Schema: Statistics Tracking Tables

This chapter contains information on the schema and supported joins for application and URL statistics tracking tables. These tables collect statistical information on:

- access control and intrusion events by application and by user
- bandwidth usage and connection decisions by application and by user
- bandwidth usage and connection decisions by URL reputation (risk) and by URL business relevance

For links to details on each table, see the following table.

Table 5-1 Application and URL Statistics Tables

See	For the table that stores statistics on...	Version
app_ids_stats_current_timeframe, page 5-4	Access control and intrusion protection activity, by application and a range of application attributes.	5.0+
app_stats_current_timeframe, page 5-7	Traffic volume and system access control activity (connections allowed or denied), by application and a range of application attributes.	5.0+
compliance_events_stats_current_timeframe, page 5-9	Compliance and allow list events	6.0+
dns_query_stats_current_timeframe, page 5-10	DNS Queries	6.0+
geolocation_stats_current_timeframe, page 5-11	Access control activity by location.	5.2+
ids_impact_stats_current_timeframe, page 5-13	Statistics for intrusion events (connections blocked and would have dropped) by impact levels.	5.1.1+
interface_stats_current_timeframe, page 5-15	Statistics for iinterfaces.	6.1+
ip_reputation_stats_current_timeframe, page 5-16	Contain statistics on the bandwidth usage and connections associated with requests to IP addresses, URLs, and DNS domains in specified Security Intelligence categories.	6.0+
qos_rule_stats_current_timeframe, page 5-18	Contain statistics on quality of service rules, where they are triggered, and how they are applied.	6.1+
session_stats_current_timeframe, page 5-19	Contain statistics for all connections. Statistics can be extracted based on bytes, connection, sensor, and time.	5.2+
si_category_session_stats_current_timeframe, page 5-20	Contain statistics for Security Intelligence..	7.2+
ssl_action_stats_current_timeframe, page 5-22	Contain statistics for SSL actions.	7.2+

Table 5-1 Application and URL Statistics Tables (continued)

See	For the table that stores statistics on...	Version
ssl_cache_stats_current_timeframe, page 5-23	Contain statistics for SSL caching.	7.2+
ssl_certificate_stats_current_timeframe, page 5-24	Contain statistics for SSL certificates.	7.2+
ssl_failure_reason_stats_current_timeframe, page 5-25	Contain statistics for SSL failures.	7.2+
ssl_session_stats_current_timeframe, page 5-26	Contain statistics for SSL sessions.	7.2+
ssl_stats_current_timeframe, page A-2	Contain statistics for SSL connections. Statistics can be extracted based on bytes, connection, sensor, and time. Deprecated in Version 7.2. Superseded by **ssl_action_stats_current_timeframe, page 5-22**, **ssl_cache_stats_current_timeframe, page 5-23**, **ssl_certificate_stats_current_timeframe, page 5-24**, **ssl_failure_reason_stats_current_timeframe, page 5-25**, **ssl_session_stats_current_timeframe, page 5-26**, **ssl_version_stats_current_timeframe, page 5-27**	5.4-7.1
ssl_version_stats_current_timeframe, page 5-27	Contain statistics for SSL versions.	7.2+
storage_stats_by_disposition_current_timeframe, page 5-28	Contain statistics for files based on disposition. Statistics can be extracted based on bytes, disposition, sensor, and time.	5.3+
storage_stats_by_file_type_current_timeframe, page 5-30	Contain statistics for files based on file type. Statistics can be extracted based on bytes, file type, sensor, and time.	5.3+
tlsfp_malware_stats_current_timeframe, page 5-31	Contain statistics for files based on file type. Statistics can be extracted based on bytes, file type, sensor, and time.	7.2+
tlsfp_processname_stats_current_timeframe, page 5-32	Contain statistics for files based on file type. Statistics can be extracted based on bytes, file type, sensor, and time.	7.2+
transmission_stats_by_file_type_current_timeframe, page 5-33	Contain statistics for connections based on file type. Statistics can be extracted based on bytes, connection, file type, sensor, and time.	5.3+
tunnel_session_stats_current_timeframe	Lookups on this table are not currently supported.	6.1+
url_category_stats_current_timeframe, page 5-34	Traffic volume and system access control activity (connections allowed or denied), by the category of the requested website.	5.0+
url_reputation_stats_current_timeframe, page 5-36	Traffic volume and system access control activity (connections allowed or denied), by the reputation of the requested website.	5.0+
user_ids_stats_current_timeframe, page 5-38	Access control and intrusion protection activity, by user.	5.0+
user_stats_current_timeframe, page 5-39	Traffic volume and system access control activity (connections allowed or denied), by user.	5.0+

Understanding Statistics Tracking Tables

A table's name ends with **current_day**, **current_month**, or **current_year** to indicate the timeframe of its data. For example, the **app_ids_stats_current_***timeframe* describes **app_stats_current_day**, **app_stats_current_month**, and **app_stats_current_year**. The **app_stats_current_year** table stores statistics for 360 days; the **current_month** table stores statistics for 30 days.

Each time the Secure Firewall Management Center receives raw counts from managed devices in your network, it updates all three table types, but does so at successively coarser resolution. The **current_day** table has the finest resolution (15 seconds or 5 minutes, depending on the particular table); the **current_year** table has the coarsest resolution (24 hours). See Storage Characteristics for Statistics Tracking Tables, page 5-3 for specific information.

Storage Characteristics for Statistics Tracking Tables

See the following table for important details.

Table 5-2 Storage Characteristics of Statistics Tables

Table Type	Interval (Resolution)	Storage Lifespan
current_day	15 seconds for **app_ids_stats_current_***timeframe* and **user_ids_stats_current_***timeframe*	current interval plus all intervals in the preceding 24 hours
	5 minutes for **app_stats_current_***timeframe*, **user_stats_current_***timeframe*, **url_category_stats_current_***timeframe*, and **url_reputation_stats_current_***timeframe*	current interval plus all intervals in the preceding 24 hours
current_month	one hour	current hour plus the hours stretching back 30 days
current_year	24 hours	current day plus the preceding 360 days

A storage interval is defined by its start time. For example, the **current_month** table contains counts for the hour `10:00:00 - 10:59:59` as one record with a timestamp of `10:00:00`. Note that a day begins at `00:00:00` and ends at `23:59:59`. Interval start times are stored as UNIX timestamps (GMT).

Specifying Time Intervals When Querying Statistics Tables

The effective time interval for a query is defined by both the table and the `time_start_sec` field in the query.

For example, if your SQL statement specifies `time_start_sec = 6:00:00`, the interval varies for each table type:

- for **current_day** tables: either `6:00:00` to `6:00:14` (for 15 second tables) or `6:00:00` to `6:04:59` (for 5 minute tables).
- for **current_month** tables: `6:00:00` to `6:59:59`.
- for **current_year** tables: `0:00:00` to `23:59:59` on the following day.

The simplest way to retrieve data is to state the interval start time. For example, to retrieve from the **app_ids_stats_current_day** table, specify one of the following:

```
00:00:00
00:00:15
00:00:30
23:59:45
```

If your query contains a timestamp that is other than an interval start time, the system modifies the request as follows:

- rounds up the start time to the nearest interval time
- rounds down the end time to the nearest interval time

For example, the following query rounds up the start time:

```
SELECT application_id
FROM app_ids_stats_current_month
WHERE start_time_sec = UNIX_TIMESTAMP("2011-12-01 12:30:00");
```

and is the same as:

```
SELECT application_id
FROM app_ids_stats_current_month
WHERE start_time_sec = UNIX_TIMESTAMP("2011-12-01 01:00:00");
```

When querying a range of intervals, the starting time interval is rounded up, and the ending time interval is rounded down. For example:

```
SELECT application_id
FROM app_ids_stats_current_month
WHERE start_time_sec BETWEEN UNIX_TIMESTAMP("2011-12-10 12:59:00") and
UNIX_TIMESTAMP("2011-12-10 16:28:00");
```

is changed to:

```
SELECT application_id
FROM app_ids_stats_current_month
WHERE start_time_sec BETWEEN UNIX_TIMESTAMP("2011-12-10 13:00:00") and
UNIX_TIMESTAMP("2011-12-12 16:00:00");
```

If your query interval extends beyond a table's time frame, you can usually obtain the additional data from another table, although the data in the other table will have a coarser resolution. For example, to retrieve bandwidth usage for the past two days, you can get results for yesterday from the **current_day** table (at 5 minute resolution), but you can get statistics for the previous day only from **current_month** (in hour chunks) or **current_year** (in day chunks).

app_ids_stats_current_timeframe

The **app_ids_stats_current_*timeframe*** tables contain statistics about application activity and intrusion events on your monitored network. Statistics can be extracted per detected application, per application type (application protocol, client application, or web application), and also per risk and business relevance of the application. The tables also track blocked connections due to intrusion policy violations and the estimated potential impact of an intrusion.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-3.

