Schema: File Event Tables

This chapter contains information on the schema and supported joins for file events. For more information, see the section listed in the following table.

Table 10-1 Schema for File Event Tables

See...	For the table that stores information on...	Version
file_event, page 10-1	File events generated when file transfers are detected in the monitored network.	5.1.1+

While the following tables are available, Cisco does not currently support lookups on them:

- `file_categories`
- `file_rules`
- `file_types`
- `file_type_rule_map`
- `file_type_category_map`

file_event

The **`file_event`** table contains information about the file events that your Firepower Management Center generates. A new file event is generated each time a file transfer is detected on the monitored network. Files identified as malware by AMP for Firepower generate both a file event and a malware event. Endpoint-based malware events do not have corresponding file events, and file events do not have AMP for Endpoints-related fields.

For more information, see the following sections:

- file_event Fields, page 10-2
- file_event Joins, page 10-5
- file_event Sample Query, page 10-6

file_event Fields

The **file_event** table contains information on files that are detected passing through the monitored network. Each file event can be correlated with a connection event. Details of the file and file transfer are recorded, including the name, size, source, destination, and direction of the file, a SHA256 hash of the file, the device that detected the file, and whether it is considered to be malware.

Table 10-2 file_event Fields

Field	Description
action	The action taken on the file based on the file type. Can have the following values: • 1 — Detect • 2 — Block • 3 — Malware Cloud Lookup • 4 — Malware Block • 5 — Malware Whitelist • 6 — Cloud Lookup Timeout
application_id	ID number that maps to the application using the file transfer.
application_name	One of the following: • the name of the application used in the connection • pending or unknown if the system cannot identify the application • blank if there is no application information in the connection
archived	Indicates whether the file has been archived.
cert_valid_end_date	The Unix timestamp on which the SSL certificate used in the connection ceases to be valid.
cert_valid_start_date	The Unix timestamp when the SSL certificate used in the connection was issued.
client_application_id	The internal identification number for the client application, if applicable.
client_application_name	The name of the client application, if applicable.
connection_sec	UNIX timestamp (seconds since 00:00:00 01/01/1970) of the connection event associated with the file event.
counter	Specific counter for the event, used to distinguish among multiple events that happened during the same second.
direction	Whether the file was uploaded or downloaded. Currently the value depends entirely on the protocol (for example, if the connection is HTTP it is a download).
disposition	The malware status of the file. Possible values include: • CLEAN — The file is clean and does not contain malware. • UNKNOWN — It is unknown whether the file contains malware. • MALWARE — The file contains malware. • UNAVAILABLE — The software was unable to send a request to the Cisco cloud for a disposition, or the Cisco cloud services did not respond to the request. • CUSTOM SIGNATURE — The file matches a user-defined hash, and is treated in a fashion designated by the user.

Table 10-2 file_event Fields (continued)

Field	Description
domain_name	Name of the domain on which the .event was detected
domain_uuid	UUID of the domain on which the event was detected. This is presented in binary.
dst_continent_name	The name of the continent of the destination host. ** — Unknown na — North America as — Asia af — Africa eu — Europe sa — South America au — Australia an — Antarctica
dst_country_id	Code for the country of the destination host.
dst_country_name	Name of the country of the destination host.
dst_ip_address_v6	Field deprecated in Version 5.2. Returns null for all queries.
dst_ipaddr	A binary representation of the IP address of the destination host involved in the triggering event.
dst_port	Port number for the destination of the connection.
event_description	The additional event information associated with the event type.
event_id	Event identification number.
file_name	Name of the detected file. This name can contain UTF-8 characters.
file_sha	SHA256 hash of the file.
file_size	Size of the detected file in bytes.
file_type	The file type of the detected or quarantined file.
file_type_category	Description of the file category.
file_type_category_id	Numeric identifier for the file category.
file_type_id	ID number that maps to the file type.
http_response_code	The response code given to the HTTP request in the event.
instance_id	Numerical ID of the Snort instance on the managed device that generated the event.
netmap_num	Netmap ID for the domain on which the event was detected.
policy_uuid	Identification number that acts as a unique identifier for the access control policy that triggered the event.

Table 10-2 file_event Fields (continued)

Field	Description
sandboxed	Indicates whether the file was sent for dynamic analysis. Possible values are: • Sent for Analysis • Failed to Send • File Size is Too Small • File Size is Too Large • Sent for Analysis • Analysis Complete • Failure (Network Issue) • Failure (Rate Limit) • Failure (File Too Large) • Failure (File Read Error) • Failure (Internal Library Error) • File Not Sent, Disposition Unavailable • Failure (Cannot Run File) • Failure (Analysis Timeout) • File Not Supported
score	A numeric value from 0 to 100 based on the potentially malicious behaviors observed during dynamic analysis.
security_context	Description of the security context (virtual firewall) that the traffic passed through. Note that the system only populates this field for ASA FirePOWER devices in multi-context mode.
sensor_address	A binary representation of the IP address of the device that provided the event.
sensor_id	ID for the device that provided the event.
sensor_name	The text name of the managed device that generated the event record. This field is null when the event refers to the reporting device itself, rather than to a connected device.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.
signature_processed	Indicated whether the file's signature was processed.
src_continent_name	The name of the continent of the source host. ** — Unknown na — North America as — Asia af — Africa eu — Europe sa — South America au — Australia an — Antarctica

Table 10-2 file_event Fields (continued)

Field	Description
src_country_id	Code for the country of the source host.
src_country_name	Name of the country of the source host.
src_ip_address_v6	Field deprecated in Version 5.2. Returns null for all queries.
src_ipaddr	A binary representation of the IPv4 or IPv6 address of the source host involved in the triggering event.
src_port	Port number for the source of the connection.
ssl_issuer_common_name	Issuer Common Name from the SSL certificate. This is typically the host and domain name of the certificate issuer, but may contain other information.
ssl_issuer_country	The country of the SSL certificate issuer.
ssl_issuer_organization	The organization of the SSL certificate issuer.
ssl_issuer_organization_unit	The organizational unit of the SSL certificate issuer.
ssl_serial_number	The serial number of the SSL certificate, assigned by the issuing CA.
ssl_subject_common_name	Subject Common name from the SSL certificate. This is typically the host and domain name of the certificate subject, but may contain other information.
ssl_subject_country	The country of the SSL certificate subject.
ssl_subject_organization	The organization of the SSL certificate subject.
ssl_subject_organization_unit	The organizational unit of the SSL certificate subject.
storage	The storage status of the file. Possible values are: • File Stored • Unable to Store File • File Size is Too Large • File Size is Too Small • Unable to Store File • File Not Stored, Disposition Unavailable
threat_name	Name of the threat.
timestamp	UNIX timestamp when enough of the file has been transmitted to identify the file type.
url	URL of the file source.
user_id	The internal identification number for the destination user; that is, the user who last logged into the destination host before the event occurred.
username	Name associated with the user_id.
web_application_id	The internal identification number for the web application, if applicable.
web_application_name	Name of the web application, if applicable.

file_event Joins

The following table describes the joins you can perform on the **file_event** table.

Table 10-3 file_event Joins

You can join this table on...	And...
application_id	application_info.application_id application_host_map.application_id application_tag_map.application_id rna_host_service_info.application_protocol_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id

file_event Sample Query

The following query returns up to 10 file events with the application name, connection information, and file name, where the disposition is not CLEAN.

```
SELECT file_event.application_name, file_event.connection_sec, file_event.counter,
file_event.file_name
FROM file_event
WHERE file_event.disposition != "CLEAN" limit 10;
```