## Splunk JDBC and UnityJDBC Driver Setup for SQuirreL SQL

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

🕽 🌍 🗢 🕌 < Local Disk (C:) 🕨 Pi	ogram Files 🕨 UnityJDBC 🕨	▼ 4	Search Uniț	yJDBC		
Organize 🔻 🏼 🛃 Open 👻 Bu	rn New folder			- - -	•	0
Name	Date modified	Туре	Size			
🐌 code	6/12/2014 2:42 PM	File folder				
퉬 drivers	5/26/2014 11:34 AM	File folder				
鷆 lib	5/26/2014 11:34 AM	File folder				
퉬 sampleDB	5/26/2014 11:34 AM	File folder				
퉬 Uninstaller	5/26/2014 11:35 AM	File folder				
鷆 webserver	5/26/2014 11:35 AM	File folder				
📄 .installationinformation	7/5/2014 12:44 PM	INSTALLATIONIN	5 KB			
🚳 initsources.bat	5/26/2014 9:40 AM	Windows Batch File	1 KB			
🚳 initsources.sh	5/26/2014 9:40 AM	Shell Script	1 KB			
📄 README.txt	6/2/2014 10:39 AM	TXT File	9 KB			
👜 unityjdbc.jar	7/5/2014 12:44 PM	Executable Jar File	1,222 KB			
UnityJDBCDoc.pdf	5/26/2014 11:14 AM	PDF File	1,460 KB			

 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.

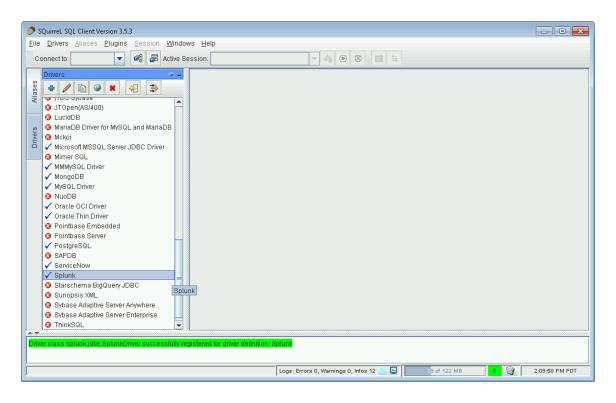
🗸 🗸 🗸 🗸 Local Disk (C:) 🕨 Pro	gram Files 🕨 squirrel-sql-3.5.3	3 ▶ lib 👻 🖣	Search lib	
Organize 🔻 🏼 🛃 Open 🔻 Burr	New folder			III 🔻 🗔 🔞
Name	Date modified	Туре	Size	
🔟 spring-beans.jar	5/11/2014 12:33 PM	Executable Jar File	468 KB	
📓 spring-context.jar	5/11/2014 12:33 PM	Executable Jar File	455 KB	
📓 spring-context-support.jar	5/11/2014 12:33 PM	Executable Jar File	91 KB	
🔳 spring-core.jar	5/11/2014 12:33 PM	Executable Jar File	276 KB	
📧 squirrel-sql.jar	5/11/2014 12:33 PM	Executable Jar File	2,183 KB	
🔳 stringtemplate.jar	5/11/2014 12:33 PM	Executable Jar File	225 KB	
🔟 swing-worker.jar	5/11/2014 12:33 PM	Executable Jar File	13 KB	
📧 treetable.jar	5/11/2014 12:33 PM	Executable Jar File	35 KB	
🔟 unityjdbc.jar	7/5/2014 12:44 PM	Executable Jar File	1,222 KB	
📧 versioncheck.jar	5/11/2014 12:33 PM	Executable Jar File	2 KB	
📧 x86.jar	5/11/2014 12:33 PM	Executable Jar File	1,952 KB	
🛋 xml-apis.jar	5/11/2014 12:33 PM	Executable Jar File	107 KB	

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

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

🥭 Add Driver 💽
Add Driver
Driver
Name: Splunk
Example URL: jdbc:splunk://localhost:8089
Website URL: http://www.unityjdbc.com
Java Class Path Extra Class Path
C:\Program Files\squirrel-sql-3.5.3\squirrel-sql.jar C:\Program Files\squirrel-sql-3.5.3\lib\antlr.jar C:\Program Files\squirrel-sql-3.5.3\lib\asm-attrs.jar C:\Program Files\squirrel-sql-3.5.3\lib\asm.jar C:\Program Files\squirrel-sql-3.5.3\lib\axis-jaxrpc.jar C:\Program Files\squirrel-sql-3.5.3\lib\axis-jaxrpc.jar C:\Program Files\squirrel-sql-3.5.3\lib\axis-saaj.jar C:\Program Files\squirrel-sql-3.5.3\lib\axis-wsdl4j.jar C:\Program Files\squirrel-sql-3.5.3\lib\axis.jar
Class Name: splunk.jdbc.SplunkDriver
OK Close

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).

