Security Event Syslog Messages

Security Event Syslog Message IDs

- 430001: Intrusion event

  This ID was introduced in release 6.3.

- 430002: Connection event logged at beginning of connection

  This ID was introduced in release 6.3.

- 430003: Connection event logged at end of connection

  This ID was introduced in release 6.3.

- 430004: File events

  Syslog support for these events was introduced in release 6.4.

- 430005: File malware events

  Syslog support for these events was introduced in release 6.4.

Intrusion Event Field Descriptions

Note Starting in release 6.3, fields with empty or unknown values are not included in syslog messages.

AccessControlRuleName

This field is included in applicable intrusion event syslog messages starting in release 6.5.

The access control rule that invoked the intrusion policy that generated the event. `Default Action` indicates that the intrusion policy where the rule is enabled is not associated with a specific access control rule but, instead, is configured as the default action of the access control policy.

This field is empty (or, for syslog messages, omitted) if there is:

- No associated rule/default action: Intrusion inspection was associated with neither an access control rule nor the default action, for example, if the packet was examined by the intrusion policy specified to handle packets that must pass before the system can determine which rule to apply. (This policy is specified in the Advanced tab of the access control policy.)
- No associated connection event: The connection event logged for the session has been purged from the database, for example, if connection events have higher turnover than intrusion events.

ACPolicy

The access control policy associated with the intrusion policy where the intrusion, preprocessor, or decoder rule that generated the event is enabled.

ApplicationProtocol

The application protocol, if available, which represents communications between hosts detected in the traffic that triggered the intrusion event.

Classification

The classification where the rule that generated the event belongs.

Client

The client application, if available, which represents software running on the monitored host detected in the traffic that triggered the intrusion event.

Connection Counter

This field was added in release 6.5.

A counter that distinguishes one connection from another simultaneous connection. This field has no significance on its own.

The following fields collectively uniquely identify the connection event associated with a particular intrusion event: DeviceUUID, First Packet Time, Connection Instance ID, and Connection Counter.

Connection Instance ID

This field was added in release 6.5

The Snort instance that processed the connection event. This field has no significance on its own.

The following fields collectively uniquely identify the connection event associated with a particular intrusion event: DeviceUUID, First Packet Time, Connection Instance ID, and Connection Counter.

DeviceUUID

This field was added in release 6.5.

The unique identifier of the device that generated an event.

The following fields collectively uniquely identify the connection event associated with a particular intrusion event: DeviceUUID, First Packet Time, Connection Instance ID, and Connection Counter.

DstIP

The IP address used by the receiving host involved in the intrusion event.

DstPort

The port number for the host receiving the traffic. For ICMP traffic, where there is no port number, this field displays the ICMP code.

EgressInterface

The egress interface of the packet that triggered the event. This interface column is not populated for a passive interface.

EgressZone

The egress security zone of the packet that triggered the event. This security zone field is not populated in a passive deployment.

First Packet Time (FirstPacketSecond)

This field was added in release 6.5.

The time the system encountered the first packet.

The following fields collectively uniquely identify the connection event associated with a particular intrusion event: DeviceUUID, First Packet Time, Connection Instance ID, and Connection Counter.

GID

Generator ID; the ID of the component that generated the event.

HTTPResponse

The HTTP status code sent in response to a client's HTTP request over the connection that triggered the event. It indicates the reason behind sucessful and failed HTTP request.

ICMPCode
See **DstPort**.
ICMPType
See **SrcPort**.
IngressInterface

The ingress interface of the packet that triggered the event. Only this interface column is populated for a passive interface.

IngressZone

The ingress security zone or tunnel zone of the packet that triggered the event. Only this security zone field is populated in a passive deployment.

InlineResult

This field became available via syslog in version 6.3.

Note This field is available only when the IPS rule is configured for Drop and Generate.

This field has:

- **`Dropped`** if the packet is dropped in an inline deployment

- **`Would have dropped`** if the packet would have been dropped if the intrusion policy had been set to drop packets in an inline deployment

In a passive deployment, the system does not drop packets, including when an inline interface is in tap mode, regardless of the rule state or the inline drop behavior of the intrusion policy.

IntrusionPolicy

This field became available via syslog in version 6.4.

The intrusion policy where the intrusion, preprocessor, or decoder rule that generated the event was enabled. You can choose an intrusion policy as the default action for an access control policy, or you can associate an intrusion policy with an access control rule.

MPLS_Label

This field is new in version 6.3.

The Multiprotocol Label Switching label associated with the packet that triggered the intrusion event.

