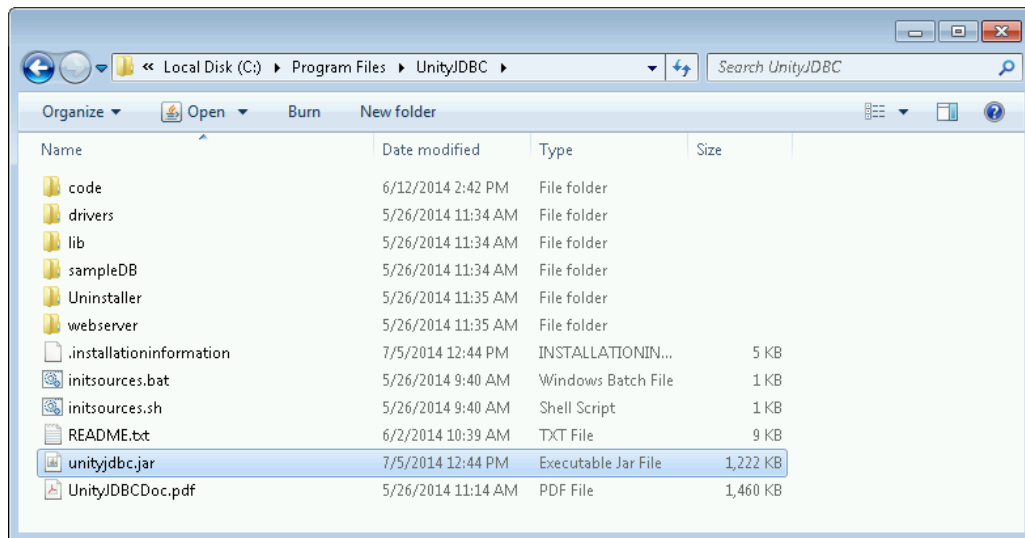
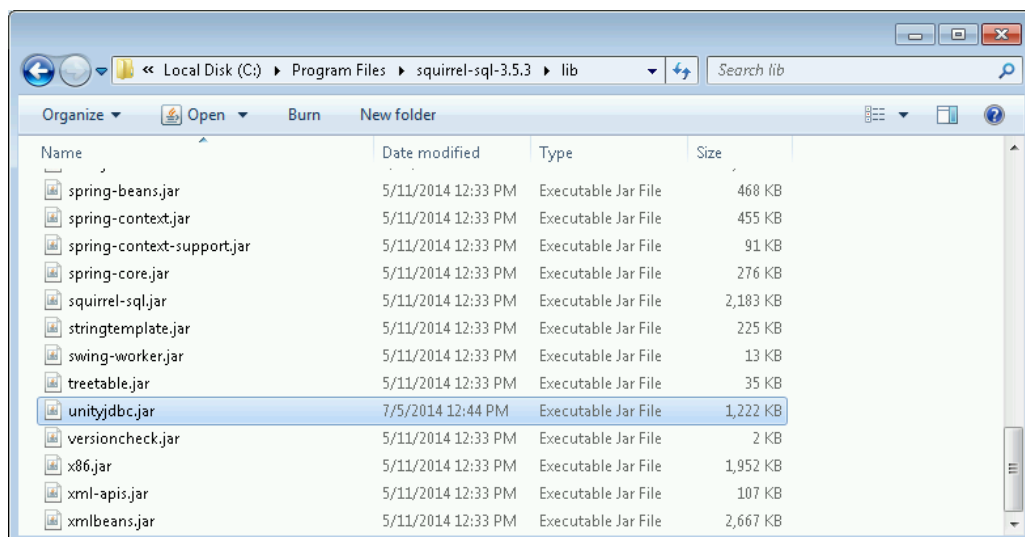



# Splunk JDBC and UnityJDBC Driver Setup for Squirrel SQL

1. Download and install UnityJDBC at <http://www.unityjdbc.com/download.php>.
2. After installation, there is a **unityjdbc.jar** file in the installation directory. On Windows, the default install path is: **C:\Program Files\UnityJDBC**

