Events Full Reference (Events Data Dictionary)

Last updated: Sep. 4, 2025

Overview

This reference contains all sensor and non-sensor events and their available documentation in one location.

Additional event resources

- **About Events [/documentation/page/he24b63c/about-events]** Learn about sensor and non-sensor events, and the references available to learn more about them.
- **Sensor Events Search [/documentation/page/ic497590/searchable-event-reference]** Search and filter results to find reference info about events sent from Falcon sensors.
- **Non-Sensor Events Reference [/documentation/page/d88d9ed6/streaming-api-event-dictionary]** Info about all non-sensor events.
- **Sensor Events Index [/documentation/page/qd3eb00a/sensor-events-index]** A table listing all sensor events and the OSes and platforms that send them.

Introduction

The Events Data Dictionary provides reference information about the events found in these locations:

- Investigate > Search > Event search [/investigate/event-search], powered by the same technology as Falcon LogScale
- Investigate > Search > Advanced event search [/investigate/search], powered by the same technology as Falcon LogScale

Event Search helps you get complete visibility into all hosts running the Falcon sensor.

This guide contains:

- A summary of events by platform
- Names and descriptions of each event
- Some key data fields for the most common events
- Copy-and-paste sample queries for the most common events

Before you begin

Searching

For more info about the search options powered by the same technology as Falcon LogScale, see Searching Events [/documentation/category/ic53d1e6/event-investigation/searching-events].

Sample queries

For some sample queries, you must insert your own data. For example, you can use a query to show a list of `EndOfProcess` events on a specific host that you specify.

Go to **Investigate > Search > Advanced event search** and run this query:

```
#event_simpleName=EndOfProcess ComputerName=my-host-name
| groupBy(ComputerName, function=(sum("MaxThreadCount", as=MaxThreadCount)))
```

For more sample queries, see Hunting Queries: CrowdStrike Query Language [/documentation/category/y907ff6d/event-investigation/hunting-queries].

Key data fields

These are some of the most commonly used data fields associated with events. Fields that begin with lowercase letters are present in all events.

Field Name	Description	Example value
`aid`	The sensor ID. This value is unique to each installation of a Falcon sensor. When a sensor is reinstalled, the host gets a new aid. In those situations, a single host could have multiple `aid` values over time.	`"a26a23c103cb4c9s5c39aa09effa5662"`
`aip`	The sensor's IP, as seen from the CrowdStrike cloud. This is typically the public IP of the sensor. This helps determine the location of a computer, depending on your network.	`"#.##.#.###"`
`ComputerName`	The name of the host.	`"my-host-name"`
`ContextProcessId`	The unique ID of a process that was spawned by another process. For example, if Process 1 spawns Process 2, the `TargetProcessId` of Process 1 will match the `ContextProcessId` of Process 2.	`"22603276734"`
`ContextThreadId`	UTID of thread originating this event.	`"395202677966"`
`ContextTimeStamp`	The time at which an event occurred on the system, as seen by the sensor. Not to be confused with `timestamp` which is the time the event was received by the cloud.	`"1309294523.160"`
`event_platform`	The platform on which the sensor is running.	`"Win"/"Mac"/"Lin"`
`event_simpleName`	The name of the event.	`"SuspiciousDnsRequest"`
`FileName`	The name of the file.	`"my_file.docx"`
`FilePath`	The full path of the file, including the file name.	`"\Device\HarddiskVolume1\sds2\1043\asdj64.exe"`
`TargetProcessId`	The unique ID of a target process. This field exists in almost all events, and it represents the ID of the process that is responsible for the activity of the event in focus. For example, the `TargetProcessId` of a process that performed thread injection in an `InjectedThread` event.	`"167558096500"`
`timestamp`	Timestamp when the event was received by the CrowdStrike cloud. Not to be confused with the time the event was generated locally on the system. `timestamp` is epoch formatted. To make timestamps reader-friendly, add the search parameter that corresponds to your environment. `| ProcessStartTime:=ProcessStartTime*1000 | ProcessStartTime:=formatTime(format="%F %T.%L", field="ProcessStartTime")`	`1508334994001`
`_time`	Timestamp of the moment that the event was received by the CrowdStrike cloud. This is not to be confused with the time the event was generated locally on the system. This is the timestamp of the event from the cloud's point of view. This value can be converted to any time format and can be used for calculations.	`"10/19/2017 18:10:29.396"`
`TreeId`	If this event is part of a detection tree, the tree ID it is part of.	`"42958187116"`

Sensor events

AgentConnect

Description

Platforms: *macOS, Windows, Linux, Falcon Container, Kubernetes, Android, iOS*
This event is generated when the sensor successfully connects to the cloud.

Platforms: *Windows Legacy*

Fields: macOS, Linux, Falcon Container

Field	Description
ConfigurationVersion	
ConfigIDBase	
ConfigIDBuild	
ConfigIDPlatform	Values: • AGENT_PLATFORM_WIN7_X86 (0x0001) • AGENT_PLATFORM_WIN7_X64 (0x0002) • AGENT_PLATFORM_MACOS (0x0004) • AGENT_PLATFORM_LINUX (0x0008) • AGENT_PLATFORM_ANDROID (0x0010) • AGENT_PLATFORM_IOS (0x0020) • AGENT_PLATFORM_LINUX_S390X (0x0040) • AGENT_PLATFORM_LINUX_AARCH64 (0x0080) • AGENT_PLATFORM_LINUX_LUMOS_X64 (0x0100) • AGENT_PLATFORM_WINDOWS_AARCH64 (0x0200) • AGENT_PLATFORM_LINUX_K8S_X64 (0x0400) • AGENT_PLATFORM_LINUX_PPC64 (0x0800) • AGENT_PLATFORM_LINUX_PPC64LE (0x1000) • AGENT_PLATFORM_WIN_LEGACY_X86 (0x2000) • AGENT_PLATFORM_WIN_LEGACY_X64 (0x4000) • AGENT_PLATFORM_VMCLUSTER (0x8000) • AGENT_PLATFORM_LINUX_K8S_AARCH64 (0x10000) • AGENT_PLATFORM_LINUX_LUMOS_AARCH64 (0x20000)
ConnectTime	
PreviousConnectTime	
FailedConnectCount	
ConnectType	The type of the connection Values: • CONNECT_INVALID (0) • CONNECT_DIRECT (1) • CONNECT_WPAD (2) • CONNECT_IE_AUTOPROXY (3) • CONNECT_IE_PROXY (4) • CONNECT_SIMPLESTORE_AUTOCONFIG (5) • CONNECT_CACHE_PROXY (6) • CONNECT_PERSISTED_PROXY (7) • CONNECT_APP_PROXY (8) • CONNECT_DIRECT_DNS_BYPASS (9) • CONNECT_CACHE_PROXYFORURL_WPAD (10) • CONNECT_CACHE_PROXYFORURL_PACURL (11) • CONNECT_CACHE_PROXYFORURL_IE_PACURL (12)
NetworkContainmentState	Values: • NETWORK_CONTAINMENT_STATE_UNCONTAINED (0x00) • NETWORK_CONTAINMENT_STATE_CONTAINED (0x01)
ProvisionState	Values: • SENSOR_NOT_PROVISIONED (0x0) • SENSOR_PROVISIONED (0x1)
VerifiedCertificate	
ConnectionAddressIP4	
ConnectionAddressIP6	

Fields: Windows Legacy

Field	Description
ConfigurationVersion	
ConfigIDBase	
ConfigIDBuild	
ConfigIDPlatform	Values:

Field	Description
	• AGENT_PLATFORM_WIN7_X86 (0x0001) • AGENT_PLATFORM_WIN7_X64 (0x0002) • AGENT_PLATFORM_MACOS (0x0004) • AGENT_PLATFORM_LINUX (0x0008) • AGENT_PLATFORM_ANDROID (0x0010) • AGENT_PLATFORM_IOS (0x0020) • AGENT_PLATFORM_LINUX_S390X (0x0040) • AGENT_PLATFORM_LINUX_AARCH64 (0x0080) • AGENT_PLATFORM_LINUX_LUMOS_X64 (0x0100) • AGENT_PLATFORM_WINDOWS_AARCH64 (0x0200) • AGENT_PLATFORM_LINUX_K8S_X64 (0x0400) • AGENT_PLATFORM_LINUX_PPC64 (0x0800) • AGENT_PLATFORM_LINUX_PPC64LE (0x1000) • AGENT_PLATFORM_WIN_LEGACY_X86 (0x2000) • AGENT_PLATFORM_WIN_LEGACY_X64 (0x4000) • AGENT_PLATFORM_VMCLUSTER (0x8000) • AGENT_PLATFORM_LINUX_K8S_AARCH64 (0x10000) • AGENT_PLATFORM_LINUX_LUMOS_AARCH64 (0x20000)
ConnectTime	
PreviousConnectTime	
FailedConnectCount	
ConnectType	The type of the connection Values: • CONNECT_INVALID (0) • CONNECT_DIRECT (1) • CONNECT_WPAD (2) • CONNECT_IE_AUTOPROXY (3) • CONNECT_IE_PROXY (4) • CONNECT_SIMPLESTORE_AUTOCONFIG (5) • CONNECT_CACHE_PROXY (6) • CONNECT_PERSISTED_PROXY (7) • CONNECT_APP_PROXY (8) • CONNECT_DIRECT_DNS_BYPASS (9) • CONNECT_CACHE_PROXYFORURL_WPAD (10) • CONNECT_CACHE_PROXYFORURL_PACURL (11) • CONNECT_CACHE_PROXYFORURL_IE_PACURL (12)
VerifiedCertificate	
ConnectionAddressIP4	
ConnectionAddressIP6	