Message

The explanatory text for the event. For rule-based intrusion events, the event message is pulled from the rule. For decoder- and preprocessor-based events, the event message is hard coded.

The Generator and Snort IDs (GID and SID) and the SID version (Revision) are appended in parentheses to the end of each message in the format of numbers separated by colons (GID:SID:version). For example **`(1:36330:2)`**.

NAPPolicy

The network analysis policy, if any, associated with the generation of the event.

This field displays the first fifty characters of the extracted URI. You can hover your pointer over the displayed portion of an abbreviated URI to display the complete URI, up to 2048 bytes. You can also display the complete URI, up to 2048 bytes, in the packet view.

NumIOC

Whether the traffic that triggered the intrusion event also triggered an indication of compromise (IOC) for a host involved in the connection.

Priority

The event priority as determined by the Cisco Talos Intelligence Group (Talos). The priority corresponds to either the value of the `priority` keyword or the value for the `classtype` keyword. For other intrusion events, the priority is determined by the decoder or preprocessor. Valid values are high, medium, and low.

Protocol

The name or number of the transport protocol used in the connection as listed in http://www.iana.org/assignments/protocol-numbers. This is the protocol associated with the source and destination port/ICMP column.

Revision

The version of the signature that was used to generate the event.

SID

The signature ID (also known as the Snort ID) of the rule that generated the event.

SSLActualAction

The action the system applied to encrypted traffic:

SrcIP

The IP address used by the sending host involved in the intrusion event.

SrcPort

The port number on the sending host. For ICMP traffic, where there is no port number, this field displays the ICMP type.

User

The username associated with the IP address of the host that initiated the connection, which may or may not be the source host of the exploit. This user value is typically known only for users on your network.

Starting in release 6.5: If applicable, the username is preceded by `<realm>\`.

VLAN_ID

This field is new in version 6.3.

The innermost VLAN ID associated with the packet that triggered the intrusion event.

WebApplication

The web application, which represents the content or requested URL for HTTP traffic detected in the traffic that triggered the intrusion event.

If the system detects an application protocol of HTTP but cannot detect a specific web application, the system supplies a generic web browsing designation instead.

Connection and Security Intelligence Event Field Descriptions

Note Starting in release 6.3, fields with empty or unknown values are not included in syslog messages.

AccessControlRuleAction

The action associated with the configuration that logged the connection.

For Security Intelligence-monitored connections, the action is that of the first non-Monitor access control rule triggered by the connection, or the default action. Similarly, because traffic matching a Monitor rule is always handled by a subsequent rule or by the default action, the action associated with a connection logged due to a Monitor rule is never Monitor. However, you can still trigger correlation policy violations on connections that match Monitor rules.

Action	Description
Allow	Connections either allowed by access control explicitly, or allowed because a user bypassed an interactive block.

Action	Description
Block, Block with reset	Blocked connections, including: • tunnels and other connections blocked by the prefilter policy • connections blocked by Security Intelligence • encrypted connections blocked by an SSL policy • connections where an exploit was blocked by an intrusion policy • connections where a file (including malware) was blocked by a file policy For connections where the system blocks an intrusion or file, system displays `Block`, even though you use access control Allow rules to invoke deep inspection.
Fastpath	Non-encrypted tunnels and other connections fastpathed by the prefilter policy.
Interactive Block, Interactive Block with reset	Connections logged when the system initially blocks a user's HTTP request using an Interactive Block rule. If the user clicks through the warning page that the system displays, additional connections logged for the session have an action of Allow.
Trust	Connections trusted by access control. The system logs trusted TCP connections differently depending on the device model.
Default Action	Connections handled by the access control policy's default action.
(Blank/empty)	The connection closed before enough packets had passed to match a rule. This can happen only if a facility other than access control, such as intrusion prevention, causes the connection to be logged.

AccessControlRuleName

The access control rule or default action that handled the connection, as well as up to eight Monitor rules matched by that connection.

If the connection matched one Monitor rule, the Secure Firewall Management Center displays the name of the rule that handled the connection, followed by the Monitor rule name. If the connection matched more than one Monitor rule, the number of matching Monitor rules is displayed, for example, `Default Action + 2 Monitor Rules`.

AccessControlRuleReason

The reason or reasons the connection was logged, if available.

Connections with a Reason of IP Block, DNS Block, and URL Block have a threshold of 15 seconds per unique initiator-responder pair. After the system blocks one of those connections, it does not generate connection events for additional blocked connections between those two hosts for the next 15 seconds, regardless of port or protocol.

ACPolicy

The access control policy that monitored the connection.

ApplicationProtocol

The application protocol, which represents communications between hosts, detected in the connection.