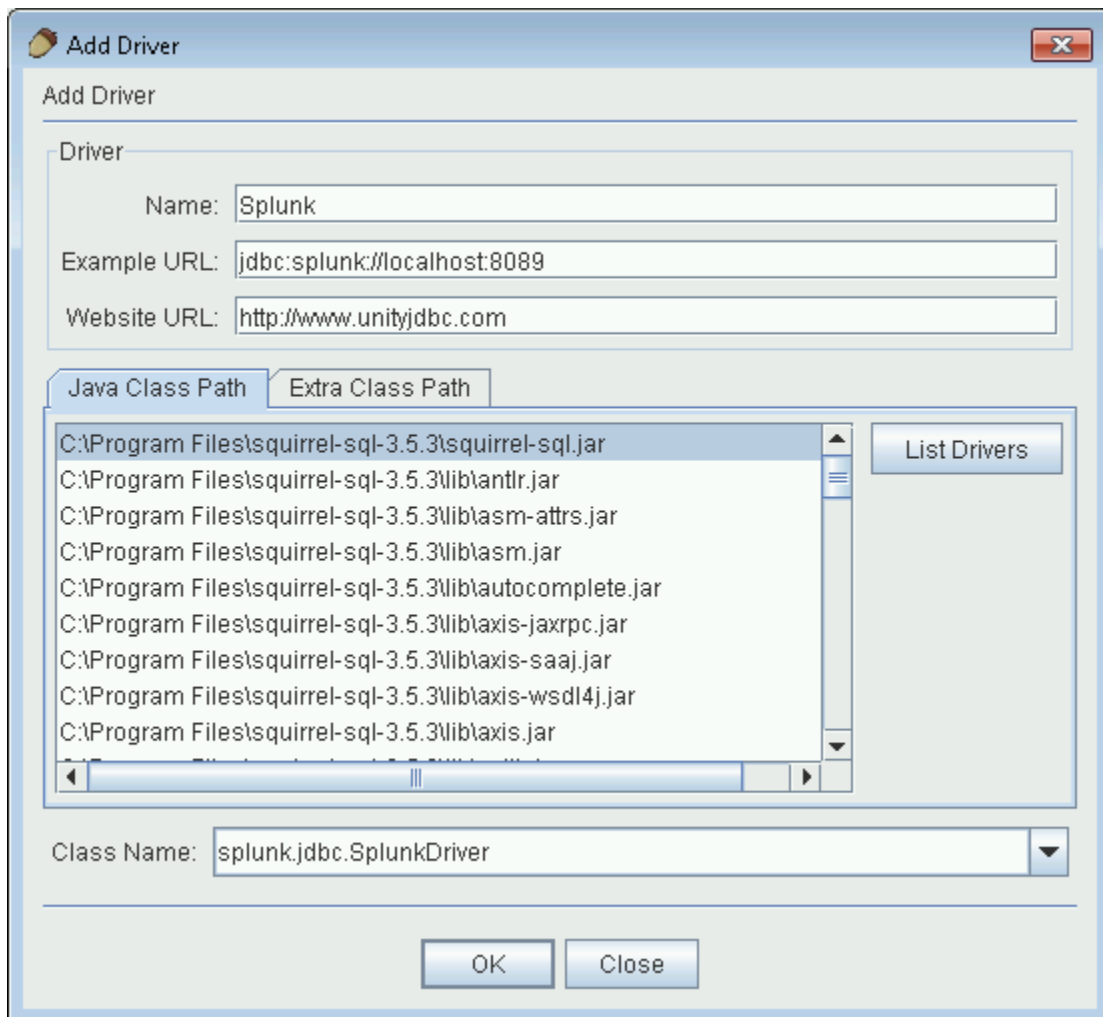


3. Copy the **unityjdbc.jar** file into the **lib** folder for your Squirrel SQL installation. For example: `C:\Program Files\squirrel-sql-3.5.3\lib`. You also need to copy the files **gson-2.2.4.jar** and **splunk-sdk-java-1.3.jar** from the subdirectory `drivers\Splunk`.

