CHAPTER 8

Schema: User Activity Tables

This chapter contains information on the schema and supported joins for user activity and identity events. The FireSIGHT System can detect user activity on your network by tracking various types of user logins, including LDAP, POP3, IMAP, SMTP, AIM, and SIP.

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

Table 8-1 Schema for User Identity Tables

See...	For the table that stores information on...	Version
discovered_users, page 8-1	Information about the users detected by the system.	5.0+
user_discovery_event, page 8-2	User discovery events, which communicate the details of user activity on your network.	5.0+

discovered_users

The **discovered_users** table contains detailed information about each user detected by the system.

The **discovered_users** table supersedes the deprecated **rua_users** table starting with Version 5.0 of the FireSIGHT System.

For more information, see the following sections:

- discovered_users Fields, page 8-1
- discovered_users Joins, page 8-2
- discovered_users Sample Query, page 8-2

discovered_users Fields

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

Table 8-2 discovered_users Fields

Field	Description
dept	The department of the user.
email	The email address for the user.
first_name	The first name for the user.

Table 8-2 discovered_users Fields (continued)

Field	Description
ip_address	This field has been deprecated and returns null for all queries.
ipaddr	A binary representation of the IPv4 or IPv6 address for the host where the user login was detected.
last_name	The last name for the user.
last_seen_sec	The UNIX timestamp of the date and time the system last reported a login for the user.
last_updated_sec	The UNIX timestamp of the date and time the user's information was last updated.
name	The name for the user.
phone	The phone number for the user.
rna_service	Field deprecated in Version 5.0. Returns null for all queries.
user_id	The internal identification number of the user who last logged onto the host.

discovered_users Joins

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

Table 8-3 discovered_users Joins

You can left join on this field...	With other tables that have join type of...
user_id	user_discovery_event.user_id user_ipaddr_history.user_id

discovered_users Sample Query

The following query returns up to 25 discovered user records that were generated since a specified date and time.

```
SELECT user_id, ip_address, email, name, last_seen_sec, last_updated_sec

FROM discovered_users

WHERE last_seen_sec >= UNIX_TIMESTAMP("2011-10-01 00:00:00")

LIMIT 0, 25;
```

user_discovery_event

The **user_discovery_event** table contains a record for each user discovery event.

Note that starting in Version 5.0, the FireSIGHT System records the detection of user activity at the managed device level, no longer by detection engine. The detection_engine_name and detection_engine_uuid fields in this table have been replaced by the sensor_name and sensor_uuid fields respectively. Queries on these fields will return information about the managed device that generated the user discovery event.

For more information, see the following sections:

user_discovery_event Fields

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

Table 8-4 user_discovery_event Fields

Field	Description
application_protocol_id	An internal identifier for the detected application protocol.
application_protocol_name	One of: • the name of the application used in the connection: LDAP, POP3, and so on • pending if the system cannot identify the application for one of several reasons • blank if there is no application information in the connection
description	The user name when the discovery event type is either Delete User Identity, or User Identity Dropped. Otherwise, blank.
event_id	An internal identification number for the discovery event.
event_time_sec	The UNIX timestamp of the date and time of the discovery event.
event_type	The type of discovery event. For example, New User Identity or User Login.
ip_address	Field deprecated in Version 5.2. Returns null for all queries.
ipaddr	A binary representation of the IP address of the host where the user activity was detected.
reported_by	The IPv4 address, IPv6 address, or NetBIOS name of the Active Directory server reporting a user login.
sensor_address	The IP address of the managed device that detected the user discovery event. Format is *ipv4_address,ipv6_address*.
sensor_name	The text name of the managed device that detected the user discovery event.
sensor_uuid	A unique identifier for the managed device, or 0 if sensor_name is null.
user_dept	The department of the user who last logged onto the host.
user_email	The email address of the user who last logged onto the host.
user_first_name	The first name of the user.
user_id	The internal identification number of the user who last logged onto the host.
user_last_name	The last name of the user.
user_last_seen_sec	The UNIX timestamp of the date and time the system last reported a login for the user.
user_last_updated_sec	The UNIX timestamp of the date and time the user’s information was last updated.
user_name	The user name for the user who last logged onto the host.
user_phone	The phone number for the user who last logged onto the host.

user_discovery_event Joins

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

Table 8-5 user_discovery_event Joins

You can join this table on...	And...
ipaddr	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr
user_id	discovered_users.user_id user_ipaddr_history.user_id

user_discovery_event Sample Query

The following query returns up to 25 user event records generated by a selected managed device since a particular date and time.

```
SELECT event_time_sec, ipaddr, sensor_name, event_type, user_name, user_last_seen_sec,
user_last_updated_sec

FROM user_discovery_event

WHERE sensor_name = sensor_name

AND user_last_seen_sec >= UNIX_TIMESTAMP("2011-10-01 00:00:00") ORDER BY event_type ASC

LIMIT 0, 25;
```