Introduction

The FireSIGHT System® database access feature allows you to query intrusion, discovery, user activity, correlation, connection, vulnerability, and application and URL statistics database tables on a Cisco Defense Center, using a third-party client that supports JDBC SSL connections.

You can use an industry-standard reporting tool such as Crystal Reports, Actuate BIRT, or JasperSoft iReport to design and submit queries. Or, you can configure your own custom application to query Cisco data under program control. For example, you can build a servlet to report intrusion and discovery event data periodically or refresh an alert dashboard.

Note that you can connect to multiple Defense Centers with a single client, but you must configure access to each one individually.

When deciding which appliance or appliances to connect to, keep in mind that querying the database on a Cisco appliance reduces available appliance resources. You should carefully design your queries and submit them at times consistent with your organization's priorities.

For more information, see the following sections:

- Major Changes for Database Access in Version 5.4, page 1-9
- Prerequisites, page 1-12
- Where Do I Begin?, page 1-14

Major Changes for Database Access in Version 5.4

If you are upgrading your FireSIGHT System deployment from Version 5.3.1 to Version 5.4, please note the following changes, some of which may require you to update your queries.

Modified Fields for Version 5.4

The `file_name` fields in `fireamp_event` and `file_event` can contain UTF-8 characters.

Modified Tables for Version 5.4

The table below lists changes to database access tables in Version 5.4.

Table 1-1 Summary of Changes to Tables in Version 5.4

Table	Description of Changes
application_host_map, page 6-5	Deprecated `application_tag_id` field
connection_log, page 7-1	Added the following fields: • `access_control_policy_uuid` • `cert_valid_start_date` • `cert_valid_end_date` • `network_analysis_policy_name` • `network_analysis_policy_UUID` • `ssl_actual_action` • `ssl_cipher_suite` • `ssl_expected_action` • `ssl_flow_flags` • `ssl_flow_messages` • `ssl_flow_status` • `ssl_issuer_common_name` • `ssl_issuer_country` • `ssl_issuer_organization` • `ssl_issuer_organization_unit` • `ssl_policy_action` • `ssl_policy_name` • `ssl_policy_reason` • `ssl_rule_action` • `ssl_rule_name` • `ssl_serial_number` • `ssl_server_name` • `ssl_subject_common_name` • `ssl_subject_country` • `ssl_subject_organization` • `ssl_subject_organization_unit` • `ssl_url_category` • `ssl_version`

Table 1-1 Summary of Changes to Tables in Version 5.4 (continued)

Table	Description of Changes
si_connection_log, page 7-16	Added the following fields: • access_control_policy_uuid • cert_valid_start_date • cert_valid_end_date • network_analysis_policy_name • network_analysis_policy_UUID • ssl_actual_action • ssl_cipher_suite • ssl_expected_action • ssl_flow_flags • ssl_flow_messages • ssl_flow_status • ssl_issuer_common_name • ssl_issuer_country • ssl_issuer_organization • ssl_issuer_organization_unit • ssl_policy_action • ssl_policy_name • ssl_policy_reason • ssl_rule_action • ssl_rule_name • ssl_serial_number • ssl_server_name • ssl_subject_common_name • ssl_subject_country • ssl_subject_organization • ssl_subject_organization_unit • ssl_url_category • ssl_version

Table 1-1 Summary of Changes to Tables in Version 5.4 (continued)

Table	Description of Changes
file_event, page 10-1	Added the following fields: • cert_valid_start_date • cert_valid_end_date • ssl_issuer_common_name • ssl_issuer_country • ssl_issuer_organization • ssl_issuer_organization_unit • ssl_serial_number • ssl_subject_common_name • ssl_subject_country • ssl_subject_organization • ssl_subject_organization_unit
fireamp_event, page 3-2	Added the following fields: • cert_valid_start_date • cert_valid_end_date • ssl_issuer_common_name • ssl_issuer_country • ssl_issuer_organization • ssl_issuer_organization_unit • ssl_serial_number • ssl_subject_common_name • ssl_subject_country • ssl_subject_organization • ssl_subject_organization_unit
intrusion_event, page 4-1	Added the following fields: • access_control_policy_UUID • network_analysis_policy_name • network_analysis_policy_UUID

Prerequisites

You must fulfill the prerequisites listed in the following sections before you can use the database access feature:

- Licensing, page 1-13
- FireSIGHT System Features and Terminology, page 1-13
- Communication Ports, page 1-13

Licensing

You can query the external database with any Cisco license installed. However, certain tables are associated with licensed features. These tables are only populated with data if the appropriate Cisco license is installed and your deployment is properly configured to generate the data. If you query these tables and the associated Cisco license is not installed, you retrieve no results. For more information about licensing, see Understanding Licensing in the *FireSIGHT System User Guide*.

