Splunk® Supported Add-ons
Splunk Add-on for Microsoft Windows released

Generated: 5/24/2022 6:20 pm

Copyright (c) 2022 Splunk Inc. All Rights Reserved

Table of Contents

Overview

About the Splunk Add-on for Windows

Version	8.5.0
Vendor products and components	Windows 8.1 Windows 10 Windows 11 Windows Server 2012/2012 R2 Windows Server 2016 Windows Server 2019 Windows Server 2022 Microsoft Active Directory Microsoft Windows DNS Server Windows Security Windows Performance Windows DHCP Windows File Server
Add-on has a web UI	No. This add-on does not contain any views.

The Splunk Add-on for Windows allows a Splunk software administrator to collect:

- CPU, disk, I/O, memory, log, configuration, and user data with data inputs.
- Active Directory and Domain Name Server debug logs from Windows hosts that act as domain controllers for a supported version of a Windows Server. You must configure Active Directory audit policy since Active Directory does not log certain events by default.
- Domain Name Server debug logs from Windows hosts that run a Windows DNS Server. Windows DNS Server does not log certain events by default, and you must enable debug logging.

This add-on provides the inputs and **CIM**-compatible knowledge to use with other Splunk apps, such as Splunk Enterprise Security, the Splunk App for PCI Compliance, the Splunk ITSI Operating System Module, the Splunk App for Windows Infrastructure, and the Splunk App for Microsoft Exchange.

Download the Splunk Add-on for Windows from Splunkbase.

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

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

See Questions related to Splunk Add-on for Windows on the Splunk Community page.

Source types for the Splunk Add-on for Windows

The Splunk Add-on for Windows provides Common Information Model mappings, the index-time and search-time knowledge for Windows events, metadata, user and group information, collaboration data, and tasks in the following formats.

Source type	Description	CIM data models
`ActiveDirectory`	Active Directory related information	n/a
`DhcpSrvLog`	Microsoft DHCP Server Log information	Network Sessions
`Perfmon:CPU` `PerfmonMk:CPU`	CPU usage statistics provided by the Performance Monitor input	Application State, Performance
`Perfmon:LogicalDisk` `PerfmonMk:LogicalDisk`	Information about logical disks on the system provided by the Performance Monitor input in single or multikv mode.	Performance
`Perfmon:Memory` `PerfmonMk:Memory`	Memory statistics provided by the Performance Monitor input in single or multikv mode	Performance
`Perfmon:Network` `PerfmonMk:Network`	Network statistics provided by the Performance Monitor input in single or multikv mode	Performance
`Perfmon:PhysicalDisk` `PerfmonMk:PhysicalDisk`	Information about physical disks on the system provided by the Performance Monitor input in single or multikv mode	n/a
`Perfmon:Process` `PerfmonMk:Process`	Information about process running on the system provided by the Performance Monitor input in single or multikv mode	Application State, Performance, Endpoint
`Perfmon:ProcessorInformation` `PerfmonMk:ProcessorInformation`	Statistics related to processor state and performance	Application State, Inventory, Endpoint, Performance, Vulnerabilities
`Perfmon:System` `PerfmonMk:System`	System Information provided by the Performance Monitor input in single or multikv mode	Application State, Performance
`Script:InstalledApps`	List of installed applications	n/a
`Script:ListeningPorts`	List of network ports that listen for traffic	Application State, Endpoint
`Script:NetworkConfiguration`	To get local IP configurations	n/a
`Script:TimesyncConfiguration`	Information on time synchronization service configuration.	n/a
`Script:TimesyncStatus`	Information on time synchronization status.	Performance
`WindowsUpdateLog`	Windows Update log file	Updates
`WinHostMon`	Windows host monitoring log	Inventory, Performance, Endpoint
`WinNetMon`	Network related information	n/a
`WinPrintMon`	Windows Printer related changes	n/a
`WinRegistry`	Windows Registry changes	Change Analysis, Endpoint, Change
`WMI:ComputerSystem`	Computer system information provided by WMI	Performance
`WMI:CPUTime`	CPU usage time provided by WMI	Application State, Performance
`WMI:FreeDiskSpace`	Free Disk Space provided by WMI	Application State, Performance
`WMI:InstalledUpdates`	List of installed updates/packages provided by WMI	Updates
`WMI:LocalNetwork`	Network statistics provided by WMI	Performance
`WMI:LocalPhysicalDisk`	Physical Disk information provided by WMI	n/a
`WMI:LogicalDisk`	Information about logical disks on the system, provided by WMI	Performance

Source type	Description	CIM data models
`WMI:LocalProcesses`	Information on processes running locally, provided by WMI	Application State, Endpoint
`WMI:Memory`	Memory information provided by WMI	Application State, Performance
`WMI:ScheduledJobs`	Information on Scheduled Jobs provided by WMI	n/a
`WMI:Service`	Information on services running locally, provided by WMI	Application State, Endpoint
`WMI:Uptime`	Information on system uptime, provided by WMI	Application State, Performance
`WMI:UserAccounts`	Information on configured user accounts, provided by WMI	Application State, Inventory
`WMI:Version`	Information on the system version, provided by WMI	Application State, Inventory
`WMI:WinEventLog:*`	Windows Event Log data for Application, System and Security - WMI	Application State, Authentication, Change Analysis, Performance, Updates, Vulnerabilities, Endpoint, Event Signatures, Change
`MSAD:NT6:Health`	Active Directory health information	n/a
`MSAD:NT6:SiteInfo`	Active Directory site information	n/a
`MSAD:NT6:Replication`	Active Directory site replication information	n/a
`MSAD:NT6:Netlogon`	Active Directory login statistics	n/a
`MSAD:SubnetAffinity`	Active Directory Domain Subnet Affinity problem information	n/a
`WinEventLog` `XmlWinEventLog`	Windows Event Log data for Application, System, Security, DFS Replication, Directory Service, File Replication Service, Key Management Service, DNS Server provided by WinEventLog in XML or standard format.	Application State, Authentication, Change Analysis, Performance, Updates, Vulnerabilities, Endpoint, Event Signatures, Change
`Perfmon:Processor` `PerfmonMk:Processor`	n/a	
`Perfmon:Network_Interface` `PerfmonMk:Network_Interface`	Network_Interface statistics provided by the Performance Monitor input in single or multikv mode	n/a
`Perfmon:DFS_Replicated_Folders` `PerfmonMk:DFS_Replicated_Folders`	Information about dfs replicated folders on the system provided by the Performance Monitor input in single or multikv mode.	n/a
`Perfmon:NTDS` `PerfmonMk:NTDS`	Information about NTDS on the system provided by the Performance Monitor input in single or multikv mode.	n/a
`Perfmon:DNS` `PerfmonMk:DNS`	Information about DNS on the system provided by the Performance Monitor input in single or multikv mode.	n/a
`MSAD:NT6:DNS-Zone-Information`	Information about DNS zones	n/a
`MSAD:NT6:DNS-Health`	Information about the health of DNS servers	n/a
`MSAD:NT6:DNS`	DNS server activity statistics	n/a

In versions 5.0.0 and later of the Splunk add-on for Windows, the source type `WinEventLog` is subdivided into `WinEventLog` for Classic channels, and `XmlWinEventLog` for XML channels. See Source and sourcetype changes for WinEventLog data.

Source types for backward compatibility

The Splunk Add-on for Windows includes the following source types for backward compatibility.

Sourcetype	Description	CIM data model(s)
`Perfmon:CPUTime`	CPU usage statistics provided by the Performance Monitor input in single or multikv mode. Included for backward compatibility.	Performance
`Perfmon:FreeDiskSpace`	Free Disk Space statistics provided by the Performance Monitor input. Included for backward compatibility.	Performance
`Perfmon:LocalNetwork`	Free Disk Space statistics provided by the Performance Monitor input. Included for backward compatibility.	Performance

Release notes for the Splunk Add-on for Windows

Version 8.5.0 of the Splunk Add-on for Windows was released on April 21, 2022.

The Splunk Add-on for Windows DNS version 1.0.1 and the Splunk Add-on for Windows Active Directory version 1.0.0 are not supported when installed alongside the Splunk Add-on for Windows versions 6.0.0 and higher. The Splunk Add-on for Windows versions 6.0.0 and higher includes the Splunk Add-on for Windows DNS and the Splunk Add-on for Microsoft Active Directory.

Compatibility

Version 8.5.0 of the Splunk Add-on for Windows is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	8.1.x, 8.2.x
CIM	4.15 and later
Platform	Windows
Vendor Products	Windows Server 2022, Windows 11, Windows Server 2019, Windows 8.1, Windows 10, Windows Server 2012/2012 R2, Windows Server 2016, Microsoft Active Directory, Microsoft Windows DNS Server

New or changed features

Version 8.5.0 of the Splunk Add-on for Windows has the following new or changed features:

- CIM enhancements for these Event Codes: 104, 1102, 4624, 4625, 4634, 4698, 4700, 4701, 4702, 4719, 720, 4732, 4740, 4800, 4801

(To review field extraction changes, please refer to Field Changes Section)

- Removed the incorrect `Endpoint:Filesystem` CIM tags from the **wineventlog_windows** event type.
- Removed the `fs_notification` event type and `fs_notification` source type extractions as Splunk no longer supports this source type.

Fixes

- Fixed the **user** field extraction issue for Event Codes 4728, 4729, 4732 when the distinguished name (DN) contains "Lastname, Firstname".

Notes:

- If the `Member:Security_ID` value uses the enriched "DOMAIN\UserName" format then the user field would be extracted as UserName.
- If the `Member:Security_ID` value uses the traditional Windows SID (S-1234-etc) format then the user field will be extracted from the first RDN section of the Member:Account Name string (which gets logged as an LDAP DN format).
- If the `Member:Security_ID` value uses the traditional Windows SID (S-1234-etc) format and the first RDN section of `Member:Account Name` as `CN=Lastname\, Firstname, OU=Users, DC=CONTOSO, DC=com`, then it can be in the `lastname,firstname` format, in which case user field will not be extracted.

Field Changes

Source - WinEventLog:System field mapping changes

Source-type	EventCode	Fields added	Fields removed
['WinEventLog']	104	object, user_name, object_category, action, result, status, change_type	

Source - XmlWinEventLog:System field mapping changes

Source-type	EventCode	Fields added	Fields removed
['WinEventLog']	104	user, object, user_name, object_category, user_data_channel, action, result, status, change_type	

Source - WinEventLog:Security field mapping changes

Source-type	EventCode	Fields added	Fields removed
['WinEventLog']	1102	result, object, user_name	
['WinEventLog']	4624	authentication_method	
['WinEventLog']	4625	authentication_method	
['WinEventLog']	4634	object_id, change_type, object, user_name, object_category, object_attrs, result, src_user, src_user_name	
['WinEventLog']	4698	object, user_name, TaskContent, object_category, object_attrs, result, change_type	
['WinEventLog']	4700	object, user_name, TaskContent, object_category, object_attrs, result, change_type	
['WinEventLog']	4701	object, user_name, TaskContent, object_category, object_attrs, result, change_type	

Source-type	EventCode	Fields added	Fields removed
['WinEventLog']	4702	object, user_name, TaskNewContent, object_category, object_attrs, result, change_type	
['WinEventLog']	4719	result, object, user_name	
['WinEventLog']	4720	src_user_name, object_id, object, user_name, object_attrs, New_Account_Account_Name, New_Account_Domain, New_Account_Security_ID	
['WinEventLog']	4732	src_user_name, object_id, Member_Security_ID, object, user_name, Member_Account_Name	
['WinEventLog']	4740	src_user_name, object_id, Account_Locked_Out_Security_ID, Account_Locked_Out_Name, object, user_name, object_attrs	
['WinEventLog']	4800	change_type, object, user_name, object_category, object_attrs, result, src_user, src_user_name	
['WinEventLog']	4801	change_type, object, user_name, object_category, object_attrs, result, src_user, src_user_name	

Source - XmlWinEventLog:Security field mapping changes

Source-type	EventCode	Fields added	Fields removed
['XmlWinEventLog']	1102	result, object, user, user_name	
['XmlWinEventLog']	4624	authentication_method	
['XmlWinEventLog']	4625	authentication_method	
['XmlWinEventLog']	4634	object_id, change_type, object, user_name, object_category, object_attrs, result, src_user, src_user_name, src_nt_domain	
['XmlWinEventLog']	4698	user, object, user_name, object_category, object_attrs, result, change_type	
['XmlWinEventLog']	4700	user, object, user_name, object_category, object_attrs, result, change_type	
['XmlWinEventLog']	4701	user, object, user_name, object_category, object_attrs, result, change_type	
['XmlWinEventLog']	4702	user, object, user_name, object_category, object_attrs, result, change_type	
['XmlWinEventLog']	4719	result, object, user, user_name	
['XmlWinEventLog']	4720	src_user_name, object_id, object, user_name, object_attrs	
['XmlWinEventLog']	4732	src_user_name, object_id, object, user_name, object_attrs	
['XmlWinEventLog']	4740	src_user_name, object, user_name, object_attrs	
['XmlWinEventLog']	4800	change_type, object, user_name, object_category, object_attrs, result, src_user, src_user_name, src_nt_domain	
['XmlWinEventLog']	4801	change_type, object, user_name, object_category, object_attrs, result, src_user, src_user_name, src_nt_domain	

Fixed Issues

Version 8.5.0 of the Splunk Add-on for Windows fixes the following issues:

Known Issues

Version 8.5.0 of the Splunk Add-on for Windows contains the following known issues. If no issues appear below, no issues have yet been reported:

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

Here are the hardware and software requirements for the Splunk Add-on for Windows:

Splunk admin requirements

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

Hardware and operating system requirements

The Splunk Add-on for Windows installs onto any type of Splunk Enterprise instance. On universal forwarders, you must configure the add-on with configuration files.

The add-on installs on Splunk Enterprise instances that run on many current versions of Windows, including:

- Windows 8.1
- Windows 10
- Windows 11
- Windows Server 2012/2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

The add-on does not support:

- Windows 8
- Windows Server 2008 R2
- Windows 7
- Windows 95/98/Me
- Windows NT Workstation/Server 3.1/3.5/4.0
- Windows Server 2008
- Windows 2000 Workstation/Server
- Windows XP
- Windows Vista

For details about supported versions of Windows for Splunk, see System requirements in the Splunk Enterprise *Installation Manual*.

Splunk platform requirements

Because this add-on runs on the Splunk platform, all of the system requirements apply to 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 plan to run this add-on entirely in Splunk Cloud, there are no additional Splunk platform requirements.
- 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 Windows

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

1. Upgrade the Splunk Add-on for Windows or Install the Splunk Add-on for Windows.
2. Configure the Splunk Add-on for Windows.
3. (Optional) Deploy the Splunk Add-on for Windows with Forwarder Management].[[Category:V:AddOns:released]

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

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

1. Upgrade the Splunk Add-on for Windows or Install the Splunk Add-on for Windows.
2. Configure the Splunk Add-on for Windows.
3. (Optional) Deploy the Splunk Add-on for Windows with Forwarder Management.

Release history for the Splunk Add-on for Windows

The latest version of the Splunk Add-on for Windows is version 8.5.0. See Release notes for the Splunk Add-on for Windows.

