIM data models
XmlWinEventLog	Windows Event Log data for Sysmon provided by WinEventLog in XML or standard format.	Endpoint Network Resolution (DNS) Network Traffic Change

Release notes

Release notes for the Splunk Add-on for Sysmon

Version 3.0.0 of the Splunk Add-on for Sysmon was released on May 30, 2022.

Compatibility

Version 3.0.0 of the Splunk Add-on for Sysmon is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	8.1, 8.2 and later
CIM	5.0 and later
Supported OS for data collection	Platform independent
Vendor products	Microsoft Sysmon version 13.33

Splunk Add-on for Sysmon field mapping changes

See the following sections for information on the differences between versions 2.0.0 of the Splunk Add-on for Microsoft Sysmon and 3.0.0 of the Splunk Add-on for Sysmon

Source-type	EventID	Fields added	Fields removed
`['xmlwineventlog']`	8, 25, 22, 5, 15, 14, 11, 4, 2, 1, 7, 16, 6, 18, 23, 9, 12, 17	dvc	

The dvc field is now defined for all Sysmon events. The field value shows where an event was generated The host field is mapped at search time to show the machine that generated the event. This is consistent with the Windows TA.

New features

Version 3.0.0 of the Splunk Add-on for Sysmon contains the following new and changed features: Support for WEF/WEC architectureWEF/WEC events can be found by adding to search string: _sourcetype=XmlWinEventLog:WEC-Sysmon If direct Sysmon events have to be found, the following search string can be used: _sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational

Fixed issues

Version 3.0.0 of the Splunk Add-on for Sysmon fixes the following, if any, issues.

Known issues

Version 3.0.0 of the Splunk Add-on for Sysmon has the following, if any, known issues.

Third-party software attributions

Version 3.0.0 of the Splunk Add-on for Sysmon does not incorporate any third-party software or libraries.

Release history for the Splunk Add-on for Sysmon

Latest release

The latest version of the Splunk Add-on for Sysmon is version 3.0.0. Please see Release notes for the Splunk Add-on for Sysmon for the release notes of this latest version.

Version 2.0.0

Version 2.0.0 of the Splunk Add-on for Sysmon was released in February 2022.

Compatibility

Version 2.0.0 of the Splunk Add-on for Sysmon is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	8.1, 8.2 and later
CIM	5.0 and later
Supported OS for data collection	Platform independent
Vendor products	Microsoft Sysmon version 13.30

Splunk Add-on for Sysmon field mapping changes

See the following sections for information on the differences between versions 1.0.1 of the Splunk Add-on for Microsoft Sysmon and 2.0.0 of the Splunk Add-on for Sysmon

Source-type	EventID	Fields added	Fields removed
`['xmlwineventlog']`	8, 10	user	
`['xmlwineventlog']`	20	DestinationNoQuotes	
`['xmlwineventlog']`	21	ConsumerNoQuotes, FilterNoQuotes	

New features

Sysmon 13.30 (schema 4.81) introduces user information for number of event IDs. The user information is in the Sysmon User field in most cases. However, in event ID 8 (https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon#event-id-8-createremotethread) and event ID 10 (https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon#event-id-10-processaccess) SourceUser and TargetUser fields are introduced.

Version 2.0.0 of the Splunk Add-on for Sysmon contains the following new and changed features: CIM user field is mapped from Sysmon User field for event ID 24. This is breaking change as it was extracted from the Sysmon ClientInfo field before. As inconsistencies were observed during testing, if the SourceUser and TargetUser field values are equal, the value is mapped to the user CIM field. The value for registry_key_name CIM field is represented as a path that is not in line with key names definition (https://docs.microsoft.com/en-us/windows/win32/sysinfo/structure-of-the-registry). Unfortunately, using data exposed by Sysmon, it is not possible to reliably determine key names. If SourceUser and TargetUser field values are not equal, due to known Sysmon issue (https://docs.microsoft.com/en-us/answers/questions/692991/sysmon-1330-sourceuser-and-targetuser-values-diffe.html), CIM user value cannot be reliably determined.

Fixed issues

Version 2.0.0 of the Splunk Add-on for Sysmon fixes the following, if any, issues.

Known issues

Version 2.0.0 of the Splunk Add-on for Sysmon has the following, if any, known issues.

Third-party software attributions

Version 2.0.0 of the Splunk Add-on for Sysmon does not incorporate any third-party software or libraries.

Version 1.0.0

The Splunk Add-on for Sysmon is different from the community-supported Splunk Add-on for Microsoft Sysmon. The community-supported add-on will continue to exist, but because the Splunk-supported add-on contains enhancements to events field mappings and Common Information Model (CIM) changes, the best practice is to migrate your Microsoft Sysmon data ingestion from the community-supported add-on to the Splunk-supported add-on. For information on the differences in the technical support for different Splunkbase app or add-ons, see the Support content topic in the Splunk Developer Guide.