For more information on the **app_ids_stats_current_*timeframe*** tables, see the following sections:

app_ids_stats_current_timeframe Fields

The following table describes the fields you can access in the **app_ids_stats_current_*timeframe*** tables. All tables of this type contain the same fields.

Table 5-3 app_ids_stats_current_timeframe Fields

Field	Description
application_id	The internal identification number for the application.
application_name	The application name that appears in the user interface.
blocked	Number of connections blocked due to violation of an intrusion policy.
business_relevance	An index (from 1 to 5) of the application's relevance to business productivity where 1 is very low and 5 is very high.
business_relevance_description	A description of business relevance (very low, low, medium, high, very high).
domain_name	Name of the domain specified for the statistics.
domain_uuid	UUID of the domain specified for the statistics. This is presented in binary.
impact_level_1	The number of impact level 1 (vulnerable) intrusion events recorded for the application.
impact_level_2	The number of impact level 2 (potentially vulnerable) intrusion events.
impact_level_3	The number of impact level 3 (host currently not vulnerable) intrusion events.
impact_level_4	The number of impact level 4 (unknown target) intrusion events.
impact_level_5	The number of impact level 5 (unknown vulnerability) intrusion events.
is_client_application	A true-false flag that indicates if the detected application is a client application.
is_server_application	A true-false flag that indicates if the detected application is an application protocol.
is_web_application	A true-false flag that indicates if the detected application is a web application.
netmap_num	Netmap ID for the domain on which the statistics were collected.
partially_dropped	Number of instances when the packet is transmitted or delivered to the destination, but the connection is then blocked.
reject_count	Number of packets which were rejected by policy.
rewrite_count	Number of packets which were rewritten based on policy.
risk	An index (from 1 to 5) of the application's estimated risk where 1 is very low risk and 5 is critical risk.
risk_description	A description of the estimated risk (very low, low, medium, high, critical).

Table 5-3 app_ids_stats_current_timeframe Fields (continued)

Field	Description
sensor_address	This field is deprecated. Use sensor_name and sensor_uuid to identify the sensor which generated the event.
sensor_id	ID of the device that provided the event.
sensor_name	The name of the managed device that generated the intrusion event.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.
start_time_sec	The UNIX timestamp of the date and time when the measurement interval starts. For detailed information, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
start_time_str	The date and time of the start of the measurement interval in human-readable format of Year-Month-Day Time. For example, February 4th, 2022 is 2022-02-04 20:18:58.
would_have_dropped	Number of packets that would have been dropped if the intrusion policy had been configured to drop packets in an inline deployment.
would_reject_count	Number of packets which would have been rejected by policy
would_rewrite_count	Number of packets which were rewritten based on policy.

app_ids_stats_current_timeframe Joins

The following table describes the joins you can perform on the **app_ids_stats_current**_*timeframe* tables.

Table 5-4 app_ids_stats_current_timeframe 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

app_ids_stats_current_timeframe Sample Query

The following query returns up to 25 application records from the **app_ids_stats_current_month** table. Each record contains the number of blocked connections and intrusion events for the application over the time interval.

```
SELECT from_unixtime(start_time_sec), sum(blocked)

FROM app_ids_stats_current_day

WHERE start_time_sec = unix_timestamp("2013-12-15");
```

app_stats_current_timeframe

The **app_stats_current_*timeframe*** tables contain statistics on bandwidth usage and access control actions (connection allowed or denied), by application and by device that monitored the traffic. You can filter these statistics by the business relevance, estimated risk, and type of the application.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-3.

For more information on the **app_stats_current_*timeframe*** tables, see the following sections:

app_stats_current_timeframe Fields

The following table describes the fields you can access in the **app_stats_current_*timeframe*** tables.

Table 5-5 app_stats_current_timeframe Fields

Field	Description
application_id	The internal identification number for the application.
application_name	The application name that appears in the user interface.
business_relevance	An index (from 1 to 5) of the application's relevance to business productivity where 1 is very low and 5 is very high.
business_relevance_description	A description of business relevance (very low, low, medium, high, very high).
bypass	Number of packets which are allowed to bypass due to delay.
bytes_in	The bytes of inbound traffic for the application during the specified interval.
bytes_out	The bytes of outbound traffic for the application during the specified interval.
connections_allowed	The number of connections allowed.
connections_denied	The number of connections denied due to violation of an access control policy.
domain_name	Name of the domain specified for the statistics.
domain_uuid	UUID of the domain specified for the statistics. This is presented in binary.
is_client_application	A true-false flag that indicates if the detected application is a client application.
is_server_application	A true-false flag that indicates if the detected application is an application protocol.
is_web_application	A true-false flag that indicates if the detected application is a web application.
netmap_num	Netmap ID for the domain on which the statistics were collected.
qos_dropped_bytes_in	Number of incoming bytes dropped due to QoS.
qos_dropped_bytes_out	Number of outgoing bytes dropped due to QoS.

Table 5-5 app_stats_current_timeframe Fields (continued)

Field	Description
risk	An index (from 1 to 5) of the application's estimated risk where 1 is very low risk and 5 is critical risk.
risk_description	A description of the estimated risk (very low, low, medium, high, critical).
sensor_address	This field is deprecated. Use sensor_name and sensor_uuid to identify the sensor which generated the event.
sensor_id	The internal identification number of the managed device that detected the traffic.
sensor_name	The name of the managed device that detected the traffic.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.
start_time_sec	The UNIX timestamp of the start of the measurement interval. For information on specifying the start time, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
start_time_str	The date and time of the start of the measurement interval in human-readable format of Year-Month-Day Time. For example, February 4th, 2022 is 2022-02-04 20:18:58.
would_bypass	Number of packets which were eligible for bypass but were inspected.

app_stats_current_timeframe Joins

The following table describes the joins you can perform on the **app_stats_current_***timeframe* tables.

Table 5-6 app_stats_current_timeframe 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.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

app_stats_current_timeframe Sample Query

The following query returns the inbound and outbound traffic load associated with applications that have low business relevance and high risk in the period of a day, for all managed devices connected to the Secure Firewall Management Center.

```
SELECT start_time_sec, sum(bytes_in), sum(bytes_out)

FROM app_stats_current_day

WHERE business_relevance <= 2
```

```
AND risk >= 4 AND start_time_sec = unix_timestamp("2013-12-15");
```

compliance_events_stats_current_timeframe

The **compliance_stats_events_current_***timeframe* tables contain statistics on the number of compliance and allow list events during a timeframe.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-3.

For more information on the **compliance_events_stats_current_***timeframe* tables, see the following sections:

- compliance_events_stats_current_timeframe Fields, page 5-9
- compliance_event_stats_current_timeframe Joins, page 5-9
- compliance_event_stats_current_timeframe Sample Query, page 5-10

compliance_events_stats_current_timeframe Fields

The following table describes the fields you can access in the **compliance_events_stats_current_***timeframe* tables.