Client

The client application detected in the connection.

If the system cannot identify the specific client used in the connection, the field displays the word "client" appended to the application protocol name to provide a generic name, for example, FTP client.

ClientVersion

The version of the client application detected in the connection, if available.

Connection Counter

This field was added in release 6.5.

A counter that distinguishes one connection from another simultaneous connection. This field has no significance on its own.

The following fields collectively uniquely identify a connection event: DeviceUUID, First Packet Time, Connection Instance ID, and Connection Counter.

Connection Instance ID

This field was added in release 6.5.

The Snort instance that processed the connection event. This field has no significance on its own.

The following fields collectively uniquely identify a connection event: DeviceUUID, First Packet Time, Connection Instance ID, and Connection Counter.

ConnectionDuration

This field was introduced in version 6.3.

This field has a value only when logging occurs at the end of the connection. For a start-of-connection syslog message, this field is not output, as it is not known at that time.

For an end-of-connection syslog message, this field indicates the number of seconds between the first packet and the last packet, which may be zero for a short connection. For example, if the timestamp of the syslog is 12:34:56 and the ConnectionDuration is 5, then the first packet was seen at 12:34:51.

DetectionType

This field was introduced in release 7.1.

This field shows the source of detection of a client application. It can be **AppID** or **Encrypted Visibility**.

DestinationSecurityGroup

This field was introduced in release 6.5.

The Security Group of the destination involved in the connection.

This field holds the text value associated with the numeric value in **DestinationSecurityGroupTag**, if available. If the group name is not available as a text value, then this field contains the same integer value as the DestinationSecurityGroupTag field.

DestinationSecurityGroupTag

This field was introduced in release 6.5.

The numeric Security Group Tag (SGT) attribute of the destination involved in the connection.

In release 6.6, this value is obtained from the source specified in the **DestinationSecurityGroupType** field.

In release 6.5, this value is obtained from ISE, either from SXP or from a user session.

See also **SourceSecurityGroupTag**.

DestinationSecurityGroupType

This field was introduced in release 6.6.

This field displays the source from which a security group tag was obtained.

Value	Description
Inline	Destination SGT value is from packet
Session Directory	Destination SGT value is from ISE via session directory topic
SXP	Destination SGT value is from ISE via SXP topic

DeviceUUID

This field was added in release 6.5.

The unique identifier of the device that generated an event.

The following fields collectively uniquely identify a connection event: DeviceUUID, First Packet Time, Connection Instance ID, and Connection Counter.

DNS_Sinkhole

The name of the sinkhole server where the system redirected a connection.

DNS_TTL

The number of seconds a DNS server caches the DNS resource record.

DNSQuery

The DNS query submitted in a connection to the name server to look up a domain name.

Starting in release 6.7 as an experimental feature:

This field can also hold the domain name for URL filtering matches when DNS filtering is enabled. In this case, the URL field will be blank and the URL Category and URL Reputation fields contain the values associated with the domain.

DNSRecordType

The type of the DNS resource record used to resolve a DNS query submitted in a connection.

DNSResponseType

The DNS response returned in a connection to the name server when queried.

DNSSICategory

See **URLSICategory**.

DstIP

The IP address (and host name, if DNS resolution is enabled) of the session responder (destination IPaddress).

For plaintext, passthrough tunnels either blocked or fastpathed by the prefilter policy, initiator and responder IP addresses represent the tunnel endpoints—the routed interfaces of the network devices on either side of the tunnel.

DstPort

The port used by the session responder.

EgressInterface

The egress interface associated with the connection. If your deployment includes an asymmetric routing configuration, the ingress and egress interface may not belong to the same inline pair.

EgressVRF

Support for this field was added in version 6.6.

In networks using virtual routing and forwarding, the name of the virtual router through which traffic exited the network.

EgressZone

The egress security zone associated with the connection.

For rezoned encapsulated connections, the egress field is blank.

Endpoint Profile

The user's endpoint device type, as identified by ISE.

EncryptedVisibilityFingerprint

Support for this field was added in version 7.4.

The TLS fingerprint detected by the Encrypted Visibility Engine (EVE) for the session.

EncryptedVisibilityProcessName

Support for this field was added in version 7.1.

Process or client in the TLS client hello packet that was analyzed by the Encrypted Visibility Engine (EVE).

EncryptedVisibilityConfidenceScore

Support for this field was added in version 7.1.

The confidence value in the range 0-100% that the encrypted visibility engine has detected the right process. For example, if the process name is Firefox and if the confidence score is 80%, it means that the engine is 80% confident that the process it has detected is Firefox.