Version 8.4.0

Version 8.4.0 of the Splunk Add-on for Windows was released on February 1, 2022.

The Splunk Add-on for Windows DNS version 1.0.1 and the Splunk Add-on for Windows Active Directory version 1.0.0 are not supported when installed alongside the Splunk Add-on for Windows versions 6.0.0 and higher. The Splunk Add-on for Windows versions 6.0.0 and higher includes the Splunk Add-on for Windows DNS and the Splunk Add-on for Microsoft Active Directory.

Compatibility

Version 8.4.0 of the Splunk Add-on for Windows is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	8.1.x, 8.2.x
CIM	4.15 and later

Platform	Windows
Vendor Products	Windows Server 2022, Windows 11, Windows Server 2019, Windows 8.1, Windows 10, Windows Server 2012/2012 R2, Windows Server 2016, Microsoft Active Directory, Microsoft Windows DNS Server

New or changed features

Version 8.4.0 of the Splunk Add-on for Windows has the following new or changed features:

Features

- Enhanced "win_listening_ports.bat" input to get the process name associated with the listening port.
- Added 'storage_free', 'storage', 'storage_used', and 'storage_used_percent' field extractions for "PerfmonMk:LogicalDisk" sourcetype.
- Added 'user_type'=computer field extraction for the EventCodes 4741, 4742, and 4743.
- Added 'dest' and 'resource_type' field extractions for the "Script:TimesyncStatus" sourcetype.
- Introduced a new eventtype 'windows_security_change_account' (with tags: 'account', 'change' and CIM datamodel: Change:Account_Management) which will only apply to Windows Event Codes: 4703, 4704, 4705, 4722, 4723, 4724, 4725, 4726, 4738, 4767, and 4781 falling under source="WinEventLog:Security" OR source="XmlWinEventLog:Security". Also enhanced the CIM mappings for these Event Codes. (To review field extraction changes, please refer to "Field Changes" Section)
- Excluded Event Codes: 4703, 4704, 4705, 4722, 4723, 4724, 4725, 4726, 4738, 4767, 4781 from 'wineventlog_windows' eventtype to remove the incorrect Endpoint:Filesystem CIM tag.
- Added support of the latest DHCP event format and enhanced the CIM mapping of the "DhcpSrvLog" sourcetype.

CIM Data Model	DHCP Event IDs before v8.4.0	DHCP Event IDs after v8.4.0
`['Network Sessions:DHCP']`	All the DHCP events (sourcetype=DhcpSrvLog)	10,11,12,13,14,15,16,17,18
`['Network Sessions:Session_Start']`	10,11,13	10,11
`['Network Sessions:Session_End']`	12,16,17	12,16,17,18

Notes:

- Removed the tags (dhcp network session) from 'DhcpSrvLog' eventtype and created new 'DhcpSrvLog_dhcp' eventtype which covers Event Codes mapped with NetworkSession:dhcp DM.
- The header for latest supported event format is [ID,Date,Time,Description,IP Address,Host Name,MAC Address,User Name, TransactionID, QResult,Probationtime, CorrelationID,Dhcid,VendorClass(Hex),VendorClass(ASCII),UserClass(Hex),UserClass(ASCII),RelayAgentInformation,Dn]

Fixes

- Removed invalid 'object' field extraction (sourcetype AS object) from all security events. (Note: Existing users relying on the 'object' field can directly use the 'sourcetype' field.)
- Fixed the 'Name' field extraction issue for "WMI:LocalProcesses" sourcetype when Name contains the space character.

Field Changes

Source - WinEventLog:Security field mapping changes

Source-type	EventCode	Fields added	Fields removed
['WinEventLog']	4703	change_type, Subject_Security_ID, Subject_Account_Domain, src_user_name, Subject_Logon_ID, Target_Security_ID, Subject_Account_Name, object_category, Target_Logon_ID, object_attrs, Target_Account_Name, user_name, user_group, Target_Account_Domain, result, object_id	
['WinEventLog']	4704	change_type, Subject_Security_ID, Subject_Account_Domain, src_user_name, Subject_Logon_ID, Subject_Account_Name, object_category, Target_Account_Name, object_attrs, user_name, user_group, result	
['WinEventLog']	4705	change_type, Subject_Security_ID, Subject_Account_Domain, src_user_name, Subject_Logon_ID, Subject_Account_Name, object_category, Target_Account_Name, object_attrs, user_name, user_group, result	
['WinEventLog']	4722	Subject_Account_Domain, src_user_name, Subject_Logon_ID, Target_Security_ID, Subject_Account_Name, Target_Account_Name, user_name, object_attrs, Target_Account_Domain, user_group, Subject_Security_ID, object_id	
['WinEventLog']	4723	Subject_Security_ID, Subject_Account_Domain, src_user_name, Subject_Logon_ID, Target_Security_ID, Subject_Account_Name, Target_Account_Name, user_name, Target_Account_Domain, user_group, result, object_id	
['WinEventLog']	4724	Subject_Security_ID, Subject_Account_Domain, src_user_name, Subject_Logon_ID, Target_Security_ID, Subject_Account_Name, Target_Account_Name, user_name, Target_Account_Domain, user_group, result, object_id	
['WinEventLog']	4725	Subject_Account_Domain, src_user_name, Subject_Logon_ID, Target_Security_ID, Subject_Account_Name, Target_Account_Name, user_name, object_attrs, Target_Account_Domain, user_group, Subject_Security_ID, object_id	
['WinEventLog']	4726	Subject_Account_Domain, src_user_name, Subject_Logon_ID, Target_Security_ID, Subject_Account_Name, Target_Account_Name, user_name, object_attrs, Target_Account_Domain, user_group, Subject_Security_ID, object_id	
['WinEventLog']	4738	Subject_Account_Domain, src_user_name, Subject_Logon_ID, Target_Security_ID, Subject_Account_Name, Target_Account_Name, user_name, object_attrs, Target_Account_Domain, user_group, Subject_Security_ID, object_id	
['WinEventLog']	4767	Subject_Account_Domain, src_user_name, Subject_Logon_ID, Target_Security_ID, Subject_Account_Name, Target_Account_Name, user_name, object_attrs, Target_Account_Domain, user_group, Subject_Security_ID, object_id	
['WinEventLog']	4781	Target_Old_Account_Name, src_user, Target_New_Account_Name, Subject_Account_Domain, src_user_name, Subject_Logon_ID, Target_Security_ID, Subject_Account_Name, user_name, Target_Account_Domain, Subject_Security_ID, object_id	

Source - XmlWinEventLog:Security field mapping changes

Source-type	EventCode	Fields added	Fields removed
['XmlWinEventLog']	4703	result, user_name, object_attrs, object_category, object_id, src_user_name, change_type	
['XmlWinEventLog']	4704	result, object_attrs, object_id, object_category, src_user_name, change_type	

Source-type	EventCode	Fields added	Fields removed
['XmlWinEventLog']	4705	result, object_attrs, object_id, object_category, src_user_name, change_type	
['XmlWinEventLog']	4722	user_name, object_attrs, src_user_name, object_id	
['XmlWinEventLog']	4723	result, user_name, src_user_name, object_id	
['XmlWinEventLog']	4724	result, user_name, src_user_name, object_id	
['XmlWinEventLog']	4725	user_name, object_attrs, src_user_name, object_id	
['XmlWinEventLog']	4726	user_name, object_attrs, src_user_name, object_id	
['XmlWinEventLog']	4738	user_name, object_attrs, src_user_name, object_id	
['XmlWinEventLog']	4767	user_name, object_attrs, src_user_name, object_id	
['XmlWinEventLog']	4781	user, user_name, src_user_name, object_id	

Fixed Issues

Version 8.4.0 of the Splunk Add-on for Windows fixes the following issues:

Known Issues

Version 8.4.0 of the Splunk Add-on for Windows contains the following known issues. If no issues appear below, no issues have yet been reported:

Version 8.3.0

Version 8.3.0 of the Splunk Add-on for Windows was released on December 8, 2021.

The Splunk Add-on for Windows 5.0.0 introduced breaking changes. If you are upgrading from a version of the Splunk Add-on for Windows that is lower than 5.0.0, you must follow the steps outlined in Upgrade the Splunk Add-on for Windows. Failure to do so can result in data loss.

The Splunk Add-on for Windows DNS version 1.0.1 and the Splunk Add-on for Windows Active Directory version 1.0.0 are not supported when installed alongside the Splunk Add-on for Windows versions 6.0.0 and higher. The Splunk Add-on for Windows versions 6.0.0 and higher includes the Splunk Add-on for Windows DNS and the Splunk Add-on for Microsoft Active Directory.

Compatibility

Version 8.3.0 of the Splunk Add-on for Windows is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	8.1.x, 8.2.x
CIM	4.15 and later
Platform	Windows
Vendor Products	Windows Server 2022, Windows 11, Windows Server 2019, Windows 8.1, Windows 10, Windows Server 2012/2012 R2, Windows Server 2016, Microsoft Active Directory, Microsoft Windows DNS Server

New or changed features

Version 8.3.0 of the Splunk Add-on for Windows has the following new or changed features:

Features

- Support for Windows Server 2022 and Windows 11

Fixed Issues

Version 8.3.0 of the Splunk Add-on for Windows fixes the following issues:

Known Issues

Version 8.3.0 of the Splunk Add-on for Windows contains the following known issues. If no issues appear below, no issues have yet been reported:

Installation

Install the Splunk Add-on for Windows

Install the Splunk Add-on for Windows:

1. Determine where and how to install this add-on in your deployment, using the tables on this page.
2. Perform any prerequisite steps before installing, if required and specified in the tables on this page.
3. 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.

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

Splunk instance type	Supported	Required	Comments
Search Heads	Yes	Yes	Install this add-on to all search heads where Windows knowledge management is required.
Indexers	Yes	Conditional	Not required if you use heavy forwarders to collect data. Required if you use universal forwarders to collect data.
Heavy Forwarders	Yes	See comments	This add-on supports forwarders of any type for data collection. The host must run on a supported version of Windows.
Universal Forwarders	Yes	See comments	

Distributed deployment feature compatibility

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

Distributed deployment feature	Supported	Comments
Search Head Clusters	Yes	You can install this add-on on a search head cluster for all search-time functionality, but configure inputs on forwarders to avoid duplicate data collection. Before you install this add-on to a cluster, make the following changes to the add-on package: Remove the `inputs.conf` file.

Distributed deployment feature	Supported	Comments
Indexer Clusters	Yes	To get data from an indexer cluster member, install the add-on into that member.
Deployment Server	Yes	Supported for deploying the configured add-on to multiple nodes.

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

Install the Splunk Add-on for Windows with Forwarder Management

If you have a deployment with many universal forwarders and want to deploy the Splunk Add-on for Windows to them, use the Splunk Enterprise Forwarder Management interface to distribute the add-on to those forwarders.

Deploying the Splunk Add-on for Windows with Forwarder Management is a different process than deploying the add-on manually. In this scenario, you download and configure the add-on first, then place it into a Splunk Enterprise instance that has the Forwarder Management capability activated. Then, you set up a server class that tells Forwarder Management to deploy the add-on to available clients. Finally, you configure the forwarders as deployment clients of the Forwarder Management instance.

Prerequisites

Before you can distribute apps and add-ons using Forwarder Management, you must complete the following steps:

- Download and configure the Splunk Add-on for Windows. See Configure the Splunk Add-on for Windows.
- Place the configured add-on into a full Splunk Enterprise instance that you have designated as a deployment server/Forwarder Management instance (All Splunk Enterprise instances have this capability enabled by default).
- Configure the universal forwarders in your deployment to be deployment clients of this Splunk Enterprise instance.
- Create a server class that tells Forwarder Management to send the add-on to all Windows universal forwarders in the deployment.

Download, configure, and install the Splunk Add-on for Windows

To use Forwarder Management, you must have at least one app or add-on available to push to forwarders. In this scenario, the add-on is the Splunk Add-on for Windows.

1. Download the Splunk Add-on for Windows.
2. Unarchive the downloaded file into an accessible location.
3. Configure the Splunk Add-on for Windows. Enable the input stanzas for the Windows data that you want the add-on to collect.

4. After enabling input stanzas, copy the Splunk Add-on for Windows folder to `%SPLUNK_HOME%\etc\deployment-apps` on the deployment server (the Splunk Enterprise instance that runs Forwarder Management.)
5. Restart Splunk Enterprise on the deployment server.
6. Write down the host name or IP address and management port of the deployment server. You need it later to configure deployment clients.

Set up universal forwarders to be deployment clients

Before you can deploy add-ons and configurations to forwarders, they must first be set up as deployment clients to the Forwarder Management instance. You can do this either when you install the forwarders, or at any time after you install them.

During forwarder installation process

On Windows hosts, the universal forwarder installer lets you specify a deployment server during the installation process. See Install a Windows universal forwarder from an installer in the *Universal Forwarder* manual.

When you reach the **Deployment server** pane during installation, specify the IP address or host name and management port of the deployment server instance.

Complete your installation, and the forwarder should then appear in the Forwarder Management page on the Forwarder Management instance.

On forwarders you have already installed

You can either use the CLI or edit a configuration file to set the deployment server on a universal forwarder. For more information on configuring a deployment server, see Configure deployment clients in the Splunk Enterprise *Updating Instances Manual*.

1. (Optional) If you have already set up a forwarder, use the CLI to configure it as a deployment client:

```
> .\splunk set deploy-poll <IP address/hostname of Forwarder Management server>:<port>
```

2. (Optional) On the universal forwarder, edit `deploymentclient.conf` in `%SPLUNK_HOME%\etc\system\local` and add the following text to the file:

```
[deployment-client]

[target-broker:deploymentServer]
targetUri= <IP address/hostname of Forwarder Management server>:<port>
```

3. After performing either method, restart the forwarder.

Set up server classes on the deployment server

After you configure the Splunk Add-on for Windows and set up the forwarders as deployment clients, define a server class for the forwarders on the deployment server instance.

1. Log in to Splunk Enterprise on the deployment server.
2. From Splunk Home, select "Settings > Forwarder Management". Splunk Enterprise loads the Forwarder Management page.
3. Click the "Server classes" tab.
4. Click "New Server Class".
5. In the dialog box that appears, type in a name for the server class.

6. Click "Save". Splunk Enterprise loads the "Edit Server Class" screen.
7. Click the "Add Apps" button. Splunk Enterprise loads the "Add Apps" screen.
8. In the "Unselected Apps" pane, click the "Splunk Add-on for WIndows" entry. It moves over to the "Selected Apps" pane. **Note:** If you do not see the Splunk Add-on for Windows in the "Unselected Apps" pane, confirm that you copied the add-on into the `%SPLUNK_HOME%\etc\deployment-apps` directory on the deployment server instance and restarted Splunk Enterprise on that instance.
9. Click "Save". Splunk Enterprise returns to the "Edit Server Class" screen.
10. Click the "Add clients" button. Splunk Enterprise loads the "Edit Clients" screen.
11. Specify the clients that you want to receive the Splunk Add-on for Windows by entering a string in the "Include (whitelist)" field that represents a list of the clients that should receive the add-on.

    You can enter host names, DNS names, IP addresses, or a wild card that represents more than one deployment client. Separate multiple hostnames with commas. Alternatively, you can specify clients that should not receive the add-on by entering host names, DNS names, IP addresses or wild cards in the "Exclude (blacklist)" field.