Fields: Windows

Field	Description
ConfigurationVersion	
ConfigIDBase	
ConfigIDBuild	
ConfigIDPlatform	Values: • AGENT_PLATFORM_WIN7_X86 (0x0001) • AGENT_PLATFORM_WIN7_X64 (0x0002) • AGENT_PLATFORM_MACOS (0x0004) • AGENT_PLATFORM_LINUX (0x0008) • AGENT_PLATFORM_ANDROID (0x0010) • AGENT_PLATFORM_IOS (0x0020) • AGENT_PLATFORM_LINUX_S390X (0x0040) • AGENT_PLATFORM_LINUX_AARCH64 (0x0080) • AGENT_PLATFORM_LINUX_LUMOS_X64 (0x0100) • AGENT_PLATFORM_WINDOWS_AARCH64 (0x0200) • AGENT_PLATFORM_LINUX_K8S_X64 (0x0400) • AGENT_PLATFORM_LINUX_PPC64 (0x0800) • AGENT_PLATFORM_LINUX_PPC64LE (0x1000) • AGENT_PLATFORM_WIN_LEGACY_X86 (0x2000) • AGENT_PLATFORM_WIN_LEGACY_X64 (0x4000)

Field	Description
	• AGENT_PLATFORM_VMCLUSTER (0x8000) • AGENT_PLATFORM_LINUX_K8S_AARCH64 (0x10000) • AGENT_PLATFORM_LINUX_LUMOS_AARCH64 (0x20000)
ConnectTime	
PreviousConnectTime	
FailedConnectCount	
ConnectType	The type of the connection Values: • CONNECT_INVALID (0) • CONNECT_DIRECT (1) • CONNECT_WPAD (2) • CONNECT_IE_AUTOPROXY (3) • CONNECT_IE_PROXY (4) • CONNECT_SIMPLESTORE_AUTOCONFIG (5) • CONNECT_CACHE_PROXY (6) • CONNECT_PERSISTED_PROXY (7) • CONNECT_APP_PROXY (8) • CONNECT_DIRECT_DNS_BYPASS (9) • CONNECT_CACHE_PROXYFORURL_WPAD (10) • CONNECT_CACHE_PROXYFORURL_PACURL (11) • CONNECT_CACHE_PROXYFORURL_IE_PACURL (12)
NetworkContainmentState	Values: • NETWORK_CONTAINMENT_STATE_UNCONTAINED (0x00) • NETWORK_CONTAINMENT_STATE_CONTAINED (0x01)
ConnectionProtocol	Values: • SP_PROT_PCT1_SERVER (1) • SP_PROT_PCT1_CLIENT (2) • SP_PROT_SSL2_SERVER (4) • SP_PROT_SSL2_CLIENT (8) • SP_PROT_SSL3_SERVER (16) • SP_PROT_SSL3_CLIENT (32) • SP_PROT_TLS1_SERVER (64) • SP_PROT_TLS1_CLIENT (128) • SP_PROT_TLS1_1_SERVER (256) • SP_PROT_TLS1_1_CLIENT (512) • SP_PROT_TLS1_2_SERVER (1024) • SP_PROT_TLS1_2_CLIENT (2048)
ConnectionCipher	Values: • CALG_3DES (0x00006603) • CALG_AES_128 (0x0000660e) • CALG_AES_256 (0x00006610) • CALG_DES (0x00006601) • CALG_RC2 (0x00006602) • CALG_RC4 (0x00006801) • NO_ENCRYPTION (0)
ConnectionCipherStrength	
ConnectionHash	Values: • CALG_MD5 (0x00008003) • CALG_SHA (0x00008004) • CALG_SHA_256 (0x0000800c) • CALG_SHA_384 (0x0000800d)
ConnectionHashStrength	
ConnectionExchange	Values: • CALG_RSA_KEYX (0x0000a400) • CALG_DH_EPHEM (0x0000aa02)
ConnectionExchangeStrength	
ProvisionState	Values: • SENSOR_NOT_PROVISIONED (0x0) • SENSOR_PROVISIONED (0x1)
VerifiedCertificate	
ConnectionAddressIP4	

Field	Description
ConnectionAddressIP6	

Fields: Kubernetes

Field	Description
K8SClusterId	
ConfigurationVersion	
ConfigIDBase	
ConfigIDBuild	
ConfigIDPlatform	Values: • AGENT_PLATFORM_WIN7_X86 (0x0001) • AGENT_PLATFORM_WIN7_X64 (0x0002) • AGENT_PLATFORM_MACOS (0x0004) • AGENT_PLATFORM_LINUX (0x0008) • AGENT_PLATFORM_ANDROID (0x0010) • AGENT_PLATFORM_IOS (0x0020) • AGENT_PLATFORM_LINUX_S390X (0x0040) • AGENT_PLATFORM_LINUX_AARCH64 (0x0080) • AGENT_PLATFORM_LINUX_LUMOS_X64 (0x0100) • AGENT_PLATFORM_WINDOWS_AARCH64 (0x0200) • AGENT_PLATFORM_LINUX_K8S_X64 (0x0400) • AGENT_PLATFORM_LINUX_PPC64 (0x0800) • AGENT_PLATFORM_LINUX_PPC64LE (0x1000) • AGENT_PLATFORM_WIN_LEGACY_X86 (0x2000) • AGENT_PLATFORM_WIN_LEGACY_X64 (0x4000) • AGENT_PLATFORM_VMCLUSTER (0x8000) • AGENT_PLATFORM_LINUX_K8S_AARCH64 (0x10000) • AGENT_PLATFORM_LINUX_LUMOS_AARCH64 (0x20000)
ConnectTime	
PreviousConnectTime	
FailedConnectCount	
ConnectType	The type of the connection Values: • CONNECT_INVALID (0) • CONNECT_DIRECT (1) • CONNECT_WPAD (2) • CONNECT_IE_AUTOPROXY (3) • CONNECT_IE_PROXY (4) • CONNECT_SIMPLESTORE_AUTOCONFIG (5) • CONNECT_CACHE_PROXY (6) • CONNECT_PERSISTED_PROXY (7) • CONNECT_APP_PROXY (8) • CONNECT_DIRECT_DNS_BYPASS (9) • CONNECT_CACHE_PROXYFORURL_WPAD (10) • CONNECT_CACHE_PROXYFORURL_PACURL (11) • CONNECT_CACHE_PROXYFORURL_IE_PACURL (12)
NetworkContainmentState	Values: • NETWORK_CONTAINMENT_STATE_UNCONTAINED (0x00) • NETWORK_CONTAINMENT_STATE_CONTAINED (0x01)
ProvisionState	Values: • SENSOR_NOT_PROVISIONED (0x0) • SENSOR_PROVISIONED (0x1)
VerifiedCertificate	
ConnectionAddressIP4	
ConnectionAddressIP6	

Fields: Android, iOS

Field	Description
ConfigurationVersion	
ConfigIDBase	
ConfigIDBuild	
ConfigIDPlatform	Values: • AGENT_PLATFORM_WIN7_X86 (0x0001) • AGENT_PLATFORM_WIN7_X64 (0x0002) • AGENT_PLATFORM_MACOS (0x0004) • AGENT_PLATFORM_LINUX (0x0008) • AGENT_PLATFORM_ANDROID (0x0010) • AGENT_PLATFORM_IOS (0x0020) • AGENT_PLATFORM_LINUX_S390X (0x0040) • AGENT_PLATFORM_LINUX_AARCH64 (0x0080) • AGENT_PLATFORM_LINUX_LUMOS_X64 (0x0100) • AGENT_PLATFORM_WINDOWS_AARCH64 (0x0200) • AGENT_PLATFORM_LINUX_K8S_X64 (0x0400) • AGENT_PLATFORM_LINUX_PPC64 (0x0800) • AGENT_PLATFORM_LINUX_PPC64LE (0x1000) • AGENT_PLATFORM_WIN_LEGACY_X86 (0x2000) • AGENT_PLATFORM_WIN_LEGACY_X64 (0x4000) • AGENT_PLATFORM_VMCLUSTER (0x8000) • AGENT_PLATFORM_LINUX_K8S_AARCH64 (0x10000) • AGENT_PLATFORM_LINUX_LUMOS_AARCH64 (0x20000)
ConnectTime	
PreviousConnectTime	
VerifiedCertificate	
NetworkContainmentState	Values: • NETWORK_CONTAINMENT_STATE_UNCONTAINED (0x00) • NETWORK_CONTAINMENT_STATE_CONTAINED (0x01)
ProvisionState	Values: • SENSOR_NOT_PROVISIONED (0x0) • SENSOR_PROVISIONED (0x1)

top [#top]

ActiveDirectoryInteractiveDomainLogon

Description

Platforms: *Windows*
Indicates an interactive logon to an Active Directry domain handled by a Domain Controller. The interactive logon is combined of initial authentication following by some service access events.