Table 5-7 compliance_events_stats_current_timeframe Fields

Field	Description
domain_name	Name of the domain specified for the statistics.
domain_uuid	UUID of the domain specified for the statistics. This is presented in binary.
netmap_num	Netmap ID for the domain on which the statistics were collected.
priority_0_events	Number of priority 0 events detected during the timeframe.
priority_1_events	Number of priority 1 events detected during the timeframe.
priority_2_events	Number of priority 2 events detected during the timeframe.
priority_3_events	Number of priority 3 events detected during the timeframe.
priority_4_events	Number of priority 4 events detected during the timeframe.
priority_5_events	Number of priority 5 events detected during the timeframe.
rule	Allow list rule which triggered the events. If this rule is empty, the events are compliance events.
start_time_sec	The UNIX timestamp of the start of the measurement interval. For information on specifying the start time, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
start_time_str	The date and time of the start of the measurement interval in human-readable format of `Year-Month-Day Time`. For example, February 4th, 2022 is `2022-02-04 20:18:58`.

compliance_event_stats_current_timeframe Joins

You cannot perform joins on the **compliance_event_stats_current_*timeframe*** table.

compliance_event_stats_current_timeframe Sample Query

The following query returns the priority 0, 1, and 2 events, and the relevant allow list rule, ordered by domain, in the period of a day.

```
SELECT domain_name, priority_0_events, priority_1_events, priority_2_events, rule
FROM compliance_event_stats_current_day
ORDER BY domain_name DESC;
```

dns_query_stats_current_timeframe

The **dns_query_stats_current_***timeframe* tables contain statistics on DNS queries.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-3.

For more information on the **dns_query_stats_current_***timeframe* tables, see the following sections:

dns_query_stats_current_timeframe Fields

The following table describes the fields you can access in the **dns_quaery_stats_current_***timeframe* tables.

Table 5-8 dns_query_stats_current_timeframe Fields

Field	Description
bytes_in	The bytes of inbound traffic during the specified interval.
bytes_out	The bytes of outbound traffic during the specified interval.
connections_allowed	The number of connections allowed for the specified DNS query.
connections_denied	The number of connections denied for the specified DNS query due to violation of an access control policy.
dns_record_type	The type of DNS lookup used in the DNS query.
domain_name	Name of the domain specified for the statistics.
domain_uuid	UUID of the domain specified for the statistics. This is presented in binary.
sensor_addres	The IP address of the managed device that monitored the traffic. Format is *ipv4_address,ipv6_address*.
sensor_id	The internal identification number of the managed device that detected the traffic.
sensor_name	The name of the managed device that detected the traffic.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.

Table 5-8 dns_query_stats_current_timeframe Fields (continued)

Field	Description
start_time_sec	The UNIX timestamp of the start of the measurement interval. For information on specifying the start time, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
start_time_str	The date and time of the start of the measurement interval in human-readable format of `Year-Month-Day Time`. For example, February 4th, 2022 is `2022-02-04 20:18:58`.

dns_query_stats_current_timeframe Joins

You cannot perform joins on the **dns_query_stats_current_*timeframe*** table.

dns_query_stats_current_timeframe Sample Query

The following query returns the number of connections associated with dns record types for each sensor in the period of a day, sorted by sensor name and limited to the `Global \ Company B \ Edge` domain.

```
SELECT sensor_name, dns_record_type, sum(connections_allowed), sum(connections_denied)
FROM dns_query_stats_current_day
ORDER BY sensor_name DESC
WHERE domain_name= "Global \ Company B \ Edge";
```

geolocation_stats_current_timeframe

The **geolocation_stats_*timeframe*** tables contain statistics regarding intrusion events based on location levels. Statistics can be extracted based on impact level, device, and how the packets are handled.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-3.

For more information on the **geolocation_stats_current_*timeframe*** tables, see the following sections:

geolocation_stats_current_timeframe Fields

The following table describes the fields you can access in the **geolocation_stats_current_*timeframe*** tables. All tables of this type contain the same fields.

Note that the geolocation information is not updated on devices with builds prior to 7.2. Information from these devices may not be accurate.

Table 5-9 geolocation_stats_current_timeframe Fields

Field	Description
bytes_from	The total number of bytes transmitted by the session responder.
bytes_to	Total number of bytes transmitted by the session initiator.
destination_continent	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
destination_country	Code for the country of the destination host.
domain_name	Name of the domain specified for the statistics.
domain_uuid	UUID of the domain specified for the statistics. This is presented in binary.
flows_allowed	The number of flows allowed.
flows_denied	The number of flows denied due to violation of an access control policy.
netmap_num	Netmap ID for the domain on which the statistics were collected.
sensor_address	This field is deprecated. Use sensor_name and sensor_uuid to identify the sensor which generated the event.
sensor_id	ID of the device that provided the event.
sensor_name	The name of the managed device that generated the intrusion event.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.
source_continent	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
source_country	Code for the country of the source host.
start_time_sec	The UNIX timestamp of the date and time when the measurement interval starts. For detailed information, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.

Table 5-9 geolocation_stats_current_timeframe Fields (continued)

Field	Description
start_time_str	The date and time of the start of the measurement interval in human-readable format of `Year-Month-Day Time`. For example, February 4th, 2022 is `2022-02-04 20:18:58`.
xff_continent	The name of the continent of the original source host when there is a proxy in the connection. `**` — Unknown `na` — North America `as` — Asia `af` — Africa `eu` — Europe `sa` — South America `au` — Australia `an` — Antarctica
xff_country	Code for the country of the original source host when there is a proxy in the connection.

geolocation_stats_current_timeframe Joins

You cannot perform joins on the **geolocation_stats_current_***timeframe* tables.

geolocation_stats_current_timeframe Sample Query

The following query returns source country and sensor name for the first 25 connection events from Asia during the current day, limited to the `Global \ Company B \ Edge` domain.

```
SELECT sensor_name, source_continent
FROM geolocation_stats_current_year
WHERE destination_continent='as' and domain_name= "Global \ Company B \ Edge"
LIMIT 20;
```

ids_impact_stats_current_timeframe

The **ids_impact_stats_***timeframe* tables contain statistics regarding intrusion events based on impact levels. Statistics can be extracted based on impact level, device, and how the packets are handled.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-3.

For more information on the **ids_impact_stats_current_***timeframe* tables, see the following sections:

- ids_impact_stats_current_timeframe Fields, page 5-14
- ids_impact_stats_current_timeframe Joins, page 5-14

- ids_impact_stats_current_timeframe Sample Query, page 5-15

ids_impact_stats_current_timeframe Fields

The following table describes the fields you can access in the **ids_impact_stats_current**_*timeframe* tables. All tables of this type contain the same fields.

Table 5-10 ids_impact_stats_current_timeframe Fields

Field	Description
blocked	Number of connections blocked due to violation of an intrusion policy.
domain_name	Name of the domain specified for the statistics.
domain_uuid	UUID of the domain specified for the statistics. This is presented in binary.
impact_level_1	The number of impact level 1 (vulnerable) intrusion events recorded for the application.
impact_level_2	The number of impact level 2 (potentially vulnerable) intrusion events.
impact_level_3	The number of impact level 3 (host currently not vulnerable) intrusion events.
impact_level_4	The number of impact level 4 (unknown target) intrusion events.
impact_level_5	The number of impact level 5 (unknown vulnerability) intrusion events.
netmap_num	Netmap ID for the domain on which the statistics were collected.
partially_dropped	Number of instances when the packet is transmitted or delivered to the destination, but the connection is then blocked.
sensor_address	This field is deprecated. Use sensor_name and sensor_uuid to identify the sensor which generated the event.
sensor_id	ID of the device that provided the event.
sensor_name	The name of the managed device that generated the intrusion event.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.
start_time_sec	The UNIX timestamp of the date and time when the measurement interval starts. For detailed information, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
start_time_str	The date and time of the start of the measurement interval in human-readable format of Year-Month-Day Time**.** For example, February 4th, 2022 is 2022-02-04 20:18:58.
would_have_dropped	Number of packets that would have been dropped if the intrusion policy had been set to drop packets in an inline deployment.

ids_impact_stats_current_timeframe Joins

You cannot perform joins on the **ids_impact_stats_current**_*timeframe* tables.

ids_impact_stats_current_timeframe Sample Query

The following query returns the first 25 `blocked` and `would_have_dropped` events during the current day, limited to the `domain_name= "Global \ Company B \ Edge"` domain.

```
SELECT blocked, would_have_dropped
FROM ids_impact_stats_current_year
WHERE domain_name= "Global \ Company B \ Edge"
LIMIT 25;
```

interface_stats_current_timeframe

The **`interface_stats_current_`***`timeframe`* tables contain statistics regarding specific interfaces.