    Note: If you specify a host in both fields, by default that host does not receive the add-on. See Use forwarder management to manage clients in the Splunk Enterprise *Updating Splunk Enterprise Instances Manual* for information on how allowlists and blockllists work.
12. Click "Save". Forwarder Management returns you to the "Edit Server Class" screen and updates to let you know which clients have received the Splunk Add-on for Windows.
13. (Optional) Make additional updates to the server class or click "Back to Forwarder Management" to return to the main Forwarder Management screen.

Upgrade the Splunk Add-on for Windows

Version 6.0.0 and above of the Splunk Add-on for Windows integrates the Splunk Add-on for Microsoft AD version 1.0.0 and the Splunk Add-on for Microsoft DNS version 1.0.1. If you are using these other add-ons, disable the add-ons before upgrading to version 6.0.0 of the Splunk Add-on for Windows.

Upgrade the Splunk Add-on for Microsoft Windows from version 8.4.0 to 8.5.0

There are no additional steps required for this version upgrade. See the Install the Splunk Add-on for Windows topic in this manual.

For Lookup updates please refer to the Lookups for the Splunk Add-on for Windows topic in this manual.

Upgrade the Splunk Add-on for Microsoft Windows from version 8.3.0 to 8.4.0

There are no additional steps required for this version upgrade. See the Install the Splunk Add-on for Windows topic in this manual.

Upgrade the Splunk Add-on for Microsoft Windows from version 8.2.0 to 8.3.0

There are no additional steps required for this version upgrade. See the Install the Splunk Add-on for Windows topic in this manual.

Upgrade the Splunk Add-on for Microsoft Windows from version 8.1.2 to 8.2.0

There are no additional steps required for this version upgrade. See the Install the Splunk Add-on for Windows topic in this manual.

Upgrade the Splunk Add-on for Microsoft Windows from version 7.0.0 or higher to 8.1.1

T There are no additional steps required for this version upgrade. See the Install the Splunk Add-on for Windows â topic in this manual.

Upgrade from version 6.0.0 to 7.0.0

Update the app from within Splunk Enterprise

To check for a newer version, go to **Manage Apps** from the Splunk menu. If there is an updated version available, there will be a link similar to this: `6.0.0|Update to 7.0.0` in the Version column. You need to be logged in to Splunk.com to download the technology add-on.

1. To update your existing technology add-on with the newer one, click the link in the version column.
2. Click **Update** to get the newer version.
3. Click **Restart**.

Update the app manually

1. Go to Splunkbase and find the new version of the add-on. Download the add-on to your desktop or local directory.
2. Install the add-on by navigating to **Manage Apps** > **Install app from file** from the Splunk Home page.
3. Browse to the add-on location and select the add-on.
4. Select **Upgrade app** so that the newer version of the add-on overwrites the older one.
5. Click **Upload**.
6. Click **Restart**.

Upgrade using .conf files

Follow these steps to install your upgraded version of the Splunk Add-on for Windows using configuration files:

1. Download the upgraded version of the Splunk Add-on for Windows from Splunkbase.
2. Expand your downloaded file.
3. Copy the expanded folder into the `$SPLUNK_HOME/etc/apps` directory.
4. Restart your Splunk Enterprise deployment.

Upgrade from version 5.0.1 to 6.0.0

If you are using versions of the Splunk Add-on for Windows earlier than version 5.0.1, first upgrade to Windows 5.0.1. See the previous topic, Upgrade the Splunk Add-on for Windows from versions earlier than 5.0.1 to upgrade to version 5.0.1. Then, complete the following steps to upgrade to version 6.0.0.

See the corresponding sections that follow if you are migrating from the Splunk Add-on for Microsoft Active Directory or the Splunk Add-on for Microsoft Windows DNS to the Splunk Add-on for Microsoft Windows 6.0.0.

WindowsUpdate.log changes for Windows 10 and Windows Server 2016

In previous versions of the Splunk Add-on for Windows, users must manually run the `Get-WindowsUpdateLog` Powershell command at regular intervals to convert ETW traces into a readable `WindowsUpdate.log` file, as well as manually update the path to index data.

Version 6.0.0 of the Splunk Add-on for Microsoft Windows automates this process:

1. (Only on Windows 10 or Windows Server 2016) Disable the current `WindowsUpdateLog` input.
2. Copy the following stanza from `default/inputs.conf` to `local/inputs.conf` to automatically generate daily `WindowsUpdate.log` files in `$SPLUNK_HOME\var\log\Splunk_TA_windows`:

   ```
   [powershell://generate_windows_update_logs]
   script = ."$SplunkHome\etc\apps\Splunk_TA_windows\bin\powershell\generate_windows_update_logs.ps1"
   schedule = 0 */24 * * *
   disabled = 1
   ```
3. Copy the following stanza from `default/inputs.conf` to `local/inputs.conf` to monitor the generated `WindowsUpdate.log` in Windows 10 and Server 2016:

   ```
   [monitor://$SPLUNK_HOME\var\log\Splunk_TA_windows\WindowsUpdate.log]
   disabled = 1
   sourcetype = WindowsUpdateLog
   ```
4. Enable both inputs by setting `disabled = 0`.

The WindowsUpdate.Log file is generated in $SPLUNK_HOME\var\log\Splunk_TA_windows.

Change `WinEventLog` collection mode

Previous versions of the Splunk Add-on for Windows collected `WinEventLog` data collection inputs in Classic mode. By default, version 6.0.0 of the Splunk Add-on for Windows collects all `WinEventLog` data collection inputs in XML mode.

To continue data collection of `WinEventLog` data inputs in Classic mode after upgrading to version 6.0.0 of the Splunk Add-on for Windows, follow these steps:

1. Create a local copy of existing `[WinEventLog://*]` stanzas in `local/inputs.conf`.
2. For each stanza, add `renderXml = false`.

Here is an example stanza for the `WinEventLog Application` inputs stanza to continue collecting data in Classic mode:

```
[WinEventLog://Application]
disabled = 1
start_from = oldest
current_only = 0
checkpointInterval = 5
renderXml = false
```

If you want to stop data collection of `WinEventLog` data inputs in Classic mode and start using XML mode, change the existing `WinEventLog` stanzas in `local/inputs.conf` to `renderXml = true`.

Migrate from the Splunk Add-on for Microsoft Windows Active Directory (AD) version 1.0.0 to the Splunk Add-on for Windows version 6.0.0

Migrate from the Splunk Add-on for Microsoft Windows Active Directory:

Configure Active Directory Inputs

1. Make sure all the inputs of the Splunk Add-on for Microsoft Windows AD are disabled in `inputs.conf`, `admon.conf`, and `perfmon.conf`, since these inputs are also in the Splunk Add-on for Windows version 6.0.0.
2. Disable the Splunk Add-on for Microsoft Windows AD.
3. Move the `Splunk_TA_microsoft_ad` from `$Splunk_Home/etc/apps to $SPLUNK_HOME/etc/disabled-apps`.
4. Copy the following input stanzas from `Splunk_TA_Windows/default/inputs.conf` to `Splunk_TA_Windows/local/inputs.conf`:
    - [WinEventLog://DFS Replication]
    - [WinEventLog://Directory Service]
    - [WinEventLog://File Replication Service]
    - [WinEventLog://Key Management Service]
    - [monitor://$WINDIR\debug\netlogon.log]
    - [script://.\bin\runpowershell.cmd nt6-repl-stat.ps1]
    - [powershell://Replication-Stats]
    - [script://.\bin\runpowershell.cmd nt6-health.ps1]
    - [powershell://AD-Health]
    - [script://.\bin\runpowershell.cmd nt6-siteinfo.ps1]
    - [powershell://Siteinfo]
    - [perfmon://Memory]
    - [perfmon://Processor]
    - [perfmon://Network_Interface]
    - [perfmon://DFS_Replicated_Folders]
    - [perfmon://NTDS]
    - [admon://default]
5. Make sure there are no duplicate stanzas in inputs.conf after migration.
6. Update index configurations as described in Configure Active Directory Indexes.
7. To continue to collect perfmon data in single mode, see Changed default Perfmon data collection mode to multikv from single for AD Perfmon inputs.
8. To continue to collect wineventlog data in classic format, see Changed default WinEventLog data collection mode to XML from classic for AD Inputs.
9. Enable the Active Directory inputs in `Splunk_TA_Windows/local/inputs.conf`.

Configure Active Directory Indexes

The `indexes.conf` file in the Splunk Add-on for Microsoft Windows AD 1.0.0 is not in the Splunk Add-on for Windows version 6.0.0, nor is the `index=*` setting from all stanzas in `inputs.conf`.

Missing the following steps means your Splunk platform deployment will not have index configurations. This can result in data loss.

1. If you were using indexes.conf or any custom index to store your data in an earlier version of the Splunk Add-on for Microsoft AD 1.0.0, copy or create the `msad`, `wineventlog`, `perfmon`, `winevents`, and `windows` stanzas from the `indexes.conf` and `inputs.conf` files in your existing Splunk Add-on for Microsoft Windows AD version 1.0.0 in the `/Splunk_TA_microsoft_ad/default/` folder to the Splunk Add-on for Windows version v6.0.0 `/Splunk_TA_Windows/local/` folder. Update the index configurations for these Active Directory inputs based on your existing configurations. Otherwise, any data collected goes to the default main index.
2. When you forward data from a Windows server using the Splunk Add-on for Windows, the indexer you send events to must also have these indexes present. Install the add-on onto the indexer, and create a new `indexes.conf` file in the `/Splunk_TA_Windows/local/` directory. After creating the indexes, specify these indexes in `inputs.conf` in the `/Splunk_TA_Windows/local/` directory.

3. Make sure there are no duplicate stanzas in `indexes.conf`.

Changed default Perfmon data collection mode to multikv from single for AD Perfmon inputs

The Splunk Add-on for Windows collects Perfmon data in Multikv mode by default. Multikv data collection has benefits over single mode.

Multikv mode has a different event format than single mode. If you want to use multikv mode, set `mode = multikv` for all required stanzas:

1. Create a local copy of all the existing [perfmon://*] stanzas in `local/inputs.conf`.
2. For each stanza add the line `mode = multikv` .

If you want to collect Perfmon data inputs in single mode event format after migrating to the Splunk Add-on for Windows to 6.0.0, follow these steps:

1. Create a local copy of all the existing AD [perfmon://*] stanzas from `Splunk_TA_Windows/default/inputs.conf` to `Splunk_TA_Windows/local/inputs.conf`.
2. For each stanza add the line `"mode = single"`.

The following is an example stanza for perfmon Processor inputs stanza to continue collecting Processor related perfmon data in single mode:

```
[perfmon://Processor]
object = Processor
counters = % Processor Time; % User Time; % Privileged Time; Interrupts/sec; % DPC Time; % Interrupt Time;
DPCs Queued/sec; DPC Rate; % Idle Time; % C1 Time; % C2 Time; % C3 Time; C1 Transitions/sec; C2
Transitions/sec; C3 Transitions/sec
instances = *
interval = 10
disabled = 1
mode = single
useEnglishOnly=true
```

Changed default WinEventLog data collection mode to XML from classic for AD Inputs

All WinEventLog data collection inputs in the Splunk Add-on for Windows version 6.0.0 are in XML mode by default.

If you want to continue data collection of WinEventLog data inputs in existing Classic mode after upgrading the Splunk Add-on for Windows to 6.0.0, follow these steps:

1. Create a local copy of all the existing AD [WinEventLog://*] stanzas from `Splunk_TA_Windows/default/inputs.conf` to `Splunk_TA_Windows/local/inputs.conf`.
2. For each stanza, add the line `"renderXml = false"`

Here is an example stanza for WinEventLog Application inputs stanza to continue collecting data in classic mode:

```
[WinEventLog://Application]
disabled = 1
start_from = oldest
current_only = 0
checkpointInterval = 5
renderXml=false
```

If you want to stop data collection of WinEventLog data inputs in existing classic mode and to use XML mode, change the existing WinEventLog stanzas in `local/inputs.conf` to `"renderXml = true"`.

Configuration file changelog for Windows 6.0.0 and AD 1.0.0

Here is a changelog for Microsoft Active Directory 1.0.0 after migrating to Windows 6.0.0:

Configuration File Name	Name of stanza removed
perfmon.conf	all
admon.conf	all
indexes.conf	all
inputs.conf	[admon://NearestDC]

WinEventLog extraction changes for Active Directory sources

The Splunk Add-on for Windows v6.0.0 updates how source and sourcetypes are assigned to WinEventLog data for AD collection. All WinEventLogs are now assigned to either the WinEventLog or the XmlWinEventLog sourcetype and are distinguished by their source.

WinEventLog format	Source in AD 1.0.0	Sourcetype in AD 1.0.0	Source in Windows 6.0.0	Sourcetype in Windows 6.0.0
Classic	WinEventLog:DFS Replication	WinEventLog:DFS-Replication	WinEventLog:DFS Replication	WinEventLog
Classic	WinEventLog:Directory Service	WinEventLog:Directory-Service	WinEventLog:Directory Service	WinEventLog
Classic	WinEventLog:File Replication Service	WinEventLog:File-Replication-Service	WinEventLog:File Replication Service	WinEventLog
Classic	WinEventLog:Key Management Service	WinEventLog:Key-Management-Service	WinEventLog:Key Management Service	WinEventLog
XML	WinEventLog:DFS Replication	WinEventLog:DFS-Replication	XmlWinEventLog:DFS Replication	XmlWinEventLog
XML	WinEventLog:Directory Service	WinEventLog:Directory-Service	XmlWinEventLog:Directory Service	XmlWinEventLog
XML	WinEventLog:File Replication Service	WinEventLog:File-Replication-Service	XmlWinEventLog:File Replication Service	XmlWinEventLog
XML	WinEventLog:Key Management Service	WinEventLog:Key-Management-Service	XmlWinEventLog:Key Management Service	XmlWinEventLog

Due to these changes, events that have already been indexed will no longer be extracted properly. The following renaming stanzas are in the Splunk Add-on For Microsoft Windows 6.0.0 to rename your already indexed events at search time:

```
[WinEventLog:DFS-Replication]
rename = wineventlog

[WinEventLog:Directory-Service]
rename = wineventlog
```

```
[WinEventLog:File-Replication-Service]
rename = wineventlog

[WinEventLog:Key-Management-Service]
rename = wineventlog
```

If you collect WinEventLog data in Xml Format in the Splunk Addon For Active Directoy 1.0.0, add the following stanzas in `/Splunk_TA_windows/local/props.conf` to rename your already indexed xml wineventlog events at search-time.

```
[WinEventLog:DFS-Replication]
rename = xmlwineventlog

[WinEventLog:Directory-Service]
rename = xmlwineventlog

[WinEventLog:File-Replication-Service]
rename = xmlwineventlog

[WinEventLog:Key-Management-Service]
rename = xmlwineventlog
```

Renamed sourcetypes are case sensitive.

Change sourcetype-based extractions to source-based (Active Directory)

If you have added custom extractions in the sourcetype-based stanza of the Splunk Add-on for Microsoft Windows AD, see convert sourcetype-based configurations to source-based extractions.