Fields: Windows

Field	Description
RemotePortSample	
LocalAddressIP4Sample	
LocalPortSample	
ContextTimeStamp	System time of event creation.
AuthenticationActivityId	
ActiveDirectoryAuthenticationMethod	The mechanism used to authenticate to the Active Directory domain. This field is set for all Active Directory activity events, not just authentications. For non-authentication events, such as an LDAP search, this field indicates the mechanism used for the preceding - or 'incorporated' - authentication that was used to authorize this activity. The value of this field and the associated event type indicates which protocol-specific fields might be set. Values: • KERBEROS (0) • NTLM_V1 (1) • NTLM_V2 (2) • SIMPLE_BIND (3)

Field	Description
	• NO_AUTHENTICATION (4) • UNKNOWN_NTLM (5)
SourceAccountSamAccountName	The `sAMAccountName` value of the account bound with this activity. Only set if available as part of the raw, sniffed data, and usually set alongside the `SourceAccountDomain` field. For stronger identification, the `SourceAccountObjectSid` or `SourceAccountObjectGuid` fields are better foreign keys - although they may not be available in some cases, such as authentication failures.
SourceAccountDomain	The domain that the account bound with this activity is a member of.
SourceAccountUserPrincipal	The `UserPrincipalName` value of the account bound with this activity. Only set if available as part of the raw, sniffed data. For stronger identification, the `SourceAccountObjectSid` or `SourceAccountObjectGuid` fields are better foreign keys - although they may not be available in some cases, such as authentication failures.
SourceAccountObjectSid	The `objectSid` value of the account bound with this activity.
SourceAccountObjectGuid	The `objectGUID` value of the account bound with this activity.
SourceEndpointAddressIP4	The IP address of the endpoint from which this activity originates. Mutually exclusive with the `SourceEndpointAddressIP6` field.
SourceEndpointAddressIP6	The IP address of the endpoint from which this activity originates. Mutually exclusive with the `SourceEndpointAddressIP4` field.
SourceEndpointNetworkType	The network type to which the `SourceEndpointAddressIP4` or `SourceEndpointAddressIP6` value belongs, depending on customer configuration. **Values:** • INTERNAL (0x1) • VPN (0x2) • WIRELESS (0x4) • NAT (0x8) • PUBLIC (0x10) • UNKNOWN (0x20)
SourceEndpointNetworkTag	The network tag to which the `SourceEndpointAddressIP4` or `SourceEndpointAddressIP6` value belongs, depending on customer configuration.
SourceEndpointHostName	The hostname of the source endpoint. Might originate either directly from the raw event data or from one of the host association resolution methods. When available, either the `SourceEndpointAccountObjectSid` or `SourceEndpointAccountObjectGuid` fields are superior for use as foreign keys.
SourceEndpointAccountObjectSid	The `objectSid` value of the source endpoint account.
SourceEndpointAccountObjectGuid	The `objectGUID` value of the source endpoint account.
TargetDomainControllerObjectSid	The `objectSid` of the domain controller (DC) account that handled the request.
TargetDomainControllerObjectGuid	The `objectGUID` of the domain controller (DC) account that handled the request.
ActivityId	A globally-unique identifier for the activity event.

top [#top]

ActiveDirectoryAuthenticationFailure

Description

Platforms: *Windows*
Indicates that the Domain Controller handled one or more failed authentications by an account on an endpoint.

Fields: Windows

Field	Description
ActivityId	A globally-unique identifier for the activity event.
AggregationWindowTimestamp	The nominal, floored to start-of-minute aggregation window timestamp.
AggregationEarliestTimestamp	The exact timestamp of the least recent activity in the aggregation window. Guaranteed to be within the same nominal minute as the `AggregationLatestTimestamp` and `AggregationWindowTimestamp` fields.
AggregationLatestTimestamp	If aggregation has occurred, that is, the `AggregationActivityCount` field is greater than 1, then this field is set to the timestamp of the most recent activity in the aggregation window.

Field	Description
	The value is guaranteed to be within the same nominal minute as AggregationEarliestTimestamp and AggregationWindowTimestamp.
AggregationActivityCount	An integer value indicating how many actual activity events are represented by this event. Guaranteed to be set if aggregation has occurred. If not set, or the value is 1, assume a single-activity event.
ActiveDirectoryAuthenticationMethod	The mechanism used to authenticate to the Active Directory domain. This field is set for all Active Directory activity events, not just authentications. For non-authentication events, such as an LDAP search, this field indicates the mechanism used for the preceding - or 'incorporated' - authentication that was used to authorize this activity. The value of this field and the associated event type indicates which protocol-specific fields might be set. **Values:** • KERBEROS (0) • NTLM_V1 (1) • NTLM_V2 (2) • SIMPLE_BIND (3) • NO_AUTHENTICATION (4) • UNKNOWN_NTLM (5)
ActiveDirectoryDataProtocol	The protocol associated with the event, if any, rather than the authentication mechanism facilitating it, which is indicated by the ActiveDirectoryAuthenticationMethod field. **Values:** • LDAP (0) • DCE_RPC (1) • RDP (2) • SMB (3) • SMB_1 (4) • SMB_2_0_2 (5) • SMB_2_1 (6) • SMB_3_0 (7) • SMB_3_0_2 (8) • SMB_3_1_1 (9)
SourceEndpointAddressIP4	The IP address of the endpoint from which this activity originates. Mutually exclusive with the SourceEndpointAddressIP6 field.
SourceEndpointAddressIP6	The IP address of the endpoint from which this activity originates. Mutually exclusive with the SourceEndpointAddressIP4 field.
SourceEndpointNetworkType	The network type to which the SourceEndpointAddressIP4 or SourceEndpointAddressIP6 value belongs, depending on customer configuration. **Values:** • INTERNAL (0x1) • VPN (0x2) • WIRELESS (0x4) • NAT (0x8) • PUBLIC (0x10) • UNKNOWN (0x20)
SourceEndpointNetworkTag	The network tag to which the SourceEndpointAddressIP4 or SourceEndpointAddressIP6 value belongs, depending on customer configuration.
SourceEndpointHostName	The hostname of the source endpoint. Might originate either directly from the raw event data or from one of the host association resolution methods. When available, either the SourceEndpointAccountObjectSid or SourceEndpointAccountObjectGuid fields are superior for use as foreign keys.
SourceEndpointHostNameResolutionMethod	The method used to resolve the SourceEndpointHostName field, given the value of the SourceEndpointAddress field. **Values:** • RAW_PACKET_DATA (0) • TRAFFIC_CACHE (1) • KERBEROS_TICKET_CACHE (2) • REVERSE_LOOKUP (3) • FORWARD_LOOKUP (4) • NETBIOS_LOOKUP (5) • DOMAIN_CONTROLLER (6) • RDP_NEGOTIATION (7) • ENTITY_HOSTNAME (8) • KERBEROS_TICKET_CLOUD_CACHE (9)
SourceEndpointAccountObjectSid	The objectSid value of the source endpoint account.

