


# Schema: System-Level Tables

This chapter contains information on the schema and supported joins for system-level functions, including auditing, appliance health monitoring, malware detection, and logging of security updates.

For more information, see the sections listed in the following table.

*Table 3-1 Schema for System-Level Tables*

| See... | For the table that stores information on... | Version |
|---|---|---|
| audit_log, page 3-1 | User interactions with the appliance's web interface. | 4.10.x+ |
| fireamp_event, page 3-2 | AMP for Endpoints malware detection and quarantine events. | 5.1+ |
| health_event, page 3-8 | Health status events for monitored appliances. | 4.10.x+ |
| syslog_event, page 3-10 | Syslog events for monitored appliances. | 7.2+ |

# audit_log

The **audit_log** table contains information on Secure Firewall users' interactions with the web interface. Keep in mind that the audit log stores records for the local appliance only, not for managed appliances.

For more information, see the following sections:

- audit_log Fields, page 3-1
- audit_log Joins, page 3-2
- audit_log Sample Query, page 3-2

## audit_log Fields

The following table describes the database fields you can access in the **audit_log** table.

*Table 3-2 audit_log Fields*

| Field | Description |
|---|---|
| action_time_sec | The UNIX timestamp of the date and time the appliance generated the audit record. |
| domain_name | Name of the domain in which the user logged in. |
| domain_uuid | UUID of the domain in which the user logged in. This is expressed in binary. |

*Table 3-2 audit_log Fields (continued)*

| Field | Description |
|---|---|
| message | The action the user performed. |
| source | The IP address of the web interface user's host, in dotted-decimal notation. |
| subsystem | The menu path the user followed to generate the audit record. |
| user | The user name of the user who triggered the audit event. |

## audit_log Joins

You cannot perform joins on the **audit_log** table.

## audit_log Sample Query

The following query returns up to the 25 most recent audit log entries, sorted by time and limited to the `Global \ Company B \ Edge` domain.

```
SELECT from_unixtime(action_time_sec)
AS Time, user, subsystem, message, source, count(*)
AS Total
FROM audit_log
GROUP BY source, subsystem, user, message
WHERE domain_name= "Global \ Company B \ Edge"
ORDER BY source DESC;
```

# fireamp_event

The **fireamp_event** table contains information on malware events detected by AMP for Endpoints as well as network-based events detected by AMP for Firepower. These events contain information on malware detected or quarantined within a cloud, the detection method, and hosts and users affected by the malware. Other information for an individual malware event can vary depending on how and why it was generated.

Because AMP for Firepower detect malware files in network traffic, network-based malware events contain port, application protocol, and originating IP address information about the connection used to transmit the file.

Malware events and IOCs imported from your AMP for Endpoints deployment do not contain contextual connection information, but they do include information obtained at download or execution time, such as file path, invoking client application, and similar information.

For more information, see the following sections:

- fireamp_event Fields, page 3-3
- fireamp_event Joins, page 3-8
- fireamp_event Sample Query, page 3-8

# fireamp_event Fields

The following table describes the database fields you can access in the **`fireamp_event`** table.

***Table 3-3 fireamp_event Fields***

| Field | Description |
|---|---|
| `application_id` | ID number that maps to the application performing the file transfer. |
| `application_name` | Name of the application performing the transfer. |
| `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. |
| `cloud_name` | The name of the cloud service from which the malware event originated. Each `cloud_name` value has an associated `cloud_uuid` value. |
| `cloud_uuid` | The internal unique ID of the cloud service from which the malware event originated. Each `cloud_uuid` value has an associated `cloud_name` value. |
| `connection_sec` | UNIX timestamp (seconds since 00:00:00 01/01/1970) of the connection event associated with the malware event. |
| `counter` | Specific counter for the event, used to distinguish among multiple events that happened during the same second. |
| `detection_name` | The name of the detected or quarantined malware. |
| `detector_type` | The detector that detected the malware. Each `detector_type` value has an associated `detector_type_id`. The possible display values and the associated IDs are:<br>• `ClamAV` — 128<br>• `ETHOS` — 8<br>• `SPERO` — 32<br>• `SHA` — 4<br>• `Tetra` — 64 |
| `detector_type_id` | The internal ID of the detection technology that detected the malware. Each `detector_type_id` value has an associated `detector_type` value. The possible display values and the associated types are:<br>• `4` — SHA<br>• `8` — ETHOS<br>• `32` — SPERO<br>• `64` — Tetra<br>• `128` — ClamAV |