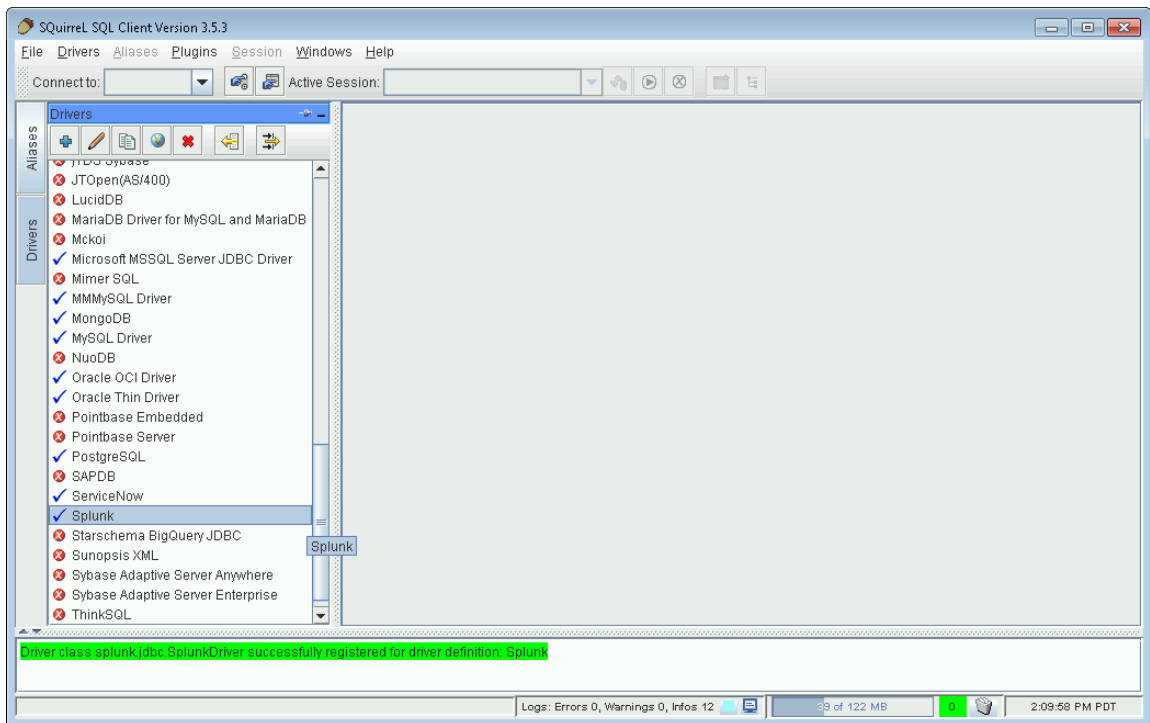


4. Start Squirrel SQL. Under the **Drivers** tab, click Add  to add a new driver. Click **OK**.  
Settings:

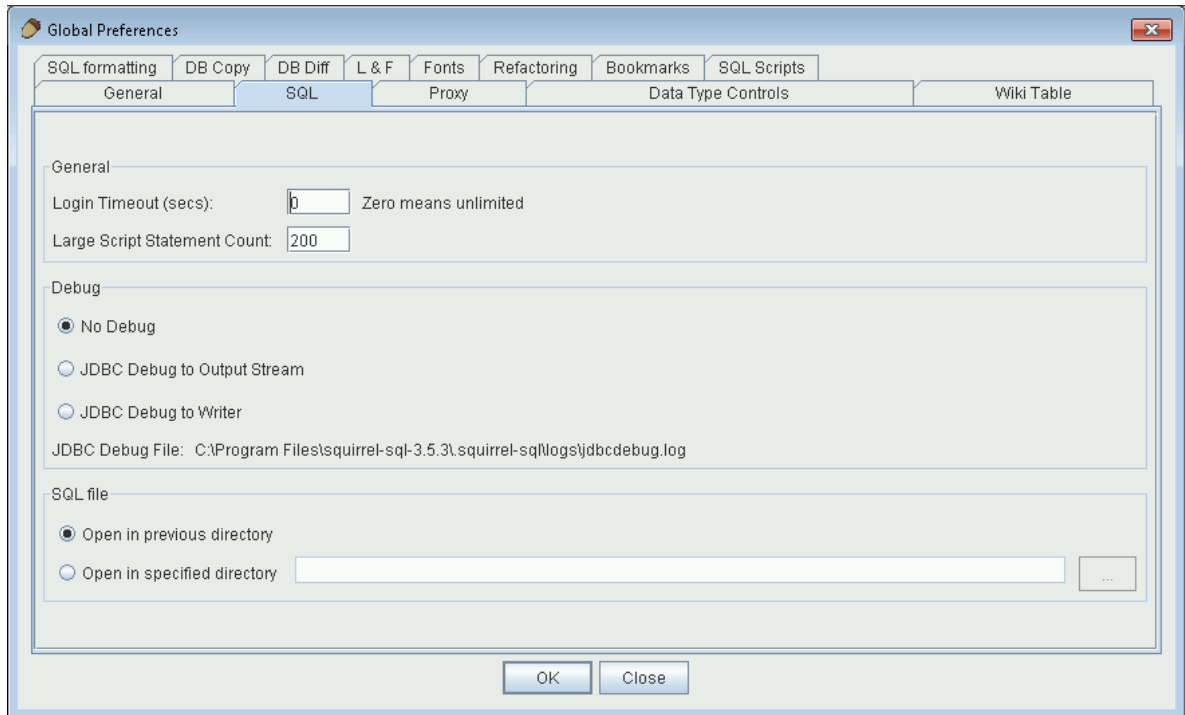
<b>Name</b>	Splunk
<b>Example URL</b>	jdbc:splunk://localhost:8089
<b>Website (Optional)</b>	http://www.unityjdbc.com
<b>Class Name:</b>	splunk.jdbc.SplunkDriver