🥭 GI	lobal Preference	5								×
S	QL formatting	DB Copy	DB Diff	L&F	Fonts R	efactori	ng Bookmarks	SQL Scripts	1	
	General		SQL		Proxy		Data	Type Controls		Wiki Table
L - C ( ( J	eneral .ogin Timeout ( .arge Script Sta Debug O No Debug JDBC Debug DBC Debug Fil	tement Cou g to Output s g to Writer	Stream	]	eans unlimit .5.3\.squirre		gs\jdbcdebug.log			
	Open in prev	vious directo	ory							
	🔾 Open in spe	cified direct	ory							
						OK	Close			

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:

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

🥭 Add Alias		×
Add Alias		
Name:	splunk_demo	
Driver:	✓ Splunk 💌 New	
URL:	jdbc:splunk://localhost:8089	
User Name:	admin	
Password:	•••••	
🔲 Auto logon	Connect at Startup	
	Properties	
Warning - Pass	words are saved in clear text	
	OK Close Test	

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.

o: splunk_demo 🛛 🔀					
splunk_demo					
splunk_demo					
Splunk					
jdbc:splunk://localhost:8089					
User: admin					
💣 Properties					
aps lock may interfere with passwords					
Connect Close					

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

-	SQuirreL SQL Client Version 3.5.3
<u>F</u> ile	
S C	onnect to: splunk_de 🔽 🦓 👼 Active Session: 1 - splunk_demo as admin 🔍 <table-cell> 🕑 🖄 🛅 🗔</table-cell>
	× 1 1-splunk_demo as admin
Aliases	Image: State in the state i
	Objects SQL
	select number, caller_id, opened_at, opened_by, S.first_name, S.last_name from incident I INNER JOIN sys_u 💌 🕴 📳 🗹 Limit Rows: 🖤 100
Drivers	
ō	
	/splunk_demo 1,1/1
	er class splunk.jdbc.SplunkDriver successfully registered for driver definition: Splunk
Plea	ase try out the Tool's popup by hitting ctri+t in the SQL Editor. Do it three times to stop this message.
	Logs: Errors 0, Warnings 0, Infos 12 📃 📮 🚺 34 of 126 MB 🛛 🍟 2:14:36 PM PDT

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

Co	nnect to: Splunk_demo 💌 🕼 慮 Active Session	n: 1 - splunk_demo as admin 💌 👌 🕞 😫					
Aliases	× 1) 1 - splunk_demo as admin C						
	Q.7						
Drivers	ዮ 🗐 splunk_demo	Metadata Status Schemas Table Ty	/pes Data Types Numeric Functions				
5	🛉 🗟 splunk	Property Name	Value				
🛉 🥐 🧱 TABLE	JDBC Driver CLASSNAME	splunk.idbc.SplunkDriver					
	- 🛄 DynamicSearch	JDBC Driver CLASSPATH	No files specified in 'Extra ClassPath' tab for driver idbc:splunk://localhost.8089				
	Errors in the last 24 hours	getURL					
	<ul> <li>Errors in the last hour</li> </ul>	isReadOnly	true				
	<ul> <li>Indexing workload</li> <li>License Usage Data Cube</li> <li>Messages by minute last 3 hours</li> </ul>	getUserName	admin				
		supportsCatalogsInTableDefinitions	false				
	<ul> <li>Big messages by minute last 3 hours</li> <li>Splunk errors last 24 hours</li> </ul>	supportsSchemasInTableDefinitions	false				
	- III TestSearch	getDriverName	SplunkJDBC				
	- Top five sourcetypes	getCatalogSeparator					
	VIP Customer	storesMixedCaseIdentifiers	false false Splunk				
	- idx audit	storesUpperCaseIdentifiers					
	- internal	getDatabaseProductName					
	idx main	getDatabaseProductVersion	0.2				
		getDatabaseMajorVersion	0				
		getIdentifierQuoteString	" true				
		supportsSchemasInDataManipulation					
		supportsStoredProcedures	false -				
		<b>▲</b>					
	/splunk demo		1,1/1				
	/sprank_demo		1,171				
****							
eas	se try out the Tools popup by hitting ctrl+t in the SQL Ed	tor. Do it three times to stop this message.					