*Table 3-3 fireamp_event Fields (continued)*

| Field | Description |
|---|---|
| direction | Value that indicates whether the file was uploaded or downloaded. Can have the following values:<br>• Download<br>• Upload<br>Currently the value depends on the protocol (for example, if the connection is HTTP it is a download). |
| disposition | The malware status of the file. Possible values include:<br>• CLEAN — The file is clean and does not contain malware.<br>• UNKNOWN — It is unknown whether the file contains malware.<br>• MALWARE — The file contains malware.<br>• 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.<br>• CUSTOM SIGNATURE — The file matches a user-defined hash, and is treated in a fashion designated by the user. |
| domain_name | Name of the domain in which the event was detected. |
| domain_uuid | UUID of the domain in which the event was detected. This is expressed in binary. |
| dst_continent_name | The name of the continent of the destination host.<br>** — Unknown<br>na — North America<br>as — Asia<br>af — Africa<br>eu — Europe<br>sa — South America<br>au — Australia<br>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 | This field has been deprecated and will now return null. |
| dst_ipaddr | A binary representation of the IPv4 or IPv6 address for the destination of the connection. |
| dst_ipaddr_str | The IP address of the destination of the connection in a human-readable format. |
| dst_port | Port number for the destination of the connection. |
| endpoint_user | The user determined by the Cisco AMP for Endpoints agent if the event was detected by the Cisco cloud. This user is not associated with LDAP and does not appear in the discovered_users table. |
| event_description | The additional event information associated with the event type. |
| event_id | The internal unique ID of the malware event. |

*Table 3-3 fireamp_event Fields (continued)*

| Field | Description |
|---|---|
| event_subtype | The action that led to malware detection. Each event_subtype value has an associated event_subtype_id value. The possible display values and the associated IDs are:<br>• Create — 1<br>• Execute — 2<br>• Move — 22<br>• Scan — 4 |
| event_subtype_id | The internal ID of the action that led to malware detection. Each event_subtype_id value has an associated event_subtype value. The possible display values and the associated subtypes are:<br>• 1 — Create<br>• 2 — Execute<br>• 4 — Scan<br>• 22 — Move |
| event_type | The type of malware event. Each event_type value has an associated event_type_id value. The possible display values and the associated IDs are:<br>• Blocked Execution — 553648168<br>• Cloud Recall Quarantine — 553648155<br>• Cloud Recall Quarantine Attempt Failed — 2164260893<br>• Cloud Recall Quarantine Started — 553648147<br>• Cloud Recall Restore from Quarantine — 553648154<br>• Cloud Recall Restore from Quarantine Failed — 2164260892<br>• Cloud Recall Restore from Quarantine Started — 553648146<br>• FireAMP IOC — 1107296256<br>• Quarantine Failure — 2164260880<br>• Quarantined Item Restored — 553648149<br>• Quarantine Restore Failed — 2164260884<br>• Quarantine Restore Started — 553648150<br>• Scan Completed, No Detections — 554696715<br>• Scan Completed With Detections — 1091567628<br>• Scan Failed — 2165309453<br>• Scan Started — 554696714<br>• Threat Detected — 1090519054<br>• Threat Detected in Exclusion — 553648145<br>• Threat Detected in Network File Transfer — 1<br>• Threat Detected in Network File Transfer (Retrospective) — 2<br>• Threat Quarantined — 553648143 |