Field	Description
SourceEndpointAccountObjectGuid	The `objectGUID` value of the source endpoint account.
SourceAccountType	The type of the Active Directory bound with this activity. **Values:** • **USER (0)** • **COMPUTER (1)** • **GROUP (2)** • **CLOUD_SERVICE (3)**
SourceAccountSamAccountName	The `sAMAccountName` value of the account bound with this activity. Only set if available as part of the raw, sniffed data, and usually set alongside the `SourceAccountDomain` field. For stronger identification, the `SourceAccountObjectSid` or `SourceAccountObjectGuid` fields are better foreign keys - although they may not be available in some cases, such as authentication failures.
SourceAccountDomain	The domain that the account bound with this activity is a member of.
SourceAccountUserPrincipal	The `UserPrincipalName` value of the account bound with this activity. Only set if available as part of the raw, sniffed data. For stronger identification, the `SourceAccountObjectSid` or `SourceAccountObjectGuid` fields are better foreign keys - although they may not be available in some cases, such as authentication failures.
SourceAccountUserName	The username associated with this activity.
SourceAccountObjectSid	The `objectSid` value of the account bound with this activity.
SourceAccountObjectGuid	The `objectGUID` value of the account bound with this activity.
NtlmProofStrHashSample	The NTLM challenge signature.
NtlmAvIds	The NTLM attribute/value (AV) IDs as a buffer of little-endian uint32 values, that retains the order specified by the client.
NtlmAvFlags	A mask of NTLM attribute/value (AV) flags, indicating server or client configuration. **Values:** • **CONSTRAINED_AUTHENTICATION (0x00000001)** • **MESSAGE_INTEGRITY (0x00000002)** • **UNTRUSTED_SPN_SOURCE (0x00000004)**
SourceEndpointRawNtlmHostName	The source endpoint's hostname, if available, as specified in the NetLogon credentials. This value may differ from the value of the `SourceEndpointHostName` field, which may be resolved from the value of the `SourceEndpointAddressIP4` or `SourceEndpointAddressIP6` fields.
TargetServerHostName	The hostname of the machine that authenticated in the NTLM NetLogon channel. Only set for NTLM NetLogon activities.
TargetServerAddressIP4	The IP address of the machine that authenticated in the NTLM NetLogon channel. Only set for NTLM NetLogon activities. Mutually exclusive with the `TargetServerAddressIP6` field.
TargetServerAddressIP6	The IP address of the machine that authenticated in the NTLM NetLogon channel. Only set for NTLM NetLogon activities Mutually exclusive with the `TargetServerAddressIP4` field.
TargetDomainControllerObjectSid	The `objectSid` of the domain controller (DC) account that handled the request.
TargetDomainControllerObjectGuid	The `objectGUID` of the domain controller (DC) account that handled the request.
DebugInfoUnicode	
RemotePortSample	
LocalAddressIP4Sample	
LocalPortSample	
TargetServiceAccessIdentifier	The raw target service identifier of a service access request, which could be either an SPN, a user principal, or just the `sAMAccountName`. As a single Active Directory account may be associated with multiple, distinct services, you can use this field to identify the accessed service, even if the `TargetAccountObjectGuid` or `TargetAccountObjectSid` fields are available.
KerberosErrorCode	The cause for a Kerberos authentication or service access failure. **Values:** • **KDC_ERR_NAME_EXP (1)** • **KDC_ERR_SERVICE_EXP (2)** • **KDC_ERR_BAD_PVNO (3)** • **KDC_ERR_C_OLD_MAST_KVNO (4)** • **KDC_ERR_S_OLD_MAST_KVNO (5)** • **KDC_ERR_C_PRINCIPAL_UNKNOWN (6)** • **KDC_ERR_S_PRINCIPAL_UNKNOWN (7)**

Field	Description
	• KDC_ERR_PRINCIPAL_NOT_UNIQUE (8) • KDC_ERR_NULL_KEY (9) • KDC_ERR_CANNOT_POSTDATE (10) • KDC_ERR_NEVER_VALID (11) • KDC_ERR_POLICY (12) • KDC_ERR_BADOPTION (13) • KDC_ERR_ENCTYPE_NOSUPP (14) • KDC_ERR_SUMTYPE_NOSUPP (15) • KDC_ERR_PADATA_TYPE_NOSUPP (16) • KDC_ERR_TRTYPE_NOSUPP (17) • KDC_ERR_CLIENT_REVOKED (18) • KDC_ERR_SERVICE_REVOKED (19) • KDC_ERR_TGT_REVOKED (20) • KDC_ERR_CLIENT_NOTYET (21) • KDC_ERR_SERVICE_NOTYET (22) • KDC_ERR_KEY_EXP (23) • KDC_ERR_PREAUTH_FAILED (24) • KDC_ERR_PREAUTH_REQUIRED (25) • KDC_ERR_SERVER_NOMATCH (26) • KDC_ERR_PATH_NOT_ACCEPTED (28) • KDC_ERR_SVC_UNAVAILABLE (29) • KRB_AP_ERR_BAD_INTEGRITY (31) • KRB_AP_ERR_TKT_EXPIRED (32) • KRB_AP_ERR_TKT_NYV (33) • KRB_AP_ERR_REPEAT (34) • KRB_AP_ERR_NOT_US (35) • KRB_AP_ERR_BADMATCH (36) • KRB_AP_ERR_SKEW (37) • KRB_AP_ERR_BADADDR (38) • KRB_AP_ERR_BADVERSION (39) • KRB_AP_ERR_MSG_TYPE (40) • KRB_AP_ERR_MODIFIED (41) • KRB_AP_ERR_BADORDER (42) • KRB_AP_ERR_BADKEYVER (44) • KRB_AP_ERR_NOKEY (45) • KRB_AP_ERR_MUT_FAIL (46) • KRB_AP_ERR_BADDIRECTION (47) • KRB_AP_ERR_METHOD (48) • KRB_AP_ERR_BADSEQ (49) • KRB_AP_ERR_INAPP_CKSUM (50) • KRB_AP_PATH_NOT_ACCEPTED (51) • KRB_ERR_RESPONSE_TOO_BIG (52) • KRB_ERR_GENERIC (60) • KRB_ERR_FIELD_TOOLONG (61) • KDC_ERR_CLIENT_NOT_TRUSTED (62) • KDC_ERR_KDC_NOT_TRUSTED (63) • KDC_ERR_INVALID_SIG (64) • KDC_ERR_DH_KEY_PARAMETERS_NOT_ACCEPTED (65) • KDC_ERR_CERTIFICATE_MISMATCH (66) • KRB_AP_ERR_NO_TGT (67) • KDC_ERR_WRONG_REALM (68) • KRB_AP_ERR_USER_TO_USER_REQUIRED (69) • KDC_ERR_CANT_VERIFY_CERTIFICATE (70) • KDC_ERR_INVALID_CERTIFICATE (71) • KDC_ERR_REVOKED_CERTIFICATE (72) • KDC_ERR_REVOCATION_STATUS_UNKNOWN (73) • KDC_ERR_REVOCATION_STATUS_UNAVAILABLE (74) • KDC_ERR_CLIENT_NAME_MISMATCH (75) • KDC_ERR_INCONSISTENT_KEY_PURPOSE (77) • KDC_ERR_DIGEST_IN_CERT_NOT_ACCEPTED (78) • KDC_ERR_PA_CHECKSUM_MUST_BE_INCLUDED (79) • KDC_ERR_DIGEST_IN_SIGNED_DATA_NOT_ACCEPTED (80) • KDC_ERR_PUBLIC_KEY_ENCRYPTION_NOT_SUPPORTED (81) • KRB_AP_ERR_IAKERB_KDC_NOT_FOUND (85) • KRB_AP_ERR_IAKERB_KDC_NO_RESPONSE (86)
KerberosRequestTicketHashSample	A hashed version of the Kerberos ticket (either TGT or TGS) associated with the first activity in the activity aggregation window. Use this field to correlate ticket-generation activity with successful ticket usage.

Field	Description
	Note: As tickets cannot be part of the aggregation-key tuple, correlating activities this way is inherently opportunistic and isn't guaranteed to succeed.
KDCOptions	A mask of the Kerberos option flags set by the client. **Values:** • FORWARDABLE (0x40000000) • FORWARDED (0x20000000) • PROXIABLE (0x10000000) • PROXY (0x08000000) • ALLOW_POSTDATE (0x04000000) • POSTDATED (0x02000000) • RENEWABLE (0x00800000) • CNAME_IN_ADDL_TKT (0x00020000) • CANONICALIZE (0x00010000) • REQUEST_ANONYMOUS (0x00008000) • DISABLE_TRANSITED_CHECK (0x00000020) • RENEWABLE_OK (0x00000010) • ENC_TKT_IN_SKEY (0x00000008) • RENEW (0x00000002) • VALIDATE (0x00000001)
DesiredKerberosEncryptionTypes	A variable sized buffer of the encryption types specified by the Kerberos client, as little-endian uint32 values, which retain the order specified by the client.
KerberosAnomaly	A mask of anomaly classifications which apply to the Kerberos flow. **Values:** • MISSING_LOGON_SERVER_IN_REQUEST_TICKET (0x00000001) • DEFAULT_PASSWORD_LAST_SET_VALUE_IN_REQUEST_TICKET (0x00000002) • UNEXPECTED_SID_IN_REQUEST_TICKET (0x00000004) • UNEXPECTED_PRIMARY_GROUP_ID_IN_REQUEST_TICKET (0x00000008) • UNEXPECTED_GROUPS_ID_IN_REQUEST_TICKET (0x00000010) • UNEXPECTED_RESOURCE_GROUPS_ID_IN_REQUEST_TICKET (0x00000020) • UNEXPECTED_EXTRAS_SID_IN_REQUEST_TICKET (0x00000040) • RC4_PAC (0x00000080) • PACLESS_TICKET_GENERATION (0x00000100) • AP_REQ_MISSING_AUTHENTICATOR_CHECKSUM (0x00000200) • AP_REQ_ZERO_FILLED_BIND_IN_AUTHENTICATOR_CHECKSUM (0x00000400) • UNEXPECTED_HOSTNAME_IN_SERVICE_ACCESS_REQUEST (0x00000800) • RUBEUS_DEFAULT_GROUPS (0x00001000) • ADMIN_IN_PAC (0x00002000) • FULL_NAME_MISMATCH (0x00004000) • INVALID_GROUP_ORDER (0x00008000) • RUBEUS_AUTH_WITH_CERTIFICATE (0x00010000)
CertificateBasedAuth	
CertificateSubjectName	
CertificateCommonName	
CertificateIssuer	
CertificateAlgorithm	
CertificateValidityPeriod	
CertificateExtensionSubjectAltName	
CertificateExtensionKeyUsage	
CertificateExtensionEnhancedKeyUsages	
CertificateExtensionEnhancedKeyUsagesCount	
CertificateTemplateExtensionV1	
CertificateTemplateExtensionV2	
AuthenticationFailureMsErrorCode	A Microsoft-specific error code annotating the authentication or service access failure, available for both Kerberos and NTLM activities. For Kerberos activities this provides a more fine-grained error cause compared to the `KerberosErrorCode` value. **Values:** • STATUS_ACCESS_DENIED (0xC0000022) • STATUS_WRONG_PASSWORD (0xC000006A) • STATUS_LOGON_FAILURE (0xC000006D)

