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	FireAMP malware detection and quarantine events.	5.1+
health_event, page 3-8	Health status events for monitored appliances.	4.10.x+
sru_import_log, page 3-10	Rule updates that have been imported on your appliances.	5.0+

audit_log

The **audit_log** table contains information on FireSIGHT System 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.
message	The action the user performed.
source	The IP address of the web interface user's host, in dotted-decimal notation.

Table 3-2 audit_log Fields (continued)

Field	Description
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.

```
SELECT from_unixtime(action_time_sec)
AS Time, user, subsystem, message, source, count(*)
AS Total
FROM audit_log
GROUP BY source, subsystem, user, message
ORDER BY source DESC;
```

fireamp_event

The **fireamp_event** table contains information on malware events. These events contain information on malware detected or quarantined within a cloud, the detection method, and hosts and users affected by the malware. New fields were added to identify the application which triggered the event, how the event is handled, and to correlate the event with connection, intrusion, and file events.

For more information, see the following sections:

- fireamp_event Fields, page 3-2
- 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.

Table 3-3 fireamp_event Fields (continued)

Field	Description
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 FireAMP 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 FireAMP 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: • ClamAV — 128 • ETHOS — 8 • SPERO — 32 • SHA — 4 • 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: • 4 — SHA • 8 — ETHOS • 32 — SPERO • 64 — Tetra • 128 — ClamAV
direction	Value that indicates whether the file was uploaded or downloaded. Can have the following values: • Download • Upload Currently the value depends on the protocol (for example, if the connection is HTTP it is a download).

Table 3-3 fireamp_event Fields (continued)

Field	Description
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.
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	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_port	Port number for the destination of the connection.
endpoint_user	The user determined by the Cisco FireAMP 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 FireAMP event.
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: • Create — 1 • Execute — 2 • Move — 22 • Scan — 4

Table 3-3 fireamp_event Fields (continued)

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

Table 3-3 fireamp_event Fields (continued)

Field	Description
event_type_id	The internal ID of the FireAMP event type. Each event_type_id value has an associated event_type value. The possible display values and the associated types are: • 553648143 — Threat Quarantined • 553648145 — Threat Detected in Exclusion • 553648146 — Cloud Recall Restore from Quarantine Started • 553648147 — Cloud Recall Quarantine Started • 553648149 — Quarantined Item Restored • 553648150 — Quarantine Restore Started • 553648154 — Cloud Recall Restore from Quarantine • 553648155 — Cloud Recall Quarantine • 553648168 — Blocked Execution • 554696714 — Scan Started • 554696715 — Scan Completed, No Detections • 1090519054 — Threat Detected • 1091567628 — Scan Completed With Detections • 1107296256 — FireAMP IOC • 2164260880 — Quarantine Failure • 2164260893 — Cloud Recall Quarantine Attempt Failed • 2164260884 — Quarantine Restore Failed • 2164260892 — Cloud Recall Restore from Quarantine Failed • 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.
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.
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	IP address of 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. ** — Unknown na — North America as — Asia af — Africa eu — Europe sa — South America au — Australia 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_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.

Table 3-3 fireamp_event Fields (continued)

Field	Description
threat_name	Name of the threat.
timestamp	The FireAMP event generation timestamp.
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

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

Table 3-4 fireamp_event Joins

You can join this table on...	And...
dst_ipaddr or src_ipaddr	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr

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 FireSIGHT System.

For more information, see the following sections:

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

health_event Fields

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

Table 3-5 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.
event_time_sec	The UNIX timestamp of the date and time the Defense 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: • red — Critical status. Limits have been exceeded for at least one health module on the appliance and the problem has not been corrected. • yellow — Warning status. Limits have been exceeded for at least one health module on the appliance and the problem has not been corrected. • green — Normal status. All health modules on the appliance are running within the limits configured in the health policy applied to the appliance. • 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. • disabled — Either the appliance is disabled or blacklisted, or is currently unreachable, or has no health policy applied to it. • 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.

```
SELECT module_name, FROM_UNIXTIME(event_time_sec)
```

```
AS event_time, description, value, units, status, sensor_name
FROM health_event
WHERE event_time_sec
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;
```

sru_import_log

The **sru_import_log** table contains information on rule update processes that have been run on your appliances. The **sru_import_log** table supersedes the deprecated **seu_import_log** table starting with Version 5.0 of the FireSIGHT System.

For more information, see the following sections:

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

sru_import_log Fields

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

Table 3-6 sru_import_log Fields

Field	Description
action	Indicates the action that has occurred for the imported rule update object type: • apply — The Reapply intrusion policies after the Rule Update import completes option was enabled for the import • changed — For a rule update component or rule, the rule update component was modified, or the rule has a higher revision number and the same GID and SID • collision — For a rule update component or rule, import was skipped because its revision conflicts with an existing component or rule on the appliance • deleted — For rules, the rule has been deleted from the rule update • disabled — For rules, the rule has been disabled in a default policy provided by Cisco • drop — For rules, the rule has been set to Drop and Generate Events in a default policy provided by Cisco • enabled — For a rule update, edit, a preprocessor, rule, or other feature provided by the rule update has been enabled in a default policy provided by Cisco • error — For a rule update or local rule file, the import failed • new — For a rule, this is the first time the object has been stored on this appliance
detail	Either a comment string unique for the change applied by the imported rule update to the component or rule, or blank, for a rule that has not changed.
generator_id	The GID for the generator for a rule.
import_time_sec	The UNIX timestamp of the date and time the rule update import was logged.
name	The name of the imported object. For rules, this corresponds to the rule message. For rule update components, this is the component name, such as online help or Snort.
policy	All, indicating that a rule is included in all default policies.
revision	Revision number for a rule.
signature_id	The SID for a rule or set of rules, decoder, or preprocessor.
sru_name	Descriptive name of the rule update.
sru_uuid	A unique identifier for the rule update.
type	Type of imported object in the rule update: update, rule, variable, and so forth.

sru_import_log Joins

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

sru_import_log Sample Query

The following query returns up to 25 results in descending order, sorted by timestamp.

```
SELECT FROM_UNIXTIME(import_time_sec)
AS time, name, type, action, generator_id, signature_id, revision, policy
FROM sru_import_log
```

```
ORDER BY time DESC
LIMIT 0, 25;
```