FireSIGHT System Features and Terminology

To understand the information in this guide, you should be familiar with the features and nomenclature of the FireSIGHT System, and the function of its components. You should be familiar with the different types of event data these components generate. Note that you can frequently obtain definitions of unfamiliar or product-specific terms in the *FireSIGHT System User Guide*. The user guide also contains additional information about the data in the fields documented in this guide.

Communication Ports

The FireSIGHT System requires the use of specific ports to communicate internally and externally, between appliances, and to enable certain functionality within the network deployment.

After you enable database access on the Defense Center, the system uses ports 1500 and 2000 for the connection that carries JDBC traffic between the client and the appliance.

Client System

On the computer that you want to use to connect to the Cisco database, you must install Java software, also known as the Java Runtime Environment (JRE) or the Java Virtual Machine (JVM). You can download the latest version of Java from `http://java.com/`.

You must download and unzip a package from the Defense Center that contains the JDBC driver files you will use to connect to the database. The package also contains executable files used to install an SSL certificate for encrypted communication with the Defense Center, and other source files for these utilities.

You should also understand how to change applicable system settings on your computer, such as environment variables.

Query Application

To query the Cisco database, you can use commercially available reporting tools such as Actuate BIRT, JasperSoft iReport, or Crystal Reports, or any other application (including custom applications) that supports JDBC SSL connections. This guide provides the information you need to connect to the

database, including the JDBC URL, driver JAR files, driver class, and so on. However, you should refer to your reporting tool documentation for detailed instructions on how to configure a JDBC SSL connection.

Cisco also provides a sample command-line Java application named RunQuery, which you can use to test your database connection, view the schema, and run basic ad hoc queries manually. The RunQuery source code is also a reference for setting up the database connection in a custom Java application. The RunQuery source code is included in the ZIP package that you download from the Defense Center.

RunQuery is a sample client only, **not** a fully featured reporting tool. Cisco **strongly** recommends against using it as your primary method of querying the database. For information on using RunQuery, refer to the README file included in the ZIP package.

Note that the database access feature uses only the following JDBC functionalities:

- database metadata, which includes information such as schema, version, and supported features
- SQL query execution

Database access does not use any other JDBC functionality, including stored procedures, transactions, batch commands, multiple result sets, or insert/update/delete functions.

Database Queries

To query the database, you should know how to construct and execute `SELECT` statements on single tables and on multiple tables using join conditions.

To assist you, this guide contains information on supported MySQL query syntax, the Cisco database schema, allowed joins, and other important query-related requirements and limitations.

Where Do I Begin?

After you have met the prerequisites described in Prerequisites, page 1-12, you can begin configuring your client system to connect to a Defense Center.

Setting Up Database Access, page 2-1 explains how to configure the appliance to allow access, how to configure your client system to connect to the appliance, and how to configure your reporting application to connect to the appliance. It also contains some basic query instructions and information on supported MySQL syntax.

The rest of the guide contains schema and join information for the database and sample queries, and is split into the following chapters:

- Schema: System-Level Tables, page 3-1 contains schema and join information for system-level tables such as the audit log and health events.
- Schema: Intrusion Tables, page 4-1 contains schema and join information for intrusion-related tables.
- Schema: Statistics Tracking Tables, page 5-1 contains schema and join information for application, URL, and user statistics tables.
- Schema: Discovery Event and Network Map Tables, page 6-1 contains schema and join information for tables that contain discovery event and network map information, that is, information on your network assets.
- Schema: Connection Log Tables, page 7-1 contains schema and join information for tables that contain connection event and connection summary event information.

- Schema: User Activity Tables, page 8-1 contains schema and join information for tables that contain user discovery and identity data.
- Schema: Correlation Tables, page 9-1 contains schema and join information for correlation-related tables, including white list events and violations and remediation status data.
- Schema: File Event Tables, page 10-1 contains schema and join information for the table that contains file events.