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

201	nnect to: splunk_demo 🔽 🥔 👼 Active Session	n: 1 - splunk_demo as admin	🔻 🐴 🕞	8 📑 E				
	× 🗍 1 - splunk_demo as admin 🕒							
				a 📬 🔍	2 3 4 🕅	E0 E0		
	Objects SQL							
١	0,7	Imported Keys Indexes	Privileges C	olumn Privileg	es Row IDs Vers	ions		
	♀	Info Content	Row Count	Colu	imns Primar	v Kev	Expo	rted Keys
				tute a	· · · · · · · · · · · · · · · · · · ·			
	- m TABLE	JSESSIONID	action	bytes	clientip	cookie		date_mda
	🕂 🔠 DynamicSearch	SD5SL6FF7ADFF53001	purchase	1167	12.130.60.5		17	15
	Errors in the last 24 hours	SD6SL4FF1ADFF52990	purchase	420	64.66.0.20		17	15
	Errors in the last hour	SD8SL10FF9ADFF52956	purchase	3531	74.53.23.135		17	15
	— Indexing workload	SD0SL9FF7ADFF52798	purchase	3187	201.42.223.29		17	15
	– 🧮 License Usage Data Cube	SD3SL5FF5ADFF52775	purchase	2421	212.235.92.150		17	15
	— 🔣 Messages by minute last 3 hours	SD10SL4FF2ADFF52743	purchase	727	211.166.11.101		17	15
	– 🧮 Splunk errors last 24 hours	SD5SL5FF8ADFF52479	purchase	2141	121.254.179.199		16	15
Drivers	- 🛄 TestSearch	SD3SL3FF10ADFF52417	purchase	3413	194.215.205.19		16	15
	<ul> <li>Top five sourcetypes</li> </ul>	SD9SL2FF4ADFF52361	purchase	623	27.35.11.11		15	15
	- 🖽 VIP Customer	SD2SL10FF4ADFF52352	purchase	640	222.41.213.238		15	15
	— 🧮 idx audit	SD1SL9FF1ADFF52322	purchase	518	175.44.24.82		15	15
	- 🧮 idx internal	SD5SL6FF6ADFF52150	purchase	2297	203.172.197.2		15	15
	idx main	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
			nurchaea	1261	len 220 210 00		1.4	15
I								
	/splunk_demo/splunk/TABLE/TestSearch							1,171
L	/splunk_demo/splunk/IABLE/lestSearch						J	1,171