5. After installation, the **Splunk** driver should be checked indicating it is ready for use. If not, make sure the **unityjdbc.jar** and the two other JAR files were installed correctly.

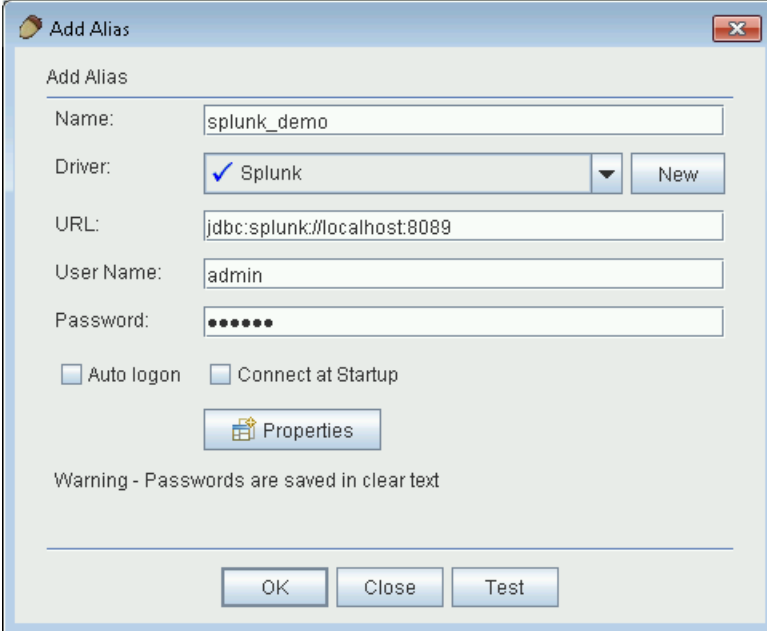


- The Splunk JDBC driver builds a schema on the first connection and caches it in a local file. This schema building may take some time. You can set Squirrel not to timeout connections. Under the **File** menu select **Global Preferences** then in the **SQL** tab set **Login Timeout** to **0** (unlimited).



7. Click on the **Aliases** tab. Then click the plus symbol  to add a new alias. Here is alias information for a sample Splunk database:

<b>Alias</b>	splunk_demo
<b>User Name</b>	admin
<b>Password</b>	admin
<b>JDBC URL</b>	jdbc:splunk://localhost:8089



Add Alias

Add Alias

Name: splunk\_demo

Driver:  Splunk


URL: jdbc:splunk://localhost:8089

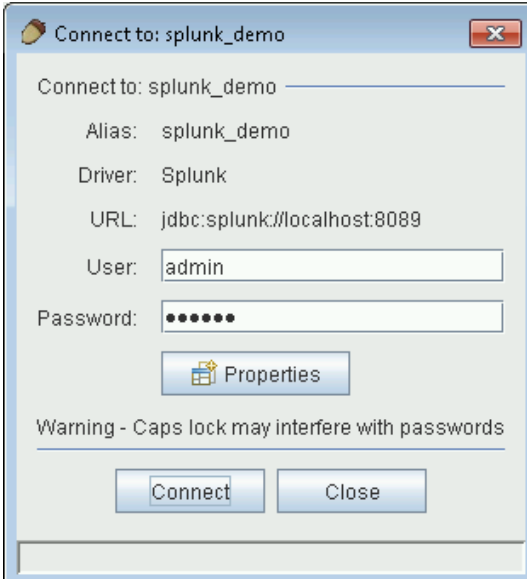
User Name: admin

Password: .....