Field	Description
	• STATUS_NO_SUCH_USER (0xC0000064) • STATUS_ACCOUNT_RESTRICTION (0xC000006E) • STATUS_INVALID_LOGON_HOURS (0xC000006F) • STATUS_INVALID_WORKSTATION (0xC0000070) • STATUS_PASSWORD_EXPIRED (0xC0000071) • STATUS_ACCOUNT_DISABLED (0xC0000072) • STATUS_LOGON_NOT_GRANTED (0xC0000155) • STATUS_LOGON_TYPE_NOT_GRANTED (0xC000015B) • STATUS_ACCOUNT_EXPIRED (0xC0000193) • STATUS_ACCOUNT_LOCKED_OUT (0xC0000234)
LdapErrorResultCode	The cause for an LDAP operation failure. **Values:** • LDAP_SUCCESS (0x00) • LDAP_OPERATIONS_ERROR (0x01) • LDAP_PROTOCOL_ERROR (0x02) • LDAP_TIMELIMIT_EXCEEDED (0x03) • LDAP_SIZELIMIT_EXCEEDED (0x04) • LDAP_COMPARE_FALSE (0x05) • LDAP_COMPARE_TRUE (0x06) • LDAP_AUTH_METHOD_NOT_SUPPORTED (0x07) • LDAP_STRONG_AUTH_REQUIRED (0x08) • LDAP_REFERRAL (0x0A) • LDAP_ADMINLIMIT_EXCEEDED (0x0B) • LDAP_UNAVAILABLE_CRITICAL_EXTENSION (0x0C) • LDAP_CONFIDENTIALITY_REQUIRED (0x0D) • LDAP_SASL_BIND_IN_PROGRESS (0x0E) • LDAP_NO_SUCH_ATTRIBUTE (0x10) • LDAP_UNDEFINED_TYPE (0x11) • LDAP_INAPPROPRIATE_MATCHING (0x12) • LDAP_CONSTRAINT_VIOLATION (0x13) • LDAP_TYPE_OR_VALUE_EXISTS (0x14) • LDAP_INVALID_SYNTAX (0x15) • LDAP_NO_SUCH_OBJECT (0x20) • LDAP_ALIAS_PROBLEM (0x21) • LDAP_INVALID_DN_SYNTAX (0x22) • LDAP_IS_LEAF (0x23) • LDAP_ALIAS_DEREF_PROBLEM (0x24) • LDAP_INAPPROPRIATE_AUTH (0x30) • LDAP_INVALID_CREDENTIALS (0x31) • LDAP_INSUFFICIENT_ACCESS (0x32) • LDAP_BUSY (0x33) • LDAP_UNAVAILABLE (0x34) • LDAP_UNWILLING_TO_PERFORM (0x35) • LDAP_LOOP_DETECT (0x36) • LDAP_NAMING_VIOLATION (0x40) • LDAP_OBJECT_CLASS_VIOLATION (0x41) • LDAP_NOT_ALLOWED_ON_NONLEAF (0x42) • LDAP_NOT_ALLOWED_ON_RDN (0x43) • LDAP_ALREADY_EXISTS (0x44) • LDAP_NO_OBJECT_CLASS_MODS (0x45) • LDAP_RESULTS_TOO_LARGE (0x46) • LDAP_AFFECTS_MULTIPLE_DSAS (0x47) • LDAP_OTHER (0x50) • LDAP_SERVER_DOWN (0x51) • LDAP_LOCAL_ERROR (0x52) • LDAP_ENCODING_ERROR (0x53) • LDAP_DECODING_ERROR (0x54) • LDAP_TIMEOUT (0x55) • LDAP_AUTH_UNKNOWN (0x56) • LDAP_FILTER_ERROR (0x57) • LDAP_USER_CANCELLED (0x58) • LDAP_PARAM_ERROR (0x59) • LDAP_NO_MEMORY (0x5a) • LDAP_CONNECT_ERROR (0x5b) • LDAP_NOT_SUPPORTED (0x5c) • LDAP_CONTROL_NOT_FOUND (0x5d) • LDAP_NO_RESULTS_RETURNED (0x5e) • LDAP_MORE_RESULTS_TO_RETURN (0x5f)

Field	Description
	• LDAP_CLIENT_LOOP (0x60) • LDAP_REFERRAL_LIMIT_EXCEEDED (0x61)
LdapSecurityType	The method used to encrypt LDAP messages reflected by this activity. NONE indicates clear-text. Set whenever the ActiveDirectoryDataProtocol is set to LDAP, for example both authentications and search operations. **Values:** • NONE (0) • TLS (1) • SASL_INTEGRITY (2) • SASL_CONFIDENTIALITY (3) • START_TLS (4)
TlsVersion	The TLS version that was used for encryption. **Values:** • V1_0 (0) • V1_1 (1) • V1_2 (2) • V1_3 (3)
SourceAccountBadPasswordCount	The value of the LDAP badPwdCount attribute of the source account of this activity. Note that the value is a static snapshot of the value when the activity was observed.
SourceAccountBadPasswordTime	The value of the LDAP badPwdTime attribute of the source account of this activity. Note that the value is a static snapshot of the value when the activity was observed.
AppliedDisposition	A bit mask of the disposition the sensor has applied.
SmbDialect	**Values:** • UNKNOWN_SMB (0x0) • SMB_1 (0x1) • SMB_2_0_2 (0x0202) • SMB_2_1 (0x0210) • SMB_3_0 (0x0300) • SMB_3_0_2 (0x0302) • SMB_3_1_1 (0x0311)

top [#top]

SetWindowsHook

Description

Platforms: *Windows*
An event that is sent from the sensor when a user mode program attempts to set a windows hook.

Fields: Windows

Field	Description
ContextTimeStamp	System time of event creation.
ContextProcessId	UPID of process originating this event.
ContextThreadId	UTID of thread originating this event
TreeId	If this event is part of a detection tree, the tree ID it is part of.
HookProcedure	
HookId	**Values:** • WH_MSGFILTER (0xffffffff) • WH_JOURNALRECORD (0) • WH_JOURNALPLAYBACK (1) • WH_KEYBOARD (2) • WH_GETMESSAGE (3) • WH_CALLWNDPROC (4) • WH_CBT (5) • WH_SYSMSGFILTER (6) • WH_MOUSE (7) • WH_HARDWARE (8)

Field	Description
	• WH_DEBUG (9) • WH_SHELL (10) • WH_FOREGROUNDIDLE (11) • WH_CALLWNDPROCRET (12) • WH_KEYBOARD_LL (13) • WH_MOUSE_LL (14)
ModuleName	
PatternId	The ID of the pattern
ImageFileName	The full path to an executable (PE) file. The context of this field provides more information as to its meaning. For `ProcessRollup2` events, this is the full path to the main executable for the created process.
CommandLine	The command line used to create this process. May be empty in some circumstances, visit here [http://msdn.microsoft.com/en-us/library/windows/desktop/ms682425(v=vs.85).aspx] for more information.
UserModeHookSource	Values: • UMPPC (0x01) • ETW (0x02)
EtwRawProcessId	
EtwRawThreadId	
ApiReturnValue	
TargetProcessId	The unique ID of a target process (in decimal, non-hex format). This field exists in almost all events, and it represents the ID of the process that is responsible for the activity of the event in focus. For example, the `TargetProcessId` of a process that performed thread injection in an `InjectedThread` event
MemoryDescriptionFlags	
ImageDirectoryClassification	Values: • UNKNOWN (0) • APPLICATION_DIRECTORY (1) • CURRENT_DIRECTORY (2) • WINDOWS_DIRECTORY (3) • SYSTEM_DIRECTORY (4) • APPLICATION_SUB_DIRECTORY (5)

top [#top]

FileDetectInfo

Description

Platforms: *macOS, Linux, Windows*

Fields: macOS, Linux, Windows

Field	Description
ContextProcessId	UPID of process originating this event.
TargetFileName	The resulting file name that was downloaded
PatternId	The ID of the pattern
ContextTimeStamp	System time of event creation.
TreeId	If this event is part of a detection tree, the tree ID it is part of.
TemplateInstanceId	
TemplateDisposition	Values: • TEMPLATE_DISPOSITION_NOACTION (0) • TEMPLATE_DISPOSITION_ANALYSIS (3) • TEMPLATE_DISPOSITION_SENSOR_ONLY (4) • TEMPLATE_DISPOSITION_INDICATOR (10) • TEMPLATE_DISPOSITION_DETECT (20) • TEMPLATE_DISPOSITION_OPERATION_BLOCK (25) • TEMPLATE_DISPOSITION_PREVENT (30) • TEMPLATE_DISPOSITION_PREVENT_KILLPARENT (60) • TEMPLATE_DISPOSITION_PREVENT_KILLSOURCE (61) • TEMPLATE_DISPOSITION_CONTAINMENT_FS_SERVER (70)

Field	Description
SourceFileName	The file's original name
AuthenticationId	Values: • INVALID_LUID (0) • NETWORK_SERVICE (996) • LOCAL_SERVICE (997) • SYSTEM (999) • RESERVED_LUID_MAX (1000)

top [#top]

AcUninstallConfirmation

Description

Platforms: *Windows, macOS, Linux*
This event is generated when a Falcon sensor is uninstalled from a host.