Move any other custom configurations from TA-AD 1.0.0 to TA-Windows 6.0.0

Copy any other custom configurations from `/Splunk_TA_microsoft_ad/` to `/Splunk_TA_windows/` in appropriate configuration files.

Migrate custom configurations of perfmon.conf (Active Directory)

If you have a `perfmon.conf` file in the Splunk Add-on for Microsoft Windows AD, it does not exist in the Splunk Add-on for Microsoft Windows. Copy any custom configurations of `perfmon.conf` to the `perfmon` stanza in `/Splunk_TA_windows/local/inputs.conf`.

Migrate custom configurations of admon.conf

If you have an `admon.conf` in the Splunk Add-on for Microsoft Windows AD, it does not exist in the Splunk Add-on for Microsoft Windows version 6.0.0. Copy any custom configuration of the `[NearestDC]` stanza of `admon.conf` to the `[admon://default]` stanza in `/Splunk_TA_windows/local/inputs.conf`.

Migrate from the Splunk Add-on for Microsoft Windows DNS to the Splunk Add-on for Microsoft Windows

Migrate from the Splunk Add-on for Microsoft Windows DNS:

Configure DNS Inputs

1. Make sure all the inputs of the Splunk Add-on for Microsoft DNS are disabled in `inputs.conf` and `perfmon.conf`, since these inputs are also in the Splunk Add-on for Windows version 6.0.0.
2. Disable the Splunk Add-on for Microsoft DNS.
3. Move the `Splunk_TA_microsoft_dns` from `$Splunk_Home/etc/apps to $SPLUNK_HOME/etc/disabled-apps`.
4. Copy the following input stanzas from `Splunk_TA_Windows/default/inputs.conf` to `Splunk_TA_Windows/local/inputs.conf`:
    - [WinEventLog://DNS Server]
    - [MonitorNoHandle://$WINDIR\System32\Dns\dns.log]
    - [script://.\bin\runpowershell.cmd dns-zoneinfo.ps1]
    - [script://.\bin\runpowershell.cmd dns-health.ps1]
    - [perfmon://Memory]
    - [perfmon://Processor]
    - [perfmon://Network_Interface]
    - [perfmon://DNS].
5. Make sure there are no duplicate stanzas in `inputs.conf` after migration.
6. Update index configurations as described in Configure DNS Indexes.
7. To continue to collect perfmon data in single mode, see Changed default Perfmon data collection mode to multikv from single for DNS Perfmon inputs.
8. To continue to collect wineventlog data in classic format, see Changed default WinEventLog data collection mode to XML from classic for DNS Inputs.
9. Enable the DNS inputs in `Splunk_TA_Windows/local/inputs.conf`.

Configure DNS Indexes

The indexes.conf file in the Splunk Add-on for Microsoft DNS 1.0.1 is not in the Splunk Add-on for Windows version 6.0.0, nor is the index=* setting from all stanzas in inputs.conf.

You must complete the following steps to create index configurations in your Splunk platform deployment and to avoid data loss.

1. If you were using `indexes.conf` or any custom index to store your data in an earlier version of the Splunk Add-on for Microsoft DNS 1.0.1, copy or create the `msad`, `wineventlog`, `perfmon`, `winevents`, and `windows` stanzas from the `indexes.conf` and `inputs.conf` files in your existing Splunk Add-on for Microsoft DNS version 1.0.1 in the `/Splunk_TA_microsoft_dns/default/` folder to the Splunk Add-on for Windows version version 6.0.0 `/Splunk_TA_Windows/local/` folder. Update the index configurations for these DNS inputs based on your existing configurations. Otherwise, any data collected goes to the default main index.
2. <When you forward data from a Windows server using the Splunk Add-on for Windows, the indexer you send events to must also have these indexes present. Install the add-on onto the indexer, and create a new `indexes.conf` file in the `/Splunk_TA_Windows/local/` directory. After creating the indexes, specify these indexes in `inputs.conf` in the `/Splunk_TA_Windows/local/` directory.
3. Make sure there are no duplicate stanzas in `indexes.conf`.

Changed default Perfmon data collection mode to multikv from single for DNS Perfmon inputs

Multikv mode of Perfmon data collection has benefits over single mode.

Multikv mode has a different event format than single mode. If you want to use multikv mode, set `mode = multikv` for all required stanzas:

1. Create a local copy of all the existing `[perfmon://*]` stanzas in your `local/inputs.conf` file.
2. For each stanza, add the line `mode = multikv`.

If you want to collect Perfmon data inputs in single mode format after migrating to the Splunk Add-on for Windows to 6.0.0, follow these steps:

1. Create a local copy of all `DNS [perfmon://*]` stanzas from `Splunk_TA_Windows/default/inputs.conf` to `Splunk_TA_Windows/local/inputs.conf`.
2. For each stanza, add the line `mode = single`.

The following is an example stanza for perfmon DNS inputs stanza to continue collecting DNS related perfmon data in single mode:

```
[perfmon://DNS]
object = DNS
counters = Total Query Received; Total Query Received/sec; UDP Query Received; UDP Query Received/sec; TCP
Query Received; TCP Query Received/sec; Total Response Sent; Total Response Sent/sec; UDP Response Sent; UDP
Response Sent/sec; TCP Response Sent; TCP Response Sent/sec; Recursive Queries; Recursive Queries/sec;
Recursive Send TimeOuts; Recursive TimeOut/sec; Recursive Query Failure; Recursive Query Failure/sec; Notify
Sent; Zone Transfer Request Received; Zone Transfer Success; Zone Transfer Failure; AXFR Request Received;
AXFR Success Sent; IXFR Request Received; IXFR Success Sent; Notify Received; Zone Transfer SOA Request
Sent; AXFR Request Sent; AXFR Response Received; AXFR Success Received; IXFR Request Sent; IXFR Response
Received; IXFR Success Received; IXFR UDP Success Received; IXFR TCP Success Received; WINS Lookup Received;
WINS Lookup Received/sec; WINS Response Sent; WINS Response Sent/sec; WINS Reverse Lookup Received; WINS
Reverse Lookup Received/sec; WINS Reverse Response Sent; WINS Reverse Response Sent/sec; Dynamic Update
Received; Dynamic Update Received/sec; Dynamic Update NoOperation; Dynamic Update NoOperation/sec; Dynamic
Update Written to Database; Dynamic Update Written to Database/sec; Dynamic Update Rejected; Dynamic Update
TimeOuts; Dynamic Update Queued; Secure Update Received; Secure Update Received/sec; Secure Update Failure;
Database Node Memory; Record Flow Memory; Caching Memory; UDP Message Memory; TCP Message Memory; Nbstat
Memory; Unmatched Responses Received
interval = 10
disabled = 0
mode = single
useEnglishOnly=true
```

Changed default WinEventLog data collection mode to XML from classic for DNS Inputs

All WinEventLog data collection inputs in the Splunk Add-on for Windows version 6.0.0 are in XML mode by default.

If you want to continue data collection of WinEventLog data inputs in existing Classic mode after upgrading the Splunk Add-on for Windows to 6.0.0, follow these steps:

1. Create a local copy of all the existing DNS [WinEventLog://*] stanzas from `Splunk_TA_Windows/default/inputs.conf` to `Splunk_TA_Windows/local/inputs.conf`.
2. For each stanza, add the line `"renderXml = false"`.

Here is an example stanza for WinEventLog Application inputs stanza to continue collecting data in classic mode:

```
[WinEventLog://Application]
disabled = 1
start_from = oldest
current_only = 0
checkpointInterval = 5
renderXml=false
```

If you want to stop data collection of WinEventLog data inputs in existing classic mode and to use XML mode, change the existing WinEventLog stanzas in `local/inputs.conf` to `"renderXml = true"`.

Configuration file changelog for Windows 6.0.0 and DNS 1.0.1

Here is a changelog for DNS 1.0.1 after migrating to Windows 6.0.0:

Configuration File Name	Name of stanza removed
perfmon.conf	all
indexes.conf	all
tags.conf	[eventtype=nt6-dns-events]

WinEventLog extraction changes for DNS sources

The Splunk Add-on for Windows version 6.0.0 updates how source and sourcetypes are assigned to WinEventLog data for DNS collection. All WinEventLogs are now assigned to either the WinEventLog or the XmlWinEventLog sourcetype and are distinguished by their source.

WinEventLog format	Source in DNS 1.0.1	Sourcetype in DNS 1.0.1	Source in Windows 6.0.0	Sourcetype in Windows 6.0.0
Classic	WinEventLog:DNS Server	WinEventLog:DNS-Server	WinEventLog:DNS Server	WinEventLog
XML	WinEventLog:DNS Server	WinEventLog:DNS-Server	XmlWinEventLog:DNS Server	XmlWinEventLog

Due to these changes, events that have already been indexed will no longer be extracted properly. The following renaming stanza is in the Splunk Add-on For Microsoft Windows 6.0.0 to rename your already indexed events at search time:

```
[WinEventLog:DNS-Server]
rename = wineventlog
```

If you have been collecting WinEventLog data in Xml Format while using Splunk Addon For Active Directory 1.0.0, add the following stanza in `/Splunk_TA_windows/local/props.conf` to rename your already indexed xml wineventlog events at search time.

```
[WinEventLog:DNS-Server]
rename = xmlwineventlog
```

Renamed sourcetypes are case sensitive.

Change sourcetype-based extractions to source-based

There are no preconfigured extractions for the sourcetype WinEventLog:DNS-Server in Splunk Addon For Microsoft Windows DNS 1.0.1. But if you have added custom extractions in its sourcetype-based stanza, see Change sourcetype-based extractions to source-based extractions.

Move any other custom configurations from TA-DNS 1.0.1 to TA-Windows 6.0.0

Copy any other custom configurations from `/Splunk_TA_microsoft_dns/` to `/Splunk_TA_windows/` in appropriate conf files.

Migrate custom configurations of perfmon.conf (DNS)

Since `perfmon.conf` in the Splunk Add-on for Microsoft DNS does not exist in the Splunk Add-on for Windows, copy any custom configuration of PERFMON:* stanzas of `perfmon.conf` to its related perfmon stanza in `/Splunk_TA_windows/local/inputs.conf`.

Upgrade the Splunk Add-on for Windows in a distributed deployment

For optimized use of your Splunk license, upgrade the Splunk Add-on for Windows by installing it on your Splunk platform components in the following order:

1. Search heads
2. Search head clusters
3. Nonclustered indexers, Windows heavy forwarders, and intermediate forwarders
4. Clustered indexers
5. Deployment servers

Upgrade the Splunk Add-on for Windows on a search head

Follow these steps to install your upgraded version of the Splunk Add-on for Windows on each search head:

1. Download the upgraded version of the Splunk Add-on for Windows from Splunkbase.
2. Expand your downloaded file.
3. On each search head, copy the expanded folder into the `$SPLUNK_HOME/etc/apps` directory.
4. Restart each search head.

Upgrade the Splunk Add-on for Windows on a search head cluster

To upgrade an add-on on a search head cluster, remove the previous version and push the upgraded version to the cluster:

1. Remove the existing `Splunk_TA_Windows` folder from the `$SPLUNK_HOME/etc/shcluster/apps` directory.
2. Push this change to the cluster using the `splunk apply shcluster-bundle` command.
3. Download the upgraded version of the Splunk Add-on for Windows from Splunkbase.
4. Expand your downloaded file.
5. Copy the expanded folder into the `$SPLUNK_HOME/etc/shcluster/apps` directory.
6. Push the upgraded version to the cluster using the `splunk apply shcluster-bundle` command.

Upgrade the Splunk Add-on for Windows on nonclustered indexers and intermediate forwarders

Complete the following steps to upgrade these components:

1. Download the upgraded version of the Splunk Add-on for Windows from Splunkbase.
2. Expand your downloaded file to a temporary location.

3. Remove the following files:
    1. `<app>/bin`
    2. `<app>/default/eventgen.conf`
    3. `<app>/default/inputs.conf`
    4. `<app>/default/wmi.conf`
    5. `<app>/default/indexes.conf`
4. Copy the expanded `Splunk_TA_Windows` folder to the `$SPLUNK_HOME/etc/apps` directory.

Upgrade the Splunk Add-on for Windows on an indexer cluster

Follow these steps to upgrade the Splunk add-on for Windows on each of your indexer clusters:

1. Download the upgraded version of the Splunk Add-on for Windows from Splunkbase.
2. Expand your downloaded file.
3. Review the use of index in all inputs associated with the Splunk Add-on for Windows and identify all indexes
4. Ensure each index has been defined in indexes.conf in the appropriate location under `$SPLUNK_HOME/etc/master_apps`
5. Copy the expanded `Splunk_TA_Windows` folder to the `$SPLUNK_HOME/etc/master_apps` directory on the cluster master.
6. Apply the cluster bundle

Upgrade the Splunk Add-on for Windows using a deployment server

You can use a deployment server to upgrade the Splunk Add-on for Windows in your distributed deployment:

1. Download the upgraded version of the Splunk Add-on for Windows from Splunkbase.
2. Expand your downloaded file.
3. Copy the expanded `Splunk_TA_Windows` folder to the `$SPLUNK_HOME/etc/deployment-apps` directory.
4. Restart the deployment server.

Configuration

Configure the Splunk Add-on for Windows

The Splunk Add-on for Windows must be configured with configuration files. You can configure the add-on manually or push a configuration with a **deployment server**. See deploy the Splunk Add-on for Windows with Forwarder Management.

The default configuration files for the Splunk Add-on for Windows reside in `%SPLUNK_HOME%\etc\apps\Splunk_TA_windows\default`. Do not edit the files in this directory because Splunk overwrites them whenever you upgrade the add-on. Create configuration files in the `%SPLUNK_HOME%\etc\apps\Splunk_TA_windows\local` directory and make your edits there.

Only modify input stanzas whose defaults you want to change. If you do not edit any files, the add-on does not collect any Windows data.

For more information about configuration files, see About configuration files in the Splunk Enterprise *Admin Manual*.

Configure props.conf

To reduce index volume, use the following best practice. Windows 5.0.1 provides an option to remove extra text and normalize inappropriate values in both Classic and XML `WinEventLog` events by using `SEDCMD`.

The `SEDCMD` configurations are commented in `default/props.conf`. The explanation for each `SEDCMD` extraction is under the `##### Explanation` line in each of the following stanzas:

```
[source::WinEventLog:System]
[source::WinEventLog:Security]
[source::WinEventLog:ForwardedEvents]
[WMI:WinEventLog:System]
[WMI:WinEventLog:Security]
```

Configure event cleanup best practices in props.conf

Remove extra text and normalize inappropriate values in both Classic and XML WinEventLog events using SEDCMD. You can use the extractions by copying the lines beginning with `SEDCMD-` in these stanzas from `default/props.conf` and pasting them in `local/props.conf`. For each one you want to use, uncomment the line.