Auto logon  Connect at Startup

Warning - Passwords are saved in clear text

8. Click **OK**. You can then connect by clicking on the Connection icon  to the left of the plus or by clicking on the **Connect** button.



Connect to: splunk\_demo

Connect to: splunk\_demo

Alias: splunk\_demo

Driver: Splunk

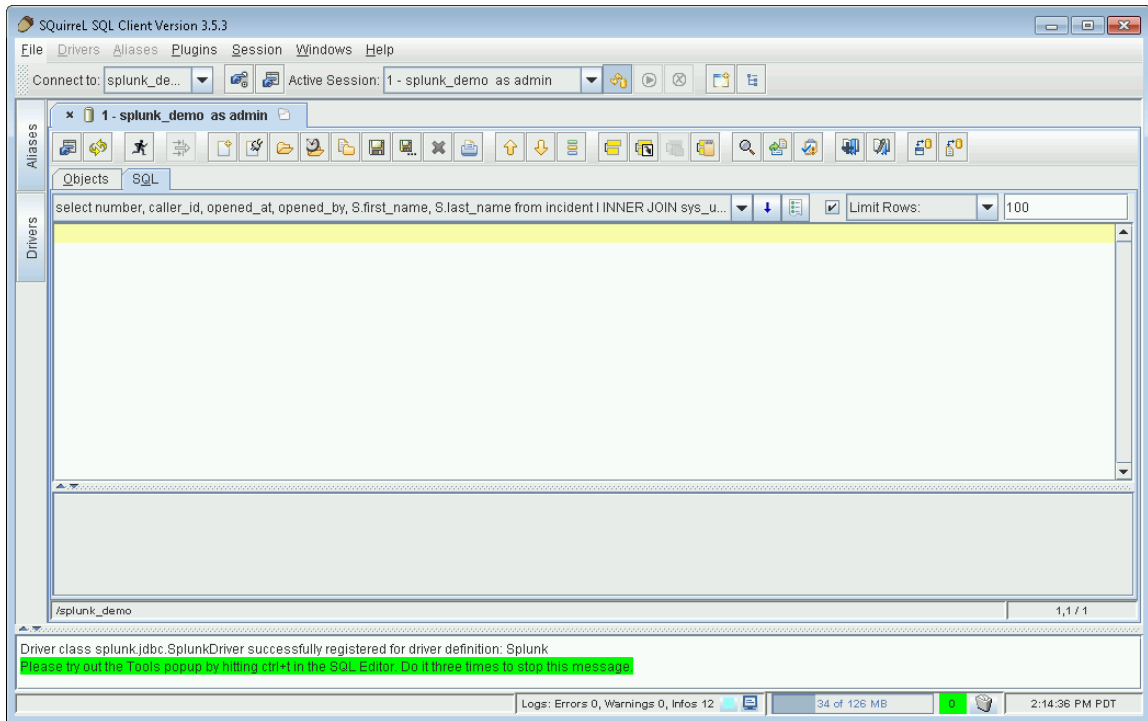
URL: jdbc:splunk://localhost:8089

User: admin

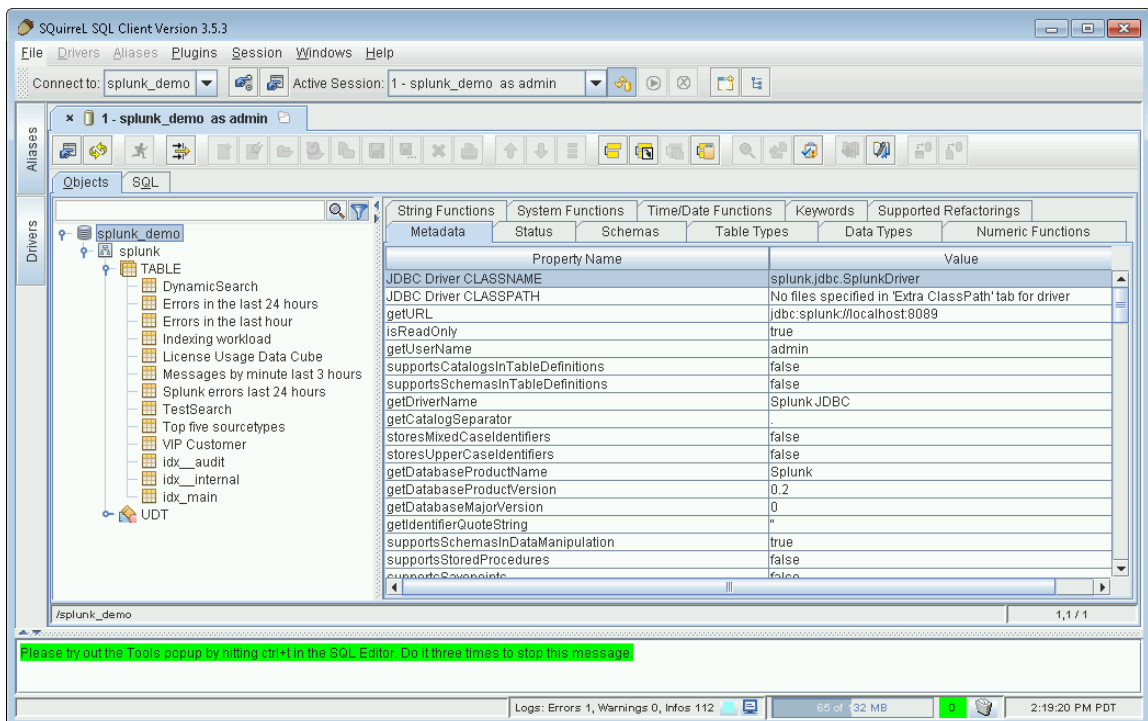
Password: .....

Warning - Caps lock may interfere with passwords

9. After connection you will see a window that allows you to enter SQL queries.



10. To browse the schema, click on the **Objects** tab.



11. View table contents by clicking on a table and selecting the **Content** tab.

Squirrel SQL Client Version 3.5.3

Connect to: splunk\_demo Active Session: 1 - splunk\_demo as admin

Objects: SQL

Drivers: splunk\_demo > splunk > TABLE

Info	Content	Row Count	Columns	Primary Key	Exported Keys
JSESSIONID	action	bytes	clientip	cookie	date_hour date_mday