> **Important:** The Falcon sensor stores events locally in a cache, which enables you to maintain data integrity even if connection to the cloud is interrupted. The cache holds a maximum of 20,000 events and sends them after a host re-establishes a connection with the cloud. However, if you reboot, the cache is lost. This means that if you uninstall a sensor off network and reboot, the cache storing those events is lost, including any AcUninstallConfirmation events.

Fields: Windows, macOS, Linux

Field	Description
ContextTimeStamp	System time of event creation.

top [#top]

AcUnloadConfirmation

Description

Platforms: *Windows, macOS, Linux*
The cloud will respond with this event as acknowledgement that a sensor was uninstalled.

Fields: Windows, macOS, Linux

Field	Description
ContextTimeStamp	System time of event creation.

top [#top]

WfpFilterTamperingFilterDeleted

Description

Platforms: *Windows*
This event is created whenever WFP indicates to our callout driver that a filter that references one of our callout functions has been deleted from the Base Filtering Engine.

Fields: Windows

Field	Description
ReferencedCalloutGuid	
ReferencedCalloutGuidAsString	
ContextTimeStamp	System time of event creation.
TamperFilterGuid	

Field	Description
TamperFilterGuidAsString	
TamperFilterId2	
TamperFilterWeight	
TamperFilterSublayerWeight	
TamperFilterFlags	
TamperFilterConditionCount	
TamperFilterAction	

top [#top]

HostInfo

Description

Platforms: *Windows*
This event is generated when:

- A host is turned on or rebooted
- A new Falcon sensor is installed on a host
- An existing Falcon sensor is updated

A host is turned on or rebooted A new Falcon sensor is installed on a host An existing Falcon sensor is updated
This event provides information about the host running the sensor. When searching for information about a specific host, you should use the much faster `aid_master` **search capability instead of searching for** `HostInfo` **events**

Platforms: *macOS, iOS*
This event is generated when:

- A host is turned on or rebooted
- A new Falcon sensor is installed on a host
- An existing Falcon sensor is updated

A host is turned on or rebooted A new Falcon sensor is installed on a host An existing Falcon sensor is updated
This event provides information about the host running the sensor. When searching for information about a specific host, you should use the much faster `aid_master` **search capability instead of searching for** `HostInfo` **events**

Platforms: *Windows Legacy*

Fields: Windows, Windows Legacy

Field	Description
MachineDomain	
BootArgs	
MachineDn	
SiteName	
DcName	

Fields: macOS

Field	Description
MachineDomain	
BootArgs	
MachineDn	
SiteName	
DcName	
SIPIsEnabled	
PasswordRequiredIsSet	
RemoteLoginIsSet	
GatekeeperIsSet	

Field	Description
ApplicationFirewallIsSet	
ScreenSharingIsSet	
InputMonitoringIsSet	
StealthModeIsSet	
InternetSharingIsSet	
AnalyticsAndImprovementsIsSet	
FullDiskAccessForFalconIsSet	
FullDiskAccessForOthersIsSet	
RemoteManagementIsSet	
RemoteAppleEventsIsSet	
AutoUpdate	Values: • AUTOMATIC_CHECK (0x01) • AUTOMATIC_DOWNLOAD (0x02) • AUTOMATIC_INSTALL (0x04) • INSTALL_CONFIG (0x08) • INSTALL_CRITICAL_UPDATE (0x10)

Fields: iOS

Field	Description
ContextTimeStamp	System time of event creation.
NetworkExtensionType	Values: • UNKNOWN (0) • CONTENT_FILTER (1) • APP_PROXY (2)
BluetoothStatus	Values: • UNKNOWN (0) • UNAVAILABLE (1) • UNAUTHORIZED (2) • OFF (3) • ON (4)
LocationStatus	Values: • UNKNOWN (0) • UNAVAILABLE (1) • UNAUTHORIZED (2) • OFF (3) • ON (4)

top [#top]

HookedDriverObject

Description

Platforms: *Windows*
This event describes the presence of a hooked pointer in a DRIVER_OBJECT structure.

Fields: Windows

Field	Description
HookedDriverObjectPointer	
HookedDriverImagePath	
HookedDriverStartAddress	
HookedDriverSize	
HookedObjectType	Values: • INVALID (0)

Field	Description
	• DRIVER_OBJECT (1) • NDIS_PROTOCOL_BLOCK (2) • NDIS_OPEN_BLOCK (3) • NDIS_FILTER_BLOCK (4) • NDIS_MINIPORT_BLOCK (5)
HookedObjectPointer	
HookedPointerType	Values: • INVALID (0) • INIT (1) • STARTIO (2) • UNLOAD (3) • DEVICEOBJECTDRIVEROBJECT (4) • IRPMJCREATE (5) • IRPMJCREATENAMEDPIPE (6) • IRPMJCLOSE (7) • IRPMJREAD (8) • IRPMJWRITE (9) • IRPMJQUERYINFORMATION (10) • IRPMJSETINFORMATION (11) • IRPMJQUERYEA (12) • IRPMJSETEA (13) • IRPMJFLUSHBUFFERS (14) • IRPMJQUERYVOLUMEINFORMATION (15) • IRPMJSETVOLUMEINFORMATION (16) • IRPMJDIRECTORYCONTROL (17) • IRPMJFILESYSTEMCONTROL (18) • IRPMJDEVICECONTROL (19) • IRPMJINTERNALDEVICECONTROL (20) • IRPMJSHUTDOWN (21) • IRPMJLOCKCONTROL (22) • IRPMJCLEANUP (23) • IRPMJCREATEMAILSLOT (24) • IRPMJQUERYSECURITY (25) • IRPMJSETSECURITY (26) • IRPMJPOWER (27) • IRPMJSYSTEMCONTROL (28) • IRPMJDEVICECHANGE (29) • IRPMJQUERYQUOTA (30) • IRPMJSETQUOTA (31) • FASTIOREAD (32) • FASTIOWRITE (33) • FASTIOQUERYBASICINFO (34) • FASTIOQUERYSTANDARDINFO (35) • FASTIODEVICECONTROL (36) • FASTIOQUERYNETWORKOPENINFO (37) • FASTIOMDLREAD (38) • FASTIOMDLREADCOMPLETE (39) • FASTIOPREPAREMDLWRITE (40) • FASTIOMDLWRITECOMPLETE (41) • FASTIOREADCOMPRESSED (42) • FASTIOWRITECOMPRESSED (43) • FASTIOMDLREADCOMPLETECOMPRESSED (44) • FASTIOMDLWRITECOMPLETECOMPRESSED (45) • FASTIOQUERYOPEN (46) • NDIS5OPENBLOCKRECEIVEHANDLER (47) • NDIS5OPENBLOCKRECEIVECOMPLETEHANDLER (48) • NDIS5OPENBLOCKRECEIVEPACKETHANDLER (49) • NDIS5OPENBLOCKSENDHANDLER (50) • NDIS5OPENBLOCKSENDCOMPLETEHANDLER (51) • NDIS5OPENBLOCKSENDPACKETSHANDLER (52) • NDIS5OPENBLOCKTRANSFERDATAHANDLER (53) • NDIS5OPENBLOCKTRANSFERDATACOMPLETEHANDLER (54) • NDIS5OPENBLOCKRECEIVENETBUFFERLISTSHANDLER (55) • NDIS6OPENBLOCKPROTOCOLSENDNETBUFFERLISTSCOMPLETEHANDLER (56) • NDIS6OPENBLOCKPROTOCOLRECEIVENETBUFFERLISTSHANDLER (57) • NDIS5MINIPORTBLOCKSENDPACKETSHANDLER (58) • NDIS6PROTOCOLBLOCKRECEIVENETBUFFERLISTSHANDLER (59)

Field	Description
	• NDIS6PROTOCOLBLOCKSENDNETBUFFERLISTSCOMPLETEHANDLER (60) • NDIS6FILTERBLOCKNEXTSENDNETBUFFERLISTSCOMPLETEHANDLER (61) • NDIS6FILTERBLOCKRETURNNETBUFFERLISTSHANDLER (62) • NDIS6FILTERBLOCKFILTERSENDNETBUFFERLISTSHANDLER (63)
HookingDriverObjectPointer	
HookingDriverImagePath	
HookingDriverStartAddress	
HookingDriverSize	
HookingAddress	

top [#top]

WfpFilterTamperingFilterAdded

Description

Platforms: *Windows*
This event is created whenever WFP indicates to our callout driver that a new filter that references one of our callout functions has been added to the Base Filtering Engine.