For an understanding of the **`current_day`**, **`current_month`**, and **`current_year`** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-3.

For more information on the **`interface_stats_current_`***`timeframe`* tables, see the following sections:

- interface_stats_current_timeframe Fields, page 5-15
- interface_stats_current_timeframe Joins, page 5-16
- interface_stats_current_timeframe Sample Query, page 5-16

interface_stats_current_timeframe Fields

The following table describes the fields you can access in the **`interface_stats_current_`***`timeframe`* tables. All tables of this type contain the same fields.

Table 5-11 interface_stats_current_timeframe Fields

Field	Description
connections_allowed	Number of connections allowed.
connections_denied	Number of connections blocked due to violation of an intrusion policy.
domain_name	Name of the domain specified for the statistics.
domain_uuid	UUID of the domain specified for the statistics. This is presented in binary.
egress_bytes	Number of egress bytes.
ingress_bytes	Number of ingress bytes.
interface_name	Name of the interface.
interface_uuid	UUID of the interface.
netmap_num	Netmap ID for the domain on which the statistics were collected.
qos_dropped_egress_bytes	Number of egress bytes dropped due to QoS.
qos_dropped_ingress_bytes	Number of ingress bytes dropped due to QoS.
sensor_address	This field is deprecated. Use `sensor_name` and `sensor_uuid` to identify the sensor which generated the event.
sensor_id	ID of the device that provided the event.
sensor_name	The name of the managed device that generated the intrusion event.

Table 5-11 interface_stats_current_timeframe Fields (continued)

Field	Description
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.
start_time_sec	The UNIX timestamp of the date and time the measurement interval starts. For detailed information, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
start_time_str	The date and time of the start of the measurement interval in human-readable format of Year-Month-Day Time. For example, February 4th, 2022 is 2022-02-04 20:18:58.

interface_stats_current_timeframe Joins

You cannot perform joins on the **interface_stats_current_***timeframe* tables.

interface_stats_current_timeframe Sample Query

The following query returns the first 25 blocked and would_have_dropped events during the current day, limited to the domain_name= "Global \ Company B \ Edge" domain.

```
SELECT blocked, would_have_dropped
FROM ids_impact_stats_current_year
WHERE domain_name= "Global \ Company B \ Edge"
LIMIT 25;
```

ip_reputation_stats_current_timeframe

The **ip_category_stats_current_***timeframe* tables contain statistics on the bandwidth usage and connections associated with requests to IP addresses, URLs, and DNS domains in specified Security Intelligence categories. You can also constrain queries on the managed device that monitored the traffic.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-3.

For more information on the **ids_impact_stats_current_***timeframe* tables, see the following sections:

- ip_reputation_stats_current_timeframe Fields, page 5-16
- ip_reputation_stats_current_timeframe Joins, page 5-17
- ip_reputation_stats_current_timeframe Sample Query, page 5-17

ip_reputation_stats_current_timeframe Fields

The following table describes the fields you can access in the **ip_reputation_stats_current_***timeframe* tables. All tables of this type contain the same fields.

Table 5-12 ip_reputation_stats_current_timeframe Fields

Field	Description
bytes_in	The bytes of inbound traffic during the specified interval.
bytes_out	The bytes of outbound traffic during the specified interval.
connections_allowed	The number of connections allowed for the specified IP.
connections_denied	The number of connections denied for the specified IP due to violation of an access control policy.
domain_name	Name of the domain specified for the statistics.
domain_uuid	UUID of the domain specified for the statistics. This is presented in binary.
name	the Security Intelligence name, for example, "URL Malware"
sensor_address	This field is deprecated. Use sensor_name and sensor_uuid to identify the sensor which generated the event.
sensor_id	ID of the device that provided the event.
sensor_name	The name of the managed device that generated the intrusion event.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.
start_time_sec	The UNIX timestamp of the date and time the measurement interval starts. For detailed information, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
start_time_str	The date and time of the start of the measurement interval in human-readable format of Year-Month-Day Time. For example, February 4th, 2022 is 2022-02-04 20:18:58.
type	Type of information in the entry. Possible values include: 0 - network security intelligence statistics. 1 - DNS security intelligence statistics. 2 - URL security intelligence statistics.

ip_reputation_stats_current_timeframe Joins

You cannot perform joins on the **ip_reputation_stats_current_***timeframe* tables.

ip_reputation_stats_current_timeframe Sample Query

The following query returns the first 25 connections showing the number of bytes in and out, number of connections, type of connection, and sensor, in order by domain during the current day, limited to the Global \ Company B \ Edge domain.

```
SELECT uuid_btoa(domain_uuid), domain_name, type, name, bytes_in, bytes_out,
connections_allowed, connections_denied, sensor_name
FROM ip_reputation_stats_current_day
ORDER BY domain_name DESC
WHERE domain_name= "Global \ Company B \ Edge";
LIMIT 25;
```

qos_rule_stats_current_timeframe

The **qos_rule_stats_current_***timeframe* tables contain statistics on quality of service rules, where they are triggered, and how they are applied.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-3.

For more information on the **qos_rules_stats_current_***timeframe* tables, see the following sections:

qos_rule_stats_current_timeframe Fields

The following table describes the fields you can access in the **qos_rule_stats_current_***timeframe* tables. All tables of this type contain the same fields.

Table 5-13 qos_rule_stats_current_timeframe Fields

Field	Description
deploy_revision	Revision UUID of the QoS policy.
domain_name	Name of the domain specified for the statistics.
domain_uuid	UUID of the domain specified for the statistics. This is presented in binary.
netmap_num	Netmap ID for the domain on which the statistics were collected.
qos_dropped_bytes_in	Number of incoming bytes dropped due to QoS.
qos_dropped_bytes_out	Number of outgoing bytes dropped due to QoS.
qos_policy_id	UUID of the QOS policy.
qos_policy_name	Name of the QoS policy.
qos_rule_id	Integer ID of the QoS rule.
qos_rule_name	Name of the QoS rule.
sensor_address	This field is deprecated. Use sensor_name and sensor_uuid to identify the sensor which generated the event.
sensor_id	ID of the device that provided the event.
sensor_name	The name of the managed device that generated the event.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.
start_time_sec	The UNIX timestamp of the date and time the measurement interval starts. For detailed information, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
start_time_str	The date and time of the start of the measurement interval in human-readable format of Year-Month-Day Time. For example, February 4th, 2022 is 2022-02-04 20:18:58.

qos_rule_stats_current_timeframe Joins

You cannot perform joins on the **qos_rule_stats_current**_*timeframe* tables.

qos_rule_stats_current_timeframe Sample Query

The following query returns the number of dropped bytes in and out due to QOS rules, the QOS policy name, QOS rule name, and the sensor name, in descending order by sensor name during the current day, limited to the `Global \ Company B \ Edge` domain.

```
SELECT qos_dropped_bytes_in, qos_dropped_bytes_in, qos_policy_name, qos_rule_name,
sensor_name
FROM qos_rule_stats_current_day
ORDER BY sensor_name DESC
WHERE domain_name= "Global \ Company B \ Edge";
```

session_stats_current_timeframe

The **session_stats**_*timeframe* tables contain statistics for all connections. Statistics can be extracted based on bytes, connection, sensor, and time.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-3.

For more information on the **session_stats_current**_*timeframe* tables, see the following sections:

- session_stats_current_timeframe Fields, page 5-19
- session_stats_current_timeframe Joins, page 5-20
- session_stats_current_timeframe Sample Query, page 5-20

session_stats_current_timeframe Fields

The following table describes the fields you can access in the **session_stats_current**_*timeframe* tables. All tables of this type contain the same fields.

Table 5-14 session_stats_current_timeframe Fields

Field	Description
bytes_in	The bytes of inbound traffic during the specified interval.
bytes_out	The bytes of outbound traffic during the specified interval.
connections_allowed	The number of connections allowed for the specified URL category.
connections_denied	The number of connections denied for the specified URL category due to violation of an access control policy.
domain_name	Name of the domain specified for the statistics.