SD5SL6FF7ADFF53001	purchase	1167	12.130.60.5		17 15
SD6SL4FF1ADFF52990	purchase	420	64.66.0.20		17 15
SD8SL10FF9ADFF52956	purchase	3531	74.53.23.135		17 15
SD0SL9FF7ADFF52798	purchase	3187	201.42.223.29		17 15
SD3SL5FF5ADFF52775	purchase	2421	212.235.92.150		17 15
SD10SL4FF2ADFF52743	purchase	727	211.166.11.101		17 15
SD5SL5FF8ADFF52479	purchase	2141	121.254.179.199		16 15
SD3SL3FF10ADFF52417	purchase	3413	194.215.205.19		16 15
SD9SL2FF4ADFF52361	purchase	623	27.35.11.11		15 15
SD2SL10FF4ADFF52352	purchase	640	222.41.213.238		15 15
SD1SL9FF1ADFF52322	purchase	518	175.44.24.82		15 15
SD5SL6FF6ADFF52150	purchase	2297	203.172.197.2		15 15
SD2SL5FF4ADFF52074	purchase	2688	201.122.42.235		15 15
SD7SL10FF8ADFF51926	purchase	899	201.122.42.235		14 15
SD2SL9FF7ADFF51891	purchase	2669	175.44.26.139		14 15
SD5SL5FF3ADFF51802	purchase	1252	118.142.68.222		14 15
SD0SL1FF6ADFF51786	purchase	999	201.42.223.29		14 15
SD2SL6FF3ADFF51740	purchase	1261	60.220.219.89		14 15