1. On your Splunk platform deployment, create or navigate to `%SPLUNK_HOME%/etc/apps/Splunk_TA_windows/local/props.conf`.

```
 [source::WinEventLog:System]
     SEDCMD-clean_info_text_from_winsystem_events_this_event = s/This event is
generated[\S\s\r\n]+$//g

 [source::WinEventLog:Security]
     SEDCMD-windows_security_event_formater = s/(?m)(^\s+[^:]+\:)\s+-?$/\1/g
     SEDCMD-windows_security_event_formater_null_sid_id = s/(?m)(:)(\s+NULL SID)$/\1/g
s/(?m)(ID:)(\s+0x0)$/\1/g
     SEDCMD-cleansrcip = s/(Source Network Address:    (\:\:1|127\.0\.0\.1))/Source Network
```

```
Address:/
     SEDCMD-cleansrcport = s/(Source Port:\s*0)/Source Port:/
     SEDCMD-remove_ffff = s/::ffff://g
     SEDCMD-clean_info_text_from_winsecurity_events_certificate_information = s/Certificate
information is only[\S\s\r\n]+$//g
     SEDCMD-clean_info_text_from_winsecurity_events_token_elevation_type = s/Token Elevation Type
indicates[\S\s\r\n]+$//g
     SEDCMD-clean_info_text_from_winsecurity_events_this_event = s/This event is
generated[\S\s\r\n]+$//g

#For XmlWinEventLog:Security
     SEDCMD-cleanxmlsrcport = s/<Data Name='IpPort'>0<\/Data>/<Data Name='IpPort'><\/Data>/
     SEDCMD-cleanxmlsrcip = s/<Data Name='IpAddress'>(\:\:1|127\.0\.0\.1)<\/Data>/<Data
Name='IpAddress'><\/Data>/

 [source::WinEventLog:ForwardedEvents]
     SEDCMD-remove_ffff = s/::ffff://g
     SEDCMD-cleansrcipxml = s/<Data Name='IpAddress'>(\:\:1|127\.0\.0\.1)<\/Data>/<Data
Name='IpAddress'><\/Data>/
     SEDCMD-cleansrcportxml=s/<Data Name='IpPort'>0<\/Data>/<Data Name='IpPort'><\/Data>/
     SEDCMD-clean_rendering_info_block = s/<RenderingInfo Culture='.*'>(?s)(.*)<\/RenderingInfo>//

 [WMI:WinEventLog:System]
     SEDCMD-clean_info_text_from_winsystem_events_this_event = s/This event is
generated[\S\s\r\n]+$//g

 [WMI:WinEventLog:Security]
     SEDCMD-windows_security_event_formater = s/(?m)(^\s+[^:]+\:)\s+-?$/\1/g
     SEDCMD-windows_security_event_formater_null_sid_id = s/(?m)(:)(\s+NULL SID)$/\1/g
s/(?m)(ID:)(\s+0x0)$/\1/g
     SEDCMD-cleansrcip = s/(Source Network Address:    (\:\:1|127\.0\.0\.1))/Source Network
Address:/
     SEDCMD-cleansrcport = s/(Source Port:\s*0)/Source Port:/
     SEDCMD-remove_ffff = s/::ffff://g
     SEDCMD-clean_info_text_from_winsecurity_events_certificate_information = s/Certificate
information is only[\S\s\r\n]+$//g
     SEDCMD-clean_info_text_from_winsecurity_events_token_elevation_type = s/Token Elevation Type
indicates[\S\s\r\n]+$//g
     SEDCMD-clean_info_text_from_winsecurity_events_this_event = s/This event is
generated[\S\s\r\n]+$//g</li>
```

2. Save your changes.

Configure indexes.conf

The `indexes.conf` file was removed in the Splunk Add-on for Windows version 5.0.0. See upgrade the Splunk Add-on for Windows.

Configure inputs.conf

Before the Splunk Add-on for Windows can collect data, you must configure `inputs.conf` and change the `disabled` attribute for the stanzas you want to enable to `0`.

> The [admon] input should only be enabled on one domain controller in a single domain. The [admon] input directly queries the Active Directory domain controllers. Enabling this input on multiple Splunk instances can disrupt your Active Directory servers and eventually make them unresponsive, preventing users from accessing needed services.

1. If `%SPLUNK_HOME%\etc\apps\Splunk_TA_Windows\local\inputs.conf` does not exist, create it.

2. Using a text editor, open the `inputs.conf` in `local` for editing.
3. Enable the inputs that you want the add-on to collect data for by setting the `disabled` attribute for those input stanzas to `0`.
4. Save the file and close it.
5. Copy the contents of the `Splunk_TA_windows` directory to `%SPLUNK_HOME%\etc\apps` on other forwarders or use a deployment server and Forwarder Management to distribute the add-on to other forwarders in your deployment.

Configure Windows Update Logs in inputs.conf

The following may cause data duplication.

Windows 8, Windows 8.1, Windows Server 2012, Windows 2008R2, and Windows 2012R2 overwrite the `WindowsUpdate.Log` file after it reaches a certain size, and then truncate the log file from the beginning. The size of the truncation depends on the size of new events.

The following applies only to Windows 10 and Windows Server 2016.

`Event Tracing for Windows (ETW) generates Windows Update logs in Windows 10 and Windows Server 2016.`

In versions 5.0 and 5.0.1 of the Splunk Add-on for Windows, this process was manual. Version 6.0.0 of the Splunk Add-on for Windows generates WindowsUpdate.Log files automatically and at regular intervals.

Start collecting WindowsUpdate.Log data automatically:

1. Copy the following stanzas from `default/inputs.conf` to `local/inputs.conf`:

```
## Enable below powershell and monitor stanzas to get WindowsUpdate.log for Windows 10 and Server
2016
## This stanza automatically generates WindowsUpdate.log every day
[powershell://generate_windows_update_logs]
script = ."$SplunkHome\etc\apps\Splunk_TA_windows\bin\powershell\generate_windows_update_logs.ps1"
schedule = 0 */24 * * *
disabled = 1

## This stanza monitors the generated WindowsUpdate.log in Windows 10 and Server 2016
[monitor://$SPLUNK_HOME\var\log\Splunk_TA_windows\WindowsUpdate.log]
disabled = 1
sourcetype = WindowsUpdateLog
```

2. Enable both inputs by setting `disabled = 0`.

The `WindowsUpdate.Log` file is generated and monitored from `$SPLUNK_HOME\var\log\Splunk_TA_windows`.

Configure File System change notifications in inputs.conf

To monitor a specific file or folder in the file system and index all change notifications in your Splunk instance, add a new stanza in `inputs.conf`:

```
[fschange:<path to monitor>]
signedaudit = <true|false>
```

Change notifications will be indexed with sourcetype `fs_notification`.

Render Windows Event Log events in Classic

You can configure the Splunk Add-on for Windows to render Windows Event Log events in Classic format. Version 6.0.0 of the Splunk Add-on for Windows renders Windows Event Log events in eXtensible Markup Language (XML) format by default.

Enable Classic Event Log events:

1. If `%SPLUNK_HOME%\etc\apps\Splunk_TA_Windows\local\inputs.conf` does not already exist, create it.
2. Using a text editor, open both `%SPLUNK_HOME%\etc\apps\Splunk_TA_Windows\local\inputs.conf` and `%SPLUNK_HOME%\etc\apps\Splunk_TA_Windows\default\inputs.conf for editing`.
3. Copy the Event Log monitoring stanzas whose defaults you want to change from `%SPLUNK_HOME%\etc\apps\Splunk_TA_Windows\default\inputs.conf` to `%SPLUNK_HOME%\etc\apps\Splunk_TA_Windows\local\inputs.conf`.
4. Add the following line to Event Log monitoring stanzas for which you want to generate Classic Event Log events:`renderXml = 0` For example, if you want the Security Event Log channel to render events in Classic, the Security Event Log stanza should look like this:

   ```
   [WinEventLog://Security]
   index=security
   current_only=1
   evt_resolve_ad_obj=0
   renderXml=0
   disabled=0
   ```
5. Save the `%SPLUNK_HOME%\etc\apps\Splunk_TA_Windows\local\inputs.conf` file and close it.
6. Deploy the add-on manually by copying the entire `Splunk_TA_windows` folder to `%SPLUNK_HOME%\etc\apps` on other Splunk Enterprise Instances, or use Forwarder Management to distribute the add-on to all forwarders in your deployment.

Collect data for forwarded Windows Event Logs using Windows Event Forwarding

The Splunk Add-on for Windows supports collecting forwarded Windows Event Logs in the default **Forwarded Events** channel of the **Windows Event Viewer**.

To collect data for the Forwarded Events channel, do the following steps.

1. Enable Windows Remote Management on a Windows Server 2008 or later collector Windows machine.
2. Create a subscription in the collector Windows machine and set the destination log as **Forwarded Events**.
3. Copy the following input stanzas in `default/inputs.conf` to `local/inputs.conf` and enable them.

   ```
   [WinEventLog://ForwardedEvents]
   disabled = 1
   start_from = oldest
   current_only = 0
   checkpointInterval = 5
   renderXml=true
   ```

To identify the source of forwarded events, use the host field.

The Splunk Add-on for Microsoft Windows 5.0.x supports only XML format for the collection of WinEventLogs using WEF. If you collect forwarded Windows event logs in plain text format, you might experience issues with indexed events and their extractions.

For performance information and considerations, refer to the Performance reference for the Splunk Add-on for Windows.

Windows OS-related configuration issues

When the Windows collector machine collects forwarded security, system, and application events, the forwarded events contain an additional <RenderingInfo> stanza in the Eventviewer in XML view that causes field extractions to be multivalued. To resolve this, copy `#SEDCMD-clean_rendering_info_block = s/<RenderingInfo Culture='.*'>(?s)(.*)<\/RenderingInfo>//` in the `[source::WinEventLog:ForwardedEvents]` stanza from `default/props.conf` to `local/props.conf`. Then, uncomment it.

Collect perfmon data and wmi:uptime data in metric index

The Splunk Add-on for Windows supports metric indexes for the following source types.

- Perfmon:CPU
- Perfmon:DFS_Replicated_Folders
- Perfmon:DNS
- Perfmon:ProcessorInformation
- Perfmon:LogicalDisk
- Perfmon:Memory
- Perfmon:Network
- Perfmon:Network_Interface
- Perfmon:NTDS
- Perfmon:PhysicalDisk
- Perfmon:Process
- Perfmon:Processor
- Perfmon:System
- WMI:Uptime

Prerequisites

- Splunk Enterprise 7.0 or later.
- Create a metric index for the supported sourcetype for which you would like to collect data.

Steps for collecting perfmon data in a Splunk metric index

1. In `inputs.conf`, replace the `mode=multikv` line from the supported Perfmon sourcetype with `mode=single`.
2. In the same stanza, add a new line `index=metric_index_name` with the name of the metric index.

```
[perfmon://CPU]
counters = % Processor Time; % User Time; % Privileged Time; Interrupts/sec; % DPC Time; % Interrupt
Time; DPCs Queued/sec; DPC Rate; % Idle Time; % C1 Time; % C2 Time; % C3 Time; C1 Transitions/sec;
C2 Transitions/sec; C3 Transitions/sec
disabled = 0
instances = *
interval = 10
mode = single
object = Processor
useEnglishOnly=true
index = metric_poc
```

3. Restart your Splunk Enterprise to enable the new configuration.

Steps for collecting WMI:Uptime data in a Splunk metric index

1. In `wmi.conf`, add a new line `index= metric_index_name` with the name of the metric index in the WMI:Uptime sourcetype.
2. Restart Splunk Enterprise to enable the new configuration.

Troubleshooting

Troubleshoot the Splunk Add-on for Windows

For troubleshooting tips that you can apply to all add-ons, see Troubleshoot add-ons in *Splunk Add-ons*. For additional resources, see Support and resource links for add-ons in *Splunk Add-ons*.

Field dest not properly extracted

Field dest not extracted properly for sources `WinEventLog:System`, `XmlWinEventLog:System`, `XmlWinEventLog:Security`, or WinEventLog:Security.

The field dest is extracted from the stanza `Computer_as_dest`, which is configured in `default/transforms.conf`. The value for this field may include "." separated values, for instance `WB-DEATHSTAR.VADER`. In the add-on version 8.0.0, this has been updated so that it extracts the entire value. For example:

```
[Computer_as_dest]
REGEX = <Computer>([^<]+)<\/Computer>
FORMAT = dest::$1
```

If, however, the expected value of the field is that the value should break at the ".", then the regex in the stanza can be changed as follows:

```
[Computer_as_dest]
REGEX = <Computer>([^.<]+).*?<\/Computer>
FORMAT = dest::$1
```

Cannot launch add-on

This add-on does not have views and is not intended to be visible in Splunk Web. If you are trying to launch or load views for this add-on and you are experiencing results you do not expect, turn off visibility for the add-on.

For more details about add-on visibility and instructions for turning visibility off, see Troubleshoot add-ons in *Splunk Add-ons*.

Upgrading from a previous version

If you recently upgraded to the Splunk Add-on for Windows version 6.0.0 and are experiencing data loss, you might have incorrectly upgraded your add-on. See Upgrade the Splunk Add-on for Windows for instructions on upgrading your add-on.

Potential data duplication issues

Windows 8, Windows 8.1, Windows Server 2012, Windows 2008R2, and Windows 2012R2 overwrite the `WindowsUpdate.Log` file after it reaches a certain size, and then truncate the log file from the beginning. The size of the truncation depends on the size of new events. This may cause data duplication.

In Windows 10 And Windows Server 2016, the `Get-WindowsUpdateLog` command will generate a static `WindowsUpdate.log` file every time the command runs. This causes re-indexing of the entire file, which may cause data duplication.

Troubleshooting searches

Use the following searches to check that the Splunk Add-on for Windows is properly configured.

Run the following search to see the count of events by sourcetype collected by the Splunk Add-on for Windows. If you are not using a custom index, run the following search with `index=main`.

```
index=<your custom index name here> | stats count by sourcetype
```

If the search does not return the expected sourcetypes, check the following.

- You have enabled the inputs included with the Splunk Add-on for Windows on each forwarder that runs the add-on.
- You have installed the add-on into the indexers or heavy forwarders in your deployment
- If you have changed the index names in `inputs.conf`, make sure that the custom indexes are present on all forwarders and indexers.

Run the following search to see if Windows Event Log and performance metric data are present in Splunk Enterprise.

```
eventtype=wineventlog_windows OR eventtype=perfmon_windows
```

If the search does not return the expected events, check the following.

- You have the "windows_admin" role added to your user. See the **Configure users and roles** section in Upgrade the Splunk Add-on for Windows.

If the search does not return expected events, make sure that you have installed the Splunk Add-on for Windows on all search heads in your Splunk Enterprise deployment.

Events missing from Splunk software

If you are noticing dropped events in your Splunk platform, it may be a result of a setting in the Windows Utility Viewer. Follow the steps below to avoid event override.

1. From a Windows desktop, open the **Event Viewer** desktop application.
2. From the **Event Viewer** navigation tree, select **Windows Logs**.
3. Right-click the log whose log size needs to be increased and select **Properties**.
4. Check to see if **Enable logging** is selected. If not, select **Enable logging**.
5. In the Maximum log size field, specify a size based on your own requirements.
6. In the **When maximum event log size is reached**, select **Overwrite events as needed (oldest events first)**.

Third party field extractions errors

The Splunk Add-on for Windows 5.0.x removes NTSyslog, Snare, MonitorWare, and Enterprise Security 2.0.2 field extractions. See Upgrade the Splunk Add-on for Windows for instructions on how to successfully upgrade the Splunk Add-on for Windows.