*Table 3-3 fireamp_event Fields (continued)*

| Field | Description |
|---|---|
| event_type_id | The internal ID of the malware event type. Each event_type_id value has an associated event_type value. The possible display values and the associated types are:<br>• 553648143 — Threat Quarantined<br>• 553648145 — Threat Detected in Exclusion<br>• 553648146 — Cloud Recall Restore from Quarantine Started<br>• 553648147 — Cloud Recall Quarantine Started<br>• 553648149 — Quarantined Item Restored<br>• 553648150 — Quarantine Restore Started<br>• 553648154 — Cloud Recall Restore from Quarantine<br>• 553648155 — Cloud Recall Quarantine<br>• 553648168 — Blocked Execution<br>• 554696714 — Scan Started<br>• 554696715 — Scan Completed, No Detections<br>• 1090519054 — Threat Detected<br>• 1091567628 — Scan Completed With Detections<br>• 1107296256 — FireAMP IOC<br>• 2164260880 — Quarantine Failure<br>• 2164260893 — Cloud Recall Quarantine Attempt Failed<br>• 2164260884 — Quarantine Restore Failed<br>• 2164260892 — Cloud Recall Restore from Quarantine Failed<br>• 2165309453 — Scan Failed |
| file_name | The name of the detected or quarantined file. This name can contain UTF-8 characters. |
| file_path | The file path, not including the file name, of the detected or quarantined file. This path can contain UTF-8 characters. |
| file_sha | The SHA-256 hash value of the detected or quarantined file. |
| file_size | The size in bytes of the detected or quarantined file. |
| file_timestamp | The creation timestamp of the detected or quarantined file. |
| file_type | The file type of the detected or quarantined file. |
| file_type_id | The internal ID of the file type of the detected or quarantined file. |
| 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. |
| ioc_count | Number of indications of compromise found in the event. |
| parent_file_name | The name of the file accessing the detected or quarantined file when detection occurred. |
| parent_file_sha | The SHA-256 hash value of the parent file accessing the detected or quarantined file when detection occurred. |
| policy_uuid | Identification number that acts as a unique identifier for the access control policy that triggered the event. |

*Table 3-3 fireamp_event Fields (continued)*

| Field | Description |
|---|---|
| retroactive_ disposition | Disposition of the file if the disposition is updated. If the disposition is not updated, this field contains the same value as the disposition field. The possible values are the same as the disposition field. |
| 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 | This field has been deprecated. Use sensor_name and sensor_uuid to identify the device that generated the event. |
| sensor_id | ID of the device that generated 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 fireamp_event.sensor_name is null. |
| src_continent_name | The name of the continent of the source host.<br>** — Unknown<br>na — North America<br>as — Asia<br>af — Africa<br>eu — Europe<br>sa — South America<br>au — Australia<br>an — Antarctica |
| 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 for the source of the connection. |
| src_ipaddr_str | The IP address of the source of the connection in a human-readable format. |
| 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. |

*Table 3-3 fireamp_event Fields (continued)*

| Field | Description |
|---|---|
| ssl_subject_organization | The organization of the SSL certificate subject. |
| ssl_subject_organization_unit | The organizational unit of the SSL certificate subject. |
| threat_name | Name of the threat. |
| timestamp | The malware event generation timestamp. |
| timestamp_str | The date and time when the malware event was generated in human-readable format of `Year-Month-Day Time`. For example, February 4th, 2022 is `2022-02-04 20:18:58`. |
| url | The URL of the source of the connection. |
| user_id | An internal identification number for the user who last logged into the host that sent or received the file. This user is in the **discovered_users** table. |
| username | The name of the user who last logged into the host that sent or received the file. |
| web_application_id | The internal identification number for the web application, if applicable. |
| web_application_name | Name of the web application, if applicable. |

## fireamp_event Joins

You cannot perform joins on the **fireamp_event** table

## fireamp_event Sample Query

The following query returns 25 malware events associated with the specified user, sorted by `timestamp` in ascending order.

```
SELECT event_id, timestamp, src_ipaddr, dst_ipaddr, username, cloud_name, event_type,
event_subtype, event_description, detection_name, detector_type, file_name,
parent_file_name

FROM fireamp_event

WHERE username="username" ORDER BY timestamp ASC

LIMIT 25;
```

# health_event

The **health_event** table contains information on health events generated by the Secure Firewall.

For more information, see the following sections:


- health_event Fields, page 3-9
- health_event Joins, page 3-9
- health_event Sample Query, page 3-10

# health_event Fields

The following table describes the database fields you can access in the **health_event** table.