Logs: Errors 1, Warnings 0, Infos 183 49 of 132 MB 2:21:34 PM PDT

12. View table fields by clicking on a table and selecting the **Columns** tab.

Squirrel SQL Client Version 3.5.3


Connect to: splunk\_demo Active Session: 1 - splunk\_demo as admin

Objects: SQL

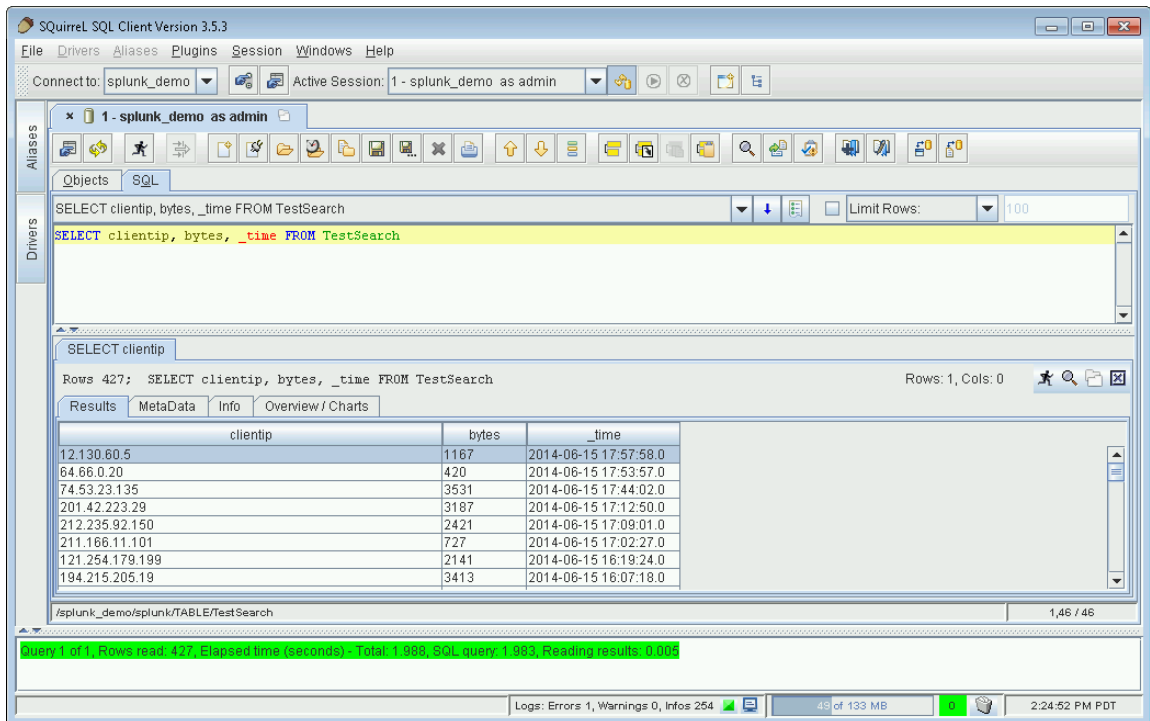
Drivers: splunk\_demo > splunk > TABLE

Info	Content	Row Count	Columns	Primary Key	Exported Keys
COLUMN_NAME	TYPE_NAME	IS_NULLABLE	DECIMAL_DIGITS	COLUMN_SIZE	COLUMN_USAGE REMARKS DATA_TYPE BUFFER_LENGTH
JSESSIONID	VARCHAR	0	10000000	<null>	12 <null>
action	VARCHAR	0	10000000	<null>	12 <null>
bytes	INTEGER	0	10	<null>	4 <null>
clientip	VARCHAR	0	10000000	<null>	12 <null>
cookie	VARCHAR	0	10000000	<null>	12 <null>
date_hour	INTEGER	0	10	<null>	4 <null>
date_mday	INTEGER	0	10	<null>	4 <null>
date_minute	INTEGER	0	10	<null>	4 <null>
date_month	VARCHAR	0	10000000	<null>	12 <null>
date_second	INTEGER	0	10	<null>	4 <null>
date_wday	VARCHAR	0	10000000	<null>	12 <null>
date_year	INTEGER	0	10	<null>	4 <null>
date_zone	VARCHAR	0	10000000	<null>	12 <null>
eventtype	VARCHAR	0	10000000	<null>	12 <null>
file	VARCHAR	0	10000000	<null>	12 <null>
host	VARCHAR	0	10000000	<null>	12 <null>
ident	VARCHAR	0	10000000	<null>	12 <null>
index	VARCHAR	0	10000000	<null>	12 <null>