Splunk events are sent to main index

The `indexes.conf` file was removed in the Splunk Add-on for Windows version 5.0.x. See Upgrade the Splunk Add-on for Windows for instructions on how to successfully upgrade the Splunk Add-on for Windows.

Error: "The following error occurred: The service has not been started. " for TimeSyncConfiguration or TimeSyncStatus

If you see the following error in your logs for sourcetype=Script:TimesyncConfiguration or sourcetype=Script:TimesyncStatus, enable the Windows Time service.

Steps

1. From the Windows desktop, open the **Run** app.
2. Search for the services.msc file
3. In the services.msc file, select Windows Time
4. Click on **Properties** and change the **service status** to **start** and change **start type** to **automatic.**
5. Save your changes.

Searches for WinEventLogs are not returning older events

Searching for `sourcetype=WinEventLog` or `sourcetype=XmlWinEventLog` does not return already indexed events. See source and sourcetype changes.

"File $SplunkHome\bin\splunk-powershell.ps1 cannot be loaded because running scripts is disabled on this system"

This issue is caused by an execution policy issue on your Microsoft Windows system. See about Execution Policies for more information on configuring execution policies on your Microsoft Windows deployment.

Reference

Lookups for the Splunk Add-on for Windows

The Splunk Add-on for Windows has the following lookups that map fields from Windows systems to CIM-compliant values in the Splunk platform. The lookup files are located in `$SPLUNK_HOME/etc/apps/Splunk_TA_windows/lookups`.

Lookup table file	Lookup definition	
dns_action_lookup.csv	dns_action_lookup	Ma
dns_recordclass_lookup.csv	dns_recordclass_lookup	Ma
dns_vendor_lookup.csv	dns_vendor_lookup	Ma
msdhcp_signatures.csv	msdhcp_signature_lookup	Pro DH
ntsyslog_mappings.csv	ntsyslog_mappings	Pro
object_category_850.csv	endpoint_change_object_category_lookup	Pro wir
status_850.csv	endpoint_change_status_lookup	Pro reg
user_types.csv	endpoint_change_user_type_lookup	Pro wir
vendor_actions.csv	endpoint_change_vendor_action_lookup	Pro
windows_actions.csv	windows_action_lookup	Pro Eve
windows_apps.csv	windows_app_lookup	Pro Se
windows_audit_changes_850.csv	windows_audit_changes_lookup	Pro Wi
windows_eventtypes.csv	windows_eventtype_lookup	Pro Wi
windows_privileges.csv	windows_privilege_lookup	Pro Wi
windows_severities.csv	windows_severity_lookup	Pro Wi
windows_signatures_850.csv	windows_signature_lookup	Pro Eve
windows_signatures_substatus_850.csv	windows_signature_lookup2	Pro me
windows_timesync_actions.csv	windows_timesync_action_lookup	Pro
windows_update_statii.csv	windows_update_status_lookup	Pro Wi
wmi_user_account_status.csv	wmi_user_account_status_lookup	Pro inf

Lookup table file	Lookup definition	
wmi_version_range.csv	wmi_version_range_lookup	Pro info
xmlsecurity_eventcode_action_multiinput.csv	xmlsecurity_eventcode_action_lookup_multiinput	Pro the
xmlsecurity_eventcode_action.csv	xmlsecurity_eventcode_action_lookup	Pro me
xmlsecurity_eventcode_errorcode_action.csv	xmlsecurity_eventcode_errorcode_action_lookup	Me + xm
windows_endpoint_port_transport.csv	windows_endpoint_port_transport_lookup	Pr fo
windows_endpoint_service_service_name.csv	windows_endpoint_service_service_name_lookup	Pro for
windows_endpoint_service_service_type.csv	windows_endpoint_service_service_type_lookup	Pro for
windows_wineventlog_change_action.csv	windows_wineventlog_change_action_lookup	Pro Wi
windows_wineventlog_change_object_fields_850.csv	windows_wineventlog_change_object_fields_lookup	Pro obj
xmlsecurity_change_audit_and_account_management_850.csv	xmlsecurity_change_audit_and_account_management_lookup	Pro Wi
windows_start_mode_lookup.csv	windows_start_mode_lookup	Pro Sy

Search time lookup: Convert Windows Event Log eventType values to strings

The Splunk Add-on for Windows includes a lookup that lets you convert a Windows event EventType numerical value to a string. To use the lookup, enter the following in a search bar on a Splunk Enterprise instance with the add-on installed:

```
| lookup windows_eventtype_lookup EventType OUTPUTNEW Description AS <new field>
```

Performance reference for the Splunk Add-on for Windows

The following table provides the average events per second (EPS) for the listed WinEventLog channels:

Log Name	Number of Events	Seconds (Classic)	EPS (Classic)	Seconds (XML)	EPS (XML)
Application	50000	8.5	5882	9.75	5128
System	50000	9.5	5263	10.2	4901
Security	45377	13.33	3404	16	2836
Powershell	50000	7.33	6821	8	6250

Common Information Model and Field Mapping Changes for the Splunk Add-on for Microsoft Windows

Version 8.1.2 of the Splunk Add-on for Microsoft Windows introduced Common Information Model (CIM) and field mapping changes to its sourcetypes. See the following sections for information on changes to the mapping of this information.

CIM model and Field Mapping changes for Wineventlog:Security

See the following comparison tables for CIM model and field mapping changes for the `Wineventlog:Security` sourcetype.

CIM model comparison for versions 4.8.4 and 8.1.2

Sourcetype	EventCode	Previous CIM model	New CIM model
`WinEventLog:Security`	4801, 4774, 4775		Authentication, Endpoint.Processes, Event_Signatures.Signatures, Endpoint.Services, Endpoint.Filesystem
`WinEventLog:Security`	1102, 1100		Event_Signatures.Signatures, Endpoint.Processes, Endpoint.Filesystem, Endpoint.Services
`WinEventLog:Security`	4768, 4769, 4624, 4625, 4648, 4771, 4777, 4776, 4672, 4957, 5025, 4627, 4622, 4713, 5157, 4932, 5155, 5154, 5152, 4933, 4907, 4906, 4904, 4902, 4634, 4985, 5444, 4701, 4700, 4703, 4702, 4705, 4704, 4931, 5449, 5446, 5478, 6417, 6416, 5448, 5137, 5136, 5030, 5031, 5033, 5034, 5035, 4946, 4889, 4608, 1104, 4800, 4688, 4689, 4963, 4662, 4663, 4660, 4661, 4664, 5058, 5059, 4616, 4614, 4611, 4610, 4697, 4696, 4817, 4690, 4950, 4698, 4826, 4954, 5156, 4670, 4673, 4674, 5041, 5040, 5043, 5045, 5044, 4947, 4699, 4945, 4944, 4948, 4647, 6145, 6144, 4770, 4778, 4779, 5447, 4956, 5441, 4953, 5442, 6273, 6272, 4653, 4799, 4656, 4793, 4658, 5061, 5024, 5450, 5140, 5142, 5145		Endpoint.Processes, Event_Signatures.Signatures, Endpoint.Services, Endpoint.Filesystem
`WinEventLog:Security`	4717, 4718		Endpoint.Services, Change.Endpoint_Changes, Endpoint.Filesystem, Change.Account_Management, Endpoint.Processes, Event_Signatures.Signatures
`WinEventLog:Security`	5461		Change.Endpoint_Changes, Endpoint.Processes, Event_Signatures.Signatures, Endpoint.Services, Endpoint.Filesystem
`WinEventLog:Security`	4912, 4715, 4719, 1101, 1105, 1108		Endpoint.Services, Change.Auditing_Changes, Change.Endpoint_Changes, Endpoint.Filesystem, Endpoint.Processes, Event_Signatures.Signatures

Sourcetype	EventCode	Previous CIM model	New CIM model
WinEventLog:Security	5158		Endpoint.Ports, Endpoint.Processes, Event_Signatures.Signatures, Endpoint.Services, Endpoint.Filesystem
WinEventLog:Security	4657		Endpoint.Registry, Endpoint.Processes, Event_Signatures.Signatures, Endpoint.Services, Endpoint.Filesystem
WinEventLog:Security	4767, 4781, 4764, 4734, 4735, 4737, 4730, 4731, 4732, 4733, 4738, 4739, 4742, 4758, 4756, 4754, 4755, 4753, 4750, 4798, 4757, 4797, 5379, 4741, 4740, 4729, 4728, 4743, 4720, 4727, 4726, 4725, 4724		Change.Endpoint_Changes, Event_Signatures.Signatures, Endpoint.Processes, Endpoint.Filesystem, Endpoint.Services

Field mapping comparison for versions 4.8.4 and 8.1.2

Source-type	EventCode	Fields added	Fields removed
wineventlog*	5024, 5025, 5033, 5034, 5478	Error_Code, category, service, service_name, ta_windows_action, vendor_product	src
wineventlog*	5156, 5157	Error_Code, category, dest_port, process_id, ta_windows_action, transport, vendor_product	src
wineventlog*	4720, 4725, 4726, 4738, 4767	Error_Code, category, result, ta_windows_action, ta_windows_security_CategoryString, vendor_product	src
wineventlog*	4625	Error_Code, category, process_id, ta_windows_action, ta_windows_status, vendor_product	src
wineventlog*	4658, 4660, 4689, 4798, 4904, 4985, 6417	Error_Code, category, process, process_name, ta_windows_action, vendor_product	src
wineventlog*	5154, 5155, 5158	Error_Code, category, process_id, ta_windows_action, transport, vendor_product	src
wineventlog*	4907	Error_Code, category, file_name, file_path, object_file_name, object_file_path, process, process_id, process_name, ta_windows_action, vendor_product	src
wineventlog*	5152	Error_Code, category, dest_port, process_id, ta_windows_action, vendor_product	src
wineventlog*	1100, 1102, 4945, 4946, 4947, 4948	Error_Code, category, object_attrs, ta_windows_action, vendor_product	src
wineventlog*	5461	category, change_type, object_attrs, object_category, result, ta_windows_action, vendor_product	src
wineventlog*	4769, 4770	Error_Code, category, service, service_id, service_name, ta_windows_action, vendor_product	
wineventlog*	4664, 5058, 5140, 5142, 5145	Error_Code, category, file_name, file_path, ta_windows_action, vendor_product	src
wineventlog*	4727, 4728, 4729, 4730, 4731, 4732, 4733, 4734, 4735, 4737, 4739, 4750, 4753, 4754, 4755, 4757, 4758, 4764, 4781	Error_Code, category, change_type, object_attrs, object_category, result, ta_windows_action, ta_windows_security_CategoryString, vendor_product	src
wineventlog*	4688	Error_Code, Token_Elevation_Type_id, category, new_process_name, parent_process_id,	src

Source-type	EventCode	Fields added	Fields removed
		parent_process_name, parent_process_path, process, process_exec, process_name, process_path, ta_windows_action, vendor_product	
wineventlog*	1101, 1108, 4719	Error_Code, category, change_type, object_attrs, object_category, ta_windows_action, vendor_product	src
wineventlog*	4717, 4718	Error_Code, category, change_type, object_attrs, object_category, result, ta_windows_action, vendor_product	src
wineventlog*	4670	Error_Code, category, process, process_name, registry_path, ta_windows_action, vendor_product	src
wineventlog*	4776, 4777	category, ta_windows_action, vendor_product	
wineventlog*	4799	Error_Code, category, object_attrs, process, process_name, ta_windows_action, vendor_product	src
wineventlog*	4741, 4742, 4743	Error_Code, category, object_attrs, result, ta_windows_action, ta_windows_security_CategoryString, vendor_product	src
wineventlog*	4624, 4648, 4674, 4696, 4703	Error_Code, category, process, process_id, process_name, ta_windows_action, vendor_product	src
wineventlog*	4756	Error_Code, Group_Domain, Group_Name, category, change_type, object_attrs, object_category, result, ta_windows_action, ta_windows_security_CategoryString, user_group, vendor_product	src
wineventlog*	4768	Error_Code, category, service, service_id, service_name, ta_windows_action, user_id, vendor_product	
wineventlog*	1104, 1105, 4608, 4610, 4611, 4614, 4622, 4627, 4634, 4647, 4653, 4672, 4690, 4698, 4699, 4700, 4701, 4702, 4704, 4705, 4713, 4715, 4774, 4775, 4797, 4800, 4801, 4826, 4889, 4902, 4906, 4912, 4931, 4932, 4933, 4944, 4950, 4953, 4954, 4956, 4957, 4963, 5031, 5040, 5041, 5043, 5044, 5045, 5059, 5061, 5136, 5137, 5379, 5441, 5442, 5444, 6144, 6272, 6273, 6416	Error_Code, category, ta_windows_action, vendor_product	src
wineventlog*	4697	Error_Code, category, service, service_name, start_mode, ta_windows_action, vendor_product	src
wineventlog*	4673	Error_Code, category, process, process_name, service, service_name, ta_windows_action, vendor_product	src
wineventlog*	4657	Error_Code, category, object_file_name, object_file_path, process, process_id, process_name, registry_path, registry_value_name, registry_value_type, ta_windows_action, vendor_product	src
wineventlog*	5030, 5035	category, service, service_name, ta_windows_action, vendor_product	src
wineventlog*	4771	Error_Code, category, service, service_name, ta_windows_action, vendor_product	
wineventlog*	4616, 5446, 5447, 5448, 5449, 5450		src

Source-type	EventCode	Fields added	Fields removed
		Error_Code, category, process_id, ta_windows_action, vendor_product	
wineventlog*	4724	Error_Code, category, object_attrs, ta_windows_action, ta_windows_security_CategoryString, vendor_product	src
wineventlog*	6145	category, ta_windows_action, vendor_product	src
wineventlog*	4740, 4793	Error_Code, category, ta_windows_action, ta_windows_security_CategoryString, vendor_product	src
wineventlog*	4656, 4661, 4663	Error_Code, category, object_file_name, object_file_path, process, process_id, process_name, ta_windows_action, vendor_product	src
wineventlog*	4778, 4779	Error_Code, category, ta_windows_action, vendor_product	
wineventlog*	4662, 4817	Error_Code, category, object_file_name, object_file_path, ta_windows_action, vendor_product	src