EncryptedVisibilityThreatConfidence

Support for this field was added in version 7.1.

The probability level that the process detected by the encrypted visibility engine contains threat. This field indicates the bands (Very High, High, Medium, Low, or Very Low) based on the value in the threat confidence score.

EncryptedVisibilityThreatConfidenceScore

The confidence value in the range 0-100% that the process detected by the encrypted visibility engine contains threat. If the threat confidence score is very high, say 90%, then the Encrypted Visibility Process Name field displays "Malware."

Event Priority

This field was added in release 6.5.

Whether or not the connection event is a high priority event. `High` priority events are connection events that are associated with an intrusion, Security Intelligence, file, or malware event. All other events are `Low` priority.

FileCount

The number of files (including malware files) detected or blocked in a connection associated with one or more file events.

First Packet Time

This field was added in release 6.5.

The time the system encountered the first packet.

The following fields collectively uniquely identify a connection event: DeviceUUID, First Packet Time, Connection Instance ID, and Connection Counter.

HTTPReferer

The HTTP referrer, which represents the referrer of a requested URL for HTTP traffic detected in the connection (such as a website that provided a link to, or imported a link from, another URL).

HTTPResponse

The HTTP status code sent in response to a client's HTTP request over a connection. It indicates the reason behind successful and failed HTTP request.

For more details about HTTP response codes, see RFC 2616 (HTTP), Section 10.

ICMPCode

The ICMP code used by the session responder.

ICMPType

The ICMP type used by the session initiator.

IngressInterface

The ingress interface associated with the connection. If your deployment includes an asymmetric routing configuration, the ingress and egress interface may not belong to the same inline pair.

IngressVRF

Support for this field was added in version 6.6.

In networks using virtual routing and forwarding, the name of the virtual router through which traffic entered the network.

IngressZone

The ingress security zone associated with the connection.

For rezoned encapsulated connections, the ingress field displays the tunnel zone you assigned, instead of the original ingress security zone.

InitiatorBytes

The total number of bytes transmitted by the session initiator.

InitiatorPackets

The total number of packets transmitted by the session initiator.

IPReputationSICategory

See **URLSICategory**.

IPSCount

The number of intrusion events, if any, associated with the connection.

NAPPolicy

The network analysis policy (NAP), if any, associated with the generation of the event.

NAT_InitiatorIP, NAT_ResponderIP

Support for this field was added in version 7.1.

The NAT translated IP address of the session initiator or responder.

NAT_InitiatorPort, NAT_ResponderPort

Support for this field was added in version 7.1.

The NAT translated port of the session initiator or responder.

NetBIOSDomain

The NetBIOS domain used in the session.

originalClientSrcIP

The original client IP address from an X-Forwarded-For (XFF), True-Client-IP, or custom-defined HTTP header. To populate this field, you must enable an access control rule that handles proxied traffic based on its original client.

Prefilter Policy

The prefilter policy that handled the connection.

Protocol

The transport protocol used in the connection. To search for a specific protocol, use the name or number protocol as listed in http://www.iana.org/assignments/protocol-numbers.

ReferencedHost

If the protocol in the connection is HTTP or HTTPS, this field displays the host name that the respective protocol was using.

ResponderBytes

The total number of bytes transmitted by the session responder.

ResponderPackets

The total number of packets received by the session responder.

SecIntMatchingIP

Which IP address matched.

Possible values: **`None`**, **`Destination`**, or **`Source`**.

Security Group

In release 6.5, this field was replaced by the **SourceSecurityGroupTag** field, and new fields for **SourceSecurityGroup**, **DestinationSecurityGroupTag**, and **DestinationSecurityGroup** were introduced.

The Security Group Tag (SGT) attribute of the packet involved in the connection. The SGT specifies the privileges of a traffic source within a trusted network. Security Group Access (a feature of both Cisco TrustSec and Cisco ISE) applies the attribute as packets enter the network.

SourceSecurityGroup

This field was introduced in release 6.5.

The Security Group of the source involved in the connection.

This field holds the text value associated with the numeric value in **SourceSecurityGroupTag**, if available. If the group name is not available as a text value, then this field contains the same integer value as the SourceSecurityGroupTag field. Tags can be obtained from inline devices (no source SGT name specified) or from ISE (which specifies a source).

SourceSecurityGroupTag

In release 6.5, this field replaced the **Security Group** field.

The numeric representation of the Security Group Tag (SGT) attribute of the packet involved in the connection. The SGT specifies the privileges of a traffic source within a trusted network. Security Group Access (a feature of both Cisco TrustSec and Cisco ISE) applies the attribute as packets enter the network.