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

:	nnect to: splunk_demo 💌 🧟 😹 Active Session	n: 1 - splunk_d	emo as adm	nin 🔻 🤞		3 8					
Aliases	× 1) 1 - splunk_demo as admin 🕤 all 🌮 🖈 🏝 🖬 🖬 🗗 🕹 🗞 11 Objects SQL				<b>T</b>	Q 21 2	) III ()		F D		
	Q.7	Imported Ke	eys Indexe	es Privilea	es   Column Pr	ivileges Ro	w IDs Ver	sions			
ers	♀	Info	Content	Row	Count	Columns	Prima	ary Key	E	xported Keys	
Drivers aid aid aid aid aid aid aid aid		COLUMN	TYPE_N	IS_NULLA	DECIMAL DIGI	. COLUMN	COLUMN	REMA	DATA T	BUFFER_LE	-
	<b>P</b> ■ TABLE	JSESSIONID			DECIMAL_DIGI	10000000	<null></null>		12	<pre><null></null></pre>	
-	<ul> <li>— III DynamicSearch</li> </ul>	action	VARCHAR		0	10000000	<null></null>		12	<null></null>	Ŧ
	Errors in the last 24 hours	bytes	INTEGER		0	10	<null></null>		4	<null></null>	-
Conner satur Conversion Conversio	Errors in the last hour     Indexing workload     Errors Usage Data Cube	clientip	VARCHAR		0	10000000	<null></null>		12	<null></null>	
		cookie	VARCHAR		0	10000000	<null></null>		12	<null></null>	۲
		date hour	INTEGER		0	10	<null></null>		4	<null></null>	-
	<ul> <li>Messages by minute last 3 hours</li> </ul>	date_mday	INTEGER		0	10	<null></null>		4	<null></null>	
	<ul> <li>— Esplunk errors last 24 hours</li> </ul>		INTEGER		0	10	<null></null>		4	<null></null>	1
	TestSearch		VARCHAR		0	10000000	<null></null>		12	<null></null>	1
	Top five sourcetypes     VIP Customer	date_second	INTEGER		0	10	<null></null>		4	<null></null>	1
	- idx_audit	date_wday	VARCHAR		0	10000000	<null></null>		12	<null></null>	1
	- idxaudit	date_year	INTEGER		0	10	<null></null>		4	<null></null>	1
	idxiidx	date_zone	VARCHAR		0	10000000	<null></null>		12	<null></null>	1
		eventtype	VARCHAR		0	10000000	<null></null>		12	<null></null>	1
		file	VARCHAR		0	10000000	<null></null>		12	<null></null>	
		host	VARCHAR		0	10000000	<null></null>		12	<null></null>	1
		ident	VARCHAR		0	10000000	<null></null>		12	<null></null>	
		indov	MADOUAD		0	110000000	znulls		12	enulls	_
											1
	/splunk_demo/splunk/TABLE/TestSearch									1,171	
_											

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 for an unlimited number of rows. More details on querying is at: http://www.unityjdbc.com/splunk/splunk\_jdbc.php

Query #1	SELECT clientip, bytes, _time FROM TestSearch
Query #2	SELECT S.clientip, D.clientip, SUM(S.bytes) as sbytes, SUM(D.bytes) as dbytes
	<pre>FROM TestSearch S INNER JOIN DynamicSearch D</pre>

Ø s	QuirreL SQL Client Version 3.5.3											
File	Elle Drivers Aliases Plugins Session Windows Help											
Connect to: splunk_demo 🔻 🥰 🖉 Active Session: 1 - splunk_demo as admin 🔻 🍖 🗵 📑												
	a 1 - splunk_demo as admin 🖻											
Aliases												
	Qbjects SQL											
	SELECT clientip, bytes, _time FROM TestSearch			<b>-</b> +	🗄 🔲 Limit Rows:	▼ 100						
Drivers	SELECT clientip, bytes, _time FROM TestSearch											
Ē												
	A.7											
	SELECT clientip											
	Rows 427; SELECT clientip, bytes, _time FROM Te	stSearch			Rows:	1, Cols: 0	* 🔍 🖻 🗵					
	Results MetaData Info Overview / Charts											
	clientip	bytes	_time									
	12.130.60.5	1167	2014-06-15 17:57:58.0									
	64.66.0.20	420	2014-06-15 17:53:57.0				- III					
	74.53.23.135	3531	2014-06-15 17:44:02.0									
	201.42.223.29	3187	2014-06-15 17:12:50.0									
	212.235.92.150	2421	2014-06-15 17:09:01.0									
	211.166.11.101	727	2014-06-15 17:02:27.0									
	121.254.179.199	2141	2014-06-15 16:19:24.0									
	194.215.205.19	3413	2014-06-15 16:07:18.0				-					
		-										
	/splunk_demo/splunk/TABLE/TestSearch						1,46 / 46					
A.7.												
Que	y 1 of 1, Rows read: 427, Elapsed time (seconds) - Total: 1.988,	SQL query: 1.	983, Reading results: 0.005									
		r										
			Logs: Errors 1, Warnings 0, Infos	\$ 254 📕 🚍	49 of 133 MB	•	2:24:52 PM PDT					