CIM model comparison for versions 7.0.0 and 8.1.2

Source	EventCode	Previous CIM model	New CIM model
WinEventLog:Security	4801		Authentication, Endpoint.Processes, Event_Signatures.Signatures, Endpoint.Services, Endpoint.Filesystem
WinEventLog:Security	1102, 1100		Event_Signatures.Signatures, Endpoint.Processes, Endpoint.Filesystem, Endpoint.Services
WinEventLog:Security	4912, 4739, 4743, 4781, 4764, 4734, 4735, 4737, 4730, 4731, 4732, 4715, 4718, 4719, 4738, 4742, 4758, 4756, 4757, 4754, 4755, 4753, 4750, 4798, 4767, 4797, 4717, 5379, 4741, 4733, 4740, 4729, 4728, 1105, 4720, 4727, 4726, 4725, 4724		Change.Endpoint_Changes, Event_Signatures.Signatures, Endpoint.Processes, Endpoint.Filesystem, Endpoint.Services
WinEventLog:Security	5461		Change.Endpoint_Changes, Endpoint.Processes, Event_Signatures.Signatures, Endpoint.Services, Endpoint.Filesystem
WinEventLog:Security	4769, 4624, 4625, 4648, 4771, 4774, 4775, 4777, 4776, 4768, 4672, 4957, 5025, 4627, 4622, 4713, 5157, 4932, 5155, 5154, 5152, 4933, 4907, 4906, 4904, 4902, 4634, 4985, 5444, 4701, 4700, 4703, 4702, 4705, 4704, 4931, 5449, 5446, 5478, 6417, 6416, 5448, 5137, 5136, 5030, 5031, 5033, 5034, 5035, 4946, 4889, 4608, 1104, 4800, 4688, 4689, 4963, 4662, 4663, 4660, 4661, 4664, 5058, 5059, 4616, 4614, 4611, 4610, 4697, 4696, 4817, 4690, 4950, 4698, 4826, 4954, 5156, 4670, 4673, 4674, 5041, 5040, 5043, 5045, 5044, 4947, 4699, 4945, 4944, 4948, 4647, 6145, 6144, 4770, 4778, 4779, 5447, 4956, 5441,		Endpoint.Processes, Event_Signatures.Signatures, Endpoint.Services, Endpoint.Filesystem

Source	EventCode	Previous CIM model	New CIM model
	4953, 5442, 6273, 6272, 4653, 4799, 4656, 4793, 4658, 5061, 5024, 5450, 5140, 5142, 5145		
`WinEventLog:Security`	1101, 1108		Endpoint.Services, Change.Auditing_Changes, Change.Endpoint_Changes, Endpoint.Filesystem, Endpoint.Processes, Event_Signatures.Signatures
`WinEventLog:Security`	5158		Endpoint.Ports, Endpoint.Processes, Event_Signatures.Signatures, Endpoint.Services, Endpoint.Filesystem
`WinEventLog:Security`	4657		Endpoint.Registry, Endpoint.Processes, Event_Signatures.Signatures, Endpoint.Services, Endpoint.Filesystem

Field mapping comparison for versions 7.0.0 and 8.1.2

Source-type	EventCode	Fields added	Fields removed
`wineventlog*`	1101, 1108, 4719	change_type, object_attrs, object_category, vendor_product	
`wineventlog*`	4768	service, service_id, service_name, user_id, vendor_product	
`wineventlog*`	4741, 4742, 4743	object_attrs, result, vendor_product	
`wineventlog*`	4717, 4718, 4727, 4728, 4729, 4730, 4731, 4732, 4733, 4734, 4735, 4737, 4739, 4750, 4753, 4754, 4755, 4756, 4757, 4758, 4764, 4781, 5461	change_type, object_attrs, object_category, result, vendor_product	
`wineventlog*`	4697	service, service_name, start_mode, vendor_product	
`wineventlog*`	4657	object_file_name, object_file_path, process, process_name, registry_path, registry_value_name, registry_value_type, vendor_product	
`wineventlog*`	4656, 4661, 4663	object_file_name, object_file_path, process, process_name, vendor_product	
`wineventlog*`	4662, 4817	object_file_name, object_file_path, vendor_product	
`wineventlog*`	4673	process, process_name, service, service_name, vendor_product	
`wineventlog*`	4670	process, process_name, registry_path, vendor_product	

Source-type	EventCode	Fields added	Fields removed
wineventlog*	4720, 4725, 4726, 4738, 4767	result, vendor_product	
wineventlog*	4664, 5058, 5140, 5142, 5145	file_name, file_path, vendor_product	
wineventlog*	4771, 5024, 5025, 5030, 5033, 5034, 5035, 5478	service, service_name, vendor_product	
wineventlog*	4799	object_attrs, process, process_name, vendor_product	
wineventlog*	4907	file_name, file_path, object_file_name, object_file_path, process, process_name, vendor_product	
wineventlog*	5154, 5155, 5156, 5157, 5158	transport, vendor_product	
wineventlog*	4624, 4648, 4658, 4660, 4674, 4689, 4696, 4703, 4798, 4904, 4985, 6417	process, process_name, vendor_product	
wineventlog*	1100, 1102, 4724	object_attrs, vendor_product	
wineventlog*	4688	Token_Elevation_Type_id, new_process_name, parent_process_id, parent_process_name, parent_process_path, process, process_exec, process_name, process_path, vendor_product	
wineventlog*	4769, 4770	service, service_id, service_name, vendor_product	
wineventlog*	1104, 1105, 4608, 4610, 4611, 4614, 4616, 4622, 4625, 4627, 4634, 4647, 4653, 4672, 4690, 4698, 4699, 4700, 4701, 4702, 4704, 4705, 4713, 4715, 4740, 4774, 4775, 4776, 4777, 4778, 4779, 4793, 4797, 4800, 4801, 4826, 4889, 4902, 4906, 4912, 4931, 4932, 4933, 4944, 4945, 4946, 4947, 4948, 4950, 4953, 4954, 4956, 4957, 4963, 5031, 5040, 5041, 5043, 5044, 5045, 5059, 5061, 5136, 5137, 5152, 5379, 5441, 5442, 5444, 5446, 5447, 5448, 5449, 5450, 6144, 6145, 6272, 6273, 6416	vendor_product	

CIM model and Field Mapping Changes for XmlWineventlog:Security

See the following comparison tables for CIM model and field mapping changes for the `XmlWineventlog:Security` sourcetype.

CIM model comparison for versions 4.8.4 and 8.1.2

Sourcetype	EventCode	Previous CIM model	New CIM model
XmlWinEventLog:Security	4672, 4957, 4624, 4625, 4648, 4769, 4768, 4771, 4776, 4932, 4933, 4931, 4948, 4670, 4673, 4674, 4800, 4778, 4779, 4770, 5450, 4985, 4902, 4907, 4906, 4904, 4662, 4663, 4660, 4661, 4664, 4705, 4704, 4701, 4700, 4703, 4702, 5152, 5156, 5154, 5025, 5024, 5145, 5140, 5141, 5142, 5441, 4713,		Endpoint.Processes, Event_Signatures.Signatures, Endpoint.Services, Endpoint.Filesystem

Sourcetype	EventCode	Previous CIM model	New CIM model
	4797, 4793, 4658, 4656, 4653, 4798, 4799, 5031, 5033, 5034, 6145, 6144, 5137, 5136, 5157, 5442, 5444, 5447, 5448, 4647, 5449, 4634, 4963, 5045, 5044, 5379, 5041, 5040, 5043, 6416, 1104, 4627, 4622, 5058, 5059, 6272, 6417, 4947, 4944, 4611, 4610, 4616, 4614, 5061, 4690, 4697, 4696, 4699, 4698, 4688, 4689, 4946, 4945, 5446, 4950, 4953, 4954, 4826, 4956, 4608, 4817, 5478		
XmlWinEventLog:Security	4719, 4715, 1108, 1105, 1101, 4912		Endpoint.Services, Change.Auditing_Changes, Change.Endpoint_Changes, Endpoint.Filesystem, Endpoint.Processes, Event_Signatures.Signatures
XmlWinEventLog:Security	4781, 4718, 4717, 4729, 4728, 4723, 4722, 4720, 4727, 4726, 4725, 4724, 4734, 4735, 4737, 4730, 4731, 4732, 4733, 4738, 4739, 4741, 4740, 4743, 4742, 4753, 4750, 4756, 4757, 4754, 4755, 4767, 4764, 4758		Endpoint.Services, Change.Endpoint_Changes, Endpoint.Filesystem, Change.Account_Management, Endpoint.Processes, Event_Signatures.Signatures
XmlWinEventLog:Security	1100, 1102		Event_Signatures.Signatures, Endpoint.Processes, Endpoint.Filesystem, Endpoint.Services
XmlWinEventLog:Security	4657		Endpoint.Registry, Endpoint.Processes, Event_Signatures.Signatures, Endpoint.Services, Endpoint.Filesystem
XmlWinEventLog:Security	5158		Endpoint.Ports, Endpoint.Processes, Event_Signatures.Signatures, Endpoint.Services, Endpoint.Filesystem
XmlWinEventLog:Security	4801		Authentication, Endpoint.Processes, Event_Signatures.Signatures, Endpoint.Services, Endpoint.Filesystem

Field Mapping Comparison for versions 4.8.4 and 8.1.2

Sourcetype	EventCode	Fields added	Fields removed
xmlWinEventLog*	4720, 4722, 4725, 4726, 4738, 4740, 4767	CategoryString, Error_Code, app, dest, dvc, dvc_nt_host, event_id, id, name, process_id, result, signature, signature_id, subject, ta_windows_action, ta_windows_security_CategoryString, user_group, vendor_product	
xmlWinEventLog*	4648	Error_Code, dvc, dvc_nt_host, event_id, id, name, parent_process_id, process, process_id, process_name, process_path, signature, signature_id, src_ip, subject, ta_windows_action, user_group, vendor_product	

Sourcetype	EventCode	Fields added	Fields removed
xmlWinEventLog*	1108	Error_Code, action, app, change_type, dest, dvc, dvc_nt_host, event_id, id, name, object_attrs, object_category, signature, signature_id, status, subject, ta_windows_action, vendor_product	
xmlWinEventLog*	4742, 4743	CategoryString, Error_Code, app, dest, dvc, dvc_nt_host, event_id, id, name, object_attrs, process_id, result, signature, signature_id, subject, ta_windows_action, ta_windows_security_CategoryString, user_group, vendor_product	
xmlWinEventLog*	4657	Error_Code, app, dest, dvc, dvc_nt_host, event_id, id, name, object_file_name, object_file_path, parent_process_id, process, process_id, process_name, process_path, registry_path, registry_value_name, registry_value_type, signature, signature_id, subject, ta_windows_action, vendor_product	
xmlWinEventLog*	5154	Error_Code, app, dest, dvc, dvc_nt_host, event_id, id, name, parent_process_id, process_id, signature, signature_id, subject, ta_windows_action, transport, vendor_product	
xmlWinEventLog*	4723, 4724	CategoryString, Error_Code, app, dest, dvc, dvc_nt_host, event_id, id, name, object_attrs, process_id, signature, signature_id, subject, ta_windows_action, ta_windows_security_CategoryString, user_group, vendor_product	
xmlWinEventLog*	5140	Error_Code, app, dest, dvc, dvc_nt_host, event_id, file_name, id, name, process_id, signature, signature_id, src_ip, subject, ta_windows_action, vendor_product	
xmlWinEventLog*	5152	Error_Code, app, dest, dest_port, dvc, dvc_nt_host, event_id, id, name, parent_process_id, process_id, signature, signature_id, subject, ta_windows_action, vendor_product	
xmlWinEventLog*	1102	Caller_User_Name, Error_Code, app, dest, dvc, dvc_nt_host, event_id, id, name, object_attrs, process_id, signature, signature_id, src_user, status, subject, ta_windows_action, vendor_product	
xmlWinEventLog*	4719	Error_Code, app, change_type, dest, dvc, dvc_nt_host, event_id, id, name, object_attrs, object_category, process_id, signature, signature_id, subject, ta_windows_action, vendor_product	
xmlWinEventLog*	4662, 4817	Error_Code, app, dest, dvc, dvc_nt_host, event_id, id, name, object_file_name, object_file_path, process_id, signature, signature_id, subject, ta_windows_action, vendor_product	
xmlWinEventLog*	4945, 4946, 4947, 4948, 4953, 4957	Error_Code, app, dest, dvc, dvc_nt_host, event_id, id, name, object_attrs, process_id, signature, signature_id, subject, ta_windows_action, vendor_product	
xmlWinEventLog*	5034	Error_Code, app, dest, dvc, dvc_nt_host, event_id, id, name, service, service_name, signature, signature_id, subject, ta_windows_action, vendor_product	
xmlWinEventLog*	4739	CategoryString, Error_Code, app, change_type, dest, dvc, dvc_nt_host, event_id, id, name, object_attrs, object_category, process_id, result, severity, signature, signature_id, subject, ta_windows_action, ta_windows_security_CategoryString, vendor_product	
xmlWinEventLog*	4624	Error_Code, dest, dvc, dvc_nt_host, event_id, id, name, parent_process_id, process, process_id, process_name, process_path, signature, signature_id, src_ip, subject, ta_windows_action, user_group, vendor_product	

Sourcetype	EventCode	Fields added	Fields removed
xmlWinEventLog*	4728, 4729, 4730, 4732, 4733, 4734, 4753, 4756, 4757, 4758, 4764	CategoryString, Error_Code, Group_Domain, Group_Name, app, change_type, dest, dvc, dvc_nt_host, event_id, id, name, object_category, process_id, result, signature, signature_id, subject, ta_windows_action, ta_windows_security_CategoryString, user_group, vendor_product	
xmlWinEventLog*	4768, 4769	app, dest, dvc, dvc_nt_host, event_id, id, name, process_id, service, service_id, service_name, signature, signature_id, subject, ta_windows_action, ta_windows_status, user_group, vendor_product	
xmlWinEventLog*	1100	Error_Code, app, dest, dvc, dvc_nt_host, event_id, id, name, object_attrs, process_id, signature, signature_id, status, subject, ta_windows_action, vendor_product	
xmlWinEventLog*	4797, 4798	Error_Code, action, app, dest, dvc, dvc_nt_host, event_id, id, process_id, signature_id, status, ta_windows_action, user_group, vendor_product	
xmlWinEventLog*	4696	Error_Code, app, dest, dvc, dvc_nt_host, event_id, id, name, parent_process_id, process_id, signature, signature_id, subject, ta_windows_action, user_group, vendor_product	dest_nt_domain
xmlWinEventLog*	4634	Error_Code, dest, dvc, dvc_nt_host, event_id, id, name, process_id, signature, signature_id, subject, ta_windows_action, user_group, vendor_product	
xmlWinEventLog*	4688	Error_Code, Process_Command_Line, Token_Elevation_Type_id, app, dest, dvc, dvc_nt_host, event_id, id, name, new_process, new_process_id, new_process_name, parent_process, parent_process_id, parent_process_name, parent_process_path, process, process_command_line_arguments, process_command_line_process, process_exec, process_id, process_name, process_path, signature, signature_id, subject, ta_windows_action, user_group, vendor_product	dest_nt_domain
xmlWinEventLog*	5156, 5157	Error_Code, app, dest, dest_port, dvc, dvc_nt_host, event_id, id, name, process_id, signature, signature_id, subject, ta_windows_action, transport, vendor_product	
xmlWinEventLog*	4625	dest, dvc, dvc_nt_host, event_id, id, name, parent_process_id, process, process_id, process_name, process_path, signature, signature_id, src_ip, subject, ta_windows_action, ta_windows_status, user_group, vendor_product	
xmlWinEventLog*	4627	Error_Code, action, dest, dvc, dvc_nt_host, event_id, id, process_id, signature_id, status, ta_windows_action, user_group, vendor_product	
xmlWinEventLog*	4799	Error_Code, Group_Domain, Group_Name, action, app, dest, dvc, dvc_nt_host, event_id, id, process_id, signature_id, status, ta_windows_action, user_group, vendor_product	
xmlWinEventLog*	4608, 4610, 4611, 4614, 4622, 4653, 4672, 4690, 4698, 4699, 4700, 4701, 4702, 4704, 4705, 4713, 4715, 4779, 4902, 4906, 4932, 4933, 4944, 4950, 4954, 4956, 4963, 5031, 5040, 5041, 5043, 5044, 5045, 5059, 5061,	Error_Code, app, dest, dvc, dvc_nt_host, event_id, id, name, process_id, signature, signature_id, subject, ta_windows_action, vendor_product	