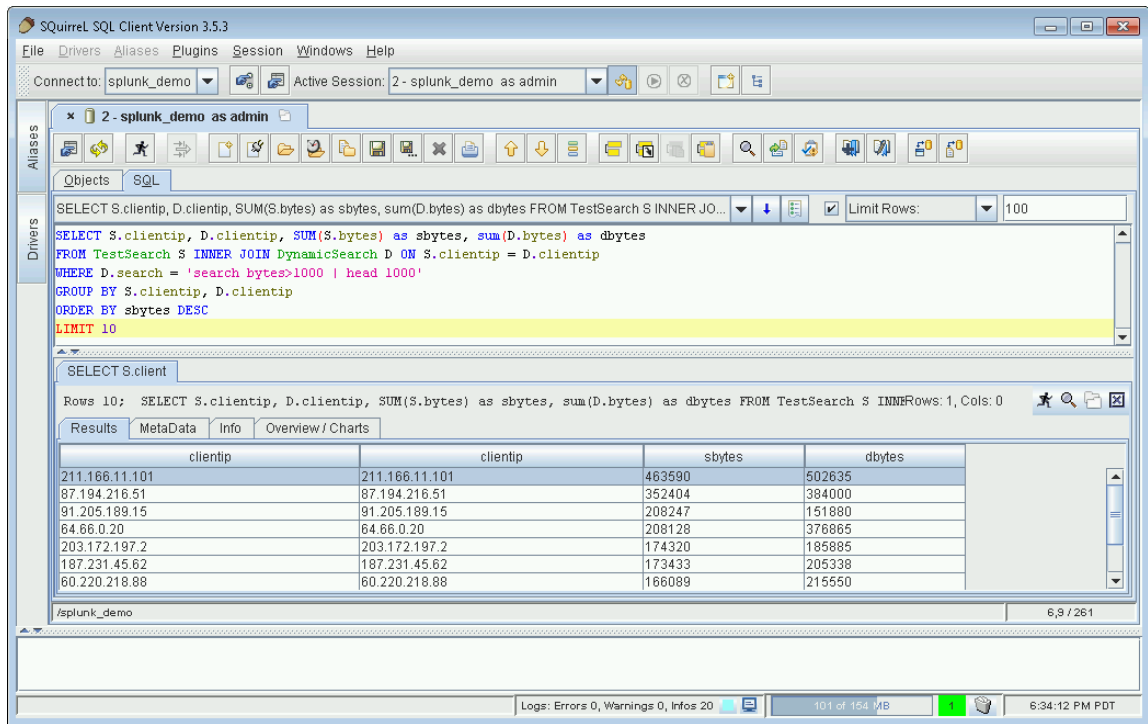
Logs: Errors 1, Warnings 0, Infos 183 49 of 132 MB 2:22:16 PM PDT

13. Click the **SQL** tab to enter queries. Click **Run**  to run a query. Here are two example queries. The first query queries a single table and runs completely on Splunk. The number of results on all queries is limited to 100 rows. The second query uses a join that requires UnityJDBC. Note that DynamicSearch is a virtual table that supports a filter on the attribute **search** which can be any Splunk search query. The trial version is limited to returning 100 rows. Upgrade to a full version at [www.unityjdbc.com](http://www.unityjdbc.com) for an unlimited number of rows. More details on querying is at: [http://www.unityjdbc.com/splunk/splunk\\_jdbc.php](http://www.unityjdbc.com/splunk/splunk_jdbc.php)

<b>Query #1</b>	<code>SELECT clientip, bytes, _time FROM TestSearch</code>
<b>Query #2</b>	<code>SELECT S.clientip, D.clientip, SUM(S.bytes) as sbytes, SUM(D.bytes) as dbytes FROM TestSearch S INNER JOIN DynamicSearch D ON S.clientip = D.clientip WHERE D.search = 'search bytes&gt;1000   head 1000' GROUP BY S.clientip, D.clientip ORDER BY sbytes DESC LIMIT 10</code>







**Notes:**

- 1) The driver automatically switches to export jobs (with JSON output) if it cannot guarantee that the number of results returned is less than 50,000 (or a user configured amount by setting the parameter **maxcsvrows** in the URL connection string). CSV exports are used for smaller jobs for faster performance.
- 2) Adding the URL parameter **debug=true** will produce more information on query execution. This information can be seen in the Squirrel log by selecting **View Squirrel Logs** from the **Windows** menu.