	SQL Client Version 3.5.3				- • •						
<u>File</u> Driver	<u>Elle D</u> rivers Aliases <mark>Plugins <u>S</u>ession Windows Help</mark>										
Connect to	to: splunk_demo 💌 🔗 🛃 Active Ses	sion: 2 - splunk_demo as admin 🛛 💌 🖓	• • •								
	🗙 🗍 2 - splunk_demo as admin 🕒										
AI											
SELE	SELECT S.clientip, D.clientip, SUM(S.bytes) as sbytes, sum(D.bytes) as dbytes FROM TestSearch S INNER JO 👻 🖡 🛐 🗹 Limit Rows: 💌 100										
FROM WHERE GROUP	CT S.clientip, D.clientip, SUM(S.by TestSearch S INMER JOIN DynamicSea E D.search = 'search bytes>1000   h P BY S.clientip, D.clientip R BY Sbytes DESC		<b>_</b>								
LIMIT											
A. 7											
Rows	estSearch S INNERows:1,Co	ls:0 🖈 🔍 🖻 🗵									
1100	sults MetaData Info Overview / Cha	110									
1100		1	sbytes	dbytes							
Í	clientip	clientip	sbytes 463590	dbytes							
211.1		1	sbytes 463590 352404	dbytes 502635 384000							
211.1 87.19	clientip 166.11.101	clientip 211.166.11.101	463590	502635							
211.1 87.19	clientip 166.11.101 94.216.51 05.189.15	clientip 211.166.11.101 87.194.216.51	463590 352404	502635 384000							
211.1 87.19 91.20 64.66	clientip 166.11.101 94.216.51 05.189.15	clientip 211.166.11.101 87.194.216.51 91.205.189.15	463590 352404 208247	502635 384000 151880							
211.1 87.19 91.20 64.66 203.1	clientip 166.11.101 94.216.51 05.189.15 6.0.20	clientip 211.166.11.101 87.194.216.51 91.205.189.15 64.66.0.20	463590 352404 208247 208128	502635 384000 151880 376865							
211.1 87.19 91.20 64.66 203.1 187.2	clientip 166.11.101 94.216.51 05.189.15 6.0.20 172.197.2	clientip 211.166.11.101 87.194.216.51 91.205.189.15 64.66.0.20 203.172.197.2	463590 352404 208247 208128 174320	502635 384000 151880 376865 185885							
211.1 87.19 91.20 64.66 203.1 187.2 60.22	clientip 166.11.101 94.216.51 05.189.15 6.0.20 172.197.2 231.45.62 20.218.88	clientip 211.166.11.101 87.194.216.51 91.205.189.15 64.66.0.20 203.172.197.2 187.231.45.62	463590 352404 208247 208128 174320 173433	502635 384000 151880 376865 185885 205338							
211.1 87.19 91.20 64.66 203.1 187.2 60.22	clientip 166.11.101 94.216.51 05.189.15 6.0.20 172.197.2 23.45.62	clientip 211.166.11.101 87.194.216.51 91.205.189.15 64.66.0.20 203.172.197.2 187.231.45.62	463590 352404 208247 208128 174320 173433	502635 384000 151880 376865 185885 205338							
211.1 87.19 91.20 64.66 203.1 187.2 60.22	clientip 166.11.101 94.216.51 05.189.15 6.0.20 172.197.2 231.45.62 20.218.88	clientip 211.166.11.101 87.194.216.51 91.205.189.15 64.66.0.20 203.172.197.2 187.231.45.62	463590 352404 208247 208128 174320 173433	502635 384000 151880 376865 185885 205338							
211.1 87.19 91.20 64.66 203.1 187.2 60.22	clientip 166.11.101 94.216.51 05.189.15 6.0.20 172.197.2 231.45.62 20.218.88	clientip 211.166.11.101 87.194.216.51 91.205.189.15 64.66.0.20 203.172.197.2 187.231.45.62	463590 352404 208247 208128 174320 173433	502635 384000 151880 376865 185885 205338							
211.1 87.19 91.20 64.66 203.1 187.2 60.22	clientip 166.11.101 94.216.51 05.189.15 6.0.20 172.197.2 231.45.62 20.218.88	clientip 211.166.11.101 87.194.216.51 91.205.189.15 64.66.0.20 203.172.197.2 187.231.45.62	463590 352404 208247 208128 174320 173433	502635 384000 151880 376865 185885 205338							
211.1 87.19 91.20 64.66 203.1 187.2 60.22	clientip 166.11.101 94.216.51 05.189.15 6.0.20 172.197.2 231.45.62 20.218.88	clientip 211.166.11.101 87.194.216.51 91.205.189.15 64.66.0.20 203.172.197.2 187.231.45.62	463590 352404 208247 208128 174320 173433 166089	502635 384000 151800 376865 185885 205338 215550							

## Notes:

- 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.
- 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.