Sourcetype	EventCode	Fields added	Fields removed
	5136, 5137, 5441, 5442, 5444, 6144, 6145, 6272		
xmlWinEventLog*	4647, 4800, 4801	Error_Code, app, dest, dvc, dvc_nt_host, event_id, id, name, process_id, signature, signature_id, subject, ta_windows_action, user_group, vendor_product	
xmlWinEventLog*	6417	Error_Code, action, app, dest, dvc, dvc_nt_host, event_id, id, parent_process_id, process, process_id, process_name, process_path, signature_id, status, ta_windows_action, vendor_product	
xmlWinEventLog*	4673	Error_Code, app, dest, dvc, dvc_nt_host, event_id, id, name, parent_process_id, process_id, service, signature, signature_id, subject, ta_windows_action, vendor_product	
xmlWinEventLog*	4741	CategoryString, Error_Code, app, dest, dvc, dvc_nt_host, event_id, id, name, object_attrs, process_id, result, signature, signature_id, status, subject, ta_windows_action, ta_windows_security_CategoryString, user_group, vendor_product	
xmlWinEventLog*	1104, 1105	Error_Code, action, app, dest, dvc, dvc_nt_host, event_id, id, name, process_id, signature, signature_id, status, subject, ta_windows_action, vendor_product	
xmlWinEventLog*	4703	Error_Code, action, app, dest, dvc, dvc_nt_host, event_id, id, parent_process_id, process, process_id, process_name, process_path, signature_id, status, ta_windows_action, user_group, vendor_product	
xmlWinEventLog*	1101	Error_Code, action, app, change_type, dest, dvc, dvc_nt_host, event_id, id, name, object_attrs, object_category, process_id, signature, signature_id, status, subject, ta_windows_action, vendor_product	
xmlWinEventLog*	4727, 4731, 4735, 4737, 4750, 4754, 4755	CategoryString, Error_Code, Group_Domain, Group_Name, app, change_type, dest, dvc, dvc_nt_host, event_id, id, name, object_attrs, object_category, process_id, result, signature, signature_id, subject, ta_windows_action, ta_windows_security_CategoryString, user_group, vendor_product	
xmlWinEventLog*	5158	Error_Code, app, dest, dvc, dvc_nt_host, event_id, id, name, parent_process_id, process_id, signature, signature_id, src_port, subject, ta_windows_action, transport, vendor_product	
xmlWinEventLog*	4793	CategoryString, Error_Code, app, dest, dvc, dvc_nt_host, event_id, id, name, signature, signature_id, subject, ta_windows_action, ta_windows_security_CategoryString, vendor_product	
xmlWinEventLog*	4664, 5058, 5142	Error_Code, app, dest, dvc, dvc_nt_host, event_id, file_name, file_path, id, name, process_id, signature, signature_id, subject, ta_windows_action, vendor_product	
xmlWinEventLog*	4697	Error_Code, app, dest, dvc, dvc_nt_host, event_id, id, name, process_id, service, service_name, signature, signature_id, start_mode, subject, ta_windows_action, vendor_product	
xmlWinEventLog*	4826, 5379, 6416	Error_Code, action, app, dest, dvc, dvc_nt_host, event_id, id, process_id, signature_id, status, ta_windows_action, vendor_product	
xmlWinEventLog*	4776		

Sourcetype	EventCode	Fields added	Fields removed
		app, dest, dvc, dvc_nt_host, event_id, id, name, process_id, signature, signature_id, subject, ta_windows_action, ta_windows_status, user_group, vendor_product	
xmlWinEventLog*	4771	app, dest, dvc, dvc_nt_host, event_id, id, name, process_id, service, service_name, signature, signature_id, subject, ta_windows_action, ta_windows_status, user_group, vendor_product	
xmlWinEventLog*	4616, 4658, 4660, 4670, 4674, 4904, 4985	Error_Code, app, dest, dvc, dvc_nt_host, event_id, id, name, parent_process_id, process, process_id, process_name, process_path, signature, signature_id, subject, ta_windows_action, vendor_product	
xmlWinEventLog*	4781	CategoryString, Error_Code, app, change_type, dest, dvc, dvc_nt_host, event_id, id, name, object_attrs, object_category, process_id, result, signature, signature_id, subject, ta_windows_action, ta_windows_security_CategoryString, vendor_product	
xmlWinEventLog*	5446, 5447, 5448, 5449, 5450	Error_Code, app, dest, dvc, dvc_nt_host, event_id, id, name, parent_process_id, process_id, signature, signature_id, subject, ta_windows_action, vendor_product	
xmlWinEventLog*	4770	Error_Code, app, dest, dvc, dvc_nt_host, event_id, id, name, process_id, service, service_id, service_name, signature, signature_id, subject, ta_windows_action, user_group, vendor_product	
xmlWinEventLog*	4717, 4718	Error_Code, app, change_type, dest, dvc, dvc_nt_host, event_id, id, name, object_attrs, object_category, process_id, result, signature, signature_id, subject, ta_windows_action, vendor_product	
xmlWinEventLog*	4912, 4931, 5141	Error_Code, app, dest, dvc, dvc_nt_host, event_id, id, name, signature, signature_id, subject, ta_windows_action, vendor_product	
xmlWinEventLog*	4656, 4661, 4663	Error_Code, app, dest, dvc, dvc_nt_host, event_id, id, name, object_file_name, object_file_path, parent_process_id, process, process_id, process_name, process_path, signature, signature_id, subject, ta_windows_action, vendor_product	
xmlWinEventLog*	4689	app, dest, dvc, dvc_nt_host, event_id, id, name, parent_process_id, process, process_id, process_name, process_path, signature, signature_id, subject, ta_windows_action, ta_windows_status, vendor_product	
xmlWinEventLog*	4778	Error_Code, app, dest, dvc, dvc_nt_host, event_id, id, name, process_id, signature, signature_id, src, subject, ta_windows_action, vendor_product	
xmlWinEventLog*	5024, 5025, 5033, 5478	Error_Code, app, dest, dvc, dvc_nt_host, event_id, id, name, process_id, service, service_name, signature, signature_id, subject, ta_windows_action, vendor_product	
xmlWinEventLog*	5145	Error_Code, app, dest, dvc, dvc_nt_host, event_id, file_name, file_path, id, name, process_id, signature, signature_id, src_ip, subject, ta_windows_action, vendor_product	
xmlWinEventLog*	4907	Error_Code, app, dest, dvc, dvc_nt_host, event_id, file_name, file_path, id, name, object_file_name, object_file_path, parent_process_id, process, process_id, process_name, process_path, signature, signature_id, subject, ta_windows_action, vendor_product	

Sourcetype	EventCode	Fields added	Fields removed

CIM model comparison for versions 7.0.0 and 8.1.2

Sourcetype	EventCode	Previous CIM model	New CIM model
XmlWinEventLog:Security	4625, 4672, 4771, 4776, 4957, 4624, 4648, 4769, 4768, 4932, 4933, 4931, 4948, 4670, 4673, 4674, 4800, 4778, 4779, 4770, 5450, 4985, 4902, 4907, 4906, 4904, 4662, 4663, 4660, 4661, 4664, 4705, 4704, 4701, 4700, 4703, 4702, 5152, 5156, 5154, 5025, 5024, 5145, 5140, 5141, 5142, 5441, 4713, 4797, 4793, 4658, 4656, 4653, 4798, 4799, 5031, 5033, 5034, 6145, 6144, 5137, 5136, 5157, 5442, 5444, 5447, 5448, 4647, 5449, 4634, 4963, 5045, 5044, 5379, 5041, 5040, 5043, 6416, 1104, 4627, 4622, 5058, 5059, 6272, 6417, 4947, 4944, 4611, 4610, 4616, 4614, 5061, 4690, 4697, 4696, 4699, 4698, 4688, 4689, 4946, 4945, 5446, 4950, 4953, 4954, 4826, 4956, 4608, 4817, 5478		Endpoint.Processes, Event_Signatures.Signatures, Endpoint.Services, Endpoint.Filesystem
XmlWinEventLog:Security	1108, 1101		Endpoint.Services, Change.Auditing_Changes, Change.Endpoint_Changes, Endpoint.Filesystem, Endpoint.Processes, Event_Signatures.Signatures
XmlWinEventLog:Security	4781, 4729, 4728, 4727, 4734, 4735, 4737, 4730, 4731, 4732, 4733, 4739, 4753, 4750, 4756, 4757, 4754, 4755, 4764, 4758		Endpoint.Services, Change.Endpoint_Changes, Endpoint.Filesystem, Change.Account_Management, Endpoint.Processes, Event_Signatures.Signatures
XmlWinEventLog:Security	1100, 1102		Event_Signatures.Signatures, Endpoint.Processes, Endpoint.Filesystem, Endpoint.Services
XmlWinEventLog:Security	4912, 4718, 4719, 4717, 4715, 4738, 1105, 4741, 4740, 4743, 4742, 4723, 4722, 4720, 4726, 4725, 4724, 4767		Change.Endpoint_Changes, Event_Signatures.Signatures, Endpoint.Processes, Endpoint.Filesystem, Endpoint.Services
XmlWinEventLog:Security	4657		Endpoint.Registry, Endpoint.Processes, Event_Signatures.Signatures, Endpoint.Services, Endpoint.Filesystem
XmlWinEventLog:Security	5158		Endpoint.Ports, Endpoint.Processes, Event_Signatures.Signatures, Endpoint.Services, Endpoint.Filesystem
XmlWinEventLog:Security	4801		Authentication, Endpoint.Processes, Event_Signatures.Signatures,

Sourcetype	EventCode	Previous CIM model	New CIM model
			Endpoint.Services, Endpoint.Filesystem

Field mapping comparison for versions 7.0.0 and 8.1.2

Source-type	EventCode	Fields added	Fields removed
xmlWinEventLog	4727, 4731, 4735, 4737, 4739, 4750, 4754, 4755	change_type, object_attrs, object_category, result, ta_windows_security_CategoryString, vendor_product	
xmlWinEventLog	4616, 4658, 4660, 4670, 4674, 4904, 4985	parent_process_id, process_name, process_path, vendor_product	
xmlWinEventLog	4771	service, service_name, vendor_product	Group_Name
xmlWinEventLog	4781	change_type, object_attrs, object_category, result, ta_windows_security_CategoryString, vendor_product	Group_Domain
xmlWinEventLog	4703	action, parent_process_id, process_name, process_path, status, vendor_product	Group_Domain, Group_Name
xmlWinEventLog	5156, 5157	transport, vendor_product	
xmlWinEventLog	5152, 5446, 5447, 5448, 5449, 5450	parent_process_id, vendor_product	
xmlWinEventLog	5024, 5025, 5033, 5034, 5478	service, service_name, vendor_product	
xmlWinEventLog	4907	file_name, file_path, object_file_name, object_file_path, parent_process_id, process_name, process_path, vendor_product	
xmlWinEventLog	4742, 4743	object_attrs, result, ta_windows_security_CategoryString, vendor_product	Group_Domain, Group_Name
xmlWinEventLog	4608, 4610, 4611, 4614, 4622, 4653, 4672, 4690, 4698, 4699, 4700, 4701, 4702, 4704, 4705, 4713, 4715, 4779, 4902, 4906, 4912, 4931, 4932, 4933, 4944, 4945, 4946, 4947, 4948, 4950, 4953, 4954, 4956, 4957, 4963, 5031, 5040, 5041, 5043, 5044, 5045, 5059, 5061, 5136, 5137, 5141, 5441, 5442, 5444, 6144, 6145, 6272	vendor_product	
xmlWinEventLog	4719	change_type, object_attrs, object_category, vendor_product	
xmlWinEventLog	4740	ta_windows_security_CategoryString, vendor_product	Group_Domain, Group_Name
xmlWinEventLog	4793	ta_windows_security_CategoryString, vendor_product	
xmlWinEventLog	4634, 4647, 4800, 4801	vendor_product	Group_Domain, Group_Name
xmlWinEventLog	1102	Caller_User_Name, object_attrs, src_user, status, vendor_product	
xmlWinEventLog	4776	vendor_product	Group_Name
xmlWinEventLog	4696	parent_process_id, vendor_product	

Source-type	EventCode	Fields added	Fields removed
			Group_Domain, Group_Name
xmlWinEventLog	1101, 1108	action, change_type, object_attrs, object_category, status, vendor_product	
xmlWinEventLog	4657	object_file_name, object_file_path, parent_process_id, process_name, process_path, registry_path, registry_value_name, registry_value_type, vendor_product	
xmlWinEventLog	4723, 4724	object_attrs, ta_windows_security_CategoryString, vendor_product	Group_Domain, Group_Name
xmlWinEventLog	4741	object_attrs, result, status, ta_windows_security_CategoryString, vendor_product	Group_Domain, Group_Name
xmlWinEventLog	5154	parent_process_id, transport, vendor_product	
xmlWinEventLog	4778	src, vendor_product	
xmlWinEventLog	4768, 4769, 4770	service, service_id, service_name, vendor_product	Group_Domain, Group_Name
xmlWinEventLog	4627, 4797, 4798	action, status, vendor_product	Group_Domain, Group_Name
xmlWinEventLog	4720, 4722, 4725, 4726, 4738, 4767	result, ta_windows_security_CategoryString, vendor_product	Group_Domain, Group_Name
xmlWinEventLog	4697	service, service_name, start_mode, vendor_product	
xmlWinEventLog	4688	Process_Command_Line, Token_Elevation_Type_id, new_process, new_process_id, new_process_name, parent_process, parent_process_id, parent_process_name, parent_process_path, process, process_command_line_arguments, process_command_line_process, process_exec, process_name, process_path, vendor_product	Group_Domain, Group_Name
xmlWinEventLog	5158	parent_process_id, src_port, transport, vendor_product	
xmlWinEventLog	4689, 6417	action, parent_process_id, process_name, process_path, status, vendor_product	
xmlWinEventLog	4656, 4661, 4663	object_file_name, object_file_path, parent_process_id, process_name, process_path, vendor_product	
xmlWinEventLog	4624, 4625, 4648	parent_process_id, process_name, process_path, vendor_product	Group_Domain, Group_Name
xmlWinEventLog	4662, 4817	object_file_name, object_file_path, vendor_product	
xmlWinEventLog	4717, 4718	change_type, object_attrs, object_category, result, vendor_product	
xmlWinEventLog	4664, 5058, 5142, 5145	file_name, file_path, vendor_product	
xmlWinEventLog	4673	parent_process_id, service, vendor_product	
xmlWinEventLog	1100	object_attrs, status, vendor_product	
xmlWinEventLog	1104, 1105, 4799, 4826, 5379, 6416	action, status, vendor_product	
xmlWinEventLog	5140	file_name, vendor_product	

Source-type	EventCode	Fields added	Fields removed
xmlWinEventLog	4728, 4729, 4730, 4732, 4733, 4734, 4753, 4756, 4757, 4758, 4764	change_type, object_category, result, ta_windows_security_CategoryString, vendor_product	