



## 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
<a href="#">file_event, page 10-1</a>	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
<code>action</code>	The action taken on the file based on the file type. Can have the following values: <ul style="list-style-type: none"> <li>1 — Detect</li> <li>2 — Block</li> <li>3 — Malware Cloud Lookup</li> <li>4 — Malware Block</li> <li>5 — Malware Whitelist</li> <li>6 — Cloud Lookup Timeout</li> </ul>
<code>application_id</code>	ID number that maps to the application using the file transfer.
<code>application_name</code>	One of the following: <ul style="list-style-type: none"> <li>the name of the application used in the connection</li> <li><code>pending</code> or <code>unknown</code> if the system cannot identify the application</li> <li>blank if there is no application information in the connection</li> </ul>
<code>archived</code>	Indicates whether the file has been archived.
<code>cert_valid_end_date</code>	The Unix timestamp on which the SSL certificate used in the connection ceases to be valid.
<code>cert_valid_start_date</code>	The Unix timestamp when the SSL certificate used in the connection was issued.
<code>client_application_id</code>	The internal identification number for the client application, if applicable.
<code>client_application_name</code>	The name of the client application, if applicable.
<code>connection_sec</code>	UNIX timestamp (seconds since 00:00:00 01/01/1970) of the connection event associated with the file event.
<code>counter</code>	Specific counter for the event, used to distinguish among multiple events that happened during the same second.
<code>direction</code>	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).
<code>disposition</code>	The malware status of the file. Possible values include: <ul style="list-style-type: none"> <li><code>CLEAN</code> — The file is clean and does not contain malware.</li> <li><code>UNKNOWN</code> — It is unknown whether the file contains malware.</li> <li><code>MALWARE</code> — The file contains malware.</li> <li><code>UNAVAILABLE</code> — 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.</li> <li><code>CUSTOM SIGNATURE</code> — The file matches a user-defined hash, and is treated in a fashion designated by the user.</li> </ul>

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: <ul style="list-style-type: none"> <li>• Sent for Analysis</li> <li>• Failed to Send</li> <li>• File Size is Too Small</li> <li>• File Size is Too Large</li> <li>• Sent for Analysis</li> <li>• Analysis Complete</li> <li>• Failure (Network Issue)</li> <li>• Failure (Rate Limit)</li> <li>• Failure (File Too Large)</li> <li>• Failure (File Read Error)</li> <li>• Failure (Internal Library Error)</li> <li>• File Not Sent, Disposition Unavailable</li> <li>• Failure (Cannot Run File)</li> <li>• Failure (Analysis Timeout)</li> <li>• File Not Supported</li> </ul>
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. <ul style="list-style-type: none"> <li>** — Unknown</li> <li>na — North America</li> <li>as — Asia</li> <li>af — Africa</li> <li>eu — Europe</li> <li>sa — South America</li> <li>au — Australia</li> <li>an — Antarctica</li> </ul>

**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: <ul style="list-style-type: none"> <li>• File Stored</li> <li>• Unable to Store File</li> <li>• File Size is Too Large</li> <li>• File Size is Too Small</li> <li>• Unable to Store File</li> <li>• File Not Stored, Disposition Unavailable</li> </ul>
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;
```