See also **DestinationSecurityGroupTag**.

SourceSecurityGroupType

This field was introduced in release 6.6.

This field displays the source from which a security group tag was obtained.

Value	Description
Inline	Source SGT value is from packet
Session Directory	Source SGT value is from ISE via session directory topic
SXP	Source SGT value is from ISE via SXP topic

SrcIP

The IP address (and host name, if DNS resolution is enabled) of the session initiator (source IP address).

For plaintext, passthrough tunnels either blocked or fastpathed by the prefilter policy, initiator and responder IP addresses represent the tunnel endpoints—the routed interfaces of the network devices on either side of the tunnel.

SrcPort

The port used by the session initiator.

SSLActualAction

The action the system applied to encrypted traffic in the SSL policy.

Action	Description
Block/Block with reset	Represents blocked encrypted connections.
Decrypt (Resign)	Represents an outgoing connection decrypted using a re-signed server certificate.
Decrypt (Replace Key)	Represents an outgoing connection decrypted using a self-signed server certificate with a substituted public key.
Decrypt (Known Key)	Represents an incoming connection decrypted using a known private key.
Default Action	Indicates the connection was handled by the default action.
Do not Decrypt	Represents a connection the system did not decrypt.

SSLCertificate

The information stored on the public key certificate used to encrypt traffic, including:

- Subject/Issuer Common Name
- Subject/Issuer Organization
- Subject/Issuer Organization Unit
- Not Valid Before/After
- Serial Number
- Certificate Fingerprint
- Public Key Fingerprint

SSLExpectedAction

The action the system expected to apply to encrypted traffic, given the SSL rules in effect.

SSLFlowStatus

The reason the system failed to decrypt encrypted traffic:

- Unknown
- No Match
- Success
- Uncached Session
- Unknown Cipher Suite
- Unsupported Cipher Suite

- Unsupported SSL Version
- SSL Compression Used
- Session Undecryptable in Passive Mode
- Handshake Error
- Decryption Error
- Pending Server Name Category Lookup
- Pending Common Name Category Lookup
- Internal Error
- Network Parameters Unavailable
- Invalid Server Certificate Handle
- Server Certificate Fingerprint Unavailable
- Cannot Cache Subject DN
- Cannot Cache Issuer DN
- Unknown SSL Version
- External Certificate List Unavailable
- External Certificate Fingerprint Unavailable
- Internal Certificate List Invalid
- Internal Certificate List Unavailable
- Internal Certificate Unavailable
- Internal Certificate Fingerprint Unavailable
- Server Certificate Validation Unavailable
- Server Certificate Validation Failure
- Invalid Action

SSLPolicy

The SSL policy that handled the connection.

Starting in release 6.7: If TLS server identity discovery is enabled in the access control policy advanced settings, and there is no SSL policy associated with the access control policy, this field holds `none` for all SSL events.

SSLRuleName

The SSL rule or default action that handled the connection, as well as the first Monitor rule matched by that connection. If the connection matched a Monitor rule, the field displays the name of the rule that handled the connection, followed by the Monitor rule name.

SSLServerCertStatus

This applies only if you configured a Certificate Status SSL rule condition. If encrypted traffic matches an SSL rule, this field displays one or more of the following server certificate status values:

- Self Signed
- Valid
- Invalid Signature
- Invalid Issuer
- Expired
- Unknown
- Not Valid Yet
- Revoked

If undecryptable traffic matches an SSL rule, this field displays `Not Checked`.

SSLServerName

Hostname of the server with which the client established an encrypted connection.

SSLSessionID

The hexadecimal Session ID negotiated between the client and server during the TLS/SSL handshake.

SSLTicketID

A hexadecimal hash value of the session ticket information sent during the TLS/SSL handshake.

SSLURLCategory

URL categories for the URL visited in the encrypted connection.

If the system identifies or blocks a TLS/SSL application, the requested URL is in encrypted traffic, so the system identifies the traffic based on an SSL certificate. For TLS/SSL applications, therefore, this field indicates the common name contained in the certificate.

SSLVersion

The TLS/SSL protocol version used to encrypt the connection:

- Unknown
- SSLv2.0
- SSLv3.0
- TLSv1.0
- TLSv1.1
- TLSv1.2

SSSLCipherSuite

A macro value representing a cipher suite used to encrypt the connection. See www.iana.org/assignments/tls-parameters/tls-parameters.xhtml for cipher suite value designations.

TCPFlags

For connections generated from NetFlow data, the TCP flags detected in the connection.