***Table 3-4 health_event Fields***

| Field | Description |
|---|---|
| description | The description of the condition that caused the associated health module to generate the health event. For example, health events generated when a process was unable to execute are labeled Unable to Execute. |
| domain_name | Name of the domain in which the event was detected. |
| domain_uuid | UUID of the domain in which the event was detected. This is presented in binary. |
| event_time_sec | The UNIX timestamp of the date and time the Secure Firewall Management Center generated the health event. |
| id | The internal identification number for the event. |
| module_name | The name of the health module that generated the event. |
| sensor_name | The text name of the managed device that generated the event record. This field is **null** when the health event refers to the reporting device itself, rather than to a connected one. |
| sensor_uuid | A unique identifier for the managed device, or zero if sensor_name is null. |
| status | The health monitor status that has been reported for the appliance identified in sensor_uuid. Values are:<br>• red — Critical status. Limits have been exceeded for at least one health module on the appliance and the problem has not been corrected.<br>• yellow — Warning status. Limits have been exceeded for at least one health module on the appliance and the problem has not been corrected.<br>• green — Normal status. All health modules on the appliance are running within the limits configured in the health policy applied to the appliance.<br>• recovered — All health modules on the appliance are running within the limits configured in the health policy applied to the appliance, including modules that were in a Critical or Warning state.<br>• disabled — Either the appliance is disabled or on a block list, or is currently unreachable, or has no health policy applied to it.<br>• error — At least one health monitoring module has failed on the appliance and has not been successfully re-run since the failure occurred |
| units | The unit of measure for results obtained by the health test. For example, **%** (of Disk Usage). |
| value | The number of units of the result obtained by the health test. For example, the value of 80% is 80. |

# health_event Joins

You cannot perform joins on the **health_event** table.

## health_event Sample Query

The following query returns up to the 25 most recent health events logged within the defined time frame and limited to the `Global \ Company B \ Edge`domain.

```
SELECT module_name, FROM_UNIXTIME(event_time_sec)
AS event_time, description, value, units, status, sensor_name
FROM health_event
WHERE event_time_sec AND domain_name= "Global \ Company B \ Edge"
BETWEEN UNIX_TIMESTAMP("2011-10-01 00:00:00")
AND UNIX_TIMESTAMP("2011-10-07 23:59:59")
ORDER BY event_time DESC
LIMIT 0, 25;
```

# syslog_event

The **`syslog_event`** table contains information on syslog events generated by the Secure Firewall. More information about syslog messages can be found in Cisco Firepower Threat Defense Syslog Messages at https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html.

For more information, see the following sections:


- syslog_event Fields, page 3-10
- syslog_event Joins, page 3-11
- syslog_event Sample Query, page 3-11


## syslog_event Fields

The following table describes the database fields you can access in the **`syslog_event`** table.

***Table 3-5 syslog_event Fields***

| Field | Description |
|---|---|
| `client_ipaddr` | IP address of the client which generated the syslog message, if applicable. |
| `domain_name` | Name of the domain in which the event was detected. |
| `domain_uuid` | UUID of the domain in which the event was detected. This is presented in binary. |
| `event_time` | The UNIX timestamp of the date and time the Secure Firewall Management Center generated the syslog event. |
| `netmap_num` | Netmap ID for the domain on which the event was generated. |
| `sensor_address` | This field has been deprecated. Use `sensor_name and sensor_uuid` to identify the device that generated the event. |
| `sensor_name` | The text name of the managed device that generated the event record. |
| `sensor_uuid` | A unique identifier for the managed device, or zero if `sensor_name` is `null`. |

*Table 3-5 syslog_event Fields (continued)*

| Field | Description |
|---|---|
| syslog_id | ID number of the syslog. |
| syslog_message | Contents of the syslog message. |
| syslog_message_class | Syslog message class. |
| syslog_message_id | ID number of the syslog message. |
| syslog_message_severity_type | Syslog severity level. Possible values are 1 through 7. |
| username | |

# syslog_event Joins

You cannot perform joins on the **syslog_event** table.

# syslog_event Sample Query

The following query returns up to the 25 most recent syslog events logged within the defined time frame and limited to the Global \ Company B \ Edgedomain.

```
SELECT syslog_id, FROM_UNIXTIME(event_time)
AS event_time, syslog_message, syslog_message_severity_type, sensor_name
FROM syslog_event
WHERE event_time AND domain_name= "Global \ Company B \ Edge"
BETWEEN UNIX_TIMESTAMP("2011-10-01 00:00:00")
AND UNIX_TIMESTAMP("2011-10-07 23:59:59")
ORDER BY event_time DESC
LIMIT 0, 25;
```