Table 5-14 session_stats_current_timeframe Fields (continued)

Field	Description
domain_uuid	UUID of the domain specified for the statistics. This is presented in binary.
id	This field is not used and will always return 0.
sensor_address	This field is deprecated. Use sensor_name and sensor_uuid to identify the sensor which generated the event.
sensor_id	ID of the device that provided the event.
sensor_name	The name of the managed device that generated the intrusion event.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.
start_time_sec	The UNIX timestamp of the date and time the measurement interval starts. For detailed information, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
start_time_str	The date and time of the start of the measurement interval in human-readable format of Year-Month-Day Time. For example, February 4th, 2022 is 2022-02-04 20:18:58.

session_stats_current_timeframe Joins

You cannot perform joins on the **session_stats_current_***timeframe* tables.

session_stats_current_timeframe Sample Query

The following query returns the number of denied and allowed connections for each sensor, in descending order by sensor_name during the current day, limited to the Global \ Company B \ Edge domain.

```
SELECT sensor_name, sensor_id, connections_denied, connections_allowed
FROM session_stats_current_day
ORDER BY sensor_name DESC
WHERE domain_name= "Global \ Company B \ Edge";
```

si_category_session_stats_current_timeframe

The **si_category_session_stats_***timeframe* tables contain statistics for all connections. Statistics can be extracted based on bytes, connection, sensor, and time.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-3.

For more information on the **si_category_session_stats_current_***timeframe* tables, see the following sections:

si_category_session_stats_current_timeframe Fields

The following table describes the fields you can access in the **session_stats_current_*timeframe*** tables. All tables of this type contain the same fields.

Table 5-15 session_stats_current_timeframe Fields

Field	Description
bytes_in	The bytes of inbound traffic during the specified interval.
bytes_out	The bytes of outbound traffic during the specified interval.
connections_allowed	The number of connections allowed for the specified URL category.
connections_denied	The number of connections denied for the specified URL category due to violation of an access control policy.
domain_name	Name of the domain specified for the statistics.
domain_uuid	UUID of the domain specified for the statistics. This is presented in binary.
name	
netmap_num	Netmap ID for the domain on which the statistics were collected.
sensor_address	This field is deprecated. Use sensor_name and sensor_uuid to identify the sensor which generated the event.
sensor_id	ID of the device that provided the event.
sensor_name	The name of the managed device that generated the intrusion event.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.
start_time_sec	The UNIX timestamp of the date and time the measurement interval starts. For detailed information, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
start_time_str	The date and time of the start of the measurement interval in human-readable format of Year-Month-Day Time**.** For example, February 4th, 2022 is 2022-02-04 20:18:58.
type	

si_category_session_stats_current_timeframe Joins

You cannot perform joins on the **si_category_session_stats_current_*timeframe*** tables.

si_category_session_stats_current_timeframe Sample Query

The following query returns the number of denied and allowed connections for each sensor, in descending order by sensor_name during the current day, limited to the Global \ Company B \ Edge domain.

```
SELECT sensor_name, sensor_id, connections_denied, connections_allowed
FROM si_category_session_stats_current_day
ORDER BY sensor_name DESC
WHERE domain_name= "Global \ Company B \ Edge";
```

ssl_action_stats_current_timeframe

The **ssl_action_stats_current_***timeframe* tables contain statistics for SSL actions.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-3.

For more information on the **ssl_action_stats_current_***timeframe* tables, see the following sections:

ssl_action_stats_current_timeframe Fields

The following table describes the fields you can access in the **ssl_action_stats_current_***timeframe* fields. All tables of this type contain the same fields.

Table 5-16 ssl_action_stats_current_timeframe Fields

Field	Description
action	Specifies the SSL rule action that indicates how the system handled an encrypted connection.
count	The number of connection in which a specific action was employed.
netmap_num	Netmap ID for the domain on which the statistics were collected.
sensor_name	The name of the managed device that generated the event.
start_time_sec	The UNIX timestamp of the date and time the measurement interval starts. For detailed information, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
start_time_str	The date and time of the start of the measurement interval in human-readable format of `Year-Month-Day Time`. For example, February 4th, 2022 is `2022-02-04 20:18:58`.

ssl_action_stats_current_timeframe Joins

You cannot perform joins on the **ssl_action_stats_current_***timeframe* tables.

ssl_action_stats_current_timeframe Sample Query

The following query returns the number of each SSL actions by sensor, in descending order by `sensor_name` during the current day, limited to the `Global \ Company B \ Edge` domain.

```
SELECT sensor_name, action, count
FROM ssl_action_stats_current_day
WHERE domain_name= "Global \ Company B \ Edge"
ORDER BY sensor_name DESC;
```

ssl_cache_stats_current_timeframe

The **ssl_cache_stats_current**_*timeframe* tables contain statistics for SSL Caching.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-3.

For more information on the **ssl_cache_stats_current**_*timeframe* tables, see the following sections:

ssl_cache_stats_current_timeframe Fields

The following table describes the fields you can access in the **ssl_cache_stats_current**_*timeframe* tables. All tables of this type contain the same fields.

Table 5-17 ssl_cache_stats_current_timeframe Fields

Field	Description
cache_status	Indicates the cache status for the SSL session ID.
count	The number of SSL connections for each possible cache status.
netmap_num	Netmap ID for the domain on which the statistics were collected.
sensor_name	The name of the managed device that generated the event.
start_time_sec	The UNIX timestamp of the date and time the measurement interval starts. For detailed information, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
start_time_str	The date and time of the start of the measurement interval in human-readable format of `Year-Month-Day Time`. For example, February 4th, 2022 is `2022-02-04 20:18:58`.

ssl_cache_stats_current_timeframe Joins

You cannot perform joins on the **ssl_cache_stats_current**_*timeframe* tables.

ssl_cache_stats_current_timeframe Sample Query

The following query returns the count of each SSL cache status for each sensor, in descending order by `sensor_name` during the current day, limited to the `Global \ Company B \ Edge` domain.

```
SELECT sensor_name, cache_status, count
FROM ssl_cache_stats_current_day
WHERE domain_name= "Global \ Company B \ Edge"
ORDER BY sensor_name DESC;
```

ssl_certificate_stats_current_timeframe

The **ssl__certificate_stats_current_***timeframe* tables contain statistics for SSL certificates.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-3.

For more information on the **ssl_certificate_stats_current_***timeframe* tables, see the following sections:

ssl_certificate_stats_current_timeframe Fields

The following table describes the fields you can access in the **ssl_certificate_stats_current_***timeframe* tables. All tables of this type contain the same fields.

Table 5-18 ssl_certificate_stats_current_timeframe Fields

Field	Description
cert_status	Status associated with the certificate used to encrypt the session.
count	The number of connections for each certificate status.
netmap_num	Netmap ID for the domain on which the statistics were collected.
sensor_name	The name of the managed device that generated the event.
start_time_sec	The UNIX timestamp of the date and time the measurement interval starts. For detailed information, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
start_time_str	The date and time of the start of the measurement interval in human-readable format of `Year-Month-Day Time`. For example, February 4th, 2022 is `2022-02-04 20:18:58`.

ssl_certificate_stats_current_timeframe Joins

You cannot perform joins on the **ssl_certificate_stats_current_***timeframe* tables.

ssl_certificate_stats_current_timeframe Sample Query

The following query returns the number of certificates with each status for each sensor, in descending order by `sensor_name` during the current day, limited to the `Global \ Company B \ Edge` domain.

```
SELECT sensor_name, cert_status, count
FROM ssl_certificate_stats_current_day
WHERE domain_name= "Global \ Company B \ Edge"
ORDER BY sensor_name DESC;
```

ssl_failure_reason_stats_current_timeframe

The **ssl_failure_reason_stats_current**_*timeframe* tables contain statistics for SSL failures.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-3.

For more information on the **ssl_failure_reason_stats_current**_*timeframe* tables, see the following sections:

ssl_failure_reason_stats_current_timeframe Fields

The following table describes the fields you can access in the **ssl_failure_reason_stats_current**_*timeframe* tables. All tables of this type contain the same fields.