Tunnel or Prefilter Rule

The tunnel rule, prefilter rule, or prefilter policy default action that handled the connection.

URL

The URL requested by the monitored host during the session.

Starting in release 6.7 as an experimental feature:

If the URL column is empty and DNS filtering is enabled, the DNS Query field shows the domain, and the URL Category and URL Reputation values apply to the domain.

URLCategory

The category, if available, of the URL requested by the monitored host during the session.

Starting in release 6.7 as an experimental feature:

If the URL column is empty and DNS filtering is enabled, the DNS Query field shows the domain, and the URL Category and URL Reputation values apply to the domain.

URLReputation

The reputation, if available, of the URL requested by the monitored host during the session.

Starting in release 6.7 as an experimental feature:

If the URL column is empty and DNS filtering is enabled, the DNS Query field shows the domain, and the URL Category and URL Reputation values apply to the domain.

URLSICategory, DNSSICategory, IPReputationSICategory

The name of the object that represents or contains the blocked URL, domain, or IP address in the connection. The Security Intelligence category can be the name of a network object or group, a Block list, a custom Security Intelligence list or feed, a TID category related to an observation, or one of the categories in the Intelligence Feed.

User

The user logged into the session initiator. If this field is populated with **No Authentication**, the user traffic:

- matched an access control policy without an associated identity policy
- did not match any rules in the identity policy

Starting in release 6.5: If applicable, the username is preceded by `<realm>\`.

UserAgent

The user-agent string application information extracted from HTTP traffic detected in the connection.

VLAN_ID

This field became available in syslog in version 6.3.

The innermost VLAN ID associated with the packet that triggered the connection.

WebApplication

The web application, which represents the content or requested URL for HTTP traffic detected in the connection.

If the web application does not match the URL for the event, the traffic is probably referred traffic, such as advertisement traffic. If the system detects referred traffic, it stores the referring application (if available) and lists that application as the web application.

If the system cannot identify the specific web application in HTTP traffic, this field displays `Web Browsing`.

File and Malware Event Field Descriptions

Syslog messages for file and malware events became available in release 6.4.

Note

- Fields with empty or unknown values are not included in security event syslog messages. However, verdicts with "Unknown" or similar values are included in file and malware event messages.
- Status field values for file and malware events reflect only the initial status; these fields do not update.

ApplicationProtocol

The application protocol used by the traffic in which a managed device detected the file.

ArchiveDepth

The level (if any) at which the file was nested in an archive file.

ArchiveFileName

The name of the archive file (if any) which contained the malware file.

ArchiveFileStatus

The status of an archive being inspected. Can have the following values:

- Pending — Archive is being inspected
- Extracted — Successfully inspected without any problems
- Failed — Failed to inspect, insufficient system resources
- Depth Exceeded — Successful, but archive exceeded the nested inspection depth
- Encrypted — Partially successful, archive was or contains an archive that is encrypted
- Not Inspectable — Partially successful, file is possibly malformed or corrupt

ArchiveSHA256

The SHA-256 hash value of the archive file (if any) which contains the malware file.

Client

The client application that runs on one host and relies on a server to send a file.

Connection Counter

This field was added in release 6.5.

A counter that distinguishes one connection from another simultaneous connection. This field has no significance on its own.

The follwing fields collectively uniquely identify the connection event associated with a particular file or malware event: DeviceUUID, First Packet Time, Connection Instance ID, and Connection Counter.

Connection Instance ID

This field was added in release 6.5.

The Snort instance that processed the connection event. This field has no significance on its own.

The follwing fields collectively uniquely identify the connection event associated with a particular file or malware event: DeviceUUID, First Packet Time, Connection Instance ID, and Connection Counter.

DeviceUUID

This field was added in release 6.5.

The unique identifier of the device that generated an event.

The follwing fields collectively uniquely identify the connection event associated with a particular file or malware event: DeviceUUID, First Packet Time, Connection Instance ID, and Connection Counter.

DstIP

The IP address of the host that responded to the connection. This may be the IP address of the sender or the recipient of the file, depending on the value in the FileDirection field:

If FileDirection is **`Upload`**, then this is the IP address of the file recipient.

If FileDirection is **`Download`**, then this is the IP address of the file sender.

See also **SrcIP**.

DstPort

The port used in the connection described under **DstIP**.

FileAction

The action associated with file policy rule that detected the file, and any associated file rule action options.

FileDirection

Whether the file was downloaded or uploaded during the connection. Possible values are:

- Download — the file was transferred from the DstIP to the SrcIP.
- Upload — the file was transferred from the SrcIP to the DstIP.