Fields: Windows

Field	Description
ReferencedCalloutGuid	
ReferencedCalloutGuidAsString	
ContextTimeStamp	System time of event creation.
TamperFilterGuid	
TamperFilterGuidAsString	
TamperFilterId2	
TamperFilterWeight	
TamperFilterSublayerWeight	
TamperFilterFlags	
TamperFilterConditionCount	
TamperFilterAction	

top [#top]

LocalIpAddressIP6

Description

Platforms: *Windows, macOS, Linux, Falcon Container, iOS, Android*
This event is generated when a host uses a new IPv6 network address.

Platforms: *Forensics*

Fields: Windows

Field	Description
CreationTimeStamp	
PrefixOrigin	
SuffixOrigin	
DadState	
ScopeZone	

Field	Description
ScopeLevel	
ValidLifetime	
PreferredLifetime	
OnLinkPrefixLength	
SkipAsSource	
NetLuidIndex	
InterfaceIndex	The index of the network interface requested for this DNSquery.
InterfaceIdentifier	
IfType	
AddressFamily	
MaxReassemblySize	
MinRouterAdvertisementInterval	
MaxRouterAdvertisementInterval	
Metric	
NlMtu	
ReachableTime	
DadTransmits	
BaseReachableTime	
RetransmitTime	
PathMtuDiscoveryTimeout	
LinkLocalAddressTimeout	
SitePrefixLength	
RouterDiscoveryBehavior	
LinkLocalAddressBehavior	
IpEntryFlags	
NetworkInterfaceGuid	
NetworkGuid	
InterfaceAlias	
InterfaceDescription	
InterfaceMtu	
InterfaceType	
PhysicalAddressLength	
TunnelType	
MediaType	
PhysicalMediumType	
AccessType	
DirectionType	
InterfaceFlags	
OperStatus	
AdminStatus	
MediaConnectState	
ConnectionType	
PhysicalAddress	The MAC address of the device
PermanentPhysicalAddress	
TransmitLinkSpeed	
ReceiveLinkSpeed	
InOctets	

Field	Description
InUcastPkts	
InNUcastPkts	
InDiscards	
InErrors	
InUnknownProtos	
InUcastOctets	
InMulticastOctets	
InBroadcastOctets	
OutOctets	
OutUcastPkts	
OutNUcastPkts	
OutDiscards	
OutErrors	
OutUcastOctets	
OutMulticastOctets	
OutBroadcastOctets	
LocalAddressIP6	
DefaultGatewayPhysicalAddress	
RouteAge	
RouteOrigin	
RouteMetric	
DefaultGatewayIP6	
PrefixLength	
LocalIpAddressPipelineSource	

Fields: macOS

Field	Description
CreationTimeStamp	
InterfaceIndex	The index of the network interface requested for this DNSquery.
InterfaceAlias	
NetLuidIndex	
InterfaceType	
PhysicalAddressLength	
PhysicalAddress	The MAC address of the device
InUcastPkts	
InOctets	
InMulticastPkts	
InErrors	
OutUcastPkts	
OutOctets	
OutMulticastPkts	
OutErrors	
InDiscards	
InUnknownProtos	
LocalAddressIP6	
LocalIpAddressPipelineSource	

Field	Description
PrefixLength	
DefaultGatewayIP6	
DefaultGatewayPhysicalAddress	

Fields: Linux, Falcon Container

Field	Description
CreationTimeStamp	
InterfaceIndex	The index of the network interface requested for this DNSquery.
InterfaceAlias	
InterfaceType	
PhysicalAddressLength	
PhysicalAddress	The MAC address of the device
LocalAddressIP6	
LocalIpAddressPipelineSource	
DefaultGatewayIP6	
PrefixLength	
DefaultGatewayPhysicalAddress	
InterfaceKind	

Fields: iOS

Field	Description
CreationTimeStamp	
InterfaceIndex	The index of the network interface requested for this DNSquery.
InterfaceAlias	
InterfaceType	
LocalAddressIP6	

Fields: Forensics

Field	Description
ContextTimeStamp	System time of event creation.
InterfaceDescription	
NetLuidIndex	
InterfaceIndex	The index of the network interface requested for this DNSquery.
InterfaceIdentifier	
IfType	
AddressFamily	
NetworkInterfaceGuid	
InterfaceAlias	
PhysicalAddressLength	
PhysicalAddress	The MAC address of the device
PermanentPhysicalAddress	
DnsSuffix	String suffix appended to a host name in order to query DNS for an IP address.
LocalAddressIP6	
DefaultGatewayIP6	

Fields: Android

Field	Description
CreationTimeStamp	
InterfaceIndex	The index of the network interface requested for this DNSquery.
InterfaceAlias	
LocalAddressIP6	

top [#top]

NeighborListIP4

Description

Platforms: *Windows, macOS, Linux, Falcon Container, Forensics*
This event shows the IPv4 network addresses and MAC addresses of other devices on the host's network, gathered using ARP on the host. The first time a device sends this event to the CrowdStrike Cloud, its entire ARP table is sent. For later events, only the changes to the ARP table are sent.
This event returns data as a MAC address, an IPv4 address, and a delimiter character (0 or 1). Each item is separated by a pipe character (|).
If the delimiter character is a 0, the preceding MAC and IP addresses belong to a device. If the delimiter character is 1, the preceding IP and MAC addresses belong to the host's gateway.

Fields: Windows, macOS, Linux, Falcon Container

Field	Description
InterfaceIndex	The index of the network interface requested for this DNSquery.
NeighborList	

Fields: Forensics

Field	Description
InterfaceIndex	The index of the network interface requested for this DNSquery.
ContextTimeStamp	System time of event creation.
NeighborList	

top [#top]

LocalIpAddressIP4

Description

Platforms: *Windows, macOS, Linux, Falcon Container, iOS, Android*
This event is generated when a host uses a new IPv4 network address.

Platforms: *Forensics*

Fields: Windows

Field	Description
CreationTimeStamp	
PrefixOrigin	
SuffixOrigin	
DadState	
ScopeZone	
ScopeLevel	
ValidLifetime	
PreferredLifetime	

Field	Description
OnLinkPrefixLength	
SkipAsSource	
NetLuidIndex	
InterfaceIndex	The index of the network interface requested for this DNSquery.
InterfaceIdentifier	
IfType	
AddressFamily	
MaxReassemblySize	
MinRouterAdvertisementInterval	
MaxRouterAdvertisementInterval	
Metric	
NlMtu	
ReachableTime	
DadTransmits	
BaseReachableTime	
RetransmitTime	
PathMtuDiscoveryTimeout	
LinkLocalAddressTimeout	
SitePrefixLength	
RouterDiscoveryBehavior	
LinkLocalAddressBehavior	
IpEntryFlags	
NetworkInterfaceGuid	
NetworkGuid	
InterfaceAlias	
InterfaceDescription	
InterfaceMtu	
InterfaceType	
PhysicalAddressLength	
TunnelType	
MediaType	
PhysicalMediumType	
AccessType	
DirectionType	
InterfaceFlags	
OperStatus	
AdminStatus	
MediaConnectState	
ConnectionType	
PhysicalAddress	The MAC address of the device
PermanentPhysicalAddress	
TransmitLinkSpeed	
ReceiveLinkSpeed	
InOctets	
InUcastPkts	
InNUcastPkts	
InDiscards	

Field	Description
InErrors	
InUnknownProtos	
InUcastOctets	
InMulticastOctets	
InBroadcastOctets	
OutOctets	
OutUcastPkts	
OutNUcastPkts	
OutDiscards	
OutErrors	
OutUcastOctets	
OutMulticastOctets	
OutBroadcastOctets	
LocalAddressIP4	
DefaultGatewayPhysicalAddress	
RouteAge	
RouteOrigin	
RouteMetric	
DefaultGatewayIP4	
PrefixLength	
LocalIpAddressPipelineSource	

Fields: macOS

Field	Description
CreationTimeStamp	
InterfaceIndex	The index of the network interface requested for this DNSquery.
InterfaceAlias	
NetLuidIndex	
InterfaceType	
PhysicalAddressLength	
PhysicalAddress	The MAC address of the device
InUcastPkts	
InOctets	
InMulticastPkts	
InErrors	
OutUcastPkts	
OutOctets	
OutMulticastPkts	
OutErrors	
InDiscards	
InUnknownProtos	
LocalAddressIP4	
LocalIpAddressPipelineSource	
PrefixLength	
DefaultGatewayIP4	
DefaultGatewayPhysicalAddress	

Fields: Linux, Falcon Container

Field	Description
CreationTimeStamp	
InterfaceIndex	The index of the network interface requested for this DNSquery.
InterfaceAlias	
InterfaceType	
PhysicalAddressLength	
PhysicalAddress	The MAC address of the device
LocalAddressIP4	
LocalIpAddressPipelineSource	
DefaultGatewayIP4	
PrefixLength	
DefaultGatewayPhysicalAddress	
InterfaceKind	