Table 5-19 ssl_failure_reason_stats_current_timeframe Fields

Field	Description
count	The number of failed SSL decryptions for each reason.
failure_reason	The reason the system fails to decrypt encrypted traffic.
netmap_num	Netmap ID for the domain on which the statistics were collected.
sensor_name	The name of the managed device that generated the event.
start_time_sec	The UNIX timestamp of the date and time the measurement interval starts. For detailed information, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
start_time_str	The date and time of the start of the measurement interval in human-readable format of `Year-Month-Day Time`. For example, February 4th, 2022 is `2022-02-04 20:18:58`.

ssl_failure_reason_stats_current_timeframe Joins

You cannot perform joins on the **ssl_failure_reason_stats_current**_*timeframe* tables.

ssl_failure_reason_stats_current_timeframe Sample Query

The following query returns the number of decryption failures for each reason on each sensor, in descending order by `sensor_name` during the current day, limited to the `Global \ Company B \ Edge` domain.

```
SELECT sensor_name, failure_reason, count
FROM ssl_failure_reason_stats_current_day
WHERE domain_name= "Global \ Company B \ Edge"
ORDER BY sensor_name DESC;
```

ssl_session_stats_current_timeframe

The **ssl_session_stats_current**_*timeframe* tables contain statistics for SSL sessions. Statistics can be extracted based on bytes, connection, sensor, and time.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-3.

For more information on the **ssl_session_stats_current**_*timeframe* tables, see the following sections:

ssl_session_stats_current_timeframe Fields

The following table describes the fields you can access in the **ssl_session_stats_current**_*timeframe* tables. All tables of this type contain the same fields.

Table 5-20 ssl_session_stats_current_timeframe Fields

Field	Description
decrypted	Number of sessions successfully decrypted.
false_positive	Number of false positives detected.
netmap_num	Netmap ID for the domain on which the statistics were collected.
not_decrypted	Number of sessions which were not decrypted.
reused_by_id	SSL sessions reused by ID.
reused_by_ticket	SSL sessions reused by ticket.
sensor_name	The name of the managed device that generated the event.
start_time_sec	The UNIX timestamp of the date and time the measurement interval starts. For detailed information, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
start_time_str	The date and time of the start of the measurement interval in human-readable format of `Year-Month-Day Time`. For example, February 4th, 2022 is `2022-02-04 20:18:58`.
total_sessions	Total number of sessions.
with_error	Number of sessions which had errors.

ssl_session_stats_current_timeframe Joins

You cannot perform joins on the **ssl_session_stats_current**_*timeframe* tables.

ssl_session_stats_current_timeframe Sample Query

The following query returns the number of SSL sessions, sessions that were decrypted andsessions that were not decrypted for each sensor, in descending order by `sensor_name` during the current day, limited to the `Global \ Company B \ Edge` domain.

```
SELECT sensor_name, total_sessions, decrypted,
not_decrypted
FROM ssl_session_stats_current_day
WHERE domain_name= "Global \ Company B \ Edge"
ORDER BY sensor_name DESC;
```

ssl_version_stats_current_timeframe

The **`ssl_version_stats_current_`***`timeframe`* tables contain statistics for SSL connections. Statistics can be extracted based on bytes, connection, sensor, and time.

For an understanding of the **`current_day`**, **`current_month`**, and **`current_year`** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-3.

For more information on the **`ssl_version_stats_current_`***`timeframe`* tables, see the following sections:

- ssl_version_stats_current_timeframe Fields, page 5-27
- ssl_version_stats_current_timeframe Joins, page 5-28
- ssl_version_stats_current_timeframe Sample Query, page 5-28

ssl_version_stats_current_timeframe Fields

The following table describes the fields you can access in the **`ssl_version_stats_current_`***`timeframe`* tables. All tables of this type contain the same fields.

Table 5-21 ssl_version_stats_current_timeframe Fields

Field	Description
`count`	The number of connections of each SSL version.
`netmap_num`	Netmap ID for the domain on which the statistics were collected.
`sensor_name`	The name of the managed device that generated the event.
`start_time_sec`	The UNIX timestamp of the date and time the measurement interval starts. For detailed information, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
`start_time_str`	The date and time of the start of the measurement interval in human-readable format of `Year-Month-Day Time`**.** For example, February 4th, 2022 is `2022-02-04 20:18:58`.
`version`	SSL version detected.

ssl_version_stats_current_timeframe Joins

You cannot perform joins on the **ssl_version_stats_current**_*timeframe* tables.

ssl_version_stats_current_timeframe Sample Query

The following query returns the number of each SSL versions on each sensor, in descending order by `sensor_name` during the current day, limited to the `Global \ Company B \ Edge` domain.

```
SELECT sensor_name, version, count
FROM ssl_version_stats_current_day
WHERE domain_name= "Global \ Company B \ Edge"
ORDER BY sensor_name DESC;
```

storage_stats_by_disposition_current_timeframe

The **storage_stats_by_disposition**_*timeframe* tables contain statistics for stores files. Statistics can be extracted based on bytes, connection, sensor, and time.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-3.

For more information on the **storage_stats_by_disposition**_*timeframe* tables, see the following sections:

storage_stats_by_disposition_current_timeframe Fields

The following table describes the fields you can access in the **storage_stats_by_disposition_current**_*timeframe* tables. All tables of this type contain the same fields.

Table 5-22 storage_stats_by_disposition_current_timeframe Fields

Field	Description
bytes_written	The size of the file, in bytes.
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.
domain_name	Name of the domain specified for the statistics.
domain_uuid	UUID of the domain specified for the statistics. This is presented in binary.
netmap_num	Netmap ID for the domain on which the statistics were collected.
number_dropped	Number of files of this disposition dropped.
number_stored	Number of files of this disposition stored.
sensor	ID of the device that detected the file.
sensor_address	This field is deprecated. Use sensor_name and sensor_uuid to identify the sensor which generated the event.
sensor	ID of the device that detected the file.
sensor_id	Internal identification number of the managed device that detected the file.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.
start_time_sec	The UNIX timestamp of the date and time the measurement interval starts. For detailed information, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
start_time_str	The date and time of the start of the measurement interval in human-readable format of Year-Month-Day Time. For example, February 4th, 2022 is 2022-02-04 20:18:58.

storage_stats_by_disposition_current_timeframe Joins

You cannot perform joins on the **session_stats_current_***timeframe* tables.

storage_stats_by_disposition_current_timeframe Sample Query

The following query returns the number of dropped and stored files for each sensor, in descending order by sensor_name during the current day, limited to the Global \ Company B \ Edge domain .

```
SELECT sensor_name, number_dropped, number_stored
FROM storage_stats_by_disposition_current_day
WHERE domain_name= "Global \ Company B \ Edge"
```

```
ORDER BY sensor_name DESC;
```

storage_stats_by_file_type_current_timeframe

The **storage_stats_by_file_type_current_***timeframe* tables contain statistics for stored files by file type. Statistics can be extracted based on bytes, connection, sensor, and time.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-3.

For more information on the **storage_stats_by_file_type_current_***timeframe* tables, see the following sections:

storage_stats_by_file_type_current_timeframe Fields

The following table describes the fields you can access in the **storage_stats_by_file_type_current_***timeframe* tables. All tables of this type contain the same fields.

Table 5-23 storage_stats_by_file_type_current_timeframe Fields

Field	Description
bytes_written	The size of the file, in bytes.
domain_name	Name of the domain specified for the statistics.
domain_uuid	UUID of the domain specified for the statistics. This is presented in binary.
file_type	The file type of the detected or quarantined file.
file_type_id	ID number that maps to the file type.
netmap_num	Netmap ID for the domain on which the statistics were collected.
number_dropped	Number of files of this type dropped.
number_stored	Number of files of this type stored.
sensor	ID of the device that detected the file.
sensor_address	This field is deprecated. Use sensor_name and sensor_uuid to identify the sensor which generated the event.
sensor_name	The name of the managed device that generated the intrusion event.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.
start_time_sec	The UNIX timestamp of the date and time the measurement interval starts. For detailed information, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
start_time_str	The date and time of the start of the measurement interval in human-readable format of Year-Month-Day Time. For example, February 4th, 2022 is 2022-02-04 20:18:58.

storage_stats_by_file_type_current_timeframe Joins

You cannot perform joins on the **session_stats_current**_*timeframe* tables.

storage_stats_by_file_type_current_timeframe Sample Query

The following query returns the number of dropped and stored files for each sensor, in descending order by `file_type` during the current day, limited to the `Global \ Company B \ Edge` domain.

```
SELECT sensor_name, number_dropped, number_stored, file_type
FROM storage_stats_by_file_type_current_day
WHERE domain_name= "Global \ Company B \ Edge"
ORDER BY file_type DESC;
```

tlsfp_malware_stats_current_timeframe

The **tlsfp_malware_stats_current**_*timeframe* tables contain statistics for TLS Malware detection.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-3.