FileName

The name of the file.

FilePolicy

The file policy that detected the file.

FileSandboxStatus

Indicates whether the file was sent for dynamic analysis and if so, the status.

FileSHA256

The SHA-256 hash value of the file.

To have a SHA256 value, the file must have been handled by one of:

- a Detect Files file rule with **Store files** enabled
- a Block Files file rule with **Store files** enabled
- a Malware Cloud Lookup file rule
- a Block Malware file rule

FileSize

The size of the file, in bytes.

Note that if the system determines the file type of a file before the file is fully received, the file size may not be calculated.

FileStorageStatus

The storage status of the file associated with the event:

Stored

Returns all events where the associated file is currently stored.

Stored in connection

Returns all events where the system captured and stored the associated file, regardless of whether the associated file is currently stored.

Failed

Returns all events where the system failed to store the associated file.

Syslog fields contain only the initial status; they do not update to reflect changed status.

FileType

The type of file, for example, HTML or MSEXE.

First Packet Time

The time the system encountered the first packet.

The follwing fields collectively uniquely identify the connection event associated with a particular file or malware event: DeviceUUID, First Packet Time, Connection Instance ID, and Connection Counter.

FirstPacketSecond

The time at which the file download or upload flow started.

The time the event occurred is captured in the message header timestamp.

Protocol

The protocol used for the connection, for example TCP or UDP.

SHA_Disposition

The file's disposition:

Clean

Indicates that the AMP cloud categorized the file as clean, or that a user added the file to the clean list. Clean files appear in the malware table only if they were changed to clean.

Custom Detection

Indicates that a user added the file to the custom detection list.

Malware

Indicates that the AMP cloud categorized the file as malware, local malware analysis identified malware, or the file's threat score exceeded the malware threshold defined in the file policy.

Unavailable

Indicates that the system could not query the AMP cloud. You may see a small percentage of events with this disposition; this is expected behavior.

Unknown

Indicates that the system queried the AMP cloud, but the file has not been assigned a disposition; in other words, the AMP cloud has not categorized the file.

File dispositions appear only for files for which the system queried the AMP cloud.

Syslog fields reflect only the initial disposition; they do not update to reflect retrospective verdicts.

SperoDisposition

Indicates whether the SPERO signature was used in file analysis. Possible values:

- Spero detection performed on file
- Spero detection not performed on file

SrcIP

The IP address of the host that initiated the connection. This may be the IP address of the sender or the recipient of the file, depending on the value in the FileDirection field:

If FileDirection is **`Upload`**, this is the IP address of the file sender.

If FileDirection is **Download**, this is the IP address of the file recipient.

See also **DstIP**.

SrcPort

The port used in the connection described under **SrcIP**.

SSLActualAction

The action the system applied to encrypted traffic:

Block or Block with reset

Represents blocked encrypted connections.

Decrypt (Resign)

Represents an outgoing connection decrypted using a re-signed server certificate.

Decrypt (Replace Key)

Represents an outgoing connection decrypted using a self-signed server certificate with a substituted public key.

Decrypt (Known Key)

Represents an incoming connection decrypted using a known private key.

Default Action

Indicates the connection was handled by the default action.

Do not Decrypt

Represents a connection the system did not decrypt.

SSLCertificate

The certificate fingerprint of the TLS/SSL server.

SSLFlowStatus

The reason the system failed to decrypt encrypted traffic:

- Unknown
- No Match
- Success
- Uncached Session
- Unknown Cipher Suite
- Unsupported Cipher Suite
- Unsupported SSL Version
- SSL Compression Used
- Session Undecryptable in Passive Mode

- Handshake Error
- Decryption Error
- Pending Server Name Category Lookup
- Pending Common Name Category Lookup
- Internal Error
- Network Parameters Unavailable
- Invalid Server Certificate Handle
- Server Certificate Fingerprint Unavailable
- Cannot Cache Subject DN
- Cannot Cache Issuer DN
- Unknown SSL Version
- External Certificate List Unavailable
- External Certificate Fingerprint Unavailable
- Internal Certificate List Invalid
- Internal Certificate List Unavailable
- Internal Certificate Unavailable
- Internal Certificate Fingerprint Unavailable
- Server Certificate Validation Unavailable
- Server Certificate Validation Failure
- Invalid Action

ThreatName

The name of the detected malware.

ThreatScore

The threat score most recently associated with this file. This is a value from 0 to 100 based on the potentially malicious behaviors observed during dynamic analysis.

URI

The URI of the connection associated with the file transaction, for example, the URL from which a user downloaded the file.