Fields: iOS

Field	Description
CreationTimeStamp	
InterfaceIndex	The index of the network interface requested for this DNSquery.
InterfaceAlias	
InterfaceType	
LocalAddressIP4	

Fields: Forensics

Field	Description
ContextTimeStamp	System time of event creation.
InterfaceDescription	
NetLuidIndex	
InterfaceIndex	The index of the network interface requested for this DNSquery.
InterfaceIdentifier	
IfType	
AddressFamily	
NetworkInterfaceGuid	
InterfaceAlias	
PhysicalAddressLength	
PhysicalAddress	The MAC address of the device
PermanentPhysicalAddress	
DnsSuffix	String suffix appended to a host name in order to query DNS for an IP address.
LocalAddressIP4	
Netmask	
DefaultGatewayIP4	
BroadcastAddressIP4	

Fields: Android

Field	Description
CreationTimeStamp	
InterfaceIndex	The index of the network interface requested for this DNSquery.
InterfaceAlias	
LocalAddressIP4	

top [#top]

NeighborListIP6

Description

Platforms: *Windows, macOS, Linux, Falcon Container*
This event shows the MAC addresses and IPv6 network addresses of other devices on the host's network, gathered using ARP on the host. The first time a device sends this event to the CrowdStrike Cloud, its entire ARP table is sent. For later events, only the changes to the ARP table are sent.
This event returns data as a MAC address, an IPv6 address, and a delimiter character (0 or 1). Each item is separated by a pipe character (|).
If the delimiter character is a 0, the preceding MAC and IP addresses belong to a device. If the delimiter character is 1, the preceding IP and MAC addresses belong to the host's gateway.

Platforms: *Forensics*

Fields: Windows, macOS, Linux, Falcon Container

Field	Description
InterfaceIndex	The index of the network interface requested for this DNSquery.
NeighborList	

Fields: Forensics

Field	Description
InterfaceIndex	The index of the network interface requested for this DNSquery.
ContextTimeStamp	System time of event creation.
NeighborList	

top [#top]

LocalIpAddressRemovedIP6

Description

Platforms: *Windows, macOS, Linux, Falcon Container, iOS, Android*
This event is generated when a host loses its IPv6 network address.

Fields: Windows, macOS

Field	Description
NetLuidIndex	
InterfaceIndex	The index of the network interface requested for this DNSquery.
LocalAddressIP6	
LocalIpAddressPipelineSource	

Fields: Linux, Falcon Container

Field	Description
InterfaceIndex	The index of the network interface requested for this DNSquery.

Field	Description
LocalAddressIP6	
LocalIpAddressPipelineSource	

Fields: iOS, Android

Field	Description
InterfaceIndex	The index of the network interface requested for this DNSquery.
LocalAddressIP6	

top [#top]

UserLogoff

Description

Platforms: *Windows, macOS*
This event is generated when a user logs off from a host.

Platforms: *Linux, ChromeOS*

Fields: Windows

Field	Description
AuthenticationId	Values: • INVALID_LUID (0) • NETWORK_SERVICE (996) • LOCAL_SERVICE (997) • SYSTEM (999) • RESERVED_LUID_MAX (1000)
LogoffTime	
UserSid	The User Security Identifier (UserSID) of the user who executed the command. A `UserSID` uniquely identifies a user in a system. Values: • SELF_RID (0x01010000000000050A000000)
UserName	Operating system username.
UserPrincipal	
LogonDomain	
AuthenticationPackage	
LogonType	Values: • INTERACTIVE (2) • NETWORK (3) • BATCH (4) • SERVICE (5) • PROXY (6) • UNLOCK (7) • NETWORK_CLEARTEXT (8) • NEW_CREDENTIALS (9) • REMOTE_INTERACTIVE (10) • CACHED_INTERACTIVE (11) • CACHED_REMOTE_INTERACTIVE (12) • CACHED_UNLOCK (13)
LogonTime	
LogonServer	
UserFlags	Values: • LOGON_OPTIMIZED (0x4000) • LOGON_WINLOGON (0x8000) • LOGON_PKINIT (0x10000) • LOGON_NOT_OPTIMIZED (0x20000)

Field	Description
PasswordLastSet	
RemoteAccount	A boolean value set to true if the user account is not an account residing on the local computer
UserIsAdmin	Set to TRUE if this user is a local admin.
UserLogonFlags	Values: • NONE (0x00000000) • LOGON_IS_SYNTHETIC (0x00000001) • USER_IS_ADMIN (0x00000002) • USER_IS_LOCAL (0x00000004) • USER_IS_BUILT_IN (0x00000008) • USER_IDENTITY_MISSING (0x00000010)
UserLogoffType	Values: • LOGOFF_EVENT_SOURCE (0x01) • LOGOFF_PROFILE_UNLOAD (0x02) • ETW (0x03) • SYNTHETIC (0x04)

Fields: Linux

Field	Description
ContextTimeStamp	System time of event creation.
UserName	Operating system username.
LogonTime	
LogoffTime	
LogonType	Values: • INTERACTIVE (2) • NETWORK (3) • BATCH (4) • SERVICE (5) • PROXY (6) • UNLOCK (7) • NETWORK_CLEARTEXT (8) • NEW_CREDENTIALS (9) • REMOTE_INTERACTIVE (10) • CACHED_INTERACTIVE (11) • CACHED_REMOTE_INTERACTIVE (12) • CACHED_UNLOCK (13)
UID	Unix User Identifier.
UserIsAdmin	Set to TRUE if this user is a local admin.
PasswordLastSet	
RemoteAddressIP4	
RemoteAddressIP6	

Fields: ChromeOS

Field	Description
ContextTimeStamp	System time of event creation.
UserName	Operating system username.
LogoffTime	
LocalAddressIP4	
LocalAddressIP6	

Fields: macOS

Field	Description
ContextTimeStamp	System time of event creation.

Field	Description
ContextProcessId	UPID of process originating this event.
RawProcessId	The operating system's internal PID. For matching, use the UPID fields which guarantee a unique process identifier
UID	Unix User Identifier.
AuditSessionId	
LogoffTime	
UserLogoffType	Values: • LOGOFF_EVENT_SOURCE (0x01) • LOGOFF_PROFILE_UNLOAD (0x02) • ETW (0x03) • SYNTHETIC (0x04)
LogonType	Values: • INTERACTIVE (2) • NETWORK (3) • BATCH (4) • SERVICE (5) • PROXY (6) • UNLOCK (7) • NETWORK_CLEARTEXT (8) • NEW_CREDENTIALS (9) • REMOTE_INTERACTIVE (10) • CACHED_INTERACTIVE (11) • CACHED_REMOTE_INTERACTIVE (12) • CACHED_UNLOCK (13)
LogonTime	
AuthenticationId	Values: • INVALID_LUID (0) • NETWORK_SERVICE (996) • LOCAL_SERVICE (997) • SYSTEM (999) • RESERVED_LUID_MAX (1000)
UserSid	The User Security Identifier (UserSID) of the user who executed the command. A `UserSID` uniquely identifies a user in a system. Values: • SELF_RID (0x01010000000000050A000000)
UserPrincipal	
UserName	Operating system username.
UserLogonFlags	Values: • NONE (0x00000000) • LOGON_IS_SYNTHETIC (0x00000001) • USER_IS_ADMIN (0x00000002) • USER_IS_LOCAL (0x00000004) • USER_IS_BUILT_IN (0x00000008) • USER_IDENTITY_MISSING (0x00000010)
UserGroupsBitmask	Values: • GROUP_BUILTIN_ADMINISTRATOR (0x0000000000000001) • GROUP_BUILTIN_POWERUSER (0x0000000000000002) • GROUP_BUILTIN_REMOTE_MANAGEMENT (0x0000000000000004) • GROUP_BUILTIN_DCOM (0x0000000000000008) • GROUP_BUILTIN_NET_OPS (0x0000000000000010) • GROUP_BUILTIN_BACKUP_OPS (0x0000000000000020) • GROUP_BUILTIN_ACCOUNT_OPS (0x0000000000000040) • GROUP_BUILTIN_USERS (0x0000000000000080) • GROUP_BUILTIN_PERF_MONITOR (0x0000000000000100) • GROUP_BUILTIN_PERF_LOG (0x0000000000000200) • GROUP_BUILTIN_GUESTS (0x0000000000000400) • GROUP_NT_AUTH_BATCH (0x0000000000000800) • GROUP_NT_AUTH_NETWORK (0x0000000000001000) • GROUP_NT_AUTH_SERVICE (0x0000000000002000) • GROUP_NT_AUTH_LOCAL_ACCOUNT (0x0000000000004000) • GROUP_NT_AUTH_LOCAL_ACCOUNT_AND_ADMIN (0x0000000000008000) • GROUP_NT_AUTH_INTERACTIVE (0x0000000000010000) • GROUP_NT_AUTH_ANONYMOUS (0x0000000000020000) • GROUP_NT_AUTH_AUTHENTICATED_USERS (0x0000000000040000)