For more information on the **tlsfp_malware_stats_current**_*timeframe* tables, see the following sections:

tlsfp_malware_stats_current_timeframe Fields

The following table describes the fields you can access in the **tlsfp_malware_stats_current**_*timeframe* tables. All tables of this type contain the same fields.

Table 5-24 tlsfp_malware_stats_current_timeframe Fields

Field	Description
count	The number of connections that match the information that appears in each row.
netmap_num	Netmap ID for the domain on which the statistics were collected.
sensor_name	The name of the managed device that generated the event.
start_time_sec	The UNIX timestamp of the date and time the measurement interval starts. For detailed information, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.

Table 5-24 tlsfp_malware_stats_current_timeframe Fields (continued)

Field	Description
start_time_str	The date and time of the start of the measurement interval in human-readable format of Year-Month-Day Time. For example, February 4th, 2022 is 2022-02-04 20:18:58.
tlsfp_malware_confidence	The confidence value in the range 0-100% that the process detected by the encrypted visibility engine (EVE) contains malware. If the malware confidence score is very high, say 90%, then the TLS fingerprint Process Name field displays "Malware."

tlsfp_malware_stats_current_timeframe Joins

You cannot perform joins on the **tlsfp_malware_stats_current**_*timeframe* tables.

tls_malware_stats_current_timeframe Sample Query

The following query returns the TLS malware confidence for each sensor, in descending order by sensor_name during the current day.

```
SELECT sensor_name, tlsfp_malware_confidence
FROM tls_malware_stats_current_day
ORDER BY sensor_name DESC;
```

tlsfp_processname_stats_current_timeframe

The **tlsfp_processname_stats_current**_*timeframe* tables contain statistics for TLS Fingerprint processes.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-3.

For more information on the **tlsfp_processname_stats_current**_*timeframe* tables, see the following sections:

- ssl_session_stats_current_timeframe Fields, page 5-26
- ssl_session_stats_current_timeframe Joins, page 5-26
- ssl_session_stats_current_timeframe Sample Query, page 5-27

tlsfp_processname_stats_current_timeframe Fields

The following table describes the fields you can access in the **tlsfp_processname_stats_current**_*timeframe* tables. All tables of this type contain the same fields.

Table 5-25 tlsfp_processname_stats_current_timeframe Fields

Field	Description
count	The number of connections that match the information that appears in each row.
netmap_num	Netmap ID for the domain on which the statistics were collected.
process_name	The name of the TLS process.
sensor_name	The name of the managed device that generated the event.

tlsfp_processname_stats_current_timeframe Joins

You cannot perform joins on the **tlsfp_processname_stats_current_***timeframe* tables.

tls_processname_stats_current_timeframe Sample Query

The following query returns the TLS process name for each sensor, in descending order by sensor_name during the current day.

```
SELECT sensor_name, process_name
FROM tls_processname_stats_current_day
ORDER BY sensor_name DESC;
```

transmission_stats_by_file_type_current_timeframe

The **transmission_stats_by_file_type_current_***timeframe* tables contain statistics for stored files by file type. Statistics can be extracted based on bytes, connection, sensor, and time.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-3.

For more information on the **transmission_stats_by_file_type_current_***timeframe* tables, see the following sections:

transmission_stats_by_file_type_current_timeframe Fields

The following table describes the fields you can access in the **transmission_stats_by_file_type_current_***timeframe* tables. All tables of this type contain the same fields.

Table 5-26 transmission_stats_by_file_type_current_timeframe Fields

Field	Description
bytes_sent	The number of transmitted bytes.
domain_name	Name of the domain specified for the statistics.
domain_uuid	UUID of the domain specified for the statistics. This is presented in binary.
file_type	The file type of the detected or quarantined file.
file_type_id	ID number that maps to the file type.
netmap_num	Netmap ID for the domain on which the statistics were collected.
number_dropped	Number of files of this type dropped.
number_sent	Number of files of this type sent.
sensor	ID of the device that detected the file.
sensor_address	This field is deprecated. Use sensor_name and sensor_uuid to identify the sensor which generated the event.
sensor_name	The name of the managed device that generated the intrusion event.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.
start_time_sec	The UNIX timestamp of the date and time the measurement interval starts. For detailed information, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
start_time_str	The date and time of the start of the measurement interval in human-readable format of Year-Month-Day Time. For example, February 4th, 2022 is 2022-02-04 20:18:58.

transmission_stats_by_file_type_current_timeframe Joins

You cannot perform joins on the **transmission_stats_by_file_type_current_***timeframe* tables.

transmission_stats_by_file_type_current_timeframe Sample Query

The following query returns the number of dropped and sent connections for each sensor, in descending order by file_type during the current day, limited to the Global \ Company B \ Edge domain.

```
SELECT sensor_name, number_dropped, number_sent, file_type
FROM transmission_stats_by_file_type_current_day
WHERE domain_name= "Global \ Company B \ Edge"
ORDER BY file_type DESC;
```

url_category_stats_current_timeframe

The **url_category_stats_current_***timeframe* tables contain statistics on the bandwidth usage and connections associated with requests to URLs in specified URL categories. You can also constrain queries on the managed device that monitored the traffic.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-3.

For more information on the **url_category_stats_current_***timeframe* tables, see the following sections:

- url_category_stats_current_timeframe Fields, page 5-35
- url_category_stats_current_timeframe Joins, page 5-35
- url_category_stats_current_timeframe Sample Query, page 5-36

url_category_stats_current_timeframe Fields

The following table describes the fields you can access in the **url_category_stats_current_***timeframe* tables.

Table 5-27 url_category_stats_current_timeframe Fields

Field	Description
bytes_in	The bytes of inbound traffic during the specified interval.
bytes_out	The bytes of outbound traffic during the specified interval.
category	The category of the URL.
connections_allowed	The number of connections allowed for the specified URL category.
connections_denied	The number of connections denied for the specified URL category due to violation of an access control policy.
domain_name	Name of the domain specified for the statistics.
domain_uuid	UUID of the domain specified for the statistics. This is presented in binary.
netmap_num	Netmap ID for the domain on which the statistics were collected.
sensor_address	This field is deprecated. Use sensor_name and sensor_uuid to identify the sensor which generated the event.
sensor_id	The internal identification number of the managed device that detected the traffic.
sensor_name	The managed device that monitored the traffic.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.
start_time_sec	The UNIX timestamp of the start of the measurement interval. For information on specifying the start time, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
start_time_str	The date and time of the start of the measurement interval in human-readable format of Year-Month-Day Time. For example, February 4th, 2022 is 2022-02-04 20:18:58.

url_category_stats_current_timeframe Joins

You cannot perform joins on the **url_category_stats_current_***timeframe* tables.

url_category_stats_current_timeframe Sample Query

The following query returns up to 25 URL category records. Each record contains the bytes of associated inbound and outbound traffic, as well as allowed and denied connections, over the specified time interval. This query is limited to the `Games` category and the `Global \ Company B \ Edge` domain.

```
SELECT category, sensor_name, start_time_sec, bytes_in, bytes_out, connections_allowed,
connections_denied
FROM url_category_stats_current_year
WHERE category="Games" AND domain_name= "Global \ Company B \ Edge"
LIMIT 0, 25;
```

url_reputation_stats_current_timeframe

The **`url_reputation_stats_current_`***`timeframe`* tables contain statistics on the bandwidth usage and connections associated with requests to URLs with specified reputations. Query results can also be constrained on the managed device that monitored the traffic.

For an understanding of the **`current_day`**, **`current_month`**, and **`current_year`** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-3.