User

The username associated with the IP address that initiated the connection. If this IP address is external to your network, the associated username is typically unknown.

Starting in release 6.5: If applicable, the username is preceded by `<realm>\`.

For file events and for malware events generated by Firewall devices, this field displays the username that was determined by an identity policy or authoritative logins. In absence of an identity policy, it displays *No Authentication Required*.

WebApplication

The application that represents the content or requested URL for HTTP traffic detected in the connection.

History for Security Event Syslog Messages

Feature	Version	Details
Updates for DNS Filtering	7.0 6.7 (Experimental feature)	When DNS filtering is enabled: • The DNSQuery field may hold the domain associated with DNS filtering matches. • If the URL field is empty but DNSQuery, URLCategory, and URLReputation have values, the event was generated by the DNS filtering feature, and the category and reputation apply to the domain specified in DNSQuery. • For additional information, see information about DNS filtering and events in the management center online help.
New connection event fields for SGT and VRF	6.6	New Security Group fields: • DestinationSecurityGroupType • SourceSecurityGroupType New Virtual Routing and Forwarding fields: • IngressVRF • EgressVRF
New connection event fields for SGT	6.5	New Security Group fields: • SourceSecurityGroup • SourceSecurityGroupTag (Replaces the Security Group field.) • DestinationSecurityGroup • DestinationSecurityGroupTag
New connection event field: Event Priority	6.5	The Event Priority field was introduced.
Unique identifier for connection event in syslogs	6.5	The following syslog fields collectively uniquely identify a connection event and also appear in syslog for intrusion, file, and malware events: DeviceUUID, First Packet Time, Connection Instance ID, an Connection Counter.

Feature	Version	Details
Syslog support for File and Malware events	6.4	File and malware event fields are now available via syslog. For details, see Security Event Syslog Message IDs, on page 1 and File and Malware Event Field Descriptions, on page 17.
Intrusion Policy field added to intrusion events field list	6.4	Intrusion event syslogs now specify the intrusion policy that triggered the event.
Improved support for connection and intrusion events	6.3	Connection events, security intelligence events, and intrusion events are now available as fully-qualified events.
Event type IDs for security events	6.3	Messages for connection, security intelligence, and intrusion events include an event type ID in the message header. For details, see Security Event Syslog Message IDs, on page 1.
Omission of empty and unknown values from security event messages	6.3	Fields with empty or unknown values are omitted from syslog messages for connection, security intelligence, and intrusion events.
Documentation improvement	6.3	Added documentation for syslog field names and descriptions for connection, security intelligence, and intrusion events. (This functionality is not new in this release.)
Firepower (SFIMS) event log format	6.2.2	Apr 30 04:33:28 192.168.1.1 Apr 30 13:57:38 firepower SFIMS: Protocol: ICMP, SrcIP: 172.16.10.10, OriginalClientIP: ::, DstIP: 172.16.20.10, ICMPType: Echo Request, ICMPCode: 0, TCPFlags: 0x0, IngressInterface: inside, EgressInterface: outside, DE: Primary Detection Engine (e357206c-a9b0-11eb-93fe-a690508a381d), Policy: Default Allow All Traffic, ConnectType: Start, AccessControlRuleName: test, AccessControlRuleAction: Allow, Prefilter Policy: Unknown, UserName: No Authentication Required, Client: ICMP client, ApplicationProtocol: ICMP, InitiatorPackets: 1, ResponderPackets: 0, InitiatorBytes: 74, ResponderBytes: 0, NAPPolicy: Balanced Security and Connectivity, DNSResponseType: No Error, Sinkhole: Unknown, URLCategory: Unknown, URLReputation: Risk unknown
Firepower (null) event log format	6.6.3	Apr 30 02:07:02 192.168.1.1 2021-04-30T11:31:19Z firepower (null) %NGIPS-1-430002: EventPriority: Low, DeviceUUID: b2433c5c-a6a1-11eb-a6e7-be0b9833091f, InstanceID: 2, FirstPacketSecond: 2021-04-30T11:31:19Z, ConnectionID: 4, AccessControlRuleAction: Allow, SrcIP: 172.16.10.10, DstIP: 172.16.20.10, ICMPType: Echo Request, ICMPCode: No Code, Protocol: icmp, IngressInterface: inside, EgressInterface: outside, ACPolicy: Default Allow All Traffic, AccessControlRuleName: test, Client: ICMP client, ApplicationProtocol: ICMP, InitiatorPackets: 1, ResponderPackets: 0, InitiatorBytes: 74, ResponderBytes: 0, NAPPolicy: Balanced Security and Connectivity