For more information on the **`url_reputation_stats_current_`***`timeframe`* tables, see the following sections:

- url_reputation_stats_current_timeframe Fields, page 5-36
- url_reputation_stats_current_timeframe Joins, page 5-37
- url_reputation_stats_current_timeframe Sample Query, page 5-37

url_reputation_stats_current_timeframe Fields

The following table describes the fields you can access in the **`url_reputation_stats_current_`***`timeframe`* tables.

Table 5-28 url_reputation_stats_current_timeframe Fields

Field	Description
`bytes_in`	The bytes of inbound traffic during the specified interval.
`bytes_out`	The bytes of outbound traffic during the specified interval.
`connections_allowed`	The number of connections allowed.
`connections_denied`	The number of connections denied due to violation of an access control policy.
`domain_name`	Name of the domain specified for the statistics.
`domain_uuid`	UUID of the domain specified for the statistics. This is presented in binary.
`netmap_num`	Netmap ID for the domain on which the statistics were collected.

Table 5-28 url_reputation_stats_current_timeframe Fields (continued)

Field	Description
reputation	The reputation associated with the requested URL. One of the following: • Trusted - Displaying behavior that indicates exceptional safety • Favorable - Displaying behavior that indicates a level of safety • Neutral - Displaying neither positive or negative behavior. However, has been evaluated. • Questionable - Displaying behavior that may indicate risk, or could be undesirable • Untrusted - Displaying behavior that is exceptionally bad, malicious, or undesirable • Unknown - Not previously evaluated, or lacking features to assert a threat level verdict
sensor_address	This field is deprecated. Use sensor_name and sensor_uuid to identify the sensor which generated the event.
sensor_id	Internal identification number of the managed device that monitored the traffic.
sensor_name	The name of the managed device that monitored the traffic.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.
start_time_sec	The UNIX timestamp of the start of the measurement interval. For information on specifying the start time, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
start_time_str	The date and time of the start of the measurement interval in human-readable format of Year-Month-Day Time. For example, February 4th, 2022 is 2022-02-04 20:18:58.

url_reputation_stats_current_timeframe Joins

You cannot perform joins on the **url_reputation_stats_current_*timeframe*** tables.

url_reputation_stats_current_timeframe Sample Query

The following query returns up to 25 URL reputation records from the **url_reputation_stats_current_month** table. Each record contains the bytes of inbound and outbound traffic, as well as allowed and denied connections over the measurement time interval. This particular query is limited to the High risk reputation and Global \ Company B \ Edge domain.

```
SELECT sensor_name, reputation, start_time_sec, bytes_in, bytes_out,
connections_allowed, connections_denied

FROM url_reputation_stats_current_year

WHERE reputation="High risk" AND domain_name= "Global \ Company B \ Edge"

LIMIT 0, 25;
```

user_ids_stats_current_timeframe

The **user_ids_stats_current_***timeframe* tables are round-robin tables that contain statistics on access filtering and impact statistics by user.

For an understanding of the **current_day**, **current_month**, and **current_year** tables in this type, see Storage Characteristics for Statistics Tracking Tables, page 5-3.

For general information on using the round robin statistics tables, see Understanding Statistics Tracking Tables, page 5-3.

For more information on the **user_ids_stats_current_***timeframe* tables, see the following sections:

user_ids_stats_current_timeframe Fields

The following table describes the fields you can access in the **user_ids_stats_current_***timeframe* tables.

Table 5-29 user_ids_stats_current_timeframe Fields

Field	Description
blocked	The number of connections blocked due to violation of an intrusion policy.
domain_name	Name of the domain specified for the statistics.
domain_uuid	UUID of the domain specified for the statistics. This is presented in binary.
impact_level_1	The number of impact level 1 (vulnerable) intrusion events recorded for the user.
impact_level_2	The number of impact level 2 (potentially vulnerable) intrusion events recorded for the user.
impact_level_3	The number of impact level 3 (host currently not vulnerable) intrusion events recorded for the user.
impact_level_4	The number of impact level 4 (unknown target) intrusion events recorded for the user.
impact_level_5	The number of impact level 5 (unknown vulnerability) intrusion events recorded for the user.
netmap_num	Netmap ID for the domain on which the statistics were collected.
partially_dropped	Number of instances when the packet is transmitted or delivered to the destination, but the connection is then blocked.
sensor_address	This field is deprecated. Use sensor_name and sensor_uuid to identify the sensor which generated the event.
sensor_id	The internal identification number of the managed device that detected the traffic.
sensor_name	The name of the managed device that detected the traffic.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.

Table 5-29 user_ids_stats_current_timeframe Fields (continued)

Field	Description
start_time_sec	The UNIX timestamp of the start of the measurement interval. For information on specifying the start time, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
start_time_str	The date and time of the start of the measurement interval in human-readable format of `Year-Month-Day Time`. For example, February 4th, 2022 is `2022-02-04 20:18:58`.
user_full_name	Full name of the user.
user_id	An internal identification number for the user who last logged into the host.
user_protocol	Protocol on which the user was detected.
username	The user name of the user who last logged into the host.
would_have_dropped	Number of packets that would have been dropped if the intrusion policy had been configured to drop packets in an inline deployment.

user_ids_stats_current_timeframe Joins

You cannot perform joins on the **user_ids_stats_current**_*timeframe* tables.

user_ids_stats_current_timeframe Sample Query

The following query returns up to 25 user records from the **user_ids_stats_current_month** table. Each record contains the number of blocked connections and intrusion events for the selected `username` with the `Global \ Company B \ Edge` domain.

```
SELECT username, start_time_sec, blocked, impact_level_1, impact_level_2,
impact_level_3, impact_level_4, impact_level_5 FROM user_ids_stats_current_year
WHERE username="username" AND domain_name= "Global \ Company B \ Edge"
LIMIT 0, 25;
```

user_stats_current_timeframe

The **user_stats_current**_*timeframe* tables contain statistics on bandwidth usage and access control actions (connection allowed or denied) by user. You can also constrain queries on the managed device that monitored the traffic.

For an understanding of the **current_day**, **current_month**, and **current_year** statistics tables, see Storage Characteristics for Statistics Tracking Tables, page 5-3.

For more information, see the following sections:

user_stats_current_timeframe Fields

The following table describes the fields you can access in the **user_stats_current**_*timeframe* tables.

Table 5-30 user_stats_current_timeframe Fields

Field	Description
bytes_in	The number of bytes of inbound traffic for the user in the measured interval.
bytes_out	The number of bytes of outbound traffic for the user in the measured interval.
connections_allowed	The number of connections allowed for this user in the measured time frame.
connections_denied	The number of connections denied for this user due to violation of an access control policy.
domain_name	Name of the domain specified for the statistics.
domain_uuid	UUID of the domain specified for the statistics. This is presented in binary.
netmap_num	Netmap ID for the domain on which the statistics were collected.
qos_dropped_bytes_in	Number of incoming bytes dropped due to QoS.
qos_dropped_bytes_out	Number of outgoing bytes dropped due to QoS.
sensor_address	This field is deprecated. Use sensor_name and sensor_uuid to identify the sensor which generated the event.
sensor_id	The internal identification number of the managed device that detected the traffic.
sensor_name	The name of the managed device that detected the traffic.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.
start_time_sec	The UNIX timestamp of the start of the measurement interval. For information on specifying the start time, see Specifying Time Intervals When Querying Statistics Tables, page 5-3.
start_time_str	The date and time of the start of the measurement interval in human-readable format of Year-Month-Day Time**.** For example, February 4th, 2022 is 2022-02-04 20:18:58.
user_full_name	Full name of the user.
user_id	The internal identification number for the user who last logged into the host that generated the traffic.
user_protocol	Protocol on which the user was detected.
username	User name for the user who last logged into the host that generated the traffic.

user_stats_current_timeframe Joins

You cannot perform joins on the **user_stats_current**_*timeframe* tables.

user_stats_current_timeframe Sample Query

The following query returns up to 25 user records. Each record contains the bytes of inbound and outbound traffic, as well as allowed and denied connections over the measurement time interval within the domain_name= "Global \ Company B \ Edge domain.

```
SELECT sensor_name, username, start_time_sec, bytes_in, bytes_out,
```

```
connections_allowed, connections_denied
FROM user_stats_current_year
WHERE username="username" AND domain_name= "Global \ Company B \ Edge"
LIMIT 0, 25;
```